KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

KİŞİSEL VERİLERİN KORUNMASINA
UZMAN BAKIŞ

Uzmanlık Tezleri Derleme Çalışması

KİŞİSEL VERİLERİN KORUNMASINA

UZMAN BAKIŞ

UZMANLIK TEZLERİ DERLEME ÇALIŞMASI

Adres: Nasuh Akar Mahallesi
1407. Sokak No:4
Balgat Çankaya/ANKARA

Bu çalışmada yer alan fikir ve görüşler
Kurumumuz görüşünü yansıtmamakta olup
yazarların görüşlerini yansıtmaktadır.

KVKK KİŞİSEL VERİLERİ KORUMA KURUMU

Kişisel Verileri Koruma Kurumu Adına İmtiyaz Sahibi
Prof. Dr. Faruk BİLİR

Editörler
Pınar ÇAĞLAYAN AKSOY
Hüseyin Can AKSOY

KVKK Yayınları No
44

ISBN: 978-605-72485-1-0
Aralık 2023

Tasarım & Mizanpaj
Ütopya Grafik
Çetin Emeç Bulvarı No:21/25 Çankaya/ANKARA
Tel: 0(312) 481 51 53 Faks: 0(312) 481 50 80
www.utopyagrafik.com

Basım Yeri
Arkadaş Basım ve Sanayi Ltd. Şti.
Macun Mahallesi 204 Cadde No: 141/A-3
Yenimahalle/ANKARA

SUNUŞ

Kişisel verilerin korunması, temel hak ve özgürlüklerin güvence altına alınmasında ve geliştirilmesinde bireylere hukuk düzeni içerisinde koruma sağlayan araçlardan biridir. Kişisel verilerin korunması, verilerin gerekli önlemler alınmak suretiyle hukuka aykırı kullanımının önüne geçilmesi ile bireylerin mahremiyetlerinin korunması amacına hizmet etmektedir. Bununla birlikte kişisel verilerin korunması, teknolojik ilerlemenin insan haklarına uyumlu olması için vazgeçilmez bir unsurdur.

Günümüzde teknolojik gelişmeler sayesinde kişisel verilerin işlendiği faaliyet alanları ciddi biçimde artış göstermekte, bu nedenle kişisel verilerin korunması her geçen gün daha da önem kazanmaktadır. Bu duruma bağlı olarak kişisel verilerin korunmasına ilişkin konularda yeni yaklaşımların ortaya koyulması ve bu yönde akademik çalışmaların yayımlanması oldukça önem taşımaktadır.

Kişisel verilerin korunmasıyla ilgili akademik çalışmalar; 6698 sayılı Kanun'un daha iyi anlaşılmasına yardımcı olmakta, teknolojik gelişmelerin kişisel verilerin korunmasına olan etkilerini değerlendirmekte, ortaya çıkan soruları ele alarak çözüme yönelik fikirler üretmektedir. Öte yandan bu tür çalışmalar, gelecekteki veri koruma stratejilerini belirlemek için temel oluşturabilecek potansiyele sahiptir.

Bu itibarla Kurumumuz farkındalık ve bilgilendirme çalışmalarının yanı sıra akademik çalışmalara da önem vermekte ve bu kapsamda çalışmalar yapmaktadır. "Kişisel Verilerin Korunmasına Akademik Bakış", "Kişisel Verileri Koruma Dergisi" çalışmaları ile Kurumumuz tarafından ulusal ve uluslararası nitelikte gerçekleştirilen kongre, zirve ve konferansları buna örnek olarak göstermek mümkündür.

"Kişisel Verilerin Korunmasına Uzman Bakış: Uzmanlık Tezleri Derleme Çalışması" ile bu hususta yaptığımız çalışmaların yeni bir boyut kazanacağına inanıyorum. Çalışma temel olarak kişisel verilerin korunması konusunun akademik açıdan ele alınmasına katkı sunmayı amaçlamaktadır. Ayrıca bu çalışma, okuyucuların farklı disiplinler arasındaki bağlantıları keşfetmelerine imkan tanıyacaktır.

Çalışmaya emek veren herkese teşekkür ediyor, tüm ilgililere faydalı olmasını diliyorum.

Prof. Dr. Faruk BİLİR
Kurum Başkanı

İÇİNDEKİLER

Haluk Odabaşıoğlu	Kişisel Verilerin İşlenmesinde Amaç Odaklı Bakış: Ölçülülük İlkesi	11
Abdullah Halis Şahin	Yapılandırılmamış Verilerin Anonim Hale Getirilmesi	41
Göksu Hazar Erdinç	Karşılaştırmalı Avrupa Birliği ve Türkiye Uygulamaları: Yurt Dışına Veri Aktarımı Yöntemi Olarak Standart Sözleşme Hükümleri ve Taahhütname	53
Kazım Alper Daştan	İlgili Kişilerin Kişisel Verilerine Erişim Hakları	87
Uğur Tokmakcı	Kişisel Verilerin Korunmasında Risk Temelli Yaklaşım	117
Arif Onur Küçükbasmacı	Kişisel Verilerin Kaydedilmesi Suçu ve 6698 sayılı Kanundaki Kabahatlerin Suçlar Karşısındaki Konumu	137
Mahsum Gönen	Kabahatler Kanunu Kapsamında 6698 Sayılı Kişisel Verilerin Korunması Kanunu'ndaki İdari Yaptırımlar	159
Amine Gülümser	Kişisel Verilerin Korunması Kanunu Bakımından "Non Bis In Idem" İlkesinin Değerlendirilmesi	177
Mustafa Koray Altun	Kişisel Verileri Koruma Kurulu'nun Mevzuat Taslakları Hakkında Görüş Verme Yetkisi	213
Reyhan Karcı	Ulusal Hukukta Kişisel Verilerin Korunması Hakkına İlişkin İstisnai Haller	243
Safiye Pergel Maşacıoğlu	İstatistiksel Amaçlar Doğrultusunda Kişisel Verilerin İşlenmesi	303
Rifat Karatay	Kolluğun Önleyici Faaliyetler Kapsamında Kişisel Veri İşlemesi	329
Tülay Selin Güner	Bir Hak Çatışması Alanı Olarak Kişisel Verilerin Korunması ve Basın Özgürlüğü	363
Burak Özer	Bir Sorumluluk Şekli Olarak Ortak Veri Sorumluluğu	393
Mert Varol	Mahremiyet Korumalı Veri Paylaşımı ve Açık Veri	415
Begüm Tuğçe Burhan	Yapay Zekâ Sistemlerinde Veri Koruma Yaklaşımları	429
Büşra Yılmaz	Nesnelerin İnterneti (IOT) Uygulamalarında Kişisel Veri Güvenliği ve Mahremiyet	445
Sefer Aktaş	Bulut Bilişim Ortamlarında Kişisel Veri Güvenliği Tedbirleri	467
Hande Öztürk	Veri Koruma Hukuku Açısından Blok Zincir Teknolojisine Bakış	487
Şükran Koçak	Kişisel Verilerin Korunması Açısından Dijital Parmak İzi	517
Neslihan Koçak	Elektronik Sözleşmeler Kapsamında Kişisel Veri İşleme Faaliyeti ve Veri Sorumlusunun Yükümlülükleri	571
Yeliz Yılmaz	Çerezler ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Uygulanması	599
Meryem Betül Muratoğlu	Hedefli Reklamcılık Uygulamalarının Kişisel Verilerin Korunması Hukuku Açısından Değerlendirilmesi	643
Tuğçe Arıcı Şirin	İş Yönetimi ve Planlaması Çerçevesinde Kişisel Verilerin İşlenmesi	677

Gökalp Yavuz	Küçük ve Orta Büyüklükteki İşletmelerin Veri Koruma Hukukuna Uyumu Sürecinde Davranış Kuralları Mekanizması	715
Atakan Yalçın	Avrupa Birliği Genel Veri Koruma Tüzüğünde Hesap Verilebilirlik Araçları	751
İrem Özdil Altak	Avrupa Birliği Veri Koruma Hukukunda Bağlantılı Otomobillere İlişkin Uygulamalar	769

KİŞİSEL VERİLERİN İŞLENMESİNDE AMAÇ ODAKLI BAKIŞ: ÖLÇÜLÜLÜK İLKESİ

Haluk ODABAŞIOĞLU

Kişisel Verileri Koruma Uzmanı

"Bu çalışma, 14.02.2023 tarihinde kabul edilen "Kişisel Verilerin İşlenmesinde Amaç Odaklı Bakış: Ölçülülük İlkesi" başlıklı uzmanlık tezinden alınmıştır."

GİRİŞ

Teknolojik gelişmelerin yaşanması ve bu gelişmelerle iç içe olan insan sayısının her geçen gün artmasıyla birlikte kişisel verinin de önemi yadsınamaz bir hal almıştır. Kişisel verinin niceliğinin artmasının yanında niteliği de daha çeşitlenmekte olup bu durum da insanların mahremiyetinin önemini ve teknolojinin getirdiği riskleri her geçen gün artırmaktadır.

Bu itibarla, kişisel verilerin korunmasına ve işlenmesine verilen önem de gün geçtikçe artmakta ve bunun için yasal düzenlenmelere ihtiyaç duyulmaktadır. Bu kapsamda ülkemizde de 2016 yılında yürürlüğe giren "6698 sayılı Kişisel Verilerin Korunması Kanunu" (6698 sayılı Kanun / Kanun) ve tüm dünyadaki mevcut düzenlemelerle kişisel verilerin korunması yasal bir zemine oturmuştur.

Kişisel verilerin işlenmesine verilen öneme binaen tüm kişisel veri işleme faaliyetlerinde uyulması gereken genel ilkelere, ulusal ve uluslararası düzenlemelerde yer verilerek genel ilkelerin kişisel veri işleme faaliyetindeki önemi fazlasıyla vurgulanmıştır. Bu ilkeler hem birbirinin tamamlayıcısı hem de her biri bu disiplinin olmazsa olmazıdır. Bu noktada bu ilkelerin en önemlilerinden biri olan

"ölçülülük ilkesi" ön plana çıkmaktadır.

6698 sayılı Kanun'da;

> *"Genel İlkeler" başlıklı 4'üncü maddesinde, kişisel verilerin ancak bu Kanun'da ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra 4 üncü maddenin ikinci fıkrasının (ç) bendinde geçen ifade "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma"*

ifadesi yer almaktadır.

Dolasıyla kişisel veriler, ancak "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü" olmak şartıyla işlenebilmektedir.

Ölçülülük ilkesi, 6698 sayılı Kanun'da olduğu gibi uluslararası mevzuatta da farklı şekillerde tanımlansa da çoğunda aynı hususlara değinilmektedir.

Anayasa'da ölçülülük ilkesi, büyük öneme haiz bir ilke olup alt ögeleriyle birlikte değerlendirilmiştir. Bu ilkeler de yine birbirinin tamamlayıcısı olup her biri kendi içinde bir bütünlük içermektedir.

Bu çerçevede, çalışmamızda Kişisel Verileri Koruma Kurulu (Kurul) Kararları ve uluslararası kararlar ve düzenlemeler çerçevesinde ölçülülük ilkesi incelenmiş olup, söz konusu ilkenin kişisel verilerin işlenmesindeki önemi ön plana çıkarılmaya çalışılacaktır.

ÖLÇÜLÜLÜK İLKESİ VE ÖNEMİ

Hukukun Temel İlkelerinin Önemi

İlke; *"herhangi bir bilgi düzeninde en genel ve en önemli gerçektir. Açıkça ortaya konmuş olan ve uygulanması gereken faaliyet kuralıdır"* (Meydan Larousse, 1971, s. 276).

Anayasa Mahkemesi'nin 10/06/1971 tarih ve 24/55 sayılı Kararı'nda

> *"Anayasa ilkeleri etki ve değer bakımından eşit olup, hangi nedenle olursa olsun birinin ötekisine üstün tutulması mümkün olmadığından, bunların bir arada birbirine getirdiği sınırlamalar içerisinde ve hukukun genel kuralları da göz önünde bulundurulmak suretiyle uygulanmaları zorunludur"*

ifadesiyle hukukun genel ilkelerine anayasal bir değerde yer verilmiştir (Bereket, 1994, s. 10)

Hukukun temel ilkeleri kavramında yer alan temel, genel ibaresi, söz konusu ilkelerin evrensel ve genel nitelikte olduğunu ifade etmektedir. Hukukun temel ilkeleri tüm insanlığın kabul edebileceği, yaygın üst normları teşkil etmektedir. Diğer bir deyişle, "hukukun gelişmesi", ancak bu özellikleri (genel, sürekli, üstün ve evrensel) taşıyan hukuk ilke ve normlarıyla gerçekleşebilir (Akıl, 2003, s. 394).

Alain Serge Mescharіakoff, hukukun genel ilkelerini;

> *"felsefi, ahlaki, sosyolojik ve ekonomik alanda ortaklaşa biçimde benimsenen kavramların hukuk dilindeki anlatımı olarak"*

tanımlamaktadır (Mescharіakoff, 1976, s. 596).

İbrahim Kaboğlu ise;

> *"çok sayıda somut durumu içine alan ve her somut durumu daha da bütüncü bir biçimde düzenleyen birçok özel norma temel oluşturan hukuk normlarını hukukun genel ilkeleri olarak"*

tanımlamıştır (Kaboğlu, 2002, s. 292).

"Hangi devirde olursa olsun, nereye gidilirse gidilsin bulunulabilen ve değişmeyen ilkelerdir" tanımı ile hukukun temel ilkelerinin değişmez olduğu ortaya konmuştur. Anayasa ile tanınan bir hakkın, konusunun, niteliğinin ve kapsamının belirlenmesinde özgürlükler için güvence olması sebebiyle hukukun genel ilkelerine ihtiyaç duyulmalıdır (Esen, 1972, s. 372, 380).

Hukukun genel ilkeleri, toplumsal bir ihtiyaca, ortak adalet duygusuna dayanır. Hukukun temel ilkeleri hukuki düşüncenin ana çatısını oluşturur ve kanunun yorumlanmasında öncelikli bir payı vardır. Muğlak ve anlaşılamayan kanuni metinlerin yorumu için de genel ilkelere ihtiyaç duyulmaktadır (Kaboğlu, 2002, s. 295-296).

Herhangi bir ülkenin veya uluslararası kuruluşun bir konuya ilişkin yürürlüğe soktuğu yasal düzenlemelerinde kabul ettiği ilkeler, o ülkenin veya kuruluşun veri koruma hukukuna olan bakış açısını da ortaya koymaktadır. Bu ilkelerin içeriğinin, amacının düzenleme biçiminin irdelenmesiyle bahsi geçen düzenlemeyle

nasıl ve hangi ölçüde veri korumasının sağlanmaya çalışıldığı ve veri koruma hukukunda ulaşılmak istenen amaç anlaşılabilmektedir (Dülger, 2019a, s. 108).

Danıştay 12'nci Dairesinin 19/3/1989 tarihli Kararında;

> *"...Anayasa ve yasa metinleri kalıplaşmış kurallardan ibaret değildir. Getirilen hükümlerle topluma yararlı belli bir amaç güdülmekte, zaman süreci içinde bu amaç toplum gereksinimlerine yanıt vererek daha da olumluya yöneltmektedir."*

ifadesiyle kanunların kalıplarına tamamıyla girmeden hukukun genel ilkeleri sayesinde daha sağlıklı kararlar alınabileceğini vurgulamıştır.

Kişisel Verilerin Korunması Hukukunun Temel İlkeleri

Kişisel verilerin işlenmesine ilişkin genel prensipler, modern kişisel verilerin korunması hukukunun temel yapı taşı olarak değerlendirilmektedir (Schwartz, 2000, s.1614). Kişisel verilerin korunmasına verilen önem sebebiyle konuya ilişkin bütün düzenlemelerde, kişisel verilerin işlenmesi başta olmak üzere, kişisel verinin mevzu bahis olduğu her faaliyete ilişkin temel ilkeler belirlemek gerekmiştir (Dülger, 2019a, s. 108). Kişisel verilerin korunması alanında farklı düzenlemeler olsa da temel ilkeler ulusal ve uluslararası mevzuatta hemen hemen benzer biçimde yer bulmaktadır. Söz konusu temel ilkeler, kişisel verilerin korunmasında çok önemli bir rol oynamaktadır.

Kişisel verilerin korunmasına hâkim olan ilkelerin birbirlerinden kesin çizgilerle ayrılması oldukça zordur. Bazı ilkeler diğer ilkelerin özünü oluştururken kimi ilkeler de birbirlerini bütünlemektedir. Bununla birlikte, bu ilkeler arasında sıkı bir bağ da bulunmaktadır (Küzeci, 2020, s. 227). Veri işleme faaliyeti sırasında, hukuka uygunluk sebeplerinin varlığının yanı sıra, belirlenen bu temel ilkelere de uyulması gerekmektedir (Deniz, 2021, s. 78).

6698 sayılı Kanun'da ise kişisel verilerin işlenmesinde sayılan genel (temel) ilkeler şunlardır:

> *"Hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme".*

Kişisel verilerin işlenmesine ilişkin temel ilkeler, bütün kişisel veri işleme faaliyetlerinin özünde bulunmalı ve bütün kişisel veri işleme faaliyetleri söz konusu ilkelere uygun bir şekilde gerçekleştirilmelidir.

Kişisel verilerin korunmasına dair yasalar ve muhtelif düzenlemelerde kişisel verilerin korunmasındaki genel ilkeler farklı unsurular barındırsa da kişisel veriler hukuka uygun bir şekilde işlenmeli, sadece belirli amaç dahilinde kullanılmalı, asgari seviyede ve amacı aşacak şekilde kullanılmamalıdır.

6698 sayılı Kanun'da Genel Veri Koruma Tüzüğünde (GDPR) olduğu gibi, kişisel verilerin işlenmesi açısından geçerli olan bu ilkelere uyulmaması durumunda veri sorumlusunun sorumluluğunun meydana geleceği, başka bir deyiş ile hesap verilebilirlik ilkesine açık bir biçimde yer verilmemiştir. Bu, Kanun açısından bir eksiklik teşkil etmemektedir çünkü veri işleme sürecinde söz konusu ilkelere uygun davranılmaması, veri işlemenin hukuka aykırı olması sonucunu doğuracak ve Kanun'un 11'inci maddesi gereğince, kişi zararını veri sorumlusundan talep edebilecektir (Taştan, 2017, s. 48).

Kişisel verilerin işlenmesine dair ilkeler, kişisel veri işleme faaliyetlerinin özünde olmalı ve bütün kişisel veri işleme faaliyetleri bu ilkelere uygun olarak yerine getirilmelidir. Kişisel veri işleme faaliyetinin *"olmazsa olmazını"* oluşturan bu ilkelere uyulması bir mecburiyettir. Kişisel veri işleme şartlarının hepsinin aynı anda bulunması halinde bile genel ilkelere riayet edilmediği anlaşılırsa hukuka aykırı bir şekilde kişisel veri işleme faaliyeti gerçekleşmiş olacaktır. Başka bir ifadeyle bu ilkelere her durum ve koşulda uyulması gerekmektedir (Umniyahasghar, 2021, s. 3).

Veri işleme faaliyeti esnasında, hukuka uygunluk sebeplerinin varlığının yanı sıra, belirlenen bu temel ilkelere de uyulması gerekmektedir. Söz konusu bu temel ilkelerin belirlenmesinin amacı; kişisel verilerin serbest dolaşımının sağlanmasıdır. Çünkü; bireyler, verilerinin korunduğu, başkaları tarafından erişilemeyeceği hususunda şüphe duymadığı takdirde, verilerin ulaşılabilirliği ve çeşitliliği artacaktır (Deniz, 2021, s. 78).

Genel ilkeler, tek başına kişisel verilerin işlenmesindeki hukuka uygunluk koşulu teşkil etmemektedir. Ancak, açık rıza olsa dahi verilerin bu ilkelere aykırı olarak işlenmesi halinde hukuka aykırı olarak veri işleme karşımıza çıkacaktır. Bundan dolayı, söz konusu genel ilkelerin bütün veri işleme faaliyetlerinde dikkate alınması gerekir (Develioğlu, 2017, s. 44).

Ölçülülük İlkesinin Ulusal ve Uluslararası Mevzuattaki Yeri

GDPR'ın 5'inci maddesinin birinci fikrasının (c) bendinde ölçülülük ifadesi:

> *"İşlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlıdır (verilerin en az seviyeye indirilmesi)."*

şekliyle yer almakta ve bu ilke *"veri minimizasyonu"* olarak da adlandırılmaktadır.

6698 sayılı Kanun'da *"Genel İlkeler"* başlıklı 4'üncü maddesinde;

> *"kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işleneceği hükme bağlandıktan sonra 4 üncü maddenin ikinci fikrasının (ç) bendinde geçen ifade şöyledir: "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma".*

Yani kişisel veriler, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmak zorundadır.

1/541 Esas Numaralı Tasarının Madde Gerekçeleri'nde şu ifadeler yer almaktadır:

> *"Kişisel verilerin, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ilkesi, işlenen verilerin, belirlenen amaçların gerçekleştirilebilmesine elverişli olmasını, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirmektedir. Yine, sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işlenebilmesi için, işlemeye ilk kez başlıyor gibi, 5 inci maddede düzenlenmiş olan kişisel verilerin işlenme şartlarından birinin gerçekleşmesi gerekecektir. Ayrıca işlenen veri, sadece amacın gerçekleştirilmesi için gerekli olanla sınırlı tutulacaktır".*

6698 sayılı Kanun'un 4'üncü maddesinin ikinci fikrasının (ç) bendinde sadece *"sınırlı"* ifadesi kullanılmışken, GDPR'da *"gerekli olanla sınırlı"* ifadesi kullanılmıştır. *"Gerekli olanla sınırlı"* ifadesine Kanun'da yer verilmemesi hükmün daha ucu açık bir şekilde değerlendirilmesine imkân tanımamalıdır. Ayrıca, Kanun'da kişisel verilerin işlendikleri amaçla ölçülü bir şekilde işlenmesinin gerektiği öngörüldüğünden, *"yeterli", "ilgili"* ve *"gerekli olanla sınırlı olma"* şartlarının hepsi bu kavram içinde değerlendirilmelidir. Ölçülülük ilkesi, *"yeterli", "ilgili"* ve *"gerekli olanla sınırlı olma"* şartlarının hepsini taşımaktadır. Bu doğrultuda, Kanun'daki ölçülülük kavramı yalnızca işleme amacı açısından yeterli olma, yani dar anlamda ölçülülüğün ötesinde, *"yeterli", "ilgili"* ve *"gerekli olanla sınırlı olma"* kavramlarını

ihtiva edecek şekilde kapsamlı bir anlamda yorumlanabilir (Yücedağ, 2019, s. 59-60).

95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi'nin (Direktif) 6'ncı maddesinin birinci fikrasının (c) bendi gereğince;

> *"kişisel veriler, toplanma ve/veya bunu izleyen işleme amaçları açısından yeterli ve onlarla ilgili olacak ve aşırı olmayacaktır."*

hükmünde yer alan ifadeler de GDPR'da geçen ibarelerle benzer şekilde yer almıştır.

108 No'lu Sözleşme'de de yine hemen hemen aynı ifadeler yer almakta ve 181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır aşan Veri Akışına İlişkin Protokol'de de Direktif ile bire bir aynı olan *"saklanma amacı için yeterli, onunla ilgili olacak ve aşırı olmayacaktır"* hükmü bulunmaktadır.

Federal Almanya Veri Koruma Yasası'nın 3 (a) hükmünde ise ölçülülük ilkesi şu şekilde yer almıştır:

> *"Veri işleme sistemleri, hiçbir verinin veya olanaklı bulunan en az miktarda kişisel verinin toplanması, işlenmesi veya kullanılması amacı doğrultusunda tasarlanmalı ve seçilmelidir. Özellikle olanaklı bulunduğunda ve maliyeti ile zahmeti korunmaya çalışılan amaç ile makul bir ilişki içinde olduğunda anonimleştirme ve takma adlaştırma kullanılır."*

Article 29 Data Protection Working Party'nin (Çalışma Grubu) hazırlamış olduğu rehberde de ölçülülük ilkesi ile ilgili şu ifadeler geçmektedir:

> *"Açık ve özel amaçlar belirlenmelidir. Ulaşılacak amacı anlamak, gerekli verinin türünü, kategorisini niteliğini ve gerçekleşmesi gereken işlemin türünü belirlemede yardımcı olacaktır. Doğru amaç sınırlandırmasının veri işlemeden etkilenen insanların sayısının azalmasına sebep olması gerekir."*

Danıştay'ın 2014/2242 Esas sayılı, 2014/4562 Esas sayılı Kararları'nda

> *"parmak izi ya da yüz tarama sistemi" gibi biyometrik yöntemlerin, kamusal alan da olsa "özel hayatın gizliliği" ilkesi kapsamında bulunduğu ve toplanan*

verilerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmadığı göz önünde tutularak hukuka aykırı bir işlem olarak"

değerlendirmelerine yer verilmiştir.

Örneğin, *"avuç izi taraması"* uygulayan bir spor salonunun bu sistemi zorunlu ve tek yol olarak sunması *"kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi"* ile bağdaşmamaktadır. Yüksek güvenlik düzeyi gerektirmeyen bir alan olan spor salonunun özel nitelikli kişisel veri olan biyometrik veri kullanması ölçülü olarak değerlendirilmemelidir.

6698 Sayılı Kanun Kapsamında Ölçülülük İlkesinin Unsurları

Kişisel verilerin korunması hakkı, Türkiye Cumhuriyeti Anayasası'nda (Anayasa) temel hak ve özgürlüklerden biri olarak düzenlenmiştir. Bu nedenle, kişisel veri işleme faaliyetlerinin de Anayasa'da belirlenmiş olan temel hak ve özgürlükler açısından tabi olması gerektiği açıktır ve bu noktada ölçülülük hususu büyük önem arz etmektedir (Kişisel Verileri Koruma Kurumu Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber).

Amaçla Bağlantılılık İlkesi

Kişisel verilerin işlenmesinde amaçla bağlılık ilkesi, kişisel verilerin önceden belirlenmiş olan hukuka uygun amaçlar için toplanmasını, bu amaçlarla örtüşmeyen kişisel verilerin ise işlenmemesi gerektiğini öngörmektedir. Kişisel verilerin amaçla bağlantılı olarak işlenmesine rıza gösterilmesi bu işlemelerin kapsamının ve hudutlarının belirlenmesi bakımından önem arz etmektedir. Şayet, ilgili kişi, kişisel verilerinin hangi amaçlarla kullanılacağını öğrenirse kişisel verilerinin işlenmesine sağlıklı bir şekilde izin verebilir ve kişisel verilerinin üzerindeki kontrolü bu şekilde sağlayabilir (Yılmaz, 2019, s. 103).

Amaçla bağlantılılık ilkesinin amacı, kişisel verilerin işlenme amaçlarını en başından belirlemekle ilgili kişinin neye, ne için rıza verdiğini öğrenmesi ve veri sorumlusunun da açıkladığı amaç doğrultusunda gerekli ve ölçülü miktarda veri işlemesini sağlamaktır.

Dolayısıyla veri sorumlusunun hangi amaç ya da amaçlar için veri işleyeceğini özenli bir şekilde belirlemesi gerekecektir. Amaçla bağlantılı olma ilkesi kapsamında, söz konusu amacın önceden, yani veri işlenmeden ya da verinin elde edildiği sırada belirlenmiş olması gerekmektedir. Nitekim kişisel verisi işlenecek olan

ilgili kişinin neye rıza verdiğini bilmesi elzemdir (Çekin, 2020, s. 71-73).

Kişisel veriler ile işlenmeleri için belirlenen amaç arasında bağlantı olmalı; amaç ve kişisel verinin niteliği birbiriyle ilintili olmalıdır. Örneğin bir ayakkabı mağazasının müşterilerine reklam yapmak amacıyla kişisel veri işleme faaliyetiyle bağıntılı veriler müşterilerin kimlik ve iletişim bilgileri iken; bir bankanın müşterisine kredi kartı imkânı sağlayıp sağlamayacağını tespit edebilmek amacıyla işleyeceği kişisel veriler, kimlik ve iletişim bilgilerinin dışında ilgili kişinin aktif olarak çalışıp çalışmadığı, aylık geliri, oturduğu ev bilgisi, sağlık durumu, mali durum bilgileri gibi verilerdir (Dülger, 2019b, s. 125).

Başka bir örnekte; online bir ayakkabı satış sitesinde üye olan bir kişiye sipariş bilgilendirilmesi yapmak için kimlik ve iletişim bilgilerinin kullanılması mecbur iken; indirimlerden ve ürün bilgilerinden düzenli bir şekilde haberdar olmak üzere e-bültene üye olmayan kişinin e-posta verisi söz konusu amaçla işlenmemelidir.

Verilen örnekte her iki amaçta da söz konusu olan kişisel veri, ilgili kişinin e-posta verisidir. Ancak ilk halde müşterinin vermiş olduğu siparişe ilişkin bilgilendirilmesi amacı mevzu bahis iken sonraki durumda ise mağazanın düzenli ürün ve indirim bilgilendirmesi yapma arzusu vardır. Sipariş alımı esansında ilgili kişinin e-posta adresini alarak sipariş oluşturma aşamasından siparişin teslim aşamasına kadar her aşamada söz konusu veriyi işleyebilecek olan veri sorumlusu; bu veriyi e-bülten aboneliğiyle ilgili amaçlar için kullanamaz. Bu durumda, veri sorumlusu, yeni bir amaç doğacağı için 6698 sayılı Kanun ile belirlenmiş olan şartları bu amaç için de belirlemelidir (Dülger, 2019b, s. 126).

Yine başka bir örnekte ise; bir erkek maktulün cinayetinin aydınlatılması için alınan kan ve saç örneği, kişinin rızası olmadığı için babalık testinde kullanılamayacaktır. Şayet cinayetten önce kişinin üzerinde cinsel saldırı suçunun da işlenmiş olduğu anlaşılırsa alınan bu örneklerin söz konusu olayın aydınlatılmasında kullanılabileceği ve bu durumun amaca bağlılık ilkesine aykırı bir durum oluşturmayacağı söylenebilir (Sert, 2018, s. 57).

Bu ilkeye göre, her kişisel veri işlemede, somut olayda işlem yapılmak istenen kişisel verinin işleme amacı için uygun olup olmadığı ve söz konusu verinin işlenmesinin bu amaca ulaşmak için gerekli olup olmadığı yönünde değerlendirme yapılmalıdır (Özdemir, 2019, s. 143). Bu yönde değerlendirme yapılırken, kişisel verilerin toplanması anındaki amaç ile daha sonraki aşamalardaki amaçlar arasındaki bağlantı, kişisel verilerin işlendiği kapsam ve ilgili kişinin sonraki aşamalardaki işleme hakkındaki beklentileri, kişisel verilerin yapısı ve sonraki

aşamalardaki veri işlemelerinin ilgili kişiler üzerindeki etkisi göz önünde bulundurulmalıdır (Article 29 Data Protection Working Party, 2013, s. 23-26).

Amaçla Sınırlılık İlkesi

Amaçla sınırlılık, kişisel verilerin korunmasındaki en etkili ilkelerden biridir. Kişisel veriler işlendikleri amaçla sınırlı olmalıdır. Mevcutta olmayan ve daha sonra meydana gelmesi planlanan amaçlarla kişisel veri işlenmemelidir. Kişisel veri işleme faaliyetinin gerçekleşmesi için olması gerekenden daha çok kişisel veri işlenmemelidir. Yani, kişisel veriler sadece açık, kesin amaçlar için ve gereken düzeyde işlenmeli, amacın gerektirdiği durumlarda kullanılmalıdır (Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu).

Kişisel veriler belirlenen amaçla sınırlı tutulmalıdır. Kişisel verilerin işlenen amaçla sınırlı tutulma ilkesi özellikle amaca ilişkin birtakım nitelikler belirleyerek, veri sorumlusunun kişisel veri işleme amacını sınırlandırma gayesini taşımaktadır. Söz konusu ilke GDPR'da *"amacın sınırlandırılması (purpose limitation)"* başlığıyla ele alınmıştır (Dülger, 2019b, s. 126).

Kişisel veriler toplandıktan sonra muhtemel farklı işleme amaçları kapsamında işleme yapmak için, verilerin ilk kez toplandığı esnada sağlanması lazım olan koşullar ortaya çıkacak olan yeni amaçlar için de yeniden sağlanmalıdır.

"Örneğin, bir taşımacılık firması tarafından taşıma sözleşmesi kapsamında kaydedilen adres verileri, daha sonra pazarlama faaliyeti için de işlenecekse, bu amaçla işleme için kişisel veri işleme şartlarının karşılanıp karşılanmadığının yeniden ele alınması gerekmektedir" (Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu).

Burada kişisel verilerin niteliğinin değişmesi şart değildir, işleme amacı değişmelidir. Elde edilecek ve işlenecek kişisel veri miktarı veri sorumlusunun saptadığı amaç doğrultusunda gerekli olduğu kadarla sınırlı tutulmalıdır. GDPR'a göre kişisel veriler; ilgili kişi için, işleme amaçları için gerekli olandan daha uzun bir süre için depolanmasına izin verilmediğini tanımlayan bir formda tutulmalıdır. Depolama süresi mümkün olan en kısa süre ile sınırlandırılmalıdır. Bu sınırlamayı sağlamak için, veri sorumlusu tarafından silme veya periyodik gözden geçirme için süre sınırları oluşturulmalıdır (Voigt/Bussche, 2017, s. 91).

Veri sorumlusu tarafından Kanun'da öngördüğü amaç şartlarına uygun olarak belirlediği işleme amacını gerektiği gibi yerine getirebilmek için ihtiyaç duyduğundan fazla kişisel veri toplanması bu ilkeye aykırılık oluşturur. Günlük hayatta, veri sorumlusunun *"ilerde belki ihtiyacımız olur"* düsturuyla gerekenden fazla kişisel veri işlendiği görülmektedir. Çünkü kurum ve kuruluşlara ve kişilere az bilgi toplamak yerine daha fazla bilgi toplamak cazip gelmektedir. Ancak özellikle kişisel verilerin korunması mevhumunun gelişmesi ve yasal düzenlemelere konu olması ve bireylere bu bilincin aşılanmasıyla beraber bu tarz alışkanlıkların bırakılması zorunlu bir hal almıştır. Bu durumda; belirlenen amacı gerçekleştirmeye yönelik yeterli veri elde edilmeli, elde edilen kişisel veriler toplanma amacına uygun bir şekilde işlenmeli ve söz konusu amaçla uyumlu olmayan başkaca amaçlar için veri işlemeden imtina edilmelidir (Dülger, 2019b, s. 127).

Yine başka bir örnekte; bir iş yerine giriş-çıkışta kartlı geçiş sistemi kullanılabiliyor ve işverenin güvenlik veya mesai takibi için yerine getirmesi için yeterli bilgi bu sistem aracılığıyla işlenebiliyorken biyometrik yöntemlerle iş yeri giriş-çıkış sağlanması, söz konusu amacı gerçekleştirmek için gereken veri işleme sınırını aşmakta olup ölçülü bulunmamaktadır.

Amaçla Ölçülülük İlkesi

Ölçülülük ilkesi, kişisel veri işleme faaliyeti ile gerçekleştirilmesi düşünülen amaç arasında *"makul, uygun bir dengenin gözetilmesi",* başka bir deyişle kişisel veri işlemenin amacı gerçekleştirecek düzeyde olması manasına gelmektedir.

Yani, kişisel veri işleme faaliyetinin gerçekleşmesi maksadıyla gerekmeyen kişisel verilerin işlenmemesi elzem olup veri sorumlusunun maksadı doğrultusunda ölçülülük ilkesine uygun bir şekilde ilgili kişiden asgari seviyede veri istenmesi ve diğer amaçlar için gerekli olmayan veri işlemeden imtina etmesi gerekmektedir.

Bu ilkeye göre, kişisel verilerin işlenmesi ilgili kişinin açık rızasına dayanarak olmuş olsa ve belirli bir amaçla bağıntılı olsa dahi açık rızanın, çok miktarda veri işlenmesini yasallaştırmayacaktır.

Bu itibarla, kişisel verilerin sadece belirlenen amaçlar için ve gereken miktarda toplanması, amacın gerektirdiği zaman yararlanılması ve amaç için gerekli olandan fazla müddet muhafaza edilmemesi gerekmektedir (Kişisel Verileri Koruma Kurulu, "25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti").

Ölçülülük ilkesi, kişisel verilerin toplanması sırasında esasında sınırların belirlenmesine imkân tanımaktadır. Bazı eserlerde orantılılık ilkesi olarak da adlandı-

rılan ölçülülük ilkesi, her ne gaye taşırsa taşısın, işlenen verilerin asgari seviyede olması amacına hizmet etmektedir.

Veriye erişmenin hangi basamağa kadar hakikaten gerekli olduğuna ölçülülük ilkesi sayesinde yanıt verilmektedir.

"Örneğin; dijitalleşen dünyada, programların çalıştırılması için birden fazla izin talep edilmektedir. Bireylerin bir uygulama çalıştırmak için gereken izinlere hepsine gerçekten ihtiyaç duyup duymadığını sorgulayabilmelerinin kişisel verilerin ölçülülük ilkesi bağlamında işlenip işlenmediğini kontrol edebilmek için geçerli bir mekanizma olacaktır" (Çekin, 2016, s. 637).

Ölçülülük ilkesi sayesinde kişisel verinin işlenme amacı ile uygunluğunun olması, veri işleme amacının gerçekleşmesi için gerekli olmasının koşulunu oluşturacaktır. Ölçülülük ilkesi, bir işe yaramayan verinin toplanmasını ve bilgi kirliliğini de engellemektedir. Ölçülülük ilkesi yorumlanırken amaç ile kişisel veri arasındaki "illiyet bağı" kavramı ile bu bağıntı açıklanmaya gayret edilmektedir. Orantılılık ilkesine göre, kişisel verilerin işlenmesinde söz konusu kişisel verinin işleme amacına uyup uymadığı ve söz konusu verinin işlenmesinin, güdülen amacın gerçekleşmesi için gerekli olup olmadığı her somut vakada ayrıca ele alınmalıdır. İncelemelerin sonunda uygunluk saptansa bile, ölçülülüğün sürekliliği ve ilgili kişilerin problem yaşamamaları maksadıyla gerekli tedbirlerin alınması da şarttır (Avcıoğlu, 2018, s. 32).

Kişisel verilerin, işlenme amacına uygun olarak ölçülü bir şekilde işlenmesi gerekmektedir. Bu açıdan *"ölçülülük",* elde edilen kişisel verinin miktarı ve niteliği ile elde edilme amacı arasındaki bağıntıyı ifade etmektedir (Akgül, 2015a, s. 154). Öte yandan, kişisel verilerin işlenmesi sırasın-da, kişisel verilerin korunması hakkına halel getirmeyecek yani en doğru aracın tercih edilmesi ölçülülük ilkesinin gereğidir (Şimşek, 2008, s. 99).

Bununla birlikte *"amaçla bağlantılı, sınırlı ve ölçülü olma"* koşulunun bütün ilgili kişiler ve kişisel veri işlenme aşamasında detaylı olarak ele alınması gerekmektedir. Nitekim, belli bir şahıs ve süreç için gereken kişisel veri, bir başkası için ölçülü olamayacaktır. Özellikle, özel nitelikli veriler için bu duruma dikkat edilmesi gerekmektedir.

Örneğin; bir iş yerinde insan kaynakları departmanınca çalışanların özlük haklarına ilişkin bir hususun belirlenebilmesi için çalışanlardan ceza mahkumiyeti verisinin alınması ölçülü olarak kabul edilebilecekken, aynı iş yerindeki bilgi sistemleri departmanı tarafından söz konusu verinin işlenmesi ölçüsüz bir işleme olacaktır.

Bu kapsamda, Danıştay, çalışanların mesai takibinde avuç içi izi, retina taraması, parmak izi, gibi biyometrik sistemlerin uygulan¬masına dair işlemlerin iptal edilmesi talebiyle açılmış olan davalarda; mesai kont¬rol yönteminin şeklini ve içeriğini de dikkate alarak, söz konusu şekilde bir uygulama ile kurum ve kuruluşlar tarafından amaçlanan kamu yararı arasında orantılılık olmadığını belirtmiştir. Danıştay'a göre, böyle bir uygulama, ölçülülük ilkesine de aykırılık teşkil etmektedir.

Özellikle, kamuda çalışanların binalarına girişlerde mesaisinin kontrolünün sağlanması ve genel güvenliğin tesis edilmesi esnasında biyometrik sistemlerin tercih edilmesi halinde kişisel verilerin korunması hakkına halel getirmeyecek en doğru vasıtanın seçilmesi ölçülülük ilkesinin gereğidir (Akgül, 2015b, s. 211). Dolayısıyla, alternatif bir yolun olmaması halinde, kişisel verilerin korunmasına ilişkin tüm önlemlerin alınmış olması şartıyla ve özellikle yüksek güvenlikle korunması gereken kamu hizmetlerinde biyometrik sistemlere başvurulmalıdır.

Ölçülülük ilkesiyle ilgili tartışmalar devam etmektedir ve edecektir. Nitekim, bir verinin gerekli olup olmadığı tartışmaya açık olup farklı kişiler tarafından değişik biçimlerde yorumlanmaya açık bir hale gelmiştir. Mahkemeler dahi bu ilkeyi farklı olarak ele almaktadır (Kılınç, 2012, s. 1110).

Anayasal Bağlamda Ölçülülük İlkesi

Anayasa'da belirtildiği üzere;

> *"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz".*

Ölçülülük ilkesi temel hak ve hürriyetlerin sınırlandırılması bakımından başlıca, esas ilkelerden biridir.

Ölçülülük ilkesinin hukuki yapısı hem anayasa hukukundan hem de anayasa altı normlardan oluşmaktadır. Anayasa gereği, ölçülülük ilkesi her durumda göz önünde bulundurulmalıdır. Bu kapsamda, kanun hükümlerinin içeriği belirlenirken, örneğin belirli olmayan hukuki nosyonlar yorumlanırken ve sonuçları

denetlenirken ölçülülük ilkesi dikkate alınmalıdır.

Ölçülülük ilkesinin özü hukuki ilişkilerin *"dengeli, adil ve makul bir şekilde"* düzenlenmesini gerektirmektedir. Ölçülülük ilkesi ilk kez 19'uncu yy.da *"Prusya Yüksek İdare Mahkemesi"* tarafından dile getirilmiştir. Ölçülülük ilkesi, temel hak ve özgürlüklerin sınırlanmasında *"sınırlamanın sınırı"*nı oluşturmaktadır. Ölçülülük ilkesi, Fransız hukukçu Guy Braibant tarafından *"sineğin çekiçle ezilmemesi"* benzetmesiyle tasvir edilmiştir (Metin, 2002, s. 19,22).

Ölçülülük ilkesi, sadece Anayasa Mahkemesi'nin dikkate alacağı bir ilke olmayıp, hayatın her alanında göz önüne alınması gereken bir ilkedir.

Ölçülülük ilkesinin ülkemizde gelişim aşamasına bakacak olursak; ölçülülük ilkesi, başka ülkelerin hukuk sistemlerinde, idare hukukunda ortaya çıkmış olup sonradan anayasa hukuku disiplinine geçmiştir. Ancak ülkemizde ölçülülük ilkesi, anayasa hukukunda yaygınca kullanıldıktan sonra idare hukuku disiplinine taşınmıştır.

Ölçülülük ilkesinin Türkiye'de anayasal açıdan pozitif temele sahip olmasının tarihi oldukça yakındır. 1961 Anayasası'nda ölçülülük ilkesine yer verilmemiştir. Ancak söz konusu yıllarda verilmiş Anayasa Mahkemesi kararlarında, nadiren de olsa ölçülülük ilkesinin bileşenlerine yer verilmiştir. 1961 Anayasası döneminde, kimi karar gerekçelerinde dolaylı bir şekilde ilkenin ögelerinin dayanak noktası oluşturulmuştur. Bu çerçevede ölçülülük ilkesi; uygulamada, Anayasa metninde yer almasından önce kabul edilmeye başlanmıştır.

Ülkemizde ölçülülük kavramı ilk olarak anayasa hukuku kapsamında incelenmiştir. Bu kavrama ilişkin en eski tanım Fazıl Sağlam tarafından yapılmıştır. Sağlam ölçülülüğü,

> *"Somut bir temel hak sınırlamasının amacı ile sınırlama önlemi arasında ilişkinin denetlenmesini, hukuk devletinin gerektirdiği rasyonel esaslara bağlayarak, keyfi sınırlamaları önleyici bir fonksiyon yerine getirmek"*

şeklinde betimlemektedir (Sağlam, 1982, s. 128).

Normatif dayanağını Anayasa'nın 13'üncü maddesinden alan ölçülülük ilkesi, toplum halinde yaşamanın bir yansıması olarak doğmuştur.

Bir diğer ifade ile ölçülülük, *"birbiriyle çatışan özgürlüklerin, ihlal edilmeksizin, birlikte var olabilmesinin anahtarıdır"* (Ceylan, 2008, s. 20).

Ölçülülük ilkesi, hak ve özgürlükleri koruyan bir prensip olmanın yanı sıra, sınırlamanın nasıl olması gerektiğini de belirten bir ilkedir. Ölçülülük ilkesinin üç bileşeninin bulunduğu Anayasa Mahkemesi kararlarında ve doktrinde olduğu üzere 2001 Anayasa değişikliği esnasındaki görüşmelerde de ifade edilmiştir; bu unsurlar şunlardır:

"Elverişlilik, gereklilik ve orantılılık". "Elverişlilik" müracaat edilen tedbirin ulaşılmak istenen amaç için elverişli olmasını, *"gereklilik"* müracaat edilen tedbirin ulaşılmak istenen amaç bakımından gerekli olmasını ve *"orantılılık"* ise müracaat edilen tedbir ve ulaşılmak istenen amaç arasında olması gereken ölçüyü ifade etmektedir.

Bu tanımlar çerçevesinde ölçülülük ilkesi Yüksel Metin'e göre;

> *"sınırlamada başvurulan vasıtanın sınırlama amacını gerçekleştirmeye elverişli olması; bu vasıtanın sınırlama amacı açısından gerekli olması ve araç ile amacın ölçülü bir oran içinde bulunması"*

olarak tanımlanmaktadır (Metin, 2002, s. 26, 30).

Anayasa Mahkemesi kararları bağlamında ölçülülük ilkesi, sınırlayıcı tedbirin güdülecek olan amaç için zorunlu ve amacı gerçekleştirmeye elverişli olmasını ve ayrıca araç ve amaç arasında *"makul bir dengenin"* bulunması gerekli olmasını ifade etmektedir. Ölçülülük ilkesinin amacı da temel hak ve özgürlüklerin gerekenden daha çok kısıtlandırılmasının önüne geçmektir.

Ölçülülük ilkesi; ölçü, araç ve amaç arasındaki üçgen şeklindeki ilişkiler olarak tasvir edilebilir. Ölçülülük ilkesi; kullanılan aracın ulaşılmak istenen araca ulaşmak için elverişli ve gerekli olup olmadığı, *"başvurulan aracın ulaşılmak istenen amaçla ölçülü bir orantı"* içinde bulunup bulunmadığı hususuyla ilgilidir. Ancak, bir kamu gücü eyleminin ölçülü ya da ölçüsüz olmasına ilişkin hukuki denetim soyut olarak yapılamaz.

Günümüzdeki hâkim görüşe göre müracaat edilen aracın, amaca ulaşma açısından gerekli, elverişli ve orantılı olması şeklinde esasını ortaya çıkarılabilecek olan ölçülülüğün, aralarından birinin pozitif olarak değerlendirilmesi sonrasında bir diğerinin uygulanabileceği ve birbirinden ayrıksı üç alt unsurdan meydana geldiği kabul edilmektedir (Doğan, 2021, s. 82).

Elverişlilik İlkesi

Elverişlilik ilkesi, alınan önlemle istenilen sonuca ulaşılmayı ifade eder. Bir başka ifadeyle sınırlamada başvurulan aracın, sınırlama amacını geçekleştirmesi, ulaşılmak istenen sonuca bir katkıda bulunması gerekir. Tercih edilen aracın imkân dahilindeki en iyi veya en elverişli araç olması zorunlu değildir. Aracın amaca ulaşmada bir etkisinin olması yeterlidir. Şayet, seçilen araç, istenilen hedefe ulaştırmayı zorlaştırıyor ya da amaç açısından herhangi bir etki göstermiyorsa kullanılan bu araç elverişli olmayacaktır.

Sınırlamada başvurulan araç, sınırlama amacı için elverişli değilse, getirilen sınırlama Anayasaya da aykırıdır. Elverişlilik unsurunun ülkemizde kullanılışının en eski ve açık örneklerinden biri Anayasa Mahkemesinin 1961 Anayasası döneminde *"Sendikalar Kanunu"*nun kimi maddelerinin yorumlandığı bir metinde görülmektedir.

Söz konusu Karar'da Mahkeme;

> *"Elverişlilik unsurunu Anayasa'ya uygunluk denetiminde açık bir şekilde kullanmış ve gözetilmesini aramıştır: ülke çapında çalışacak sendikaların kurulmasının engellenmesi, işyeri sendikalarının ya da belli kentlerde veya bölgelerde iş kolu sendikalarının kurulmasını ve böylelikle bu sınırlama ile önlenmek istenen sendika sayısındaki şişkinliğin ve birçok güçsüz sendikaların ortaya çıkmasının gerçekleşmesi sonucunu doğuracaktır. Böylece kanunun kuralı ile ulaşılmak istenen amaç değil, tam tersi gerçekleşecektir. Bu da kuralın konuluşunda kamu yararını korumaya elverişlilik olmadığını göstermektedir."*

Müdahalenin hedeflenen amaca ulaşmaya katkısı bulunuyorsa bu müdahale "elverişli" bir müdahaledir. Burada müdahalenin ne kadar katkı sağladığının bir önemi yoktur, az da olsa bir etkisinin olmuş olması yeterlidir. Başka bir ifadeyle, müdahale bariz bir şekilde amacına erişemiyor ya da amaca aykırı bir sonuç doğuruyorsa elverişsiz olur. Öte yandan, müdahalenin hedeflenen amaca tamamıyla uyması gerekmemektedir. Çünkü ölçülülük ilkesi, hedeflenen amaca farklı şekillerde uygun olarak seçilen müdahaleler arasından hangisinin tercih edileceğini değil, sadece o müdahalenin elverişlilik ya da elverişsizlik denetimini sağlar.

Müracaat edilen yöntemin işleme amacına ulaşılabilmesi açısından elverişli olması, kişisel veri işleme faaliyetinin ulaşılacak olan amaç için uygun olması, bu ilke ile veri sorumlusunun *"ulaşmak istediği amaç bakımından başvuracağı yöntemin elverişli olması"* hususu ifade edilmektedir. Anayasa Mahkemesi'nin

"28/09/2017 tarihli ve E.2016/125, K.2017/143" numaralı kararında elverişlilik,

> *"Getirilen kuralın ulaşılmak istenen amaç için elverişli olması" şeklinde tanımlanmıştır. Gereklilik ilkesi, aynı amaca ulaşılabilmesine imkân tanıyan birden fazla vasıtanın bulunması halinde bunlar arasından en az müdahaleci olan vasıtanın seçilmesidir.*

Yine başka bir Anayasa Mahkemesi Kararı'nda da;

> *"Türkiye çapında çalışacak sendikaların kurulmasının engellenmesi, işyeri sendikalarının ya da belli kentlerde veya bölgelerde iş kolu sendikalarının kurulmasını ve böylelikle bu sınırlama ile önlenmek istenen sendika sayısındaki şişkinliğin ve birçok güçsüz sendikaların ortaya çıkmasının gerçekleşmesi sonucunu doğuracaktır. Demek ki yasa kuralı ile varılmak istenen erek değil, onun tam tersi gerçekleşecektir. Bu da kuralın konuluşunda kamu yararını korumaya elverişlilik olmadığını göstermektedir."*

ifadesiyle elverişlilik ilkesine vurgu yapılmıştır.

Gereklilik İlkesi

Gereklilik ilkesi, hedeflenen amaca aynı derecede elverişli birden çok araç arasından en az müdahaleci olan araçla ulaşmayı ifade etmektedir. Federal Alman Anayasa Mahkemesi kararlarında gereklilik ilkesi şöyle ifade edilir:

> *"Amaca ulaşmada aynı etkiye sahip, bireylere daha az yükümlülük getiren başka bir araç yoksa seçilen araç gereklidir. Sınırlamada başvurulan aracın gerekliliği 'yumuşak araç'*

olarak tanımlanmaktadır.

Gereklilik, izlenen hedef için önlemin etkinliğinin ve aynı hedefe ulaşmak için diğer seçeneklere göre daha az müdahaleci olup olmadığına dair gerçeklere dayalı bir değerlendirme ihtiyacını ifade etmektedir.

Havlayan köpekten rahatsız olma durumunda; köpeğin öldürülmesi yönündeki görüş elverişlidir ancak gerekli değildir. Köpeğin bodrum katta bulunan kömürlükte tutulması yönündeki uyarı yeterlidir.

İlgili kişinin, kişisel verilerinin işlenme amacını önceden bilmesi ise, ilgili kişinin

kendi verileri üzerinde bir denetimi olması ve kişisel verileri hakkında önleyici koruma imkânı sağlayacaktır (Şimşek, 2008, s. 83).

Mesela, suç takibi için telefon dinlemesi yapılırken bu amaçla ilişkili olmayan telefon kayıtlarının kullanılması doğru değildir. Ayrıca, internette kullanıcıların bilgi taleplerinin giderilmesi için üyelik gerektiren sitelerde gereği olmayan kişisel verilerin toplanması durumundaki gibi, kişisel veriyi işleyen kişinin amaca ulaşmak için gerekli olmayan kişisel verileri katiyen toplamaması gerekir (Şahin, 2011, s.79).

Ölçülülük denetiminde amaca ulaşmak için tercih edilen aracın gerekli olup olmadığı denetlenir. Gereklilik, aslında ağır sonuçları olan, başka bir deyişle en katı yöntemin son çare olarak kullanılması anlamına gelmektedir.

Orantılılık İlkesi

Orantılılık ilkesi aslında *"dar anlamda ölçülülük"* olarak da ifade edilmektedir. Kullanılan araç ile ulaşılmak istenen amaç arasında ölçülü bir orantı bulunmalıdır. Sınırlamada amacı ile sınırlamada başvurulan aracın ölçüsüz bir oran içinde olmaması gerekir. Amaç ve araç aralarında makul ve dengeli bir ilişkide olmalı ve ölçüsüz bir ilişki içinde olmamalıdır.

Orantılılık ilkesi araç ve amacın adeta bir terazinin kefesine konulup tartılmasını gerektirmektedir. Sınırlayıcı tedbirin orantılılık ilkesine uygun olup olmadığı, genellikle tedbirin ilgililere ölçü olmayan yükümlülükler getirip getirmediğine, onlar için katlanılabilir nitelikte olup olmadığına bakılarak değerlendirilir (Metin, 2002, s. 30,31).

Orantılılık ilkesinin ilk tezahürü olan uygun bir önlemin tercih edilmesi ve kararın bu yönde verilmesi, meşru amaç çerçevesinde kanundaki düzenlemeye binaen uygun olarak alınan önlemin güdülen amaç doğrultusunda orantılı bir önlem olması anlamına gelmektedir (Mutlu, 2019, s. 144).

"Örneğin, bir tekstil firması tarafından müşterilere ilişkin kimlik ya da iletişim verilerinin işlenmesi satış işlemlerinin takibi gibi amaçlarla örtüşürken, müşterilerin finansal geçmişine ilişkin verilerin toplanmasının amaçla bağlantılı ve orantılı olduğu söylenemez" (Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu).

Yüksek mahkeme kararlarında;

"adil denge", "makul ölçü", "nispet", "fiil ile ceza arasında uyum", "yapılan idari ihlal ile uygulan ceza arasında bir denge ve orantı bulunması"

gerektiği ifadeleriyle ölçülülük ilkesinin orantılılık unsuruna yer verilmektedir. Orantılılık ilkesinde müdahalenin niteliğiyle müdahalenin haklı olmasını sağlayacak sebeplerin ehemmiyeti arasında bir ölçüm yapılmaktadır (Metin, 2002, s. 37).

Anayasa Mahkemesi'nin 28.09.2017 tarihli ve E.2016/125, K.2017/143 numaralı kararında orantılılık *"getirilen kural ile ulaşılmak istenen amaç arasında olması gereken ölçü"* şeklinde tanımlanmıştır. Orantılılık ilkesi, *"araç ile amacın arasında ölçülü bir orantının bulunması durumudur"* (Metin, 2002, s. 13).

KURUL VE YARGI KARARLARI ÇERÇEVESİNDE ÖLÇÜLÜLÜK İLKESİ

Kişisel Verileri Koruma Kurulu Kararları Çerçevesinde Ölçülülük İlkesi

Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/81 sayılı Kararı ve 31/05/2019 tarihli ve 2019/165 sayılı Kararı:

> *"(...) Spor kulübünde giriş çıkış kontrolünün yapılabilmesi ve kulüp hizmetlerinden faydalanmak isteyen kişilere ilişkin giriş kontrolünün alternatif yollar ile sağlanması mümkün iken kişilerin biyometrik veri niteliğindeki avuç içi izi verisinin alınmasının 6698 sayılı Kişisel Verilerin Korunması Kanununun 4 üncü maddesinin (2) numaralı fıkrasında yer alan "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesi ile bağdaşmadığı (...)"*

şeklinde ifade edilmiştir.

Anılan Kurul Kararı'nda da ifade edildiği üzere; herhangi bir alternatifin bulunması durumunda biyometrik verilerin işlenmesi ölçülü olmayacaktır.

*"Bir havayolu taşımacılık şirketinin (veri sorumlusu) sunduğu sadakat programını kullanan ilgili kişinin kullanıcı adı ve parola bilgilerini değiştirme talebi karşısında ilgili kişiden arkalı önlü kimlik görüntüsü talep eden veri sorumlusu" hakkında Kişisel Verileri Koruma Kurulunun "01/10/2019 Tarihli ve 2019/294 sayılı Karar Özeti"*nde:

> *"Bir havayolu taşımacılık şirketinin (veri sorumlusu) sunmuş olduğu sadakat programını kullanırken kullanıcı adı ve parola bilgilerini değiştirme talebiyle veri sorumlusuna başvuran ilgili kişiye, arkalı önlü kimlik görüntüsünü iletmesi halinde talebinin yerine getirileceği cevabının verilmesi, o sırada bilet bil-*

gilerine erişmek için kimlik görüntüsünü elektronik olarak ileten, ancak daha sonra veri sorumlusuna başvurmak suretiyle kimlik görüntülerinin silinmesi ve kişisel verileri üçüncü kişilere aktarıldıysa, verilerin aktarılan üçüncü kişilerin kayıtlarından da silinmesi talebine kişisel verilerinin sistemlerinde tutulmadığı ve üçüncü kişilerle paylaşılmadığı yanıtını alan ilgili kişinin Kuruma yaptığı başvurunun incelenmesi neticesinde,

Başvuruya konu olay Genel İlkeler bakımından değerlendirildiğinde,

- *Veri sorumlusunun kimlik görüntülerini işlemesinde hangi hukuki işleme şartına dayandığı hususunun ilgili kişiye verilen cevapta ve kurumumuza intikal eden yazıda belirtilmediği, bu nedenle veri sorumlusunun veri işleme faaliyetinin belirli, açık ve meşru amaçlar için işlenme ilkesine aykırı olduğu,*

- *Kimlik doğrulama işlemi için daha az verinin işlenmesinin mümkün olduğundan hareketle veri sorumlusunun somut olayda işlediği kimlik görüntüsünün işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırı olduğu,*

- *Veri sorumlusunun kimlik görüntüsünü işlediği gibi, kimlik doğrulama işlemi bittikten sonra bu verileri silmediği, Kurumumuzca bilgi belge talep edilmesi üzerine sildiğini beyan ettiği gerçeğinden yola çıkarak, veri sorumlusunun veri işleme faaliyetinin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesine de aykırı olduğu,*

- *Diğer yandan, veri sorumlusunun, Kanun kapsamındaki başvurusuna cevap verebilmek amacıyla ilgili kişinin kimliğinin teyidi noktasında ek bilgi istemesinin yerinde olduğu değerlendirilmekle birlikte, ilgili kişinin din ve kan grubu gibi özel nitelikli kişisel verilerini de içeren arkalı önlü kimlik görüntüsünün talep edilmesinin, Kanunun "Genel İlkeler" başlıklı 4 üncü maddesinde düzenlenen "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine uygun olmadığı gibi, Kanunun özel nitelikli kişisel verilerin işlenmesini düzenleyen 6 ncı maddesine de uygun olmadığı, zira veri sorumlusunun da yapığı savunmada, somut olayda çağrı merkezi ekibi tarafından yazılı çalışma kurallarına aykırı şekilde kimlik belgesi talep edildiğini belirterek, olaya ilişkin ikrarda bulunduğu,*

- *Veri sorumlusunun Kurumumuza ilettiği yazıda, kişisel verilerinin silindiği hususunda ilgili kişinin bilgilendirileceğini belirtmiş olmasına rağmen, inceleme sürecinde bu bilgilendirmenin yapıldığına dair taraflardan gelen herhangi bir bildirim olmadığı dikkate alındığında, ilgili kişinin kimlik görüntüsünü içeren kişisel ve özel nitelikli kişisel verilerinin veri sorumlusu ve veri işleyenlerin sistemlerinden silindiği bilgisinin ilgili kişiye bildirilerek Kurumumuza bilgi verilmesi, önceden bildirildi ise bunu tevsik edecek bilgi ve belgelerin Kurumumuza iletilmesi konusunda veri sorumlusunun talimatlandırılmasına,*

- *Kişisel verileri işlenen müşterilerin bundan sonraki taleplerinde benzer karışıklıklara meydan vermemek amacıyla, sadakat kart uygulaması ve diğer hizmetlerin sunulması sürecinde kendi adına veya bir başkası adına kişisel verilere ilişkin talepte bulunan kişilerin kimliklerinin teyit edilmesi noktasında uygulanacak yöntem ve bu durumda işlenecek kişisel verilere ilişkin kurumsal düzenlemeleri Kanun kapsamında gözden geçirerek, ilgili birimleri ile veri işleyenleri bilgilendirmesi hususunda veri sorumlusunun talimatlandırılmasına,*

karar verilmiştir.

Başka bir Kurul Kararı'nda: ilgili kişinin kredi borcunun gecikmesine ilişkin veri sorumlusu tarafından farklı cep telefonlarından sürekli olarak arandığı iddiasına ilişkin olarak;

"...gerçekleşen aramaların veri sorumlusu tarafından belirlenen arama adetlerine uygun olarak gerçekleştirildiğinin ifade edildiği ve veri sorumlusunun Kuruma ilettiği cevabi yazı ekinde ilgili kişiye yönelik, yaklaşık üç hafta içerisinde yirmi bir defa arama kaydının bulunduğu dikkate alındığında söz konusu arama faaliyetinin Kanunun 4 üncü maddesinin ikinci fıkrasının (ç) bendinde yer alan "amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine aykırı olduğu kanaatine varılmıştır. Ölçülülük ilkesi, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması, diğer bir ifadeyle veri işlemenin amacı gerçekleştirecek ölçüde olması demektir. Buna göre kişisel veriler yalnızca belirli amaçlar için ve gerektiği kadar kullanılmalıdır. Veri sorumlusu tarafından ilgili kişi tarafından ölçülülük ilkesine aykırı şekilde işlenmesi nedeniyle, veri sorumlusunun Kanunun "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12 nci maddesinin birinci fıkrasının (a) bendinde öngörülen "Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek" yükümlülüğünü yerine getirmediği kanaatine varıldığından, veri sorumlusu hakkında, Kanunun "Kabahatler" başlıklı 18 inci maddesinin birinci fıkrasının (b) bendi uyarınca, idari para cezası verilmesinin uygun olacağı sonucuna varılmıştır.

Avrupa Birliği Adalet Divanı Kararlar Çerçevesinde Ölçülülük İlkesi

"Digital Rights Ireland" davasında Avrupa Birliği Adalet Divanı;

> *"organize suç ve terör gibi ciddi bir suçla mücadele amacıyla ilgili verilerin yetkili makamlara olası aktarımları için kamuya açık elektronik haberleşme servisleri ve ağları tarafından oluşturulan veya işlenen kişisel verilerin saklanmasına ilişkin yerel hukuklarda yer alan hükümlerin yeknesaklaştırılmasını amaçlayan Veri Saklama Direktifinin geçerliliğini incelemiştir. Genel olarak ciddi bir suçla mücadele meşru bir menfaat olarak düşünülse de bu direktifin "bir fark, sınır veya istisna gözetmeksizin tüm bireyleri ve her tür elektronik haberleşme ile trafik verisini" kapsaması sorunlu bulunmuştur".*

Mahkeme'ye göre, belirli suçların önlenmesine ve cezalandırılmasına katkıda bulunmak amacıyla veri tabanlarının derlenmesi, içlerinde depolanan bilgileri en üst düzeye çıkarmak için aşırı bir çabayla uygulanamaz. Bu tür mekanizmalara atfedilen meşru amaçlar karşısında gerekli orantılılık gözetilmeksizin, Devletlerin Sözleşme uyarınca kendi yargı yetkisi altındaki kişilere güvence altına almak zorunda oldukları hak ve özgürlüklere yol açabilecekleri ciddi ihlaller, bu mekanizmaların avantajlarından daha ağır basacaktır.

Ayrım gözetmeyen ve süresiz bir saklama planı bağlamında, *"ne kadar çok veri tutulursa, o kadar çok suç önlenir"* argümanı pratikte tüm nüfus bilgisi ve ölen akrabaları hakkındaki bilgilerin saklanmasını haklı çıkarmakla eşdeğer olacaktır.

"Huber Kararı"nda; Avrupa Adalet Divanı, ikamet hakkından sorumlu makamlara destek sağlamak amacıyla yabancı bir sicilin kullanılmasının ilke olarak meşru olduğuna ve belirtilen milliyet temelinde ayrımcılık yasağı ile uyumlu olduğuna karar verdi. European Council on Foreign Relations'a (ECFR) göre; Üye Devletlerin, diğer Üye Devletlerin vatandaşları için kendi topraklarında ikamet hakkının bulunup bulunmadığını tespit etmek için ilgili bilgi ve belgelere sahip olması gereklidir. Ancak bu, sicilin yalnızca bu amaçlar için gerekli verileri içermesini ve merkezi yapısının ilgili mevzuatın daha etkin bir şekilde uygulanmasını mümkün kılmasını gerektirir.

Suçla mücadele açısından, ABAD, işlenen suçların ve işlenen suçların kovuşturulmasının faillerin uyruğundan bağımsız olduğuna karar vermiştir. Bir Üye Devletin vatandaşları ve vatandaşları olmayanlar arasındaki herhangi bir farklı muamele, ECFR tarafından yasaklanan ayrımcılık teşkil eder. Bu nedenle Üye Devletlerin, vatandaş olmayanlara özel kişisel verileri işleyerek suçla mücadele amacıyla sistemler kurmasını engellemektedir.

Court of Justice of the European Union (CJEU) Schecke Kararı'nda; Mahkeme tarafından kamu fonlarından yararlanan tüm yararlanıcıların kişisel verilerinin yayınlanmasının gerekliliğini incelenirken, yasa koyucunun, aldıkları sürelere göre bu yararlanıcılarla yayınlanmasını sınırlamak gibi alternatif, daha az müdahaleci önlemleri dikkate alınmadığı vurgulanmıştır.

Mahkeme ayrıca, bu tedbirlerin bir araya getirilmesiyle daha az müdahaleci bir yaklaşımın elde edilebileceğini vurgulamıştır:

> *"İsimle yapılan bu tür sınırlı yayınlara, uygun olması halinde, EAGF ve EAFRD kapsamındaki yardımlardan yararlanan diğer gerçek kişiler ve aldıkları tutarlar". Mahkeme: "Kişisel verilerin korunmasına ilişkin istisna ve sınırlamaların yalnızca kesinlikle gerekli olduğu ölçüde uygulanması gerektiği ve önlem alınmasının mümkün olduğu konusunda gerçek kişilerin bu temel hakkını daha az olumsuz etkileyen ve halen söz konusu Avrupa Birliği kurallarının amaçlarına etkin bir şekilde katkıda bulunan..."*

şeklinde sonuca varmıştır.

AG Opinion 1/15 (Request for an opinion submitted by the European Parliament) on the Draft Agreement between Canada and the EU on the transfer and processing of PNR Kararı'nda;

> *"Tedbirin kesin gerekliliği ile ilgili olarak, PNR Taslak Anlaşmasının şartlarının Kamu güvenliğinin sağlanması için, bu alternatif önlemlerin de yeterince etkili olması gerekir. Bu anlaşma ile izlenen amaç; bu gereklilik testine yönelik olarak tedbirin çeşitli yönlerini ele almaktadır, anlaşmanın ekinde yer alan veri kategorileri, herhangi bir takdir yetkisine bırakılmadan, daha özlü ve daha kesin bir şekilde kaleme alınmalıdır. İlgili makamlara PNR verilerini işleme yetkisi verebilecek suçları kesinlikle gerekli olanlarla sınırlamak ve verileri Kanada makamlarına aktarılan yolcuların yasal güvenliğini sağlamak için kapsamlı bir şekilde listelenmelidir."*

Uygulamada, taslak tedbirin belirli bir yönü veya içerdiği hüküm hem gereklilik hem de orantılılık değerlendirmeleriyle ilgili olabilir. Örneğin, bir tedbirin herhangi bir suçu mu yoksa sadece ağır suçları mı hedef alması gerektiği sorusu bir zorunluluk olarak değerlendirilebilir; ancak, böyle bir hükmün gerekli olarak değerlendirilmesi halinde, orantılılığının ve demokratik bir toplumun değerlerini aşındırma riskinin değerlendirilmesine yine de ihtiyaç duyulacaktır.

Ayrıca, ABAD, yasal düzenlemelerle ilgili davaların büyük çoğunluğunda, bir işleme işleminin hem kişisel verilerin korunması hakkını hem de özel hayata saygı hakkını sınırladığına karar vermiştir. Mahkeme ayrıca bir sınırlamanın tesis edilmesi için "özel hayata ilişkin söz konusu bilgilerin hassas olup olmamasının veya ilgili kişilerin herhangi bir şekilde rahatsız edilip edilmemesinin önemli olmadığını" belirtmiştir.

6698 Sayılı Kanun Kapsamında Ölçülülük İlkesinin Değerlendirilmesi

6698 sayılı Kanun'a göre, kişisel veriler, *"işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmak zorundadır".* Bu ilke, işlenen verilerin, belirlenen amaçların gerçekleştirilebilmesine "elverişli" olmasını, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirmektedir.

Amaçla sınırlılık bağlamında mevcutta olmayan ve sonradan gerçekleşmesi düşünülen amaçlarla kişisel veri elde edilmemelidir. Kişisel veri işleme faaliyetinin gerçekleşmesi için gereğinden fazla kişisel veri toplanmamalı ve/veya işlenmemelidir. Kişisel veriler yalnızca belirli amaçlar için ve gerektiği kadar toplanmalı, amacın gerektirdiği yerlerde kullanılmalıdır.

Kişisel veriler ile işlenmeleri üzerine öngörülen amaç arasında bağlantı olmalı; amaç ve kişisel verinin niteliği birbiriyle ilişkili olmalıdır. *"Kişisel verilerin işlenmesinde amaçla bağlılık ilkesi"*, kişisel verilerin önceden belirlenmiş olan hukuka uygun amaçlar için toplanmasını, bu amaçlarla bağdaşmayan verilerin ise işlenmemesini gerektirmektedir.

Ölçülülük ilkesi, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında *"makul bir dengenin kurulmasını"* gerektirir. Ölçülülük ilkesinin temelinde hukuki ilişkilerin *"adaletli, dengeli ve ölçülü bir şekilde"* düzenlenmesi düşüncesi yatmaktadır. Ölçülülük ilkesi; kullanılan aracın ulaşılmak istenen araca erişmek için *"elverişli ve gerekli olup olmadığı, başvurulan aracın ulaşılmak istenen amaçla ölçülü bir orantı içinde"* bulunup bulunmadığı sorunuyla ilgilidir. Amaç ve araç ölçüsüz bir ilişki içinde olmamalı, aralarında makul ve dengeli bir ilişki olmalıdır.

SONUÇ

Kişisel verilerin işlenmesi, kişisel verilerin toplanması ile başlayan ve silinmesine kadar süren uzun bir süreç olup birden fazla işlemi içerebildiği için kişisel verilerin işlenmesi kişisel veri kavramından daha kapsamlı bir kavramı ifade etmektedir.

Hukukun genel ilkeleri, toplumsal bir gereksinime dayanmakta olup hukuki düşüncenin ana çatısını oluşturmakta ve kanunun veya alt düzenlemelerin yorumlanmasında öncelikli olarak ele alınması gerekmektedir. Belirsiz ve anlaşılamayan kanuni metinlerin yorumu için genel ilkelere ihtiyaç duyulmaktadır.

Kişisel verilerin işlenmesine ilişkin genel ilkeler, modern kişisel verilerin korunması hukukunun temel yapı taşını oluşturmaktadır. Kişisel verilerin korunmasına verilen değer sebebiyle konuya ilişkin bütün düzenlemelerde, kişisel verilerin işlenmesi başta olmak üzere, kişisel verinin mevzu bahis olduğu her faaliyete ilişkin temel ilkeler belirlemek gerekmiştir.

Kişisel verilerin işlenmesine ilişkin bu ilkelerin, kişisel veri işleme faaliyetlerinin özünde bulunması ve bütün kişisel veri işleme faaliyetlerinin bu ilkelere uygun olarak yerine getirilmesi gerekmektedir. Bu doğrultuda, başta 6698 sayılı Kanun'un 4'üncü maddesinde ve düzenlenen genel ilkeler ve diğer düzenlemeler kişisel veri işleme faaliyetlerinin "olmazsa olmazı" niteliğinde unsurlar olarak kabul edilmektedir.

Söz konusu ilkelerin en önemlilerinden biri olan ölçülülük ilkesine de 6698 sayılı Kanun'da ve uluslararası mevzuatta farklı biçimlerde ele alınılsa anlatılmak istenen şey benzerdir.

Ölçülülük ilkesi 6698 sayılı Kanun kapsamında amaçla bağlantılı, sınırlı ve ölçülülük ilkesi bendiyle yer almaktadır. Amaçla bağlantılılıkla kastedilmek istenen; kişisel verilerin önceden belirlenmiş olan hukuka uygun amaçlar için toplanmasını, bu amaçlarla bağdaşmayan kişisel verilerin ise işlenmemesini amaçlamaktadır. Amaçla sınırlılık, kişisel verilerin korunmasındaki en etkili ilkelerden biri olup kişisel veriler işlendikleri "amaçla sınırlı" olmalı ve mevcutta olmayan ve daha sonra meydana gelmesi planlanan amaçlarla kişisel veri işlenmemelidir. Amaçla ölçülülük ilkesi ise, kişisel veri işleme faaliyeti ile gerçekleştirilmesi düşünülen amaç arasında *"makul, uygun bir dengenin kurulması",* başka bir ifadeyle kişisel veri işlemenin amacı gerçekleştirecek ölçüde olması manasına gelmektedir.

Ölçülülük ilkesi, sadece kanunlarda dikkate alınacak bir ilke olmayıp, devlet ve toplum hayatının her alanında göz önüne alınması gereken bir ilkedir.

Ölçülülük ilkesinin hukuki yapısı hem anayasa hukukundan hem de anayasa altı normlardan oluşmaktadır. Ölçülülük ilkesi hem hukuk normlarının konulmasında hem de bu normların uygulanmasında dikkate alınması gereken bir ilkedir.

Anayasal bağlamda ölçülülük ilkesi elverişlilik, gereklilik ve orantılılık ögelerinden oluşmakta olup, Elverişlilik ilkesi, alınan önlemle istenilen sonuca ulaşılmayı ifade etmektedir. Yani, sınırlamada başvurulan aracın, sınırlama amacını geçekleştirmesi, ulaşılmak istenen sonuca bir katkıda bulunması gerekmektedir. Elverişlilik denetiminde öncelikle hem aracın hem de amacın anayasaya uygunluğu araştırılmalıdır. Eğer biri ya da diğeri anayasal açıdan geçersizse elverişlilik denetimine gerek kalmaz. Gereklilik ilkesi, hedeflenen amaca aynı derecede elverişli birden çok araç arasından en az müdahaleci olan araçla ulaşmayı ifade etmektedir. Amaç ne kadar somutlaştırılmışsa gereklilik denetimi de o kadar kolay yapılır. Orantılılık ilkesi ise aslında dar anlamda ölçülülük olarak da ifade edilmektedir. Kullanılan "araç ile ulaşılmak istenen amaç arasında ölçülü bir orantı" bulunmalıdır. Sınırlamada amacı ile sınırlamada başvurulan aracın ölçüsüz bir oran içinde olmaması gerekmektedir. Elverişlilik ve gereklilik ilkeleri mutlaka bir amaç araç ilişkisini zorunlu kılarken, orantılılık ilkesin uygulanması için böyle bir ilişkinin bulunması zorunlu değildir.

Kişisel veriler asgari seviyede işlenmelidir. Burada söz konusu olan veri işlemenin mutlak bir asgari seviyeye indirgenmesi değil, veri toplamanın işleme amaçlarına uygun bir seviyeye indirilmesidir. Bu nedenle, öngörülen işleme faaliyetlerinin orantılığının değerlendirilmesini gerektirir. Veri işlemeyi en aza indirgeme; veri toplama işleminin, veri işleme faaliyetinin gerçekleştirilebilmesi için mümkün olan en düşük seviyeye indirilmesini amaçlamaktadır.

Ölçülülük ilkesi; amaç, araç ve ölçü arasındaki üçgen şeklindeki ilişkiler olarak kavranabilir. Ölçülülük ilkesi; "kullanılan aracın ulaşılmak istenen araca erişmek için elverişli ve gerekli olup olmadığı, başvurulan aracın ulaşılmak istenen amaçla ölçülü bir orantı içinde" bulunup bulunmadığı sorunuyla ilgilidir.

Sonuç olarak, ölçülülük ilkesi kişisel verilerin işlenmesi hususunda ölçülülük ilkesinin olay bazlı düşünülmesi gerekir. Her durum kendi içerisinde değerlendirilmelidir. Ölçülülüğün sağlanması için denge testleri yapılmalı ve ölçülülük bu şekilde uygulanmalıdır. ◆

KAYNAKÇA

- Anayasa Mahkemesi. (2017). 28.09.2017 tarihli ve E.2016/125, K.2017/143 sayılı Karar. Erişim adresi: https://normkararlarbilgibankasi.anayasa.gov.tr
- Akgül, A. (2015a). *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması.* Beta Basım Yayım, İstanbul
- Akgül, A. (2015b). *Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı. TBB Dergisi, 118, 200-222*
- Akıl, A. (2003). *Hukukun Genel İlkeleri ve Hukukun Gelişimine Etkisi. AÜEHFD, C. VII, 3-4*
- Article 29 Data Protection Working Party. (2013). Opinion 03/2013 on purpose limitation.
- Avcıoğlu, N. H. (2018). *Türk Hukukunda Kişisel Verilerin Korunması Hakkı. Yüksek Lisans Tezi, Konya*
- Bereket, Z. (1994). *Hukukun Genel İlkeleri ve Danıştay. Yüksek Lisans Tezi, İstanbul*
- Ceylan, A. (2008). *Teori ve Uygulamada Ölçülülük İlkesi, Yüksek Lisans Tezi, Ankara*
- Çekin, M. S. (2016). *6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Sayı 2*
- Çekin, M. S. (2020). *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku.* On iki Levha Yayıncılık, İstanbul
- Deniz, İ. (2021). *Çocuklara Ait Kişisel Verilerin Türk Medeni Kanunu ve Kişisel Verilerin Korunması Kanunu Kapsamında Korunması. Yüksek Lisans Tezi, Antalya*
- Develioğlu, H. M. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması.* On İki Levha Yayıncılık, İstanbul

◊ Doğan, M. T. (2021). *İşverenin İşlediği Kişisel Verilerin İşçiyi Koruma Borcu ve Ölçülülük İlkesi Çerçevesinde İncelenmesi. Yüksek Lisans Tezi, İstanbul*

◊ Dülger, M. V. (2019-a). *Kişisel Verilerin Korunması Hukuku.* Hukuk Akademisi, İstanbul

◊ Dülger, M. V. (2019-b). *Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması. Yaşar Hukuk Dergisi, Sayı 2*

◊ Judgment of The Court (Grand Chamber) (2010). Volker und Markus Schecke and Eifert

◊ European Court of Justice Judgment (2006). Case C-524/06 Heinz Huber-Bundesrepublik Deutschland

◊ Esen, B. N. (1972). *Anayasanın Anayasa Mahkemesince Yorumlanması. AÜHF yayınları, Sayı: 301*

◊ Judgment of 08.04.2014. joıned cases c-293/12 and c-594/12 Digital Rights Ireland and Others

◊ Kaboğlu, İ. (2002). *Özgürlükler Hukuku.* Ankara

◊ Kılınç, D. (2012). *Anayasal Bir Hak Olarak Kişisel Verilerin Korunması. Ankara Üniversitesi Hukuk Fakültesi Dergisi, Sayı 3*

◊ Küzeci, E. (2020). *Kişisel Verilerin Korunması.* On iki Levha Yayıncılık, İstanbul

◊ Kişisel Verileri Koruma Kurumu. 100 Soruda Kişisel Verilerin Korunması Kanunu. Erişim adresi: https://kvkk.gov.tr/Icerik/2030/Rehberler

◊ Kişisel Verileri Koruma Kurumu. Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber. Erişim adresi: https://www.kvkk.gov.tr/Icerik/7047/Biyometrik-Verilerin-Islenmesinde-Dikkat-Edilmesi-Gereken-Hususlara-Iliskin-Rehber

◊ Kişisel Verileri Koruma Kurulu. (2020). 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar. Erişim adresi: https://www.kvkk.gov.tr

◊ Kişisel Verileri Koruma Kurulu. (2019). 01/10/2019 Tarihli ve 2019/294 sayılı Karar. Erişim adresi: https://www.kvkk.gov.tr

◊ Kişisel Verileri Koruma Kurulu. (2019). 25/03/2019 tarihli ve 2019/81 sayılı Karar ve 31/05/2019 tarihli ve 2019/165 sayılı Kararı. Erişim adresi: https://www.kvkk.gov.tr

◊ Meschariakoff, A. S. (1976). *La notion de principes généraux du droit dans la jurisprudence récente.* A.J.D.A.

◊ Metin, Y. (2002). *Ölçülülük İlkesi Karşılaştırmalı Bir Anayasa Hukuku İncelemesi.* Seçkin, Ankara

◊ Meydan Larousse. (1971). Büyük Lügat Ansiklopedisi. *İstanbul, C: VI*

◊ Mutlu, M. S. (2019). *Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması. Yüksek Lisans Tezi, İstanbul*

◊ Opinion 1/15 Of The Court (Grand Chamber) (2017). Opinion 1/15 on the Draft Agreement between Canada and the EU on the transfer and processing of PNR. Erişim adresi: https://curia.europa.eu/juris/document

◊ Özdemir, H. (2009). *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması.* Seçkin, Ankara

◊ Sağlam, F. (1982). *Temel Hakların Sınırlandırılması ve Özü. AÜSBF Yayınları, Ankara, Sayı 506*

◊ Schwartz, P. M. (2000). *Privacy And Democracy in Cyberspace,* Vanderbilt Law Review. *Vol. 52*

◊ Sert, Ş. (2018). *Kişisel Verilerin 5237 Sayılı Türk Ceza Kanunu Kapsamında Korunması. Yüksek Lisans Tezi, Erzurum*

◊ Şahin, O. (2011). *Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğinin Korunması. Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu*

◊ Şimşek, O. (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması.* Beta Yayınevi, İstanbul

◊ Taştan, F. G. (2017). *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması.* Oniki Levha Yayıncılık, İstanbul

◊ Umniyahasghar, Y. (2021). *Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler. Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi, Sayı 1*

◊ Voigt P. / Bussche A. (2017). *The EU General Data Protection Regulation (GDPR), A Practical Guide.* Springer, Switzerland

◊ Yılmaz, B. (2019). *Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması. Doktora Tezi, Ankara*

◊ Yücedağ, N. (2019). *Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler. Kişisel Verileri Koruma Dergisi, Sayı 1s*

YAPILANDIRILMAMIŞ VERİLERİN ANONİM HALE GETİRİLMESİ

Abdullah Halis ŞAHİN

Kişisel Verileri Koruma Uzmanı

“Bu çalışma, 14.02.2023 tarihinde kabul edilen “Kişisel Verilerin Anonim Hale Getirilmesinde Fayda Temelli Yöntemler” başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Bilgi teknolojilerindeki hızlı ilerleme ve gelişmeler hem ürün hem de hizmet bakımından yeni alt dalların ortaya çıkmasıyla sonuçlanmıştır. Bilişimin her alanında kapasite ve hız artarken maliyet ise düşmeye devam etmektedir. Bugün bilgiye erişimin kolay, haberleşmenin ise görece ucuz olduğu dijital bir dünyada yaşıyoruz. İçme suyuna erişimin olmadığı bölgeler iletişim ağlarıyla kuşatılmış halde ve dünya da en ücra köşesine kadar birbiriyle bağlantılı durumdadır.

Son 50 yılda teknolojinin seyrindeki değişim lineer bir çizgi şeklinde değil logaritmik bir eğri şeklinde oldu. 1970’lerin ortalarından itibaren kullanılmaya başlanan kişisel bilgisayarlar büyük değişimler geçirdiler. İnternet çok sayıda kullanıcının birbirleriyle bilgisayar üzerinden haberleşmesini mümkün kıldı. 1980’li yıllarda bilgisayarlar küçük bir grubun uzmanlık alanına girerken, bugün yüz milyonlarca insan her türlü işlemlerinde bilgisayarlarını kullanabilmektedir.

20. yüzyılın sonlarından bu yana, veri miktarındaki inanılmaz artış ve verinin yayılabileceği araçlardaki muazzam büyüme, endüstri tabanlı ekonomilerden veri temelli ekonomilere geçişi tetiklemiştir. Kişisel veri kavramının hukuki zeminde

ortaya çıkması ve kişisel verilerin insan hakkı kapsamında değerlendirilmesi bu konuya ilişkin teknolojik düzenlemeleri oldukça önemli hale getirmiştir.

Sanayi toplumundan bilgi toplumuna geçişle birlikte hem toplumsal hem de hukuki anlamda büyük dönüşümler yaşanmış ve bu dönüşümler yeni hukuki düzenlemelere ve bu hukuki düzenlemeler de teknolojik cihazlarla üretimi çok yüksek hızla artan kişisel verilerin kullanımına limitler getirmiştir.

Verilerin son derece değerli bir varlığa dönüşmesinin oldukça etkili sonuçları hukuk alanında düzenlemeleri gerekli kılmış ve bu hukuki düzenlemeler işletmelerin hem sahip oldukları verileri muhafaza etme yöntemlerine hem de bu verilere üçüncü tarafların erişme durumuna kapsamlı ve bağlayıcı kurallar getirmiştir dolayısıyla kişisel verilerin korunması alanındaki hukuki düzenlemeler, şirketlerin iş modellerini değiştirmeye mecbur bırakmıştır.

Bir yanda kişisel verilerin korunmasını bir hak olarak gören ve kişisel verilerin mahremiyetine güvence sağlayan hukuki düzenlemeler varken diğer yanda üretimde ve ticarette verimlilik artışı, istatistiksel araştırmalar, akıllı şehir projeksiyonları gibi birçok alanda kişisel verilerin kullanılması talebinde bulunan taraflar arasında, temel bir insan hakkı olan kişisel verilerin korunması hakkından taviz vermeden denge içerisinde çözümler bulunmaya çalışılmakta ve teknoloji sektörü de kendini buna göre yeniden dizayn etmek için çözüm arayışlarına dahil olmaya çalışmaktadır.

Dünya çapında üretilen veri miktarı katlanarak artarken teknolojik gelişmeler, sürekli üretilme döngüsü içinde bulunan kişisel verilerle hayatın tüm alanlarını olumlu yönde dönüştürme potansiyeline sahiptir. Kişisel verilerin, tüketim planlaması, üretimde verimliliğin sağlanması, trafik çözümleri, çalışma performans iyileştirmeleri, sağlık araştırmaları gibi pek çok alanda kullanılması bu alanda karşılaşılan problemleri daha hızlı ve daha kesin bir şekilde çözüme ulaştırmada oldukça önemli bir yere sahiptir (Waldfogel, 2018) ancak neredeyse tüm dünya çapında kişisel verilerin işlenmesine ilişkin sınırlamalar getiren hukuki düzenlemeler bu tür araştırma ve geliştirme çalışmalarının yapılması için ön şart niteliğinde olan belirli bir kurallar hiyerarşisi getirmektedir.

Üretilen verilerin teknolojik gelişmelerle hayatın her alanında yenilikçi çözümler sunması için bu verileri kişisel veri niteliğinden arındırarak yani kişisel verileri anonim hale getirerek kullanmak bir alternatif olarak ortaya çıkmıştır. Anonim hale getirme yöntemleriyle birlikte birçok problem için çözüm olabilecek olan ve potansiyel halde bekleyen kişisel veriler faydalı hale getirilebilmektedir. Kişisel verilerin anonim hale getirilmesiyle, veri kişisel olma vasfını kaybederek kişisel verileri koruma mevzuatı kapsamından çıkmış olmaktadır. Anonim hale getirme işlemleri doğru yapıldığında, kişisel veri koruma mevzuatı kapsamından çıkartılıp, verilerin daha geniş bir kitleyle paylaşılmasına veya yayımlanmasına izin verilmektedir. Bu nedenle anonim hale getirme, dünya çapında hem kamu sektöründeki hem de özel sektördeki kuruluşlar için oldukça önem arz eden bir konudur.

Anonim hale getirme teknik ve modelleri sayısal ve kategorik formatta olan veri tabanları, tablolar gibi verilere yönelik olarak geliştirilmiştir ancak bu verilerin yanında, sadece görüntü, ses, metin veya konum gibi yapılandırılmamış veriler de kişisel veri seti havuzunun önemli bir bileşeni olarak yer alabilmektedir. Sayısal ya da kategorik formatta olmayan yapılandırılmamış veriler için kullanılacak anonim hale getirme yöntemlerinin, veri tabanı veya tablolar için tercih edilen anonim hale getirme yöntemlerinden farklı olması gerektirecektir.

GÖRÜNTÜ VERİLERİNİN ANONİM HALE GETİRİLMESİ

Günümüzde kameralar, güvenlikten veri madenciliğine, akıllı şehir uygulamalarından yapay zekâ destekli teknolojilerin gelişimine kadar çeşitli konular için her yerde bulunmakta ve kullanılmaktadır. Otonom araçların, yüksek çözünürlüklü haritaların geliştirilmesi, her gün halka açık olarak büyük miktarda görüntü ve video verisinin toplanmasını gerektirir. Kamusal alanları izleyen kameraların artan sayısı aynı zamanda bu kameralarla toplanan verilerin anonim hale getirilmesi ihtiyacını da gündeme getirecektir.

Sayısal veya kategorik formatta olmayan verilerden olan görüntü verilerinin anonim hale getirilmesinde literatürde geçen teknik ve modeller kullanılmaz. Bunun yerine ya bir uzman ya da yapay zekâ kullanan programlar yoluyla daha farklı tekniklerin uygulanması gerekecektir. (Gözüküçük, 2014) Görüntü ve video verilerine uygulanan anonim hale getirme, yüz, vücut veya plaka gibi kişisel verilerin sansürlenmesini veya bozulmasını içerir.

Bu şekilde, görüntülerdeki ve videolardaki kişisel olarak tanımlanabilir bilgiler, yüz veya plaka tanıma yazılımı aracılığıyla kimlik tespitine karşı da korunur. Bu anonim hale getirme, elle yapılabileceği gibi programlar vasıtasıyla da yapılabilir. Bu tür verilerde büyük veri setleri veya çok sayıda kişisel veri için elle çalışma yavaş ve yüksek maliyetli olacaktır. Otomatik çözümler ise çok daha hızlıdır dolayısıyla görüntü ve video verilerinde kimlik korumanın en kolay yolu yapay zekaya dayalı anonim hale getirme yazılımlarıdır. Yapay zekâ teknolojileri, nesneleri al-

gılamada son derece verimlidir ve bu nedenle herhangi bir insan dahil olmadan, hızlı ve güvenli bir şekilde görüntü veya video redaksiyonunu otomatikleştirmek için kullanılabilir.

Şekil 1. Orijinal yüz fotoğrafı ve anonim hale getirilmiş yüz fotoğrafı

Şekil 1'de yapay zekâ tarafında üretilen bir kişiye ait yüz fotoğrafi verilmiştir. Bu fotoğraf otomatik yollarla yapay zekâ kullanan programlar aracılığıyla yüzdeki göz, kaş, burun, ağız, kulak, alın, çene, saç gibi organları değiştirmiş ve sayısal ya da kategorik bir veri olmayan görüntü verisini anonim hale getirilmiştir. Bu tür anonim hale getirmede fayda oranı yüksekken, anonim hale getirilmiş görüntü verisinin yeniden tanımlanma oranı da o derece yüksektir.

Şekil 2. Orijinal yüz fotoğrafı ve anonim hale getirilmiş yüz fotoğrafı

Şekil 2'de başka bir kişiye ait yüz fotoğrafi verilmiştir. Bu fotoğraf otomatik yollarla doğrudan bulanıklaştırılmış ve sayısal ya da kategorik bir veri olmayan görüntü verisini anonim hale getirilmiştir. Bu tür anonim hale getirmede fayda düşükken, anonim hale getirilmiş görüntü verisinin yeniden tanımlanma oranı da o derece düşüktür.

Kişilerin fotoğraflarının veya CCTV'ler aracılığıyla toplanan görüntülerinin yanı sıra, araç plakaları da kişisel veri niteliği taşımaktadır. Şekil 3'te örnek olarak verilen bu araçların plakaları da fotoğraflar gibi ya plaka bilgisi değiştirilerek ya da bulanık hale getirilerek anonim hale getirilmelidir.

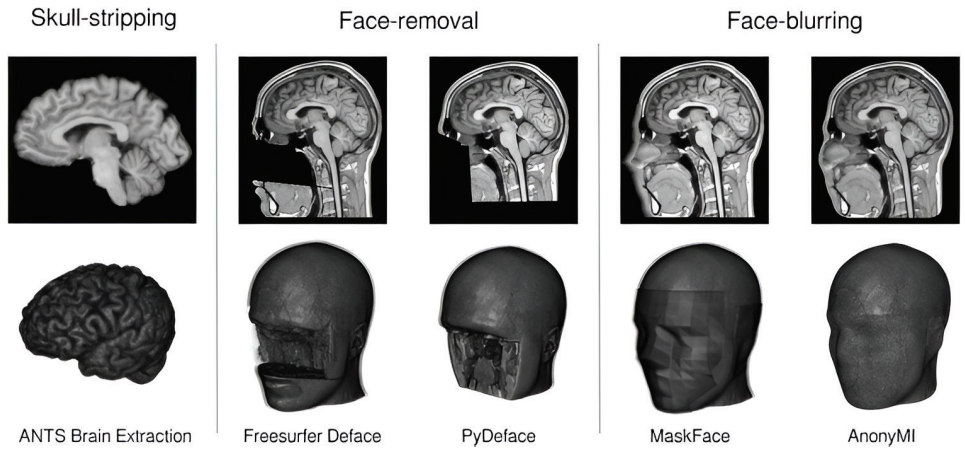
Şekil 3. Sırasıyla orijinal plaka, değiştirilmiş plaka ve bulanıklaştırılmış plaka

Görüntü verileri açısından bir diğer önemli konu ise özel nitelikli kişisel veriler olan MR (Manyetik Rezonans) ve BT (Bilgisayarlı Tomografi) gibi görüntüleme yöntemleri sonucunda elde edilen görüntülerdir. MR ve BT yöntemleri biyomedikal araştırmalarda yaygın olarak kullanılmaktadır. Kafanın MR ve BT görüntüleri, yüzün yüksek çözünürlüklü temsillerini oluşturmak için kullanılabilir ve potansiyel olarak bu tür araştırmalara dahil olan insanların tanımlanmasına izin verebilir. MR (Manyetik Rezonans) ve BT (Bilgisayarlı Tomografi) görüntülerinin anonim hale getirilmesi oldukça önemlidir çünkü bu görüntülerin anonim hale getirilmesi sonunda hem fayda hem de gizlilik oranı yüksek olmalıdır. Bu görüntülerin anonim hale getirilmesi ilk başta gereksiz görünebilir, zira meşru bir amaç için görüntü verilerinin işlenmesi söz konusudur ancak otomatik yüz tanıma yazılımlarındaki ilerleme kişilerin MR ve BT görüntülerinden tanımlanmasını mümkün kılabilir. Otomatik yüz tanıma yazılımları, BT taramalarının 3 boyutlu görüntülerini çok yüksek bir oranda fotoğraflarla eşleştirebilmiştir.

Şekil 4'te gösterildiği üzere, MR görüntülerinin anonim hale getirilmesi için üç örnek sunulmuştur. İlk grupta kafatası soyma örneği, 2. grupta yüz kaldırma örneği, 3. ve 4. gruplarda yüz bulanıklaştırma örnekleri gösterilmiştir ve bu yollarla özel nitelikli kişisel veriler arasında yer alan MR görüntüleri anonim hale getirilmiştir. (Eke ve diğerleri, 2021).

Görüntü verilerinin anonim hale getirilmesinin tamamen bir yazılımla yapılmasının etkili bir anonim hale getirme yöntemi olmadığı durumlar söz konusu olabilmektedir. Çünkü, yazılımların düşük kaliteli veriler, karmaşık görüntüler ya da geniş açılı görüntülerde veya videoda nasıl performans göstereceği belirsizdir. Örneğin, bazı durağan görüntülerden yüz bölümü değiştirilmiş ya da maskelen-

miş bir kişi dövmeleri veya kendine has bir giyim tarzı gibi özellikleri sayesinde tanımlanabilir; dolayısıyla yapılandırılmamış veriler arasında yer alan görüntü ve video verilerinin anonim hale getirilmesinde verilerin durumu ve verilerin taşıdığı riske göre yazılım haricinde bir uzman kullanıcının müdahalesi gerekebilecektir.



Şekil 4. 3 boyutlu hale getirilmiş MR görüntüsünün anonim hale getirilmesi

SES VERİLERİNİN ANONİM HALE GETİRİLMESİ

Sosyal medyayla beraber kullanıcıların ses, görüntü, video gibi multimedya belgelerini kolayca yükleyebilecekleri ve paylaşabilecekleri çok sayıda internet hizmeti üretilmiş durumdadır. Bu tür hizmetlerin popülaritesine ve rahatlığına rağmen, konuşma verileri de dahil olmak üzere bu tür doğası gereği kişisel verilerin paylaşılması, güvenlik ve gizlilik endişelerine sebep olmaktadır. Özellikle, bir kullanıcının ses verileri, aynı kullanıcının konuşmacı kimliğini yansıtan yüksek kaliteli konuşma ifadeleri üretmek için konuşma sentez sistemleriyle birlikte alınabilir ve kullanılabilir. Bu ifadeler daha sonra ses doğrulama sistemlerine saldırmak için kullanılabilir. Birkaç saniyelik referans konuşmalardan, ilgili kişiye ait tüm sesleri üretmek mümkün olabilmektedir. (Fang ve diğerleri, 2021)

Akıllı şehirlere yönelik uygulamalarda gürültü kirliliğini izlemek amacıyla kamusal alanlardan veri toplanabilmektedir. Mekanlar kamusal alanlar olsa da ortamdaki insanlar algılayıcılar tarafından ne derece kaydedilebileceklerini tam olarak bilemeyebilir ve bu da mahremiyetin ihlali olarak görülebilir dolayısıyla kamusal alanlarda kaydedilen insanların seslerini anonim hale getirmek gereklidir. Görüntü verilerinin anonim hale getirilmesinde bahsedildiği gibi sesler de bu işe

özgü uygulamalarla bulanıklaştırılarak, genlik, incelik, kalınlık, bas, tiz, perde gibi özellikleri değiştirilerek anonim hale getirilebilmektedir. (Fang ve diğerleri, 2021)

Ses verilerinin anonim hale getirilmesinin tamamen bir yazılımla yapılmasının etkili bir anonim hale getirme yöntemi olmadığı durumlar söz konusu olabilmektedir. Örneğin kontrollü ses bozulması kullanarak ses verileri belli bir derecede anonim hale getirilebilmektedir. Ses bozulması sonucunda, yalnızca konuşmacının sesine göre tanımlamayı önleyebilir, ancak konuşma kalıpları veya konuşmada isimlerden bahsedilmesi gibi ses parçasında bulunabilecek diğer tanımlayıcı ipuçlarını kaldıramaz.

METİN İÇEREN VERİLERİN ANONİM HALE GETİRİLMESİ

HÂKİMLER VE SAVCILAR KURULU
İKİNCİ DAİRE KARARI

Esas No	Karar No	Karar Tarihi
.....	.....	.....

Hâkimler ve Savcılar Kurulu İkinci Dairesi aşağıda isimleri yazılı üyelerin katılımı ile ..... tarihinde toplandı.

..... **Cumhuriyet Savcısı** ..... hakkında, Hâkimler ve Savcılar Kurulu ..... Dairesinin ..... sayılı soruşturma evrakı ile ..... tarihli ve ..... sayılı soruşturma izni üzerine HSK Başmüfettişi tarafından düzenlenen ..... tarihli soruşturma raporu ve eki evrak havi Dairemizin ..... sayılı dosyası incelendi.

..... **Cumhuriyet Savcısı** ..... **hakkında yapılan soruşturma:**
Belirlenen durum ve sürelerde mal beyanında bulunmadığı, bu cümleden olarak;
A) ..... tarihinde edinilen ..... TL bedelli hususi otonun ..... ,
B) ..... İli, ... ilçesindeki hisseli arsaların ..... tarihinde satışından gelen ..... -TL'nin çevrildiği ..... USD dövizin ..... ,
Tarihlerindeki ek ve genel beyanlarına gecikmeli olarak bildirildiği,
Konusundan ibarettir.

İLGİLİNİN SAVUNMASI KARARTILMIŞTIR.

Şekil 5. HSK'nın internet sayfasında yer alan anonim hale getirilmiş bir disiplin cezası

Görüntü ve ses verileri gibi metin içeren veriler de sayısal veya kategorik formatta olmayan veriler arasında yer alır. Metnin anonim hale getirilmesi sonucunda hem anlamlı ve işe yarar bir metin elde etmek hem de gizliliği muhafaza sağlamak için en çok tercih edilen teknik maskeleme tekniğidir.

Kişisel Verileri Koruma Kurulu'nun internet sayfasındaki bazı kararlar ve başka bir örnek olarak Hakimler ve Savcılar Kurulu'nun internet sayfasında bazı disiplin kararları kamuya açık olarak yayımlanmaktadır. Bu kararlarda yer alan kişisel veriler bazı verilerin maskelenmesi veya bazı verilerin metinden tamamen çıkarılmasıyla anonim hale getirilmiştir. Şekil 5'te gösterildiği gibi Hakimler ve Savcılar Kurulu tarafından verilen bir disiplin cezasında kişisel verilerin tanımlanmasını mümkün kılabilecek veri alanları boş bırakılarak ve bazı bölümler karartılarak burada yer alan veriler çıkarılmıştır. (HSK Disiplin Kararları, 2021)

KONUM VERİLERİNİN ANONİM HALE GETİRİLMESİ

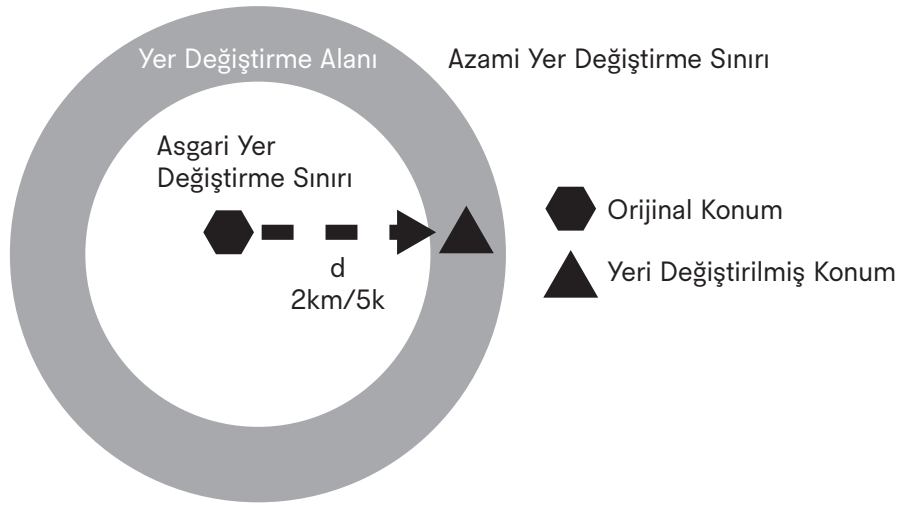
GPS (Global Positioning System: Küresel Konumlandırma Sistemi) teknolojilerindeki gelişmeler, kullanıcıların konumunu kullanan çeşitli hizmetlerin ortaya çıkmasını sağlamıştır. Cep telefonları, akıllı saatler, navigasyon cihazları, araçlardaki akıllı sistemler aracılığıyla GPS'in kullanımı günden güne artmaktadır. Konum bilgisinin, kendisiyle beraber başka verileri açığa çıkarabilme potansiyelinden dolayı konum gizliliğinin korunması başlı başına büyük bir önem arz etmektedir.

Cep telefonları, akıllı saatler ve GPS cihazları, insanların ve araçların hareketlerini algılar ve izler, mahalle, ilçe, il ve ülke çapında hareketlilik veri tabanları üretir. Hareketlilik verileri yeni ürün ve hizmetler için önemli bir kaynak olmasına rağmen, bu verilerin anonim hale getirilmeden ya da yeterli şekilde anonim hale getirilmeden yayımlanması veya üçüncü taraflarla paylaşılması yanında çok büyük riskleri beraberinde getirmektedir. GPS hareketlerinin anonim hale getirilmesi yani ilgili kişilerin kimliğinin çıkarılması genellikle çok zayıf bir korumadır. Belçika'daki 1,5 milyon cep telefonu kullanıcısının 15 aylık verilerinden anonim hale getirilmiş bir veri setini analiz edilmesiyle tespit edilen dört referans noktasına göre ilgili kişiler %95 oranında yeniden tanımlanabilmiştir. (Montjoye, Hidalgo, Verleysen, Blondel, 2013).

GPS ya da diğer teknolojik aletlerden elde edilen konum verilerinin yanı sıra giderek artan anket sonuçlarıyla veya kamusal ihtiyaçlar için toplanan veri tabanlarıyla beraber ayrıntılı coğrafi konum verileri toplanmaya başladı. Bu veriler, araştırmacılar tarafından mekânsal etki araştırmasında kullanılırken, farklı kaynaklardan gelen verileri de kullanabilmekte ve bu farklı veri setlerinin ilişkilendirilerek anonim hale getirilmiş verilerin yeniden tanımlanma riski ortaya çıkmaktadır.

Konum verilerini anonim hale getirmenin bir yolu, CBS (Coğrafi Bilgi Sistemleri) özniteliklerini kaldırmak ve bunun yerine il, bölge gibi diğer coğrafi öznitelikleri

kullanmak veya bu öznitelikleri oluşturmaktır. Ancak bu yaklaşım, konum verilerinin faydalarını da ortadan kaldırır. Diğer bir seçenek de konum verilerinin yer aldığı alanların veya kayıtların yerlerinin değiştirilmesi veya karıştırılmasıdır. (Emam ve Arbuckle, 2013).



Şekil 6. Konum verilerinin 2-5 km'lik mesafeler içinde yerlerinin değiştirilmesi

Konum verilerinin anonim hale getirilmesi, iki düzeyde gerçekleştirilebilir: ilk olarak, aynı numaralandırma alanından gelen veriler tek bir nokta koordinatında toplanır; daha sonra koordinat, GPS (küresel konumlandırma sistemi) koordinat yer değiştirme işlemi kullanılarak maskelenir. İkinci olarak, GPS koordinat yer değiştirme süreci Şekil 6'da gösterildiği gibi şu şekilde gerçekleştirilir: kentsel alanlardaki verilerin iki kilometreye (0-2 km) kadar bir mesafe içinde yeri değiştirilir, kırsal alanlardaki verilerin beş kilometreye (0-5 km) kadar bir mesafe içinde yeri değiştirilir, kırsal alanlardaki verilerin daha seyrek alanlar içinde seçilenleri ise 10 kilometreye (0-10 km) kadar bir mesafe içinde yeri değiştirilir.

SONUÇ

Teknolojik gelişmelere bağlı olarak hem akıllı cihazların hayatın ayrılmaz bir parçası olması hem de kişisel verilerin bir değer teşkil etmesi, kişisel verilerin korunması ihtiyacını ortaya çıkarmıştır. Bilgi toplumun yükselişiyle bu ihtiyaca binaen bir hak olarak ortaya çıkan kişisel verilerin korunması hakkı hukuki metinlerdeki yerini günden güne artırmaktadır. Kişisel verilerin korunmasına yönelik anayasal ve yasal düzenlemelerin yanında daha alt dallara ilişkin olarak kişisel verilerin işlendikleri amaç için gerekli olan azami süre sonunda yok etme, silme ve anonim hale getirme işlemlerinden birinin uygulanması gerekliliği ve anonim hale getirmeye dair kuralların ülkemizde yönetmelik seviyesinde bir hukuki metinle düzenlenmesi bu konuya verilen önemin bir göstergesidir.

Kişisel verilerin anonim hale getirilmesiyle bu verilerden araştırma, dış kaynak kullanımı, iş birliği, açık veri, veri ambarı, halk sağlığı ve gözetimi, tıbbî cihazlar, yazılım testi gibi konularda istifade edebilmek mümkündür. Veri sorumluları kişisel verileri anonim hale getirerek bahsi geçen konularda fayda temin edebilmesinin yanında veri sorumluları veri ihlali gibi olumsuz sonuçların önüne geçmek amacıyla kişisel verilerin anonim hale getirilmesini tercih edebilmesi mümkündür.

Kişisel verilerin anonim hale getirilmesinde uygulanacak teknik ve yöntemler her veri seti için farklılık gösterdiğinden tek bir anonim hale getirme teknik ve yöntemi bulunmamaktadır. Etkili bir anonim hale getirme için her bir veri setinin özellikleri ayrı ayrı değerlendirilmeli ve anonim hale getirme sonrası için risklere yönelik çalışmalar planlanmış olmalıdır. (Elliot ve diğerleri, 2015)

Kişisel veri içeren veri setlerinin anonim hale getirilmesi bahsi geçen yönetmelikle yok etme ve silmenin alternatifi olarak görülmektedir ancak bununla birlikte anonim hale getirmenin asıl amacı büyük bir potansiyel taşıyan veri setlerini kişisel verilerden arındırarak bu veri setlerinden fayda sağlamaktır. Anonim hale getirmeden elde edilecek faydanın miktarı riskle doğru orantılıdır dolayısıyla fayda arttıkça kişisel verilerin yeniden tanımlanma riski o düzeyde artacaktır ve bu süreçte bir ödünleşme gündeme gelecektir. Azami düzeyde fayda elde etmeye yönelik bir anonim hale getirme sonucunda yeniden tanımlama risk düzeyi de azami noktaya ulaşacağından etkili bir anonim hale getirmeden söz etmek mümkün olmayacaktır.

Etkili bir anonim hale getirme için düşük risk sağlamak amacıyla fayda oranından da taviz verilerek üretilmiş bir anonim hale getirilmiş veri setinin bile ne kadar süreye kadar güvenli bir şekilde anonim kalacağı büyük bir problem alanıdır zira akıllı ev sistemlerinden mobil cihazlara kadar çeşitli teknolojik cihazlar tarafından anbean üretilen kişisel verilerle sürekli büyüyen kişisel veri hacmi, yeniden tanımlanma riskini sürekli beslemektedir.

Hem kişisel verilerin korunması hakkından vazgeçmeden hem de anonim hale getirilmiş verilerin yeniden tanımlanma riskinin önüne geçmek amacıyla anonim hale getirilmiş verilerin kamuya açılmasına, açık veri olarak sunulmasına kısıtlamalar getirilmesi bir çözüm olabilir. Buna ek olarak, kişisel verilerin ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesinin zorunlu olduğu gibi, anonim hale getirilmiş veri setlerinin de ilanihaye değil ancak belirli bir süre boyunca saklanmasının zorunlu tutulması yeniden tanımlanma riski için önemli bir tedbir olarak görülebilir. ◆

KAYNAKÇA

- El Emam, K., Arbuckle, L. (2013) Anonymizing Health Data: Case Studies and Methods to Get You Started. Kaliforniya: O'Reilly Media.
- Eke, D., Aasebo, I., Akintoye S., Kinght, W. ve Karakidis, A. (2021). Pseudonymisation of neuroimages and data protection: Increasing access to data while retaining scientific utility. Neuroimage: Reports, Cilt 1 (4), 1-12. DOI: https://doi.org/10.1016/j.ynirp.2021.100053.
- Elliot, Mark, MACKEY, Elaine, O'HARA, Kieron, TUDOR, Caroline, The Anonymisation Decision-Making Framework, UKAN Publications, 2016.
- Fang, F., Wang, X., Yamagishi, J., Echizen, I., Todisco, M., Evans, N., Bonastre, J. F. (2019). Speaker Anonymization Using X-Vector and Neural Waveform Models. https://doi.org/10.48550/arXiv.1905.13561 adresinden 24.11.2021 tarihinde alınmıştır.
- Gözüküçük, M, (2014). Veri İşleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonim Hale Getirmesi, (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi, İstanbul.
- Hakimler ve Savcılar Kurulu, Disiplin Kararları, https://www.hsk.gov.tr/disiplin-kararlari_1419 adresinden 11.12.2021 tarihinde alınmıştır.
- Montjoye, Y., Hidalgo, C. A., Verleysen, M., Blondel, V.D., Unique in the crowd: The Privacy Bounds of Human Mobility. Scientific Reports, Sayı 3, Yıl 2013, 1-5. DOI:10.1038/srep01376.
- Waldfogel, J. (2018) Digital Renaissance, Princeton: Princeton University Press.

KARŞILAŞTIRMALI AVRUPA BİRLİĞİ VE TÜRKİYE UYGULAMALARI: YURT DIŞINA VERİ AKTARIMI YÖNTEMİ OLARAK STANDART SÖZLEŞME HÜKÜMLERİ VE TAAHHÜTNAME

Göksu Hazar ERDİNÇ
Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "Yurt Dışına Veri Aktarımı: Karşılaştırmalı Avrupa Birliği ve Türkiye Uygulamaları" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Günümüzde teknolojinin de artmasıyla birlikte dijitalleşme artmış, fiziksel ortamda artan veri paylaşımı yerini sanal ortama bırakmıştır. İçinde kişisel veriyi de barındıran *"veri"* kavramı, birçok sektör bakımından en önemli kaynaklardan biri haline gelerek ekonomiyi şekillendiren en önemli unsurlardan biri olmuştur.

Bahsi geçen hususlar ile kişisel verilerin hem uluslararası hem ulusal boyutta korunması gereksinimini ortaya çıkmıştır. Keza, bu gereksinim ülkemizde 2010 yılında Türkiye Cumhuriyeti Anayasasının 20. maddesinde yapılan değişikliği takiben, 7 Nisan 2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanununun (6698 sayılı Kanun) yayımlanarak yürürlüğe girmesiyle son bulmuştur.

6698 sayılı Kanun ile kişisel verilerin korunmasına yönelik temel başlıklar belirlenerek bu başlıklara ilişkin çeşitli düzenlemeler getirilmiştir. Bu çerçevede, kişisel verilerin işlenmesine ilişkin genel ilkeler, kişisel verilerin işlenmesi şartları,

kişisel verilerin yurt içinde ve yurt dışında aktarımı, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi, aydınlatma yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, Veri Sorumluları Siciline kayıt yükümlülüğü başta olmak üzere veri sorumlularına getirilen yükümlülükler, kişisel verileri işlenen ilgili kişilerin hakları, istisnalar gibi hususlar 6698 sayılı Kanun kapsamında düzenlenmiştir.

Ulusal ve uluslararası pek çok hukuksal düzenlemede belirtildiği üzere kişisel veri genel olarak *"belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi"*yi ifade etmektedir. (Küzeci, 2020). Kişisel verileri işlenmesi kavramına ilişkin tanım da aynı şekilde büyük oranda benzer olup, 6698 sayılı Kanundaki tanım göz önünde bulundurulduğunda, *"kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi"* (Bkz. 6698 sayılı Kanun madde (m.) 3(1)(e)) ifade etmektedir. Kişisel verilerin işlenmesi tanımından da görülebileceği üzere aktarım da bir kişisel veri işleme faaliyeti olup ilgili mevzuatta öngörülen düzenlemelere tabi olacaktır.

Bununla birlikte, aktarımın ne olduğuna ilişkin olarak Ekonomik Kalkınma ve İş Birliği Örgütünün (OECD) görüşleri dışında veri koruma mevzuatlarında herhangi bir tanıma yer verilmemiştir. Aktarım kavramına ilişkin olarak genel geçer söylenebilecek tek şey, kişisel veri işleme faaliyetinin bir parçası olduğudur.

Ticaret, bankacılık, sanayi, turizm sektörleri başta olmak üzere birçok sektörde kişisel veri aktarımı gerçekleşmektedir. Ancak, birçok ülkenin iç hukuk düzenlemeleri kişisel verilerin sınır ötesi aktarımına ilişkin uygun güvencelerin sağlanmasını teminen farklı koruma kuralları öngörebilmektedir. Bazı ülkelere göre yurt dışına veri aktarımı müessesesi katı kurallara tabi iken bazı düzenlemeler uyarınca çok daha esnek olabilmektedir. Örneğin, Katar'ın kişisel veri düzenlemesi olan *"Kişisel Veri Mahremiyetini Koruma Kanunu"*nun 15 inci maddesinde aktarım faaliyetinin bu kanun hükümlerine aykırı olması veya ilgili kişinin kişisel verilerine ya da mahremiyetine önemli derecede zarar verebileceği durumlar hariç olmak üzere kişisel verilerin sınır-ötesi aktarımının veri sorumluları tarafından sınırlandırılmasının yasak olduğu hüküm altına alınmıştır. Öte yandan Avrupa Birliği (Birlik) ile ülkemiz düzenlemelerine göre yurt dışına veri aktarımının gerçekleşebilmesi ise mevzuattaki koşulların bulunmasına bağlıdır.

Çeşitli ülkelerin kişisel verilerin korunmasına ilişkin mevzuatları farklılık gösterdiğinden yukarıda da yer verilen sektörler bakımından veri akışı meselesi değer kazanmış olup, her alanda mahremiyetin korunması meselesi önemli hale gelmiştir. Dijitalleşen dünyada gerçekleşen hızlı veri akışı, mahremiyet açısından riskler barındırdığından iki konu arasında köprü kurmak son derece önem teşkil etmektedir. Diğer bir deyişle, kişisel verilerin işlenmesi faaliyeti ile özel hayatın gizliliğinin dengelenmesi önem arz etmektedir.

Yurt dışına veri aktarımı konusu 6698 sayılı Kanunun 9. maddesi altında düzenlenmiş olup, anılan hükümde yeterli korumanın bulunduğu ve bulunmadığı durumlarda aktarımın ne şekilde gerçekleşeceğine yönelik hükümler almaktadır. Benzer şekilde, Birlik hukukunda da yurt dışına veri aktarımı meselesi "Bölüm V" altında düzenlenmiş olup aktarıma ilişkin genel ilkeler, yeterlilik kararına dayanan aktarımlar, uygun tedbirlere tabi aktarımlar ve istisnalar başlıklarına ilişkin hükümlere yer verilmiştir.

Bu noktada belirtmek gerekir ki, halihazırda Birlik mevzuatına uyum çerçevesinde ülkemizin çeşitli strateji belgelerinde ve eylem planlarında 6698 sayılı Kanunun Birlik müktesebatı ile uyumlaştırılması öngörülmektedir. Bu kapsamda, 11 inci Kalkınma Planında, İnsan Hakları Eylem Planında, Türkiye Uluslararası Doğrudan Yatırım Stratejisi (2021-2023)'nde ve 2021 Yatırım Ortamını İyileştirme Koordinasyon Kurulu (YOİKK) Eylem Planı ile 2022 YOİKK Taslak Eylem Planında bu yönde hedeflere yer verilmektedir. Uyumlaştırılması önem teşkil eden maddelerden biri de yurt dışına veri aktarımını düzenleyen 9. madde olup, bu anlamda Kanun uyum çalışmaları kapsamında da Birlik uygulamaları ile Türkiye uygulamalarının karşılaştırılmasının son derece önem teşkil ettiği değerlendirilmektedir. Bu noktada farklılık arz eden yöntemlerden biri de Komisyon tarafından onaylanan ve herhangi bir izin mekanizmasına gerek olmayan *"Standart Sözleşme Hükümleri"*dir.

Öte yandan, Kişisel Verileri Koruma Kurulu (Kurul) kararlarında yer alan değerlendirmelerde uygun olduğu ölçüde Birlik uygulamalarına da yer verildiği görülmekte olup, Birlik'in kişisel veri alandaki içtihadının Kişisel Verileri Koruma Kurumu (Kurum) açısından da önem arz ettiği değerlendirilmektedir.

Bu çerçevede, bu çalışma kapsamında hem Ülkemizde yurt dışına veri aktarımı için öngörülen önemli yöntemlerden biri olan Taahhütnameler hakkında bilgi verilecek hem Avrupa Birliği uygulamalarının önemli bir parçası olması hasebiyle *"Standart Sözleşme Hükümleri"* (SCC metni) hakkında detaylı bilgi verilerek olası bir kişisel veri mevzuatı revizyonuna ilişkin ışık tutulmaya çalışılacaktır.

6698 SAYILI KANUN KAPSAMINDA TAAHHÜTNAMELER

6698 sayılı Kanunun 9. maddesinin (2) numaralı fıkrasının (b) bendi, *"(...) b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir."* hükmünü amirdir. Mezkûr hükümden de görülebileceği üzere, Kurul tarafından verilmiş bir yeterlilik kararının bulunmaması durumunda yurt dışına veri aktarımı Kurul tarafından izne tabi olup, bu izin mekanizmalarından biri de *"Taahhütnameler"*dir.

Kurum tarafından hem veri sorumlusundan veri sorumlusuna hem de veri sorumlusundan veri işleyene gerçekleştirilecek yurt dışına kişisel veri aktarımlarında kullanılmak üzere iki tür taahhütname hazırlanmış olup, *"Kurul'un 02/04/2018 tarih ve 2018/33 numaralı kararı ile kişisel verilerin, Türkiye'de yerleşik veri sorumlusu tarafından yeterli veri koruması bulunmayan ülkelerde yerleşik veri sorumlusuna aktarımına ilişkin olarak 6698 sayılı Kanunun 9 uncu maddesinin (2) numaralı fıkrasının (b) bendine istinaden hazırlanacak taahhütnamelerde bulunması gereken asgari unsurlar"* Kurum resmi internet sitesinde yayımlanmıştır. Yurt dışına kişisel veri aktarımı gerçekleştirmek amacıyla yapılan başvurular, Kurumun ilgili birimleri tarafından hukuki ve teknik boyutlarıyla incelenmekte olup, yapılan inceleme sonucunda başvuruculara geri dönüş yapılarak eksikliklerin tamamlanması veya düzeltmelerin yapılması için gerekli yönlendirmeler yapılmaktadır.

Ayrıca, Taahhütnamelerin hazırlanmasında veri sorumluları tarafından dikkat edilmesi gereken gerek usule gerek esasa ilişkin hususlar ile ilgili *"Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru"* (Duyuru) başlıklı bir kamuoyu duyurusu hazırlanarak Kurum resmi internet sitesinde 7 Mayıs 2020 tarihinde yayımlanmıştır. Söz konusu Duyuruda Taahhütname hazırlanırken usule ve esasa ilişkin dikkat edilmesi gereken hususlar detaylı bir şekilde açıklanmıştır. Bu çerçevede, veri sorumlularının Taahhütname doldururken dikkat etmeleri gereken hususlara ilişkin açıklamalara aşağıdaki alt başlıklar altında yer verilecektir.

Usule İlişkin Olarak Dikkat Edilmesi Gereken Hususlar

Kurumun 7 Mayıs 2020 tarihli Duyurusunda usule ilişkin dikkat edilmesi gereken hususlar, aşağıdaki şekilde sayılmıştır:

- Kuruma intikal eden başvurularda başvuruculara başvurmaya yetkili olduğunu gösterir tevsik edici bilgi ve belgeleri Kuruma iletmesi gerekmektedir. Duyuruda da ifade edildiği üzere, *"(...) tüzel kişiler tarafından yapılacak başvuruların, ilgili veri sorumlusunu bu konuda temsil ve ilzama yetkili kişiler tarafından yapılması ile başvuruya bu hususu tevsik edici belgelerin eklenmesi; ayrıca, vekil marifetiyle yapılacak başvurularda da vekâletname aslı veya onaylı örneğinin bulunması gerekmektedir."* ("Kişisel Verileri Koruma Kurumu", 2020).

- Taahhütnamede ve Ek-1 kısmında başvuruda bulunan her iki tarafın da parafı, en sondaki imza kısmında da kaşe ve imzanın bulunması gerekmektedir. (Kişisel Verileri Koruma Kurumu, 2020). Bu noktada, her iki tarafın da hem Taahhütnameyi hem Taahhütname Ek-1'i içeren bütün sayfaları paraflamalıdır. İmza kısımları ise ilgili metinlerin en son kısmında yer almaktadır.

Veri Aktaran Adına	Veri Alıcısı Adına
Ad Soyad: Açık Adres: İrtibat Numarası: E-posta: (Varsa sözleşmenin bağlayıcı olması için belirtilmesi gereken diğer bilgiler) İmza/Kaşe	Ad Soyad: Açık Adres: İrtibat Numarası: E-posta: (Varsa sözleşmenin bağlayıcı olması için belirtilmesi gereken diğer bilgiler) İmza/Kaşe

Şekil 1. Taahhütname imza kaşe kısmı

- Yine başvuruda imzası bulunan kişilerin yetkilerini tevsik eden her türlü açıklayıcı bilgi ve belgeye Taahhütname başvurusu kapsamında Kuruma iletilmelidir. (Kişisel Verileri Koruma Kurumu, 2020). Bu durum ise Duyuruda;

"3. İmzacıların yetkisini göstermesi bakımından, Taahhütname ekine Türkiye'de mukim şirketler için ticaret sicili müdürlükleri tarafından düzenlenen sicil tasdiknamesi, Yabancı Resmî Belgelerin Tasdiki Mecburiyetinin Kaldırılması Sözleşmesine taraf olan ülkelerde mukim veri alıcısı bakımından ise imzalayanın imzaya yetkili olduğunu gösterir apostil şerhli belgenin aslı veya onaylı örneği eklenmelidir. Anılan Sözleşmeye taraf ülkelerin resmi makamlarınca hazırlanmış her belgede apostil şerhi bulunmalı, Sözleşmeye taraf ol-

mayan ülkeler bakımından ise, belgelerin Türkiye'de hukuken geçerli olmasına ilişkin süreç işletilmelidir."

şeklinde ifade edilmiştir.

Görüldüğü üzere, yurt dışı menşeili şirketlerde başvuruculaların yetkisini göstermesi bakımından *"Yabancı Resmî Belgelerin Tasdiki Mecburiyetinin Kaldırılması Sözleşmesi"*ne taraf olan ülkeler bakımından apostil şerhli belgelerin aslı veya onaylı örneklerinin, taraf olmayan ülkeler bakımından belgelerin Türkiye'de geçerli olmasına ilişkin sürecin yürütülerek (sunulacak belgelerin noter onaylı çevirisinin bulunması gibi) Kuruma başvuruda bulunulmalıdır (Kişisel Verileri Koruma Kurumu, 2020).

Bu çerçevede, Kuruma iletilecek her bir belgenin hangi yabancı dilde olursa olsun noter onaylı çevirisinin bulunmasının zorunlu olup, öte yandan Kuruma intikal eden başvurularda sunulan belgelerin Türkçesi esas alınacaktır. Dolayısıyla belgenin Türkçesi ile kendisi arasında çeviriden kaynaklı farklılıkların bulunması durumunda yabancı dilde olan belgenin esas alınması talep edilemeyecek olup, herhangi bir çelişkinin bulunması durumunda başvurucular esas olarak Türkçe olarak sundukları içerikten sorumlu olacaklardır.

Yabancı dildeki **her belgenin noter onaylı çevirisi** başvuruda bulunmalıdır.	Özellikle yabancı dildeki sunulacak olan **apostil şerhli belgelerin** aslı veya onaylı örneklerinin de noter onaylı çevirilerinin mutlaka başvurulara eklenerek kuruma sunulması gerekmektedir.	İdari ve teknik tedbirler için kuruma sunulan tevşik edici yabancı dildeki belgelerin de (sertifika vb.) noter onaylı çevirileri bulunmalıdır.

Şekil 1. Yabancı dildeki belgelerin kuruma iletilmesinde usul bakımından dikkat edilmesi gereken hususlar (Kişisel Verileri Koruma Kurumu, 2020).

Diğer taraftan, 6102 sayılı Türk Ticaret Kanunun *"Tescil ve ilan"* başlıklı 373. maddesinin (3) numaralı fıkrasında, *"(3)Kamu kurum ve kuruluşları tarafından, ticaret siciline tescil olunan temsile yetkili kişiler ile bunların temsil şekilleri hakkında ticaret sicili kayıtları esas alınır ve şirketten bu kayıtlara ilişkin ticaret sicili mü-*

dürlüklerince düzenlenen belgeler ile Türkiye Ticaret Sicili Gazetesinde yayımlanan ilan dışında hiçbir belge istenemez." düzenlenmiş olup, söz konusu hükme ilişkin değişiklik 3 Şubat 2021 tarihinde 31384 sayılı Resmi Gazete'de yayımlanmıştır. Anılan maddenin gerekçesinde de belirtildiği üzere, MERSİS ve Türkiye Ticaret Sicili Gazetesinden sermaye şirketlerinin temsil şekilleri ile bu şirketi temsil edenlerin bilgileri görüntülenebilmekte olup, hukuki işlem güvenliğinin sağlanmasını teminen pek çok kamu kurum ve kuruluş, başvuran şirketlerden imza sirküsü gibi aslında mevzuatımızda bulunmayan ancak zaman içerisinde uygulamada ortaya çıkan ilave belgeler talep edebilmektedir (Türkiye Büyük Millet Meclisi, 2022). Gerekçede devamla (Türkiye Büyük Millet Meclisi, 2022);

"Ticaret sicili kayıtları anlık olarak MERSİS'e işlendiğinden ve elektronik ortamda anlık olarak görüntülenebildiğinden esasında imza sirküsü gibi belgeler tek başına hukuki işlem güvenliğini sağlamaya yetmemektedir. Kaldı ki, tescil ve ilan olunan bir olgu ile ilgili olarak, üçüncü kişiler imza sirküsüne güvenerek işlem yapmış olsa dahi, 6102 sayılı Türk Ticaret Kanunu'nun 36 ncı maddesinin üçüncü fıkrası uyarınca, üçüncü kişilerin kendilerine karşı sonuç doğurmaya başlayan ticaret sicili kayıtlarını bilmediklerine ilişkin iddiaları dinlenmeyeceğinden mağduriyet yaşamaları da kaçınılmaz olmaktadır. Ayrıca benzer belgelere ihtiyaç duyulması tacirin hem zaman hem de mali açıdan ilave yükümlülüklere neden olmaktadır.

Bu minvalde, 6102 sayılı Türk Ticaret Kanununun 373 üncü maddesine eklenen üçüncü fıkra ile; ticaret siciline tescil olunan temsile yetkili kişiler ile bunların temsil şekilleri hakkında kamu kurum ve kuruluşlarınca ticaret sicili müdürlüklerince düzenlenen belge ve Türkiye Ticaret Sicili Gazetesinde yayımlanan ilanlar dışında ilave belge aranmaması hususunda düzenleme yapılarak hukuki işlem güvenliğinin sağlanması ve tacirler bakımından ilave işlem ve maliyet doğuran uygulamanın sonlandırılması amaçlanmaktadır."

ifade edilmiş olup, kamu kurum ve kuruluşlarının şirketlerden imza sirkülerini talep etmesi müessesesini ortadan kaldırmıştır. Dolayısıyla imza sirküleri zorunlu olmamakla birlikte, Taahhütname başvurularında şirketlerin onaylı sicil tasdiknamelerini Kuruma göndermeleri yeterli olacaktır.

- Öte yandan Kurumun resmi sitesinde iki model Taahhütname örneği bulunmaktadır. Bunlardan biri *"Veri Sorumlusundan Veri Sorumlusuna Aktarım"*a; diğeri ise *"Veri Sorumlusundan Veri İşleyene Aktarım"*a ilişkindir. Kurul'dan yurt dışına kişisel veri aktarımı için izin talep eden Başvurucu, Kurumu resmi internet sitesinde yayımlanan Taahhütname örneklerinde yer alan hüküm-

lere asgari olarak aynen yer vermeli, ilave hükümler eklemek istemesi durumunda ise ilave hususlara *"İlave Hükümler"* başlığı altında ayrıca yer vermelidir (Kişisel Verileri Koruma Kurumu, 2020). Her ne kadar Kuruma iletilen bazı başvuruların GVKT esas alınarak hazırlandığı argümanı öne sürülerek Kurum internet sayfasında yer alan başvuru şablonlarından farklı olduğu görülse de, başvurunun GVKT'ye uygun hazırlanması 6698 sayılı Kanuna da uygun olduğu anlamına gelmeyeceğinden Kurum tarafından hazırlanmış olan başvuru şablonları esas alınmalıdır.

- Yine Duyuruda belirtildiği üzere, başvurucu veri sorumlularının taahhüt içeren cümlelerde gelecek zaman kipini kullanmaları vurgulanmıştır (Kişisel Verileri Koruma Kurumu, 2020).

- Ayrıca Kuruma başvuran veri sorumlusu şirketin Kuruma başvurduğu esnada birleşme, bölünme, tür değiştirme gibi işlemleri söz konusu ise, söz konusu işlemler bitince sonucundan Kurul'a haber vermesi, güncel unvanı ile başvuruda bulunması gerekmektedir.

Esasa İlişkin Olarak Dikkat Edilmesi Gereken Hususlar

- Veri sorumlusundan veri sorumlusuna ya da veri sorumlusundan veri işleyene yapılacak olan aktarımlar için yapılan başvurularda tarafların hukuki statülerine ilişkin (veri sorumlusu-veri işleyen sıfatı bakımından) anlaşılır detayda açıklamalara yer vermeleri, bu kapsamda örneğin veri sorumlusu ile veri işleyen arasındaki ilişkiyi gösteren tevsik edici belgelerin (ör. gizlilik sözleşmesi, protokol vb.) Taahhütname ile gönderilmesi önem arz etmektedir. Aktarımın tarafları arasındaki ilişki doğru bir şekilde belirlenmesi, uygun olan Taahhütname örneğinin seçilmesi bakımından önem teşkil etmektedir (Kişisel Verileri Koruma Kurumu, 2020).

Bu noktada belirtmekte fayda görülmektedir ki, veri sorumlusu ve veri işleyen ilişkisinin belirlenmesinde Kurum internet sitesinde yayımlanan *"Veri sorumlusu ve veri işleyenin tespitinde göz önünde bulundurulması gereken hususlar ile aydınlatma yükümlülüğünün kim tarafından yerine getirileceği"ne ilişkin Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı Karar Özeti"*nden faydalanılması mümkündür. Mezkûr karar kapsamında veri sorumlusu ve veri işleyen kavramlarına ilişkin temel kriterlere yer verilmektedir. Söz konusu kriterler değerlendirilerek veri aktarımı yapılması planlanan tarafın veri sorumlusu mu veri işleyen mi olduğu başvuran veri sorumlusu tarafından değerlendirilmeli, ilgili başlıklar altında konuya ilişkin detaylı açıklamalara yer verilmelidir.

Taahhütnamede aktarım taraflarından birinin birden fazla olması durumunda da (Örneğin veri aktaran veri sorumlusu birden fazla olabilir veya verilerin aktarıldığı veri sorumlusu veya veri işleyen birden fazla olabilir) aynı Taahhütname metninin Kurula sunulması durumunda söz konusu Taahhütnamenin kabul edilip edilemeyeceği hususu tartışmalı olup, somut olay özelinde yapılacak değerlendirmeler Kurul'un takdirindedir. Konuya ilişkin değerlendirmenin takdiri Kurul'a ait olmakla birlikte, her iki senaryoya ilişkin olarak aşağıdaki değerlendirmelerin yapılabileceği düşünülmektedir:

◇ *Senaryo 1 - Verilerin aktarıldığı tarafın birden fazla olması durumu:* Veri sorumlusundan veri sorumlusuna veya veri sorumlusundan veri işleyene yapılacak aktarımlarda verilerin aktarılacağı karşı tarafın (yani veri sorumlusundan veri sorumlusuna aktarıma ilişkin taahhütname örneğinde *'veri alıcısı'*; veri sorumlusundan veri işleyene aktarıma ilişkin taahhütname örneğinde ise *'veri işleyen'*) birden fazla olması durumunda, taahhütnameye konu veri aktarım amaçları, aktarıma konu tüm veri kategorileri ve veri konusu kişi grupları ile aynı şekilde veri aktarımının hukuki sebeplerinin de tüm veri kategorileri ve veri konusu kişi grupları için ortak olduğu varsayımında tek bir taahhütname metni üzerinden Kuruma başvurulabileceği değerlendirilmektedir.

◇ *Senaryo 2 – Veri aktaran birden fazla veri sorumlusunun tek Taahhütname ile aktarım yapmayı istemesi:* Bu senaryonun 1 numaralı senaryoya nazaran daha tartışmalı olduğu düşünülmektedir. Aşağıdaki başlıklarda da açıklanacağı üzere, GVKT uyarınca herhangi bir izne tabi olmayan SCC metinleri ile veri aktaran tarafın birden fazla olabilmesi mümkündür. Keza müşterek veri sorumlusu müessesesi de GVKT uyarınca düzenlenmiştir. 6698 sayılı Kanunda müşterek veri sorumlusu kavramı düzenlenmemiş olmakla birlikte, Kurul kararlarına da konu olduğu üzere, somut olay özelinde müşterek veri sorumlusunun bulunduğu durumlar söz konusu olabilmektedir. Diğer taraftan, 6698 sayılı Kanuna göre GVKT'den farklı olarak yükümlülükler bakımından veri sorumluları muhatap alınmıştır. Bunun bir diğer anlamı da veri işleyenin kusurundan kaynaklı bir veri ihlalinin meydana gelmesi durumunda idari para cezasının verildiği takdirde cezanın muhatabı veri sorumlusu olacak, veri işleyen bakımından ise veri işleyene rücu edebilecektir.

Senaryo 1'deki aynı mantık bu senaryoda da düşünüldüğünde, yani birden fazla veri sorumlusunun aynı veri sorumlusu veya veri işleyene aktarım yapmayı istemesi halinde bu veri sorumlularının müşterek veri sorumlusu olması, tüm veri aktaran veri sorumlularının veri aktarım amaçları, aktarıma konu tüm veri kategorileri ve veri konusu kişi grupları ile aynı şekilde veri aktarımının hukuki sebeplerinin de tüm veri kategorileri ve veri konusu kişi grupları için ortak ol-

ması durumunda tek bir Taahhütname metninin imzalanmasının kabul edilebileceği değerlendirilebilecektir. Ancak bu noktada da örneğin veri aktaran veri sorumlularının müşterek değil ayrı ayrı veri sorumluları olduğu senaryosunda Taahhütnameden kaynaklı bir veri ihlali meydana geldiğinde veri ihlalinin kaynağının ve muhatabının dolayısıyla yaptırımın muhatabının tespitinin zor olacağı değerlendirilmektedir. Örneğin 20 ayrı veri sorumlusunun tek bir Taahhütname metni doldurduğunu, Kurul'dan izin aldığını ve veri aktarımını gerçekleştirdiğini varsayalım. Söz konusu Taahhütnamede bir veri ihlali meydana geldiğinde Kurul'un muhatap olarak alacağı veri sorumlusunu tespit edebilmesi için 20 veri sorumlusuna bilgi belge talebinde bulunması, söz konusu belgeleri değerlendirmesi gibi bir süreç izlenecek olup bu durum ilgili kişiler bakımından da inceleme süreci daha uzun süreceği için olumsuz olabilecektir. Söz konusu bilgi ve belgelerin incelenmesi neticesinde muhatabın tespit edilememesi durumunun da yaşanması olası olabilecektir.

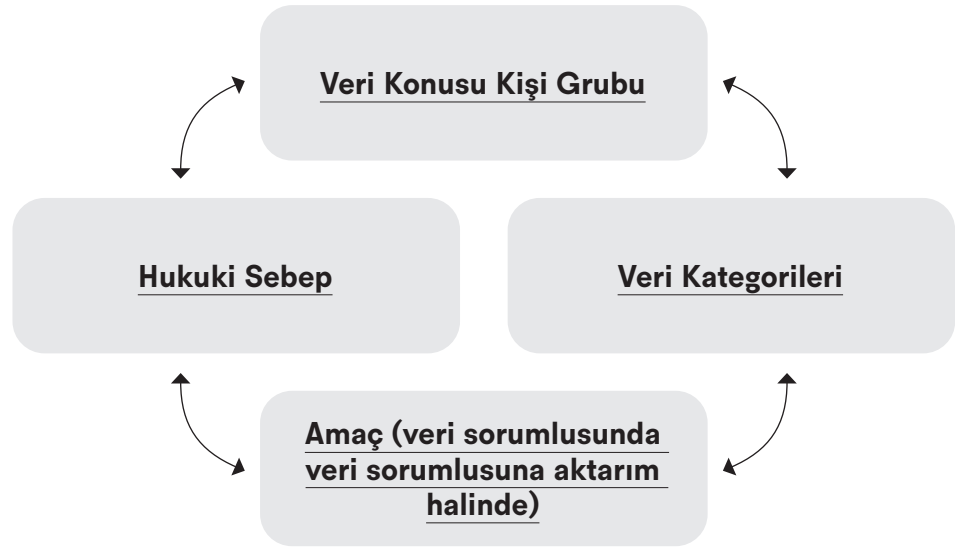
Benzer şekilde, birden fazla müşterek olmayan veri sorumlusunun veri aktaran olduğu Taahhütname başvurusuna Kurul tarafından izin verilmiş olması halinde, söz konusu Taahhütname kapsamında bir sorun çıktığında sorunun muhatabının bulunması bakımından tüm veri aktaran veri sorumlularına yazılması gerekecek, inceleme süreci uzun zaman alacak ve süreç karmaşıklaşabilecektir.

Tüm bu hususlar göz önünde bulundurulduğunda, takdiri Kurul'a ait olmakla birlikte, özellikle veri aktaran veri sorumlularının ayrı ayrı veri sorumluları olarak hareket ettiği varsayımında her bir veri sorumlusunun ayrı ayrı taahhütname metni hazırlaması yönteminin izlenerek Kuruma başvurması gerektiği değerlendirilmektedir. Bu şekilde inceleme sürecindeki muhatabın kolaylıkla belirlenebilmesi ile bahsi geçen olası sorunlar da bertaraf edilmiş olacağı ve sürecin daha hızlı ilerleyeceği değerlendirilmektedir.

- Öte yandan *"6698 sayılı Kanunda yer alan terminoloji birebir kullanılmalı, yapılacak tanımlar Kanunda ya da ikincil düzenlemelerde yer alan tanımlarla uyumlu olmalıdır."* (Kişisel Verileri Koruma Kurumu, 2020). Bu kapsamda örnek vermek gerekirse, *"veri kontrolörü"* yerine *"veri sorumlusu"*; *"veri sahibi/öznesi"* yerine *"ilgili kişi"* kavramlarının kullanılması gerekmektedir.

- Taahhütname Ek-1'de yer alan birbirleri ile ilişkili başlıklar arasında bağ kurulmalıdır. Bu çerçevede, *"hangi veri konusu kişi grubunun, hangi kişisel verilerinin, hangi amaca ve hukuki sebebe bağlı olarak aktarılacağı hususu, söz konusu başlıklar arasında bağ kurulmak suretiyle anlaşılır detayda açıklanmalıdır."* (Kişisel Verileri Koruma Kurumu, 2020). Diğer bir deyişle, *"Taahhütnameye konu kişisel veri aktarım faaliyetinin Kanunun 5 inci maddesinin ikinci fıkrası ile 6 ncı maddesinin üçüncü fıkrasında belirtilen kişisel veri işleme şartlarından hangisine dayalı olarak gerçekleştirildiği; aktarıma konu veri konusu kişi grubu, yurtdışına veri aktarımının amacı ve aktarıma konu kişisel veri kategorileri arasında bağ kurulmak suretiyle anlaşılır detayda açıklanması gerekmektedir."* (Kişisel Verileri Koruma Kurumu, 2020).

Bu çerçevede, Taahhütname kapsamında sağlık ve cinsel hayata ilişkin verilerin ve diğer özel nitelikli kişisel verilerin ilgili kişilerin açık rızası olmaksızın yurt dışına aktarımında; 6698 sayılı Kanunun 6. maddesinin üçüncü fıkrasında tahdidi olarak sayılmış olan işleme şartlarından birinin mevcut olması gerekmekte olup, aksi takdirde, açık rıza ile aktarım yapılabilir ki bu durumda söz konusu kişisel veri aktarımı Taahhütname kapsamı dışında kalacaktır. Söz konusu başlıklar arasında bağ kurulması bakımından tablo kullanılmasının başvurucu bakımından faydalı olabileceği değerlendirilmektedir.



Şekil 3. Taahhütnamede bağ kurulacak başlıklar

- Taahhütnamenin kapsamına ilişkin olarak, açık rıza şartına dayalı olarak gerçekleştirilecek yurt dışına kişisel veri aktarımları Taahhütnameye konu edilemeyecektir (Kişisel Verileri Koruma Kurumu, 2020). Yani, yurt dışına veri aktarımının ilgili kişiden açık rızanın alınması yoluyla gerçekleşmesi durumunda Kurul tarafından izin verilmesine gerek bulunmaksızın açık rızaya dayanarak yurt dışına kişisel veri aktarımları gerçekleşebilecektir.

- 6698 sayılı Kanunun temel ilkeleri diyebileceğimiz genel ilkelerini düzenleyen *"Genel ilkeler"* başlıklı 4. maddesinde, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceği ve kişisel verilerin işlenmesinde maddede; *"-Hukuka ve dürüstlük kurallarına uygun olma, -Doğru ve gerektiğinde güncel olma, -Belirli, açık ve meşru amaçlar için işlenme, -İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, -İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme"* şeklinde sayılan ilkelere uyulmasının zorunlu olduğu hüküm altına alınmış olup, anılan ilkelerin kişisel veri işleme faaliyetinin tüm süreçlerinde, her hal ve şartta uygulanması hukuki bir gerekliliktir (Kişisel Verileri Koruma Kurumu, 2020).

- Taahhütname Ek-1'de yer alan *"Veri konusu kişi grubu ve grupları"* başlığı altında, *"gibi, ve benzeri, olası, muhtemel,..."* gibi muğlak ifadelerin kullanımından kaçınılarak veri net bir şekilde ortaya konulmalıdır ("Kişisel Verileri Koruma Kurumu", 2020). Nitekim söz konusu muğlak ifadeler 6698 sayılı Kanunun 4 üncü maddesinin (ç) bendinde düzenlenen *"işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma"* ilkesine aykırılık teşkil etmiş olacaktır.

- Taahhütname Ek-1'de *"Veri kategorileri"* başlığı altında, veri kategorileri ile amaç arasında bağ kurulmalı, ayrıca veri kategorilerine ve verilerin işlenme amacına (*"amaç"* başlığı veri sorumlusundan veri sorumlusuna taahhütname örneğinde bulunmaktadır) ilişkin olarak Duyuru metninde (Kişisel Verileri Koruma Kurumu, 2020);

  "(...) özellikle Kanunun "Genel İlkeler" başlıklı 4 üncü maddesinin ikinci fıkrasının (ç) bendinde yer alan "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine riayet edilmelidir. Bu anlamda, ancak belirli, açık ve meşru bir veri aktarımı amacıyla bağlantılı, sınırlı ve ölçülü olacak şekilde veri kategorileri belirlenmelidir. Veri kategorileri ifade edilirken muğlak, anlaşılması zor ve geniş ifadelerden kaçınılmalı, kategoriler anlaşılır detayda ortaya konulmalıdır. Aktarılacak kişisel verilerin, "Veri konusu kişi grubu ve grupları" başlığı ile bağ kurulmak suretiyle, bu başlık altında sayılan kişi gruplarından hangisine ait olduğu açıkça belirtilmeli ve herhangi bir muğlak ifadeye yer verilmemelidir. (...)"

ifadelerine yer verilmiştir.

- Ayrıca Kuruma intikal eden bazı başvurularda veri kategorilerine ilişkin olarak sadece *"kişisel veri"* ya da *"özel nitelikli kişisel veri"* ifadesinin kullanıldığı

görülmekte olup, başvurunun açık, net ve daha anlaşılır olması bakımından örneğin kimlik veri kategorisi altında (*kimlik numarası, isim, soy isim*); iletişim veri kategorisi altında (*telefon numarası, e-posta adresi*); özel nitelikli kişisel veri kategorisi altında (*ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler*) gibi alt veri kategorilerine de detaylı bir biçimde yer verilmesi beklenmektedir.

- Veri Sorumlusundan Veri Sorumlusuna Taahhütname Ek-1'de *"Alıcı ve alıcı grupları"* başlığı ile, *"veri alıcısı tarafından örneğin verilerin ifşası veya aktarılması suretiyle gerçekleştirilecek sonraki devam eden aktarımlarda veri alıcısının bulunduğu ülkede mukim olan veri sorumlusu veya veri işleyen"* ifade edilmektedir (Kişisel Verileri Koruma Kurumu, 2020). Bu başlık altında sonraki aktarımlar bakımından taraf veri sorumlularının kişisel verinin aktarıldığı veri alıcısının mevzuatta öngörülen hukuki yükümlülükleri gereğince veri aktarmasını gerektiren yetkili kurum ve kuruluşlar kapsamında olması gerekmekte olup, alıcının mukim olduğu ülkede yerleşik farklı bir veri sorumlusuna ya da veri alıcısının mukim olduğu ülkeden başka bir ülkede yerleşik veri sorumlusu veya veri işleyene, Taahhütname kapsamında sonraki devam eden veri aktarımı gerçekleşemeyecektir (Kişisel Verileri Koruma Kurumu, 2020). Duyuruda da ifade edildiği üzere, *"Böyle bir durumda, aktarımın amacı ve niteliğine uygun düştüğü ölçüde, farklılıklar varsa bu farklılıklar da her bir veri sorumlusu ya da veri işleyen bakımından açık ve net bir şekilde ortaya konulmak suretiyle tek bir taahhütname metninin veri aktarılan veri alıcısı ile söz konusu veri sorumluları ya da veri işleyenler tarafından birlikte imzalanması da mümkündür."*

"Aktarımın gerçekleşeceği ülkede yetkili kamu kurum ve kuruluşları ile mahkemeler" alıcı grupları arasında değerlendirilmekte olup, yine "yetkili kamu kurum ve kuruluşlarının rekabet, telekomünikasyon otoritesi gibi belirlenebilir olması halinde bunların açıkça ortaya konulması gerekmektedir" (Kişisel Verileri Koruma Kurumu, 2020).

- Taahhütname Ek-1'de *"Veri alıcısı tarafından alınacak teknik ve idari tedbirler" başlığı altında, "kişisel verilerin işlenmesi sürecinde veri sorumlularının alması gereken teknik ve idari tedbirler konusunda uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması amacıyla hazırlanan ve Kurum resmi internet sitesinde yayımlanan "Kişisel Veri Güvenliği Rehberi (Teknik Ve İdari Tedbirler)"nin dikkate alınması, taahhüt edilen teknik ve idari tedbirlerin ayrı*

başlıklar halinde açıklanarak, bu tedbirlere ilişkin tevsik edici belgelerin de başvuruya eklenmesi" gerekmektedir (Kişisel Verileri Koruma Kurumu, 2020).

- Taahhütname Ek-1'de *"Özel Nitelikli Kişisel veriler için alınan ek önlemler" başlığı altında "Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" başlıklı kararı ile belirlenen ve özel nitelikli kişisel verilerin işlenmesi sırasında alınması zorunlu olan teknik ve idari tedbirlere yer verilmesi ve söz konusu tedbirleri tevsik edici belgelerin de başvuruya eklenmesi"* gerekmektedir (Kişisel Verileri Koruma Kurumu, 2020).

- Taahhütname Ek-1'de VERBİS başlığına ilişkin olarak başvuran veri sorumlusunun *"kayıt yükümlülüğünün bulunup bulunmadığı bilgisinin gerekçesi ile birlikte açıklanması ve kayıt yükümlülüğünün bulunması halinde VERBİS bilgilerine bu başlık altında yer verilmesi"* gerekmektedir (Kişisel Verileri Koruma Kurumu, 2020). Kuruma iletilen bazı Taahhütname başvurularında Taahhütnamenin içeriğinde açıklanan hususlar ile VERBİS kaydında açıklanan hususların çeliştiği görülmektedir. Bu doğrultuda, Taahhütname metninin içeriği ile VERBİS bilgilerinin birbiriyle uyumlu olması, VERBİS kaydında yer verilen açıklamalar ile çelişen hususların Taahhütname metninde yer almaması gerekmektedir.

- Taahhütname Ek-1'de *"Ek faydalı bilgiler"* başlığı altında saklama süreleri ve ilgili diğer bilgiler yer almalı, *"kişisel verilerin işlenme süresinin en azından azami süreyi gösterecek şekilde gerekçesine de yer verilmek suretiyle belirtilmesi"* gerekmektedir (Kişisel Verileri Koruma Kurumu, 2020). Ayrıca, sürelerin belirlenmesinde Kanunun 4 üncü maddesinin ikinci fikrasının (d) bendinde yer alan, *"İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme." ilkesinin gözetilmesi, mevzuattan kaynaklı bir sürenin mevcut olması durumunda, sürenin hangi mevzuat hükmüne dayandırıldığının belirtilmesi gerekmektedir."* (Kişisel Verileri Koruma Kurumu, 2020). Ayrıca Taahhütname ekinde yer alan başlıklar dışında ayrıca ifade edilmesi istenen hususlar da bu başlık altında yer almalıdır.

- İrtibat kişisine ait bilgiler Taahhütname Ek-1'de *"İrtibat kişisi iletişim bilgileri"* başlığı altında bulunmalıdır (Kişisel Verileri Koruma Kurumu, 2020).

- *"Veri Sorumlusundan Veri İşleyene Aktarım"* başlıklı Taahhütname örneği Ek-1'deki *"Veri Sorumlusu"* ve *"Veri İşleyen"* başlıklarına yönelik yapılacak açıklamalarda *"veri sorumlusu ve veri işleyenin faaliyet alanlarının açıklanması ile veri sorumlusunun veri aktarımına, veri işleyenin ise aktarım sonrasında gerçekleştireceği işleme faaliyetlerine ilişkin açıklamaların anlaşılır detayda ortaya konulması"* gerekmektedir (Kişisel Verileri Koruma Kurumu, 2020). Ayrıca mezkûr Taahhütname örneğinin Ek-1'inde yer alan *"İşleme faaliyetleri"* başlığında ise *"aktarılan kişisel verilerin aktarım amacıyla bağlantılı olacak şekilde ne tür bir işleme faaliyetine tabi tutulacağı hususu somut aktarım özelinde anlaşılır detayda ve netlikte ortaya konulmalıdır."* (Kişisel Verileri Koruma Kurumu, 2020). Örneğin veri aktarımından sonra, 6698 sayılı Kanunun 3 üncü maddesinin birinci fikrasının (e) bendi kapsamında veri alıcısı konumunda bulunan veri işleyenin söz konusu kişisel verileri *"elde etmesi, kaydetmesi, depolaması, muhafaza etmesi, değiştirmesi, yeniden düzenlemesi, açıklaması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen"* hangi işleme faaliyetinde bulunduğu açıkça yazılmalıdır.

- Ayrıca, veri sorumluları TEB Arval Araç Filo Kiralama A.Ş., Amazon Turkey Perakende Hizmetleri Ltd. Şti., Amazon Turkey Yönetim Destek Hizmetleri Ltd. Şti., Turksport Spor Ürünleri San. Tic. Ltd. Şti., Türkiye Futbol Federasyonu, Otokoç Otomotiv Ticaret ve Sanayi Anonim Şirketi ve Google Reklamcılık ve Pazarlama Limited Şirketi tarafından Kuruma iletilmiş olan Taahhütname başvurularına Kurul tarafından izin verilmiştir. Diğer bir deyişle, Eylül 2023 tarihine kadar toplam yedi adet Taahhütname başvurusuna Kurul tarafından izin verilmiştir.

AVRUPA BİRLİĞİ HUKUKUNDA GVKT KAPSAMINDA KİŞİSEL VERİLERİN ÜÇÜNCÜ ÜLKELERE VEYA ULUSLARARASI KURULUŞLARA AKTARILMASI

Birlik Hukukunda yurt dışına veri aktarımı müessesine ilişkin olarak Türk Hukuku ile arasındaki farkların ortaya konulabilmesini teminen konuya ilişkin olarak bu başlık altında daha detaylı açıklamalara yer verilecektir. Bu çerçevede Birlik Hukukunda yurt dışına veri aktarımının tarihçesi, düzenlemenin gerekçeleri, genel ilkeler, uygun tedbirlere tabi aktarımlar ve SCC metinleri başlıkları altında konu irdelenecektir.

Tarihçe ve Düzenlemenin Gerekçeleri

Sınır ötesi veri aktarımı, esas olarak kırk yılı aşkın bir süredir önem teşkil eden meselelerden biridir (Wagner, 2018). 1973 yılında ise İsveç, yetkili İsveç makamının izni ile üçüncü ülkelere aktarılabileceğini düzenleyen ilk ülke olmuştur (Wagner, 2018). Yine 1978 yılında Avusturya kendi ülkesindeki tedbirlere eşit tedbirler

sağlayabilecek ülkelere veri aktarımının yapılabileceğini düzenleyerek İsveç'i takip etmiştir (Wagner, 2018). 1980 yılında ise OECD, ülkelerin farklı veri koruma seviyelerinin olması sebebiyle, bu seviyeler arasındaki farklılıkları en aza indirgemek ve veri korumada asgari standartları belirleyebilmek için sınır ötesi veri aktarımına ilişkin ilk uluslararası düzenlemeleri kabul etmiştir (Wagner, 2018).

Birlik ise önemli bir ekonomik ve siyasi birlik niteliğini haiz olup, uyguladığı hukuk sistemi geniş alanda etkili olmaktadır (Turan, 2021). Kişisel verilerin korunmasında birçok düzenleme ile kurumsal çalışmalar, 1990'lı yıllarda başlamış olup, özellikle 2000'li yıllarda önemli derecede artış göstermiştir (Turan, 2021). Birlik hukukunda, Avrupa dışına kişisel verilerin serbest akışı yirmi yılı aşkın süredir sınırlandırılmıştır (Ustaran, 2018a). Veri sorumluları uygun tedbirleri sağlamayan üçüncü ülkelere herhangi bir kısıtlama olmaksızın veri aktarırsa, bu takdirde Birlik hukukunun getirdiği korumanın bir anlamı kalmayacağı için söz konusu veri aktarımları Birlik hukuku uyarınca birtakım sınırlamalara tabi tutulmuştur (Ustaran, 2018a). Söz konusu sınırlandırmalar için küresel ticaretin önünde bir engel olduğu endişesiyle uluslararası kuruluşlar başta olmak üzere birçok kuruluş tarafından eleştiriler hâsıl olmuştur (Ustaran, 2018a). Birlik üyelerinin iç hukukları uyarınca düzenlenen kişisel verileri koruma standartları arasındaki farklılıkların Birlik iç pazarında kişisel veri aktarılmasında sıkıntı teşkil etmesi sebebiyle Komisyon, 1990 yılında mezkûr standartların yeknesak hâle getirilmesinin bu konuda bir direktif hazırlanmasını teklif etmiştir (Ustaran, 2018a). Bu çerçevede, 24 Aralık 1995'te *"Kişisel verilerin işlenmesi ve serbest dolaşımına ilişkin olarak kişilerin korunmasına ilişkin 95/46/EC sayılı Direktif"* kabul edilmiştir.

Mezkûr direktif, bireylerin kişisel verilerinin işlenmesi faaliyetlerine karşı korunmasının ve bu verilerin Birlik içerisindeki akışının düzenlenmesini kapsamaktadır (Kaya ve Tolun, 2022). Kişisel verilerin Birlik Üye Devletleri ile İzlanda, Lihtenştayn ve Norveç'i kapsayan Avrupa Ekonomik Alanından (AEA) sınır ötesine kişisel veri aktarımları bakımından aktarılması hususu, mülga 95/46/EC sayılı Direktif'in IV numaralı Bölümünde düzenlenmiştir. Mülga direktife göre, Birlik dışına kişisel verilerin aktarımı ancak aktarımın yapılacağı üçüncü ülkenin uygun tedbirleri sağlaması ile mümkün kılınmıştır. Diğer bir deyişle, gerek ulusal düzenlemeler gerek uluslararası düzenlemeler ve taahhütler göz önünde bulundurulduğunda, yeterli korumanın sağlanacağına kural olarak Komisyon tarafından karar verilmiş olma şartı aranmaktadır (Akçalı Gür, 2019). Ancak Avrupa Komisyonu'nun (Komisyon) yeterlilik kararının yaygınlaşmasının zorluğu, kişisel tercihler ve ekonomik hayatın gerekleri gerekçeleriyle söz konusu kurala birtakım istisnalar da getirilmiş olup, söz konusu istisnalar ise mezkûr direktifin 26. maddesinde (Akçalı Gür, 2019);

- Söz konusu aktarıma İlgili kişinin açık bir şekilde rıza vermiş olması,
- Aktarımın ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebine istinaden alınan sözleşme öncesi tedbirlerin uygulanması için gerekli olması,
- Aktarımın veri sorumlusu ile üçüncü bir taraf arasında akdedilen ilgili kişi lehine bir sözleşmenin kurulabilmesi veya ifası için aktarım gerekli olması,
- Kamu yararına ilişkin önemli veya yasal sebepler bakımından aktarımın gerekli olması veya yasal taleplerin tesisi, kullanılması veya korunması için aktarımın gerekli olması,
- İlgili kişinin önemli menfaatlerinin korunması için aktarımın gerekli olması,
- Birlik veya Üye Devlet hukukuna göre kamuya bilgi sağlamayı amaçlayan ve genel olarak kamunun veya meşru menfaati olduğunu ispatlayabilen ilgili kişilerin incelemesine açık olan sicilden ancak Birlik veya Üye Devlet hukukun incelemeye ilişkin şartlarının yerine getirebildiği ölçüde aktarımın yapılması,

şeklinde sayılmıştır. Bu noktada belirtmekte fayda görülmektedir ki, 95/46/EC sayılı Direktif kapsamında düzenlenen istisnalar GVKT ile büyük ölçüde benzerlik göstermektedir.

Bununla birlikte, kişisel verilerin korunması hukukundaki en etkili düzenlemelerden biri olarak kabul edilen 95/46/EC sayılı Direktif'ten sonra kişisel verilerin korunması hakkına verilen önem daha da artmış ve söz konusu hak, temel bir insan hakkı olarak Avrupa Birliği Temel Haklar Bildirgesi'nin 8. maddesinde ve Avrupa Birliği'nin İşleyişi Hakkında Anlaşma'nın 16. maddesinde hüküm altına alınmıştır (Develioğlu, 2017).

Avrupa Birliği Temel Haklar Bildirgesi *"Kişisel verilerin korunması"* başlıklı 8. Maddesi (Avrupa Komisyonu, t.y.);

> *"(1) Herkes kendisiyle ilgili kişisel verilerin korunması hakkına sahiptir.*
>
> *(2) Bu tür veriler, belirtilen amaçlarla ve ilgili kişinin rızasına veya yasalarda öngörülen başka bir hukuki sebebe dayanılarak adil bir şekilde işlenmelidir. Herkes, kendisi hakkında toplanmış verilere erişme ve bunların düzeltilmesini*

isteme hakkına sahiptir.

(3) Bu hükümlere riayet edilmesi, bağımsız bir otoritenin denetimine tâbiidir."

hükmünü amirdir. Diğer taraftan, Avrupa Birliği'nin İşleyişi Hakkında Antlaşma'nın 16. maddesi ise aşağıdaki şekilde düzenlenmiştir ("Avrupa Birliği Başkanlığı", t.y.);

"(1) Herkes kendisiyle ilgili kişisel verilerinin korunması hakkına sahiptir.

(2) Avrupa Parlamentosu ve Konsey, Birlik hukuku kapsamına giren faaliyetlerin yürütülmesinde, Birlik kurum, organ, ofis veya ajansları ile üye devletler tarafından kişisel verilerin işlenmesi sırasında bireylerin korunmasına ve bu bilgilerin serbest dolaşımına ilişkin kuralları olağan yasama usulü uyarınca belirler. Bu kurallara uyulması, bağımsız otoritelerin denetimine tabidir.

Bu maddeye dayanarak kabul edilen kurallar, Avrupa Birliği Antlaşması'nın 39. maddesinde yer alan spesifik kurallara halel getirmez."

Görüldüğü üzere, kişisel verilerin işlenmesi hukuku, uluslararası hukukta giderek etkisini artırarak temel meselelerden biri hâline gelmiştir. Teknolojinin hızlı gelişimi ve kişisel verilerin küreselleşmede merkez unsurlardan biri hâline gelmesi ile birlikte 95/46/EC sayılı Direktif, Birlik ihtiyaçlarını karşılayamaz duruma gelmiştir (Akçalı Gür, 2019).

Bununla birlikte, kişisel verilerin korunmasına yönelik standartların yeknesak olarak düzenlenmesine ve küreselleşme koşullarına daha uyumlu bir düzenlemeye duyulan ihtiyaç neticesinde, 2016/679 sayılı Genel Veri Koruma Tüzüğü hazırlanmıştır. GVKT 4 Mayıs 2016 tarihinde Avrupa Birliği Resmi gazetesinde yayımlanmış olup, 25 Mayıs 2018 tarihinden itibaren yürürlüğe girmiştir.

Bu noktada belirtmekte fayda görülmektedir ki, GVKT'nin direktif yerine tüzük niteliğinde olması büyük önem taşımaktadır; çünkü Birlik hukukuna göre direktif hükümlerinin uygulanması Üye devletlerin iç hukukuna aktarılmasıyla mümkün iken, Tüzükte ise durum tam tersidir (Develioğlu, 2017). Diğer bir deyişle, 95/46/EC sayılı Direktif her bir Üye Devlet tarafından yasal düzenleme ile iç hukuklarına aktarılmış olduğundan Birlik hukukunda kişisel verilerin korunması bakımından her ne kadar temelde aynı prensiplere dayansalar da yirmi sekiz (Brexit'e kadar) tane farklı yasal düzenleme kabul edilmiştir ve söz konusu düzenlemeler arasında önemli farklılıklar da bulunmaktadır (Develioğlu, 2017). Söz konusu farklılıklar ise hem Birlik içerisindeki hem de üçüncü ülkelere veri akışını uzun ve karışık

hâle getirmekte olup, Birlik'te standartlar yeknesak şekilde belirlenemediğinden ilgili kişilerce veri işleme sürecine erişilmesi ve öngörülmesi de zorlaşmıştır (Toparlak, 2021). Birlik hukukunda kişisel verilerin korunmasının yeknesak standartlara haiz olması başta dijital ortak Pazar stratejisi olmak üzere önem teşkil etmekte olup, söz konusu düzenlemenin her bir Üye Devlette doğrudan uygulanabilir olan bir tüzük ile düzenlenmesi büyük gelişmelerden biri olarak değerlendirilmektedir (Develioğlu, 2017). Diğer bir deyişle, kişisel verilerin korunması hukuku bakımından tüm Üye Devletlere aynı kuralların uygulanması ile hem Avrupa iç pazarındaki rekabeti güçlendirmek hem de Birlik içerisindeki gerçek kişilerin Birlik içinde ve verilerin aktarıldığı üçüncü ülkelerde Avrupa Birliği Temel Haklar Bildirgesi'nde düzenlenen kişisel verilere ilişkin kişilik haklarının korunması amaçlarının gerçekleştirilmesinin hedeflendiği ifade edilebilecektir (Toparlak, 2021).

Bununla birlikte, GVKT uyarınca 95/46/EC sayılı Direktif'te üçüncü ülkelere ve uluslararası kuruluşlara yapılacak aktarımlar bakımından hâkim olan yaklaşım aynı şekilde sürdürülmüştür. Bu çerçevede, Birliğe üye ülkeler ile birlikte İzlanda, Lihtenştayn ve Norveç'ten oluşan AEA dışındaki herhangi bir ülkeye yapılacak kişisel veri aktarımları bakımından GVKT'nin V. Bölümünde yer alan düzenlemelere riayet edilmesi gerektiği hüküm altına alınmıştır (Ustaran, 2018a).

GVKT'nin (101) numaralı Resital hükmünde veri aktarımına ilişkin sınırlandırmaların neden getirildiğine ilişkin açıklamalara yer verilmiştir. Mezkûr Resitalde, Birlik dışındaki ülkelere ve uluslararası kuruluşlara veri akışının uluslararası ticaret ve iş birliği bakımından gerekli olduğu; ancak söz konusu veri akışının artmasıyla birlikte kişisel verilerin korunmasına yönelik sıkıntıların ve endişelerin de arttığı ifade edilmiştir (Avrupa Komisyonu, 2016). Ayrıca belirtmek gerekir ki, sonraki yapılan aktarımlar da dâhil olmak üzere, üçüncü ülkeler veya uluslararası kuruluşlar bünyesindeki veri sorumlularına, veri işleyenlere ve alıcılara Birlik'ten yapılan veri aktarımında, Birlik vatandaşlarının kişisel verilerinin korunmasına ilişkin düzenlemelere halel getirilmemesi hususu, (101) numaralı Resital hükmünde de ayrıca vurgulanmıştır (Avrupa Komisyonu, 2016). Diğer bir deyişle, Birlik dışına veri aktarımının yapılabilmesi ancak GVKT hükümlerine uyulması şartıyla mümkün olabilecektir. Bu doğrultuda, Birlik'in veri aktarım hükümleri konum eksenli yaklaşımı benimsemektedir (Avrupa Komisyonu, 2016).

Aktarımın Genel İlkeleri

GVKT'nin temel amaçlarından biri de kişisel verilerin korunmasına ilişkin kabul edilen ilkeler üzerinden kişisel verilerin Üye Devletler arasında serbest veri

akışının gerçekleşmesidir (Ustaran, 2018b). Bununla birlikte, verilerin üçüncü ülkelere aktarımı bakımından özel koşullar kabul edilmektedir (Ustaran, 2018b). Birliğe üye ülkeler ile birlikte İzlanda, Lihtenştayn ve Norveç'ten oluşan AEA dışındaki ülkelere veya uluslararası kuruluşlara veri aktarımının yapılması hususu, GVKT'nin V (Beş) numaralı Bölümünde, 44. ve 50. maddeler arasında hüküm altına alınmıştır. Bu çerçevede, aşağıdaki durumlardan birinin olması durumunda veri aktarımının gerçekleşebilmesi mümkündür;

- Komisyon tarafından verilmiş yeterlilik kararına dayanılarak aktarımın gerçekleşmesi,

- Yeterlilik kararı yoksa veri aktarmak isteyen veri sorumlusu veya veri işleyenin ilgili kişi haklarının da etkin bir şekilde icrasını sağlayan uygun tedbirleri sağlayarak aktarımın gerçekleşmesi,

- Yeterlilik kararının veya uygun tedbirlerin bulunmaması durumunda ise GVKT m. 49'da düzenlenen özel istisnalardan birine dayanılarak aktarımın gerçekleşmesi.

GVKT'nin 44. maddesi (Develioğlu, 2017);

> *"İşlenmekte olan veya bir üçüncü ülkeye veya uluslararası kuruluşa aktarıldıktan sonra işlenmesi planlanan kişisel verilerin aktarımı, üçüncü ülke veya uluslararası kuruluştan diğer bir üçüncü ülkeye veya uluslararası kuruluşa yapılacak sonraki aktarımlar dâhil olmak üzere, ancak, bu Tüzük'ün diğer hükümlerine tabi olmak kaydıyla, bu Bölüm'de yer alan şartlara veri sorumlusu veya veri işleyen tarafından uyulması kaydıyla gerçekleştirilebilir. Bu Tüzük ile gerçek kişilere sağlanan koruma seviyesinin zarar görmemesi için bu Bölüm'de yer alan düzenlemeler uygulanacaktır."*

hükmünü amirdir. Görüldüğü üzere, sonraki aktarımlar da dâhil olmak üzere, üçüncü ülkelere veya uluslararası kuruluşlara veri sorumlusu veya veri işleyen tarafından yapılacak veri aktarımlarında, GVKT V. Bölüm hükümlerine riayet edilmesi gerekmektedir. Kişisel verilerin üçüncü ülkelere aktarılması Birlik'teki ilgili kişilerin hakları bakımından risk teşkil etmekte olduğundan söz konusu riskin azaltılması adına GVKT m. 44 düzenlenmiştir (Toparlak, 2021).

Bununla birlikte, GVKT kapsamında aktarımın nasıl olması gerektiği tanımlanmamıştır. Bu noktada belirtmek gerekir ki, aktarım ifadesinden transfer edilmesi anlaşılmamalıdır; zira aktarımı tamamlayan üçüncü ülkenin veriyi işlemesi faaliyetidir (Ustaran, 2018b). Bu nedenle üçüncü ülke, ülkesine aktarılan kişisel veri üzerinde birtakım esaslı işleme faaliyetleri gerçekleştirmediği müddetçe, safi o verinin EEA dışında üçüncü ülkeye aktarılması hususu GVKT kapsamında kısıtlamalara tabi olacağı anlamına gelmeyecektir (Ustaran, 2018b). Ayrıca her ne kadar ilgili hükümde V. Bölüme vurgu yapılmış olsa da, GVKT'nin maddi kapsamı başlıklı ikinci ve bölgesel kapsam başlıklı üçüncü maddelerinde yer verilen hükümlerin de dikkate alınması gerekmektedir (Turan, 2021). Bu çerçevede, GVKT'nin bölgesel kapsam maddesi göz önünde bulundurularak işlenen kişisel verilerin veri sorumlusu ya da veri işleyenin etkinlikleri kapsamında Birlik içerisinde ikamet etmesi ya da yerleşik olması kaydıyla, verilerin işlenmesinin Birlik içerisinde ya da dışında olmasının da bir önemi bulunmamaktadır (Turan, 2021).

Bu kapsamda, örneğin, GVKT'nin 44. maddesine göre, Fransa'da mukim bir şirketin işçilerinin verilerinin Türkiye'deki şubesine aktarılması durumunda Türkiye üçüncü ülke olacak ve GVKT V. Bölüm'de hüküm altına alınan aktarım koşullarından birine riayet edilerek aktarım hukuka uygun bir şekilde gerçekleşebilecektir. Aktarımın yapıldığı üçüncü ülkelerin de GVKT'ye uyumlu olmaları gerekmekte olup, bu durum küresel olarak ekonomik, ticari, finansal, turizm, vb. gibi alanlarda önemli etkiler doğurmaktadır (Turan, 2021).

Bununla birlikte, Birlik'in Üye Devlet vatandaşının başka bir ülkede sunucusu bulunan bir internet sitesine kişisel veri yüklemesine ilişkin ABAD'ın Kasım 2003 tarihli Bodil Lindqvist (C-101/01) İsveç davasında, internet kullanan herhangi bir bireyin söz konusu verilere erişimi üçüncü ülkeye kişisel veri aktarımı olarak değerlendirilmemektedir (Ustaran, 2018b). Ancak, kişisel verilerin elde edildikten sonra otomatik olarak işlenmesi amacıyla bireyler hakkında uluslararası bir bilgi alışverişi söz konusu olduğunda, her ne kadar orijinal bilgi alışverişi safi kişisel veri üzerine kurulmamış olsa da, söz konusu aktarım GVKT amaçları kapsamında bir aktarım olarak değerlendirilecektir (Ustaran, 2018b). Bunun bir örneği olarak ise, Birlik'teki bir birey tarafından üçüncü ülkedeki birine telefonla bilgilerin sağlandığı ve daha sonra bu bilgilerin üçüncü ülkedeki birey tarafından bilgisayara girilmesi gösterilebilir (Ustaran, 2018b).

Bununla birlikte, GVKT'nin 44. maddesinin (9) numaralı fikrasında 95/46/EC sayılı Direktif döneminde verilen uygunluk kararlarının GVKT'nin yürürlüğe girmesinden sonra geçerliliğini koruyacağı hususunu tedbir altına alınmış olup, Komisyon vermiş olduğu uygunluk kararlarını dört yılda bir gözden geçirmektedir (Wagner, 2018).

Yukarıda da ifade edildiği üzere, GVKT m. 44'e göre kişisel verilerin üçüncü ül-

kelere veya uluslararası kuruluşlara aktarılabilmesi için GVKT Bölüm V altında düzenlenen hükümlerin yanı sıra GVKT'de düzenlenen başka hükümlere de riayet edilmesi gerekmektedir. Bu çerçevede, her bir aktarım GVKT m. 5'te düzenlenen temel ilkeler, m. 6'da düzenlenen veri işleme şartları ve m. 9'da düzenlenen özel nitelikli kişisel verilerin işlenmesi şartları ile uyumlu olması gerekmektedir (Avrupa Komisyonu, 2022a). Bu minvalde, verilerin aktarılması bakımından iki aşamalı bir test uygulanmalıdır. İlk aşamada GVKT genel hükümlerine uyulması, ikinci aşamada ise sınır ötesi veri aktarımını düzenleyen GVKT Bölüm V altında yer verilen hükümlere uyulması gözetilmelidir (Avrupa Komisyonu, 2022a).

Ayrıca belirtmekte fayda görülmektedir ki, Birlik üyesi devletlerde aktarım bir çeşit veri işleme olarak kabul edilmekte olup, aktarımın yasal bir temelinin bulunması gereklidir (Küzeci, 2020). Söz konusu gereklilik, Üye Devletler arasında gerçekleşecek aktarımda da mevcut olacaktır (Küzeci, 2020). Bu çerçevede, GVKT'de kişisel verilerin Birlik hukukuna uygun olarak aktarılabilmesi için kişisel veri işleme ilkeleri, kişisel veri işleme şartları, çocukların kişisel verilerinin işlenmesi şartları, özel nitelikli kişisel veriler ile özel nitelikli kişisel verileri işleme şartları gibi hususları düzenleyen Bölüm II ile ilgili kişi haklarını detaylarıyla düzenleyen Bölüm III kapsamında yer alan hükümlere de uyulmasının son derece önem teşkil ettiği de değerlendirilmektedir.

Uygun Tedbirlere Tabi Gerçekleşen Aktarımlar

Günümüzde hakkında yeterlilik kararı verilen ülke sayısının oldukça az olduğu düşünüldüğünde, veri sorumluları veya veri işleyenler sınır ötesi aktarımı gerçekleştirebilmek açısından verinin korunmasını teminen uygun tedbirleri sağlamayı istemektedir (Ustaran, 2018a).

GVKT'nin 46. maddesine göre, Komisyon'un GVKT m. 45 çerçevesinde bir yeterlilik kararının bulunmaması durumunda, veri sorumlusu veya veri işleyenin kişisel verileri bir üçüncü ülkeye veya uluslararası kuruluşa aktarabilmesi için mezkûr maddede sayılan uygun tedbirlerden birinin sağlanması gerekmektedir. Anılan önlemler temelde Birlik içerisindeki hak ve yükümlülüklerin aktarımın yapılacağı ülkede de korunacağını taahhüt etmekte olup, aktarımın Birlik ülkelerindeki Yetkili Makamlar tarafından izlenmesini ve denetlenmesini de aynı zamanda sağlamaktadır (Toparlak, 2021). GVKT (108) numaralı Resital hükmünde de ifade edildiği üzere, anılan tedbirler bağlayıcı şirket kurallarını, Komisyon tarafından belirlenen veya Yetkili Makam tarafından belirlenip Komisyon tarafından kabul edilen standart sözleşme hükümlerini, onaylanmış davranış kurallarını veya sertifikasyonu içerebilmektedir (Avrupa Komisyonu, 2016).

GVKT m. 46'da uygun tedbirler bakımından ikili bir ayrıma gidilmiştir. Bunlardan ilki (2) numaralı fıkrada sayılmış olup, mezkûr tedbirlere aşağıda yer verilmektedir (Avrupa Komisyonu, 2016):

Kamu makamları veya kuruluşları arasında hukuken bağlayıcılığı bulunan ve icra edilebilir bir belgenin bulunması,

GVKT m. 47'de düzenlenen bağlayıcı şirket kurallarının bulunması,

- Komisyon tarafından kabul edilen standart veri koruma hükümlerinin bulunması,
- Yetkili Makam tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma hükümlerinin bulunması,
- Veri sorumlusu veya veri işleyenin uygun tedbirleri uygulayabilmesini teminen ilgili kişi haklarını da içeren bağlayıcı ve icra edilebilir taahhütleri de kapsayan m. 40'ta düzenlenen onaylanmış davranış kurallarının bulunması,
- Veri sorumlusu veya veri işleyenin uygun tedbirleri uygulayabilmesini teminen ilgili kişi haklarını da içeren bağlayıcı ve icra edilebilir taahhütleri de kapsayan m. 42'de hüküm düzenlenen sertifikasyon mekanizmasının bulunması.

Diğer aktarım koşulları ise Yetkili Makam tarafından izin verilmesi gereken uygun tedbirler olup, söz konusu koşullar mezkûr maddenin (3) numaralı fıkrasında sayılmıştır. Bu kapsamda, Yetkili Makam tarafından izin verilmiş olması kaydıyla, aşağıdaki uygun tedbirlerden biri sağlanarak aktarım gerçekleşebilecektir (Avrupa Komisyonu, 2016):

- Veri sorumlusu veya veri işleyen ile üçüncü ülkedeki veya uluslararası kuruluştaki veri sorumlusu, veri işleyen, veri alıcısı veya arasındaki sözleşme hükümleri,
- Kamu makamları veya kuruluşları arasında yapılacak idari anlaşmalara icra edilebilir ve etkili ilgili kişi hakları içeren hükümler de dahil olmak üzere hükümler eklenmesi.

Yukarıda sayılan aktarım koşulları göz önünde bulundurulduğunda, söz konusu koşullar 95/46/EC sayılı Direktif'e kıyasen veri sorumluları ve veri işleyenler için

daha fazla seçenek ve esneklik sunmaktadır (Ustaran, 2018a).

Standart Veri Koruma Hükümleri
(Standart Sözleşme Hükümleri/SCC Metinleri)

Standart veri koruma hükümleri, GVKT m. 46(2) çerçevesinde hüküm altına alınan uygun tedbirlere tabi sınır ötesi veri aktarımı mekanizmalarından biridir. Bununla birlikte, günümüzde uygun koruma tedbirlerine tabi ve hukuka uygun olarak sınır ötesi veri aktarımlarının gerçekleştirilmesinde en sık başvurulan yöntem de "model hükümler" olarak da adlandırılan *"standart veri koruma hükümleri"*dir (Ustaran, 2018a). Bu yönteme ilişkin olarak Komisyon tarafından kabul edilen veyahut üçüncü kişilerce yapılıp Komisyon tarafından onaylanan sözleşmeler kullanılabilmektedir (Toparlak, 2021). Söz konusu sözleşme hükümleri, aktarımın yapıldığı üçüncü ülkede de GVKT korumasının temin edilmesini sağlamaktadır (Toparlak, 2021).

SCC'ler, veri sorumlularının ve veri işleyenlerin AB hukuku kapsamındaki yükümlülüklerine uymalarını sağlayan, önceden onaylanmış ve standardize edilmiş model veri koruma hükümleridir (Avrupa Komisyonu, 2022b). Söz konusu hükümler, veri sorumluları ile veri işleyenlerin ticari ortaklar gibi diğer taraflarla sözleşmesel yükümlülüklerinin bir parçası olabilmektedir (Avrupa Komisyonu, 2022b). Bu noktada ayrıca belirtmek gerekir ki, SCC'lerin kullanılması zorunlu olmayıp kişisel verilerin korunmasına ilişkin bir uyum mekanizması olarak uyulması gereken sözleşmesel yükümlülükler kapsamında gönüllülük esaslı kullanılacaktır (Avrupa Komisyonu, 2022b).

Komisyon, aşağıda belirtilen SCC'leri kabul etme yetkisine sahiptir (Avrupa Komisyonu, 2022b);

a) Veri sorumluları ve veri işleyenler arasındaki ilişkiyi belirleyen: GVKT m. 28(3), 2018/1725 sayılı Tüzük m. 4 uyarınca öngörülen yükümlülüklerin yerine getirilmesini teminen düzenlenen bu SCC'ler, kamu kurumları ve özel kuruluşlar tarafından olduğu kadar Birlik makamları, kurumları veya kuruluşları tarafından da kullanılabilecektir (Avrupa Komisyonu, 2022b). Ancak bu nitelikteki SCC metinlerinin geçerliliği yetkili makamın iznine tabidir.

GVKT m. 28(8)'e göre veri koruma otoriteleri, veri sorumluları ile veri işleyenler arasındaki ilişkiyi düzenleyen SCC metinlerini kabul edebilir. Bu noktada belirtmek gerekir ki, veri koruma otoriteleri tarafından kabul edilen bu SCC metinleri, anılan veri koruma otoritesinin yetki alanında geçerli olacak olup, diğer ülkelerde geçerli olup olmayacağı hususu ise o ülkelerin veri koruma otoritelerinin kararına bağlı bırakılmaktadır.

Bununla birlikte, GVKT m. 28(7) uyarınca Komisyon tarafından kabul edilen SCC'ler ise tüm AEA genelinde geçerli olup, AEA sınırları içerisindeki tüm veri koruma otoriteleri bakımından bağlayıcıdır. Zira bu metinler AEA geneline ilişkin yeknesak yaklaşımlar içermekte olup, Komisyon tarafından kabul edilen SCC metinlerinin geçersizliği ancak ABAD nezdinde öne sürülebilir.

b) AEA dışı ülkelere veri aktarımının yapılmasını sağlayan: Bu SCC'ler, AEA dışındaki ülkelere veri aktarımının yapılabilmesini teminen düzenlenmiştir. Mezkûr SCC'ler ile AEA dışındaki ülkelere veri aktarımının yapılması durumunda kişisel verilerin yüksek seviyede korunabilmesi için alınması gereken özel tedbirlere yer verilmektedir (Avrupa Komisyonu, 2022b). Anılan SCC'ler ile göndericiler, herhangi bir veri koruma otoritesi tarafından izin alınmaksızın bu SCC'leri kullanarak veri aktarımını gerçekleştirebilecektir (Avrupa Komisyonu, 2022b). Yurt dışına veri aktarımına ilişkin SCC metinleri bu kategori kapsamında olduğundan AEA dışı ülkelere veri aktarımının yapılmasını sağlayan SCC'lere ilişkin detaylı açıklamalara bu başlık altında yer verilecektir.

4 Haziran 2021 tarihinde Komisyon Birlik/AEA'daki (ve diğer türlü GVKT'ye tabi olan) veri sorumlusundan veya veri işleyenden Birlik/AEA dışındaki (ve GVKT'ye tâbi olmayan) veri sorumlusuna veya veri işleyene veri aktarımı yapılabilmesini teminen modernize edilmiş standart sözleşme hükümlerini düzenlemiştir (Avrupa Komisyonu, 2022c). Söz konusu standart sözleşme hükümleri, mülga 95/46/EC sayılı Direktif zamanında kabul edilen 3 set standart sözleşme hükümlerini (söz konusu setlere aşağıda değinilecektir) ilga etmiş olup, 27 Eylül 2021 tarihinden bu yana eski SCC metinleri olanlar artık kullanılmayacaktır (Avrupa Komisyonu, 2022c). Esas sözleşmeye konu veri işleme faaliyetlerinin değişmemiş olması koşuluyla, 27 Eylül 2021 tarihinden önce eski set standart sözleşme hükümlerini kullanan veri sorumlularının ve veri işleyenlerin söz konusu SCC metinlerini 27 Aralık 2022 tarihine kadar kullanabilmeleri mümkündür (Avrupa Komisyonu, 2022c). 27 Aralık 2022 tarihinden sonra eski SCC metinlerine dayanarak veri aktarımının gerçekleştirilmesi mümkün olmayacaktır (Avrupa Komisyonu, 2022b). Güncel standart sözleşme hükümlerine bakıldığı zaman;

- *Veri sorumlusundan veri sorumlusuna,*
- *Veri sorumlusundan veri işleyene,*
- *Veri işleyenden veri işleyene,*
- *Veri işleyenden veri sorumlusuna*

olmak üzere 4 farklı set (modül) sözleşme seçeneğinin bulunduğu görülmektedir. 95/46/EC sayılı Direktif döneminde ise (2001) veri sorumlusundan veri sorumlusuna; (2004) alternatif veri sorumlusundan veri sorumlusuna; (2010) veri sorumlusundan veri işleyene olmak üzere 3 adet sözleşme seti mevcut idi (Ustaran, 2018a). Görüldüğü üzere, mülga Direktif döneminde sadece veri sorumlusu tarafından gerçekleştirilecek aktarımlar için standart sözleşme hükümleri bulunmaktaydı. Bunun sebebine ilişkin olarak ise standart sözleşme hükümlerinde veri işleyenlerin, Avrupa'dan aktarılan verilere erişen her bir alt yükleniciden söz konusu sözleşme hükümlerinin kabul edildiğine dair taahhüt alınmasının öngörülmesiydi; ancak internet hizmet sağlayıcıları ile ödeme hizmet sağlayıcıları gibi şirketlerin çoğunlukla alt yüklenicilerle iş birliği yaparak söz konusu sözleşme hükümlerini uygulatması oldukça zordu (Determann, 2021). ABAD'ın Ekim 2015'te Amerika merkezli veri işleme hizmet sağlayıcıları için Güvenli Liman seçeneği ortadan kaldırıldığında ve Temmuz 2016'da Birlik-ABD Gizlilik Kalkanı onaylanma sürecine kadar geçen süreçte birçok ABD şirketi sözleşme hükümlerini kabul etmiş olup, bu sayede standart sözleşme hükümleri uluslararası bir standart haline gelmişti (Determann, 2021).

Ancak veri işleyen tarafından yapılacak aktarımlar için standart sözleşme hükümlerinin bulunmaması uygulamada da çeşitli zorluklar çıkarabiliyordu. Yeni güncellenen 4 adet sete bakıldığında ise artık veri işleyen tarafından yapılacak aktarımlar bakımından da sözleşme hükümlerinin getirildiği görülmektedir. Nitekim standart sözleşme hükümlerinin veri işleyenler bakımından da güncelleneceği hususuna Birlik 2017 Strateji Kararında da değinilmiştir. Buna göre mezkûr dokümanda, Birlik'in GVKT'nin sınır ötesi aktarımlar için düzenlediği mekanizmaların uygulamadaki tam potansiyeli hakkında endüstri, sivil topluluklar ve veri koruma otoriteleri ile birlikte çalışacakları ifade edilmiştir (Avrupa Komisyonu, 2022d).

Bununla birlikte, yine Birlik Strateji Kararında eski 29 Numaralı Çalışma Grubu şimdiki Avrupa Veri Koruma Kurulu (AVKK) iş birliği ile reformun uygulanmasına ilişkin olarak öncelikli alanların belirlenmesini teminen paydaşlarla diyalogların sürdürüldüğü, bu kapsamda önceden sürecin başlatıldığı veri işleyenden veri işleyen temalı standart sözleşme hükümlerinin tamamlanmasının da planlandığı hususu yine ifade edilmiştir (Avrupa Komisyonu, 2022d). Günümüzde ise yeni setlerin yayımlanması ile Birlik'in bu stratejisini gerçekleştirdiği de görülmektedir. Bu çerçevede, veri işleyenden veri işleyene yapılacak aktarımlar için de sözleşme hükümlerinin getirilmesi, GVKT reformu sonrası getirilen önemli yeniliklerden biri olmuştur (Avrupa Komisyonu, 2022b). Ayrıca belirtmekte fayda görülmektedir ki, GVKT m. 97'ye göre 25 Mayıs 2020 itibariyle her dört yılda bir

Komisyon, GVKT'nin gözden geçirilmesine ve değerlendirilmesine ilişkin rapor sunmakta olup, SCC'lerin uygulanmasına ilişkin Komisyon tespitlerinin de 2024 yılı itibariyle sunulması beklenmektedir (Avrupa Komisyonu, 2022b).

Standardize edilmiş olmaları ve herhangi bir izne tabi olmamaları hususları göz önünde bulundurulduğunda, anılan SCC'ler uygulanması kolay araçlardan biri olarak kabul edilmektedir. SCC'lerin sağladığı bu avantajlar, özellikle KOBİ'ler veya ticari ortaklarının her biri ile ayrı sözleşme müzakere edecek kaynaklara sahip olmayan diğer şirketler için önem arz etmektedir. Öte yandan anılan SCC'ler, bahsi geçen avantajları ile veri transferi için yapılan geçici sözleşmeler gibi ulusal veri koruma otoritesinden izin alınmasını gerektiren veya sertifikasyon mekanizması gibi uygulanması genellikle maliyetli olan diğer uyum mekanizmalarından da ayrılmaktadır (Avrupa Komisyonu, 2022b). Ayrıca belirtmekte fayda görülmektedir ki, paydaşlardan alınan geri bildirimler doğrultusunda Avrupalı şirketler tarafından en çok kullanılan aracın SCC'ler olduğu görülmektedir (Avrupa Komisyonu, 2022b).

Diğer taraftan, SCC metinleri;

- Metinde yer verilen spesifik seçenekler ve/veya modüllerin seçilmesi,
- Kare kutucuklarda belirtilen doldurulması gerekli metinler (örneğin yetkili mahkemelerin ve kurumların, zaman aralıklarının belirtileceği kısımlar gibi)
- Eklerin (Annex) doldurulacağı kısımlar,
- Kişisel verilerin korunmasına ilişkin alınacak ek tedbirlerin ekleneceği kısımlar,

haricinde değiştirilemez (Avrupa Komisyonu, 2022b). Söz konusu doldurulması beklenen metinler, esas metne etki edecek nitelikte olarak değerlendirilmemektedir (Avrupa Komisyonu, 2022b).

Aktarım taraflarının yukarıda belirtilen doldurulması gerekli metinler haricinde SCC metinlerinin içeriğini değiştirmeyi istemeleri durumunda veri aktarımının gerçekleştirilebilmesi, GVKT m. 46(3)(a)'ya göre *"geçici hükümler"* (ad hoc clauses) niteliğini haiz olarak ilgili veri koruma otoritesi tarafından izin alınması suretiyle gerçekleşebilecektir (Avrupa Komisyonu, 2022b). Yine belirtmekte fayda görülmektedir ki, diğer sözleşme hükümleri doğrudan veya dolaylı olarak SCC metni ile çelişmediği veya ilgili kişi haklarına halel getirmediği müddetçe Taraflar, SCC

metnine ek hükümler getirebilir veya SCC metnini daha geniş bir çerçeveye dahil edebilir (Avrupa Komisyonu, 2022b). Ayrıca Taraflar SCC metinlerinde kendi durumları ile uyan durumları seçmelidir ve uygulanmayacak olan modüller ve/veya seçenekler de silinmelidir (Avrupa Komisyonu, 2022b).

Her ne kadar eski SCC metinlerinde yer alan temel unsurlar korunmuş olsa da, yeni SCC metinleri ile getirilen önemli yeniliklere aşağıda yer verilmektedir:

1. SCC metinlerinin yapısı değiştirilmiştir:

- Bilindiği üzere, eski SCC metinlerinde veri sorumlusu tarafından yapılan aktarımlar kapsamda iken, bu defa ek aktarım senaryoları getirilerek veri işleyen tarafından aktarımın gerçekleşeceği senaryolar da kabul edilmiştir (Avrupa Komisyonu, 2022b).

- İki aktarım senaryosunu kapsayan üç ayrı SCC seti, modüler yapıya sahip bir set ile değiştirilmiştir (Avrupa Komisyonu, 2022b). Aktarım tarafları, kendi durumlarına uyan senaryoyu seçerek genel hükümleri uygulamalıdır (Avrupa Komisyonu, 2022b). Bu noktada ayrıca belirtmek gerekir ki, aynı taraflar için aynı zamanda birden fazla senaryonun (yukarıda da belirtildiği üzere, 4 adet modül bulunmakta olup toplam 4 adet senaryo mevcuttur) uyması durumunda kendilerine uyan senaryoyu seçerek tarafların birden fazla SCC metnini düzenleyebilmesi mümkündür (Avrupa Komisyonu, 2022b).

- *"Yerleştirme hükümleri" (docking clause)* ile yeni bir taraf daha önceden imzalanmış olan SCC'lere eklenebilmektedir (Avrupa Komisyonu, 2022b).

- SCC metinlerinin ekinde *(Annex)*, özel nitelikli kişisel verilerin korumasına ilişkin ek tedbirler, alınacak tedbirlerin listesi, taraflara ve tarafların rollerine ilişkin bilgiler gibi somut bilgilere yer verilerek SCC metinleri tamamlanmaktadır (Avrupa Komisyonu, 2022b).

2. Aşağıdaki gibi birtakım önemli yenilikler getirilmiştir:

- Geliştirilmiş şeffaflık yükümlülüğü ile ilgili kişi haklarına, veri ihlal bildirimine ve sonraki aktarıma dair kurallara ilişkin daha detaylı düzenlemeler gibi GVKT kapsamında düzenlenen yeni yükümlülükler SCC metinlerine dahil edilmiştir (Avrupa Komisyonu, 2022b).

- Veri sorumlusundan veri işleyene veya veri işleyenden alt veri işleyene yapılacak veri aktarımları bakımından GVKT m. 28 kapsamında düzenlenen yükümlülükler SCC metinlerine eklenmiştir. Bu sayede, GVKT m.28'e uyulmasını teminen şirketlerin ayrı bir sözleşme imzalamasına da gerek bulunmamaktadır (Avrupa Komisyonu, 2022b).

- ABAD'ın Schrems II kararının bir uzantısı olarak taraflar artık aktarımlarının özel koşullarını, aktarıldığı ülkedeki yasaları ve kişisel verilerin korunmasını teminen uygulanacak ek tedbirleri belgeleyen korumak için uygulamaya koydukları ek önlemleri ile aktarımın gerçekleştiği yerdeki ekonomik sektörü, verinin türünü ve kategorilerini, alıcının türünü ve işleme sürecinin zamanını belgeleyen bir *"aktarım etki değerlendirmesi" (transfer impact assessment)* yapacaktır (Avrupa Komisyonu, 2022b). Söz konusu etki değerlendirmesi neticesinde olumsuz bir sonuç ortaya çıkarsa, bu durumda taraflar SCC'ye konu aktarımı sadece ek önlemlerin alınması ve bu sayede SCC metninde yer alan hükümlere de uyulması suretiyle gerçekleştirebilecektir (Avrupa Komisyonu, 2022b). SCC'nin imzalanmasından sonra verinin aktarıldığı üçüncü ülkedeki mevzuatın değişmesi başta olmak üzere, Veri Alıcısının artık SCC hükümleri ile uyumlu hareket etmediği Veri Aktaran tarafından anlaşıldığında da aynı prosedür uygulanacaktır (Avrupa Komisyonu, 2022b).

- Kamu kurumlarının aktarım yapılan verilere doğrudan veya dolaylı olarak erişmesi durumunda Veri Aktaran tarafa bilgi verme yükümlülüğü ile hukuka aykırı taleplere itiraz etme yükümlülüğü gibi yeni yükümlülükler getirilmiştir (Avrupa Komisyonu, 2022b). Örneğin, Veri Alıcısının ulusal mevzuatı uyarınca devlet erişiminin sağlandığına ilişkin bildirimde bulunmasına izin verilmediği bazı durumlarda, Veri Alıcısı mümkün olan en kısa sürede mümkün olduğunca fazla bilgiyi iletmek amacıyla yasaktan feragat etmek için elinden gelen çabayı göstermelidir (Avrupa Komisyonu, 2022b). Veri Alıcısı tarafın veri işleyen olduğu durumlarda ise veri işleyenin bu durumu veri sorumlusuna iletmesi gerekmektedir (Avrupa Komisyonu, 2022b). Bununla birlikte Veri Alıcısı, aldığı erişim talepleri hakkında toplu bilgileri düzenli aralıklarla Veri Aktarana sağlamalıdır (Avrupa Komisyonu, 2022b). Bu yükümlülük yalnızca Veri Alıcısının kendi ulusal kanunları uyarınca bu tür bilgileri sağlamasına izin veriliyorsa geçerli olup, Veri Alıcısının veri işleyen olması durumunda bu bildirim yükümlülüğünü veri sorumlusuna yapması gerekmektedir (Avrupa Komisyonu, 2022b). Diğer taraftan, İkincisi, SCC'ler, Veri Alıcısının SCC'de yer alan hükümlere uymasını engelleyen yasa ve/veya uygulamalara tabi olması durumunda ek bildirim gereklilikleri içerir.

SONUÇ

Yukarıda yer verilen açıklamalarda da görülebileceği üzere, gerek 6698 sayılı Kanun gerek Birlik hukuku açısından yurt dışına veri aktarımı müessesesi son derece önem arz etmektedir. 6698 sayılı Kanun ile GVKT'nin yurt dışına veri aktarımına hükümleri arasında benzerlikler olduğu gibi farklılıkların da olduğu görülmektedir.

Ülkemizde yurt dışına veri aktarımı 6698 sayılı Kanunun 9. maddesinde hüküm altına alınmış olup, kişisel verilerin ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamayacağı; 6698 sayılı Kanunun 5. ve 6. maddelerinde belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması veya yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın kişisel verilerin yurt dışına aktarabilmesinin mümkün olduğu hükme bağlanmıştır. Diğer bir deyişle, 6698 sayılı Kanun uyarınca SCC metinleri gibi Kurul tarafından önceden onaylanmış metinlerin doldurulması suretiyle yurt dışına veri aktarımının gerçekleşmesi gibi bir imkân tanınmamaktadır. Her ne kadar Taahhütname metinleri Birlik'in SCC metinleri ile benzer içerikte olsa da ülkemizde Taahhütnamelere dayanılarak yurt dışına veri aktarımı ancak ve ancak bu Taahhütnamelere Kurul tarafından izin verilmesi ile mümkün kılınmıştır.

Yukarıda da ifade edildiği üzere, Birlik hukukuna göre de benzer düzenlemeler bulunmakta olup uygun tedbirlere tabi aktarımlar bakımından farklılıklar öngörülmektedir. Buna göre, Türkiye'de taahhütnameler Kurul iznine tabi iken Birlik Hukukunda yer alan SCC metinleri diye nitelendirilen taahhütname metinleri ise herhangi bir izne tabi değildir.

Yurt dışına veri aktarımı bağlamında ülkemizin ticari ve ekonomik açıdan güç kazanabilmesi ve diğer ülkeleri yatırıma teşvik edebilmesi için yurt dışına veri aktarımının güven mekanizmaları tesis edilerek çok katı düzenlemelere tabi tutulmaması gerektiği düşünülmektedir. Nitekim yurt dışına kişisel veri aktarımında katı düzenlemelerin öngörülmesi çoğu ülke ve sektör bakımından caydırıcı olarak görülmektedir. Olası bir kanun değişikliğinde SCC metinleri gibi yetkili makam (ülkemizde Kurul olacağı düşünülmektedir) tarafından önceden onaylanmış metinlere dayanılarak yurt dışına veri aktarımının herhangi bir izne tabi olmaksızın aktarılmasına ilişkin mekanizmanın getirilmesinin önem teşkil ettiği değerlendirilmektedir.

Bununla birlikte belirtmekte fayda görülmektedir ki, özellikle uluslararası bağlamda Birlik düzenlemeleri önem teşkil etmekte olup ülkeler arasında yapılan veri aktarımına ilişkin anlaşmalarda Birlik hukuku kapsamında düzenlenen uygun güvencelere yer verilmesi hususu da aranabilmektedir. Bu ahvalde, özellikle uygun tedbirlere tabi aktarımlar bakımından GVKT hükümleri ile ABAD içtihatı, Avrupa Veri Koruma Kurulu'nun (eski hali Madde 29 Çalışma Grubu) görüşleri ve rehberlerinde yer alan kriterlerin mevcut olması, güven çerçevesinde serbest veri akışı gerçekleşmesinde büyük rol oynamaktadır. Özellikle Avrupa Birliği Adalet Divanının Schrems I ve Schrems -II kararlarından sonra Birlik hukukuna göre uygun güvencelerin tesis edilmesinde özellikle aktarımın yapıldığı üçüncü ülkede etkili ve icra edilebilir ilgili kişi haklarının bulunması ile kamu makamlarının aktarılan verilere erişimine ilişkin ek yükümlülüklerin getirilmesi unsurları önem teşkil etmektedir.

GVKT'deki farklılıklardan biri de veri işleyenin de temel aktörlerden biri olarak muhatap alınmasıdır. Bu çerçevede, veri aktarımında veri işleyenler de veri aktaran olabilmektedir. 6698 sayılı Kanunda ise sadece veri sorumlusu muhatap alınmakta olup veri işleyen sadece veri alıcısı taraf olabilmektedir.

Bu doğrultuda, halihazırda yürütülen 6698 sayılı Kanunun Avrupa Birliği ile uyumlaştırılması sürecinde de 9. maddenin değişmesi durumunda davranış kuralları, sertifikasyon, standart taahhütname metinleri gibi mekanizmaların hukukumuzda yer alacağı değerlendirilmektedir. Bu tür mekanizmalar kanun kapsamında detaylı düzenlenmeyecek olsa bile gerek ikincil düzenlemelerle gerek Kurum tarafından çıkarılan açıklayıcı rehberlerle detaylı olarak düzenlenebileceği değerlendirilmektedir. ◆

KAYNAKÇA

- Akçalı Gür, B. (2019). Uluslararası hukuk ve AB hukuku boyutuyla kişisel verilerin yurt dışına aktarılması. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi. Cilt 25. Sayı 2. 850-872.
- Avrupa Birliği Başkanlığı. (t.y.) Avrupa Birliği Antlaşması ve Avrupa Birliği'nin İşleyişi Hakkında Antlaşma. https://www.ab.gov.tr/files/pub/antlasmalar.pdf adresinden 20.04.2022 tarihinde alınmıştır.
- Avrupa Komisyonu. (2022a). Guidelines 07/2022 on certification as a tool for transfers. 5-6. https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf adresinden 11.09.2022 tarihinde alınmıştır. s. 5-6, 11.09.2022.
- Avrupa Komisyonu. (2022b). The new standard contractual clauses- questions and answers overview. 4. https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf adresinden 14.08.2022 tarihinde alınmıştır.
- Avrupa Komisyonu. (2022c). Standard contractual clauses (SCC). https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en adresinden 08.05.2022 tarihinde alınmıştır.
- Avrupa Komisyonu. (2022d). "Communication from the Commission to the European Parliament and the Council-exchanging and protecting personal data in a globalised world", https://eur-lex.europa.eu /legalcontent/EN/TXT/HTML/?uri=CELEX:52017DC0007 &from=EN adresinden 03.05.2022 tarihinde alınmıştır.
- Avrupa Komisyonu. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN adresinden 19.04.2022 tarihinde alınmıştır.
- Avrupa Komisyonu. (t.y.). Charter of fundamental rights of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN adresinden 20.04.2022 tarihinde alınmıştır.
- Determann L. (2021). Kişisel Verilerin Korunması Uygulama Kılavuzu (Av. H. Temel, Çev.). İstanbul: On İki Levha Yayıncılık.
- Develioğlu, H.M. (2017). Avrupa Birliği Genel Veri Koruma Tüzüğü. İstanbul: On İki Levha Yayıncılık.
- Kaya, İ.S., Tolun Y. (2022). Uygulayıcılar İçin Türkiye'de, Avrupa'da ve California'da Kişisel Verilerin İşlenmesi. Ankara: Adalet Yayınevi.
- Kişisel Verileri Koruma Kurumu. (2020). Yurtdışına veri aktarımı kamuoyu duyurusu. https://www.kvkk.gov.tr/Icerik/6828/YURTDISINA-VERI-AKTARIMI-KAMUOYU-DUYURUSU adresinden 19.09.2022 tarihinde alınmıştır.
- Küzeci, E. (2020). Kişisel Verilerin Korunması. İstanbul: On İki Levha Yayıncılık.
- Toparlak, R.T. (2021). Veri Koruması Hukukunda Bağlayıcı Şirket Kuralları: 2016/679 sayılı Genel Veri Koruma Tüzüğü ve 6698 sayılı Kişisel Verilerin Korunması Kanunu Karşılaştırması, İstanbul: On İki Levha Yayıncılık.
- Turan, M. (2021). Karşılaştırmalı Hukukta Kişisel Verilerin Korunması. Ankara: Seçkin Yayıncılık.
- Türkiye Büyük Millet Meclisi. (2022). "Sanayi, Ticaret, Enerji, Tabii Kaynaklar, Bilgi ve Teknoloji Komisyonu Raporu", s.14, https://www5.tbmm.gov.tr/sirasayi/donem27/yil01/ss229.pdf, adresinden 18.09.2022 tarihinde alınmıştır.
- Ustaran, E. (2018a). International Data Transfers", Data Protection A Practical Guide to UK and EU Law. P. Carey (Yay. haz.). Birleşik Krallık: Oxford University Yayıncılık.
- Ustaran, E. (2018b). "International Data Transfers", European Law: Law and Practice, E. Ustaran (Yay. haz.). Amerika: International Association of Privacy Professionals (IAPP).
- Wagner, J. (2018). The transfer of personal data to third countries under GDPR: when does a recipient country provide an adequate level of protection?, International Data Privacy Law. Cilt 8. 318-337.

İLGİLİ KİŞİLERİN KİŞİSEL VERİLERİNE ERİŞİM HAKLARI

Kazım Alper DAŞTAN

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "6698 sayılı Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında İlgili Kişilerin Kişisel Verilerine Erişim Hakları" başlıklı Uzmanlık Tezinden alınmıştır.

GİRİŞ

İngiliz filozof ve devlet adamı Francis Bacon'ın *"Knowledge itself is power.",* yani *"Bilgi, bizzat güçtür."* sözünden, 2010 ile 2016 yılları arasında Birleşik Krallık Başbakanlığı vazifesini icrâ eden İngiliz Muhafazakâr Partisinin lideri David Cameron'ın, TEDTalk 2010'da yaptığı ve gelişen teknoloji ve dijitalleşme vasıtasıyla elde edilen verilerin davranışsalcı ekonomi ilkelerine uygulanmasıyla hükûmetlerin idarî ve iktisadî gücünün yavaş yavaş merkezden yerele ve devletten sivil yapılara geçebileceğini ifade ettiği "The Next Age of Government" (Hükûmetin Gelecek Çağı) başlıklı sunumuna kadar; devletler, iktidarlar, ekonomistler, filozoflar yahut şirketler, dolayısıyla esasen herkes "veri"nin ve aslında veriyle birlikte, o veri kümesinin içermekte olduğu anlamlı bilginin, günümüzün en önemli ürünlerinden biri olduğunun farkındadır. Zira kişisel verilerin belirli amaç doğrultusunda, doğru teknolojik yöntemlerle işlenmesi durumunda insanlar hakkında belki kendilerinin dahi farkında olmadığı yeni veriler üretmek veya insanların siyasî veya ekonomik tercihlerini manipüle etmek mümkün hâle gelebilmektedir. Elbette kişisel verilerin işlenmesi, bu gibi insan gözüne menfi görünen amaçların yanı sıra; örneğin dijital dönüşüm vasıtasıyla devlet idaresine halkın katılımını veya kamunun hesap verebilirliğini artırmak ya da veri temelli ekonominin uy-

gulanmasıyla, ülke dâhilindeki ekonomik çıktıyı, refahı ve verimliliği artırmak yönünde, olumlu sonuçlar da doğurabilir.

Kişisel verilerin işlenmesinin, insanların lehinde yahut aleyhinde sonuçlar doğurması ise kişisel verilerin korunması alanında tatbik edilen ulusal ve uluslararası müktesebata uyum sağlanıp sağlanmamasına bağlı olarak değişecektir. İnsanların kişisel verilerinin hukuka aykırı, orantısız veya onların aleyhlerine sonuç doğuracak şekilde, istismar edilerek işlenmelerine mâni olunması ve diğer tüm olumsuz sonuçlardan kaçınabilmek için bireylerin kişisel verilerinin belirli prosedürlere bağlanarak, orantılı ve hukuka uygun bir şekilde işlenebilmesi adına lüzumlu yasal düzenlemeleri yapmak, gerek dünya gerekse de ülkemiz için ihtiyaç hâline gelmiştir. Nitekim şu anda ülkemizde, 07.04.2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiş bulunan 6698 sayılı Kişisel Verilerin Korunması Kanunu meriyette iken Avrupa Birliği sathında ise Avrupa Birliği Parlamentosu tarafından 14.04.2016 tarihinde kabul edilen Avrupa Birliği Genel Veri Koruma Tüzüğü, Mayıs 2018 tarihinden itibaren yürürlüktedir. Günümüzde kişisel verilerin korunması hukukunun önemi artık kavranmış olmakla birlikte, bu hukukun insan hak ve onuruna yaraşır bir şekilde tatbik ve tahakkuk ettirilmesi, halen gündemdeki önemini ve tazeliğini korumaktadır. Kişisel verilerin korunması hukukunun önemli sac ayaklarından bir tanesi de bu çalışmamızın konusunu teşkil eden *"İlgili kişilerin, kişisel verilerine erişme hakları"*dır. Zira bu hak, ilgili kişilerin, kişisel verilerin korunması hukukuna tâbi hakları bakımından adeta bir ilk adım olarak görülmektedir. Bu hakkının kullanımıyla ilgili kişi; verilerinin işlenip işlenmediğini, işlendiyse nasıl, ne şekilde ve hangi hukukî dayanağa istinaden işlendiğini öğrenmekle birlikte, verilerinin doğru işlenip işlenmediğini ve güncel tutulup tutulmadığını da denetleyebilir ve gerekli düzeltmeleri sağlayabilir. Bu hakkını kullanmaksızın, örneğin ilgili kişi, kendisi hakkında hatalı bir veri işlendiğinden haberdar olmayıp kişisel verileri koruma hukukunun kendisine sağladığı "düzeltme hakkı"nı kullanamayabilir. Bu bağlamda kişisel verilere erişme hakkının kritik bir önem arz ettiği söylenebilir.

Bu çalışmanın amacı; Kişisel Verileri Koruma Kurulu'na intikal eden çeşitli şikâyet ve ihbarlarda da kullanıldığı sıkça görülebilen, *"ilgili kişinin, işlenen kişisel verilerine erişmeyi talep etme hakkının"* mahiyeti, sınırları ve nasıl anlaşılması gerektiği üzerinde, Avrupa Birliği Genel Veri Koruma Tüzüğü ve 6698 sayılı Kişisel Verilerin Korunması Kanunu bakımından mukayeseli bir incelemede bulunmaktır.

VERİLERE ERİŞİM HAKKININ ULUSLARARASI KAYNAKLARI

Avrupa İnsan Hakları Sözleşmesi

Uluslararası anlamda kişisel verilerin korunmasına ilişkin olarak yorumlanabilecek ilk düzenleme, ülkemizin de kurucu üyeleri arasında bulunduğu Avrupa Konseyi *(Council of Europe)* tarafından hazırlanıp 4 Kasım 1950 tarihinde Roma'da imzalanarak 3 Eylül 1953 tarihinde yürürlüğe giren *Avrupa İnsan Hakları Sözleşmesi*dir (AİHS). Sözleşmenin *"Özel ve aile hayatına saygı hakkı"* başlıklı 8'inci maddesinin birinci fıkrası *"Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir."* hükmünü amir iken aynı maddenin ikinci fıkrası *"Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."* şeklinde bir düzenleme getirmektedir. Söz konusu düzenlemelerde doğrudan doğruya kişisel verilerin koruması alanına hasredilebilecek bir ifade bulunmasa dahi Avrupa İnsan Hakları Mahkemesi'nin (AİHM) içtihatlarıyla kişisel veriler, koruma altına alınmıştır. İletişimin dinlenmesi, özel ya da kamu sektörünce yapılan izleme faaliyetleri, orantısız ve ölçüsüz bir şekilde kamu gücü tarafından kişisel veri depolanması gibi konularda aldığı kararlarla AİHM, yukarıda ifade edilen 8'nci madde hükümleri doğrultusunda, kişisel verilerin gizliliğini koruma altına alacak şekilde içtihatlar geliştirmiştir (European Union Agency for Fundamental Rights (FRA), 2018).

AİHM'in içtihatları doğrultusunda, AİHS'nin 8'inci maddesinin içeriğinde "kişisel verilere erişim hakkı"nın da var olduğunu kabul etmek gerekir (European Court of Human Rights (ECHR), 1989).

Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) Rehber İlkeleri

İkinci Dünya Savaşı sonrası dönemde harp nedeniyle kötü duruma düşmüş ve yeni dönemde ABD müttefiki olacak Batı Bloku ülkelerinin ekonomilerini, serbest ticaret ve demokratik değerler ekseninde onarmak gayesiyle kurulmuş olan Ekonomik Kalkınma ve İş Birliği Örgütü'nün (OECD) kişisel verilerin işlenmesi ve korunması alanına ilişkin ilk uluslararası belgeyi ortaya koyması bir tesadüf değildir. Zira devletlerin; ulusal güvenlik, yerli girişimleri destekleme gibi gerekçelerle birbirinden veri koruma standartları belirlemeleri, ulusal mevzuatların birbirinden ciddi derecede ayrışması ve bunun neticesinde de ekonomik iş birliği imkânlarının zedelenmesi ve korumacı ekonomilerin güçlenmesi neticesini

doğuracaktır (Akçalı Gür, 2019). OECD ise bizzat böylesi bir durumun bir daha uluslararası ortamda oluşamaması için kurulmuş bir yapıdır. OECD tarafından bu maksatlarla 23 Eylül 1980 tarihinde kabul edilen *"Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler"*in amacı, serbest piyasa ekonomisinde verilerin serbest dolaşımını sağlamak, ilgili kişilerin menfaatlerinin korunmasına yönelik düzenlemeler yaparak sınır ötesi veri akışının engellenmesine yol açacak durumları ortadan kaldırmaktır (Develioğlu, 2017).

OECD tarafından ortaya konulan ilkeler, üzerinde uzlaşılması nispeten kolay olan temel ve genel ilkelerden oluşmakla birlikte, tamamen tavsiye niteliğinde olup üye ülkeleri bağlar herhangi bir hukukî vasıf da taşımamaktadır. Ancak dünyadaki pek çok ülkenin veri koruma alanındaki yasal düzenlemelerini bu ilkeleri temel kabul ederek gerçekleştirdiği bilinen bir hadisedir (Cate, Cullen ve Mayer-Schönberger, 2014).

İşte bu ilkelerden bir tanesi de *"Individual Participation"* (Bireysel Katılım) ismini taşımakta olup bu prensip; ilgili kişilerin, veri sorumlularına başvuruda bulunmak suretiyle, kendileriyle alâkalı olarak işlenen bir kişisel veri olup olmadığını makul bir zaman aralığı içerisinde öğrenme, böyle bir verinin mevcudiyeti hâlinde ise bu veriye yine makul bir zaman aralığı içerisinde erişmeyi, ayrıca bu isteklerinin reddi hâlinde ise karara itiraz edebilmelerini içerir.

Söz konusu Rehber İlkeler, aslında veri aktarım olanaklarının günümüze göre son derece sınırlı olduğu ve belki de en önemlisi, "sosyal medya" gibi bir kavramdan mahrum bir dünyada ortaya konulduğundan bu ilkelerin güncellenmesi ihtiyacı hâsıl olmuş ve bu güncelleme de 2013 yılında gerçekleşmiştir.

108 sayılı Avrupa Konseyi Sözleşmesi (ETS 108)

OECD Rehber İlkeleri'nin yayınlanmasını müteakip 28 Ocak 1981'de Avrupa Konseyi'nin *"Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunmasına Dair 108 sayılı Sözleşme"*si, Strasbourg'da imzaya açılmıştır. Konsey üyeleri dışındaki ülkelerin de imzasına açık olan ve 1 Ekim 1995 tarihinde yürürlüğe giren sözleşmeyi 28 Ocak 1981 tarihinde imzalayan Türkiye'de 17 Mart 2016 tarihli ve 29656 sayılı Resmî Gazete'de yayımlanmasıyla birlikte sözleşme, iç hukuka dâhil edilmiştir. Sözleşmenin, Avrupa Konseyine üye olmayan devletlerin de imzasına açık olması, bu sözleşmenin veri koruma alanındaki önemli ve evrensel konumuna katkıda bulunmuştur.

108 Sayılı Sözleşme'nin ortaya çıkmasını sağlayan asıl endişe, ülkelerin birbirine

benzer veri koruma mevzuatları olsa dahi bu kanunlardan ya da hukuk kurallarının pratik hayata tatbik edilmesinden kaynaklanan sorunları en aza indirgemekti. Artık özel şirketlerin ve kamu sektörünün büyük veri bankaları oluşturmaya başladığı, çokuluslu şirketlerin ve bilgisayarlar vasıtasıyla otomatik olarak veri işlemenin/aktarmanın yaygınlaştığı bir dünyada, bir ülkedeki ilgili kişinin kişisel verileri, dünyanın başka bir yerindeki bir şirketin veri tabanında bulunabilmekteydi. Böyle bir durumda ilgili kişinin haklarını nasıl kullanacağının ya da hangi ülkenin mevzuatının somut hadiseye uygulanacağının bilinememesi ortada bir muğlaklık oluşturuyordu. İşte bu tür sorunlara karşı üretilen çözüm, OECD Rehber İlkeleri'nin ya da Avrupa Konseyi'nin bu sözleşmenin ortaya çıkmasından önce aldığı kararların aksine "tavsiye" niteliğini taşımayan, bağlayıcı ve uluslararası iş birliğini teşkil edecek bir sözleşme akdedilmesiydi ki zaten yukarıda arz edilen sıkıntılar, bu sözleşmenin hazırlanış gerekçelerini oluşturmaktadır (Council of Europe (CoE), 1981). Sözleşmeye, Türkiye'nin 8 Kasım 2001 tarihinde imzaladığı bir ek protokol de yapılmış, bu ek protokol ile imzacı devletlerin, ülkelerinde kişisel verilerin korunması alanında yetkili bir veri koruma otoritesi ihdası taahhüt altına alınmıştır. Sözleşmenin imzaya açıldığı tarihten itibaren geçen uzun zaman diliminde yaşanan teknolojik gelişmeler nedeniyle, 17-18 Mayıs 2018 tarihlerinde gerçekleştirilen 128'inci Avrupa Konseyi Bakanlar Komitesi Toplantısında kabul edilen 223 sayılı Protokol ile "108+ Sözleşme" adıyla sözleşme tadil edilmiş olup Türkiye henüz bu yeni sözleşmeyi imzalamamıştır.

ETS 108'in 8'inci maddesinin (b) bendinde, *herkesin makul aralıklarla ve aşırı gecikmeye veya masrafa maruz kalmadan kendisi ile ilgili kişisel verilerin otomatik dosyada bulunup bulunmadığının teyidini almak ve bu bilgilerin kendisine anlaşılır bir biçim altında iletilmesini sağlamak hakkına* sahip olduğu ifade edilmektedir. Güncellenmiş 108 sayılı Sözleşme'nin (108 +) 9'uncu maddesinin birinci fırkasının (b) bendinde de yukarıda belirtilen hak, varlığını sürdürmektedir. Bununla birlikte, Güncellenmiş 108 sayılı Sözleşme'ye İlişkin Açıklayıcı Rapor'da da ilgili kişilere sunulacak bilgilerin kolayca erişilebilir, açık, anlaşılabilir ve ilgili kişiye özel olarak düzenlenmiş uygun bir formatta olması gerektiği açıklamaları yer almaktadır (CoE, 2018).

Birleşmiş Milletler (BM) Rehber İlkeleri

10 Aralık 1948 tarihli Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi'nin 12'nci maddesinde *"Kimsenin özel yaşamına, ailesine, konutuna ya da haberleşmesine keyfî olarak karışılamaz, şeref ve adına saldırılamaz."* ilkesi, 16 Aralık 1966 tarihli ve 2200 A (XXI) sayılı Birleşmiş Milletler Genel Kurulu Kararıyla kabul edilerek imzaya açılan ve 23 Mart 1976 tarihinde yürürlüğe giren Kişisel ve Siya-

sal Haklar Uluslararası Sözleşmesi'nin 17'nci maddesinde ise büyük oranda aynı ifadelerle *"Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfî veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz."* hükmü yer almaktadır. Bu Sözleşme'nin 40'ıncı maddesinin dördüncü fıkrasıyla kendisine sözleşme hükümlerine dair "genel yorumda bulunma" yetkisi verilen Birleşmiş Milletler İnsan Hakları Komitesi, Sözleşme'nin 17'nci maddesine açıklık getirmek üzere yaptığı 1988 tarihli ve 16 sayılı Genel Yorum ile kişisel verilerin korunması hakkının, özel yaşamın gizliliği içerisinde mündemiç bulunduğunu belirtmiştir (Küzeci, 2021). Bu durumda sözleşme ile hemen hemen aynı ifadeleri içeren Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi'nin 12'nci maddesinin de aynı şekilde yorumlanması gereği ortaya çıkmıştır.

Nitekim Birleşmiş Milletler (BM), 1976 tarihinde kişisel veri mahremiyetine yönelik standartları belirlemek gayesine matuf olarak *45/95 sayılı Bilgisayarlarla İşlenen Kişisel Veri Dosyalarına ilişkin Rehber İlkeler* adıyla on maddeden müteşekkil bir kılavuz hazırlamışsa da bu ilkelerin yayımı, söz konusu görüşün verilmesini müteakip olarak 14 Aralık 1990 tarihini bulmuştur. Bu kılavuz yayımlandığı tarihte OECD ve Avrupa Konseyi'nin yukarıda belirtilen çalışmaları hâlihazırda belirli bir olgunluğa eriştiği için BM Rehber İlkeleri'nin etkisi oldukça sınırlı kalmıştır (Develioğlu, 2017). Hâlbuki BM Rehber İlkeleri, ortaya koyduğu veri koruma ilkelerine riayet edilip edilmediğini denetlemek amacıyla bir denetim makamı kurmayı öneren bir hukuk metni olması bakımından örneğin 108 sayılı Sözleşme ya da OECD İlkelerine oranla günümüze daha yakın standartlar öngörmekteydi.

BM Rehber İlkelerinin *"Interested Person Access"* (İlgili Kişi Erişimi) prensibi, kendisi hakkında kişisel veri işlendiğine dair kanıt sunabilen herkesin; uygunsuz bir gecikme ya da masraf olmaksızın kişisel verilerine dair bilgi edinebileceği, anlaşılabilir bir şekilde verilerine erişebileceği ya da hukuka aykırı, gereksiz veya yanlış bir şekilde işlenmiş verileri üzerinde düzenleme ya da silme işlemleri gerçekleştirebileceği belirtilmiştir.

95/46/EC sayılı Avrupa Birliği (AB) Direktifi ve Avrupa Birliği Temel Haklar Şartı

24 Ekim 1995 tarihinde yürürlüğe giren 95/46/EC sayılı *"Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi",* kişisel verilerin korunması alanında bir mihenk taşı olarak kabul edilmektedir. Nitekim 3-4 Haziran 1999 tarihlerinde gerçekleştirilen Köln Zirvesini müteakip açıklanan Sonuç Bildirgesinde, AB sathında kabul edilen temel hakların bir bildirgede ilan edilerek bir araya getirilmesi gerekliliği

ifade edilmiş olup 7 Aralık 2000 tarihinde Fransa'nın Nice şehrinde akdedilen *"Avrupa Birliği Temel Haklar Şartı"* ile sürdürülen çabalar meyvesini vermiştir (Avrupa Birliği ile İlişkiler Genel Müdürlüğü, 2001). Bu anlamda AB Temel Haklar Şartı'nın 8'inci maddesinde *"Kişisel verilerin korunması"* başlığının yer alıyor olmasının, 95/46/EC sayılı Direktifin ortaya koyduğu düzenlemelerin bir ürünü olduğu söylenebilir. Fakat bu noktada şunu da belirtmek gerekir ki, Avrupa Birliği müktesebatı açısından "kişisel verilerin korunması hakkı", bir "mutlak hak" değildir. Bu bağlamda kişisel verilerin korunmasına dair haklar icrâ edilirken, diğer temel haklarla arasında bir dengeleme yapılması gerekecektir (Court of Justice of the European Union (CJEU), 2010). Konumuz bakımından şunu da ilave etmek gerekir ki, Avrupa Birliği Temel Haklar Şartı'nın 8'inci maddesinin ikinci fıkrasında, *"Herkesin kendisi hakkında tutulan verilere erişme ve bunların düzeltilmesini isteme"* hakkının bulunduğu, hukukî teminat altına alınmıştır.

Aslında hazırlanış maksadı bakımından esas olarak yine yukarıda arz edilen rehber ilkeler ya da düzenlemeler gibi ticarî ve ekonomik kaygıları yansıtan ve AB üyesi ülkelerin ulusal mevzuatlarının uyumlaştırılarak verilerin serbest dolaşımının sağlanması amacında olan (Akıncı, 2017) bu direktif ile kişisel verilerin korunması alanında ilk defa temel ve genel prensiplerin ortaya konulmasıyla yetinilmeyerek konuya ilişkin detaylı düzenlemelere gidilmiş; üye devletlerce direktif kurallarına uyulmasının denetlenmesi amacıyla bağımsız bir denetim makamı *(Veri Koruma Otoritesi – Data Protection Authority)* ihdas edilmesi kayda bağlanmış, öte yandan da direktifin tatbikine ilişkin sorunları, tereddütleri gidererek gerekli uygulama birliğini sağlamak amacıyla önerilerde bulunmak üzere bağımsız bir danışma kurulu hüviyetindeki "Madde 29 Çalışma Grubu" *(Article 29 Working Party)* teşkil edilmiştir. Direktifin, veri koruma hukuku alanındaki önceki uluslararası metinlerden bir diğer farkı da örneğin 108 sayılı Sözleşme'nin 3'üncü maddesinde taraf ülkelere, sözleşme ilkelerini salt gerçek kişilere ait verilere değil, tüzel kişilerin verilerine de uygulayabilecekleri konusunda yetki verilmesine karşın Direktif'te yalnızca gerçek kişilere ait verilerin hukukî koruma altına alınmış ve "kişisel veri" kavramının sınırının bu şekilde çizilmiş olmasıdır. Ayrıca 108 sayılı Sözleşme'den farklı olarak Direktif, otomatik vasıtalarla veri işlemenin yanında manüel metotlarla veri işlenmesini de hukukî koruma altına almaktadır.

Direktif'in yarattığı etki, bilhassa AB sınırları dışına yapılacak veri aktarımını "transferin yapılacağı ülkede yeterli veri koruma önlemlerinin alınmış olması" şartına bağlaması sebebiyle yalnız AB içerisinde kalmayarak tüm dünyaya sirayet etmiş olsa da AB hukuk müktesebatı içerisinde "direktif" seviyesindeki bir düzenlemenin üye devletler tarafından yapılacak gerekli yasal düzenlemeler vasıtasıyla iç hukuka dâhil edilmesi gerektiğinden, her ne kadar aynı esaslar doğrultusunda

hareket edilerek ortaya konulmuş da olsalar bu yasal düzenlemelerin getirdiği uygulama farklılıkları nedeniyle AB düzeyinde yeknesak bir hukukî ortam oluşturabilmek mümkün olmamıştır. Bu sebeple Birlik düzeyinde, AB müesseselerince kişisel veri işlenmesi durumunda uyulacak veri işleme kurallarını içeren 18 Aralık 2000 tarihli ve 45/2001 sayılı *"Kişisel Verilerin AB Kurum ve Organları Tarafından İşlenmesi Karşısında Bireylerin Korunması ve Bu Verilerin Serbest Dolaşımına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Tüzüğü"* de ayrıca kabul edilmiştir. Bu Tüzük ile birlikte getirilen en önemli yenilik, AB düzeyinde veri mahremiyetine ilişkin kuralların uygulanışını denetlemek amacıyla bir Avrupa Veri Koruma Denetmeni (*European Data Protection Supervisor* – EDPS) kurulmuş olmasıdır.

İlgili kişinin kişisel verilerine erişim hakkı, Direktif'in 12'nci maddesinde kendisine yer bulmuştur.

2016/679 sayılı Avrupa Birliği (AB) Genel Veri Koruma Tüzüğü

Avrupa Birliği içerisinde daha güçlü ve yeknesak bir veri koruma ortamı oluşturmak amacıyla devam eden çalışmalar, AB Komisyonu tarafından 4 Kasım 2010 tarihinde yapılan *"Avrupa Birliği Dâhilinde Kişisel Veri Koruması Üzerine Kapsayıcı Bir Yaklaşım"* (European Commission, 2010) başlıklı bir açıklama ile kamuoyu ile paylaşılmıştır.

Küreselleşme ve teknoloji alanındaki hızlı değişimlerin kişisel verilerin korunmasına ilişkin yeni zorluklar yarattığı zorluklara dikkat çekilen bu açıklamada, tahmin edilemeyen boyutta verinin tespiti artık çok daha zor olan sofistike metotlarla işlenebildiğinden çocukların çevrim içi mahremiyetine kadar geniş bir alanda genel bir çerçeve çizilmiş ve veri koruma alanına dair yapılacakların bir yol haritası çıkartılmaya çalışılmıştır. İşte bu çalışmaların vardığı yer, AB nezdinde geçerli olacak yeni bir Tüzük hazırlanması olacaktır.

95/46/EC sayılı Direktifin AB müktesebatı içerisinde bulunduğu konumdan dolayı ortaya çıkan problemler sebebiyle, yapılacak yeni düzenlemenin üye devletler tarafından iç hukuka dâhil edilmesi gerekecek bir direktif olarak değil de direkt olarak uygulanabilecek bir tüzük mahiyetinde olması gerektiği düşüncesi, otoritelerce uzun müddettir dile getirilmekteydi. Öyle ki AB Genel Veri Koruma Tüzüğü, Avrupa Veri Koruma Denetmeni tarafından 7 Mart 2012 tarafından verilen görüşte de müşahede edilebildiği üzere, bu konuda büyük bir reform ve ilerleme olarak görülmektedir (EDPS, 2012).

27 Nisan 2016 tarihinde kabul edilerek AB Resmî Gazetesi'nin 4 Mayıs 2016 tarihli nüshasında yayımlanan 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (*General Data Protection Regulation - GDPR*), 25 Mayıs 2018 tarihinde ise yürürlüğe girmiştir.

Tüzüğün mülga Direktiften en önemli farkı, belki de yer bakımından uygulanma biçimidir. 95/46/EC sayılı Direktifin dördüncü maddesinde AB üyesi ülkelerce söz konusu Direktifin uygulanması adına çıkartılacak yasalar tarif edilirken, Direktifin sınır ötesi olarak uygulanabilmesi için bu kanunların, *"AB sınırları içerisinde olmayan işletmelerce gerçekleştirilecek veri işleme faaliyetlerinin, üye devletlerde bulunacak araçlarla gerçekleştirmeleri hâlinde Direktif kurallarının uygulanacağının öngörmesi"*nin lüzumu ifade edilmiştir. Bu durumda Direktif, yalnızca veri sorumlusunun ya da veri işleme faaliyetinin üye devletler sınırları içerisinde olması hâlinde uygulanabilecektir. Madde 29 Çalışma Grubu tarafından da eleştirilen bu yöntem, Tüzük ile değiştirilmiş olup Tüzüğün üçüncü maddesinin ikinci fıkrasında; AB sınırları içerisinde bulunmayan veri sorumlusu ya da veri işleyenin veri işleme faaliyetinin, AB vatandaşı bireyleri hedef alarak, bu ilgili kişilere mal veya hizmet sunumuna ilişkin olması ya da yine bu ilgili kişilerin AB sınırları içerisindeki çevrimiçi hareketlerinin gözlenmesine ilişkin verileri içermesi durumunda Tüzüğün uygulama alanı bulacağı hükme bağlanmıştır. Direktif ile Kurulan Madde 29 Çalışma Grubu da yerini Avrupa Birliği Veri Koruma Kurulu'na (European Data Protection Board) bırakmıştır.

Tüzük'te Direktif'te var olan erişim hakkı, 15'inci maddede muhafaza edilmekle birlikte; nüsha sağlama mekanizması, veri taşınabilirliği hakkı gibi ilave korumalarla daha da güçlendirilmiştir.

VERİLERE ERİŞİM HAKKININ ULUSAL KAYNAKLARI

Ülkemiz her ne kadar Avrupa Konseyince imzaya açılan Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunmasına Dair 108 sayılı Sözleşmeyi imzaya açıldığı tarih olan 28 Ocak 1981'de imza etse de, bu sözleşme uzun bir müddetle onaylanarak iç hukukumuza dâhil edilmemiştir. Bunun nedeni olarak söz konusu sözleşmenin dördüncü maddesinin birinci fıkrasında imzacı tarafların, kendi iç hukuklarında sözleşmede yer alan verilerin korunmasına ilişkin temel ilkelere işlerlik kazandırmak amacıyla gerekli önlemleri alacağının; ikinci fıkrasında ise bu önlemlerin en geç sözleşmenin kendisi bakımından yürürlüğe girdiği tarihte alınmasının zorunlu olacağının belirtilmesi gösterilmektedir (Atak, 2010). Bu durum, Türkiye'nin Avrupa Birliği nezdinde yaşadığı tam üyelik sürecini sekteye uğratmış ve AB'nin Türkiye hakkında hazırladığı İlerleme Raporlarında; müzakere fasıllarından özellikle 23'üncü fasıl olan *"Yargı ve Temel*

Haklar" ile 24'üncü faslı teşkil eden *"Adalet, Özgürlük ve Güvenlik"* konularıyla alâkalı olarak eleştirilere yol açmıştır (Civelek, 2011).

Ülkemizde kişisel verilerin korunması alanında yapılan ilk düzenlemeler, 2004 yılında çıkartılan 5237 sayılı Türk Ceza Kanunu kapsamında yapılmıştır. 5237 sayılı Türk Ceza Kanunu'nun 135 ila 138'inci maddelerinde kişisel verilerin korunmasına ilişkin bağımsız suç tipleri düzenlenmiş olup bu suçlar; "kişisel verilerin hukuka aykırı olarak kaydedilmesi", "verileri hukuka aykırı olarak verme ya da ele geçirme" ve "verileri yok etmeme" olarak tespit olunmuştur. Fakat uygulama alanı sınırlı kanunlarda yer alan birkaç hükümle devasa bir alanın düzenlenemeyeceğinden kişisel verilerin korunması alanını düzenleyecek müstakil ve bütüncül bir kanuna ihtiyaç duyulmuştur.

Teknolojinin gelişimi ile birlikte yaygınlaşması ve Türkiye'nin 2000'li yılların başından bugüne yaşadığı iktisadî büyüme neticesinde internete erişim, cep telefonu kullanımı, akıllı TV sahipliği vb. veri işleme faaliyeti yürüten teknolojik vasıtalara ulaşım imkânının artmasına paralel olarak aynı gelişimin hukukî sahada yaşanmaması, yalnızca sonuç bölümü kamuoyu ile paylaşılan T.C. Cumhurbaşkanlığı Devlet Denetleme Kurulu'nun "GİZLİ" ibareli 2013 yılındaki raporuna da konu olan endişe verici gelişmelere sebep olmuştu. Bu raporun 790'ıncı sayfasında 8'inci Tespit ve Öneri olarak, *"Var olan yasal altyapının yeterli olmadığı, kişisel verilerin korunması konusunda çerçeve bir kanuna ihtiyaç olduğu..."* ifade edilmiştir.

Bu ihtiyacın giderilebilmesi için kişisel verilerin korunması alanında bir kanun hazırlanmasının gerekliliği anlaşılmış ve bu konuda çalışmalarda bulunmak üzere 13 Eylül 1995 tarihinde bir komisyon oluşturulmuş; ancak bu komisyon çalışmalarını tamamlayamadan 2000 yılında yeniden teşkil edilmiştir. 2003, 2008 ve 2014 yıllarında hazırlanan tasarılar Türkiye Büyük Millet Meclisi'ne sunulmuş ise de kanunlaşamamıştır (Oğuz, 2013).

Kişisel verilerin korunması alanına yönelik bir kanun hazırlanması çalışmaları sürerken bu çalışmaların bir türlü nihayete erememesi neticesinde, öncelikle 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun'un 2'nci maddesi vasıtasıyla 1982 tarihli Türkiye Cumhuriyeti Anayasasının "Özel hayatın gizliliği" başlığını haiz 20'nci maddesine *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* hükmünü içeren üçüncü bir fıkra eklenmesi teklif edilmiştir. Madde gerekçesinde; anayasada kişisel verilerin korunmasına ilişkin dolaylı ifadeler bulunmasına karşın bu hükümlerin yeterli olmadığı, mukayeseli hukuk ve taraf olunan uluslararası sözleşmelerin kişisel verilerin korunmasını önemle vurguladığı, bu maddeyle herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkının anayasal bir hak olarak teminat altına alınmış olacağı, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğunun ve kişisel verilerin hangi hâllerde işlenebileceğinin hükme bağlanırken kişisel verilerin korunmasına ilişkin esas ve usullerin ise kanunla düzenleneceği ifade edilmiştir. Bu düzenlemenin yapılmasından önce Anayasamızda kişisel verilerin korunmasına dair müstakil bir hüküm bulunmasa da Anayasa'nın Başlangıç bölümünün 6'ncı paragrafında *"Her Türk vatandaşının bu Anayasadaki temel hak ve hürriyetlerden eşitlik ve sosyal adalet gereklerince yararlanarak milli kültür, medeniyet ve hukuk düzeni içinde onurlu bir hayat sürdürme ve maddi ve manevi varlığını bu yönde geliştirme hak ve yetkisine doğuştan sahip olduğu"* ifade edilmekle birlikte Anayasa'nın *"Kişinin dokunulmazlığı, maddi ve manevi varlığı"* başlıklı 17'nci maddesinin birinci fıkrası da "Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir." hükmünü ihtiva etmektedir. Yine Anayasa'nın "*Özel hayatın gizliliği*"ni düzenleyen 20'nci maddesinin birinci fıkrası da kişisel verilerin korunmasını isteme hakkıyla alâkalı üçüncü fıkra eklenmeden önceki *"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz."* hükmünü içermekteydi. Ayrıca Anayasamızın *"Düşünce ve kanaat hürriyeti"* başlığını haiz 25'inci maddesinin ikinci fıkrasında *"Her ne sebep ve amaçla olursa olsun kimse, düşünce ve kanaatlerini açıklamaya zorlanamaz; düşünce kanaatleri sebebiyle kınanamaz ve suçlanamaz."* denilmektedir. Kişisel verilerin korunması hakkının, bu temel hak ve özgürlükler ile yakın irtibatı sebebiyle, 2010 yılında gerçekleştirilen anayasa değişikliğinden önce kişisel verilerin hukukumuzda hiçbir şekilde korunmadığını söylemek doğru olmaz. Örneğin Anayasa Mahkemesi'nin 5429 sayılı Türkiye İstatistik Kanunu'nun, haklarında veri toplanacak gerçek ve tüzel kişilerin bu bilgileri vermekle yükümlü olmalarına dair maddesine ilişkin olarak 2006/167 Esas, 2008/86 Karar sayılı Kararında bu irtibat vurgulanmıştır.

108 sayılı Sözleşme, 6669 sayılı Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile onaylanarak 18 Şubat 2016 tarihli Resmî Gazetede yayımlanmıştır. Bu sırada hâlihazırda 18 Ocak 2016 tarihinde Türkiye Büyük Millet Meclisi Başkanlığına sevk edilen Kişisel Verilerin Korunması Kanunu tasarısı,

24 Mart 2016 tarihinde TBMM Genel Kurulu tarafından kabul edilerek kanunlaşmış ve 7 Nisan 2016 tarihli ve 29677 sayılı Resmî Gazetede *"6698 sayılı Kişisel Verilerin Korunması Kanunu"* ismiyle yayımlanarak yürürlüğe girmiştir. Kanunun hazırlanmasında yer alan ve yukarıda gösterilen sebepler, Adalet Komisyonu Raporunda kendisine yer bulmuştur (Türkiye Büyük Millet Meclisi Adalet Komisyonu, 2016).

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun *"İlgili kişinin hakları"* başlığını taşıyan 11'inci maddesinin (b) bendi, *"Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;... b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,... haklarına sahiptir."* hükmünü amirdir. Görüleceği üzere, ilgili kişinin hakları arasında lafzen "kişisel verilerine erişme hakkı" zikredilmemiştir. Ancak söz konusu kanunun dayanağı olan Türkiye Cumhuriyeti Anayasası'nın *"Özel hayatın gizliliği"*ni düzenleyen 20'nci maddesinin üçüncü fıkrasında, herkesin verilere erişme hakkının var olduğu da ortaya konulduğundan ve normlar hiyerarşisi uyarınca, anayasal bir teminatı açıklamak üzere çıkartılan kanun, söz konusu anayasal hükmü daraltamayacağından, bu bentte ifade edilen hükmün ilgili kişilerin verilerine erişim hakkını da kapsadığı yönünde yorumlanması gerekecektir. Nitekim Kişisel Verileri Koruma Kurulu'nun 2021/470 sayılı Kararında; 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun *"İlgili kişinin hakları"*nı düzenleyen 11'inci maddesinin (1) numaralı fıkrasının (b) bendinde yer alan *"Kişisel verileri işlenmişse buna ilişkin bilgi talep etme"* hakkının, söz konusu veriye erişim hakkını da kapsadığı; erişim hakkının, ilgili kişinin bilgi talep etme hakkını tamamlayarak ilgili kişinin kişisel verileri üzerindeki haklarını kullanabilmesi için kişisel verilerinin ne şekilde işlendiğine dair tam olarak bilgi sahibi olmasına imkân sağladığı belirtilerek ilgili kişilerin kişisel verilerine erişme hakkının 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda var olduğu yorumu yapılmıştır.

VERİLERE ERİŞİM HAKKI

Verilere Erişim Hakkının Amacı ve Muhtevası

İlgili kişilerin kendilerine ilişkin olan verileri üzerindeki nisbî hâkimiyetlerini yitirmemeleri, yani işlenen verilerinin akıbetinden belirli bir çerçeve üzerinden de olsa bilgi sahibi olmaları, şeffaflığın bir aracı olmakla birlikte aynı zamanda da kişisel verilerin korunması mevzuatının ulaşmayı arzuladığı temel amaçlar arasındadır. Zira ilgili kişinin, kendisine dair işlenmekte olan verilerden hiçbir şekilde haberdar olamadığı, bu verilerle ne yapıldığını asla bilemediği bir ortamda kişisel verilerin korunmasından ya da hukuka uygun veri işlenmesinden elbette ki söz edilemez. Nitekim kişisel verilerinin işlendiğinden haberdar olmayan bir

kişinin, diğer haklarını kullanarak bu verilerini var olan hukukî korumadan yararlandırması ya da eksik veya yanlış işlenmiş olan kişisel verilerini düzeltmesi yahut tamamlaması mümkün olmaz.

İşte bu amaca ulaşmayı sağlayacak enstrümanlardan belki de en önemlisi, ilgili kişilerin kendilerine dair işlenmekte olan kişisel verilerine erişme hakkıdır. Bu hakkın varlığı, daha önce de belirttiğimiz şekilde, kişisel verilerin korunması hakkının bir "insan hakkı" yaklaşımından bakılmak suretiyle değerlendirildiğinin delilidir. İnsan hakları bağlamından bakıldığında bireyin, kendisine ilişkin verileri üzerindeki hâkimiyeti asla sona ermez. Çünkü bu hakkın sona erdiği düşünüldüğünde verinin artık ilgili kişiye ait olmadığı, yani verinin mülkiyetinin ilgili kişiden veri sorumlusuna ya da işleyene devredildiği anlaşılacaktır (Göçmen Uyarer, 2019). Bu sebeple olsa gerek Almanya Anayasa Mahkemesi 15 Aralık 1983 tarihli kararıyla; insan onurunun ve kişiliğin korunması haklarına referansla *"Bilgilerin Geleceğini Belirleme Hakkı"nı ("Informationalle Selbstbestimmung")* ortaya koymuştur ki, bu hak da bireylerin kendilerine ilişkin verilerine dair daimî bir bilgi sahibi olma ve çeşitli diğer haklarıyla bu verilerin işlenme sürecine müdahil olma yetkisi bulunduğunu ifade etmektedir (Küzeci, 2021). Bu nedenle verilere erişim hakkının; ilgili kişi bakımından verilerinin doğru ve güncel tutulup tutulmadığını denetleme, bir hatayı düzeltme ya da verilerinin imha edilmesini talep etme gibi haklarının bir ön şartı olarak, yalnızca bunlardan ibaret bulunmadığının da kabulü kaydıyla, değerlendirilmesi mümkündür. Örneğin ilgili kişinin, doğum tarihinin veri sorumlusu tarafından doğru tutulup tutulmadığını bilebilmesi için muhakkak işlenen doğum tarihi verisini görmesi gerekecektir. İlgili kişiye yalnızca *"doğum tarihi veriniz tutulmaktadır"* bilgisinin verilmesi, bu konu bakımından yeterli olmayacaktır.

Verilere Erişim Hakkının İşleyişi

AB Genel Veri Koruma Tüzüğü'nün 63'üncü resitalinde *"Erişim Hakkı"* ele alınmış olup ilgili kişinin, kendisine ilişkin olarak elde edilmiş olan kişisel verilere zahmetsizce ve makul bir zaman aralığı içerisinde; bilgi edinmek, doğrulamak ya da hukukilik unsurunu denetlemek amaçlarıyla erişme hakkının bulunduğu, bu hakkın kendisine ilişkin teşhisler ya da tahlil sonuçları gibi sağlık verilerini de içereceği, mümkün olan durumlarda veri sorumlusunun, ilgili kişiye verisine doğrudan erişim sağlamak amacıyla verinin tutulduğu sisteme uzaktan erişme imkânı tanıması gerektiği, verilere erişim hakkının üçüncü tarafların hakları ya da hürriyetlerine halel getiremeyeceği, ticarî sırlar ya da fikrî mülkiyet haklarının özellikle korunacağı ancak bu ifadelerin de ilgili kişiye talep ettiği tüm bilgilerin sağlanmamasının mümkün olduğu şeklinde yorumlanamayacağı, ilgili kişiyle

alâkalı olarak son derece yüksek miktarda veri işleniyor olması hâlinde, veri sorumlusunun ilgili kişiden talebini daha belirgin hâle getirmesinin isteyebileceği hususları ifade edilmekle birlikte, erişim hakkı ile ilgili olarak temel çerçeve bu şekilde çizilmiştir.

Tüzük'ün 15'inci maddesi ilgili kişinin erişim hakkını düzenlemekte olup ilgili kişinin, kendisi ile ilgili kişisel veri işlenip işlenmediğini veri sorumlusundan teyit etme ve bir işleme faaliyetinin var olması hâlinde; işleme amaçları, işlenen kişisel veri kategorileri, üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar başta olmak üzere kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri, mümkün olması halinde, kişisel verilerin saklanması açısından öngörülen süre veya bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacıyla kullanılacak kriterler, veri sorumlusundan; yanlış işlenen kişisel verilerin düzeltilmesini ya da silinmesini veya söz konusu verilerin işlenmesinin kısıtlanmasını talep etme veya bu veri işleme faaliyetine itiraz etme hakkının varlığı, bir denetim makamına şikâyet bulunma hakkının varlığı, ilgili kişiye dair kişisel verilerin ilgili kişiden değil de üçüncü bir taraftan elde edilmiş olması halinde, bu verinin kaynaklarına ilişkin mevcut bilgiler, profil çıkarma da dâhil olmak üzere otomatik karar verme mekanizmalarının varlığı halinde bu mekanizmanın işleyişi ve ilgili kişi hakkında varabileceği öngörülen sonuçlar hakkında bilgiler hususlarında bilgi edinme hakkı bulunduğunu ifade etmektedir. Bu ifadelerle ilgili kişilerin verileri üzerindeki hâkimiyetlerinin yitirmemeleri noktasındaki değerlendirmelerimiz tasdik edilmekle birlikte, konunun yine aynı amaçla düzenlenmiş bulunan "aydınlatma yükümlülüğü" ile yakın ilişkisi de dikkat çekicidir. Buna ilaveten, yukarıda da arz edildiği üzere Tüzük'ün 15'inci maddesinin üçüncü fikrasında *"Kontrolör işleme faaliyetinden geçen kişisel verilerin bir nüshasını sağlar. Veri sahibi tarafından talep edilen diğer nüshalar açısında, kontrolör idari masraflara dayalı olarak makul bir ücret talep edebilir. Veri sahibinin talebi elektronik yollarla yapması halinde ve veri sahibi tarafından aksi talep edilmedikçe, bilgiler yaygın kullanılan bir elektronik yolla sağlanır."* hükmü, bahse konu maddenin dördüncü fikrasında ise nüsha elde etme hakkının başkalarının hak ve özgürlüklerini olumsuz yönde etkilememesi gerektiği ilkesi yer almaktadır.

Bu noktada belirtilmesi gereken bir diğer husus da Tüzük ile birlikte getirilen *"veri taşınabilirliği hakkı"*dır. Tüzük'ün 20'nci maddesinde gösterilen belirli şartlar dâhilinde, ilgili kişilerin, kendileriyle alakalı olarak veri sorumlusuna sağlamış oldukları kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta almak ve herhangi bir engelleme ile karşılaşmaksızın bu verileri başka bir veri sorumlusuna iletme hakları mevcuttur. Bu hakkın, ilgili kişilerin verilerine erişim hakkı ile yakından irtibatlı olduğu aşikâr olmakla birlikte, Madde 29 Çalışma Grubu bu hak ile Tek Dijital Pazar hedefi doğrultusunda verilerin serbest dolaşımının ve veri sorumluları arasındaki rekabetin iyileşeceğini öngörmektedir (Article 29 Working Party (WP29), 2017).

İlgili kişinin, işlenmekte olan kişisel verilerine erişme hakkının aslında pek çok hakkını kullanabilmesi adına bir "öncelikli hak" olduğu söylenebilir. Verilere erişim hakkının kullanılmasıyla birlikte ilgili kişi; şeffaf ve yeterli bir şekilde verilerinin işlenmesiyle alâkalı bilgilere ulaşabileceğinden, işlenen verilerinin doğruluğundan ya da söz konusu veri işleme faaliyetinin hukukiliğinden emin olabilir (CJEU, C-434/16). Dolayısıyla yanlış işlenen kişisel verilerin düzeltilmesi ve hukuka aykırı işlendiği ortaya çıkan kişisel verilerin ise imha edilmesi gibi haklar, verilere erişim hakkının kullanılmasıyla daha kolay ve isabetli bir şekilde işletilebilecektir. Ancak elbette, bu hakkın kullanımının diğer hakların kullanımı bakımından bir ön şart olmadığının da bilinmesi gerekir. İlgili kişiler, bu haklarını ayrık olarak da kullanabilirler.

Verilere erişim hakkını, kamu organına karşı, karar alma süreçlerine katılma, şeffaflık sağlama ya da iyi yönetişime ulaşma amaçlarıyla kullanılabilen örneğin *"Bilgi Edinme Hakkı"* çerçevesinde çeşitli kamusal dokümanlara erişme hakkı gibi haklardan ayıran en temel fark, ilgili kişinin verilerine erişim talebi için veri sorumlusuna herhangi bir sebep göstermek zorunda olmamasıdır. Bu bakımdan veri sorumlusunun, ilgili kişinin bu talebiyle kendisine dair işlenen kişisel verilerin doğruluğunu, bu veri işleme faaliyetinin hukukiliğini denetlemesine yardımcı olup olamayacağı ya da ilgili kişinin diğer haklarını kullanmasını kolaylaştırıp kolaylaştıramayacağı gibi hususlarda bir değerlendirme yapmaksızın söz konusu talebi yerine getirmesi gerekir (CJEU, C-141/12 and C-372/12 and Others).

Avrupa Veri Koruma Kurulu'na (EDPB) göre verilere erişim hakkının doğru uygulanması üç sac ayaktan teşekkül etmektedir: İlgili kişinin kişisel verilerinin işlenip işlenmediğinin belirlenmesi, işlenen kişisel verilerin bizzat kendisine erişim ve bunun yanı sıra yürütülen veri işleme faaliyetinin amacı, işleme süresi, alıcı grupları, yurt dışına veri aktarımı, alınan güvenlik tedbirleri gibi, sürece dair ikincil bilgiler (EDPB, 2022).

Burada yeri gelmişken belirtilmesi gereken bir diğer husus da verilere erişim hakkının, yalnızca ilgili kişiyle alâkalı olarak veri sorumlusunca elde edilmiş bulunan verileri kapsamadığıdır. Örneğin veri sorumlusunun ilgili kişiye ilişkin olarak elde ettiği kişisel verileri işlemesi sırasında bu verilerden hareketle yeni kişisel verileri çıkarsaması, mesela ilgili kişiyi profillemesi ya da ilgili kişiyle alâkalı olarak bazı çıkarımlarda bulunması, birtakım sonuçlara varması gibi durumlarda,

bu yeni veriler de ilgili kişi tarafından kullanılabilecek verilere erişim hakkının konusu hâline gelecektir (EDPB, 2022).

Kendisine ulaşan kişisel verilere erişim talebini değerlendirirken veri sorumlusunun tespit etmesi gereken ilk şey, talebi yapan ilgili kişiye ait bir kişisel verinin nezdinde işleniyor olup olmadığıdır. Şayet işlenmiyorsa ilgili kişiye verilecek bilgi, kendisine dair herhangi bir kişisel verinin, veri sorumlusuna ait veri kayıt sistemlerinde işlenmiyor ve bulunmuyor olduğundan ibaret kalacaktır. Ancak veri sorumlusu, ilgili kişiye ait kişisel verilerin işlendiğini tespit etmiş ise bu tespitini ilgili kişiye karşı da doğrulamak durumundadır.

Bu işlemin gerçekleştirilebilmesi ise ancak öncelikle veri sorumlusuna başvuruda bulunarak verilerine erişme talebinde bulunan gerçek kişinin kimliğinin tespit edilmesi ile mümkün olacaktır. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün *"Teşhis gerektirmeyen işleme faaliyeti"* başlıklı 11'inci maddesinin birinci fıkrasında *"Bir kontrolörün kişisel veri işleme amaçlarının kontrolör tarafından bir veri sahibinin teşhis edilmesini gerektirmemesi veya artık buna gerek kalmaması halinde, kontrolör yalnızca bu Tüzük'e uygunluk sağlamak amacıyla veri sahibini teşhis etmek üzere ek bilgi tutmak, elde etmek veya işlemek zorunda değildir."* hükmü; ikinci fıkrasında ise *"Bu maddenin 1. paragrafında atıfta bulunulan hallerde, kontrolörün veri sahibini teşhis edecek bir konumda bulunmadığını gösterebilmesi durumunda, kontrolör, mümkün olması halinde, veri sahibini bu durumdan haberdar eder. Bu durumlarda, 15 ila 20. maddeler, veri sahibinin bu maddeler kapsamındaki haklarını kullanmak amacıyla teşhis edilmesine olanak tanıyan ek bilgiler sağlaması haricinde, uygulanmaz."* hükmü dile getirilmiş olup Tüzüğün *"Veri sahibinin haklarının kullanımına ilişkin şeffaf bilgilendirme, bildirim ve yöntemler"* başlıklı 12'nci maddesinin ikinci fıkrasının *"Kontrolör, veri sahibinin 15 ila 22. maddeler kapsamındaki haklarının kullanılmasına kolaylık sağlar. 11(2) maddesinde atıfta bulunulan hallerde, kontrolörün veri sahibini teşhis edemeyecek bir konumda bulunduğunu göstermemesi halinde; kontrolör, veri sahibinin 15 ila 22. maddeler kapsamındaki haklarının kullanılması yönündeki talebini işleme koymayı reddedemez."* hükmü uyarınca veri sorumlusu, ilgili kişinin kimliğini tespit etmenin olanaksız olduğu durumlarda başvuruda bulunan şahıstan ilave bilgiler talep edebilir. Ancak bu bilgi talebi, elde bilgilerle eşleştirmek suretiyle ilgili kişinin kimliğini kesin olarak tespit etmeye yarayacak bilgi miktarını aşamayacaktır (EDPB, 2022). Böyle bir durum gerçekleşmediği takdirde ise veri sorumlusunun, ilgili kişinin başvurusunu cevapsız bırakma hakkı olmayacaktır.

Veri sorumlusu, ilgili kişilerin kendisine yapacağı verilere erişim taleplerine proaktif bir yaklaşım izlemek suretiyle tamamen hazır olmak zorundadır. Yani ilgili

kişinin talebi hakkında yürütülecek tüm idarî ve teknik süreçler, alâkalı güvenlik tedbirleri alınmış bir şekilde hâlihazırda planlanmış olmalıdır. Bu süreçler; verilere erişim talebinin yapılmasını sağlamak için gerekli mekanizmaların (çevrim içi modül, dilekçe kabul vs.) teşkil edilmesi, söz konusu talebin değerlendirilebilmesi adına yetkin ve uzman personelle teçhiz edilmiş idarî bölümlerin kurulması, gereksiz gecikmeler ya da makul olmayan zaman kaybı olmaksızın ilgili kişinin talebine uygun bir şekilde (çevrim içi modül vasıtasıyla, matbu yazı ile vs.), yeterli açıklamaları havi olarak yanıt verilmesi unsurlarını da kapsamakta olup tüm bu konulardaki işlemlerin gerektiği şekilde yürütülmesi, veri sorumlusunun mesuliyeti içerisindedir.

İlgili kişinin "verilere erişim talebi", ya kendisi ya da mevzuata uygun bir şekilde yetkilendirilmiş bir üçüncü kişi tarafından yapılmalıdır. Bununla birlikte, ilgili kişi ulaşmayı istediği verinin kendisi hakkındaki bir kişisel veri olduğuna emin olmalıdır. Örneğin veri sorumlusunun idari yapısı, veri işleme faaliyetleri, iş modelleri gibi veri sorumlusu hakkındaki genel nitelikteki bilgiler; ilgili kişinin kişisel verisi ile doğrudan bağları olmadığı müddetçe olarak kabul edilemez. Dolayısıyla veri sorumlusu, kişisel verileri koruma hukuku uyarınca bu bilgileri ilgili kişi ile verilere erişim talebi kapsamında paylaşmak zaruretinde değildir. Diğer taraftan ilgili kişinin veri sorumlusu nezdindeki anonimleştirilmiş verileri de artık verilere erişim talebi dâhilinde değerlendirilemeyecektir. Ancak anonimleştirilmiş verinin aksine ilave bilgiler ile ilgili kişi ile arasındaki bağ yeniden teşkil edilebilen *"Takma İsimlendirilmiş Veri"* (Pseudonymised Data) halen kişisel veri mahiyetini taşıdığından verilere erişim hakkı kullanıldığında ilgili kişiye iletilebilecektir.

İlgili kişiye talebini teşkil eden kişisel veri işleme faaliyeti hakkında sağlanacak tüm bilgilerin tam, güncel ve doğru olması, söz konusu talebin de makul bir süre içerisinde, ivedilikle yerine getirilmesi gerekir. İlgili kişiye hatalı veya yanlış, güncelliğini yitirmiş, artık hukukî veri işleme nedenini kaybetmiş kişisel veriler iletilemez. İlgili kişi, veri sorumlusunun hukuka uygun bir şekilde, doğru ve güncel veri işleyip işlemediğini tespit etmek amacıyla ya da bir hatalı verisinin kaynağını öğrenmek maksadıyla da verilerine erişim talebinde bulunabilir. Veri sorumlusu bu talep karşısında verilerini günceller, doğru ve tam hâle getirir ya da hukukî mesnedini kaybetmiş kişisel veri işleme faaliyetlerini sonlandırır ise verilere erişim hakkı doğru bir şekilde kullanılmış olacaktır. Aksi takdirde ilgili kişi, diğer haklarını kullanabilir.

Bu doğrulamayı müteakip ilgili kişinin kendisi hakkında işlenen kişisel verilerine doğrudan erişme hakkını kullanması mümkündür. İlgili kişi hakkında işlenen kişisel veri isim, soy isim bilgisinden sağlık ya da finansal kayıtlarına kadar çok

uzun bir skalada uzanabilir. Burada önemli olan nokta, ilgili kişilerin işlenmekte olan kişisel verilerinin bizzat kendisine erişme hakkı olduğudur. Yalnızca işlenen verilerin ya da veri kategorilerinin genel bir tarifi bu hakkın gereğinin yerine getirildiğini söylemek için yeterli değildir. İşlenen verinin tipi ya da türü öne sürülerek bu hakka bir sınırlama getirilmesi, hakkın, veri işleme sürecine dair ilgili kişinin ilk elden bilgi sahibi olması amacını engelleyeceğinden mümkün olamayacaktır.

Verinin kendisine bizzat erişmekte kasıt, doğrudan doğruya söz konusu verinin elde edilmesi değildir. Örneğin ilgili kişinin veri sorumlusu bünyesindeki bir personelle yaptığı telefon görüşmesinin kayıtlarını istemesi durumunda direkt olarak bu ses kaydının sağlanması bir zorunluluk değildir. Zira söz konusu kayıt, zorunlu olarak üçüncü bir tarafin, yani ilgili kişinin muhatabının sesini, dolayısıyla kişisel verisini içerecektir. Şu hâlde, konuşmanın dinlenerek yazılı dökümünün yapılması ve transkripsiyonunun ilgili kişiye verilmesi durumunda da verilere erişim hakkı yerine getirilmiş sayılacaktır. Bu minvalde, verilerin kendisine erişimin direkt olarak kayıt sistemini elde etmek olmadığı, veri güvenliğine ilişkin tedbirler ve teknik kısıtlar da dikkate alınarak ilgili kişiye makul bir içeriğin sağlanmasının da somut hadisenin özelliklerine göre yeterli olacağı değerlendirilebilir. Bu verilerin doğruluğu hakkında şüpheye düşülmesi durumunda ise yargı mercileri eliyle kaydın kendisinin de celbi talep edilerek teyit mekanizması işletilebilecektir.

Tüzük'te ücretsiz nüsha sağlama şartı, ilgili kişilerin yapmış olduğu verilere erişim talebi kapsamında ilk kopyayı karşıladığı için ilgili kişi tarafından yapılacak ilave nüsha talepleri, makul bir seviyede olması kaydıyla veri sorumlusunca belirlenecek bir bedel ile karşılaşacaktır. Fakat aradan belirli bir süre zaman geçtikten sonra kişisel veri işleme sürecine ilişkin parametreler değişebileceği için bu zaman zarfını müteakip ilgili kişi tarafından yinelenecek talepler, yeni bir kişisel veri erişim talebi olarak değerlendirilerek yine ilgili kişiye kişisel verilerinin ücretsiz bir nüshasının sağlanması gerekecektir (EDPB, 2022).

İlgili kişi, kişisel verilerine erişim talebinde bulunduğu sırada bu talebini kişisel verileri koruma mevzuatı dışında üçüncü bir özel mevzuata, örneğin bir sektörel düzenlemeye dayandırmış ise böylesi bir talebin öncelikle bu sektörel düzenlemede yer alan kural ve kaidelere uygun bir şekilde yerine getirilmesi daha doğru olacaktır. Dolayısıyla şayet bu düzenlemelerde ilgili kişilerin erişmeyi talep ettikleri kişisel verilere ilişkin bir kısıtlama, muafiyet ya da istisna var ise veri sorumlusu, ilgili kişinin verilere erişim talebini yerine getirirken bunları göz ardı etmemelidir. Şayet ilgili kişi esasen sektörel düzenlemelere tâbi olan verilere erişim talebini ayrıca bir de kişisel verileri koruma mevzuatına dayandırarak yapmakta ise o hâlde veri sorumlusu, kişisel verileri koruma hukukunda aranan şartların tamamen sağlanıp sağlanmadığını değerlendirmeli, bunu müteakiben ise söz konusu hukukî düzenlemeler uyarınca ilgili kişiye ayrı ayrı düzenlenmiş yanıtlar göndermelidir. Ancak bu durum, bu farklı yanıtların birbirinden farklı bilgiler içermesi gerekliliğini göstermez. Zira özel sektörel düzenlemelerde yer alan kısıtlar, kişisel verileri koruma hukuku çerçevesinde ilgili kişiye verilecek yanıtta da aynen geçerli olacağından ilgili kişiye bu düzenlemelerden yer alan kurallardan ayrık uygulama yapılarak, örneğin ilave bir bilgi sağlanamaz (EDPB, 2022).

Şayet ilgili kişi, işlenmekte olan kişisel verilerine erişmekle ilgili bir talepte bulunmuş, bu talebi de hukuka uygun bir şekilde veri sorumlusu tarafından karşılanmış ve aradan belirli bir zaman zarfi da geçmiş ise ilgili kişinin tekrar verilerine erişim talebinde bulunması hâlinde, kendisine yalnızca son talebinde yer almayan ya da üzerinde değişiklik yapılan verileri ile alâkalı bilgi iletilmesi ve yalnızca bu verilere erişim sağlanması, ilgili kişinin rızası ve kabulü olmadıkça uygun olmayacaktır. Veri sorumlusu, bu talebi yeni bir hak kullanımı olarak görmek ve ilgili kişinin talep ettiği tüm verilere eksiksiz bir şekilde erişim sağlamakla yükümlüdür, velev ki ileteceği tüm veriler, önceki talep kapsamında iletilmiş bulunanlardan farklı olmasın (EDPB, 2022).

Verilere erişim talebi yerine getirilirken çeşitli yasal kısıtlamalar; örneğin fikrî mülkiyet hakları, ticarî sırlar, yasal istisnalar göz önüne alınmalı ancak bu haklar önüne sürülerek ilgili kişilerin verilere erişim talepleri de reddedilmemelidir. Zira bu hakların korunması suretiyle de verilere erişim hakkı, kısıtlı da olsa yerine getirilebilir. Nitekim bu hususlar, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Başlangıç bölümünün 63'üncü paragrafında sarahaten ifade edilmektedir.

Verilere Erişim Hakkının Doğal Sınırları

İlgili kişinin verilere erişim talebinde bulunması sırasında bu talebini sınırlamaması hâlinde, bu talepten ilgili kişinin veri sorumlusu nezdinde işlenen tüm kişisel verilerine erişim talebinde bulunduğu anlaşılmalıdır. Veri sorumlusu kendiliğinden bu talebi yorumlayarak ilgili kişinin erişimine açacağı verinin tipini ya da miktarını sınırlamak salâhiyetini haiz değildir.

İlgili kişinin, talebini bir veri alt kümesi ile sınırladığı durumlarda ise veri sorumlusu, ilgili kişinin verilere erişim talebinin muhtevasını ve çerçevesini ele alarak ilgili kişiye iradesi ve arzusu hilafina eksik bilgi vermemek adına bu talebi-

ni yorumlamalı ve gerektiği takdirde, ilgili kişinin iradesine daha uygun düştüğü yorumunu yaptığı birtakım bağlantılı ilave bilgileri de ilgili kişinin kendisine iletebilmelidir.

Veri sorumlusunca, ilgili kişinin talebinden bağımsız olarak, iletilecek veri miktarına ya da tipine sınırlama getirilmesine olanak tanıyan bazı özel durumlar vardır. Bu özel durumlar, adeta bu hakkın kullanılmasına ilişkin "doğan sınırları" teşkil ederler. Literatürde ve EDPB'nin rehber dokümanlarında bulunan bu özel durumlar; ilgili kişiye dair yüksek miktarda veri işleniyor olmasının meydana getirdiği zorluklar ve mevzuat tarafından ortaya konulan istisnalar ve sınırlamalar etrafında ele alınmaktadır.

- **İlgili Kişi Hakkında Yüksek Miktarda Veri İşleniyor Olması Durumu:** Veri sorumlusu nezdinde ilgili kişiye ilişkin fazla miktarda kişisel veri işlendiği hâllerde, şayet ilgili kişi de genel bir şekilde "verilere erişim talebi"nde bulunuyorsa bu durum veri sorumlusunca dikkatli bir şekilde değerlendirilmesi gereken bir durumdur. Zira bu talebin aynen yanıtlanması ve ilgili kişi hakkında işlenen tüm türdeki verilerin ilgili kişiye iletilmesi hâlinde ilgili kişiye anlayamayacağı, elinde gerekli araçlar olmadığından kullanamayacağı, doğru bir şekilde değerlendiremeyeceği, üzerinden hareketle veri sorumlusu nezdinde işlenen kişisel verilerinin akıbeti hakkında bir yorumda bulunamayacağı ham bilgilerin iletilmesi durumu ortaya çıkabilir. Ayrıca söz konusu talebi gerçekleştiren ilgili kişinin niyeti, esasen kendisi hakkında işlenen tüm verilere ulaşmak değil, bunlar hakkında genel bir bilgi ve intiba edinmek olabilir. Böylesi bir durumda veri sorumlusu hem ilgili kişinin niyeti ve dile getirdiği talepleri noktasında tam ve eksiksiz bir yanıt vermeli hem de ilgili kişiyi işine yaramayacak bir lüzumsuz veri bombardımanına tâbi tutmaktan kaçınmalıdır. Bunu gerçekleştirebilmek için veri sorumlusu, ilgili kişinin kendisine gönderilecek verileri kullanması ya da anlayabilmesi için gerekli teknik araçları çevrim içi metotlarla, örneğin bir CD içerisinde ilgili kişiye iletebilir ya da böylesi bir durumda ilgili kişinin son derece genel talebini karşılamanın imkânsızlığını ilgili kişiye izah etmek suretiyle ilgili kişiden genel nitelikli talebini biraz daha belirli hâle getirmesini talep edebilir. Nitekim Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Giriş Bölümünün 63'üncü paragrafında ilgili kişiyle alâkalı olarak son derece yüksek miktarda veri işleniyor olması hâlinde, veri sorumlusunun ilgili kişiden talebini daha belirgin hâle getirmesinin isteyebileceği hüküm altına alınmıştır. Örneğin ilgili kişinin kişisel verilerini uzun müddet boyunca çeşitli amaç ve vasıtalarla işlemiş bulunan ve birden fazla departmanında kullanan büyük şirketler ya da kamu müesseseleri Avrupa Birliği Hukuku uyarınca bu yönteme başvurabilmektedir.

- **İlgili Kişinin Talebinin Bir İstisna ya da Sınırlama Kapsamında Olması:** İlgili kişinin erişmeyi talep ettiği ve kendisine ilişkin kişisel veri içeren bilgi ya da belgeler, yasal mevzuatça belirlenen bir istisna kapsamında ise veya ilgili kişinin talebi, mevzuatın belirlediği sınırları aşıyorsa ilgili kişinin veri sorumlusu tarafından bu konuda bilgilendirilip istisna ya da sınırlama kapsamına girmeyen verilerine erişim talebinin yerine getirilmesi yeterli olacaktır.

Bu noktada ele alınması gereken bir diğer mesele de ilgili kişilerin hangi kişisel verilerine erişebileceği meselesidir. Daha önceden de nakledildiği üzere, gerek ulusal ya da uluslararası mahkeme içtihatları gerek yine ulusal veya uluslararası mevzuat hükümleri gerek ilgili kurum ve kuruluşlar tarafından ortaya konulan rehber metinler, "kişisel veri" kavramına genellikle bir tahdit getirmemekte ve ilgili kişiye ilişkin hemen her türlü bilgiye, üçüncü bir tarafın hak ve hürriyetlerine bir halel getirmemek kaydıyla erişilebileceğini ifade etmektedir. Ancak kimi zaman bu analizi yapmak güçleşebilmektedir.

Örneğin Avrupa Birliği Adalet Divanı, göçmenlik başvurusunda bulunan bir kişinin, başvurusunun reddini müteakip, görevlinin düzenlediği zabıtta yer alan hukukî değerlendirmeleri içeren zabıtların "verilere erişim hakkı" kapsamında kendisine teslim edilmesini talep etmesine dair davaya ilişkin olarak verdiği kararında; zabıtlarda yer alan ve ilgili kişilere ait bulunan isim, soy isim, doğum tarihi, uyruk, cinsiyet, etnik köken, din ve dil verileri ile ilgili kişiye ilişkin olduğu görüldüğü takdirde söz konusu evraktaki hukukî değerlendirmenin içerdiği verilerin "kişisel veri" olarak kabul edilebilerek ilgili kişiye iletilebileceğine ancak bu hukukî analizin bizzat kendisinin ilgili kişiye ilişkin bir "kişisel veri" hüviyetinde olamayacağını belirtmiştir (CJEU, 2014).

Bu kararın gerekçesine bakıldığında, verilere erişim hakkının doğuracağı doğal sonucun, itiraz edilen hukukî kararın gerekçesini teşkil eden bilgilerde bir yanlışlık olması hâlinde bunları düzeltme ya da yanlış bilgilerin silinmesi şeklinde tezahür edeceği fakat ilgili kişinin, söz konusu karara gerekçe oluşturan yasal mütalaaların doğruluğunu kontrol etme mercii olmadığı, yani bu mütalaaları elde etse bile bunları düzeltme yetkisi ve kabiliyeti olamayacağı noktasında kanaat hâsıl olduğu görülmektedir (EDPB, 2022). Diğer taraftan verilere erişim hakkı kapsamında ilgili kişiye mezkûr hukukî değerlendirmelere erişim hakkı verilmesi, ilgili kişinin mahremiyetinin korunmasına hizmet etmektense kamunun idarî dokümanlarına erişime hizmet edecektir. Bu noktada bu arzunun, belki de kişisel verilerin korunması hukukundan çok "Bilgi Edinme Hakkı"nın konusu olduğu yorumunun yapılması mümkündür.

Hülâsa, buradan hareketle, verilere erişim hakkının, ilgili kişinin diğer haklarını kullanabileceği ve verilerinin doğruluğunu teyit edebileceği bir şekilde kullanılması gerektiği, aksi hâlde ilgili kişinin verilerine erişebilmesinin bir anlamı olmayacağı söylenebilir. Bir verinin ilgili kişiye ilişkin olduğu ve bu erişim hakkının ilgili kişinin diğer haklarını kullanmasına dair sonuç doğurabileceği "her durumda" ise o verinin, erişim hakkının konusu olacağı söylenebilir. Örneğin bir iş mülâkatında ilgili kişinin giyimi, davranışları, fiziksel görünümü, konuşma şekli, nezaketi, bilgi birikimi gibi insanın aklına gelebilecek hemen her konuda bir değerlendirilmeye tâbi tutulması, bunların görevli tarafından notlarının alınması hâlinde, bu notlar görevlinin sübjektif görüşlerini de yansıtıyor olsa yine ilgili kişinin talebi hâlinde veri sorumlusu, söz konusu notları ilgili kişiye teslim etmek zorunda kalacaktır (EDPB, 2022)

Ancak verilere erişimin doğal sınırları tartışılırken unutulmaması gereken bir diğer husus ise ilgili kişinin erişim talep ettiği verilerin üçüncü bir tarafla alakalı olarak da bilgi içerdiği durumların, erişim hakkının kullanılmasını fazla "kısıtlayıcı" bir şekilde yorumlanmaması gerektiğidir. Her ne kadar Avrupa Birliği müktesebatından hareketle oluşturulan ve doktrinde kabul gören yorum, verilere erişim hakkının üçüncü bir tarafın hak ve hürriyetlerini haleldar edeceği durumlarda kısıtlanabileceğini ifade ediyor da olsa, kimi durumlarda, erişim talep edilen veri zorunlu olarak üçüncü bir kişinin de kişisel verilerini içerir. Örneğin yukarıda da belirtildiği gibi, veri sorumlusunun çağrı merkezi ile yapılan telefon görüşmelerinde, ilgili kişi ile operatörün sesi veri sorumlusu tarafından kaydedilecektir. Bir anlaşmazlık durumunda ilgili kişi, kendi kişisel verisi olduğunu öne sürerek söz konusu kaydın kendisine ya da dökümüne erişim talebinde bulunabilir. Veri sorumlusunun bu talebi "üçüncü bir tarafın haklarının haleldar olacağı" gerekçesiyle iletmemesi, erişim hakkının kullanılmasını imkânsızlaştıracağından doğru bir yaklaşım olarak görülemez. Böylesi bir durumda örneğin kaydın dökümü yapılarak operatörün kişisel verisi hüviyetinde olan sesi gizlenebilir. Bu yapılamıyor ise kaydın kendisi verilerek; bu kaydın üçüncü bir tarafa ait de kişisel verileri barındırdığı, bu kaydın kendisi tarafından farklı bir amaçla kullanılması, örneğin yayımlanması vb. durumlarda ilgili kişinin "veri sorumlusu" sıfatını kazanacağı ve ses kaydında yer alan diğer kişinin "ilgili kişi" sıfatıyla kendisine yönelik birtakım taleplerde bulunabileceği hususlarının ilgili kişiye hatırlatılması mümkündür (EDPB, 2022).

WP29 da "veri taşınabilirliğine" ilişkin rehberinde; pek çok durumda veri sorumlularının, birden fazla ilgili kişiye ait kişisel verileri aynı anda barındıran verileri işlediğini, böyle durumlar söz konusu olduğu vakit veri sorumlularının, "kişisel verinin ilgili kişiye ilişkin olması" ilkesini çok kısıtlayıcı bir şekilde yorumlaması gerektiğini, örneğin telefon görüşmesi kayıtlarının tabiatıyla birden fazla ilgili kişiye ait kişisel veri barındıracağını ancak halen bu kayıtların ilgili kişi tarafından kullanılacak haklarını konusu olarak kalacağını ve elde edilebileceğini belirtmektedir (WP29, 2017).

Kimi durumlarda ise veri sorumlusu, ilgili kişiyle alakalı olarak işlediği kişisel verilere dair kayıtları tamamen arşive kaldırmış ve birtakım yasal zorunluluk gereği saklamakta olabilir. Bu noktada her ne kadar veri sorumlusu, esas faaliyet alanı dâhilinde ilgili kişiyle alakalı olarak kişisel veri işleme faaliyetini sonlandırmış da olsa, en nihayetinde bir veriyi saklamak, muhafaza etmek ve arşivlemek de "kişisel veri işleme faaliyeti" olduğundan, ilgili kişinin talebi hâlinde veri sorumlusunun, teknik açıdan yönetilebilir olduğu müddetçe arşivde saklanan veriyi ilgili kişinin erişimine aşmak mecburiyeti hâsıl olacaktır (EDPB, 2022).

Verilere Erişimin Sağlanma Şekli

Verilere erişimin sağlanması, genellikle küçük işletmelerdeki bazı basit kayıtlara, örneğin sipariş geçmişine erişim talep edilmesi gibi kimi durumlarda oldukça kolay bir şekilde gerçekleştirilebilir iken kişisel veri işleme süreçlerinin; çeşitli veri kategorilerine ve birden fazla ilgili kişiye dair olmak kaydıyla, daha karmaşık, büyük çapta ve yekûnda gerçekleştirildiği, ayrıca bu verilerin diğer üçüncü taraflara aktarıldığı veri işleme faaliyetlerinde, verilere erişim hakkının kullanılma imkânı da tabiatıyla farklılaşmaktadır.

İlgili kişinin talebi veri sorumlusuna ulaştığında, veri sorumlusunun gerek bilgisayar sistemleriyle gerekse de manüel metotlarla işlediği kişisel verileri tespit edebilmek için bilgisayar sistemlerinde ve dosya evrakları içerisinde bir tarama yapması gerekmektedir.

Veri sorumlusu şayet ilgili kişiye ait kişisel verileri işleme görevini anlaştığı bir veri işleyene tevdi etmiş ise bu arama sürecine veri işleyen nezdindeki veri kayıt sistemleri de dâhil edilmelidir. Fakat eğer veri sorumlusu, ilgili kişiye örneğin müşteri numarası gibi bir kod atamış ve tüm işlemleri bu kod üzerinden yürütmüş ise kayıtlarında yapacağı aramayı bu kod ile sınırlı tutabilir ancak şayet bu kod dışında da ayrıyeten örneğin ilgili kişinin kimlik numarası gibi diğer verilerine ilişkin tutulan veriler de varsa yapılan arama, bunları da kapsayacak şekilde genişletilmek zorundadır.

Daha önceden de belirtildiği üzere, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün *"Veri sahibinin haklarının kullanımına ilişkin şeffaf bilgilendirme, bildirim ve yön-*

temler" başlıklı 12'nci maddesinin birinci fıkrası *"Kontrolör spesifik olarak bir çocuğa yönelik her türlü bilgi başta olmak üzere işleme faaliyeti ile alakalı olarak 13 ve 14. maddelerde atıfta bulunulan her türlü bilgi ile 15 ila 22. ve 34. maddeler kapsamındaki her türlü bildirimi öz, şeffaf, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanarak veri sahibine sağlamak için gerekli tedbirleri alır. Bilgileri yazılı olarak veya, uygun olduğu hallerde, elektronik yollar da dahil olmak üzere diğer yollarla sağlar. Veri sahibi tarafından talep edilmesi durumunda, veri sahibinin kimliğinin diğer yollarla doğrulanması koşuluyla, bilgiler sözlü olarak sağlanabilir."* hükmünü, ikinci fıkrası *"Kontrolör veri sahibinin 15 ila 22. maddeler kapsamındaki haklarının kullanılmasına kolaylık sağlar. 11(2) maddesinde atıfta bulunulan hallerde, kontrolörün veri sahibini teşhis edemeyecek bir konumda bulunduğunu göstermemesi halinde, kontrolör veri sahibinin 15 ila 22. maddeler kapsamındaki haklarının kullanılması yönündeki talebini işleme koymayı reddedemez."* hükmünü amirdir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 11'inci maddesinde ise ilgili kişinin hakları sayılmakla birlikte bu hakların "verilere erişim hakkını" da kapsadığını daha öncesinde belirtmiştik. Diğer taraftan kanunun *"Veri güvenliğine ilişkin yükümlülükler"*i düzenleyen 12'nci maddesinin (1) numaralı fıkrasında *"Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır."* hükmüne yer verilmektedir.

Bu mevzuat hükümlerinden anlaşılan, veri sorumlularının gerektiğinde ilgili kişilerin verilere erişim haklarını kullanmak amacıyla yapacakları başvurulara idarî ve teknik anlamda hazır olmaları gerektiğidir. Veri sorumlusu; ilgili kişilerin bu başvurularına yanıt verebilecek ve talepleri karşılayabilecek teknik kabiliyete, idarî örgütlenmeye ve nitelikli personele sahip olmak mecburiyetindedir. Bu "gerekli teknik ve idarî tedbirler", erişim talebinde bulunan ilgili kişinin ya da erişilecek verinin niteliğine göre değişiklik gösterebilir. Örneğin erişim talebinde bulunan ilgili kişinin bir çocuk, verinin niteliğinin ise engellilik verisi olması durumunda, kullanımda olması gereken tedbirlerin normal seviyeye oranla daha üst seviye önlemler olması gerekeceği aşikârdır. Nitekim bu durum, verinin ilgili kişiye iletiliş biçimini de etkileyecektir; bu tür bir verinin örneğin şifreli bir haricî USB diski, CD ya da ancak gerekli anahtarla aktive edilebilen e-posta ile iletilmesi daha makul olacaktır. Fakat bu önlemler alınırken, veri sorumlusunun ilgili kişiye karşı şeffaf hareket etmekle ve erişim sağladığı verileri "anlaşılabilir" bir formatta iletmekle yükümlü olduğu da unutulmamalıdır.

Dolayısıyla veri sorumlusunun; tüm departmanlarında ve şayet varsa veri işleyende bulunan bütün verileri taraması, ardından gerekli güvenlik tedbirlerini almış bir şekilde ilgili kişiye, bu verileri toplulaştırarak, farklı departmanlarca verilecek mükerrer cevaplardan kaçınmak suretiyle iletmesi gerekmektedir. Bu talebi yerine getirmenin çok zor olduğu durumlarda ise "self service" araçları kullanılabilir. Örneğin bugün Twitter gibi milyonlarca üyesi olan sosyal medya şirketleri, kullanıcılarına kendi kişisel verilerini indirme seçeneği sunmaktadır. Fakat bu seçenek sunulurken; ilgili kişiye sağlanması gereken; alınan teknik ve idarî tedbirler, veri işleme süresi, hukukî dayanağı vb. bilgilerin de ilgili kişiye gönderilmesinin lüzumu ile iletilen veri kümesinin anlaşılabilir bir formatta sunuluyor olması gerektiği hatırdan çıkarılmamalıdır. Örneğin ilgili kişinin talebi üzerine ilgili kişiye log kayıtları iletilmesinin, ilgili kişinin gerekli teknik bilgiyi haiz olmaması durumunda ilgili kişi açısından fazla bir manası olmayacaktır. Dolayısıyla söz konusu verinin ilgili kişi için "anlamlı" bir hâle büründürecek açıklamaların da veri sorumlusunca ilgili kişiye gönderilmesi yerinde olacaktır.

Veri iletilirken, uygun başlık ve paragraflar kullanılmalı, bu suretle ilgili kişinin metni kolayca okuması ve anlaması sağlanmalıdır. Ayrıca meselâ verinin iletildiği ilgili kişi bir çocuk ise veri iletilirken ona uygun bir dil ve üslûb kullanılması gerekir. Aynı şekilde, örneğin engelli bir bireye verileri iletilecek ise verinin bu kişinin engelleri göz önüne kılınarak "erişilebilir" kılınması gerekmektedir (EDPB, 2022).

Verilere erişimin sağlanması terimi, zorunlu olarak *"ilgili kişinin, kendisine ait verileri aktif bir şekilde, diğer bilgiler ya da veri kümeleri arasında arayıp bulmaya çalışmaması"*nı ifade etmektedir (WP29, 2018). Şu hâlde, ilgili kişiye bu verilerin iletilmesi ya da söz konusu verilerin bulunduğu ortama erişim sağlanması haricinde, ilgili kişinin birçok veri içerisinden kendisinin arayıp bulmasını gerektirecek bir iletim biçimi, tam ve eksiksiz bir şekilde tahakkuk etmiş bir "verilere erişimin sağlanması" metodu olarak kabul edilemeyecektir.

Kimi durumlarda ise ilgili kişiye örneğin nüsha sağlanması ya da söz konusu veri kayıt ortamına erişim vasıtasıyla bir iletimden daha kolay bir şekilde, kalıcı olmayan çeşitli metotlarla verilere erişim hakkı kullandırılabilir. Bu yöntemler arasında; ilgili kişinin şifahen bilgilendirilmesi, dosyayı incelemek üzerine bizzat veri sorumlusuna gelinmesi, verilerin indirilmesine olanak tanınmaksızın veri sorumlusu nezdindeki veri kayıt sistemlerine uzaktan erişim sağlanması sayılabilir (WP29, 2018). Ancak bu yöntemler, sadece geçici bazı durumlarda kullanılmalı ve ilgili kişinin verilerin doğrudan erişme hakkı, bu metotların kolaylığı öne sürülerek ortadan kaldırılmamalıdır. Örneğin ilgili kişinin yalnızca bir sipariş kaydını teyit etmek amacıyla veri sorumlusuna ulaşması durumunda veri sorumlusu,

ilgili kişiye bu veriyi direkt olarak sözlü bir şekilde iletip teyidini yapabilir. Ancak şayet ilgili kişi tüm sipariş kayıtlarını talep ederse, bunların hepsini telefonda ilgili kişiye okumanın bir anlamı olmayacaktır.

Öte yandan fazla sayıda ilgili kişiye ilişkin olarak son derece yüksek miktarda veri işleyen veri sorumluları, kendilerine ulaşan verilere erişim taleplerini yanıtlayabilmek adına katmanlı bir yaklaşımı benimseyebilirler. Bu yaklaşım, genellikle çevrimiçi bir çözüm olarak önerilmekle birlikte veri sorumluları, kendilerine ulaşan ilgili kişi talebinin niteliğini ve bu talebin amacını, ayrıca ilgili kişinin kendisine iletilecek veri kümesinden ne anlayacağını da göz önüne alarak, ilgili kişinin maksadına ulaşabilmesini sağlayacak olan ve anlayabileceği verileri, en azından asgari miktarda ilgili kişiye iletebilir. Fakat bu sistemin, ilgili kişinin haklarını kullanması noktasında bir engel teşkil etmemesi adına dikkatlice planlanması ve uygulanması gerekecektir. Örneğin böyle bir sistem uygulandığında, ilgili kişinin işlendiği bilmediği bir verinin veri sorumlusu tarafından ilgili kişiye iletilmesi, ilgili kişinin talebinin niteliği ve amacı ile en iyi şekilde eşleşen veriler arandığından mümkün olmayabilir. Dolayısıyla şeffaflık, hukuka ve dürüstlük kurallarına uygunluk prensipleri gereği, veri sorumlusunun böyle bir veriyi mu-
hakkak ilgili kişiye bildirmek için gerekli tedbirleri alabilmiş olması beklenir.

Bu yaklaşımın her koşulda, her veri sorumlusu tarafından sürekli olarak uygulanamayacağı ise göz önünde olan bir husustur.

SONUÇ

Kişisel verilerin korunması hukuku, her gün değişen ve gelişen teknoloji vasıtasıyla çeşitlenen ve yenilenen kişisel veri işleme faaliyetleri karşısında bireyin değerini ve korunmasını önceleyen bir hukuk dalıdır. Bu sebeple, aslında ilgili kişilerin kişisel verilerinin korunması meselesi, çalışmamızda da gösterildiği üzere, doktrindeki hâkim görüşü teşkil edecek şekilde, bir "insan hakkı" olarak doğmuş ve gelişmiş bir alan olarak görülmektedir. Bu hukuk alanı, ilk olarak kamu sektörü ve özel girişimler tarafından bilgisayar gibi otomatik sistemlerin kullanılmaya başladığı tarihlerde, bireylerin kişisel verilerinin yüklü miktarda toplanmasının, işlenmesinin ve muhafaza edilmesinin mümkün olmaya başlaması üzerine gündeme gelmiş, devletler tarafından düzenlenmeye başlanmış ve ülkeler arasında serbest ticarete dayalı bir ortak pazar yaratma fikri etrafında da uluslararası sözleşmelere ve ilkelere de konu olmuştur. Bugün de hızla ilerleyen teknoloji karşısında yenilenmeye ve güncellenmeye muhtaç olan kişisel verileri koruma hukuku, maalesef değişen teknolojiyle aynı hızda olmasa da gelişmeye devam etmektedir.

Çalışmamızda gösterildiği üzere; gerek Avrupa Birliği Genel Veri Koruma Tüzüğü, gerekse de 6698 sayılı Kişisel Verilerin Korunması Kanunu, uluslararası sözleşme ve rehber ilkelere uygun bir şekilde, gerçek kişilerin kendilerine ait olan kişisel verilere erişme talebini tanımakta ve kabul etmektedir. Ülkemizde ve Avrupa'da meskûn bulunan veri koruma otoriteleri, ilgili kişilerin verilerine erişim haklarının olduğu hususunda benzer yorumlarda bulunmuşlardır. Fakat buradaki önemli bir fark, Avrupa Birliği Genel Veri Koruma Tüzüğü'nde ayrı bir başlık olarak ve detaylıca düzenlenmiş bulunan verilere erişim hakkının, ülkemizde câri olan mevzuatta bu şekilde düzenlenmemiş olmasıdır. Zira Avrupa Birliği Genel Veri Koruma Tüzüğü içerisinde verilere erişim hakkı, ülkemizde meriyette olan kanuna göre çok daha detaylı ve sarih ifadeler kullanmış, lafzi anlamda da örneğin "ücretsiz nüsha edinme hakkı" gibi ileri düzenlemelere yer vermiştir. Böylece gerek veri koruma otoriteleri bu konuda daha kolay kararlar alabilmekte gerekse de veri sorumluları, bu düzenlemeler kapsamında gerekli mekanizmaları teşkil ettiğinden bu konudaki ilgili kişi taleplerini daha süratle ve kolayca karşılayabilmektedir. Ülkemizde meriyette olan mevzuatta bu açıklıkta ifadelerin yer almaması, bu hakkın tatbikinde bazı zorluklara yol açabilmekte ise de Türkiye Cumhuriyeti Anayasasına 2010 itibariyle eklenen hükmün verilere erişim hakkını da içerdiği sarih olduğundan, yapılan makul bir yorum ile kanunumuzun da bu hakkı içerdiği yorumu yapılarak bu mesele çözüme kavuşturulmuştur. ◆

KAYNAKÇA

- Akçalı Gür, B. (2019). Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 25, Sayı 2, ss. 850-872. DOI: 10.33433/maruhad.665460.

- Akıncı, A. N. (2017). Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, T.C. Kalkınma Bakanlığı Çalışma Raporu. http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf.

- Article 29 Working Party (2017). Guidelines on the Right to Data Portability, WP 242. http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

- Article 29 Working Party (2018). Guidelines on Transparency under Regulation 2016/679, WP260 rev.01. https://ec.europa.eu/newsroom/article29/redirection/document/51025.

- Atak, S. (2010). Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, TBB Dergisi, Sayı: 87, ss. 90-120. http://tbbdergisi.barobirlik.org.tr/m2010-87-606.

- Avrupa Birliği ile İlişkiler Genel Müdürlüğü (2001). Avrupa Birliği Temel Haklar Şartı. Kasım 2001.

- Cate, F. H.; Cullen, P.; Mayer-Schönberger, V. (2014). Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines.

- Civelek, D. Y. (2011). Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Uzmanlık Tezi). T.C. Başbakanlık Devlet Planlama Teşkilatı, Ankara. https://www.sbb.gov.tr/wp-content/uploads/2022/08/Kisisel-Verilerin-Korunmasi-ve-Bir-Kurumsal-Yapilanma-Onerisi-Dilek-Yuksel-Civelek.pdf.

- Council of Europe (1981). Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg. https://rm.coe.int/16800ca434.

- Council of Europe (2018). Explanatory Report of Modernised Convention 108. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

- Court of Justice of the European Union (CJEU) (2010). Joined Cases C-92/09 and C-93/09. https://curia.europa.eu/juris/liste.jsf?num=C-92/09&language=en

- Court of Justice of the European Union (2014). Joined Cases C-141/12 and C-372/12, YS and Others. https://curia.europa.eu/juris/liste.jsf?num=C-141/12&language=en.

- Develioğlu, H. M. (2017). 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku. On İki Levha Yayıncılık, İstanbul.

- European Commission (2010). A Comprehensive Approach on Personal Data Protection in The European Union, COM (2010) 609. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF.

- European Union Agency For Fundamental Rights (FRA) vd. (2018). Handbook on European Data Protection Law, Luxembourg. https://www.echr.coe.int/documents/d/echr/handbook_data_protection_ENG.

- European Court of Human Rights (EHCR) (1989). Gaskin v. The United Kingdom, No: 10454/83. https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-72424&filename=GASKIN%20v.%20THE%20UNITED%20KINGDOM.pdf.

- European Data Protection Board (EDPB) (2022). Guidelines 01/2022 on Data Subject Rights – "Right of Access" version 1.0. https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.

- Göçmen Uyarer, S. (2019). 6698 Kişisel Verilerin Korunması Kanunu ve 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması. Yüksek Lisans Tezi, İstanbul: 2019. https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=FgmkGchPKo23qQqBeqzVZk2aH3QaYRV5OAHB6rSoDQjh3JBR0jk3kvnwYhxM_77y.

◊ Küzeci, E. (2021). Kişisel Verilerin Korunması. On İki Levha Yayınları, 4. Baskıdan Tıpkıbasım, İstanbul.

◊ Oğuz, H. (2013). Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum. Uyuşmazlık Mahkemesi Dergisi, Sayı: 3, 2013, ss. 1-38. https://dergipark.org.tr/tr/pub/mdergi/issue/16883/175778.

◊ Türkiye Büyük Millet Meclisi Adalet Komisyonu (2016). Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu. Yasama Yılı: 1, Dönem: 26. https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf.

KİŞİSEL VERİLERİN KORUNMASINDA RİSK TEMELLİ YAKLAŞIM

Uğur TOKMAKCI

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "Veri Güvenliği İhlallerinde Kapsamında Risk Değerlendirmesi ve Model Önerisi" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Risk, insana ilişkin hayatın doğasında bulunur, bu sebeple de riskten kaçınmak ya da en aza indirmek, riske ilişkin analiz veya değerlendirmeler yapmak gibi kararları vermek de insanın doğal yaşamında sürekli karşısına çıkan bir süreçtir. İnsan hayatının doğasında olmasının en büyük göstergesi, insanların bunu bilinçsizce ve refleks olarak yapmasıdır. Kurumlar için de riskin değerlendirilmesi ve azaltılması süreci kritik bir noktada yer almaktadır. Artık, risklerin etkin ve doğru biçimde yönetilmesi kurumların uzun vadede başarısını direkt olarak etkileyen faktörlerin başında gelmektedir.

Risk temelli yaklaşım da Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GVKT) yürürlüğe girmesiyle beraber kişisel verilerin korunmasında tartışılan kavramların içerisinde ciddi bir yer tutmaktadır. Bu kapsamda da anlaşılması ve irdelenmesi gereken bir konu olarak öne çıkmaktadır. Hem veri sorumluları/veri işleyenler tarafından hem de veri koruma otoriteleri tarafından iyi anlaşılması gereken bir kavram olarak bu konuda yazılmış çok fazla materyale ulaşılamamaktadır. Bu çalışma da kişisel verilerin korunması alanındaki risk kavramını ele

alıp buna ilişkin kavramları tanımlamaya çalışmakta ve risk temelli yaklaşımın anlaşılmasına katkıda bulunmaya çalışmaktadır.

RİSK ve RİSKE İLİŞKİN KAVRAMLAR

Risk

Günlük dilde risk genellikle, gelecekteki potansiyel tehlike fikriyle, yani "sadece bir dereceye kadar öngörülebilen nihai bir tehlike" ile ilişkilendirilir. İnsanların günlük hayatının içinde sürekli karşı karşıya olduğu risk kavramı belirli bir sektöre ya da bilimsel alana has bir olgu değildir. İnsanın varoluşundan beri yer alan risk, belirsizliği ve soyutluğu, her alanda kullanımının olması gibi sebeplerle açıklanması zor ya da her kullanıldığı alan için farklı anlamlar taşıyan, farklı şekilde tanımlanan bir kavramdır. Hemen hemen her sektörün kendisine ait bir risk tanımı yapılmış, riskin belirlenmesinde doğruluğu sağlamak amacıyla çeşitli risk analiz yöntemleri, istatistiksel ve matematiksel yöntemler kullanılmıştır. Campbell çalışmasında (Özdemir, 2019), kendi kendine hiçbir şeyin risk olamayacağını ve gerçekte riskin var olmadığından buna karşın her şeyin de risk olarak değerlendirilebileceğinden bahseder.

Bu sebeple riskin herkes için değişmesi riskin tanımının da analizinin de yapılmasını güçleştirmektedir. Kişisel verilerin korunması alanında da riskin tanımlanmasını zorlaştıran bazı etmenler vardır. Bunlardan birkaçı; kişisel veriler, verilere karşı tehditler ve bu tehditlere karşı alınan tedbirlerin arasındaki etkileşimdir. Örnek olarak müşterilerine daha iyi hizmet verebilmek için çalışan sayısının artması aynı zamanda çalışan hatasından kaynaklı kişisel veri ihlallerinin de artması riskini beraberinde getirir.

Bir diğer zorluk ise kişisel verilerin korunması alanının disiplinler arası bir noktada yer almasından ve teknolojiyle olan iç içeliğinden ötürü, çok çabuk gelişen, değişen teknolojiden etkilenmesinden kaynaklanmaktadır. Teknoloji sağladığı kolaylıkların yanında kişisel verilerin korunması alanı için aynı zamanda bir tehdit unsurudur. Bu sebeple risk analizinin unsurlarından biri olan tehdidin değişmesi neticesinde kişisel veriler için de riskin tanımı ve analizi zorlaşmaktadır.

Riske, kavramsal olarak ele alınmaya başladığı andan itibaren aynı şekilde yaklaşılmamaktadır. Literatürde "Geleneksel Yaklaşım" olarak adlandırılan yaklaşıma göre; kurum değerini korumak amacıyla risk olumsuz bir faktör olarak yer alır ve sübjektif yönüyle öne çıkar. "Yeni Yaklaşıma" göre ise risk bir firsat olarak ele alınır, ölçülebilir ve bir bütün olarak kurum çapında yönetilmesi gerekir.

Riskin alınma sebebi ise elde edilecek bir değerin olmasıdır. Veri sorumluları-kişisel verileri işleyerek bir risk alır. Bunun sonucunda ise veri sorumluları bir kazanç elde etme, maliyetten tasarruf etme, kamu görevini ifa etme gibi bir değer elde etmiş olur. Kişisel verilerin korunması alanında alınan risk öncesi tedbir alıp almama veri sorumlularının inisiyatifine bırakılmamıştır. Veri sorumluları hem riski alma yani kişisel verileri işleme aşamasından önce hem de sonra bazı yükümlülüklere tabi tutulmuştur. "Privacy by design" (Tasarımda Gizlilik), "Privacy by default" (Varsayılan Olarak Gizlilik) gibi ilkelerin yanı sıra Kişisel Veri Güvenliği Rehberi (Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), 2018))'nde de belirtildiği üzere; *"Kişisel verilerin güvenliğinin sağlanması için öncelikle veri sorumlusu tarafından işlenen tüm kişisel verilerin neler olduğunun, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınması gerekmektedir."*

Türk Dil Kurumu'nda zarara uğrama tehlikesi ("sozluk.gov.tr", t.y.) olarak tanımlanan risk, Bilgi Sistemleri Denetim ve Kontrol Derneği (ISACA)'nin Terimler Sözlüğüne (ISACA, 2018) göre bir olayın olasılığının ve sonuçlarının kombinasyonudur. Bilgi güvenliğinde ise risk; "varlık ya da varlık gruplarının zayıflıklarını kullanacak ve bu yolla organizasyona zarar verecek potansiyel durum" olarak tanımlanmaktadır.

Madde 29 Çalışma Grubu (WP 29) tarafından risk, "bir olayın ve sonuçlarının, ciddiyet ve olasılık açısından tahmin edilen bir senaryo" olarak tanımlanmıştır. Risk, olayların tahminine dayalı, ileriye dönük bir karar verme aracı olarak düşünülebilir. Riski tanımlarken yalnızca tehlike olarak ele almak eleştirilen bir durumdur. Risk, olabilecek veya olmayabilecek ve hem olumlu hem de olumsuz birçok sonucu olan olaydır. Bu nedenle ISO riskten bir olay olarak bahsederken Fransa Veri Koruma Otoritesi (CNIL) korkulan olay olarak söz eder (Gellert, 2020).

GVKT kapsamında riskin tam olarak tanımı yapılmamakla birlikte 24 üncü maddesinde riskin iki unsura dayandırıldığını anlayabiliriz. Bunlardan ilki gerçekleşme ihtimali, diğeri ise riskin gerçekleşmesi durumunda kişilerin hak ve özgürlükleri üzerinde doğuracağı etkinin ağırlığı. Bu durumda veri sorumluları için kişisel verilerin işlenmesinde riskin ölçümlenmesi için bu iki unsuru doğru bir şekilde belirleyebilmek sorumluluğu doğuyor. Bunların yanında, bir veri koruma riskinden bahsedilecekse, en genel anlamıyla veri koruma riski, bir kişisel veri işlenmesi faaliyetinin, işlenen bireyleri olumsuz etkileme (yani zarar verme) olasılığı olarak tanımlanabilir (Gellert, 2020).

Riske İlişkin Kavramlar

Riskin tanımlanmasında ve anlaşılmasında kullanılan çeşitli risk kavramları vardır. Bunlardan biri risk faktörüdür. Risk faktörleri riskin gerçekleşip gerçekleşmeyeceğini ve nasıl gerçekleşeceğini (olasılık) ve ayrıca riskin ciddiyetini belirler. Bunlara ayrıca tehditler de denilebilir. CNIL'e göre, bir riskin ortaya çıkmasını mümkün kılan şey bir tehdittir. Başka bir deyişle, riskin gerçekleşip gerçekleşmeyeceğini, ne oranda gerçekleşeceğini (olasılığı) ve ayrıca riskin ciddiyetini belirler (örneğin işlenen veri miktarı bir risk faktörüdür) (Gellert, 2020).

Risk ile ilgili bir başka kavram risk kaynağıdır. ISO'ya göre risk kaynağı, *"tek başına veya bir arada riske yol açma potansiyeline sahip olan unsurdur* (örneğin bilgisayar)". CNIL'e göre, risk kaynağı bazen tehdit olarak da adlandırılan risk faktörlerinin kaynağı olduğu için risklere yol açar (Gellert, 2020).

Riskin sonucunda bir sonuç ya da etki ortaya çıkar. Korkulan olaydan kaynaklanan etkiler olumsuz olduğunda zarar (yani temel hakların ihlali ve bunun sonucunda ortaya çıkan zararlar) olarak, olumlu olduklarında ise fayda olarak adlandırılabilirler (Gellert, 2020).

Veri koruma açısından üç risk faktöründen bahsedilebilir. Artan veri işleme kapasitelerinin bir sonucu olarak artan veri miktarı; veriler arasındaki bağlantının bir sonucu olarak verilerin artan kullanımı, verilere erişimin artması ve yeni bir uzman sınıfının yükselişi. Bu risk faktörleri doğrudan bir dizi riske yol açabilir. Bu da birtakım zararlara yol açabilir (Gellert, 2020).

İşlenen veri miktarının artması, iki nedenden dolayı risk faktörü olarak kabul edilebilir. Bir yandan, bilgisayarların hızlı ve verimli veri işleme kapasiteleri nedeniyle, kuruluşlar teknik olarak mümkün olduğu kadar çok veriyi işlemeye ve kaynaklarını yalnızca sistemin verimliliğine adamaya teşvik edilir, böylece artan teknoloji maliyetleri nedeniyle oluşan bozulan maliyetleri dengeler. Öte yandan, elektronik dosyalar manuel olanlardan daha az esnektir ve bu nedenle hatalara ve yanlış sınıflandırmalara daha yatkındır. Bu tür hataların ve dikkatsizliklerin bir sonucu olarak birçok veri işleme hatalı hale gelmektedir. Yanlışlıktan kaynaklanan tipik zararlar arasında hatalı faturalar, haksız ihtar mektupları vb. rahatsızlıklar ortaya çıkabilmektedir. Bunlar da nihayetinde güven eksikliğine yol açabilmektedir. Güven kaybı genel olarak insanların refahını etkilediği için ilk bakışta göründüğü kadar zararsız değildir ancak işyeri gibi ortamlarda gizli etkileri de vardır. Bu tür rahatsızlıkların en önemli sonucu ise toplumsal huzursuzluktur (Gellert, 2020).

İkinci risk faktörü olarak işlemenin özelliklerinden olan verilere erişimin ve verilerin kullanımının artmasıdır. Artan işleme kapasitelerinin etkisiyle fazla sayıda bireyi içeren, önemli veri tabanlarının oluşturulması mümkün hale gelmiştir. Yine aynı sebeple, veri tabanlarının birbirine bağlanması da mümkün hale gelmiştir. Bu durum da çok sayıda kişinin artık bilgiye erişebileceği ve daha sonra onu kendi amaçları için kullanabileceği anlamına gelmektedir. Buna karşılık verileri kimin kullandığı ve ne işe yaradığı konusunda çok az bilgi ve kontrol vardır (Gellert, 2020).

Artan veri tabanlarından kaynaklı Dragnet Etkisi *("bir popülasyondaki belirli özelliklere sahip birkaç üyeyi keşfetmek için o popülasyonun tüm üyelerinin otomatik olarak taranması"*) ciddi zararlara yol açmaktadır. Dragnet Etkisiyle masum vatandaşlar masumiyetlerini kanıtlama yükünü taşımak zorunda kalacakları bir konuma getirilmektedir. Gözetim yöntemlerinin giderek daha fazla kullanılması, herkesin bir şüpheli olduğu ve dolayısıyla keyfi uygulamalara kapı açan bir etkiye yol açtığı savunulmaktadır (Gellert, 2020). Veri tabanlarının birbirine bağlanması sonucu da kişisel veriler üzerinde kontrolün kaybı anlamına gelmektedir. Kontrol kaybı da ilgili kişilerin verilerine erişememe ve bunları düzeltememe ile ilgili başka zararlara yol açabilir (Gellert, 2020).

Son risk faktörü veri işleme türü ile ilgilidir. Büyük kurum ve kuruluşların bilgisayarların artan veri işleme yeteneklerini temel alan davranışlarıdır. Bu kayıtlar istatistiksel amaçlarla az ya da çok risk altında olan nüfus profillerinin oluşturulması için kullanılır. Sosyal kontrol riski olarak adlandırılan riskten doğan zararlar; insanların bireyselliklerinden ve anlamlı bir varoluşlarından sıyrıldıklarını hissetmeleri, insanlıktan çıkmış ve yabancılaşmış hissetmek gibi duygusal, psikolojik ve ahlaki zararlara maruz kalmalarıdır (Gellert, 2020). Risk tanımlarına bakıldığında riskin üç unsurunun bulunduğu göze çarpmaktadır: Varlık, açıklık (zafiyet) ve tehdit. Dolayısıyla riskin tanımlanmasına ve risk analizine yer verirken bu unsurların da tanımlanması gerekir.

- Varlık; insanlar, bilgi, altyapı, finans ve itibar da dahil olmak üzere, korunmaya değer somut ya da maddi olmayan değer taşıyan bir şey olarak ifade edilebilir (ISACA, 2018). Varlıklar, Bilgi Güvenliği kapsamında genel olarak, donanım, yazılım, belgeler gibi araçlarla tanımlanır. Ancak kişisel verilerin korunması alanında yapılacak risk analizinde varlıkların kapsamı biraz daha daralarak kişisel verileri ifade edecektir. Varlıkların doğru şekilde belirlenebilmesi risk analizi için önemli bir yer tutar. Bir varlığa karşı, zararla sonuçlanabilecek şekilde hareket edebilecek herhangi bir şey (ör., nesne, madde, insan) tehdit olarak adlandırılır (ISACA, 2018). Tehditler pek çok sınıflandır-

ma çeşidi olmakla beraber, insan/insan dışı faktörler, ağ kaynaklı, çevresel tehditler, iç-dış tehditler şeklinde sınıflandırmalara tabi tutulmuştur.

- Zafiyetler/Açıklıklar ise sistemi, tehdit olaylarından kaynaklanan olumsuz tehditlere maruz bırakabilecek bir sürece ait tasarım, uygulama, işletme veya iç kontrolündeki bir zayıflık olarak tanımlanmaktadır (ISACA, 2018). Yazılımdan, donanımdan, ağdan, personelden kaynaklı zafiyetler olabilir.

- Tehditler, zafiyetler ve varlıklar arasındaki ilişki risk değerlendirmesi yaparken riskin anlaşılması ve olasılıkların büyük çapta değerlendirebilmesini sağlama konusunda önemlidir. Örneğin, bir kurumla iş ilişkisi sona ermiş bir çalışanın kurumun sistemlerine girmeye devam etmesi bir açıklık olarak değerlendirilebilir. Bu açıklıkla birlikte tehdit işten ayrılmış eski çalışan olur ve kurumun sistemine ulaşıp kişisel verilere erişme ve bu verileri kullanma tehdit eylemi şeklinde kendisini gösterebilir. Bunların sonucunda da eski çalışanın kişisel verilerin bütünlüğünü bozabilmesi ya da kişisel verilerin dışarıya aktarılması şeklinde veri ihlali ortaya çıkabilir. Veri ihlali sonucunda ilgili kişilerin veri koruma hukuku bağlamında bazı hak ve özgürlükleri zarar görebilecektir.

GVKT'nin 75 ve 76'ncı gerekçeleri, genel olarak risk değerlendirilirken ilgili kişilerin haklarına ve özgürlüklerine yönelik riskin hem olasılığının hem de ciddiyetinin dikkate alınması gerektiğini önermektedir. Ayrıca riskin objektif bir değerlendirme temelinde değerlendirmesi gerektiğini belirtmektedir.

WP29'a göre, bir ihlalin sonucu olarak bireylere yönelik riski değerlendirirken veri sorumlusu; potansiyel etkinin ciddiyeti ve bunun meydana gelme olasılığı da dahil olmak üzere ihlalin özel koşullarını göz önünde bulundurmalıdır. WP29, değerlendirme yapılırken;

- İhlalin türü,
- Kişisel verilerin niteliği, hassasiyeti ve hacmi,
- Kişilerin tanımlanması kolaylığı,
- Bireyler için sonuçların ciddiyeti,
- Bireyin kendine has özellikleri,
- Veri sorumlusunun özel nitelikleri,
- Etkilenen kişi sayısı,
- Genel noktalar

kriterlerinin dikkate alınması gerektiğini ifade eder.

RİSK TEMELLİ YAKLAŞIM

Risk temelli yaklaşım, 2010'ların başından itibaren popüler olan ve kişisel verilerin korunmasında daha iyi bir yol sunmaya çalışan bir eğilimi ifade eder (Gellert, 2020). Risk yönetimi hemen hemen her konuda ve ülkede kullanılan bir kavram olmakla birlikte, risk temelli yaklaşım da yeni bir kavram değildir. GVKT'den önce de izlerini bulabileceğimiz risk temelli yaklaşım, GVKT ile birlikte tartışmalara yol açması sebebiyle görünür hale gelmiştir. Risk temelli yaklaşımın ilk izlerini ise RAND Corporation tarafından İngiltere Veri Koruma Otoritesi (Information Commissioner's Office/Bilgi Komiserliği Ofisi – ICO) adına 2009 yılında ortaya konan raporda bulmak mümkündür.

Risk temelli yaklaşım, veri koruma hukukunda ana hat tartışmalardan biri olan, korumanın hak temelli mi yoksa risk/zarar temelli mi olacağı tartışmasının karşı karşıya geldiği kavramlardan biri olmuştur. Genel olarak GVKT'nin bu tartışmayı hak temelli anlayıştan risk temelli anlayışa doğru kaydırdığı söylenebilir. GVKT'nin kabul edilme sürecinde risk temelli yaklaşıma karşı temel tartışma, bu kavramın veri koruma hukukunun hükümlerini gevşettiği, veri sorumlularının çıkarlarına yönelik olduğu, AB'nin temel haklara dayalı veri koruma doğasına aykırı olan "ABD" eksenli zarar temelli bir korumaya yol açacağı ekseninde gelişmiştir (Gellert, 2020).

GVKT'nin hak temelli yaklaşım ekseninden risk temelli yaklaşıma doğru kaymasının çeşitli anlamları vardır. Hak temelli yaklaşımda, ikili bir bakış açısı söz konusudur. Bir veri işleme ya yasaldır ya da yasal değildir; veri korumanın temel ilkelerine ya uyar ya da uymaz. Risk temelli yaklaşımda ise temel problem ne kadar risk alınabileceğinin belirlenmesi meselesidir.

İkinci olarak, hak temelli yaklaşım eşitlikçi bir bakış açısı güderken risk temelli yaklaşım adil bir bakış açısı ortaya koymaktadır. İlki, veri işlemenin riski veya zararından bağımsız olarak herkese aynı kuralları uygular ve tüm bireyler için asgari ve müzakere edilemez bir koruma düzeyi vadeder.

Risk temelli yaklaşım ise öncelikle tasarlanan veri işleme faaliyetinin sunduğu riskleri değerlendirme ve bu hususta işlem yapılıp yapılmayacağına karar verme yönünde bir anlayış sergiler. Yani söz konusu risklerin yönetimi söz konusudur. Bu anlamda söz konusu riskin düzeyine, zarar ve yarar hesaplamalarına dayandırılması açısından hak temelli yaklaşımla zıttır. Bu sebeple risk temelli yaklaşımın eşit olmayan bir koruma sağladığı söylenebilir (Gellert, 2020). Ancak eşit olmayan bir koruma sağlaması, bu korumanın adil olmadığı anlamına gelmemelidir.

Risk temelli yaklaşıma geçişi, kişisel verilerin korunması alanında teoriden ziyade pratiğe daha çok odaklanılması olarak görebiliriz. Bu sayede de veri koruma hukukunun ilkeleri ve kuralları görece olarak daha etkin bir şekilde uygulanmaya çalışılmaktadır. Aynı zamanda bu yaklaşım veri sorumluları tarafından yasal gerekliliklerin kalibrasyonu için bir referans noktası işlevi görür (Quelle, 2017).

Risk temelli yaklaşım, veri sorumluları arasında veri koruma kültürünün içselleştirilmesini sağlayabilir. Ülkemizdeki gibi kişisel verilerin korunması alanının yeni yeni geliştiği ülkeler açısından özellikle faydalı olabilir. Ayrıca veri sorumluları ve veri işleyenler için veri koruma hukukuna uyumluluk maliyetini azaltabileceği de düşünülebilir. Risk temelli yaklaşım, veri sorumlularının amaçları doğrultusunda mevcut durum analizi yaparak gerekli veri güvenliği tedbirlerini almaları hususunda yol gösterebilmektedir. Bunun yanında, risk temelli yaklaşımın esnek doğası gereği, gelişen teknolojilere ayak uydurmaya da yardımcı olabilir.

Veri koruma anlayışının risk temelli bir yaklaşıma doğru evirilmesinin getirmiş olduğu bazı soru işaretleri de mevcuttur. Bunlardan biri, risk temelli anlayışın, riskin doğru anlaşılabildiği ve tanımlanabildiği ölçüde kişisel verilerin korunmasını etkin olarak sağlayacak olmasıdır. Bundan belki de daha önemli bir soru işareti de veri koruma alanında veri sorumlularına etkin ve önemli bir görevin bu anlayışla verilmiş olmasıdır. Veri sorumlularının dürüstlükten uzak bir risk temelli anlayışı benimsemesi, hedef alınan noktaya ulaşmayı zorlaştıracaktır.

GVKT'deki risk kavramına benzer şekilde, risk temelli yaklaşım da anlaşılması zor ve tanımlanmayan bir kavram olarak öne çıkar. Kavramın belirsizliği hususunda GVKT'nin 35 inci maddesi örnek olarak gösterilebilir. GVKT Madde 35'te;

"(...) bir işleme türünün gerçek kişilerin hak ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, veri sorumlusu işleme faaliyetinden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunması üzerindeki etkisine ilişkin bir değerlendirme yapar."

hükmüne yer verilmiştir. Söz konusu maddede ilk olarak gerçek kişilerin hak ve özgürleri üzerinde yüksek bir risk oluşmasından bahsetmektedir. Yani gerçek kişilerin hak ve özgürlükleri üzerindeki etkinin bir değerlendirmesi yapılsın ki böyle bir yüksek riskin muhtemel olup olmadığına karar verilebilsin. İkinci olarak ise kişisel verilerin korunması üzerindeki etkiye ilişkin bir değerlendirmeden bahsetmektedir. Değerlendirilmesi gerekenin, gerçek kişilerin hak ve özgürlüklerine yönelik olası yüksek risk mi yoksa kişisel verilerin korunması üzerindeki etkisi mi olduğuna ilişkin bir çelişki gözükmektedir. Benzer şekilde, veri koruma ilkelerine

uymanın ve gerçek kişilerin hak ve özgürlüklerine yönelik riskleri azaltmanın iki farklı şey olduğu öne sürülmüştür (Gellert, 2017). WP29 ile birlikte değerlendirildiğinde 35 inci maddedeki hükümden kastedilenin "ilgili kişilerin üzerindeki (hakları, özgürlükleri ve çıkarları) olası olumsuz etki" ile ilgili olduğu söylenebilir.

Raphaël Gellert tarafından öne sürülen hipotez, bu çelişkiyi çözümlemenin tek yolunun, GVKT'nin kalbinde yer alan risk kavramının, bir uyum riski olarak anlaşılması gerektiğidir (Gellert, 2017). Uyum riskiyle anlatılmak istenen, bir kişisel veri işlemenin, ilgili kişilerin temel hak ve özgürlüklerini ihlal etme olasılığını ve ihlal ettiği takdirde ciddiyetini belirlemek yerine, GVKT'yi ihlal etme olasılığını ve ciddiyetini belirlemek gerektiğidir. Uyum riski, planlanan kişisel veri işleme faaliyetinin ne kadar zararlı olduğunu belirlemek yerine, veri işlemenin veri koruma mevzuatında yer alan zorunlu güvenlik önlemlerini ne kadar ihlal edebileceğine odaklanır.

Risk temelli yaklaşımın ana hedeflerinden biri, kişisel verilerin korunması alanında ortaya konmuş yasal çerçeveye daha iyi uyum sağlanmasına ve daha iyi uygulanmasına sebep olmaktır. Uyum riski kavramı, GVKT kapsamındaki risk temelli yaklaşım için bir araçtır. Yasal çerçeveye uyum ne kadar düşükse ilgili kişilerin temel haklarının ihlal edilme olasılığı da o kadar yüksektir. Örneğin, kişisel verilerin güncel bir şekilde tutulmaması ilgili kişinin temel haklarının ihlal edilmesine yol açabilir. Dolayısıyla, GVKT'nin 35 inci maddesinin (1) numaralı fıkrası şu şekilde yorumlanabilir: İlgili kişilerin hak ve özgürlüklerinin ihlal edilme olasılığının yüksek olması, yüksek riske ve çok düşük bir uyum düzeyine işaret eder (Gellert, 2020).

Risk temelli yaklaşım, yalnızca kişisel veri ihlali durumlarında değil kişisel verileri korumanın tüm hükümlerine karşı bir savunma sağlayabilir. Benzer şekilde, rıza ve ilgili kişi hakları hükümlerine de uygulanabileceği gibi bu konularda da mevzuata uyumun sağlanmasında bir araç olabilir (Maldoff, 2016).

Risk temeli bir yaklaşımın benimsenmesi halinde, kişilerin kişisel verileriyle ilgili haklarının zayıflaması söz konusu değildir. Söz konusu işleme nispeten düşük riskli olsa bile, bu haklar aynı derecede güçlü olmalıdır. Bunun yerine riske dayalı yasal yükümlülüklerin ölçeklenebilirliği, uyum mekanizmalarını ele alır. Bu, işlemesi nispeten düşük riskli olan bir veri sorumlusunun, işlemesi yüksek riskli bir veri sorumlusu kadar yasal yükümlülüklerine uymak zorunda kalmayacağı anlamına gelir (Madde 29 Çalışma Grubu WP 218, 2014).

İlgili kişiler, kuruluşun büyüklüğüne veya işlediği veri miktarına bakılmaksızın

aynı koruma düzeyine sahip olmalıdır. WP29, ölçeklenebilir bir şekilde yapılabilmesine rağmen, tüm veri sorumlularınım yasalara uygun hareket etmesi gerektiğini düşünüyor (Madde 29 Çalışma Grubu WP 218, 2014).

Son olarak; WP29 tarafından "Veri Koruma Yasal Çerçevelerinde Risk Temelli Bir Yaklaşımın Rolüne İlişkin Açıklama" isimli rehberinde 13 tane ilke belirlemiştir. Bunlardan bazıları şunlardır (Madde 29 Çalışma Grubu WP 218, 2014):

- *"AB Hukuku tarafından ilgili kişiye tanınan haklara, ilgili veri işleme yoluyla maruz kalınan risklerin düzeyine bakılmaksızın saygı gösterilmelidir. Veri sorumluları için geçerli olan temel ilkeler de (meşruiyet, veri minimizasyonu, amaç sınırlaması, şeffaflık vb.), işleme ve ilgili kişiler için riskler ne olursa olsun aynı kalmalıdır.*

- *Söz konusu işlemenin oluşturduğu riske bağlı olarak farklı düzeylerde hesap verebilirlik yükümlülükleri olabilir. Bununla birlikte, veri sorumluları, işlemenin niteliği, kapsamı, bağlamı, amaçları ve ilgili kişilere yönelik riskler ne olursa olsun, herhangi bir veri işlemeyle ilgili uyumun gösterilmesi dahil olmak üzere veri koruma yükümlülüklerine uyumdan her zaman sorumlu olmalıdır.*

- *Veri sorumlularının yükümlülüklerinin hesap verebilirlik araçları ve önlemleri (etki değerlendirmesi, tasarım yoluyla veri koruması, veri ihlal bildirimi vb.) yoluyla uygulanması, işleme türüne ve ilgili kişiler için mahremiyet risklerine göre değişebilir ve değiştirilmelidir. Her durumda her hesap verebilirlik yükümlülüğünün gerekli olmadığı kabul edilmelidir.*

- *İşleme faaliyetlerinin belgelenme şekli, işlemenin oluşturduğu riske göre farklılık gösterebilir. Yine de tüm veri sorumluları, şeffaflığı ve hesap verebilirliği artırmak için işleme faaliyetlerini en azından bir dereceye kadar belgelemelidir.*

- *İlgili kişinin hakları, özgürlükleri ve çıkarları üzerinde olası olumsuz etkilere ilişkin riskler, kişisel verilerin niteliği, etkilenen kişi kategorisi, etkilenen kişi sayısı ve işlemenin amacı; ilgili kişilerin hak ve özgürlükleri üzerindeki etkilerin ciddiyeti ve olasılığı, kişinin mahremiyetine yönelik risklerin değerlendirilmesinde dikkate alınması gereken unsurları oluşturur.*

- *Risk temelli yaklaşım, belirli riskler tanımlandığında ek önlemler gerektirir ve bir etki değerlendirmesi ile yüksek riskli işleme tespit edildiğinde veri koruma otoritesine danışılmalıdır.*

- *Aynı kişiyle ilgili verilerin, kimliğini bilmeye gerek kalmadan toplanmasını sağlamak için kimlikleri gizlemek için takma ad kullanma tekniklerinin kullanılmasının, bireylere yönelik risklerin azaltılmasına yardımcı olabileceğini de kabul etmiştir.*

- *Risk temelli yaklaşım, yalnızca hasara odaklanan ve kişi üzerindeki etkiden çok geniş bir ölçekte genel bir toplumsal etki açısından değerlendirilen, gerçek olumsuz etkilerin yanı sıra her potansiyeli de dikkate alması gereken dar bir "zarar temelli yaklaşımın" ötesine geçer.*

- *Veri koruma otoritelerinin risk temelli yaklaşıma ilişkin rolü aşağıdakilerden oluşacaktır:*

» *Özü itibariyle belirli riskler sunduğu düşünülebilecek işleme listesinin güncellenmesi,*
» *Etki değerlendirmeleri ve diğer hesap verebilirlik araçları hakkında yönergeler geliştirmek.*
» *Veri sorumluları tarafından gerçekleştirilen diğer önlemlerin yanı sıra zorlu risk analizi, etki değerlendirmeleri gerektirebilecek veri sorumlularının uyumsuzluğu durumunda icra prosedürlerinin yürütülmesi,*
» *En büyük risk altındaki alanlarda uyum eylemi ve uygulama faaliyetini hedeflemek."*

HESAP VEREBİLİRLİK İLKESİ

GDPR'da risk temelli yaklaşım kavramının direkt olarak yer almadığı göz önüne alındığında, bu kavramın hesap verebilirlik ilkesinde ve tasarım gereği veri koruma ilkesinde somutlaştığı iddia edilebilir (Gellert, 2020).

GDPR'ın yaklaşımına göre, veri sorumlusunun veri işleme faaliyetindeki risk seviyesi arttıkça, hesap verebilirliğe ilişkin yükümlülükleri de ağırlaşmaktadır. Bu sebeple hesap verebilirlik ilkesinin ne olduğunun da bilinmesi gereklidir. WP29'un hesap verebilirlik ilkesine ilişkin önerisi, GDPR'da karşılığını bulmuştur. Hesap verebilirlik ilkesi, Avrupa Birliği'nde kişisel verilerin korunması konusunun direktif ("directive") ile düzenleme yönteminden tüzük ("regulation") ile düzenleme yöntemine geçilmiş olmasıyla yatay düzeyde doğrudan uygulanan yeni veri koruma hukuku düzeninin üzerine kurulduğu ilkedir (Kaya, 2020). GDPR'ın 5 inci maddesinin 2 numaralı fikrasında hesap verilebilirlik (accountability) şeklinde düzenlenen ilke, kişisel verilerin korunması alanında yükümlülüklerinin yerine getirilip getirilmediği konusunda ispat yükünü veri sorumlusuna yüklemektedir

(Dülger, 2019). Hesap verebilirlik ilkesine GDPR'da yalnızca iki kez geçmesine rağmen bu derecede bir önem atfedilmektedir. Çünkü bu ilke ile, kişisel verilerin korunması alanında hukuka aykırılıkla mücadele veri sorumlusunun cephesine taşınmıştır. Avrupa Birliği hukukunda kişisel verilerin korunması alanındaki bu temel paradigma değişikliğiyle, devlet tarafından denetlenme unsuru arka plana geçerek, sorumluluk veri sorumlusu ve/veya veri işleyene yüklenmektedir (Çekin, 2018).

WP29'a göre, kişisel veriler alanında hesap verebilirliği gerekli kılan üç temel gelişme vardır:

"Veri tufanı etkisi olarak nitelendirilecek şekilde, var olan kişisel verilerin işlenmesinin ve transferinin hızlıca artması, Sürekli artan kişisel bilgilerin sosyal, politik ve ekonomik bağlamda değerinin artması, Kişisel bilgilerin ihlallerinin artmasının hem kamuda hem özel sektördeki veri sorumluları için önemli olumsuz etkilerinin olması." (Madde 29 Çalışma Grubu, WP 173)

Veri koruma hukukunda veri sorumlularına ve/veya veri işleyenlere çeşitli yükümlülükler getirilmekte ve bu yükümlülüklere uymaları beklenmektedir. Bunlar veri güvenliğine ilişkin yükümlülükler olabildiği gibi ilgili kişilerin haklarını kullanması yönünde de olabilir. Hesap verebilirlik ilkesi, veri sorumlusunun bu yükümlülüklerini yerine getirmesi ve aynı zamanda ne oranda ve şekilde yerine getirildiğinin, talep üzerine denetleyici makamlara bunu göstermeye yarar. Bu bağlamda WP29, sorumluluk ile hesap verebilirliğin aynı madalyonun iki yüzü ve iyi yönetişimin temel unsurları olduğunu belirtmiştir (Madde 29 Çalışma Grubu, WP 173).

GDPR'ın 5 nci maddesinin (2) numaralı fıkrasında hesap verebilirlik ilkesi düzenlenmiştir. Hesap verebilirlik ilkesi "Veri Sorumlusunun Sorumluluğu" başlığını taşıyan 24 üncü maddede daha da geliştirilmiştir. Bu ise, hesap verebilirlik ve sorumluluk ilkesinin aynı madalyonun iki yüzü olduğu konusunda görüşleri destekler niteliktedir (Gellert, 2020).

Hesap verebilirlik ilkesine göre, veri sorumluları üst yönetimden onay alması gereken gizlilik politikalarını benimsemeli ve bu politikalara etki edecek mekanizmaları devreye sokmalıdır. Bunlar veri koruma etki değerlendirmeleri veya personel eğitimi ve öğretimi gibi karar verme araçlarını içerir. Bu tür mekanizmalar, veri toplayan veya veri işleyen tüm iş süreçlerine yerleştirilmelidir (Gellert, 2020).

VERİ KORUMA ETKİ DEĞERLENDİRMESİ

Veri Koruma Etki Değerlendirmesi (Data Privacy Impact Assesment – DPIA), işlemeyi tanımlamak, gerekliliğini ve orantılılığını değerlendirmek ve kişisel verilerin işlenmesinden kaynaklanan gerçek kişilerin hak ve özgürlüklerine yönelik riskleri, bunları değerlendirerek ve bunlara yönelik önlemleri belirleyerek yönetmeye yardımcı olmak için tasarlanmış bir süreçtir (Madde 29 Çalışma Grubu, WP248). DPIA, veri sorumlularının yalnızca GDPR gerekliliklerine uymalarına değil, aynı zamanda GDPR ile uyumu sağlamak için uygun önlemlerin alındığını göstermelerine yardımcı olduğundan, hesap verebilirlik için en önemli araçlardan bir tanesidir. Başka bir deyişle, DPIA, uyumluluğu oluşturmaya ve göstermeye yönelik bir süreçtir. Tek bir değerlendirmede benzeri yüksek riskler taşıyan bir dizi benzer işleme faaliyetinin ele alınması mümkündür (Kaya, 2020).

Veri koruma etki değerlendirmesi/analizi veya farklı ifadeyle mahremiyet etki analizi, "kişisel veri işlemeyi içeren bir projenin, politikanın, programın, hizmetin, ürünün veya başka bir girişimin mahremiyet üzerindeki etkilerinin değerlendirildiği ve diğer paydaşlarla da danışarak, olumsuz etkileri önlemek veya asgariye indirmek için gerekli telafi edici eylemlerin alındığı bir süreçtir" (Zurawski, Wright ve de Hert, 2012).

Literatürde veri koruma etki değerlendirmesi, bir erken uyarı mekanizmasına (Kaya, 2020) ve testi kırılmadan testinin kırılma simülasyonunu hazırlamaya benzetilmektedir (Kaya, 2020). DPIA, veri koruma düzeyindeki ilk risk yönetimi aracı olarak kabul edilir. DPIA'nın izi 1970'lere kadar uzanabilse de önemli bir veri koruma mekanizması olarak ortaya çıkışları, esas olarak Anglo-Sakson ülkelerinde 1990'ların ortalarına kadar uzanmaktadır (Gellert, 2020).

GDPR'ın öngördüğü risk temelli yaklaşıma uygun olarak, bütün veri işleme faaliyetleri için DPIA yapılması zorunlu değildir. DPIA, yalnızca işlemenin *"gerçek kişilerin hak ve özgürlüklerine yönelik yüksek bir riskle sonuçlanması muhtemel"* olduğunda gereklidir. Bununla birlikte, DPIA'yı gerçekleştirme yükümlülüğünü gerektiren koşulların yerine gelmemiş olması, veri sorumlularının ilgili kişilerin haklarına ve özgürlüklerine yönelik riskleri uygun şekilde yönetmek için alınan önlemleri uygulamaya yönelik genel yükümlülüğünü azaltmaz. Uygulamada bu durum, bir işleme türünün ne zaman *"gerçek kişilerin hak ve özgürlükleri için yüksek bir riske yol açması muhtemel"* olduğunu belirlemek için veri sorumlularının işleme faaliyetleri tarafından yaratılan riskleri sürekli olarak değerlendirmesi gerektiği anlamına gelir (Madde 29 Çalışma Grubu WP259, 2018).

DPIA'nın yapılması yüksek riskle sonuçlanması muhtemel işlemeler için zorunlu tutulmuştur. GDPR 35 inci maddenin (3) numaralı fikrasıyla yüksek riskle sonuçlanması muhtemel işleme faaliyetlerine örnekler sunulmuştur. Bunlar;

- *"Profil çıkarma dahil otomatik işlemeye dayanan ve gerçek kişiyle ilgili hukuki sonuçlar doğuran veya gerçek kişiyi benzer şekilde önemli ölçüde etkileyen kararların dayandığı, gerçek kişilerle ilgili kişisel yönlerin sistematik ve kapsamlı bir değerlendirmesi,*
- *Özel nitelikli kişisel verilerin büyük ölçekte işlenmesi ve*
- *Kamuya açık bir alanın büyük ölçekte sistematik olarak izlenmesidir."*

Bu maddenin başındaki özellikle kelimesi, listenin kapsamlı bir liste olmadığını, bu listede yer almayan ancak yine de benzer şekilde yüksek riskler oluşturan yüksek riskli işleme operasyonları olabileceğini bize ifade etmektedir. Bu işleme operasyonları da DPIA'ya tabi olmalıdır. Bu nedenle WP29 tarafından yüksek riskli bir işlemle sonuçlanması muhtemel işleme operasyonlarına ilişkin dokuz kriter geliştirilmiştir. Veri sorumluları, bu kriterlerin iki tanesini karşılayan bir işleme için DPIA'nın gerekli olacağını düşünebilir. Genel olarak WP29, işleme tarafından ne kadar fazla kriter karşılanırsa, ilgili kişilerin hakları ve özgürlükleri için yüksek risk oluşturma olasılığının o kadar yüksek olduğunu ve bu nedenle veri sorumlusunun öngördüğü önlemlerden bağımsız olarak bir DPIA gerçekleştirmeyi benimsemesi gerektiğini düşünmektedir.

Bir DPIA'nın gerekli olup olmadığının net olmadığı durumlarda, WP29, DPIA'nın gerçekleştirilmesini tavsiye etmektedir. Çünkü DPIA, veri sorumlularının veri koruma yasasına uymasına yardımcı olmak için yararlı bir araçtır (Madde 29 Çalışma Grubu, WP259).
Bunların yanında DPIA işlemeden önce gerçekleştirilmelidir ve veri sorumlusu DPIA'nın yürütülmesini sağlamaktan sorumludur (Madde 29 Çalışma Grubu, WP259). GDPR, DPIA'da yer alması gereken asgari unsurları 35 inci maddenin (7) numaralı fikrasında belirlemiştir (Madde 29 Çalışma Grubu, WP259):

- *"Öngörülen işleme operasyonlarının tanımı ve işlemenin amaçları,*
- *İşlemenin gerekliliği ve orantılılığına ilişkin bir değerlendirme,*
- *İlgili kişilerin haklarına ve özgürlüklerine yönelik risklerin değerlendirilmesi,*
- *Kişisel verilerin korunmasının sağlanması ve GDPR'a uygun hareket edildiğinin gösterilmesiyle ilgili güvenceler, güvenlik tedbirleri ve mekanizmalar da dahil olmak üzere risklerin ele alınması hususunda öngörülen tedbirler."*

GVKT'nin 90. Gerekçesi, iyi tanımlanmış risk yönetimi bileşenleriyle örtüşen

DPIA'nın bir dizi bileşenini özetlemektedir. Risk yönetimi açısından, bir DPIA, aşağıdaki süreçleri kullanarak gerçek kişilerin hak ve özgürlüklerine yönelik riskleri yönetmeyi amaçlar (Madde 29 Çalışma Grubu WP259, 2018):

- *"Bağlamın oluşturulması: "işlemenin doğası, kapsamı, bağlamı ve amaçlar ile riskin kaynakları dikkate alınarak"*
- *Risklerin değerlendirilmesi: "yüksek riskin özel olasılığını ve ciddiyetini değerlendirerek"*
- *Riskleri tedavi etmek: "riski azaltmak" ve "kişisel verilerin korunmasını sağlamak" ve "GDPR'a uygunluğunu göstermek".*

Veri koruma etki değerlendirmesi, veri güvenliğine yönelik riskleri belirlemek ve olası tehditlere engel olmak amacıyla önleyici yolların belirlenmesi sürecidir. GVKT'nin35 inci madde kapsamında öngörülen veri koruma etki değerlendirmesi; veri işlemenin çeşitli riskler arz ettiği hallerde ayrıca verinin mahremiyeti açısından kontrol edilmesine yönelik bir denetim mekanizması vazifesi görmektedir. Veri koruma etki değerlendirmesi yönteminde, ilk değerlendirmenin veri sorumlusu tarafından gerçekleştirilmesi, değerlendirmenin sonucuna göre gerekirse denetim makamına başvurulması aranmakta, veri sorumlularının üzerindeki yük azaltılmaktadır (Develioğlu, 2017).

DPIA, genel olarak potansiyel bir ihlalin meydana gelme olasılığına ve ilgili kişilerin bundan kaynaklanabilecek zararına bakar; başka bir deyişle, varsayımsal bir olayın değerlendirilmesidir. Fiili bir ihlalde olay zaten meydana gelmiştir ve bu nedenle odak tamamen ihlalin bireyler üzerindeki etkisinin ortaya çıkan riski ile ilgilidir (Madde 29 Çalışma Grubu, WP250, 2018).

TASARIM YOLUYLA VERİ KORUMA – VARSAYILAN OLARAK VERİ KORUMA

Veri korumaya yönelik risk temelli yaklaşımın, hesap verebilirlik ve tasarım yoluyla veri koruma ilkeleri aracılığıyla somutlaştığından bahsedilmişti. Tasarım yoluyla ve varsayılan olarak veri koruma da hesap verebilirlik ilkesine yardımcı olan bir ilkedir. Özel ve olağan veri koruma olarak da literatürde geçmektedir.

Tasarım ve varsayılan olarak veri koruma ilkelerine GVKT'nin 25 inci maddesinde yer verilmiştir. Risk temelli yaklaşım çerçevesinde, hizmetlerin sunulurken bu hizmetlerin süreçlerinde veri mahremiyetinin korunması, hizmetin tüm aşamalarında veri mahremiyetin yer bulması gerektiğini düzenleyen ilkedir. Bir hizmet sunulmadan, erken bir aşamada hizmetlerin tasarımına veri mahremiyeti yerleştirilecek ve böylelikle kişisel veri mahremiyeti için daha etkin ve daha

uygun maliyetli bir koruma sağlanacaktır. Tasarım yoluyla veri koruma, nihai olarak herhangi bir sistemin, hizmetin, ürünün veya sürecin tasarım aşamasında ve daha sonra yaşam döngüsü boyunca gizlilik ve veri koruma kurallarını dikkate almanızı sağlayan bir yaklaşımdır (Data protection by design and default, t.y.). Yani "önce gizlilik" yaklaşımının belirlenmesi esastır. Bu doğrultuda bir ürünün ve hizmetin kullanımını sağlamak için kullanıcı tarafından verilen kişisel veriler yalnızca ürünü veya hizmeti sağlamak için gereken süre boyunca saklanmalıdır. Ayrıca, veri işlenmeye başlamadan önce hangi verilerin ne şekilde işleneceğini konusunda kişiler uygun şekilde bilgilendirilmeli ve yalnızca ürün veya hizmetin amacıyla bağlantılı olarak veri minimizasyonu ilkesi doğrultusunda yalnızca amaç için gerekli kişisel veriler işlenmelidir.

Varsayılan olarak gizlilik ya da başka bir deyişle olağan olarak veri koruma ise bir hizmetin ayarlarının otomatik olarak veri mahremiyeti dostu olması gerektiği ve yalnızca işlemenin her bir özel amacı için gerekli olan verilerin toplanması gerektiği anlamına gelir. Varsayılan olarak veri koruması, bu verileri işleme başlamadan önce belirtmeniz, bireyleri uygun şekilde bilgilendirmeniz ve yalnızca ihtiyacınız olan verileri amacınız için işlemeniz gerektiği anlamına gelir.

Kanunda yer verilmeyen bu ilkelere Kurulun vermiş olduğu kararlarda görmek mümkündür. Verilen kararlarla *"sistemin tasarım aşamasından itibaren doğru bir şekilde planlanmadığı ve gerekli kontrollerin yapılmadığının göstergesi olduğu"* (Kişisel Verileri Koruma Kurulu, 2020) ve *"web sayfası tasarım aşamasında iken yapılan testlerin yetersiz olduğunun veya gerekli testlerin yapılmadığının göstergesi olduğu"* (Kişisel Verileri Koruma Kurulu, 2020) tasarım yoluyla veri koruma ilkesine uymayan veri sorumlularına idari para cezası yaptırımında bulunulduğu görülmektedir.

SONUÇ

Kişisel verilerin işleme olanakları arttıkça bu verilerin ihlali neticesinde ortaya çıkacak riskin büyüklüğü de artmaktadır. Bunun nedeni olarak işlenen verilerin gerek hacim gerek nitelik olarak artması, bu verilerden faydalanabilecek insan niteliğinin fazlalaşması gösterilebilir. Bu kapsamda hem veri sorumluları hem de karar vericiler için kişisel verilerin korunması alanında riski saptamanın önemi giderek artmaktadır. Veri sorumluları açısından yapılacak yerinde bir risk değerlendirmesi, kendisine veri ihlallerine karşı etkin bir şekilde koruyacak olmasının yanı sıra, kaynakların israf edilmeden kullanılmasına da yol açacaktır. ◆

KAYNAKÇA

- “Bir perakende giyim firmasının veri ihlal bildirimi hakkında” Kişisel Verileri Koruma Kurulunun 20/01/2020 tarih ve 2020/50 sayılı Karar Özeti”, https://kvkk.gov.tr/Icerik/7026/2020-50 adresinden 25.04.2022 tarihinde alınmıştır.
- “Data protection by design and default” https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dpd3 adresinden 25.04.2022 tarihinde alınmıştır.
- “Marriott International Inc. hakkında Kişisel Verileri Koruma Kurulunun 16.05.2019 tarih ve 2019/143 sayılı Karar Özeti”, https://kvkk.gov.tr/Icerik/5479/2019-143 adresinden 25.04.2022 tarihinde alınmıştır.
- Madde 29 Çalışma Grubu. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, https://ec.europa.eu/newsroom/article29/items/623051/en adresinden alınmıştır.
- Artıcle 29 Data Protectıon Workıng Party, Guidelines on Personal data breach notification under Regulation 2016/679.
- Artıcle 29 Data Protectıon Workıng Party, Statement on the role of a risk-based approach in data protection legal frameworks.
- Quelle, C., The ‘risk revolution’ in EU data protection law: We can’t have our cake and eat it, too, Tilburg Law School Legal Studies Research Paper Series No. 17/2017.
- Dülger, M. V. (2019). Kişisel Verilerin Korunması Hukuku. İstanbul, Hukuk Akademisi.
- Gellert, R. (2017). Why the GDPR risk-based approach is about compliance risk, and why it’s not a bad thing, In S. Erich, F. Kummer, & C. Sorge (Eds.), Trends und Communities der Rechtsinformatik - Trends and communities of legal informatics : Tagungsband des 20. Internationalen Rechtsinformatik Symposions - IRIS 2017 - Proceedings of the 20th International Legal Informatics Symposium.

- Gellert, R. (2020). The Risk-Based Approach to Data Protection, Oxford University Press.
- Develioğlu, H. M., 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, 2017.
- ISACA Glossary of Terms English – Turkish First Edition (2018).
- Maldoff, Gabriel. The Risk-Based Approach in the GDPR: Interpretation and Implications, 2016, CIPP/US, IAPP Westin Fellow.
- Kaya M. B., “Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi”, İstanbul Hukuk Mecmuası, 78 (4), Yıl 2020, ss. 1859-1897, s.1881.
- Kişisel Verileri Koruma Kurumu. (2022). Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler). https://kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf adresinden alındı.
- Çekin M. S., Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu, On İki Levha, 2018.
- Zurawski, N. Wright, D. and de Hert, P (eds), Privacy Impact Assessment, Springer, International Data Privacy Law, 2012, ss. 316–317, s. 316.
- Özdemir, M. (2019). Kurumsal Risk Yönetimi İçin Web Tabanlı Risk Analiz Platformu Tasarımı (Yayımlanmamış yüksek lisans tezi). Aksaray Üniversitesi Sosyal Bilimler Enstitüsü, Aksaray.
- Review of the European Data Protection Directive, https://www.rand.org/pubs/technical_reports/TR710.html, adresinden 04.04.2022 tarihinde ulaşılmıştır.
- Türk Dil Kurumu, Güncel Türkçe Sözlük” https://sozluk.gov.tr/ adresinden 22.03.2022 tarihinde alınmıştır.

KİŞİSEL VERİLERİN KAYDEDİLMESİ SUÇU VE 6698 SAYILI KANUNDAKİ KABAHATLERİN SUÇLAR KARŞISINDAKİ KONUMU

Arif Onur KÜÇÜKBASMACI

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "6698 sayılı Kişisel Verilerin Korunması Kanunu ile 5237 sayılı Türk Ceza Kanunu İlişkisi" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

KVKK'nın yürürlüğe girdiği tarihten önce mevzuatta *"kişisel veri"*nin bir tanımına yer verilmemesinin *kanunilik ve belirlilik* ilkeleri açısından sakıncalar doğurabileceği uygulamada ifade edilmiştir (Ünver, 2008). Kişisel verilerin korunmasına ilişkin ceza normlarının uygulanmasında kanunilik ilkesine ilişkin tereddütler yargıda da oluşmuş olup KVKK'nın yürürlüğe girdiği tarihten sonra TCK madde 135 ve devamında yer alan maddelerle ilgili verilen kararlarda ciddi bir artış yaşanmıştır (Orhan, 2021).

Kişisel verilerin korunması, büyük oranda özel hukuk ve kabahatler hukuku yoluyla sağlanmaktaysa da ceza hukukunun bu alanda gün geçtikçe artan bir etkisi bulunmaktadır. Bazı ülkeler tarafından kişisel verilerin korunması kanunlarına ve ceza kanunlarına ceza hükümleri de konulmakta ve bazı davranışlar suç kabul edilmektedir. Bu alanda daha etkin bir korumanın sağlanması için bir zorunluluk olan bu husus; ceza hukukunun temel ilkelerinin kişisel verilerin korunmasına ilişkin cezai normlara uygulanmasını kaçınılmaz hale getirmektedir (Orhan, 2021).

Bu makalenin birinci bölümünde kişisel verilerin kaydedilmesi suçu incelenecek, ikinci bölümünde ise TCK madde 135-140 arasında düzenlenen suç tipleri ile KVKK madde 18'de düzenlenen kabahatlerin aynı anda işlenmesi, farklı durumlar karşılaştırılarak incelenecektir.

KİŞİSEL VERİLERİN KAYDEDİLMESİ SUÇU

TCK madde 135'in gerekçesinde belirtildiği üzere kişisel verilerin sanal ortamda ya da fiziki ortamda kaydedilmesi tipikliğin oluşması açısından bir fark yaratmayacaktır. Kişisel verilerin kaydedilmesi suçu, serbest hareketli bir suç tipidir. Bu suç tipinin oluşması için kişisel verilerin kaydedilmesinden sonra ifşa edilmesi gerekmemektedir. Tek başına kaydetme fiili suç tipinin oluşması için yeterlidir (Dülger, 2016).

Bu suç, kişisel veriler kaydedildikten sonra belirli bir süre saklanma şartı öngörülmediğinden ani hareketli bir suç tipidir. Ayrıca, kaydetme tipik hareketi icrai bir hareket olup suç tanımında ihmali hareketle işlenebileceği belirtilmediğinden suç ancak icrai hareketle işlenebilir (Kangal, 2019).

"Kişisel verilerin kaydedilmesi suçu", Anayasadaki özel hayatın gizliliği başlıklı 20 nci madde düzenlemesine paralel olarak TCK'nın *"özel hayata ve hayatın gizli alanına karşı suçlar"* başlıklı dokuzuncu bölümünde yer almaktadır. AİHS'nin 8 inci maddesinde de düzenlenen *"özel hayatın gizliliği hakkı"* TCK 135 ve devamında yer alan suç tipleriyle bir hukuksal değer olarak korunmaktadır (Dülger, 2019). Her norm bir varlık ya da menfaati koruduğundan bütün suç tiplerinin hukuki konusu bulunmaktadır. Suç tipi ile korunan hukuki konu ise suçu düzenleyen maddenin koruduğu ve suç teşkil eden fiil ile ihlal edilen hukuki menfaattir (Orhan, 2021).

Anayasa madde 20/3'te düzenlenen *"kişisel verilerin korunmasını isteme hakkı",* kişilerin dokunulmaması gereken bir özgürlük alanı olarak değil talep edilebilir bir hak olarak tanınmıştır. Kişisel veri işleme şartlarının da düzenlenmesiyle bu hakka ilişkin müdahalelerin kanunla yapılmasının öngörülmesi kamu otoritelerinin de kişisel verilerin korunması açısından sınırlandırıldığının bir göstergesidir. Doktrinde bu hak, teknolojinin kötüye kullanılmasının önüne geçebilmek için dördüncü kuşak haklar arasında da değerlendirilmektedir. Dolayısıyla, kişisel verilerin korunmasını isteme hakkının özel hayatın gizliliği veya kişilik haklarından ayrışarak bağımsız bir hal aldığı sonucu ortaya çıkmaktadır (Sınar, 2020).

Kişisel verilerin korunmasını isteme hakkı Anayasada özel hayatın gizliliği başlığı altında ayrı bir hak olarak düzenlendiğinden TCK madde 135 ile korunan değerin kişisel verilerin korunmasını isteme hakkı olduğu kabul edilmelidir (Koca, Üzülmez, 2019).

Suçun Unsurları

Suçun maddi (objektif) unsurları, suçu oluşturan hareketin dış dünyadaki görünüş biçimidir. Suç tipinin tanımında yer alan objektif unsurları; fail, mağdur, suçun konusu, hareket, hareketin tür ve şekilleri ile neticedir. Manevi (sübjektif) unsurlar ise failin iç dünyasına ait olan unsurlardır. Kişinin iç dünyasına ait bu unsurlar, kişi ile gerçekleştirdiği fiil arasındaki bağı oluşturan kast, taksir ve fiilin hareket bakımından ifade ettiği değersizlikle ilgili diğer manevi unsurlardır (Koca ve Üzülmez, 2017).

TCK madde 135'te fail bakımından özel bir nitelik aranmadığından bu suç herkes tarafından işlenebilir. Ancak TCK'nın 137 nci maddesindeki nitelikli haller belirli sıfata sahip kişilerce (kamu görevlisi tarafından ve belirli bir meslek ve sanatın sağladığı kolaylıktan faydalanan kişi tarafından) işlenebileceğinden burada *görünüşte özgü suç* özelliği gözlemlenmektedir (Korkmaz, 2017).

Mağdur ise suçun konusunun yani kişisel verilerin sahibi olan kişidir. İlgili kişi, KVKK'da açıkça düzenlendiği üzere kişisel verisi işlenen gerçek kişidir. Bununla birlikte, TCK'nın 135 inci maddesinin gerekçesinde kişisel verinin gerçek kişiyle ilgili her türlü bilgi olduğuna değinilmiştir. Dolayısıyla mağdur, gerçek kişiler olacaktır (Sert, 2019).

Tüzel kişiler bu suçun mağduru olamazlar. Ancak suçtan zarar gören olmaları mümkündür. Diğer taraftan, ilgili kişi, kişisel verisi işlenen gerçek kişi olduğundan kaydetme hareketinin gerçekleştirildiği tarihte verisi kaydedilen kişi yaşamıyorsa bu durumda kişisel verileri kaydetme suçu oluşmayacaktır. Ancak şartlarının oluşması halinde TCK'nın 130 uncu maddesinin birinci fıkrasında düzenlenen kişinin hatırasına hakaret suçu oluşabilir (Kangal, 2019).

Suçun Konusu

Suçun konusu ilgili kişiye ait kişisel verilerdir. Kişisel veri; KVKK'daki tanım gereği gerçek kişiyi belirli ya da belirlenebilir kılan her çeşit bilgidir. Suçun konusu olan kişisel verilerin KVKK'da ya da TCK'da tüketici bir sayımı yapılmamıştır. Gelişen ve değişen teknoloji karşısında bu şekilde bir sayım yapılması olanaklı olmadığı gibi gerekli de değildir. Suçun konusunu oluşturan verinin ilgili kişileri belirli ya

da belirlenebilir kılan kişisel veri olması yeterlidir (Koca ve Üzülmez, 2019). Örneğin anonim hale getirilmiş kişisel veriler; ait oldukları ilgili kişilerle bağlantıları kesilmiş olduğundan ilgili kişileri belirli veya belirlenebilir kılamayacaktır. Bu nedenle suçun konusunu da oluşturmayacaklardır. Öte yandan, kişisel verilerin sadece belirli kişi ve kuruluşların elinde bulunan vasıtaların sağladığı imkânlarla ilgili kişilerle ilişkilendirilebildiği hallerde de o verinin kişisel veri olduğu kabul edilmelidir. Örneğin araç plaka numarası, emniyet teşkilatının sistemi üzerinden ilgili kişilerle ilişkilendirilerek kişileri belirli kılabilir. Ancak araç plaka numarasını kaydeden kişinin emniyet teşkilatının sistemine erişimi olmaması sebebiyle araç plakasının kime ait olduğunu bilmediği ve dolayısıyla plakanın suçun konusunu oluşturmayacağı yorumu yapılamayacaktır.

Diğer taraftan, KVKK'nın 5/2(d) maddesinde yer alan kişisel verilerin ilgili kişinin kendisi tarafından alenileştirilmiş olması şartı bakımından konunun değerlendirilmesi gerekmektedir. İlgili kişinin kendisine ait kişisel verilerini alenileştirmiş olması halinde (örneğin resmini sosyal medyada yayınlamış olması) bu verilerin başkaları tarafından toplanması, elde edilmesi, kaydedilmesi veya açıklanması TCK 135 ve 136'da yer alan suç tiplerini oluşturmayacaktır. Böyle bir durumda kişi, özel hayatına ilişkin bilginin mahremiyetini kendisi kaldırmış olmakta ve hukukun sağladığı korumadan vazgeçmektedir (Koca ve Üzülmez, 2019).

Kişisel verilerin alenileştirilmesiyle ilgili Kurum tarafından yayınlanan 16.12.2020 tarihli kamuoyu duyurusunda ise şu şekilde görüş belirtilmiştir: *"Kişisel verinin alenileştirilmiş olarak kabul edilebilmesi için ilgili kişinin ne amaç ile kişisel verilerini alenileştirdiğinin de tespit edilmesi gerekmektedir. Nitekim alenileştirme eylemi; ilgili kişilerin, kişisel verilerini kamuoyu ile paylaşması amacı ile sınırlıdır. Veri sorumlularının; ilgili kişinin alenileştirme amacından farklı ya da bu amacı aşan şekilde kişisel veri işleme faaliyetinde bulunmaları, başkaca bir işleme şartına dayanılmadığı sürece, Kanuna aykırılık oluşturacaktır. Diğer bir deyişle verinin ilgili kişi tarafından alenileştirilmiş olması, veri sorumluları tarafından her türlü amaçla gerçekleştirilecek işleme faaliyetini hukuka uygun hale getirmeyecektir. Örneğin bir internet sitesi aracılığıyla aracını satışa çıkaran bir kişinin bu sitede paylaşmış olduğu iletişim bilgileri sadece aracı satın almak veya bu ilanla ilgili bilgi almak amacı ile kullanılabilecek olup, bunun dışında bir amaçla kullanılması Kanuna aykırılık teşkil edecektir."*

Dolayısıyla, Kurulun KVKK'da yer alan kabahatler bakımından yerleşik uygulamasına göre, kişisel verilerin alenileştirilmesi bu kişisel verilerin her türlü amaç için kullanılabileceği sonucunu doğurmayacaktır. Söz konusu kişisel verilerin; ilgili kişinin alenileştirme iradesinin yöneldiği amaçtan başka amaçlarla hukuka aykırı olarak işlenmesi halinde KVKK'ya aykırılık oluşacaktır. Dülger'e göre de (2016) benzer şekilde kişisel verilerin alenileştirme iradesinin yöneldiği amaç haricinde işlenmesi hukuka aykırı olacaktır.

Hareket

Kanunda belirtilen şekillerde fiillerin gerçekleştirilmesi ile tipe uygun haksızlık ortaya çıkar. Kanunda yer almayan fiiller ceza hukuku açısından önem teşkil etmez (Görkemli, 2020). Tipikliğin gerçekleşmesi için gerekli olan hareket kaydetme fiilidir. Suçun oluşması için bu fiil bilişim sistemleri gibi herhangi bir araç vasıtasıyla gerçekleştirilebileceği gibi fiziki ortamda kişisel verilerin kaydedilmesi de yeterli olacaktır. Dolayısıyla, TCK madde 135'teki tipik fiilin gerçekleşmesi için KVKK'nın 2 nci maddesi kapsamında otomatik vasıtalarla işlenme ya da veri kayıt sisteminin bulunması şartları geçerli olmayacaktır (Kangal, 2019). Zira, TCK madde 135'e göre kişisel verilerin kaydedilmesi suçu bakımından kayıt işleminin yapıldığı yerin bir veri kayıt sistemi olması gerektiğine dair düzenleme bulunmamaktadır. Örneğin ilgili kişinin kişisel verilerinin bir kâğıt parçasına kaydedilmesi de suçun oluşması için yeterli bir hareket sayılacaktır (Sert, 2019).

Kişisel verilerin kaydedilmesi suçu, icrai hareketle işlenebilir. Maddenin lafzından suçun oluşması için kaydetme fiilinin gerçekleştirilmesinin yeterli olduğu anlaşılmaktadır. Kaydetme fiili birçok şekilde (Flash belleğe, CD'ye, bilgisayara, cep telefonuna kaydetme gibi) yapılabileceğinden bu suç serbest hareketli bir suçtur. Suçun işlenmesi için bir neticenin meydana gelmesi sonucu aranmadığından kaydetme fiilinin gerçekleştiği anda suç işlenmiş olacaktır. Suça konu hareket ile bir neticenin meydana gelmesi zorunlu olmadığından bu suçun soyut tehlike suçu olduğu söylenebilecektir (Göçmen Uyarer, 2019).

Nitelikli Hal Unsuru

KVKK'nın 6/1 inci maddesinin gerekçesinde de belirtildiği üzere özel nitelikli kişisel veriler, üçüncü kişilerce elde edildiği takdirde ilgili kişilerin mağduriyetinin daha fazla olabileceği ya da ayrımcılığa uğrayabileceği öngörülerek düzenleme altına alınmış ve diğer kişisel verilerden daha sıkı korumaya tabi tutulmuştur. Bu düşünceyle paralel olarak kanun koyucu tarafından TCK madde 135/2'de bazı kişisel verilerin suçun konusunu oluşturması halinde cezanın yarı oranında artırılacağı düzenlenmiştir. Bununla birlikte, TCK'nın KVKK'dan önce yürürlüğe girmesi sebebiyle KVKK'nın 6/1 inci maddesinde sınırlı sayıda sayılan özel nitelikli kişisel verilerin tamamı TCK madde 135/2'de yer almamaktadır. Bu nedenle söz konusu nitelikli hal sadece TCK 135/2'de yer alan kişisel veriler bakımından

uygulama alanı bulacaktır. KVKK'da sayılıp TCK madde 135/2'de sayılmayan özel nitelikli kişisel verilerin kaydedilmesi fiili ise ancak suçun basit haliyle cezalandırılabilecektir (Koca ve Üzülmez, 2019).

TCK'nın 137 nci maddesinde, TCK 135 bakımından uygulama alanı bulacak iki farklı nitelikli hal daha düzenlenmiştir. Bunlar; suçun kamu görevlisi tarafından görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi ve suçun belirli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesidir.

Kamu görevlisi, TCK madde 6/1-c'de tanımlanmıştır. Kamusal faaliyetin yürütülmesinde rol alan kişilerin bunun karşılığında ücret alıp almadıkları, işi sürekli ya da geçici yapmaları nitelikli halin uygulanması bakımından önemli değildir. Bu nitelikli halin uygulama alanı bulması için failin fiili gerçekleştirdiği sırada kamu görevlisi olması yeterli değildir. Failin aynı zamanda kamu görevinin verdiği yetkiyi kötüye kullanarak kişisel verileri kaydetmiş olması gerekmektedir. Ayrıca kişisel verilerin kaydedilmesi işlemi kamu görevlisinin görevinin gereği olmalıdır ve kamu görevlisinin görevi kapsamı dışına çıkarak kaydetme hareketini yapması halinde nitelikli hal uygulanacaktır (Kangal, 2019).

TCK madde 137/1-b'de düzenlenen diğer nitelikli halin uygulanabilmesi için fail, meslek ve sanat olarak kabul edilecek herhangi bir işle iştigal etmeli ve bu meslek ve sanatla iştigal etme faile kişisel verilerin kaydedilmesi hususunda kolaylık sağlamalıdır. Örneğin; bir banka çalışanının bankanın sisteminde kayıtlı bilgilere ulaşıp bu verileri mesleğinin sağladığı kolaylıktan yararlanarak kendi bilgisayarına kaydetmesi halinde bu nitelikli hal uygulanacaktır (Sert, 2019).

Netice

TCK'da yer alan suç tiplerinin çoğunluğu, icrai veya ihmali bir hareketin yapılması ile tamamlanır. Ancak tamamlanması için herhangi bir neticenin aranmadığı suç tipleri sırf hareket suçlarıdır (Koca ve Üzülmez, 2017). Suçun gerçekleşmesi için, kanun koyucu tarafından kaydetme fiilinin gerçekleştirilmesinden sonra ayrı bir netice aranmamıştır. Bu nedenle TCK madde 135'te düzenlenen suç, sırf hareket suçudur (Koca ve Üzülmez, 2019).

Bununla birlikte, Aydın'a göre (2015) TCK madde 135 düzenlemesi gereği kaydetme fiilinin netice olarak değerlendirilmesi gerekmekte olup TCK madde 135'teki suç neticeli bir suçtur.

Manevi Unsurlar

TCK madde 21'in ilk cümlesinde suçun oluşmasının kasta bağlı olduğu belirtilmiştir. Yine TCK'nın 22 nci maddesinin birinci firkasında ise "*taksirle işlenen fiiller, kanunun açıkça belirttiği hallerde cezalandırılır*" düzenlemesiyle suçun kastla işlenebileceği kuralının istisnası düzenlenmiştir. Dolayısıyla TCK açısından bir suçun kastla işlenmesi kural, taksirle işlenmesi ise istisnadır (Koca ve Üzülmez, 2019). Failin kastının bulunduğundan söz edebilmek için ise suç teşkil eden fiilin istenmesiyle birlikte bilinmesi de gerekmektedir (Hafizoğulları ve Özen, 2014). TCK madde 135'te düzenlenen suç sadece kastla işlenebilir. Suç tipi düzenlemesinde failin özel bir maksadı aranmamıştır (Sert, 2019).

Fail, kaydettiği verilerin kişisel veri niteliği taşıdığını bilmiyorsa TCK madde 30/1 kapsamında suçun maddi unsurlarında hata söz konusudur. Bu durum suçun maddi koşullarına dâhil olan normatif bir unsurda hataya düşülmesi anlamına gelecektir. Tipikliğin normatif unsuru da kastın kapsamında yer aldığından kast ortadan kalkacaktır. Failin taksirle hataya düşmesinin de bir önemi olmayacaktır çünkü suçun taksirli hali kanunda düzenlenmemiştir. Ayrıca fail, bir bilgiyi kişisel veri niteliği olmamasına rağmen kişisel veri niteliği taşıdığını sanarak kaydetmişse bu durumda işlenemez suç söz konusu olacaktır. Çünkü gerçekleştirilen hareket suçun konusu üzerinde zarar tehlikesi yaratmaya elverişli değildir (Kangal, 2019).

Hukuka Aykırılık Unsuru

Hukuka aykırılık, tipikliğin oluşması için gerekli bir unsur olmayıp suçun yapısal bir unsurudur. Fiilin tipikliğinin belirlenmesi, hukuka aykırılık değerlendirmesinden önce gelir. Çünkü bir fiil hakkındaki hukuka aykırılık yargısı tipe dayalıdır. Herhangi bir tipiklik oluşturmayan fiil hakkında hukuka aykırılık değerlendirmesi yapmaya gerek yoktur. Dolayısıyla hukuka aykırılığın varlık temeli tipikliktir ve tipiklik hukuka aykırılığa karine oluşturur. Bu nedenle hukuka aykırılığın suçun yasal tanımında ayrıca belirtilmesine gerek bulunmamaktadır. Ancak suç tanımlarının bazılarında hukuka aykırılık unsuru ayrıca belirtilmektedir (Göktürk, 2016). TCK 135'te kişisel verilerin kaydedilmesi fiilinin *"hukuka aykırı olarak"* gerçekleştirilmesi halinde cezalandırılacağı belirtilmiştir. TCK'da yer alan bu tip düzenlemelerle suç tipinde yer alan eylemin hukuka aykırı olmasının gerekliliğine özel olarak dikkat çekilmektedir. Bu nedenle, yasa koyucu işlenen fiilin hukuka aykırı olduğunun fail tarafından bilinmesini yani, failin işlediği fiilin hukuka aykırı olduğu hususunda *"doğrudan kastının"* olmasını aramıştır. Yani suç tipinin tanımında hukuka aykırılığın özellikle belirtilmesi halinde bu suç ancak

doğrudan kastla işlenebilecektir (Özgenç, 2019). Bu gibi ifadelerle özel biçimde aranan hukuka aykırılığı, suçun yapısal unsuru olan hukuka aykırılıktan ayırmak için bu hallerde *"hukuka özel aykırılığın"* varlığından bahsedilecektir (İçel, 2020).

Bir suçu düzenleyen maddede hukuka aykırılığın ayrıca belirtilmesinin hukuksal bir amacı ve önemi vardır. Diğer hukuka aykırılık durumlarında failin kastının hukuka aykırılığı kapsayıp kapsamadığı aranmaz. Ancak *hukuka özel aykırılığın* arandığı hallerde failin kastının özel olarak belirtilen hukuka aykırılığı içermesi aranmakta ve faile cezai müeyyideye maruz kalması için bu durumun da ispatlanması gerekmektedir (İçel, 2020). Hukuka aykırılığın suç tipinde özel olarak belirtildiği hallerde, fiilin tipe uygun olması onun aynı zamanda hukuka aykırı olduğu anlamına gelmez. Bazı fiiller, mevzuatta yer alan diğer düzenlemeler nedeniyle, tipiklik gerçekleşmiş olsa bile hukuka uygun olabilir. Örneğin kişisel verilerin belirli şartlarla kaydedilmesine bir kanun tarafından izin veriliyorsa bu şartlar doğrultusunda kişisel verileri kaydeden kişiye ceza verilmeyecektir. Aksi halde bir kanun tarafından hukuka uygun görülen fiilin diğer kanun tarafından cezalandırılması hukuk düzeninin kendi içinde çatışmasını ortaya çıkaracaktır (Korkmaz, 2017). Dolayısıyla hukuk sisteminin birliği ilkesi nedeniyle fiil, bir hukuk dalında hukuka uygun sayılırken diğerinde hukuka aykırı olamayacaktır. Bu sebeple hukuka aykırılığı kaldıran sebepler hukuk düzeninin bütününe bakılarak belirlenmelidir. Ceza hukuku dışında kalan özel veya kamu hukukundan kaynaklanan hukuka uygunluk sebepleri ceza hukukunda uygulanabileceği gibi tamamen ceza hukukundan kaynaklanan hukuka uygunluk sebepleri de diğer hukuk dalları bakımından uygulanabilecektir (Koca ve Üzülmez, 2017).

Teşebbüs

Kişisel verilerin kaydedilmesi suçu sırf hareket suçu olsa da kaydetme hareketinin kısımlara ayrılabildiği hallerde teşebbüs söz konusu olabilecektir. Ancak kişi bir başkasına ait kişisel verileri hukuka aykırı olarak ele geçirdikten sonra kaydetme fiilini elinde olmayan nedenlerle tamamlayamamışsa bu durumda failin kişisel verilerin kaydedilmesi suçuna teşebbüsten değil TCK madde 136'da yer alan *"verileri hukuka aykırı olarak verme veya ele geçirme"* suçundan cezalandırılması gerekmektedir. Diğer taraftan, failin kayıt işlemine başladıktan sonra teknik sorunlar yaşaması veya yakalanması nedeniyle kayıt işlemini tamamlayamaması halinde suç teşebbüs aşamasında kalmış sayılır (Kangal, 2019).

İştirak

İştirak; kanunun suç olarak düzenlediği eylemin birden çok kişi tarafından birlikte işlenmesine denir (Hafzıoğulları ve Özen, 2014). TCK madde 135'te düzenlenen suç iştirak açısından farklı bir özellik göstermemekte olup TCK'nın iştirak düzenlemelerindeki ihtimallerin tamamı bu suç açısından gerçekleşebilecektir (Akdağ, 2010).

Burada belirtmek gerekir ki, suçun kamu görevlisi olmayan bir kişi ile kamu görevlisinin görevinin verdiği yetkiyi kötüye kullanarak ortak fail olarak birlikte işlendiği ihtimalde, TCK 137'de düzenlenen nitelikli hal sadece kamu görevlisi bakımından uygulanacaktır. Bu durum *failliğin şerikliğe asliliği* kuralından ileri gelmekte olup kamu görevlisi olmayan kişi sadece TCK 135'de yer alan suçun basit halinden cezalandırılacaktır (Koca ve Üzülmez, 2019).

İçtima

Türk Ceza Hukuku sisteminde kural, gerçek içtimaın uygulanması olup işlenen fiil sonucu oluşan her suçtan ayrı cezaya hükmedilir. Ancak, işlenmiş olan suçların sayısına göre cezalandırma zorunluluğu içtima konusunun kanunda ayrıca düzenlenmesine bağlıdır (Göktürk, 2014). Kişisel verilerin kaydedilmesi suçu bakımından ayrı bir içtima düzenlemesi olmadığından TCK'da yer alan genel hükümler çerçevesinde içtima kuralları devreye girecektir.

Öte yandan, TCK madde 136'da düzenlenen suçun, 135 inci maddedeki kaydetme fiiliyle birlikte işlenmesine gerek bulunmamaktadır. Diğer bir ifadeyle, hukuka aykırı olarak kaydedilen kişisel veriler, 136 ncı maddedeki suç tipinin konusunu oluşturabilecektir. Bu halde hem 135 inci maddedeki hem de 136 ncı maddedeki suç işlenmiş olup gerçek içtima kuralları uygulama alanı bulacaktır (Değirmenci, 2005).

Kişisel verilerin kaydedilmesi fiilinin gerçekleştirildiği hallerde, TCK madde 134'te düzenlenen *"özel hayatın gizliliğini ihlal"* suçunun oluşabileceği durumların da göz önünde bulundurulması gerekmektedir. TCK'nın 134 üncü maddesinde, kişinin özel hayatının gizliliğinin, görüntü ve seslerin kaydedilmesiyle ihlal edilmesi durumunda uygulanacak cezanın bir kat artırılacağı öngörülmüştür. İlgili kişilere ait görüntü ve sesler, özel hayat alanına girse de girmese de kişisel veri niteliğinde sayılacaktır. Ancak kaydedilen görüntü ve seslerin özel hayat alanına ilişkin olması halinde kişisel verilerin kaydedilmesi suçu değil özel hayatın gizliliğini ihlal suçu oluşacaktır. TCK madde 134 ve 135 arasında bu anlamda bir genel-özel norm ilişkisi bulunmakta olup özel norm olan 134 üncü madde öncelikli olarak uygulanacaktır (Çakır, 2020).

Nitekim, *"Yargıtay 12. Ceza Dairesinin 19.01.2015 tarihli 2014/11530 Esas numaralı ve 2015/ 584 Karar sayılı" Kararında şu hususlar belirtilmiştir: "Sanıkların, mağdurla arkadaşlık kurdukları ve mağdurun, internet ortamından rızası ile gönderdiği çıplak fotoğraflarını flash diske kaydedip, babası M. 'ye vermek suretiyle ifşa ettiklerinin iddia edildiği olayda; mağdurun, cinsel ve fiziksel mahremiyetine ilişkin çıplak görüntüleri kişisel veri kapsamında değerlendirilemeyeceğinden, eylemin, kişisel verilerin kaydedilmesi suçunu değil, TCK'nın 134/1. maddesinin 2. cümlesi ve 134/2. maddesine uyan özel hayatın gizliliğini ihlal suçlarını oluşturacağı, bu suçların, aynı Kanunun 139/1. maddesi uyarınca soruşturulması ve kovuşturulması şikayete bağlı olup, mağdurun, soruşturma ve kovuşturma aşamalarındaki ifadelerinde, sanıklardan şikayetçi olmadığı anlaşıldığından, sanıklar hakkında açılan davanın düşmesi yerine sanıkların mahkumiyetine hükmedilmesi, kanuna aykırı olup..."*

Diğer taraftan, doktrinde KVKK'nın yürürlüğe girmesinden sonra Yargıtay'ın bu uygulamasının artık geçerliliğini yitirdiğine dair görüşler de yer almaktadır. Ketizmen'e göre bunun sebebi KVKK'nın 17 nci maddesidir. Söz konusu maddenin birinci fıkrasında KVKK kapsamında kalan kişisel veri işleme faaliyetleri açısından oluşacak hukuka aykırılıklar bakımından uygulanacak suç tiplerinin TCK madde 135-140 arasındaki maddelerde düzenlenen suçlar olduğu düzenlenmektedir. Uygulanacak suç tiplerinin TCK madde 135-140 arasında sınırlı tutulmasının bir sonucu olarak hukuka aykırı şekilde işlenen kişisel verilerin, kişilerin özel hayat alanına ilişkin ses ve görüntüler olması halinde TCK 134'ün değil 135-140 arasında yer alan maddelerin uygulanması gerekmektedir (Ketizmen ve Kart, 2021).

Kişisel verilerin kaydedilmesi suçu TCK'nın 244 üncü maddesinde düzenlenen *"sistemi engelleme, bozma, verileri yok etme veya değiştirme"* suçu ile de aynı anda işlenebilecektir. 244 üncü maddedeki sisteme veri yerleştirme fiili ile 135 inci maddedeki verileri kaydetme fiili aynı anlama gelmektedir. Ancak, 244 üncü maddedeki suçun konusu her türlü veriyken 135 inci maddedeki suçun konusu sadece kişisel verilerdir. Dolayısıyla bilişim sistemine kişisel verilerin yerleştirilmesi halinde fikri içtima hükümleri uygulanacak olup yerleştirilen veri kişisel veri değilse, 244 üncü maddedeki suç oluşacaktır (Çakır, 2020).

KABAHATLER İLE SUÇLARIN İÇTİMAI

Bir fiil hem kabahat hem de suç olarak tanımlanmışsa, 5326 sayılı Kabahatler Kanununun 15/3 üncü maddesi kapsamında sadece suçtan yaptırım uygulanabilecektir. Suçtan yaptırım uygulanamayan hallerde ise kabahatten yaptırım uygulanabilir. Bu başlık altında KVKK'da yer alan kabahatler ile TCK'daki suç tiplerinin

birlikte bulunduğu ihtimaller değerlendirilecektir. Bu durumda üç ihtimal söz konusu olabilecektir. Bunlar; gerçek kişinin fiiliyle tüzel kişi veri sorumlusu bünyesinde ihlal meydana gelmesi, gerçek kişinin fiiliyle gerçek kişi veri sorumlusu bünyesinde ihlalin meydana gelmesi ve gerçek kişi veri sorumlusunun kendi fiiliyle ihlalin meydana gelmesi halleridir.

Gerçek Kişinin Fiiliyle Tüzel Kişi Veri Sorumlusu Bünyesinde İhlal Meydana Gelmesi

TCK madde 20'nin gerekçesinde ceza sorumluluğunun şahsiliğinden dolayı sadece gerçek kişilerin suç faili olabileceği belirtildikten sonra tüzel kişiler hakkında idari yaptırımların uygulanabileceği ifade edilmiştir.

Benzer şekilde 5326 sayılı Kabahatler Kanunu'nun 8 inci maddesinde: *"Madde 8- (1) Organ veya temsilcilik görevi yapan ya da organ veya temsilci olmamakla birlikte, tüzel kişinin faaliyeti çerçevesinde görev üstlenen kişinin bu görevi kapsamında işlemiş bulunduğu kabahatten dolayı tüzel kişi hakkında da idarî yaptırım uygulanabilir."* düzenlemesine yer verilmiştir.

Ancak bu hüküm, tüzel kişileri kabahat faili haline getirmemekte olup aksine, maddede tüzel kişilerin bizzat kabahat işleyemeyecekleri belirtilmektedir. Burada tüzel kişi; organ, temsilci veya faaliyeti çerçevesinde görev üstlenen kişinin davranışı sebebiyle idari para cezasına çarptırılmaktadır. Maddede *"tüzel kişi hakkında da idari yaptırım uygulanabilir."* ifadesi yer almakta olup buradaki *"da"* bağlacı ile tüzel kişi hakkında idari yaptırım uygulanmasının tüzel kişi adına hareket eden gerçek kişinin işlediği kabahatten dolayı sorumluluğunu ortadan kaldırmadığı ortaya konmuştur. Dolayısıyla tüzel kişilerin görevini üstlenen gerçek kişilerin kabahat teşkil eden fiilleri sebebiyle hem gerçek kişiler hakkında hem de tüzel kişiler hakkında idari yaptırım uygulanabilecektir (Pehlivan, 2020). Tüzel kişilerin faaliyetleri, bünyesinde bulunan gerçek kişiler tarafından gerçekleştirildiği için bünyesindeki gerçek kişilerin fiilleri nedeniyle tüzel kişilerin idari yaptırıma maruz kalması son derece olağandır.

Bununla birlikte, KVKK'nın 18 inci maddesi kapsamındaki bir kabahatin tüzel kişi bünyesinde çalışan bir gerçek kişi tarafından işlenmesi halinde ise kabahate konu idari para cezası sadece *veri sorumlusu* olan tüzel kişi hakkında uygulanacaktır. Çünkü KVKK madde 18/2'de idari para cezalarının sadece KVKK kapsamında *"veri sorumlusu"* olan gerçek ve özel hukuk tüzel kişilerine uygulanabileceği belirtilmektedir (Kangal, 2019). Kişisel veri işleme faaliyetinin gerçekleştirildiği tüzel kişi bünyesinde kişisel veri işleme faaliyetlerinin yerine getirilmesinden

sorumlu gerçek kişiler, KVKK kapsamında veri sorumlusu değildirler. Veri sorumlusunun tüzel kişi olması halinde yükümlülük ilgili tüzel kişilik üzerinde doğacaktır. Dolayısıyla veri sorumlusu tüzel kişi bünyesindeki gerçek kişilerin veri ihlaline sebep olmaları halinde bu kişiler KVKK kapsamında veri sorumlusu olarak kabul edilmeyeceklerinden haklarında idari para cezası uygulanması mümkün olmayacaktır. Diğer taraftan, bu ihtimalde tüzel kişinin bünyesinde çalışan gerçek kişilerin fiillerinin aynı zamanda TCK 135 ve devamında yer alan suçları oluşturması halinde bu hükümlere göre işlem yapılması açısından da bir engel bulunmamaktadır.

Nitekim Kurul'un yerleşik uygulamaları da bu yöndedir. Kurul'un 26/11/2019 tarih ve 2019/352 sayılı kararında veri sorumlusu bankanın çalışanları tarafından müşterilerin kişisel verilerinin sızdırılması sonucu ortaya çıkan kişisel veri ihlalinde veri sorumlusu olan banka tüzel kişiliği hakkında idari para cezası uygulanmış, ihlali gerçekleştiren gerçek kişi banka çalışanları hakkında ise idari para cezasına hükmedilmemiştir. Benzer yönde bir başka karar ise 03/02/2021 tarihli ve 2021/78 sayılı Kurul kararıdır.

Benzer şekilde Kurul'un 13/02/2020 tarihli ve 2020/124 sayılı kararında; veri sorumlusu hava yolu şirketi bünyesindeki çalışanın, ilgili kişiye ait kişisel verileri KVKK'ya aykırı olarak ele geçirmesi şeklinde gerçekleşen olayda veri sorumlusu hakkında veri güvenliğinin sağlanmasına ilişkin yeterli teknik ve idari tedbirlerin alınmaması sebebiyle idari para cezası uygulanmıştır. Diğer taraftan aynı kararda; ilgili kişi tarafından kişisel verileri ele geçiren veri sorumlusunun çalışanı hakkında suç duyurusunda bulunulduğundan, çalışan bakımından Cumhuriyet Başsavcılığına suç duyurusunda bulunulmasına gerek olmadığına karar verilmiştir. Somut olay kapsamında çalışan hakkında daha önce suç duyurusunda bulunulmamış olması ihtimalinde Kurul tarafından suç oluşturabileceği değerlendirilen eylemin Cumhuriyet Başsavcılığına bildirileceği gerekçeden anlaşılmaktadır. Kurul'un bu yönde pek çok kararı bulunmakta olup bunlara Kurum'un resmi internet sitesinden erişilebilmektedir.

Veri sorumlusu tüzel kişilik hakkında, çalışanlarının fiilleri dolayısıyla idari para cezasının uygulandığı Kişisel Verileri Koruma Kurulunun 30/09/2021 tarihli ve 2021/993 sayılı ile 30/01/2020 tarihli ve 2020/78 sayılı kararları da örnek olarak gösterilebilecektir.

KVKK'ya aykırı fiilin tüzel kişinin çalışanları dışında üçüncü bir kişi tarafından gerçekleştirilmesi halinde de yaptırımlar bakımından sonuç değişmeyecektir. Yine aynı şekilde, veri sorumlusu tüzel kişi veri güvenliğine ilişkin yeterli teknik

ve idari tedbirleri almaması sebebiyle idari para cezasına maruz kalırken fiili gerçekleştiren gerçek kişi hakkında, fiilin suç oluşturması halinde, TCK hükümlerine göre işlem yapılacaktır.

Burada KVKK'da yer alan kabahatler bakımından, Kabahatler Kanunu madde 15/3 kapsamında sadece suçtan dolayı yaptırım uygulanabileceği akla gelse de bu yorum doğru olmayacaktır. Çünkü, anılan maddede *bir fiilin* hem suç hem kabahat teşkil etmesinden söz edilmektedir. Örneğin; veri sorumlusu bünyesinde çalışan kişi tarafından kişisel verilerin hukuka aykırı olarak *kaydedilmesinin* TCK kapsamında suç olarak düzenlendiği açık olmakla birlikte; aynı olayda çalışanın fiili nedeniyle veri sorumlusunun *veri güvenliğine ilişkin yükümlülüklerini ihmali davranışla yerine getirmediğinin* anlaşıldığı bir durumda (örneğin Kanunun 12 nci maddesi gereği gerekli tedbirlerin alınmadığı hallerde) ortada iki ayrı fiil bulunmaktadır. Dolayısıyla bu durumda veri sorumlusu olan tüzel kişi bakımından KVKK kapsamında idari yaptırım uygulanırken ihlale sebep olan gerçek kişi ise suç tipinin oluşması halinde TCK madde 135'e göre cezalandırılacaktır.

Gerçek Kişinin Fiiliyle Gerçek Kişi Veri Sorumlusu Bünyesinde İhlal Meydana Gelmesi

Kabahatler Kanununun 8 inci maddesinin ikinci fıkrasında; *"(2) Temsilci sıfatıyla hareket eden kişinin bu sıfatla bağlantılı olarak işlemiş bulunduğu kabahatten dolayı temsil edilen gerçek kişi hakkında da idarî yaptırım uygulanabilir. Gerçek kişiye ait bir işte çalışan kişinin bu faaliyeti çerçevesinde işlemiş bulunduğu kabahatten dolayı, iş sahibi kişi hakkında da idarî yaptırım uygulanabilir."* düzenlemesine yer verilmiştir.

Bir önceki başlıkta yapılan açıklamalara benzer şekilde burada da hem işveren hem de çalışan gerçek kişi hakkında idari para cezası uygulanabileceği düzenleme altına alınmaktadır.

Gerçek kişi kavramı, insanlarla sınırlı olarak düşünülmemeli, tüzel kişiliği olmamakla beraber kişi toplulukları da bu kapsamda değerlendirilmelidir. Örneğin, adi şirketler, tüzel kişiliği haiz olmayan hastaneler, avukatlık büroları, doktor muayenehanelerinde çalışan kişilerin kabahat teşkil eden fiilleriyle ilgili bu kişilerin çalıştığı yerlerin sahipleri hakkında da idari yaptırım uygulanabilecektir (Pehlivan, 2020).

Ancak, gerçek kişi veri sorumlularının yanında çalışmakta olan kişilerin fiilleri nedeniyle KVKK'nın 18 nci maddesinde yer alan kabahatlerin işlenmesi halinde

ise yine anılan maddenin ikinci fıkrası gereği idari para cezası sadece veri sorumlusu olan gerçek kişi hakkında uygulanabilecektir. Çünkü burada veri sorumlusu KVKK'nın 3 üncü maddesinin (ı) bendi gereği, *"kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek kişi"*, yani işveren olacaktır. Yine, gerçek kişi veri sorumlusu bakımından KVKK kapsamında idari para cezası uygulanabilirken gerçek kişi veri sorumlusu bünyesinde çalışan kişinin, kabahat oluşturan fiilin aynı zamanda TCK 135 ve devamındaki hükümlere göre suç teşkil etmesi halinde fiili işleyen gerçek kişi çalışana karşı bu hükümlerin uygulanması gerekmektedir.

Diğer taraftan, KVKK'ya aykırılığın gerçek kişi veri sorumlusunun çalışanları dışında üçüncü bir kişi tarafından gerçekleştirilmesi halinde de yaptırımlar bakımından sonuç değişmeyecektir. Yine aynı şekilde veri sorumlusu gerçek kişi, veri güvenliğine ilişkin yeterli teknik ve idari tedbirleri almaması sebebiyle idari para cezasına maruz kalırken fiili gerçekleştiren gerçek kişi hakkında TCK hükümlerine göre işlem yapılması mümkündür. Nitekim, Kurulun 07/05/2020 tarihli ve 2020/355 sayılı kararında da uygulamanın bu yönde benimsendiği görülmektedir. Anılan kararda şu değerlendirmelere yer verilmiştir:*"İl Sağlık Müdürlüğüne verilen bir dilekçede, dilekçe sahibinin bir eczacının sağlık problemleri nedeniyle işini yapamayacak durumda olduğunu belirterek dilekçe ekinde sağlık problemleri bulunduğunu belirttiği eczacının tanı ve ilaç bilgilerinin medula sisteminden çıktısının yer aldığı ifade edilmiştir. Dilekçeyi il sağlık müdürlüğüne veren kişinin eşinin de eczacı olduğu göz önünde bulundurulduğunda dilekçe sahibinin tanı ve ilaç bilgilerini eşinin erişiminde olan medula sisteminden aldığı araştırılmış ve Sosyal Güvenlik Kurumu'ndan alınan bilgilerle doğrulanmıştır. Bu doğrultuda veri sorumlusu eczacıya, Sosyal Güvenlik Kurumu ile yaptığı sözleşme kapsamında medula sistemine üçüncü kişilerin erişimini önlemek üzere veri güvenliğine ilişkin tedbirleri almadığından idari para cezası uygulanmıştır. Öte yandan veri sorumlusu eczacının eşi hakkında ise TCK madde 136'da düzenlenen Verileri hukuka aykırı olarak verme veya ele geçirme suçunun oluştuğu kanaatine varıldığından savcılığa suç duyurusunda bulunulmasına karar verilmiştir.".*

Gerçek kişi veri sorumlusunun çalışanı tarafından KVKK'ya aykırılık teşkil eden fiilin işlenmesi halinde bir üst başlıkta belirtildiği gibi Kabahatler Kanunu'nun 15/3 üncü maddesi uygulama alanı bulmayacaktır. Çünkü veri sorumlusu gerçek kişi tarafından veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi fiiliyle (örneğin çalışanlara yeterli eğitimin verilmemiş olması ya da çalışanların kişisel verileri hukuka aykırı olarak işlemesini önleyici mekanizmaları kurmamış olması) kabahat işlenmektedir. Veri sorumlusunun çalışanının fiili de burada farklı bir fiil olduğundan (örneğin kişisel verilerin hukuka aykırı olarak ele geçirilmesi) *iki ayrı fiil* söz konusu olacaktır. Dolayısıyla bu ihtimalde gerçek kişi veri sorumlusu bakımından KVKK'nın 18 inci maddesi kapsamında idari para cezası uygulanırken, gerçek kişi veri sorumlusunun çalışanı hakkında TCK 135 ve devamında yer alan suç tipleri bakımından cezai yaptırım uygulanabilecektir.

Gerçek Kişi Veri Sorumlusunun Kendi Fiiliyle İhlalin Meydana Gelmesi

Kabahat teşkil eden fiillerin aynı zamanda TCK hükümleri kapsamındaki suç tiplerini oluşturması durumunda izlenecek yol Kabahatler Kanununun 15/3'üncü maddesinde düzenlenmiş olup söz konusu kanun maddesine yukarıda değinilmişti. Yasa koyucu tarafından Kabahatler ile suçlar arasında oluşan içtimada suça ağırlık verilmesi, suçun haksızlık içeriğinin kabahate göre daha fazla olduğu düşüncesinin bir sonucudur (Akbulut, 2014).

Kabahatler Kanununun 15/3'üncü maddesinde kabahatler ile suçlar arasında *non bis in idem* kuralının uygulanması açıkça öngörülmüştür. *Non bis in idem ilkesi* AİHS'ne ek 7 No'lu protokolün 4. maddesinde düzenlenmiş olup AİHS'deki bu düzenlemeye benzer şekilde somut ve bağımsız bir düzenleme ise Anayasada yer almamaktadır. Anayasa Mahkemesi bu ilkeyi adil yargılanma hakkını düzenleyen Anayasanın 36 ncı maddesi kapsamında incelemektedir (Horozgil, 2021).

Gerçek kişi veri sorumlularının KVKK kapsamında kabahat teşkil eden fiili bizzat kendilerinin gerçekleştirmeleri ve bu fiilin aynı zamanda TCK 135 ve devamında yer alan suçları oluşturması halinde *aynı kişi tarafından aynı fiil ile* hem suç hem de kabahat işlenmiş olacağından bu ihtimal bakımından *non bis in idem* ilkesine uygun hareket edilmesi gerektiği değerlendirilmektedir.

Nitekim, Genel Veri Koruma Tüzüğü'nün 149 uncu resitalinde de üye devletler tarafından idari yaptırımlarla birlikte cezai yaptırımların da belirlenebileceği ancak bu durumun *non bis in idem* ilkesine aykırılık teşkil etmeyecek şekilde gerçekleştirilmesi gerektiği ifade edilmiştir.

Anayasa Mahkemesinin 04/11/2021 tarihli 2019/4 Esas ve 2021/78 Karar sayılı kararında; 213 sayılı Vergi Usul Kanununun, 340 ncı maddesinin ikinci fıkrasının, 359 uncu maddesinin son paragrafının ve 367 nci maddesinin beşinci fıkrasının iptali talebi incelenmiştir. Mezkûr kararda incelenen maddelerde vergi kaçakçılığı suçunun işlenmesi halinde fiili işleyen kişiye aynı zamanda bir vergi kabahati olan vergi zıyaı cezasının da uygulanabileceği düzenlenmekte yani aynı kişiye aynı fiilinden dolayı hem suç hem de kabahatten yaptırım uygulanabilmektedir (Horozgil, 2021). Ayrıca söz konusu kararda, idari yaptırımlar ile suç yaptırım-

larının aynı anda uygulanması *non bis in idem* ilkesi açısından ayrıntılı şekilde inceleme konusu yapılmıştır.

Anayasa Mahkemesinin söz konusu kararında, Kabahatler Kanununun 15 inci maddesinin üçüncü fıkrasının istisnası niteliğinde olan ve kabahat ile suç yaptırımlarının aynı anda uygulanmasını öngören Vergi Usul Kanununun 340 ıncı maddesinin ikinci fıkrasının, 359 uncu maddesinin son paragrafının ve 367 nci maddesinin beşinci fıkrasının iptal istemi şu gerekçeyle reddedilmiştir: *"İtiraz konusu kurallarla esas olarak kaçakçılık suçu nedeniyle hürriyeti bağlayıcı ceza ile cezalandırılmanın vergi kabahatleri için idari para cezası ile cezalandırılmaya engel olamayacağı, bu cezaların içtima hükümlerine göre birleştirilmeyeceği hüküm altına alınmakta dolayısıyla aynı fiil için birden fazla cezanın uygulanması ve cezaların birleştirilmemesi hususları düzenlenmektedir. Aynı fiilden dolayı birden fazla yargılanmama veya cezalandırılmama ilkesi belirli şartların sağlanması halinde ikili bir yargılama/cezalandırma sürecini, dolayısıyla birden fazla cezanın uygulanmasını dışlamamaktadır. Süreçlerin bir bütünün parçaları olacak biçimde bağlantılı yürütülmelerine ilişkin güvencelerin sağlanması halinde birden fazla cezanın uygulanması kanun koyucunun takdir yetkisindedir. Buna göre, cezalandırmaya ilişkin süreçlerin bağlantılı yürütülmesini dışlamayıp sadece birden fazla cezanın uygulanmasını ve bunların birleştirilmesine izin verilmemesini öngören kuralların aynı fiilden dolayı birden fazla yargılanmama veya cezalandırılmama ilkesine aykırı bir yönü bulunmamaktadır."*

Belirtmek gerekir ki, Anayasa Mahkemesi'nin Anayasa'ya aykırı olmadığına kanaat getirdiği bu hükümlerde hem idari yaptırımın hem de suç yaptırımının birlikte uygulanabileceği ayrıca düzenlenmiştir. Failin gerçekleştirdiği fiil nedeniyle hem suçtan hem de kabahatten dolayı yaptırım uygulanabileceğine ilişkin bir düzenleme ise KVKK ve ilgili diğer mevzuatta yer almamaktadır. Dolayısıyla gerçek kişi veri sorumlusunun bizzat kendisi tarafından gerçekleştirilen bir fiilin hem kabahat hem de suç oluşturduğu hallerde, genel hüküm niteliğindeki Kabahatler Kanununun 15/3 üncü maddesinin uygulama alanı bulacağı değerlendirilmektedir. Gerçek kişi veri sorumlusunun tek fiiliyle hem kabahat hem suç işlediği halde sadece suçtan dolayı yaptırım uygulanabilecektir.

Öte yandan, söz konusu Anayasa Mahkemesi kararında da belirtildiği üzere, kovuşturmaya yer olmadığı kararı ya da zamanaşımı nedeniyle düşme kararı gibi ilgili kişinin cezai sorumluluğuyla ilgili değerlendirmeleri içermeyen kararların beraat kararı olarak nitelendirilemeyecek olması nedeniyle, bu gibi durumlarda Kurul tarafından veri sorumlusu gerçek kişi hakkında idari yaptırım uygulanabileceği değerlendirilmektedir.

Kabahatler Kanununun 9 uncu maddesine göre kabahatler hem kast hem de taksirle işlenebilirken, TCK'nın 22/1 nci maddesine göre bir suçun taksirli hali ancak kanunda açıkça suç olarak düzenleniyorsa cezalandırılır. TCK 135 ve devamında yer alan suç tiplerinin taksirli hali ise kanunda düzenlenmemiş olup ancak *doğrudan kastla* işlenebilecekleri yukarıda açıklanmıştı. Dolayısıyla, taksirle işlenen bir fiilin varlığında suç tiplerinin oluştuğundan bahsedilemeyeceğinden kabahatten yaptırım uygulanması gerekmektedir. Söz konusu fiilin suç oluşturması için failin, fiili doğrudan kastla gerçekleştirmesi gerekmektedir. Aksi halde suç oluşmayacağından KVKK'da yer alan yaptırımlar uygulama alanı bulacaktır.

Öte yandan Kabahatler Kanunu madde 15/3 gereği suçtan dolayı yaptırım uygulanamayan hallerde kabahat dolayısıyla yaptırım uygulanacağı düzenleme altına alınmıştır. Eğer fiilde bir hukuka uygunluk nedeni bulunuyorsa, zamanaşımına uğramışsa, şikâyete bağlı suçta şikâyet şartı gerçekleşmemişse *suçtan dolayı yaptırım uygulanamayan hal* söz konusu olacaktır (Ketizmen ve Kart, 2021). Ancak TCK 135-136-138'de düzenlenen suçların soruşturulmasının ve kovuşturulmasının şikâyete bağlı kılınmadığı göz önünde bulundurulduğunda; bu suçlar bakımından şikâyetin yokluğu, suçtan dolayı yaptırım uygulanamayan bir halin doğumuna yol açmayacak ve bu durumda Kurulun suç teşkil eden fiil hakkında şikâyette bulunulmadığı gerekçesiyle inceleme yürüterek yaptırım uygulaması mümkün olmayacaktır. Çünkü suç teşkil eden fiil şikâyete bağlı olmadığından her zaman re'sen soruşturulabilecektir. TCK'da yer alan 6 aylık şikâyet süresi re'sen soruşturulan bu hükümler bakımından uygulanmayacak olduğundan suç teşkil eden fiil her an suçtan dolayı yaptırım uygulanabilir nitelikte olmaya devam edecektir.

SONUÇ

Hukuka özel aykırılık unsuru içeren TCK 135 ve devamındaki suç tipleri ancak *doğrudan kastla* işlenebilecek olup bu durum kabahat ve suçlar arasında non bis in idem ilkesi bakımından yapılacak değerlendirmede önem arz etmektedir. Zira, gerçek kişi veri sorumlusunun kişisel veri ihlali teşkil eden fiili doğrudan kast ile işlemediği hallerde suç oluşmayacağından KVKK'da düzenlenen kabahatlerden yaptırım uygulanması söz konusu olacaktır. Aynı şekilde gerçek kişi veri sorumlusu tarafından fiilin taksirle işlenmesi halinde de suç oluşmayacağından kabahatten yaptırım uygulanabilecektir. Diğer taraftan, gerçek veya tüzel kişi veri sorumlusu bünyesinde çalışan kişiler tarafından KVKK ihlalinin gerçekleştirildiği ihtimalde ise çalışan kişinin fiili suç oluştursa dahi veri sorumlusu hakkında idari yaptırım uygulanabilecektir. Çünkü suç işleyen gerçek kişi çalışan ile kabahat işleyen veri sorumlusunun fiilleri farklılık göstermekte olup farklı fiiller nedeniyle, farklı kişilere farklı cezaların uygulanmasının önünde bir engel bulunmamaktadır. Öte yandan, aynı zamanda hem suç hem de kabahat teşkil eden fiilin gerçek kişi veri sorumlusunun bizzat kendisi tarafından işlenmesi halinde ise 5326 sayılı Kabahatler Kanununun 15/3 üncü maddesi kapsamında sadece suçtan dolayı yaptırım uygulanabileceği değerlendirilmekte olup ancak suçtan dolayı yaptırım uygulanamayan hallerde KVKK'nın 18 inci maddesinde yer alan kabahatler kapsamında idari para cezası uygulanabilecektir. ◆

KAYNAKÇA

- Ünver, Y. (2008). Kişisel Verilerin Korunması. Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Cilt No: 1, s. 163-196.
- Orhan, U. (2021). Kişisel Verilerin Korunmasına İlişkin Türk Ceza Hukuku Düzenlemeleri Üzerine Değerlendirmeler. Ankara Üniversitesi Hukuk Fakültesi Dergisi, Sayı:70(4), ss. 1359-1384.
- Dülger, M.V. (2016). Kişisel Verilerin Korunması kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, Sayı 3 (2), ss.101-167.
- Kangal, Z. (2019). Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması, İstanbul, On iki levha Yayınları.
- Dülger, M.V. (2019). Kişisel Verilerin Korunması Hukuku, İstanbul, Hukuk Akademisi Yayınları.
- Sınar, H. (2020). Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu. Kişisel Verileri Koruma Dergisi, Cilt 2 Sayı 1, ss. 33-62.
- Koca, M., Üzülmez, İ. (2019). Kişisel Verilerin Kaydedilmesi Suçu. D.E.Ü. Hukuk Fakültesi Dergisi Prof. Dr. Durmuş TEZCAN'a Armağan, C.21 Özel S., ss. 69-93.
- Koca, M. Üzülmez, İ. (2017). Türk Ceza Hukuku Genel Hükümler, Ankara, Seçkin Yayıncılık.
- Korkmaz, İ. (2017). Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Ankara, Seçkin Yayıncılık.
- Sert, Ş. (2019). Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması. Ankara, Seçkin Yayıncılık.
- Görkemli, B. (2020). Türk Ceza Hukukunda Kişisel Verilerin Kaydedilmesi Suçu, Ceza Hukuku Dergisi, Cilt 15 Sayı 44, ss. 967-995.

◊ Kişisel Verileri Koruma Kurumu, "Alenileştirme Hakkında Kamuoyu Duyurusu", https://kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU. 04.09.2022.

◊ Göçmen Uyarer, S. (2019). 6698 sayılı Kişisel Verilerin Korunması Kanunu ve 5237 sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması (Yayımlanmış Yüksek Lisans Tezi). Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

◊ Aydın, S.E. (2015). AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, İstanbul, On İki Levha Yayıncılık.

◊ Hafizoğulları, Z., Özen, M. (2014). Türk Ceza Hukuku Genel Hükümler, Ankara, US-A Yayıncılık.

◊ Göktürk, N. (2016). Suçun Yasal Tanımında Yer Alan 'Hukuka Aykırılık' İfadesinin İcra Ettiği Fonksiyon. İnönü Üniversitesi Hukuk Fakültesi Dergisi Cilt 7 Sayı 1, ss.407-450.

◊ Özgenç, İ. (2019). Türk Ceza Hukuku Genel Hükümler, Ankara, Seçkin Yayınları.

◊ Kayıhan, İ. (2020). Ceza Hukuku Açısından Kişisel Verilerin Korunmasında Kişisel Veri ve Hukuka Aykırılık Kavramları. İstanbul Barosu Dergisi, Sayı: 2, ss.16-23.

◊ Akdağ, H. (2010). Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması (Yayımlanmış Yüksek Lisans Tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

◊ Göktürk, N. (2014). Türk Hukuku'nda Suçların İçtimaı. Ceza Hukuku ve Kriminoloji Dergisi, Cilt 2 Sayı 1-2, ss.31-59.

◊ Değirmenci, O. (2005) 2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi. TBB Dergisi, Sayı 58, ss.195-208.

◊ Çakır, K. (2020). Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135). Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, Cilt:8 Sayı: 16, ss. 569-596.

◊ Ketizmen, M., Kart, A. (2021). Kişisel Verilerin Korunması Kanununun 17. Maddesi ve Yargıtay Kararları Doğrultusunda, Kişisel Verilerin Korunmasına İlişkin Suç Teşkil Eden Fiiller Açısından Uygulanacak Norm Hakkında Değerlendirme. Kırıkkale Hukuk Mecmuası, Cilt:1 Sayı:2, ss. 256-268.

◊ Pehlivan, A. (2020). Kabahatler Hukukunun Genel Esasları. İstanbul, Beta Yayıncılık.

◊ Akbulut, B. (2014). Türk Ceza Kanunu ile Kabahatler Kanunu Hükümlerinin Yaptırım Hükümleri Dışında Karşılaştırmalı Olarak İncelenmesi. Adalet Yayınevi.

◊ Horozgil, D. (2021). AİHM ve Anayasa Mahkemesi Kararları Işığında Vergi Cezalarında Non Bis In Idem İlkesi. TBB Dergisi, Sayı: 157, ss. 255-294.

KABAHATLER KANUNU KAPSAMINDA 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU'NDAKİ İDARİ YAPTIRIMLAR

Mahsum GÖNEN

Kişisel Verileri Koruma Uzmanı

"Bu çalışma, 14.02.2023 tarihinde kabul edilen "Kabahatler Kanunu Kapsamında 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndaki Kabahatler" başlıklı uzmanlık tezinden alınmıştır."

GİRİŞ

Bilgi ve iletişim teknolojilerinin gelişmesi ve internetin yaygınlaşmasıyla ortaya çıkan dijitalleşme süreci ile birlikte veriler, dijital ortama aktarılmaya başlanarak kişisel verilerin toplanması, saklanması ve kişiler, kuruluşlar ve hatta ülkeler arasında paylaşılması günden güne kolaylaşmıştır. Bu durum, birtakım kolaylıklar ya da avantajlar sağlamış olsa da kişisel veri işleme faaliyetinde bulunanlar ile kişisel verisi işlenen kişiler arasındaki menfaat dengesini ilgili kişiler aleyhine bozmuş ve kişisel verilerin istismar edilme riskini beraberinde getirmiştir. Böylece, ilgili kişilerin maddi ve manevi varlıkları tehlikeye girmeye başlamış olup çıkarlarının korunması ihtiyacı ortaya çıkmıştır. 1970'li yıllardan itibaren başta Avrupa ülkeleri olmak üzere uluslararası hukukta bu konuda tartışmalar başlamış olup akabinde çeşitli uluslararası düzenlemelerle ilk olarak özel hayatın gizliliği kapsamında dolaylı olarak, daha sonraları ise gerek ulusal gerekse uluslararası düzenlemelerle temel hak ve özgürlükler bağlamında doğrudan kişisel verilerin korunması hakkı şeklinde tanımlanarak bireylerin kişisel verilerinin korunması hakkı hukuki güvenceye kavuşturulmuştur.

Ülkemizde, kişisel verilerin korunması hukukunun geçmişi çok uzun olmamakla birlikte 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin (108 sayılı Sözleşme) imzalanmasıyla beraber bu alan ülkemizin gündeminde yer almakta olup imzalandığı tarihten itibaren kişisel verilerin korunmasının yasal zeminde bir hak olarak tanımlanmasına yönelik süreçler yürütülmüştür. Yapılan çalışmalar neticesinde, 2010 yılındaki Anayasa değişikliğiyle birlikte kişisel verilerin korunması hakkı anayasal güvenceye kavuşturulmuş ve ardından 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun/6698 sayılı Kanun) yürürlüğe konulmuştur.

6698 sayılı Kanunda, veri sorumlularına birtakım yükümlülükler ve yükümlülüklerin yerine getirilmemesi durumunda uygulanacak idari yaptırımlar düzenlenmiştir. Kanunda idari para cezası ve idari tedbir yaptırımlarının uygulanması öngörülmüştür. Aydınlatma yükümlülüğüne, veri güvenliğine ilişkin yükümlülüklere, 15 inci madde uyarınca alınan Kişisel Verileri Koruma Kurulu (Kurul) kararlarına ve veri sorumluları siciline kayıt ve bildirim yükümlülüklerine aykırı davranılması durumunda ilgili veri sorumlusu hakkında idari para cezası yaptırımı uygulanması gündeme gelecektir. Diğer yandan; yürütülen inceleme neticesinde ihlalin varlığının anlaşılması hâlinde hukuka aykırılığın en geç 30 gün içerisinde giderilmesi noktasında veri sorumlusunun talimatlandırılması ve telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde ise veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulması yönünde karar alınması, diğer bir idari yaptırım türünden olan idari tedbir şeklinde karşımıza çıkmaktadır. Bu idari tedbir kararlarına uyulmaması durumunda ise bu kez 15 inci madde uyarınca alınan Kurul kararlarının yerine getirilmemesinden hareketle idari para cezası yaptırımı uygulanacaktır. İdari para cezaları, yalnızca veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanmaktadır. Burada kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının Kanundan muaf olduğu sonucu çıkarılmamalıdır. Zira bu durum, Kişisel Verileri Koruma Kurumu'nun bağımsız idari otorite vasfi ile tutarlı olmayacaktır. Bu bakımdan, idari yaptırıma kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi durumunda ise ilgili görevli/ler hakkında disiplin hükümlerine göre işlem yapılması ve sonucundan Kurula bilgi verilmesi gerekmektedir.

Kanun gerekçesinde, kabahatlerle ilgili hüküm bulunmayan hâllerde genel kanun niteliğindeki Kabahatler Kanunu hükümlerinin uygulanacağı ifade edilmiştir. Nitekim Kabahatler Kanunu'nun 3'üncü maddesi uyarınca Kabahatler Kanunu'nun özel kanunlarda düzenlenen kabahatler bakımından genel kanun niteliğinde olması sebebiyle Kabahatler Kanunu'nda sayılan genel ilkeler, Kanunda tanımlı idari yaptırıma konu fiiller hakkında da geçerlilik arz etmektedir.

Bu çalışmada, 6698 sayılı Kanunda düzenlenen kabahatler ve idari yaptırım türleri incelenerek konu hakkında bilgiler verilmesi amaçlanmaktadır. Bu doğrultuda, Kabahatler Kanunu'nun genel ilkelerinin düzenlendiği ilgili maddeleri üzerinde durularak bu maddelerin Kanunda düzenlenen kabahatler ve idari yaptırımlar bakımından incelemesi yapılacaktır. Bu kapsamda Kanunda düzenlenen kabahatler ve idari yaptırım türleri incelenecek, idari para cezası miktarı belirlenirken göz önünde bulundurulması gereken hususların nasıl değerlendirilmesi gerektiği örneklerle açıklanacak ve Kurulun bu yetkisini kullanırken nelere dikkat ettiği üzerinde durulacaktır. Bununla birlikte, idari yaptırım kararı ve idari yaptırım kararına karşı başvuru yolları hakkında bilgiler verilerek değerlendirmelerde bulunulacaktır.

AYDINLATMA YÜKÜMLÜLÜĞÜ

Aydınlatma, kişisel verilerin elde edilmesi sırasında veri sorumluları ya da yetkilendirdiği kişiler tarafından kişisel verilerin kim tarafından, hangi amaçlarla ve hukuki sebeplerle işlenebileceği, kimlere hangi amaçlarla aktarılabileceği konularında ilgili kişilerin bilgilendirilmesi anlamına gelmekte olup Kanun 10'uncu maddesinde *(Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür.)* bir yükümlülük olarak tanımlanmıştır. Aydınlatma yükümlülüğünün amacı, ilgili kişilerin var olan haklarıyla ilgili olarak bilgilendirilerek, kişisel verileri üzerindeki hakimiyetlerini tamamen yitirmelerini önlemek ve kişisel verileri üzerindeki kontrol gücünü artırmaktır. Bu sebeple aydınlatma yükümlülüğünün varlığı, şeffaflık ilkesinin bir gereği olup şeffaflığın şartının da ilgili kişinin anlaşılabilir bir şekilde bilgilendirilmesidir. Bu yükümlülük, ilgili kişinin talebine istinaden yerine getirilmesi gereken bir yükümlülük olmayıp veri sorumlusunun özen yükümlülüğü bulunmaktadır. Bu doğrultuda hazırlanan bir aydınlatma metninin, yapılan işlem bazında kullanılan kişisel verilerine ilişkin ilgili kişilere bilgilendirme sağlaması beklenmektedir. Bu yükümlülük, yalnızca ilgili kişinin korunması ve bilgilendirilmesi bakımından olumlu olmakla kalmayıp aynı zamanda ilgili kişiye ait kişisel verilerin işleme faaliyeti ile ilgili olarak veri sorumlusu için bir kontrol mekanizması niteliğinde olması itibariyle veri sorumlusunun da yararınadır (Çekin, 2020).

Kanun'un 10'uncu maddesinde, aydınlatma yükümlülüğünün ne şekilde yerine getirileceğine dair detaylar mevcut değildir. Kurul tarafından, Kanun'un 10'uncu maddesinde yer alan mezkûr düzenlemenin uygulamada anlaşılabilir kılınması amacıyla Aydınlatma Yükümlülüğün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği (Aydınlatma Tebliği) yayımlanmıştır. Kanunda bilgilendirme yapılması istenen beş konu ile ilgili olarak Aydınlatma Tebliği'nde "asgari" olarak bu konularda bilgilendirme yapılması gerektiği belirtilmiştir. Bu itibarla, sayılan konuların tamamı hakkında mutlak surette bilgilendirme yapılması gerekmekte olup ayrıca kişisel verilerin elde edilmesi esnasında başka konularda da bilgilendirmede bulunulması gerekiyorsa bu bilgilendirmenin de yapılması gerekmektedir.

VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLER

Kişisel verilerin korunması alanının temeli, kişisel verilerin güvenli bir şekilde işlenmesidir. Veri sorumluları ve veri işleyenler, kişisel verilerin hukuka uygun bir biçimde işlenebilmesi adına kişisel verilerin ilk elde edildiği andan itibaren her aşamada gerekli önlemleri alarak yeterli güvenliği sağlamak zorundadır. Unutulmamalıdır ki, güvenliğin sağlanması bir aşamaya veya veriye özgü değil, süregelen bir sorumluluktur. Bu nedenle, veri güvenliğiyle ilgili tedbirlerin belirlenmesi ve uygulanması ile sadece bir kez yetinmek yeterli değildir. Veri sorumluları tarafından alınan önlemler, değişen ve gelişen teknolojiler ve mevcut güvenlik uygulamaları dikkate alınarak güncellenmelidir (Dülger, 2019). Aksi takdirde yeterli güvenlik önlemlerinin alındığı söylenemeyecek olup kişisel verilere yetkisiz bir biçimde erişilmesi, hukuka uygun olmayan bir biçimde aktarılması ve kişisel verilerin kaybolması durumları meydana gelebilir ve bu da ilgili kişinin hak kaybının doğmasına neden olabilir.

Veri güvenliği kısaca kişisel verilerin yetkisiz üçüncü kişiler tarafından erişilmesinin önüne geçilmesi anlamına gelmekte olup Kanun'un 12'nci maddesinde *("(1) Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. (2) "Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur. (3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. (4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder. (5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.")* veri güvenliği konusunda yerine getirilmesi gereken birtakım yükümlülükler düzenlenmiştir. Kanun'un 12'nci maddesine bakıldığında bu yükümlülüklerin; teknik ve idari tedbirler alma yükümlülüğü, denetim yapma yükümlülüğü, sır saklama yükümlülüğü ile ilgili kişi ve Kurula bildirim yükümlülüğü olmak üzere dört adet yükümlülük olduğundan bahsedilebilir.

Kişisel veri güvenliğinin ne şekilde sağlanacağına ilişkin veri sorumlularına yol gösterici olması bakımından ise Kurul tarafından "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)" hazırlanıp yayımlanmıştır.

KURUL KARARLARININ YERİNE GETİRİLMESİ YÜKÜMLÜLÜĞÜ

Kurul kararları, Kurul tarafından alınan kararları ifade etmekte olup görev alanına giren konulara ilişkin inceleme yürütmesi ile ilgili olarak Kurulun incelemenin usul ve esaslarının düzenlendiği Kanun'un 15'inci maddesinde *("(1)Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar. (2) 1/11/1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde belirtilen şartları taşımayan ihbar veya şikâyetler incelemeye alınmaz. (3) Devlet sırrı niteliğindeki bilgi ve belgeler hariç; veri sorumlusu, Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri on beş gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadır. (4)Şikâyet üzerine Kurul, talebi inceleyerek ilgililere bir cevap verir. Şikâyet tarihinden itibaren altmış gün içinde cevap verilmezse talep reddedilmiş sayılır. (5) Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir. (6) Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin yaygın olduğunun tespit edilmesi hâlinde Kurul, bu konuda ilke kararı alır ve bu kararı yayımlar. Kurul, ilke kararı almadan önce ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşlerini de alabilir. (7) Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verebilir.")* kapsamında verdiği kararların yerine getirilmesi, veri sorumlusunun bir yükümlülüğüdür.

VERİ SORUMLULARI SİCİLİNE KAYIT VE BİLDİRİM YÜKÜMLÜLÜĞÜ

Kişisel verilerin korunması bağlamında şeffaflık ilkesi önem arz etmektedir. Teknolojide meydana gelen gelişmeler neticesinde çeşitliliği artan kişisel veri işleme faaliyetleri karşısında şeffaflık ilkesine dikkat edilmesi ihtiyacı her geçen gün artmaktadır. Bu amaca hizmet etmesi amacıyla kanun koyucu tarafından Kanun'un 16'ncı maddesinde *("(1) Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulur. (2) Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir. (3) Veri Sorumluları Siciline kayıt başvurusu aşağıdaki hususları içeren bir bildirimle yapılır: a) Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri. b) Kişisel verilerin hangi amaçla işleneceği. c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar. ç) Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları. d) Yabancı ülkelere aktarımı öngörülen kişisel veriler. e) Kişisel veri güvenliğine ilişkin alınan tedbirler. f) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre. (4) Üçüncü fıkra uyarınca verilen bilgilerde meydana gelen değişiklikler derhâl Başkanlığa bildirilir. (5)Veri Sorumluları Siciline ilişkin diğer usul ve esaslar yönetmelikle düzenlenir.")* ile veri sorumluları sicilinin oluşturulması öngörülmüştür. Bu sebeple herkesçe sicilin incelenebilmesi mümkün olup kimlerin veri sorumlusu olduğu görülebilecektir. Böylece, anayasada tanımlı bir hak olan kişisel verilerin korunması hakkının tesisine ve hak ihlallerinin önüne geçilmesine katkıda bulunacaktır. Veri sorumluları sicili ise kural olarak veri sorumluları tarafından kişisel veri işleme faaliyetine başlamadan önce kayıt olunması ve kişisel verileri işleme faaliyetine dair bilgilerin beyan edilmesi gerekli olan kamuya açık bir kayıt sistemi olup veri sorumlularının kural olarak sicile kayıt ve bildirim yükümlülüğü bulunmaktadır (Kişisel Verileri Koruma Kurumu, Veri Sorumluları Sicili, 2018). Bu amaçla, Veri Sorumluları Sicil Bilgi Sistemi ("VERBİS") oluşturulmuştur. Kanun'un 16'ncı maddesinin ikinci fıkrasındaki hükme istinaden Kurul tarafından veri sorumluları sicili kaydına ilişkin objektif kriterler belirlenmiş olup anılan maddenin beşinci fıkrasına istinaden içeriği Kurul tarafından düzenleyici işlemle doldurulması suretiyle hazırlanıp 30.12.2017 tarihli Resmî Gazete'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelikte (Sicil Yönetmeliği) bu kriterler sayılmıştır. Belirtmek gerekir ki; sicile kayıt yükümlülüğüne muafiyet getirilmiş olması, veri sorumlusu tarafından hiçbir suretle Kanunda tanımlı diğer yükümlülüklerin yerine getirilmesine gerek olmadığı şeklinde yorumlanmamalıdır.

YER BAKIMINDAN UYGULANMASI

Kişisel veri işleme faaliyetinin günümüzde uluslararası düzeyde rahatça gerçekleşmesi sebebiyle kabahatin işlendiği yerin ve idari yaptırıma dair düzenlemelerin yer bakımından uygulanması hususunun önem arz ettiği anlaşılmaktadır. Nitekim bu konu Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR) coğrafi bakımından kapsamı, Avrupa Birliği'nde de tartışılan önemli konulardan bir tanesidir. 6698 sayılı Kanunda yer bakımından uygulama kapsamına ilişkin açık bir düzenleme bulunmamaktadır. Bu durumda KK 6'ncı maddeye *(5237 sayılı Türk Ceza Kanununun yer bakımından uygulamaya ilişkin 8 inci maddesi hükümleri, kabahatler bakımından da uygulanır. Ancak, kanunlarda aksine hüküm bulunan haller saklıdır.)* ve TCK'ye göre esas olan mülkilik ilkesi ortaya çıkmaktadır. Fakat, kişisel verilerin korunması hukukunun geldiği ve bu denli hızlı bir değişimin yaşandığı noktada, aslında mülkilik ilkesinin sınırlarının esnek tutularak yorumlanması gerektiği değerlendirilmektedir. Zira, kişisel verilerin korunması hakkının AY. 20'nci maddenin üçüncü fıkrasındabir temel hak ve özgürlük olarak düzenlenmesi, sınır ötesi işlemeye olanak sağlayan tekniklerin yaygınlaşması nedenleriyle mülkilik ilkesinin katı bir şekilde yorumlanmasının bu hakkın korunması amacına hizmet bakımından eksiklik meydana getirebileceği değerlendirilmektedir. Bu anlamda da Kanun vasıtasıyla ilgili kişilere mümkün olabilecek en geniş kapsamda korumanın sağlanması gereğinden hareketle mülkilik ilkesi esnek yorumlanmalıdır. Diğer bir deyişle, Kanunun *"mülkilik ilkesi"*ne uygun olarak yalnızca ulusal sınırlar içerisinde gerçekleştirilen işleme faaliyetleri bakımından uygulama alanı bulacağının kabulünün etkin bir veri koruma hukuku uygulamasını temin etme amacına hizmet etmeyeceği, Kanun vasıtasıyla ilgili kişilere mümkün olabilecek en geniş kapsamda korumanın sağlanması gerektiği değerlendirilmektedir (Kişisel Verileri Koruma Kurumu, Çarşamba Semineri, 2021).

İCRAİ VEYA İHMALİ DAVRANIŞLA İŞLENMESİ

Kabahatin icrai veya ihmali davranışla işlenmesi bakımından ise KK 7'nci maddede yer alan düzenlemeye göre, bir eylemin yapılması yahut yapılmaması bir kanun hükmü ile yasak edilmiş olmasına karşın söz konusu eylemde bulunulması durumunda, bir kabahatin işlendiğinden bahsedilebilecektir. Ancak, kabahatin ihmalen işlendiğinden bahsedilebilmesi için o eylemin yapılması gerektiği konusunda bir yükümlülük olmalıdır. Ayrıca bu düzenleme, kanunda icrai bir eylemle işlenebileceği öngörülen bir kabahatin ihmali olarak da işlenmesi durumunda sorumluluğun şartlarının kanunda yer almasının gerekmesi sebebiyle kanunilik ilkesi ile bağdaşmaktadır. Bu şart ise hukuki yükümlülüğün olması olarak tanımlanmıştır (Akbulut, 2010).

Bilindiği üzere kabahatlerin, icrai ya da ihmali hareketle işlenebilmesi mümkündür. Aydınlatma yükümlülüğünün yerine getirilmemesi kabahati, ancak ihmali hareket ile meydana gelebilir. Çünkü Kanunda, aydınlatmanın yapılması yükümlülüğü tanımlanmış yani belli bir icrai davranışta bulunma yükümlülüğü mevcut olup bu eylemin yerine getirilmemesi yani ilgili kişinin kişisel verileri elde edilirken Kanunda sayılı hususlarda bilgilendirmede bulunulmaması yaptırıma bağlanmıştır. Dolayısıyla mezkûr kabahatin icrai hareketle işlenemeyeceğinden bahsedilebilir (Kangal, Kişisel Verilerin Ceza ve Kabahatler Bakımından Korunması, 2019).

Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi kabahati, icrai veya ihmali hareket ile meydana gelebilir. Şöyle ki; teknik ve idari tedbirler alma yükümlülüğü, denetim yapma yükümlülüğü ve ilgili kişi ile Kurula bildirim yükümlülüğü eyleminin yerine getirilmemesi ihmali bir hareket olup bunun yerine getirilmemesi yaptırıma bağlanmıştır. Diğer taraftan sır saklama yükümlülüğünün yerine getirilmemesi ise icrai bir eylemle meydana gelebilecek olup bu kapsamda veri güvenliğine ilişkin yükümlülüğüne muhalefet edilebilecektir.

Kanun'un 15'inci maddesiuyarınca Kurul tarafından verilen kararların yerine getirilmemesi kabahati, icrai veya ihmali hareket ile meydana gelebilir. Örneğin; veri sorumlusu, Kurul tarafından istenen hukuka aykırılığın giderilmesi konusundaki kararına dair herhangi bir işlem tesis edilmemesi ihmali bir hareket olup bunun yerine getirilmemesi yaptırıma bağlanmıştır. Diğer taraftan veri işleme veya aktarım faaliyetinin durdurulmasına karar verilmiş olmasına karşın veri sorumlusu tarafından bu karara uyulmayıp söz konusu eylemlere devam edilmesi durumunda ise bahse konu kabahat icrai bir eylemle meydana gelebilecek olup bu kapsamda mezkûr kararın yerine getirilmesi yükümlülüğüne aykırı bir davranış sergilenmiş olacaktır (Kangal, Kişisel Verilerin Ceza ve Kabahatler Bakımından Korunması, 2019).

Veri sorumluları siciline kayıt ve bildirim yükümlülüğünün yerine getirilmemesi kabahati, tıpkı aydınlatma yükümlülüğünün yerine getirilmemesi kabahatinde olduğu gibi ancak ihmali hareket ile meydana gelebilir. Çünkü Kanun kayıt ve bildirimin yapılması yükümlülüğünü tanımlamış olup bu eylemin yerine getirilmemesini yaptırıma bağlamıştır.

KAST VEYA TAKSİRLE İŞLENEBİLMESİ DURUMLARI

KK 9'uncu maddeye göre kanunda açıkça hüküm bulunmayan hâllerde, kabahatlerin kasten yahut taksirle işlenebilmesi mümkün olup diğer bir deyişle kabahatlerin taksirle de işlenebileceği düzenleme altına alınmıştır. Bu düzenlemeye göre bir eyleme kabahat denilebilmesi için kural olarak bu eylemin kasten ya da taksirle işlenmiş olması gerekir. Yani, kabahate konu eylem bakımından kasten ya da taksirle hareket edilmesinin bir önemi bulunmamaktadır.

Buradan hareketle Kanunda tanımlı kabahatler incelendiğinde, Kanunda açıkça hüküm bulunmadığından ötürü Kanun kapsamında tesis edilen idari yaptırıma konu eylemlerin kast veya taksirle işlenmesi mümkündür. Fakat, bu eylemlerin kast veya taksirle işlenip işlenmediği hususu örneğin uygulanacak idari para cezası miktarı belirlenirken aşağıda da değinilecek olan KK 17'nci maddenin ikinci fıkrası kapsamında kast veya taksirin olup olmadığı dikkate alınmalıdır (Kangal, Kişisel Verilerin Ceza ve Kabahatler Bakımından Korunması, 2019).

TEŞEBBÜS

KK 13'üncü madde, teşebbüs hâlinin cezalandırılması için kanunda hüküm bulunması gerektiğini belirtmiştir. Bu minvalde, Kanun kapsamında tesis edilen idari yaptırımlara konu eylemlere teşebbüs edilmesi kabahat olarak düzenlenmediğinden dolayı bu eylemlere teşebbüs edilmesi durumunda idari yaptırım uygulanamayacaktır.

İDARİ YAPTIRIM

İdari yaptırımın idari bir organın görevlerini yerine getirmesi durumunda idari görev dahilinde yer alan hususlarda yapılan aykırılıklar için yargı kararı olmaksızın verilebileceği yaptırım şeklinde tanımlanabilmesi mümkündür. KK 16'ncı maddeye göre, işlenen kabahat neticesinde idare tarafından idari yaptırım niteliğindeki idari para cezası ile idari tedbirler yaptırımı uygulanabilecektir. Belirtmek gerekir ki idari tedbirler ifadesinden, mülkiyetin kamuya geçirilmesi ile ilgili kanunlarda yer alan diğer tedbirler anlaşılmalıdır.

6698 sayılı Kanuna bakıldığında, yukarıda da arz edildiği üzere 18'inci maddenin birinci fıkrasında aydınlatma yükümlülüğünün yerine getirilmemesi, veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi, 15'inci madde uyarınca Kurul kararlarının yerine getirilmemesi ve Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı davranılması kabahatleri idari para cezası yaptırımına bağlanmıştır. Diğer taraftan Kanunun 15'inci maddesi kapsamında inceleme neticesinde ihlalin varlığının tespiti durumunda bu hukuka aykırılığın giderilmesi yönünde verilen talimatlandırma kararı ile telafisi güç/imkânsız zararların doğması ve açıkça hukuka aykırılık olması durumunda tedbir amaçlı uygulanan veri

işlemenin durdurulması kararı bir idari tedbir kararı olup idari yaptırım türü olarak karşımıza çıkmaktadır.

İdari yaptırım konusunun daha net anlaşılabilmesi adına idari para cezası ile idari tedbir yaptırımı niteliğindeki hukuka aykırılığın giderilmesine yönelik talimatlandırma kararları ve veri işleme faaliyetlerinin durdurulması kararları ayrı ayrı ele alınacaktır.

İdari Para Cezaları

Kanun'un 18'inci maddesinin birinci fikrasındatanımlı kabahatlere ilişkin öngörülen alt ve üst sınır geniş tutulmuş olup madde gerekçesine bakıldığında kanun koyucu tarafından kasıtlı olarak bu yola gidildiği anlaşılmaktadır. Kanun kapsamında uygulanacak yaptırım miktarı, genel kanun niteliğindeki KK'nin ilgili hükmü çerçevesinde değerlendirilerek belirlenmelidir. KK 17'nci maddenin ikinci fikrasına göre idari para cezalarının kanunda alt ve üst sınırı gösterilerek belirlendiği hâllerde kabahat olarak tanımlanan eylem için yaptırım tutarı;

» İşlenen kabahatin haksızlık içeriği,
» Failin kusuru,
» Failin ekonomik durumu

birlikte göz önünde bulundurularak tayin edilir. Buna göre, idari para cezası yaptırımına, belirtilen kriterlerin gözetilerek karar verilmesi ve idareye tanınan takdir yetkisinin ise hukuka uygun olarak kullanıldığına dair yargısal denetimin yapılabilecek bir biçimde kullanılması gerekmektedir.

İdari para cezalarının alt ve üst sınır gösterilerek belirlenen durumlarda, alt sınırdan uzaklaşılarak idari para cezası verilebilmesi için haklı bir nedenin mevcut olması ve idari merciin somut bir biçimde bu nedeni gerekçelendirmesi önem arz etmektedir. Aksi hâlde şüphesiz ki idari mercii tarafından hukuka aykırı ve ölçüsüz bir ceza tesis edilmiş olacaktır. Kabahatin işlenmesi, kanunda öngörülen alt sınırdan ceza tayin edilmesi için yeterli olmasına karşın alt sınırın üzerinde bir miktar belirlenebilmesi için bu kabahatin işlenmesinin yanında alt sınırdan uzaklaşılması nedeninin olması gerekmektedir.

Kanunda tanımlı idari para cezası yaptırımlarının uygulanış biçimi, KK 17'nci maddenin ikinci fikrası kapsamında şu şekilde ele alınabilir:

a. Kabahatin Haksızlık İçeriği: İdari para cezalarının alt ve üst sınırlarının belirlenmesinde en önemli husus, kabahatlerin haksızlık içeriğidir (Kangal, Kabahatler Hukuku, 2019). Bu ifade, Kurul tarafından yürütülen inceleme konusu ihlalin mevzuata aykırılığın ölçüsünün yanında ihlal neticesinde meydana gelen sonuçları da kapsamaktadır. Burada, elde edilen menfaatin ya da kabahat konusunun veya koruduğu hukuki değerin türü ve önemi ile konuya veya hukuki değere yönelik zarar veya tehlikenin kapsamı ve boyutu önemlidir. Bu durumda, veri sorumlusuna isnat edilen eylemin, kendisine yüklenen yükümlülükleri ne boyutta ihlal ettiğinin ele alınması önem arz etmektedir. Örneğin, kabahatin icrai bir hareket ile işlenmesi ile ihmali bir hareket ile işlenmesi arasında bir fark bulunmaktadır. Benzer şekilde kabahatin işlenmesinde hangi araçların kullanıldığı, yani daha fazla sayıda kişinin işlenen kabahatin mağduru olacak şekilde bir davranış sergilenip sergilenmediği hususu kabahatin haksızlık içeriği bakımından değerlendirme yapılmasında önemli bir rol oynamaktadır. Bunun yanında, alt sınırdan uzaklaşılmasını sağlayacak olan özel nitelikli kişisel veriler dâhil kişisel veri kategorileri, kabahatten etkilenen kişi sayısı ile etkilenen kişilerin uğradığı ve/veya uğraması muhtemel zararın boyutu, kabahatin işlenmesinden sonraki süreçte veri sorumlusunun olumlu/olumsuz davranışı, veri sorumlusu tarafından daha önce incelemeye konu kabahatin ve/veya Kanun'un 18'inci maddesinin birinci fikrasındatanımlı diğer kabahatlerin işlenip işlenmediği, işlenen kabahatten Kurulun haberdar olma biçimi, kabahatin işlenmesindeki amacın ne olduğu gibi hususların kabahatlerin haksızlık içeriği değerlendirmesinde göz önünde bulundurulması gerekmektedir. Bunun yanında, veri sorumlusuna isnat edilen eylemin hukuka aykırılık boyutu durumunda, yerine getirilmesi gereken yükümlülüklere ne ölçüde uyulduğu ve veri sorumlusunun eksik veya yanlış olan bazı teşebbüslerde bulunup bulunmadığı değerlendirilmelidir. Aslında bir ihlalin hukuki sonuçları açısından kabahatin haksızlık içeriği, genel olarak Kanun'un 12'nci maddesinde tanımlı yükümlülüklere uyulmamasında ortaya çıkmaktadır. Zira Kanun kapsamında kişisel veri işleme faaliyetinin özünde bu yükümlülüklere uyulması yer almakta ve Kanuna aykırılık genel olarak bu yükümlülüklerin yerine getirilmemesinden kaynaklı olarak meydana gelmektedir. Bu yükümlülüklerin yerine getirilmemesi nedeniyle kişisel verileri ifşa olan ya da hukuka aykırı olarak ele geçirilen kişi sayısının fazla olması, veri ihlaline konu kişisel verilerin hassas niteliği ve bu verilerin üçüncü kişilerce öğrenilmesi sebebiyle ilgili kişinin maruz kaldığı ve/veya kalacağı muhtemel zararlar göz önünde bulundurularak idari para cezasının miktarı tayin edilmelidir. Benzer şekilde Kanun'un 10'uncu maddesinde tanımlı yükümlülük durumunda, bu yükümlülüğün yerine getirilmemesi ile eksik/hatalı yerine getirilmesi aynı ölçüde değerlendirilmemelidir. Aynı durum veri sorumluları siciline kayıt ve bildirim yükümlülüğünün yerine getirilmesi ve

veri güvenliğine ilişkin yükümlülüklerin yerine getirilmesi ile ilgili olarak da geçerlilik arz etmektedir (Altındağ, 2021). Özetle bu kriter; işlenen kabahatin zarara/zarar tehlikesine sebebiyet verip vermediği, bu kabahatin ne şekilde işlendiği, tek başına/birden fazla kişi tarafından işlenip işlenmediği gibi hususlara atıfta bulunmaktadır.

b. Veri Sorumlusunun Kusuru: KK'ye göre kabahatin kast veya taksirle işlenmesinin, sorumluluk bakımından herhangi bir farkı olmamakla birlikte, tayin edilecek ceza miktarının belirlenmesi için bu husus önem arz etmektedir. Örneğin, kabahatin kasten veya taksirle işlenip işlenmediğinin incelenmesi gerekir. Hem kast hem de taksirle işlenebilen kabahatin, kabahati işleyen tarafından kastla işlenmesi durumunda taksirle işlenmesine nazaran alt sınırdan daha uzak bir biçimde yaptırım uygulanmalıdır. Ayrıca Kanun'un 12'nci maddesinde tanımlı yükümlülüklerin veri sorumlusu tarafından ne ölçüde dikkate alındığı da kusur derecesini ortaya koyabilecek olup idari para cezası tayin edilirken göz önünde bulundurulmalıdır. TCK'de yer alan kusurun ortadan kaldırılmasına dair nedenler KK 12'nci maddesi gereği kabahatler için de geçerlidir. Bu minvalde TCK'de düzenlenen kusuru azaltan nedenler kabahatlerde uygulanamayacaktır. Ancak kusuru azaltan sebepler alt ve üst sınırları kanunla belirlenen idari para cezasının belirlenmesinde değerlendirilebilecektir. Özetle; veri sorumlusunun kusuruna ilişkin olarak veri sorumlusunun kabahati taksirle mi yoksa kasten mi işlediği gibi unsurlar dikkate alınmalıdır.

c. Veri Sorumlusunun Ekonomik Durumu: Düzenleyici cezaların caydırıcılığını sağlamanın bir yolu, cezaya çarptırılan veri sorumlusunun mali büyüklüğüne göre ceza miktarının tayin edilmesidir (Altındağ, 2021). İdari para cezasının belirlenmesinde failin ekonomik durumu önemli bir faktördür. Buna göre, idari para cezası belirlenirken failin geliri ve mal varlığının yanında ekonomik açıdan önemli diğer koşulları dikkate alınmalıdır. KK 17'nci maddenin ikinci fıkrasında tanımlı ilk iki kriteri aynı derecede olan fakat ekonomik büyüklükleri farklı olan iki veri sorumlusu tarafından aynı kabahatin işlenmesi hâlinde, yalnızca ekonomik büyüklüklerinden kaynaklı olarak farklı miktarlarda ceza miktarı belirlenmelidir. Nitekim Kanunda idari para cezalarına ilişkin alt ve üst sınırın bu denli geniş aralıklı olması bu yüzdendir. Ayrıca veri sorumlusunun gerçek kişi veya tüzel kişi olması, ödeme güçlerinin farklı olması sebebiyle önemli bir kriter olarak kabul edilmektedir. Ödeme gücünün zayıf olması durumunda idari para cezası alt sınıra yakın bir miktar belirlenecek şekilde değerlendirme yapılmalıdır. Burada veri sorumlusunun yalnızca ulusal çapta faaliyette bulunup bulunmadığı, birden fazla sektörde hizmet verip vermediği gibi hususlar akla gelmektedir. Veri sorumlusunun ekonomik durumu kapsamında geliri, yıllık cirosu, piyasadaki gücü, malvarlığı ve ekonomik açıdan önem taşıyan diğer koşullar (işletmelerinin sayısı, yaygınlığı, personel sayısı, hitap ettiği kitle, ulusal ve/veya uluslararası çapta faaliyet gösterme vb.) dikkate alınmalıdır.

İdari Tedbirler

İdari tedbir yaptırımının dayanağı Kanun'un 15'inci maddesidir. İdari tedbir yaptırımı, Kanun'un 15'inci maddenin beşinci ve yedinci fıkrasının uygulama alanı bulduğu durumda ortaya çıkmaktadır.

İlk olarak, Kanun'un 15'inci maddesinin beşinci fıkrasına bakıldığında, burada "ihlal" ifadesinin kullanıldığı görülmektedir. Yani yürütülen incelemede ihlalin varlığının anlaşılması hâlinde Kurul tarafından hukuka aykırılığın giderilmesi yönünde talimatlandırma kararı verilecek olup veri sorumlusu tarafından bu aykırılığın giderilmesi gerekmektedir. Giderilmemesi durumunda yani talimatlandırma kararının yerine getirilmemesi hâlinde bu kez Kanun'un 18'inci maddesinin birinci fıkrasının (c) bendi kapsamında idari para cezasının uygulanması gündeme gelebilecektir.

Kanun'un 15'inci maddesinin yedinci fıkrasındade ise veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulması kararı alınabileceğine dair düzenleme getirilmiştir. Bu kararın alınmasını müteakip veri sorumlusu tarafından bu durdurma eyleminin gerçekleştirilmesi gerekmektedir. Durdurulmaması durumunda bahse konu kabahat işlenmiş olacak ve bu kez Kanun'un 18'inci maddesinin birinci fıkrasının (c) bendi kapsamında idari para cezası uygulanabilecektir.

Kanun'un 15'inci maddesinin altıncı fıkrasında ise Kurulun ilke kararı alabileceği düzenlenmiştir. Belirtmek gerekir ki; ilke kararları, Kurul'un düzenleme yetkisini kullandığı adsız düzenleyici işlemlerden biridir. Şöyle ki; bilindiği üzere idare, kanunun çizdiği çerçeve dışına çıkmayacak şekilde yetkili olduğu hususlarda işlem tesis edebilir. Düzenleme yetkisi ise; idarenin genel, objektif, bireysel olmayan işlemler ölçütündeki tasarrufta bulunma yetkisi olarak tanımlanmaktadır (Duran, 1983). Kurul, düzenleyici işlem yetkisine Kanun'un 22'nci maddesinin birinci fıkrasının (e) bendi ile sahiptir. Kurul, düzenleyici işlemler aracılığıyla düzenleme yetkisini kullanır. Kurul, ilke kararı alarak yetkisine giren işleri yapmak üzere hukuka aykırı olmayan genel hükümler koymak suretiyle bunların uygulanmasını sağlamak amacıyla genel nitelikteki düzenleme getirme yetkisini kullanır. Kurul, ilke kararlarının alınması ile farklı şekillerde karşılaşılabilecek veri işlemeye ilişkin hukuka aykırı fiillere karşı kişisel verilerin korunması amacıyla

gerekli tedbirlerin alınmasını amaçlamaktadır (Schütz, 2012). Kurul, tespit ettiği yaygın ihlaller için yeni ilke kararları alabilir veya gerektiğinde önceki kararları günün ihtiyaçlarına göre düzeltebilir *("Danıştay, kamu hizmetine egemen ilkelerden biri olan uyarlama (değişkenlik) ilkesi uyarınca idarelerin düzenleme yetkisine sahip olduğu alanlarda, dönemin gereklerine ve toplumun gereksinimlerine şekilde uygulamalarını değiştirip, yeniden düzenleyebileceğini belirtmektedir.",* Danıştay, 2010). Kanun'un 18'inci maddesinin birinci fikrasının (c) bendi kapsamında değerlendirme yapılacak olursa, burada düzenlenen kabahatin konusunu birel idari işlemler oluşturmakta olup; Kurulun ilke kararına aykırı davranılmasına değil, yürütmüş olduğu inceleme neticesinde almış olduğu kararlara uyulmaması durumunda söz konusu kabahat işlenmiş olacaktır. Fakat ilke kararlarına aykırı bir davranış sergilenmesi Kurul tarafından göz ardı edilmemekte olup idari para cezası miktarı belirlenirken KK 17'nci maddesinin ikinci fikrasında yer alan hususlar çerçevesinde alt sınırdan uzaklaştırıcı bir neden olarak değerlendirilebilecektir.

İDARİ YAPTIRIM KARARLARINA KARŞI BAŞVURU YOLU

Kanun Tasarısının ilk hâlinde Kurulun vermiş olduğu idari yaptırım kararlarına karşı idare mahkemelerinin görevli olduğu açıkça düzenlenmiş olmasına karşın bu hüküm Alt Komisyon'da çıkarılmış olup idari yaptırımların KK'deki görev hükümlerine tabi olması benimsenmiştir. Fakat, KK'de tanımlanan kabahatlerin niteliğine ve bu kabahatler neticesinde uygulanması öngörülen idari para cezalarının miktarı ile Kurul tarafından ve hatta diğer düzenleyici ve denetleyici kurumların verdiği idari para cezalarının miktarı ile bu yaptırıma konu kabahatlerin oldukça büyük farklılıklar arz etmektedir. Zira KK, oluşturduğu etki bakımından daha hafif nitelikte eylemler ve yaptırımlar ile ilgilidir. Fakat Kurulun veya diğer düzenleyici ve denetleyici kurumların uyguladığı cezalar teknik ve uzmanlık bilgisine ihtiyaç olan, ihlalin değerlendirilmesi için kapsamlı bir inceleme gerektiren ve ihlalin anlaşılması durumunda KK'ye konu fiillere yönelik uygulanan yaptırımlara nazaran çok yüksek miktarda para cezalarının uygulandığı fiillerdir (Altındağ, 2021). Bunun yanında yargısal denetimin de daha geniş ve kapsamlı yürütülmesi gerekmektedir. Ayrıca diğer düzenleyici ve denetleyici kurumların vermiş olduğu idari para cezalarında görevli yargı yeri idari yargı olmasına karşın sadece Kurulun tayin ettiği idari para cezalarına karşı sulh ceza hakimlikleri görevlidir. Kanunda idari yaptırım kararlarına ilişkin ayrıca bir başvuru yeri gösterilmemiştir. Kanunda ayrıca bir düzenleme olmadığı için bu konuda genel kanun niteliği olan KK uygulanacaktır. KK 3'üncü maddesinin birinci fikrasının (a) bendi ile 27'nci maddesi gereğince, Kurul tarafından Kanun'un 18'inci maddesinin birinci fikrası uyarınca verilecek idari para cezalarına karşı kararın veri

sorumlusuna tebliğinden itibaren 15 gün içinde sulh ceza mahkemesine başvurulabilecektir. Bu süre içinde başvuru yapılmaması durumunda idari para cezası kesinleşecek olup şayet belirtilen süre içinde başvuru yapılması durumunda ise kesinleşmesi önlenecektir. Kurulca aynı veri sorumlusu hakkında idari para cezası dışında veya yanında idari yargının görev alanına giren bir idari yaptırım uygulanması halinde (veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulması gibi) ise KK 27'nci maddesinin sekizinci fikrasındaki istisnai hüküm gereğince idare mahkemesinde iptal davası açılabilecektir. Örneğin Kurul tarafından veri sorumlusu hakkında idari para cezası kararının dışında veya yanında veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulması kararının alınması durumunda açılacak davalarda görevli ve yetkili yargı yeri Ankara İdare Mahkemesi'dir.

SONUÇ

Bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte kişisel veri işleme faaliyetinde önemli bir ölçüde artış gerçekleşmiş olup kişisel verilerin korunması, teknik alanın yanında hukuken de önem arz eden bir konu hâline gelmiş ve bir hak olarak tanımlanması gereği doğmuştur. Kişisel verilerin korunması, ilk defa uluslararası kuruluşlar tarafından tartışılmış olup zamanla gerek uluslararası sözleşmelerde gerekse ülkelerin kendi iç mevzuatlarında bir hak olarak düzenleme altına alınmıştır. Anayasa ve 6698 sayılı Kanuna bakıldığında, kişisel verilerin korunması hakkının insan onuru ve mahremiyetinin korunması kapsamında bir insan hakkı olduğu şeklinde bir yaklaşım sergilenmiştir. Ülkemizde kişisel verilerin sınırsız biçimde ve gelişigüzel toplanmasının, yetkisiz kişilerin erişimine açılmasının, açıklanması veya amaç dışı ya da kötüye kullanımı sonucu kişilik haklarının ihlal edilmesinin önüne geçilmesi amacıyla Kanun yürürlüğe konulmuş olup 18'inci maddede kabahatlere ilişkin hükümler yer almakta ayrıca 15'inci maddede ise idari yaptırım niteliğindeki idari tedbir kararlarının alınmasına imkân tanıyan düzenlemeler mevcuttur. İdari yaptırıma konu eylemler ile ilgili olarak, genel kanun niteliğindeki KK hükümleri uygulanmaktadır.

Kişisel verilerin korunması mevzuatına konu olayların nasıl meydana geldiği, Kurul tarafından inceleme süreçleri yürütülürken nelere dikkat edildiği ve kişisel verilerin korunması mevzuatının ne şekilde ele alındığı gibi konular hakkında bilgi sahibi olunması adına Kurul tarafından alınan bazı kararların özetleri Kurumun resmi internet sayfasında yayınlanarak kamuoyu bilgilendirilmektedir. Kurul karar özetlerinden anlaşılacağı üzere, Kurul tarafından tesis edilen idari yaptırımların veri sorumlularının yükümlülüklerini yerine getirmede önemli etkisinin olduğu anlaşılmaktadır. Ayrıca Kurulun inceleme başlatılan konuya ilişkin olarak; tüm taraflardan açıklama talep ettiği ve mevzuata aykırılık durumunu gerekçeli olarak ele aldığı görülmektedir.

Diğer taraftan, idari yaptırım kararına karşı başvuru yoluna ilişkin ise, Kurulun uyguladığı cezaların teknik ve uzmanlık bilgisine ihtiyaç olan, ihlalin değerlendirilmesi için kapsamlı bir inceleme gerektiren ve ihlalin anlaşılması durumunda KK'ye konu fiillere yönelik uygulanan yaptırımlara nazaran çok yüksek miktarda para cezalarının uygulandığı fiiller olması ve bunun yanında yargısal denetimin de daha geniş ve kapsamlı yürütülmesi gerekmesi sebebiyle görevli yargı yeri değişikliğinin İdare Mahkemeleri olmasının yerinde bir adım olacağı söylenebilecektir.

KAYNAKÇA

- Akbulut, B. (2010). *Türk Ceza Kanunu ile Kabahatler Kanununun Genel Hükümlerinin Yaptırım Hükümleri Dışında Karşılaştırmalı Olarak İncelenmesi.* Ankara.
- Altındağ, H. (2021). *Kişisel Verileri Koruma Kurulu Tarafından Verilen İdari Para Cezaları.* Ankara: Adalet Yayınevi.
- Çekin, M.S. (2020). *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku,* 3. Baskı, İstanbul: On İki Levha Yayıncılık.
- Danıştay. (2010). 2009/8191 Esas ve 2010/1394 sayılı Karar. Erişim Adresi: https://www.tdb.org.tr/tdb/v2/ekler/Danistay_8.Dairesi_Karari_Esas_No_2009-8191.pdf.
- Duran, L. (1983). "Düzenleme Yetkisi Özerk Sayılabilir Mi?", İdare Hukuku ve İlimleri Dergisi, 4, 1 – 3.
- Dülger, M.V. (2019). *Kişisel Verilerin Korunması Hukuku,* 2. Baskı, İstanbul: Hukuk Akademisi.
- Kangal, Z.T. (2019). *Kabahatler Hukuku.* 2. Baskı, İstanbul: On İki Levha Yayıncılık.
- Kangal, Z.T. (2019). *Kişisel Verilerin Ceza ve Kabahatler Bakımından Korunması.* İstanbul: On İki Levha Yayıncılık.
- Kişisel Verileri Koruma Kurumu, (2018). 100 Soruda Kişisel Verilerin Korunması Kanunu, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf, 19.05.2022.
- Kişisel Verileri Koruma Kurumu, (2018). Veri Sorumluları Sicili, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/ed040488-ee55-40de-b503-646c8e1bc916.pdf, 19.05.2022.

◊ "Kişisel Verileri Koruma Kurumu, (2021). Kişisel Verilerin Korunması Kanununun Uygulanmasında Güncel Konular Konulu Çarşamba Semineri", Kişisel Verileri Koruma Kurumu, https://www.youtube.com/watch?v=EBS-TLORqa0, 23.04.2022.

◊ Schütz, P. (2012). "Comparing Formal Independence of Data Protection Authorities in Selected EU Member States", Conference Paper for the 4th Biennial ECPR Standing Group for Regulatory Governance Conference.

KİŞİSEL VERİLERİN KORUNMASI KANUNU BAKIMINDAN "NON BIS IN IDEM" İLKESİNİN DEĞERLENDİRİLMESİ

Amine GÜLÜMSER

Kişisel Verileri Koruma Uzmanı

"Bu çalışma, 14/02/2023 tarihinde kabul edilen; "Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlularının Yükümlülüklerinin İhlali, Uygulanan Yaptırım Türleri ve Bu Çerçevede "Non Bis In Idem" İlkesinin Değerlendirilmesi" başlıklı uzmanlık tezinden alınmıştır."

GİRİŞ

Kişisel veri kavramı ve bu minvalde kişisel verilerin korunması hukuku ülkemiz bakımından henüz olgunlaşmamış bir alandır ve bu hukuk dalının gelişim süreci gerek dünya genelinde gerek ülkemizde durmaksızın devam etmektedir. Ülkemiz bakımından anayasal niteliği haiz bir temel hak olarak karşımıza çıkan kişisel verilerin korunmasını isteme hakkı hem bireylerin özel yaşamlarına müdahalenin en aza indirilmesi hem de mahremiyet olgusunun toplum nezdinde kanıksanması adına oldukça önemli bir yere sahiptir. Kişisel verilerin korunması hakkının ülkemiz mevzuatında kendine yer edinmesi ile hayatımıza oldukça farklı kavramlar eklenmiş olup kişisel verilerin işlenmesine yönelik süreçlerin yürütülmesi bakımından çeşitli yükümlülükler ve yaptırımlar ortaya çıkmıştır.

Bu kapsamda veri sorumlusu kavramı ve veri sorumlusunun 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (6698 sayılı Kanun) uyarınca haiz olduğu yükümlülükler, kişisel verilerin korunması hukukunun insan yaşamına, iş ve sosyal hayata etkisinin somut olarak görülebilmesini sağlamaktadır. Zira

veri sorumlusu sıfatını taşıyan kişilerin yükümlülüklerinin muhatabı doğrudan ilgili kişiler yani kişisel verilerin korunması hakkına müdahale edilen kişilerdir. Veri sorumlularının 6698 sayılı Kanundan kaynaklanan pek çok yükümlülüğü bulunmakta olup bunlar genel anlamda; aydınlatma yükümlülüğünün yerine getirilmesi, veri sorumluları siciline kayıt ve bildirim, kişisel veri işleme envanteri ile kişisel veri işleme ve saklama politikası hazırlama, ilgili kişiye cevap verme, veri güvenliğinin sağlanması, Kişisel Verileri Koruma Kurulu kararlarının yerine getirilmesi ve imha yükümlülüğü olarak karşımıza çıkmaktadır. Bahsedilen bu temel yükümlülükler de kendi içlerinde başkaca kuralları ve yükümlülükleri barındırmaktadır.

Bununla birlikte kişisel verilerin korunması hakkının öneminden ötürü bu koruma sadece 6698 sayılı Kanun ile sınırlı kalmamıştır. Öyle ki çerçeve bir kanun niteliğini haiz olan 6698 sayılı Kanunun 2016 yılında yürürlüğe girmesinden evvel, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda (TCK) kişisel verilerin korunmasına yönelik hükümler bulunmaktadır. TCK'nın dokuzuncu bölümünde özel hayata ve hayatın gizli alanına karşı suçlar düzenlenmiştir. Anılan bölümde haberleşmenin gizliliğinin ihlali, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğini ihlal gibi suçların yanı sıra münhasıran kişisel verilerle alakalı suçlara da yer verilmiştir. TCK'nın 135 inci maddesinde *"kişisel verilerin kaydedilmesi"* suçu, 136 ncı maddesinde *"Verileri hukuka aykırı olarak verme veya ele geçirme"* suçu, 137 nci maddesinde bahse konu suçların *"Nitelikli haller"*i, 138 inci maddesinde ise *"Verileri yok etmeme"* suçu düzenlenmiştir. Kişisel verilerin korunmasına ilişkin TCK'da dolaylı bir biçimde koruma sağlayan hükümler de bulunmakta olup bunlar örneğin; TCK'nın *"Haberleşmenin gizliliğini ihlal"* başlıklı 132 nci maddesi, *"Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması"* başlığını altında düzenlenen 133 üncü maddesi, *"Özel hayatın gizliliğini ihlal"* başlığını haiz 134 üncü maddesi, *"Bilişim sistemine girme"* başlıklı 243 üncü maddesidir.

Kişisel verilerin korunması hakkını koruyan hükümler 6698 sayılı Kanun ve TCK ile sınırlı olmayıp pek çok mevzuatta çeşitli şekillerde düzenlemelere tabi tutulmuştur. Birden fazla mevzuatta düzenleme altına alınan bir husus bakımından "non bis in idem" ilkesinin işlerlik kazanması kaçınılmaz bir sonuçtur. Kabahatler hukukuna da sirayet eden bir ceza genel ilkesi olan non bis in idem ilkesi oldukça karmaşık ve çetrefilli bir konu olmasının yanı sıra gerek hukuk devleti ile adaletin tesisi bakımından gerek kişilerin hukuki güvenliğinin sağlanması adına oldukça önemli bir kavram olarak karşımıza çıkmaktadır. Bu sebeple konunun önemine binaen çalışmamızda non bis in idem ilkesinin hukukumuza yansıma biçimi ve hukukumuzdaki çeşitli görünümleri ele alınarak non bis in idem ilkesinin suçlar

ve kabahatler bakımından özellik arz eden durumları üzerinde bilhassa durulmuştur.

VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

Kavram

6698 sayılı Kanunun 3 üncü maddesinin birinci fıkrasının (ı) bendinde; *"Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi."* şeklinde tanımlanan "veri sorumlusu" sıfatını kimlerin taşıdığının belirlenmesi kişisel verilere ilişkin korunma sağlayan hukuk dalının külli olarak anlaşılabilmesi ve açıklanabilmesi için oldukça ehemmiyetlidir. Zira, her ne kadar 6698 sayılı Kanunun 12 nci maddesinin ikinci fıkrasında bulunan; *"Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur."* düzenlemesi ile kişisel veri işleme faaliyetleri bakımından veri sorumlusu konumunda olan kişiler ve veri işleyen niteliğini haiz kişiler arasında bir müşterek sorumluluk tesis edilmiş olsa da 6698 sayılı Kanunun düzenlediği yükümlülükler ile yaptırımların muhatabı veri sorumlusudur (Küzeci, 2021; Dülger, 2020; Kangal, 2019; Çekin, 2020; Kişisel Verileri Koruma Kurumu [KVKK], 2019a). Kişisel verilerin hukuka uygun işlenmesi bakımından veri işleyenlerin de yükümlülük altında bulunmasına rağmen, veri işleyenlerin veri sorumlusunun kararları doğrultusunda veri sorumlusu adına hareket etmesinden ötürü, idari para cezalarının muhatabı olmaları söz konusu değildir. Zira, "veri işleyen" kavramı; 6698 sayılı Kanunun 3 üncü maddesinin birinci fıkrasının (ğ) bendinde; *"Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi."* biçiminde tanımlanmıştır. Nitekim, 6698 sayılı Kanunun "Kabahatler" başlığını taşıyan 18 inci maddesinin birinci fıkrasında, 6698 sayılı Kanun kapsamındaki kabahatlere uygulanacak idari para cezaları düzenleme altına alınmış ve aynı maddenin ikinci fıkrasında; *"Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır."* düzenlemesine yer verilerek idari para cezalarının muhatabının veri sorumluları olduğu açıkça ifade edilmiştir (Demirezen, 2020). Bununla birlikte "veri sorumlusu" şeklindeki sıfat ile "veri işleyen" olarak karşımıza çıkan sıfatın aynı kişide birleşmesi de mümkündür (Özkan, 2020).

Veri sorumlusu ile veri işleyenlerin tayininde kullanılacak kriterler ise Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı kararı ile belirlenmiştir (Kişisel Verileri Koruma Kurulu, 30/01/2020 tarihli ve 2020/71 sayılı

Karar). Anılan karar uyarınca; *"kişisel verilerin toplanması ve toplama yöntemi, toplanacak kişisel veri türleri, hangi bireylerin kişisel verilerinin toplanacağı, kişisel verinin işlenmesine ve kimin işleyeceğine karar verme, işleme faaliyetinin temel unsurlarına karar verme (hangi kişisel verilerin toplanacağı, toplanan verilerin hangi amaçlarla kullanılacağı ve ne şekilde işleneceği, verilerin ne kadar süreyle saklanacağı, veri saklama politikasının ne şekilde olacağı, verilere kimlerin erişme yetkisi olacağı, alıcıların kim olacağı gibi hususlar işlemenin temel unsurlarına örnek olarak gösterilebilir, toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı, kişisel verilerin işlenmesinde üst düzeyde, herhangi bir emir ve talimat almadan karar verebilme, ilgili kişilerle doğrudan muhatap olma, kendi adına veri işleme faaliyetini yürütecek bir veri işleyen atama, işleme faaliyetinden menfaat sağlama."* hususlarına yönelik olarak karar alan kişiler veri sorumlusu olarak kabul edilecektir. Yine anılan karar uyarınca veri işleyenin tespitinde, *"kişisel veri işlemek için başkasından talimat alınması, kişisel verilerin kişilerden toplanması sürecinde karar verme yetkisine sahip olmamak, kişisel verilerin kullanım amaçlarının belirlenmemesi, verilerin ne şekilde ifşa olabileceğine, kimlerin bu verilere erişebileceğine karar verme yetkisine sahip olmamak, veri saklama sürecine karar verme yetkisine sahip olmamak, veri işlemenin sonuçlarından sorumlu olmaması, veri sorumlusu ile yapılacak sözleşme gibi yasal bağlayıcılığı olan anlaşmalar çerçevesinde veri sorumlusunun verdiği yetkiler çerçevesinde kişisel verilerin işlenmesine yönelik birtakım karar verme mekanizmalarının söz konusu olup olmadığı."* hususları değerlendirilerek karar verilecektir.

6698 sayılı Kanun, ne "veri sorumlusu" kavramının tanımında ne de "veri işleyen" kavramının tanımında kamu kurumlarının niteliğini irdelememiştir. Bununla birlikte, 6698 sayılı Kanun hükümlerinin hem özel hukuk bakımından söz konusu olan tüzel kişiler için hem de kamu hukukundaki tüzel kişiler için bağlayıcı olmasından ötürü kamu kurumlarının da veri sorumlusu yahut veri işleyen sıfatını haiz olacağının kabulü gerekir (Küzeci, 2021; KVKK, 2019b; Korkmaz, 2017; Göçmen Uyarer, 2020; Özkan, 2020). Zira, 6698 sayılı Kanunun genel gerekçesinde; *"...Günümüzde bu veriler, gerek özel sektör ve gerekse kamu sektörü tarafından bilişim sistemleri üzerinden otomatik yollarla sıkça kullanılmaktadır..."* açıklaması, 2 nci maddesinin gerekçesinde ise; *"...Buna göre Kanun, kişisel verileri işlenen gerçek kişiler ile bu verileri işleyen gerçek ve tüzel kişiler hakkında uygulanacaktır. Özel sektör ile kamu sektörü bakımından bir ayrım yapılmamış olup, öngörülen usul ve esasların her iki sektörde de uygulanması benimsenmektedir. Kişisel verilerin otomatik olan veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi bakımından da herhangi bir fark öngörülmemektedir..."* açıklamasına yer verilmiştir.

Tekraren belirtmek gerekir ki; bir kişisel veri işleme faaliyetinin söz konusu olması halinde, sorumluluk esasen veri sorumlusuna ait olup veri işleyen, veri sorumlusunun veri işleyene verdiği yetki çerçevesinde, veri sorumlusunun adına kişisel veri işleme faaliyetlerini gerçekleştirmektedir (Küzeci, 2021; Yılmaz ve Çavuşoğlu, 2020; Çekin, 2020). Bir sermaye şirketinin veri sorumlusu niteliğini haiz olması mümkün olduğu gibi şahıs şirketleri ve kamu hukuku tüzel kişileri de veri sorumlusu sıfatını haiz olabilmektedir (Demirezen, 2020). Ayrıca gerçek kişilerin de veri sorumlusu olabilmesi mümkün iken uygulamada tüzel kişilerin veri sorumlusu olduğu daha çok görülmektedir. Nitekim gerçek kişiler tarafından gerçekleştirilen kişisel veri işleme faaliyetleri çoğunlukla bir veri kayıt sistemi olmaksızın gerçekleştirilmesi dolayısıyla 6698 sayılı Kanun kapsamında değerlendirilmemektedir ve bu durumlar Türk Ceza Kanunu çerçevesinde ele alınabilmektedir (Dülger, 2020). Bu noktada belirtmek gerekir ki; gerçek kişilerin her zaman TCK kapsamında ele alınması söz konusu değildir. Kurulun çeşitli kararlarında gerçek kişilerin veri sorumlusu olarak kabul edildiği ve yaptırıma tabii tutulduğu görülmektedir (Kişisel Verileri Koruma Kurulu, 07/11/2019 tarihli ve 2019/332 sayılı Kararı). Tüzel kişiler bakımından ise bizzat tüzel kişiliğin kendisi veri sorumlusu sıfatını haizdir (Çekin, 2020; Demirezen, 2020; Yılmaz ve Çavuşoğlu, 2020; Özkan, 2020; Altındere, 2020). Nitekim 30/12/2017 tarihli ve 30286 sayılı Resmi Gazetede yayımlanması suretiyle yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmeliğin (Sicil Yönetmeliği) 11 inci maddesinin birinci fıkrasında; *"Tüzel kişilerde veri sorumlusu tüzel kişiliğin kendisidir. Türkiye'de yerleşik olan tüzel kişilerin Kanun kapsamındaki veri sorumlusu yükümlülükleri, ilgili mevzuat hükümlerine göre tüzel kişiliği temsil ve ilzama yetkili organ veya ilgili mevzuatta belirtilen kişi veya kişiler marifetiyle yerine getirilir. Tüzel kişiliği temsile yetkili organ, Kanunun uygulanması bakımından yerine getirilecek yükümlülükler ile ilgili olarak bir veya birden fazla kişiyi görevlendirebilir. Bu görevlendirme Kanun hükümleri uyarınca tüzel kişiliğin sorumluluğunu ortadan kaldırmaz."* hükmü yer almaktadır. Kimliği belirsiz kişiler ise veri sorumlusu olarak ele alınamamaktadır (Altındere, 2020). Nitekim, Kurulun 13/09/2018 tarihli ve 2018/106 sayılı kararında da; *"... kimliği belirsiz kişi veya kişilerin veri sorumlusu olarak tanımlanamayacağı..."* açıkça ifade edilmiştir (Kişisel Verileri Koruma Kurulu, 13/09/2018 tarihli ve 2018/106 sayılı karar).

Yükümlülükler

Veri sorumlusunun 6698 sayılı Kanunun çeşitli hükümlerinden kaynaklanan yükümlülükleri bulunmaktadır. Kişisel verilerin korunmasına yönelik temel hakkın farklı şekillerde ihlal edilmesi söz konusu olabilmektedir. Bu ihlallerin kimisi ceza hukuku alanında benzer bir şekilde ele alınmış ve suç olarak düzenlenmiştir,

kimisi ise suç olarak ele alınmamış ve kabahat olarak düzenlenerek idari yaptırımlara tabii tutulmuştur (Kangal, 2019).

6698 sayılı Kanunun "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10 uncu maddesi; *"(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlüdür."* şeklindedir. Görüldüğü üzere; veri sorumlusunun kişisel verilerin elde edilmesi esnasında ilgili kişilere birtakım bilgileri sağlaması gerekmektedir ve bu durum veri sorumlusu için bir yükümlülük olmakla birlikte ilgili kişiler için bir hak niteliğindedir (Kangal, 2019; KVKK, 2019c; KVKK, 2020; Yılmaz ve Çavuşoğlu, 2020).

6698 sayılı Kanunun 16 ncı maddesinde; Veri Sorumluları Siciline (Sicil) yönelik düzenlemelere yer verilmiştir. Anılan madde;

"(1) Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulur.

(2) Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir.

(3) Veri Sorumluları Siciline kayıt başvurusu aşağıdaki hususları içeren bir bildirimle yapılır:

a) Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri.

b) Kişisel verilerin hangi amaçla işleneceği.

c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar.

ç) Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları.

d) Yabancı ülkelere aktarımı öngörülen kişisel veriler.

e) Kişisel veri güvenliğine ilişkin alınan tedbirler.

f) Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

(4) Üçüncü fıkra uyarınca verilen bilgilerde meydana gelen değişiklikler derhâl Başkanlığa bildirilir.

(5) Veri Sorumluları Siciline ilişkin diğer usul ve esaslar yönetmelikle düzenlenir." şeklindedir. Görüldüğü üzere; Kişisel Verileri Koruma Kurumu Başkanlığı tarafından Kişisel Verileri Koruma Kurulunun gözetiminde, kamuya açık olarak Veri Sorumluları Sicilinin tutulması gerekmekte olup veri sorumluları sicile kayıt yükümlülüklerini Kişisel Verileri Koruma Kurumunun resmi internet sitesi vasıtasıyla gerçekleştirmektedir.

Veri sorumlularının, Sicile kayıt yükümlülüğüne bağlı olarak, *"Kişisel veri işleme envanteri"* ile *"Kişisel veri saklama ve imha politikası"* hazırlama yükümlülüğü bulunmaktadır (KVKK, 2019ç; Saka, Çağlayan ve Koca, 2020). Kişisel veri işleme envanteri, Sicil Yönetmeliğinin 4 üncü maddesinin birinci fıkrasının (h) bendinde; *"Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter."* olarak tanımlanmıştır. Söz konusu envanter esasen, veri sorumlularınca kişisel veri işleme sürecinin başlangıcından sonuna kadar tüm işleyişi içerecek şekilde bütün detayların yer aldığı bir rapordur (Özkan, 2020). Veri sorumlularına yüklenen kişisel veri işleme envanteri hazırlama yükümlülüğünün asıl gayesi; veri sorumlularının gerçekleştirdikleri kişisel veri işleme süreçleri bakımından kendi kendilerini test etmelerinin sağlanması olup böylelikle veri sorumluları tarafından 6698 sayılı Kanun ve ilgili ikincil mevzuata aykırı bir durumun bulunup bulunmadığının tespitinin sağlanması ile aykırılıklar varsa bu aykırılığın giderilmesidir (Çekin, 2020; Özkan, 2020; KVKK, 2019d). Dolayısıyla, kişisel veri işleme envanterinin hazırlanması, veri sorumlusu tarafından veri güvenliğinin sağlanması adına alınacak idari tedbirlerin en önemlilerindendir (Demirezen, 2020).

6698 sayılı Kanunun "İlgili kişinin hakları" başlıklı 11 inci maddesi uyarınca; *"herkes, veri sorumlusuna başvurarak kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğren-*

me, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme, Kanunun 7 nci maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, 11 inci maddenin birinci fıkrasının (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme" haklarına sahiptir. Bununla birlikte 6698 sayılı Kanunun "Veri sorumlusuna başvuru" başlıklı 13 üncü maddesinin birinci fıkrası; *"İlgili kişi, bu Kanunun uygulanmasıyla ilgili taleplerini yazılı olarak veya Kurulun belirleyeceği diğer yöntemlerle veri sorumlusuna iletir."* hükmünü, ikinci fıkrası ise; *"Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifedeki ücret alınabilir."* hükmünü amirdir. Ayrıca aynı maddenin üçüncü fıkrası uyarınca, veri sorumlusu ilgili kişinin talebini kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir (Saka, Çağlayan ve Koca, 2020).

10/03/2018 tarihli ve 30356 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in (Başvuru Tebliği) "Başvuru hakkı" başlıklı 4 üncü maddesinin birinci fıkrasında; *"Kişisel verisi işlenen gerçek kişiler, veri sorumlusuna başvuru hakkına sahiptir."* hükmü bulunmaktadır. Yine Başvuru Tebliğinin "Başvuruya cevap" başlıklı 6 ncı maddesinin birinci fıkrası; *"Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür."* hükmünü, ikinci fıkrası; *"Veri sorumlusu, başvuruyu kabul eder veya gerekçesini açıklayarak reddeder."* hükmünü amirdir. Görüldüğü üzere; veri sorumlularının ilgili kişilerin taleplerini gerek Kanunun 13 üncü maddesinin üçüncü fıkrası gerek Başvuru Tebliğinin 6 ncı maddesi uyarınca; ya kabul etmesi ya da gerekçesini açıklayarak reddetmesi gerekmektedir (Turan, 2021; Göçmen Uyarer, 2020). Dolayısıyla veri sorumlularının ilgili kişilerin taleplerine karşın iki seçimlik hareketten birini ifa etme yükümlülüğü bulunduğundan ötürü veri sorumlularının kendilerine iletilen talepler karşısında hareketsiz kalması mümkün değildir.

Öncelikle belirtmek gerekir ki; veri güvenliği kavramı ile kişisel verilerin korunması kavramı eş anlamlı değildir (Küzeci, 2021). Zira veri güvenliği hususu daha ziyade teknik hususları ihtiva etmekte ve belirli standartlara uygunluğun sağlan-

masını esas almaktayken veri güvenliği kavramı, kişisel verilerin korunmasının yalnızca bir kısmını teşkil etmektedir (Çekin, 2020). Öyle ki kişisel verilerin güvenliğinin sağlanması hususu kişisel veri işleme faaliyetinin belirli bir aşaması yahut belirli bir veriye özgülenmiş olmayıp veri sorumlusunca kişisel verilerin elde edilmesinden itibaren sürekli olarak kişisel veri işleme faaliyetinin her aşamasında ifa edilmesi gereken bir yükümlülüktür (Dülger, 2020). 6698 sayılı Kanunun 12 nci maddesinde veri güvenliğine ilişkin yükümlülükler belirlenmiştir. Kanunun 12 nci maddesinin birinci fıkrası uyarınca veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Öte yandan Kanunun 3 üncü maddesindeki kişisel verilerin işlenmesinin; *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"* şeklindeki tanımından hareketle, kişisel verilerin hukuka aykırı olarak işlenmesinin engellenmesi ile oldukça geniş bir koruma sağlanmaktadır. Kişisel verilerin işlenmesinin, kişisel veriler üzerinde gerçekleştirilecek her türlü işlem olmasından ötürü kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel veriler üzerinde gerçekleştirilecek her türlü işlemin hukuka aykırılığının engellenmesi anlamına gelmektedir. Alınacak teknik ve idari tedbirlere ilişkin olarak, Kurumun resmi internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinden faydalanılabilmesi mümkün olup söz konusu yükümlülüğün tam anlamıyla yerine getirilebilmesi adına veri sorumlusu tarafından değişen ve gelişen teknolojilerin sürekli olarak takibi ve bu kapsamda gerekli aksiyonların alınması gerekmektedir (Dülger, 2020). Ayrıca veri güvenliği kapsamında, özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler ise; Kurulun 31/01/2018 tarihli ve 2018/10 sayılı kararı ile belirlenerek Kurumun resmi internet sitesinde yayımlanmıştır (Kişisel Verileri Koruma Kurulu, 31/01/2018 tarihli ve 2018/10 sayılı Karar). Bu noktada önemle belirtmek gerekir ki; 6698 sayılı Kanun kapsamında sağlanması gereken veri güvenliğine yönelik olarak veri sorumlusu tarafından alınması gereken tedbirler bakımından Kanunda açık bir düzenlemenin yer almamasının sebebi; söz konusu tedbirlerin sınırlılık arz etmemesinden ötürüdür (Demirezen, 2020). Nitekim veri sorumlusu tarafından icra edilen faaliyetin kapsam ve sınırları, işleme faaliyetine konu edilen kişisel verinin türü ve miktarı, veri sorumlusunun bünyesinde istihdam edilen personel sayısı ve personelin farkındalık düzeyi, veri sorumlusunun yapısı gibi hususlar doğrultusunda, veri güvenliğinin sağlanması

adına alınacak tedbirler de farklılaşacaktır (Demirezen, 2020). Kişisel verilerin hukuka aykırı işlenmesinin önlenmesi yükümlülüğünün yerine getirilebilmesi için, 6698 sayılı Kanunun 4 ila 9 uncu maddelerine bilhassa riayet edilmesi gerekmektedir (Çekin, 2020). Bu bağlamda veri sorumlusu tarafından kişisel verilerin 6698 sayılı Kanunda belirlenen işleme şartlarına uygun bir şekilde işlenmesi ve aktarılmasının yanı sıra 4 üncü maddede sayılan temel ilkelere uygunluğun bilhassa da yalnızca gerektiği kadar kişisel verinin işlendiğinin sürekli olarak gözetilmesi gerekmektedir (Çekin, 2020; Dülger, 2020).

6698 sayılı Kanunun 15 inci maddesinde, Kurulun şikayet üzerine yahut resen gerçekleştirdiği incelemenin usul ve esaslarına yönelik düzenlenmelere yer verilmiştir. Anılan maddenin beşinci fıkrası; *"Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilir."* hükmünü amirdir. 6698 saylı Kanunun "Kabahatler" başlıklı 18 inci maddesinin birinci fıkrasının (c) bendi gereğince ise; Kanunun 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası uygulanmaktadır. Görüldüğü üzere; veri sorumlularının haklarında yürütülen bir inceleme neticesinde tesis edilen Kurul kararının gereğini en geç otuz gün içinde yerine getirmesi gerekmektedir ve aksi halde söz konusu yükümlülüğün ihlali sonucunda idari para cezasına tabi bir kabahat oluşacaktır (Yılmaz ve Çavuşoğlu, 2020).

6698 sayılı Kanunun 7 nci maddesi; *"(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.*

(2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.

(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir." hükmünü amirdir. İlgili hükmün üçüncü fıkrası uyarınca; "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" (İmha Yönetmeliği) 28/10/2017 tarihli ve 30224 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Bu noktada belirtmek gerekir ki; kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi kavramlarını kapsayan üst kavram "imha"dır (Dülger, 2020). Zira İmha Yönetmeliğinin "Tanımlar" başlıklı 4 üncü maddesinin birinci fıkrasının (c) bendinde "imha" kavramı; *"Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi."* olarak tanımlanmıştır. İmha Yönetmeliğinin 5 inci maddesinin birinci fıkrasında ise; *"Kanunun 16 ncı maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan veri sorumluları, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası hazırlamakla yükümlüdür."* hükmü bulunmaktadır. Sicil Yönetmeliğinin 9 uncu maddesinin beşinci fıkrası; *"Veri sorumluları, kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin belirlenmesi, bu sürelerin kişisel veri işleme envanterinde belirtilen bilgilerle uyumu ve azami sürenin aşılıp aşılmadığının takibi için kişisel veri saklama ve imha politikası hazırlayarak, bu politikanın uygulanmasını temin ederler."* şeklinde olup "kişisel veri saklama ve imha politikası" gerek bu Yönetmeliğin 4 üncü maddesinin birinci fıkrasının (ı) bendinde gerek İmha Yönetmeliğinin 4 üncü maddesinin birinci fıkrasının (f) bendinde; *"Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politika."* olarak tanımlanmıştır. Veri sorumluları tarafından kişisel veri saklama ve imha politikalarının hazırlanması, veri sorumlularının gerek Sicile kayıt yükümlülüğü ve kişisel veri işleme envanteri hazırlama yükümlülüğü ile, gerek veri güvenliğinin sağlanması ve imha yükümlülüğü ile ilgisi olan bir husustur (Dülger, 2020; Turan, 2021; Altındere, 2020). Nitekim, İmha Yönetmeliğinin 7 nci maddesinin dördüncü fıkrasında; *"Veri sorumlusu, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklamakla yükümlüdür."* hükmü yer almaktadır. Görüldüğü üzere; veri sorumlusunun imha yükümlülüğü ile bağlantılı olarak kişisel veri saklama ve imha politikası oluşturma yükümlülüğü, bununla bağlantılı olarak da veri sorumlusunca hazırlanan kişisel veri saklama ve imha politikasında kişisel verilerin imhasına yönelik olarak uygulanan yöntemleri açıklama yükümlülüğü bulunmaktadır (Dülger, 2020).

"NON BIS IN IDEM" İLKESİ

Kavram

"Ne bis in idem" olarak da kullanılan "non bis in idem" ilkesi, kişilerin gerçekleştirdiği aynı eylemden ötürü birden fazla kez yargılanmaması ve bu kişi hakkında birden fazla cezanın uygulanmaması anlamına gelmektedir (Yerdelen, 2013; Karabel, 2015). Bu ilke, oldukça eski bir ilke olup temeli Roma Hukukuna ve dahi Kilise Hukukuna dayanmaktadır ve hem mahkumiyete ilişkin kararlar bakımından hem de beraat hükümleri açısından kendisine uygulama alanı bulmuştur (Özen, 2010; Cebeci, 2018; Geçer, 2016). Her ne kadar Roma Hukukunda suç kavramı; topluma karşı işlenen suçlar ve kişilere karşı işlenen suçlar olarak iki şekilde ele

alınsa da her iki durumda da yalnızca tek bir dava açılabilmekteydi (Cebeci, 2018). Öyle ki aynı kişiye ilişkin olarak aynı fiilinden ötürü ikinci defa dava açılması halinde, hakkında dava açılan bu kişiye yönelik olarak *"exceptio rei judicatae"* adı verilen bir kesin hüküm def'i tanınması suretiyle kişi hakkında açılan ikinci dava engellenirdi (Cebeci, 2018).

Bu ilkenin, modern hukuktaki ilk görünümü ise; İngiliz Hukukunda karşımıza çıkmakta olup *"double jeopardy"* (çifte yargılama) yasağı şeklinde adlandırılmaktadır ve ilk zamanlarda Kilise Hukukunda işlevselliğini göstermiştir (Cebeci, 2018). Şöyle ki II. Henry'nin hüküm sürdüğü 1176 yılında, Kilise Hukukuna göre yargılanmış ve cezalandırılmış olan ruhban sınıfına mensup kişilerin kraliyet mahkemeleri nezdinde tekraren yargılanması istenildiğinde, Thomas Becket tarafından, halihazırda Kilise Hukukuna göre yargılanan bu kişilerin yeniden kraliyet mahkemelerinde yargılanmasının *"Hiç kimse aynı suçtan iki kere yargılanamaz."* ilkesine uygun olmadığının belirtilmesi suretiyle itirazlarda bulunmuştur (Cebeci, 2018). Görüldüğü üzere; anılan ilkenin hukuken kabulü oldukça eski çağlara dayanmaktadır ve bu ilkenin ortaya çıkmasının özünde kişinin hukuki güvenliğinin sağlanması hususu bulunmaktadır, zira kişinin daimi olarak gerçekleştirdiği bir fiilden ötürü yargılanma yahut cezalandırılma korkusu içinde yaşamasının engellenmesi kişinin kendisini hukuken güvende hissetmesinin bir gereğidir (Özen, 2010). *"Tabiri caiz ise, Demoklesin kılıcının kişi üzerinde yaşam boyu durması, hukuki güvensizliği ortaya çıkaracaktır."* ve *"Non bis in idem ilkesinin çıkış felsefesi, Demoklesin kılıcının sürekli olarak bir ceza tehdidi ile kişinin üzerinde asılı durmasının doğuracağı acıyı ortadan kaldırmaktadır."* (Özen, 2010). Zira, hem hukuk devleti olmanın bir gereği olarak hem de hukuk güvenliğinin tesisi bakımından bu ilke oldukça önemlidir (Cebeci, 2018).

Bu ilke giderek evrensel hukukta da yer edinmiş ve Amerika'da, Fransa'da, Almanya'da, İsveç'te, Hollanda'da ve pek çok ülke mevzuatında ceza hukukuna hakim olan genel ilkeler arasında düzenlenmiştir (Cebeci, 2018). Bununla birlikte, anılan ilke bazı ülkelerde anayasal olarak düzenlenmiş olmakla birlikte bazı ülkelerin ceza kanunlarında kendine yer bulmuştur (Cebeci, 2018).

Ülkemizde ise; non bis in idem ilkesi Türkiye Cumhuriyeti Anayasasında düzenlenmemiştir (Geçer, 2016). Bununla birlikte söz konusu ilke, Avrupa İnsan Hakları Sözleşmesinin 7 numaralı protokolünde de yer almaktadır fakat bu protokolün ülkemiz tarafından onaylanması 25/03/2016 tarihini bulmuştur (6684 Sayılı Kanun Onayı, 2016). Nitekim bu durum Anayasa Mahkemesinin 26/12/2017 tarihli, 2014/13229 başvuru sayılı kararında; *"16. Anayasa'nın 148. maddesinin üçüncü fıkrası ile 30/3/2011 tarihli ve 6216 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 45. maddesinin (1) numaralı fıkrası gereği Anayasa Mahkemesine yapılan bir bireysel başvurunun esasının incelenebilmesi için kamu gücü tarafından ihlal edildiği iddia edilen hakkın Anayasa'da güvence altına alınmış olmasının yanı sıra Avrupa İnsan Hakları Sözleşmesi (Sözleşme) veya Türkiye'nin taraf olduğu ek protokollerin kapsamına da girmesi gerekir. Bir başka ifadeyle Anayasa ve Sözleşme'nin ortak koruma alanı dışında kalan bir hak ihlali iddiasını içeren başvurunun kabul edilebilir olduğuna karar verilmesi mümkün değildir (Onurhan Solmaz, B. No: 2012/1049, 26/3/2013, § 18).*

17. Aynı suçtan iki kez yargılanmama ve cezalandırılmama hakkı, Sözleşme'ye ek 7 numaralı Protokol'ün 4. maddesinde yer alsa da, söz konusu Protokol'ün uygun bulunmasına dair 6684 sayılı Kanun'un Türkiye Büyük Millet Meclisi tarafından 10/3/2016 tarihinde kabul edildiği ve 25/3/2016 tarihinde Resmi Gazete'de yayınlandığı, 28/3/2016 tarihinde de Bakanlar Kurulunca onaylanan Protokol'ün Türkiye açısından 1/8/2016 tarihinde yürürlüğe girdiği göz önünde bulundurulduğunda, başvuruya konu ihlal iddiası tarihi itibarıyla anılan Protokol Türkiye açısından yürürlükte olmadığından başvurucunun hak iddiasının Anayasa ve Sözleşme'nin ortak koruma alanının dışında kaldığı anlaşılmaktadır (İffet İnci Gültekin, B. No: 2013/9585, 9/3/2016, § 42).

18. Başvurucunun aynı suçtan iki kez yargılandığı yönündeki iddiasının adil yargılanma hakkı altında incelenmesi de mümkün değildir. Aksi bir yaklaşım belirtilen ilkenin Sözleşme'yle teminat altına alınanlardan farklı bir hak olarak ek 7 No.lu Protokol içinde düzenlenmesiyle ve anılan Protokol'e taraf olmamak suretiyle ortaya konulan iradeyle bağdaşmaz (İffet İnci Gültekin, § 45).

19. Açıklanan nedenlerle başvurucunun iddiasının konu bakımından yetkisizlik nedeniyle kabul edilemez olduğuna karar verilmesi gerekir." şeklinde açıklanmıştır *(Anayasa Mahkemesi, 26/12/2017 tarihli, 2014/13229 başvuru sayılı karar).*

Öte yandan anılan ilke, 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun (CMK) *"Duruşmanın sona ermesi ve hüküm"* başlığını taşıyan 223 üncü maddesinin yedinci fıkrasında; *"Aynı fiil nedeniyle, aynı sanık için önceden verilmiş bir hüküm veya açılmış bir dava varsa davanın reddine karar verilir."* denilmek suretiyle hüküm altına alınmıştır. TCK'nın "Fikri içtima" başlığını taşıyan 44 üncü maddesinde ise; *"İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır."* hükmü yer almakta olup anılan maddenin gerekçesinde non bis in idem ilkesine yer verilmiştir. TCK'nın 44 üncü maddesinin gerekçesi; *"Madde metninde, farklı neviden fikri içtima düzenlenmiştir.*

Kişi, işlediği bir fiil ile birden fazla farklı suçun oluşumuna neden olabilir; ancak non bis in idem kuralı gereğince bu fiilden dolayı ancak bir defa cezalandırılabilir. Gerçekleştirdiği fiilin birden fazla farklı suçun oluşumuna neden olması durumunda, failin bu suçlardan en ağır cezayı gerektiren suç nedeniyle cezalandırılması yoluna gidilmelidir. Böylece, bir fiilden dolayı kişinin birden fazla cezalandırılmasının önünde geçilmek amaçlanmıştır..." şeklindedir (Artuk, Gökcen ve Yenidünya, 2014). Görüldüğü üzere, non bis in idem ilkesi, fikri içtima kurumunun da temelini teşkil etmektedir ve failin teklik arz eden fiili ile iki veya daha fazla suça vücut vermesi durumunda yalnızca bu suçlardan cezası en ağır olan uyarınca cezalandırılması suretiyle, kişinin aynı fiilinden ötürü birden fazla kez cezalandırılmasının engellenmesi amaçlanmıştır (Özgenç, 2019; Meran, 2015). Bu doğrultuda ayrıca CMK'nın 172 nci maddesinin ikinci fıkrası da; *"Kovuşturmaya yer olmadığına dair karar verildikten sonra kamu davasının açılması için yeterli şüphe oluşturacak yeni delil elde edilmedikçe ve bu hususta sulh ceza hâkimliğince bir karar verilmedikçe, aynı fiilden dolayı kamu davası açılamaz."* hükmünü amirdir.

Unsurları

Non bis in idem ilkesinin iki unsuru bulunmakta olup bunlar "aynı kişi" ve "aynı fiil"dir (Özen, 2010).

"Aynı Fiil" Unsuru

"Aynı fiil" kavramı ile kastedilenin ne olduğuna ilişkin olarak mevzuatta bir düzenleme bulunmamaktadır fakat ceza hukuku kapsamında "fiil" kavramı; bir kimsenin kendi iradesi doğrultusunda gerçekleşmesini niyet ettiği bir sonucun meydana gelmesi adına dış dünyada etki doğuran davranışı olarak ele alınmaktadır (Özgenç, 2019). "Aynı fiil" kavramına ilişkin ise; doktrinde fikir birliği bulunmamaktadır. Kimi yazarlara göre ceza hukuku bağlamında "aynı fiil" kavramından anlaşılması gereken iddianamede açıklanan ve sınırları belirlenen eylem iken başkaca yazarlar tarafından "aynı fiil" kavramının uyuşmazlık konusunu teşkil eden olay olduğu savunulmaktadır (Cebeci, 2018). Bu noktada belirtmek gerekir ki CMK'nın 225 inci maddesi; *"(1) Hüküm, ancak iddianamede unsurları gösterilen suça ilişkin fiil ve faili hakkında verilir. (2) Mahkeme, fiilin nitelendirilmesinde iddia ve savunmalarla bağlı değildir."* hükmünü amirdir. Bu maddenin ikinci fırkasında görüldüğü üzere, mahkeme fiilin nitelendirilmesi bakımından tarafların iddia ve savunmaları ile bağlı olmayıp mahkemenin işaret ettiği fiil dolayısıyla hüküm kurulmaktadır. Yargıtay 1. Ceza Dairesinin 16/04/1994 tarihli, 1994/1547 esas sayılı ve 1994/1538 sayılı kararında; sanığa ilişkin kararın kesinleşmesinden daha sonra suç mağdurunun ateşli silah yaralanmasından ötürü

kafatasında oluşan kırık ve beyin lezyonu dolayısıyla hayatını kaybetmesi üzerine, öldürmeye teşebbüs suçundan yargılanan ve hakkındaki mahkumiyet kararı kesinleşen sanığa yönelik olarak temyiz başvurusunda bulunulmuş olup Yargıtay kararında mahkemenin fiilin aynılığı bakımından iddianamede bulunan maddi vakıa ile sınırlı olduğunu belirterek önceki kesinleşen kararın yargılanması esnasında "ölüm" olgusunun bulunmamasından ötürü mahkemece bu hususun gözetilmesinin mümkün olmadığı ve dolayısıyla yargılamanın yenilenmesinin söz konusu olmayacağı ifade edilmiştir (Bu konuda daha ayrıntılı bilgi için bkz. Cebeci, 2018).

"Aynı Kişi" Unsuru

Non bis in idem ilkesi için söz konusu olan "aynı kişi" unsuru; Cumhuriyet savcısı tarafından hazırlanan iddianamede bulunan ve bu iddianame doğrultusunda o kişi hakkında dava açılan veya hüküm tesis edilen kişiye yönelik olarak başka bir davanın açılmaması yahut hüküm verilmemesi anlamına gelmekte olup; non bis in idem ilkesi gereğince ikinci kez yargılanması/cezalandırılması yasaklanan kişi, kesin hükümle sonuçlanmış olan davaya yahut verilen hükme esas oluşturan iddianamede nüfus bilgileri ile fiziki nitelikleri somut olarak belirlenmiş olan kişidir (Özen, 2010; Karabel, 2015). Dolayısıyla, "aynı kişi" kavramı ile, iddianamede ve hükümde bulunan kişinin aynılığı anlaşılmalıdır (Cebeci, 2018).

Birinci yargılama/cezalandırma süjesinin tüzel kişiliği haiz olması halinde, bahse konu tüzel kişinin, tüzel kişiliğin kendisini oluşturan gerçek kişilerden ve çalışanlarından bağımsız bir şekilde ele alınması gerekmektedir (Bockel, 2009). Aynı suç dolayısıyla bir gerçek kişiye yönelik olarak yürütülen yargılamanın bir tüzel kişi için, bir tüzel kişiye yönelik olarak yürütülen yargılamanın ise bir gerçek kişi bakımından non bis in idem ilkesi kapsamında değerlendirilmesi mümkün değildir (Karabel, 2015).

"NON BIS IN IDEM" İLKESİNİN KABAHATLER BAKIMINDAN DEĞERLENDİRİLMESİ

Bir Fiilin Aynı Anda İki Farklı Kabahat Teşkil Etmesi

Non bis in idem ilkesinin hukukumuzdaki bir başka görünümü; 30/3/2005 tarihli ve 5326 sayılı Kabahatler Kanununda (5326 sayılı Kanun) yer alan 15 inci maddede karşımıza çıkmaktadır. 5326 sayılı Kanunun 15 inci maddesi; *"(1) Bir fiil ile birden fazla kabahatin işlenmesi halinde bu kabahatlere ilişkin tanımlarda sadece idarî para cezası öngörülmüşse, en ağır idarî para cezası verilir. Bu kabahatlerle*

ilgili olarak kanunda idarî para cezasından başka idarî yaptırımlar da öngörülmüş ise, bu yaptırımların her birinin uygulanmasına karar verilir.

(2) Aynı kabahatin birden fazla işlenmesi halinde her bir kabahatle ilgili olarak ayrı ayrı idarî para cezası verilir. Kesintisiz fiille işlenebilen kabahatlerde, bu nedenle idarî yaptırım kararı verilinceye kadar fiil tek sayılır.

(3) Bir fiil hem kabahat hem de suç olarak tanımlanmış ise, sadece suçtan dolayı yaptırım uygulanabilir. Ancak, suçtan dolayı yaptırım uygulanamayan hallerde kabahat dolayısıyla yaptırım uygulanır." düzenlemesini amirdir. Anılan maddenin birinci fıkrasında, TCK'nın 44 üncü maddesinde düzenlenmiş olan fikri içtima hükümlerine paralel olan hükme yer verilmiştir (Meran, 2015). Bununla birlikte belirtmek gerekir ki söz konusu fikrada açıkça, yalnızca idari para cezası öngörülen kabahatler bakımından, bir fiilin ifa edilmesi suretiyle birden fazla kabahatin oluşması durumunda en ağır idari para cezasının uygulanmasının söz konusu olacağı hükme bağlanmış olup meydana gelen kabahatlere yönelik olarak idari para cezasının dışında başkaca idari yaptırımların uygulanacağına ilişkin hükümlerin bulunması halinde, bahse konu idari yaptırımların hepsine birlikte karar verilmesi mümkündür (Meran, 2015; Geçer, 2016). Böylelikle birden fazla idari para cezasının konusunu teşkil eden kabahati oluşturur fiil meydana geldiğinde bu kabahat için düzenlenmiş en ağır idari para cezası ile birlikte bu kabahat için söz konusu olan diğer idari yaptırımlara ilişkin hükümler ayrı ayrı uygulanacaktır (Meran, 2015).

Kabahat Teşkil Eden Bir Fiilin Aynı Kişi Tarafından Birden Fazla Kez İşlenmesi

5236 sayılı Kanun 15 inci maddesinin ikinci fıkrası uyarınca; aynı kabahatin aynı fail tarafından birden fazla kez işlenmesi durumunda işlenen her kabahat için ayrı ayrı idari para cezası tesis edilecektir ve böylelikle TCK'nın zincirleme suça yönelik düzenlemeleri içerir 43 üncü maddesi kabahatler bakımından uygulanmayacaktır (Meran, 2015). TCK'nın *"Zincirleme suç"* başlığını taşıyan 43 üncü maddesi; *"(1) Bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda, bir cezaya hükmedilir. Ancak bu ceza, dörtte birinden dörtte üçüne kadar artırılır. Bir suçun temel şekli ile daha ağır veya daha az cezayı gerektiren nitelikli şekilleri, aynı suç sayılır. (Ek cümle: 29/6/2005 – 5377/6 md.) Mağduru belli bir kişi olmayan suçlarda da bu fıkra hükmü uygulanır.*

2) Aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi durumunda da, birinci fıkra hükmü uygulanır. Kasten öldürme, kasten yaralama, işkence ve yağma suçlarında bu madde hükümleri uygulanmaz." şeklinde düzenleme altına alınmıştır. TCK'nın aksine 5326 sayılı Kanunun 15 inci maddesinin ikinci fıkrasının birinci cümlesi gereğince bir kabahatin iki veya daha fazla kez işlenmesi durumunda gerçek içtimayı düzenleyen hükümler uygulanacak olup kabahat teşkil eden her bir fiile ilişkin ayrı ayrı idarî para cezasına hükmedilecektir. Gerçek içtima kavramı; *"Kaç fiil varsa o kadar suç, kaç suç varsa o kadar ceza vardır."* anlamına gelmektedir (Özgenç, 2019). 5326 sayılı Kanunun 15 inci maddesinin ikinci fıkrasının gerekçesinde de; *"Maddenin ikinci fıkrasında, Türk Ceza Kanununun zincirleme suça ilişkin hükümlerinin kabahatler açısından uygulanamayacağı vurgulanmıştır. Bir kabahatin birden fazla işlenmesi durumunda gerçek içtima hükümlerine göre, her bir fiille ilgili olarak ayrı ayrı idarî para cezasına karar verilecektir."* ifadesi yer almaktadır. Öte yandan, yine 5326 sayılı Kanunun 15 inci maddesinin ikinci fıkrasında; *"... Kesintisiz fiille işlenebilen kabahatlerde, bu nedenle idarî yaptırım kararı verilinceye kadar fiil tek sayılır."* cümlesine yer verilmiştir. Kesintisiz fiille işlenebilen kabahat kavramının temelini kesintisiz/mütemadi suçlar teşkil etmektedir. Mütemadi suçlarda çeşitli hareketlerin kanun koyucu tarafından birleştirilmesi suretiyle tek hareket olarak değerlendirilmesi söz konusu olmaktadır. Mütemadi suçlar bakımından hareketin birden fazla olması yani tekrarlanması, hukuka aykırılığın meydana gelmesi ve devam etmesi bakımından bir zorunluluktur. Örneğin; kişiyi hürriyetinden yoksun kılma suçunda olduğu gibi bu tür suçlarda hareket tipik anlamda tek bir hareket olup devam eden husus netice değil hareketin icrasıdır. Kısacası; kesintisiz suçlarda "suçun tamamlanması" ile "suçun bitmesi" farklılık arz etmekte olup kanuni tanımda yer alan fiilin icrası bir anda tamamlanmamaktadır (Özgenç, 2019). Suça ilişkin kanuni tanımda yer alan ve suç oluşturan hareketin ifa edilmesi ile suç meydana gelmiş ve suç tamamlanmıştır fakat suça vücut veren fiilin ifası bir müddet daha devam etmektedir (Göktürk, Özgenç ve Üzülmez, 2012). 5326 sayılı Kanunun 15 inci maddesinin ikinci fıkrasında *"kesintisiz fiille işlenebilen kabahatler"* ifadesi ile kastedilen de; kabahati meydana getiren fiilin devamlılık arz etmesidir. Kabahate vücut veren hareketin ifa edilmesi yahut edilmemesi ile kabahat meydana gelmiştir fakat kabahate vücut veren hareket devam etmektedir. Aynı fikra ile, bu tür fiiller bakımından idari yaptırım cezası uygulanana kadar devamlılık arz eden ve kabahati oluşturan fiilin tek bir fiil sayılacağı hükme bağlanmıştır. Bu fıkra uyarınca; kesintisiz fiille işlenebilen kabahatlere ilişkin olarak idari yaptırım kararının uygulanması kesinti olarak kabul edilmiş olup bu durumda söz konusu eylem hukuki kesintiye uğramaktadır. Bu cümle gereğince; bir kabahatin kesintisiz fiille işlenmesi durumunda, bu kabahat için idari para cezası verilinceye değin kabahati oluşturan fiil tek bir fiil sayılacaktır. Zira, kabahat oluşturan fiile ilişkin ceza tesis edilmesi ile ilgili eylem hukuki olarak kesintiye uğramış olmaktadır ve kesintiye uğramadan

sonra aynı fiilin icrasına devam edilmesi halinde, zincirleme suç hükümlerinin kıyasen uygulanmaması dolayısıyla yeni bir idari para cezasının tesisi söz konusu olabilecektir (Meran, 2015). Kesintisiz fiillerin ifa edilmesi suretiyle işlenebilen kabahatler bakımından, o kabahate ilişkin şikayet sürecinin nihayete ermiş olması ya da idari yaptırım kararının gereğinin ifa edilmesi önem arz etmemekte olup kabahat teşkil eden kesintisiz eylem idari yaptırıma karar verilmesi suretiyle kesintiye uğrayacaktır. Bu nedenle kesintisiz fiillerin ifa edilmesi suretiyle işlenebilen kabahatlerde somut olaya konu fiil sebebiyle idari yaptırım kararı tesis edilmesine karşın o fiili gerçekleştiren kişi söz konusu fiilin ifasını sürdürüyorsa, o fiile ilişkin olarak idari yaptırım kararının tesis edilmesi ile fiil için kesinti meydana geleceği için idari yaptırım kararının ardından gerçekleştirilen fiil için ayrıca idari yaptırım kararının tesis edilebilmesi mümkündür. Kesintisiz fiille işlenen kabahate ilişkin olarak soruşturmaya/incelemeye başlanmasının ardından ancak idari yaptırıma ilişkin karar verilmeden evvel işlenen kabahat için ise, bu kabahati meydana getiren eylem soruşturulan kabahatin kesintisiz devamı niteliğinde ise ayrıca cezalandırmayı gerektirmeyecektir. Bu noktada belirtmek gerekir ki işlenen kabahatin fail tarafından suç işleme kararına istinaden işlenmesi önem arz etmemektedir ve suç işleme kararına istinaden kabahat işlense dahi zincirleme suça ilişkin düzenlemeler uygulanmayacaktır (Meran, 2015).

"NON BIS IN IDEM" İLKESİNİN SUÇLAR VE KABAHATLER BAKIMINDAN DEĞERLENDİRİLMESİ

5236 sayılı Kanunun 15 inci maddesinin üçüncü fıkrasında; *"Bir fiil hem kabahat hem de suç olarak tanımlanmış ise, sadece suçtan dolayı yaptırım uygulanabilir. Ancak, suçtan dolayı yaptırım uygulanamayan hallerde kabahat dolayısıyla yaptırım uygulanır."* düzenlemesi yer almaktadır. Bu hüküm ile, bir hareketin hem suç hem kabahat teşkil etmesi halinde non bis in idem ilkesinin işlerlik kazanacağı düzenlenmiştir. İlgili hükmün gerekçesinde de bu ilke açıkça dile getirilmiş ve *"Bir fiil, bazı durumlarda hem suç hem de kabahat oluşturabilir. Maddenin üçüncü fıkrası, bu hallere özgü ve fakat sadece içtima ile ilgili bir hüküm içermektedir. Bu gibi durumlarda kişi hakkında sadece suçtan dolayı ceza veya güvenlik tedbirine hükmedilebilecektir; fiilin kabahat oluşturması dolayısıyla ayrıca idarî yaptırım uygulanamayacaktır. Böylece, "non bis in idem" kuralına suçlarla kabahatler arasında da geçerlilik tanınmıştır. Ancak, suçtan dolayı ceza veya güvenlik tedbirine hükmedilemeyen hallerde, kabahat dolayısıyla yaptırım uygulanabilecektir."* açıklamasına yer verilmiştir.

5236 sayılı Kanunun üçüncü fıkrası gereğince; fail tarafından icra edilen fiilin aynı anda hem suç hem de kabahat niteliğini taşıması durumunda, yalnızca suçtan ötürü yaptırım uygulanabilmektedir (Meran, 2015; Geçer, 2016; Cebeci, 2018). Hem suç hem kabahat teşkil eden fiilden ötürü suçtan ötürü yaptırım uygulanmamış olması halinde, kabahatten ötürü yaptırım uygulanabilecektir (Meran, 2015; Cebeci, 2018). Bahse konu fıkra, ceza hukuku ile kabahat hukukunun çakıştığı noktada non bis in idem ilkesinin görünümünü teşkil etmektedir (Cebeci, 2018).

Görüldüğü üzere, non bis in idem ilkesi, failin icra ettiği tek bir fiilden ötürü gerek birden fazla kez yargılanmasını gerek birden fazla defa cezalandırılmasını önlemektedir (Şirin, 2016; Cebeci, 2018). Bununla birlikte, söz konusu ilkenin bir ceza hukuku ilkesi olmasından hareketle aynı kişinin aynı nitelikte olan ve cezalandırılan fiilinden ötürü, ceza davasının yanı sıra idari davanın yahut özel hukuk davasının açılabilmesi mümkündür (Ünver ve Hakeri, 2017). Bu durum Anayasa Mahkemesinin 31/05/2017 tarihli, 2017/28 esas sayılı ve 2017/107 karar sayılı kararında; *"Öte yandan, hukuk devleti ilkesi ve ceza hukukunun temel ilkeleri arasında yer alan "aynı fiilden dolayı iki kez yargılama olmaz (ne bis in idem)" ilkesi gereğince, kişi aynı fiil nedeniyle birden fazla yargılanamaz ve cezalandırılamaz. Ancak, bu ilke mutlak olmayıp, korunan hukuki yararı, unsurları, amacı ve neticesi farklı olması nedeniyle ayrı hukuk disiplinleri kapsamında aynı fiilin farklı şekillerde mütalaa edilmesi mümkündür. Bu ilke sadece ceza davalarına ilişkin olduğu için aynı fiilden dolayı ceza soruşturması yanında ayrıca hukuk davası veya disiplin soruşturması açılmasına engel teşkil etmez. Dolayısıyla bir fiilin söz konusu hukuk disiplinlerinin öngördüğü farklı yaptırımlarla cezalandırılması hukuk devleti ve "aynı fiilden dolayı iki kez yargılama olmaz" ilkesine aykırılık oluşturmaz..."* şeklinde izah edilmiştir (Anayasa Mahkemesi, 31/05/2017 tarihli, 2017/28 esas sayılı ve 2017/107 karar sayılı karar). Danıştay İdari Dava Daireleri Kurulunun 26/10/2020 tarihli, 2019/760 esas sayılı ve 2020/1979 karar sayılı kararında da; *"Hukuk devleti ilkesi ve ceza hukukunun temel ilkeleri arasında yer alan "aynı fiilden dolayı iki kez yargılama olmaz (ne bis in idem)" ilkesi gereğince, kişinin aynı eylem nedeniyle birden fazla yargılanamayacağı ve cezalandırılamayacağı, ancak, bu ilkenin mutlak olmadığı, konu bakımından birbirine benzeseler dahi, korunan hukuki yararı, unsurları, amacı ve neticesi farklı olması nedeniyle aynı fiilin ayrı hukuk disiplinleri kapsamında farklı şekillerde mütalaa edilmesinin mümkün olduğu (Bkz. Anayasa Mahkemesinin 05/03/2015 tarih ve E:2014/124; K:2015/24 sayılı kararı); Öğretide, bu ilkenin idare hukuku içinde de sınırlı bir uygulama alanı bulduğu; idarenin aynı kişiye, iki ayrı sıfatı ve durumu bakımından değerlendirme yapıp aynı eylemden dolayı birden fazla ceza verebildiği, dolayısıyla idari yaptırımlar alanında "ne bis in idem" ilkesinin genellikle geçerli olmadığının kabul edildiği (İlhan Özay, İdari Yaptırımlar, İÜ Yayın No:3326, İstanbul, 1985, s.63,64)"* açıklamalarına yer verilmiştir (Danıştay İdari Dava Daireleri Kurulu, 26/10/2020 tarihli, 2019/760 esas sayılı ve 2020/1979 karar sayılı karar).

"NON BIS IN IDEM" İLKESİNİN 6698 SAYILI KANUN BAKIMINDAN DEĞERLENDİRİLMESİ

Bir Fiilin Aynı Anda İki Farklı Kabahat Teşkil Etmesine İlişkin Olarak

Bilindiği üzere, 5236 sayılı Kanunun 15 inci maddesinin birinci fikrasında bulunan; *"Bir fiil ile birden fazla kabahatin işlenmesi halinde bu kabahatlere ilişkin tanımlarda sadece idarî para cezası öngörülmüşse, en ağır idarî para cezası verilir. Bu kabahatlerle ilgili olarak kanunda idarî para cezasından başka idarî yaptırımlar da öngörülmüş ise, bu yaptırımların her birinin uygulanmasına karar verilir."* hükmü uyarınca; bir fiilin ifa edilmesi suretiyle birden fazla kabahatin oluşması durumunda en ağır idari para cezası uygulanacaktır fakat meydana gelen kabahatlere yönelik olarak idari para cezasının dışında başkaca idari yaptırımların uygulanacağına ilişkin hükümlerin bulunması halinde, bahse konu idari yaptırımların hepsine birlikte karar verilmesi mümkündür (Meran, 2015; Geçer, 2016). Böylelikle, birden fazla idari para cezasının konusunu teşkil eden kabahati oluşturur fiil meydana geldiğinde bu kabahat için düzenlenmiş en ağır idari para cezası ile birlikte söz konusu kabahat için söz konusu olan diğer idari yaptırımlara ilişkin hükümler ayrı ayrı uygulanacaktır (Meran, 2015). Dolayısıyla kişisel verilerin işlenmesi adına gerçekleştirilen bir fiilin hem 6698 sayılı Kanun hem de başkaca bir kanun kapsamında kabahat niteliğini haiz olması durumunda en ağır para cezasının uygulanmasının gerektiği değerlendirilmektedir. Bununla birlikte, 6698 sayılı Kanunun haricindeki para cezasının daha ağır olması dolayısıyla o kanuna ilişkin idari para cezası yaptırımın uygulanmasının Kurul tarafından idari para cezasının dışındaki yaptırımlara karar verilmesi bakımından bir engel teşkil etmeyeceği düşünülmekte olup örneğin, başkaca bir kanundan ötürü idari para cezası uygulanmış bir fiil için Kurulca 6698 sayılı Kanunun 15 inci maddesinin yedinci fikrasında bulunan; *"Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verebilir."* hükmü uyarınca idari yaptırım kararı tesis edilebilecektir.

Kabahat Teşkil Eden Bir Fiilin Aynı Kişi Tarafından Birden Fazla Kez İşlenmesine İlişkin Olarak

Bilindiği üzere; 5236 sayılı Kanun 15 inci maddesinin ikinci fikrası uyarınca; aynı kabahatin aynı fail tarafından birden fazla kez işlenmesi durumunda işlenen her kabahat için ayrı ayrı idari para cezası tesis edilecektir. Dolayısıyla, aynı veri sorumlusu tarafından 6698 sayılı Kanuna aykırılık teşkil eden fiilin tekraren işlenmesi halinde, meydana getirilen her kabahat için veri sorumlusu hakkında ayrı ayrı idari para cezasının kesilebileceği değerlendirilmektedir. Bununla birlikte, yine 5326 sayılı Kanunun 15 inci maddesinin ikinci fikrasında bulunan; *"... Kesintisiz fiille işlenebilen kabahatlerde, bu nedenle idarî yaptırım kararı verilinceye kadar fiil tek sayılır."* cümlesi dolayısıyla 6698 sayılı Kanuna aykırılık teşkil eden ve kesintisizlik arz eden fiil bakımından Kurulca bir idari yaptırıma ilişkin karar tesis edilinceye değin bu fiil tek sayılacaktır. Örneğin; 6698 sayılı Kanunun 12 nci maddesindeki veri güvenliğinin sağlanmasına yönelik yükümlülükler bakımından, aynı veri sorumlusu tarafından farklı tarihlerde, farklı şubelerde ve farklı çalışanlar tarafından gerçekleştirilen veri ihlallerinin kaynağını teşkil eden ve alınmayan teknik ve idari tedbirin, her bir veri ihlali için ayrı ayrı alınması gerekip gerekmediğinin, bu ihlallerin oluşumu bakımından başlangıçta alınmayan tek bir teknik ve idari tedbirin etkili olup olmadığının, aynı veri sorumlusu bünyesinde farklı tarihlerde, farklı şubelerde ve farklı çalışanlar tarafından gerçekleştirilen veri ihlallerinin her biri için teknik ve idari tedbirlerin münhasıran alınıp alınmamasının etkili olup olmadığının her bir veri ihlali özelinde değerlendirilmesi gerekmektedir. Bu kapsamda, her bir veri ihlalinin temelini teşkil eden teknik veya idari tedbirin (örneğin; başlangıçta alınması gereken ve veri ihlallerinin tamamının önlenmesi bakımından yeterli olacak teknik bir tedbir) veri sorumlusu tarafından alınmamış olması ve bu sebeple birden çok veri ihlalinin meydana gelmesi durumunda "kesintisiz fiille işlenen kabahat"ten bahsedilebilecektir. Burada önemli olan, söz konusu tedbirin alınmamasının, ihlallerin meydana geldiği süreçte veri sorumlusunun tek bir fiili olarak ele alınıp alınamayacağıdır. Diğer taraftan, her bir veri ihlalinin temelini teşkil eden teknik veya idari tedbirin (örneğin; her bir veri ihlali bakımından, somut durum özelinde alınması gereken bir idari tedbir) veri sorumlusu tarafından alınmamış olması ve bu sebeple spesifik olarak ihlallerden birinin meydana gelmesi durumunda "kesintisiz fiille işlenen kabahat"ten bahsedilemeyeceği ve her bir kabahat bakımından ayrı ayrı yaptırım uygulanması gerektiği değerlendirilmektedir.

Bir Fiilin Hem Suç Hem Kabahat Teşkil Etmesine İlişkin Olarak

Öncelikle belirtmek gerekir ki 6698 sayılı Kanunun 15 inci maddesinin ikinci fikrası; *"1/11/1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde belirtilen şartları taşımayan ihbar veya şikâyetler incelemeye alınmaz."* hükmünü amir olup 1/11/1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinin (b) bendi uyarınca; yargı mercilerinin görev alanına dahil olan konulara dair olan dilekçeler incelenememektedir. Bir fiilin hem suç hem kabahat teşkil ettiği hallerde, fiilin suç boyutunun yargı mercilerinin görevine girdiği muhakkaktır fakat bu fiilin kabahat boyutu idari makamların görev alanına girmektedir. Bir fiilin aynı zamanda

hem suç hem kabahat teşkil ettiği halde ise bu durum Kabahatler Kanununun 15 inci maddesinin üçüncü fıkrası kapsamında değerlendirilecek ve bahse konu fiil hakkında suçtan dolayı bir yaptırım uygulanmışsa, artık kabahatten dolayı yaptırım uygulanamayacaktır.

Tüzel Kişilik ile Tüzel Kişiliğin Parçası Olan Gerçek Kişiliğe İlişkin Olarak

Non bis in idem ilkesini tüzel kişiliğin organları yahut çalışanları ile tüzel kişiliğin bizzat kendisi arasında işlerlik kazanmayacağını yukarıda belirtmiştik. Zira, tüzel kişilikten ayrı kişiliği haiz olan gerçek kişilerin yargılanmalarından ötürü tüzel kişiliğin non bis in idem ilkesi kapsamında değerlendirilmesi halinde, ilkenin fiili gerçekleştirenin "aynı kişi" olması unsurunun karşılandığı söylenemeyecektir. Bu çerçevede, Örneğin Kişisel Verileri Koruma Kurumuna intikal eden bir şikayet yahut ihbar dosyası doğrultusunda şikayet edilen kişinin kim olduğunun, bir tüzel kişiliğe ilişkin bir ihbar veya şikayet dosyası kapsamında tüzel kişiliğin bizzat kendisinin mi yoksa tüzel kişiliğin bir organının yahut çalışanının mı şikayet edildiğinin net bir şekilde ortaya konulması suretiyle veri sorumlusunun doğru bir şekilde tespit edilmesi gerekmektedir. Dolayısıyla, Kurumumuza yapılan şikâyet, şayet tüzel kişiliğe yönelik yapıldıysa ve bu tüzel kişilik somut olay özelinde veri sorumlusu niteliğindeyse, bu tüzel kişiliğin bir organına yahut yöneticisine veya çalışanına ilişkin olarak bir ceza yargılaması yürütülüyor ise yahut ceza davasının sonunda hüküm kurulmuşsa; non bis in idem ilkesinin "aynı kişi" unsurunun söz konusu olmayacağı bu sebeple bu ilkenin işlerlik kazanmayacağı ve tüzel kişilik için Kişisel Verileri Koruma Kurulu tarafından ayrıca bir inceleme sürecinin yürütülebileceği değerlendirilmektedir.

Kaldı ki 5236 sayılı Kanunun 8 inci maddesinin birinci fıkrası; *"Organ veya temsilcilik görevi yapan ya da organ veya temsilci olmamakla birlikte, tüzel kişinin faaliyeti çerçevesinde görev üstlenen kişinin bu görevi kapsamında işlemiş bulunduğu kabahatten dolayı tüzel kişi hakkında da idarî yaptırım uygulanabilir."* hükmünü amir olup bu hüküm uyarınca tüzel kişinin gerçekleştirdiği faaliyetleri kapsamında görev üstlenen kişilerin icra ettikleri görevlerinden ötürü işledikleri kabahatten dolayı tüzel kişiye ilişkin olarak idari yaptırım uygulanabilmektedir.

Öte yandan belirtmek gerekir ki bir tüzel kişilik nezdinde tüzel kişiliğin faaliyetleri doğrultusunda gerçekleştirilen kişisel veri işlemeleri bakımından; çalışanlar, genel müdür, genel müdür yardımcısı ya da yönetim kurulu üyeleri değil tüzel kişiliğin bizzat kendisi veri sorumlusu sıfatını haiz olmaktadır ve 6698 sayılı Kanunun 18 inci maddesinin ikinci fıkrasında, bahse konu maddede düzenlenen idari paralara ilişkin cezaların muhatabının veri sorumlusu sıfatını haiz gerçek

kişi konumundaki kişiler ile özel hukuka tabi tüzel kişiler olduğu hükme bağlanmıştır. Örneğin; tüzel kişiliği bulunan bir şirket nezdinde meydana gelen kişisel veri ihlalleri bakımından, yapılacak incelemede veri sorumlusu olarak ilgili tüzel kişiliğin herhangi bir organı değil bizzat kendisi dikkate alınmaktadır. Bu kapsamda, tüzel kişiliği haiz organizasyon dâhilinde gerçekleşen kişisel veri ihlali bakımından sorumluluğun kimde olduğunun belirlenmesi ve bu doğrultuda genel hükümler uyarınca gerekli rücu mekanizmalarının işletilmesi ile sorumluluğun paylaştırılması hususları, veri sorumlusu tüzel kişiliğin kendi iç işleyişi çerçevesinde ayrıca değerlendirilmesi gereken bir konudur.

Bu çerçevede belirtmek gerekir ki; veri sorumlusu sıfatını haiz tüzel kişilikler nezdinde meydana gelen hukuka aykırı kişisel veri işleme faaliyetleri bakımından, hukuka aykırı fiil yahut fiilleri gerçekleştiren gerçek kişilerin TCK'da düzenlenen suçlar doğrultusunda cezai sorumluluklarının bulunup bulunmadığına ilişkin olarak yargı makamlarınca yapılacak yargılamanın dışında; 6698 sayılı Kanunun 18 inci maddesinin birinci fıkrasının (b) bendi kapsamında Kişisel Verileri Koruma Kurulu tarafından, veri sorumlusu tüzel kişiliğin söz konusu hukuka aykırılık teşkil eden kişisel veri işleme faaliyeti bakımından kişisel verilerin hukuka aykırılık teşkil edecek şekilde işlenmesini engelleyecek gereken tüm teknik ve idari tedbirleri alıp almadığı yönünde inceleme yapılabileceği değerlendirilmektedir. Zira, Kanunda ve ilgili mevzuatta yer alan, veri sorumlusuna ilişkin yükümlülüklerin yerine getirilmesinin veri sorumlusu sıfatını haiz kişilerin sorumluluğunda olduğu; veri güvenliğine ilişkin gerekli idari ve teknik tedbirlerin alınmamasından ötürü meydana gelecek kişisel veri ihlalleri ve hukuka aykırı kişisel veri işleme faaliyetleri dolayısıyla veri sorumlusu niteliğini haiz kişiliğin sorumlu olacağı açıktır.

Kişisel Verileri Koruma Kurumuna intikal eden bir şikâyet yahut ihbar tüzel kişinin bir organı, yöneticisi veya çalışanı konumunda bir kimseye yönelik olarak yani tüzel kişiliğin bünyesinde faaliyet gösteren bir gerçek kişiye ilişkin olarak gerçekleştirildiyse öncelikle bu gerçek kişinin tüzel kişilikten bağımsız olarak veri sorumlusu sıfatını haiz olup olmadığının değerlendirilmesi gerekmektedir. Kural olarak, tüzel kişinin bir organı, yöneticisi veya çalışanı konumunda bulunan bir kimsenin yani tüzel kişiliğin bünyesinde faaliyet gösteren bir gerçek kişinin gerçekleştirdiği hukuka aykırı kişisel veri işleme faaliyeti bakımından, bu kimseyi bünyesinde istihdam eden tüzel kişiliğin sorumluluğu söz konusu olacaktır. Nitekim, veri sorumlusu, bünyesinde istihdam ettiği çalışanlarının 6698 sayılı Kanuna ve ilgili ikincil mevzuata uygun hareket etmelerini sağlamaya yönelik olarak sorumluluk altında olup çalışanların ayrı bir veri sorumlusu sıfatı bulunmamaktadır ve veri sorumlusunun gereken veri güvenliği düzeyini temin etmeye

ilişkin olarak hayata geçirmesi gereken idari tedbirlerden biri de; çalışanların eğitilmesi ve farkındalık çalışmalarının yürütülmesidir.

Aynı Tüzel Kişinin Gerçekleştirdiği Fiilin
Hem Suç Hem Kabahat Teşkil Etmesine İlişkin Olarak

Hakkında dava açılan ve şikayette veya ihbarda bulunulan kişinin aynı tüzel kişi olması ve bu tüzel kişinin veri sorumlusu sıfatını haiz olması durumunda ise TCK'nın 140 ıncı maddesinde yer alan; *"Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* hükmü uyarınca kişisel verilere yönelik suçlardan biri ile yargılanan ve suçun faili konumundaki tüzel kişiler için TCK'nın 60 ıncı maddesinde düzenlenmiş olan güvenlik tedbirlerine hükmedilebilecektir (Gökcan ve Artuç, 2021; Korkmaz, 2017; Orak, 2020; Gültaş, 2017; Sert, 2019). 5326 sayılı Kanunun 15 inci maddesinin üçüncü fikrası uyarınca; ancak suçtan ötürü yaptırım uygulanmamışsa kabahat dolayısıyla yaptırım uygulanabildiğinden, hakkında dava açılan ve şikayette veya ihbarda bulunulan aynı tüzel kişiye ilişkin olarak yargı makamlarınca tüzel kişilere münhasır güvenlik tedbirlerine hükmedilmiş olması hasebiyle yaptırım uygulanmışsa, artık 6698 sayılı Kanun uyarınca idari yaptırım uygulanamayacaktır. Fakat, tüzel kişi hakkında suçtan ötürü herhangi bir yaptırım yani güvenlik tedbiri uygulanmamışsa kabahatten ötürü yaptırım uygulanması mümkündür (Meran, 2015). Bununla birlikte, hakkında güvenlik tedbirine hükmedilen tüzel kişi bakımından söz konusu cezai yaptırımın hangi suçtan ötürü uygulandığı önem arz etmektedir.

Zira, TCK'nın 135 inci maddesi uyarınca kişisel verilerin kaydedilmesi bir suç olarak düzenlenmiş olup kişisel verilerin kaydedilmesi de 6698 sayılı Kanun gereğince bir işleme faaliyeti niteliğindedir. TCK'nın 136 ncı maddesinde ise; kişisel verilerin verilmesi, yayılması ve ele geçirilmesi gibi durumlar suç olarak düzenlenmiş olup bu fiiller de kişisel verilerin işlenmesi anlamına gelecektir, zira 6698 sayılı Kanunun kişisel verilerin işlenmesine yönelik düzenleme içerir hükmünde *"ele geçirme", "açıklama", "aktarılma"* gibi fiiller de kişisel verilerin işlenmesi faaliyetine örnek olarak sayılmıştır. TCK'nın 137 nci maddesinde ise kişisel verilerin yok edilmemesi suçu düzenlenmiştir ve kişisel verilerin yok edilmesi 6698 sayılı Kanun kapsamında kişisel verilerin imhası olarak karşımıza çıkmaktadır (Dülger, 2020; Turan, 2021). Görüldüğü üzere; TCK'da düzenlenen kişisel verilere yönelik suçlar ile 6698 sayılı Kanunda bulunan kişisel verilere ilişkin kabahatlerin çakıştığı noktalar bulunmaktadır. Bu durumlarda, hakkında dava açılan ve şikayette veya ihbarda bulunulan aynı tüzel kişinin gerçekleştirdiği fiil dikkatle irdelenmeli, TCK ve 6698 sayılı Kanun kapsamında "aynı fiil" olarak ele alınıp alınamayacağı

değerlendirilmelidir. Bu kapsamda örneğin; 6698 sayılı Kanunun 18 inci maddesinin birinci fikrasının (b) bendi kapsamında Kişisel Verileri Koruma Kurulu tarafından, veri sorumlusu tüzel kişiliğin söz konusu hukuka aykırı kişisel veri işleme faaliyeti bakımından kişisel verilerin hukuka aykırılık teşkil edecek bir biçimde işlenmesini engelleyecek gerekli ve yeterli bütün teknik ve idari önlemleri alıp almadığı yönünde inceleme yapılabileceği değerlendirilmektedir. Zira, 6698 sayılı Kanunda ve ilgili mevzuatta yer alan, veri sorumlusuna ilişkin yükümlülüklerin yerine getirilmesinin veri sorumlusu sıfatını haiz kişilerin sorumluluğunda olduğu; veri güvenliğine ilişkin gerekli idari ve teknik tedbirlerin alınmamasından ötürü meydana gelecek kişisel veri ihlalleri ve hukuka aykırı kişisel veri işleme faaliyetleri dolayısıyla veri sorumlusu niteliğini haiz kişiliğin sorumlu olacağı açık olup 6698 sayılı Kanunun 12 nci maddesinin birinci fikrası uyarınca kişisel verilerin hukuka aykırılık teşkil edecek şekilde işlenmesini engellemek, kişisel verilere hukuka aykırı olacak biçimde erişilmesini önlemek ve işlenen kişisel verilerin muhafazasını yani korunmasını sağlamak maksadıyla gerekli olan uygun veri güvenliği seviyesini temin etmeye yarayacak gereken tüm teknik ve idari tedbirleri alma fiilinin TCK'da karşılığının bulunmadığı değerlendirilmektedir. Benzer şekilde, 6698 sayılı Kanun kapsamında yaptırıma tabii tutulan aydınlatma yükümlülüğünün yerine getirilmemesi, Kurul kararlarının gereğinin yerine getirilmemesi, Sicile kayıt ve bildirim yükümlülüğünün ihlalinin de TCK'da suç olarak bir karşılığının bulunmamasından ötürü bu yükümlülüklere uygulanan yaptırımlar bakımından "aynı fiilin hem suç hem kabahat teşkil etmesi" noktasında non bis in idem ilkesinin işlerlik kazanmayacağı kanaatindeyiz.

Aynı Gerçek Kişinin Gerçekleştirdiği Fiilin
Hem Suç Hem Kabahat Teşkil Etmesine İlişkin Olarak

Hakkında dava açılan ve şikayette veya ihbarda bulunulan kişinin aynı gerçek kişi olması ve bu gerçek kişinin veri sorumlusu sıfatını haiz olması durumunda farklılıklar ortaya çıkacaktır. Zira, 6698 sayılı Kanunun 3 üncü maddesinin birinci fikrasının (ı) bendinde bulunan; *"Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi."* şeklindeki tanım uyarınca gerçek kişilerin de veri sorumlusu sıfatına sahip olması mümkündür. Yeter ki bu gerçek kişilerce kişisel verilerin işleme amaçları ile vasıtaları belirlensin ve bu gerçek kişiler, veri kayıt sisteminin kurulması fiilinden ve bu sistemin yönetilmesinden sorumlu olsunlar. Hakkında dava açılan ve şikayette veya ihbarda bulunulan kişinin aynı gerçek kişi olması ve bu gerçek kişinin veri sorumlusu sıfatını haiz olması durumunda, non bis in idem ilkesinin "aynı kişi" unsuru sağlanmış olacağından, bu kişinin ifa ettiği fiilin aynı zamanda hem suç hem kabahat teşkil etmesi halinde non bis in idem ilkesi

işlerlik kazanacaktır. Zira, TCK'nın 135 inci maddesi uyarınca kişisel verilerin kaydedilmesi bir suç olarak düzenlenmiş olup kişisel verilerin kaydedilmesi de 6698 sayılı Kanun gereğince bir işleme faaliyeti niteliğindedir. TCK'nın 136 ncı maddesinde ise; kişisel verilerin üçüncü bir kişiye verilmesi, yayılması ve kişisel verilerin hukuka aykırılık teşkil edecek şekilde ele geçirilmesi gibi durumlar suç şeklinde düzenlenmiş olup sözü edilen fiiller de kişisel verilerin işlenmesi anlamına gelecektir, zira 6698 sayılı Kanunun kişisel verilerin işlenmesine yönelik düzenleme içerir hükmünde *"ele geçirme", "açıklama", "aktarılma"* gibi fiiller de kişisel verilerin işlenmesi faaliyetine örnek olarak sayılmıştır. TCK'nın 137 nci maddesinde ise, kişisel verilerin yok edilmemesi suçu düzenlenmiştir ve kişisel verilerin yok edilmesi 6698 sayılı Kanun kapsamında kişisel verilerin imhası olarak karşımıza çıkmaktadır (Dülger, 2020; Turan, 2021). Görüldüğü üzere; TCK'da düzenlenen kişisel verilere yönelik suçlar ile 6698 sayılı Kanunda bulunan kişisel verilere ilişkin kabahatlerin çakıştığı noktalar bulunmaktadır. Bu durumlarda, hakkında dava açılan ve şikayette veya ihbarda bulunulan aynı gerçek kişinin gerçekleştirdiği fiil dikkatle irdelenmeli, TCK ve 6698 sayılı Kanun kapsamında "aynı fiil" olarak ele alınıp alınamayacağı değerlendirilmelidir. Bu kapsamda örneğin, 6698 sayılı Kanunun 18 inci maddesinin birinci fıkrasının (b) bendi kapsamında Kişisel Verileri Koruma Kurulu tarafından, veri sorumlusu gerçek kişinin söz konusu hukuka aykırı kişisel veri işleme faaliyeti bakımından kişisel verilerin hukuka aykırı olacak şekilde işlenmesini engelleyecek gereken teknik ve idari tedbirleri alıp almadığı yönünde inceleme yapılabileceği değerlendirilmektedir. Zira, 6698 sayılı Kanunda ve ilgili mevzuatta yer alan, veri sorumlusuna ilişkin yükümlülüklerin yerine getirilmesinin veri sorumlusu sıfatını haiz kişilerin sorumluluğunda olduğu; veri güvenliğine ilişkin gerekli idari ve teknik tedbirlerin alınmamasından ötürü meydana gelecek kişisel veri ihlalleri ve hukuka aykırı kişisel veri işleme faaliyetleri dolayısıyla veri sorumlusu niteliğini haiz kişiliğin sorumlu olacağı açık olup 6698 sayılı Kanunun 12 nci maddesinin birinci fıkrası uyarınca kişisel verilerin hukuka aykırılık teşkil edecek şekilde işlenmesini engellemek, kişisel verilere hukuka aykırı olacak biçimde erişilmesini önlemek ve işlenen kişisel verilerin muhafazasını yani korunmasını sağlamak maksadıyla gerekli olan uygun veri güvenlik seviyesini temin etmeye yarayacak gereken tüm teknik ve idari tedbirleri alma fiilinin TCK'da karşılığının bulunmadığı değerlendirilmektedir. Benzer şekilde, 6698 sayılı Kanun kapsamında yaptırıma tabii tutulan aydınlatma yükümlülüğünün yerine getirilmemesi, Kurul kararlarının gereğinin yerine getirilmemesi, Sicile kayıt ve bildirim yükümlülüğünün ihlalinin de TCK'da suç olarak bir karşılığının bulunmamasından ötürü bu yükümlülüklere uygulanan yaptırımlar bakımından "aynı fiilin hem suç hem kabahat teşkil etmesi" noktasında non bis in idem ilkesinin işlerlik kazanmayacağı kanaatindeyiz.

Bununla birlikte, TCK'nın 135 inci maddesinde hüküm altına alınan kişisel verilerin kaydedilmesi fiilinin, TCK'nın 136 ncı maddesinde bulunan kişisel verilerin üçüncü bir kişiye verilmesi, yayılması ve ele geçirilmesi fiillerinin ve TCK'nın 137 nci maddesindeki kişisel verilerin yok edilmemesine yönelik fiilin 6698 sayılı Kanun kapsamında kişisel verilerin işlenmesinin ve imhasının doğrudan karşılığı olarak kabul edilmesi ve 6698 sayılı Kanunun 18 inci maddesinin birinci fıkrasının (b) bendinde düzenlenen yaptırımın suç teşkil eden aynı nitelikteki fiiller bakımından uygulandığının düşünülmesi halinde ise, veri sorumlusu sıfatını haiz gerçek kişinin ilgili suçtan ötürü yargılanmış olması söz konusuysa yargılamanın sonucunda bu kişi hakkında yaptırım uygulanıp uygulanmadığı ve yaptırımın mahiyeti irdelenmelidir. Örneğin; bu gerçek kişi hakkında önceden yapılan yargılama sonucunda CMK'nın 223 üncü maddesinin ikinci fıkrasının (e) bendinde yer alan; *"Yüklenen suçun sanık tarafından işlendiğinin sabit olmaması."* düzenlemesine istinaden verilen beraate ilişkin kararın; bahse konu kişi hakkında aynı hareket dolayısıyla idari yaptırım uygulanmasına, bu sebeple de Kişisel Verileri Koruma Kurumuna intikal eden şikâyetin yahut ihbarın incelenmesine engel teşkil etmeyeceği düşünülmektedir. Zira, 5236 sayılı Kanunun 15 inci maddesinin üçüncü fıkrası uyarınca; suçtan ötürü yaptırım uygulanamayan durumlarda kabahatten ötürü yaptırım uygulanabilecek olup, şikayet yahut ihbar edilen kişi hakkında, CMK'nın 223 üncü maddesinin ikinci fıkrasının (e) bendi uyarınca hüküm kurulması yani yüklenen suçun işlendiğinin sabit olmaması gerekçesiyle beraat kararı verilmesi halinde bu kişi hakkında suçtan dolayı herhangi bir yaptırım uygulanmamıştır. TCK'nın 45 inci maddesi gereğince; bir suç söz konusu olduğunda uygulanan yaptırımlar hapis cezası ile adli para cezası olup; beraat kararı bir yaptırım olmayıp bir hüküm niteliğindedir (Çınar, 2019).

Öte yandan ceza mahkemesi tarafından, davaya konu fiilin hakkında dava açılan kişinin işlememesinden ötürü, yani CMK'nın 223 üncü maddesinin ikinci fıkrasının (b) bendinde yer alan; *"Yüklenen suçun sanık tarafından işlenmediğinin sabit olması."* düzenlemesine istinaden beraate ilişkin kararın verilmesi halinde, hakkında dava açılan ve Kişisel Verileri Koruma Kurumuna şikayet yahut ihbar edilen kişi hakkında idari para cezasının uygulanmamasının gerektiği kanaatindeyiz. Zira, artık bir idari otorite olan Kişisel Verileri Koruma Kurumunun, bahse konu kişinin davaya ve şikayete yahut ihbara konu edilen fiili işlemediğine dair kesin hüküm (yargı kararı) ile bağlı olacağı değerlendirilmektedir (Karabel, 2015). Ancak, hakkında dava açılan ve şikayet veya ihbarda bulunulan kişiye yönelik olarak CMK'nın 223 üncü maddesinin ikinci fıkrasının (b) bendi uyarınca yüklenen suçu işlemediğinin sabit olması dolayısıyla değil de CMK'nın 223 üncü maddesinin ikinci fıkrasının (e) bendi uyarınca yüklenen suçu işlediğinin sabit olmaması dolayısıyla beraat kararı verilmesi durumları arasında önemli bir

fark bulunmaktadır. Delil yetersizliğinden ötürü beraat olarak da kabul edilen CMK'nın 223 üncü maddesinin ikinci fıkrasının (e) bendi (Ormanoğlu, 2016), "şüpheden sanık yararlanır ilkesi" kapsamında, hâkim tarafından mahkumiyet kararı verilebilmesi için hakkında dava açılan kişiye ilişkin olarak tam bir kanaate varılamaması halinde devreye girmektedir. Bu noktada, hakim nezdinde oluşan şüphe, daha doğrusu hakimin sanık hakkında şüpheye yer bırakmayacak tam bir kanaate sahip olmaması rol oynamaktadır (Şenses, 2012). Dolayısıyla hakkında dava açılan ve şikayette veya ihbarda bulunulan kişi hakkında CMK'nın 223 üncü maddesinin ikinci fıkrasının (e) bendi gereğince verilen beraat kararı, bahse konu suçun o kişi tarafından işlenmediğinin bir yargı makamı tarafından kesin hükme bağlanması anlamına gelmemektedir. Zira, ceza mahkemesince sanığın suçsuzluğunun sabit olmasına karar verilmesinin bağlayıcı bir olgu olmasının yanı sıra, suçluluğun sabit olmadığı kararı maddi bir gerçeğin tespitine değil, aksine tespit edilememesine ilişkindir (Bahçeci, 2018). Örneğin Kişisel Verileri Koruma Kurulunca incelenen bir şikâyet bakımından, hakkında dava açılan ve şikayette bulunulan kişiye ilişkin olarak TCK'nın 136 ncı maddesine aykırılık dolayısıyla açılan ceza davası neticesinde beraat kararı verilmiş ve dosyadan anlaşıldığı kadarıyla istinaf yoluna başvurulmamasının sonucu olarak bu karar kesinleşmişse, Kişisel Verileri Koruma Kurumuna intikal eden şikâyetin içeriği bu kişinin fiilinin kabahat boyutu olduğundan, yukarıda açıklandığı üzere bahse konu fiilin suç boyutu uyarınca bahse konu kişi hakkında yaptırım uygulanmamış olması dolayısıyla, söz konusu kabahat için idari yaptırım uygulanmasının önünde hiçbir engel olmadığı ve bu doğrultuda da şikâyet başvurusunun incelenmesi bakımından herhangi bir engelin bulunmayacağı değerlendirilmektedir.

SONUÇ

Kişisel verilerin korunmasına yönelik düzenlemeler, ülkemiz bakımından yeni yeni oluşmaya başlamış olup bu sürecin daha uzun ve karmaşık bir yol olacağı kanaatindeyiz. Çalışmamızda mevcut düzenlemeler, doktrin, içtihat ve Kurul kararları doğrultusunda kişisel verilerin korunması hukukunun temel aktörlerinden olan veri sorumlusu kavramı ve veri sorumlusunun yükümlülüklerine ilişkin hususlar açıklanmıştır. Bu noktada önemle belirtmek gerekir ki; veri sorumlusunun haiz olduğu yükümlülükler oldukça önemlidir, zira, kişisel verilerin korunmasını isteme şeklinde isimlendirilen anayasal niteliği haiz temel hakka müdahalenin sınırlarını büyük oranda bu yükümlülükler çizmektedir. Öte yandan temel hakkına müdahale edilen ilgili kişiler çoğunlukla, bu yükümlülüklerin doğrudan muhatabı konumunda olduğundan veri sorumluları tarafından kendilerine yüklenen yükümlülüklerin gereği gibi yerine getirilmesi ilgili kişilerin haklarının korunması bakımından da gereklidir. Diğer taraftan konunun kamu düzenini ilgilendiren boyutu da gözden kaçırılmamalıdır. Zira, bireylerin sürekli takip ediliyor gibi hissetmelerinin, mahremiyetlerinin sınırlarının aşılmamasının, kendilerine ait bilgiler üzerinde kendi denetim mekanizmalarını yürütebilmelerinin bir gereği olarak kişisel verilerin korunması hakkı karşımıza çıkmakta olup bu konuda kendini güvende hisseden bireyler topluma ve Devlete karşı da daha güven dolu yaklaşmaktadır.

Veri sorumlularının gerçekleştirdiği kişisel veri işleme faaliyetlerinin her aşamasında 6698 sayılı Kanunda düzenleme altına alınan kurallara ve prensiplere uygun hareket etmelerinin gerekmesinin yanı sıra bu Kanundan kaynaklanan pek çok yükümlülükleri de bulunmaktadır. Bu yükümlülükler genel anlamda; aydınlatma yükümlülüğünün yerine getirilmesi, veri sorumluları siciline kayıt ve bildirim, kişisel veri işleme envanteri ve kişisel veri işleme ve saklama politikası hazırlama, ilgili kişiye cevap verme, veri güvenliğinin sağlanması, Kişisel Verileri Koruma Kurulu kararlarının yerine getirilmesi ve imha yükümlülüğü olarak karşımıza çıkmaktadır. Bahsedilen bu temel yükümlülükler de kendi içlerinde başkaca kuralları ve yükümlülükleri barındırmaktadır.

Kişisel verilerin korunması hakkı o kadar ehemmiyetlidir ki bu hakka ilişkin koruma yalnızca 6698 sayılı Kanun ile sınırlı kalmamıştır. Öyle ki çerçeve bir kanun niteliğini haiz olan 6698 sayılı Kanunun 2016 yılında yürürlüğe girmesinden evvel, TCK'da kişisel verilerin korunmasına yönelik hükümler bulunmaktadır. TCK'nın dokuzuncu bölümünde özel hayata ve hayatın gizli alanına karşı suçlar düzenlenmiştir. Anılan bölümde haberleşmenin gizliliğinin ihlali, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğini

ihlal gibi suçların yanı sıra münhasıran kişisel verilerle alakalı suçlara da yer verilmiştir. TCK'nın 135 inci maddesinde *"kişisel verilerin kaydedilmesi"* suçu, 136 ncı maddesinde *"Verileri hukuka aykırı olarak verme veya ele geçirme"* suçu, 137 nci maddesinde bahse konu suçların *"Nitelikli haller"*i, 138 inci maddesinde ise *"Verileri yok etmeme"* suçu düzenlenmiştir. Kişisel verilerin korunmasına ilişkin TCK'da dolaylı bir biçimde koruma sağlayan hükümler de bulunmakta olup bunlar örneğin; TCK'nın *"Haberleşmenin gizliliğini ihlal"* başlıklı 132 nci maddesi, *"Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması"* başlığı altında düzenlenen 133 üncü maddesi, *"Özel hayatın gizliliğini ihlal"* başlığını haiz 134 üncü maddesi, *"Bilişim sistemine girme"* başlıklı 243 üncü maddesidir.

Kişisel verilerin korunması hakkını koruyan hükümler 6698 sayılı Kanun ve TCK ile sınırlı olmayıp pek çok mevzuatta çeşitli şekillerde düzenlemelere tabi tutulmuştur. Birden fazla mevzuatta düzenleme altına alınan bir husus bakımından "non bis in idem" ilkesinin işlerlik kazanması kaçınılmaz bir sonuçtur. Kabahatler hukukuna da sirayet eden bir ceza genel ilkesi olan non bis in idem ilkesi oldukça karmaşık ve çetrefilli bir konu olmasının yanı sıra gerek hukuk devleti ile adaletin tesisi bakımından gerek kişilerin hukuki güvenliğinin sağlanması adına oldukça önemli bir kavram olarak karşımıza çıkmaktadır. Bu sebeple konunun önemine binaen çalışmamızda non bis in idem ilkesi açıklanmış, bu ilkenin hukukumuza yansıma biçimi ve hukukumuzdaki çeşitli görünümleri ele alınmıştır. Bu minvalde, non bis in idem ilkesinin suçlar ve kabahatler bakımından özellik arz eden durumları üzerinde bilhassa durulmuştur.

Non bis in idem ilkesi, bazı ülkelerde anayasal bir ilke olarak düzenlenmişken ülkemiz için bir ceza genel ilkesi olarak kabul edilmiştir. Bununla birlikte, non bis in idem ilkesi, Avrupa İnsan Hakları Sözleşmesinin 7 numaralı protokolünde de yer almaktadır fakat bu protokolün ülkemiz tarafından onaylanması 25/03/2016 tarihini bulmuştur. Bu ilkenin, iki unsuru bulunmakta olup bunlar "aynı kişi" ve "aynı fiil"dir. Söz konusu ilkenin işlerlik kazandığı durumlarda bu iki unsurun sağlanıp sağlanmadığının dikkatle irdelenmesi gerekmekte olup 6698 sayılı Kanun çerçevesinde her bir değerlendirmenin somut olay özelinde gerçekleştirilmesi yerinde olacaktır. ◆

KAYNAKÇA

- Altındere, M. (2020). *Kişisel Verilerin Korunması Hukuku ve Uygulaması.* Ankara: Adalet Yayınevi.
- Artuk, M. E., Gökcen A. ve Yenidünya C. (2014). *Türk Ceza Kanunu Şerhi,* 1. Ankara: Adalet Yayınevi.
- Bahçeci, B. (2018). İHAM'ın Vergi Cezalarında Ne Bis İn İdem İçtihadı ile Türk Hukukunun Uyum Sorunu, *Türkiye Barolar Birliği Dergisi,* 136, 141-166, Erişim adresi: https://kutuphane.dogus.edu.tr/mvt/pdf.php?pdf=0021564&lng=0
- Bockel, W. B. van, (2009), *The ne bis in idem principle in EU law – A conceptual and jurisprudential analysis,* (Doktora Tezi). Erişim adresi: https://openaccess.leidenuniv.nl/bitstream/handle/1887/13844/000-diss-VanBockel-26-05-2009.pdf?sequence=1
- Cebeci, Ş. (2018). *Türk Ceza Hukuku Bağlamında Ne Bis In Idem İlkesi,* (Yüksek Lisans Tezi), Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=mr5rRtpWjamI4RGv23L7sA&no=nrzkEHoAS1dBA4BhRz2xnA
- Çekin, M. S. (2020). *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku.* İstanbul: On İki Levha Yayıncılık.
- Çınar A.R. (2009). Hükmün Konusu ve Eylemi (Fiili) Değerlendirmede Mahkemenin Yetkisi, *Türkiye Barolar Birliği Dergisi,* 22(84) 31-62, Erişim adresi: https://www.jurix.com.tr/article/10702
- Demirezen, M. (2020). *Kişisel Verilerin Korunması Hukuku ve Uyum Projelerinin Yürütülmesi,* İstanbul: Platon Hukuk Yayınevi.
- Dülger, M. V. (2020). *Kişisel Verilerin Korunması Hukuku.* İstanbul: Hukuk Akademisi Eğitim ve Yayıncılık.
- Geçer, A. E., (2016), Vergi Ceza Hukukunda Non Bis In Idem İlkesi, *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 65(2), 315-348, Erişim adresi: https://dergipark.org.tr/tr/download/article-file/622047

◊ Göçmen Uyarer, S. (2020). *Kişisel Verilerin Korunması.* Ankara: Seçkin Yayıncılık.

◊ Gökcan, H.T. ve Artuç, M. (2021). *Pratik Türk Ceza Kanunu.* Ankara: Adalet Yayınevi.

◊ Göktürk, N., Özgenç, İ. ve Üzülmez İ. (2012). *Ceza Hukukuna Giriş.* Eskişehir: Anadolu Üniversitesi.

◊ Gültaş, V. (2017). *Özel Hayata Karşı Suçlar.* Ankara: Bilge Yayınevi.

◊ Kangal, Z.T. (2019). *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması.* İstanbul: On İki Levha Yayıncılık.

◊ Karabel, G. (2015). *Rekabet Hukukunda Ne Bis In Idem İlkesi,* (Uzmanlık Tezi), Ankara: Rekabet Kurumu. Erişim adresi: https://www.rekabet.gov.tr/Dosya/uzmanlik-tezleri/142-pdf#:~:text=Ne%20bis%20in%20idem%2C%20ayn%C4%B1,(%C3%96zay%201985%2C%2035).

◊ Kişisel Verileri Koruma Kurumu. (2019a). *Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular Rehberi.* Ankara: KVKK Yayınları. Erişim adresi: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/c148901d-cd7f-43ff-ae9a-978fb78fb43c.pdf

◊ Kişisel Verileri Koruma Kurumu. (2019b). *Örneklerle Kişisel Verilerin Korunması.* Ankara: KVKK Yayınları 29. Erişim adresi: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/a23bfe08-9b3a-4c2f-8a97-a259dcc0e667.PDF

◊ Kişisel Verileri Koruma Kurumu. (2019c). *Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi.* Ankara. Erişim adresi: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf

◊ Kişisel Verileri Koruma Kurumu. (2019ç). *Kişisel Verilerin Korunması Kanunu Uyum Sürecine İlişkin Duyuru* Erişim adresi: https://kvkk.gov.tr/Icerik/6554/Kisisel-Verilerin-Korunmasi-Kanunu-Uyum-Surecine-Iliskin-Duyuru/

◊ Kişisel Verileri Koruma Kurumu. (2019d). *Kişisel Veri İşleme Envanteri Hazırlama Rehberi,* Ankara: KVKK Yayınları 30. Erişim adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/14a17049-71da-4417-a07b-961f75a0070e.PDF

◊ Kişisel Verileri Koruma Kurumu. (2020). *Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu Duyurusu.* Erişim adresi: https://kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU

◊ Korkmaz, İ. (2019). *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması.* Ankara: Seçkin Yayıncılık.

◊ Küzeci, E. (2021). *Kişisel Verilerin Korunması.* Ankara: Turhan Kitabevi.

◊ Meran, N. (2015). *Kabahatler Kanunu ve Özel Kanunlarda İdari Para Cezaları.* Ankara: Adalet Yayınevi.

◊ Orak, B. (2020). *Kişisel Sağlık Verilerinin Korunması.* Ankara: Yetkin Yayınları.

◊ Ormanoğlu, H. D. (2016). Anayasal Bağlamda ve Avrupa İnsan Hakları Sözleşmesi Boyutuyla Suçsuzluk Karinesi, *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 65(4), 2241-2276, Erişim adresi: https://dergipark.org.tr/tr/pub/auhfd/issue/42360/510004

◊ Özen, M. (2010). Non Bis In Idem (Aynı Fiilden Dolayı İki Kez Yargılama Olmaz) İlkesi, *Ankara Hacı Bayram Üniversitesi Hukuk Fakültesi Dergisi,* 14(1), 389-471, Erişim adresi: https://dergipark.org.tr/tr/download/article-file/789560

◊ Özgenç, İ. (2019). *Türk Ceza Hukuku Genel Hükümle.* Ankara: Seçkin Yayıncılık.

◊ Özkan, O. (2020). *Kişisel Verilerin Korunması.* Ankara: Yetkin Yayınları.

◊ Saka, R., Çağlayan, R., ve Koca, M. (2020). *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası.* Ankara: Seçkin Yayıncılık.

◊ Sert, Ş. (2019). *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması.* Ankara: Seçkin Yayıncılık.

◊ Şenses, E. (2012). Ceza Muhakemesinde "Beraat" Hükmü Verilen Haller, TBB Dergisi (98), 345-362, Erişim adresi: http://www.erkansenses.av.tr/makale/cezamuhakemesinde.pdf

◊ Şirin, T. (2016). İnsan Hakları Avrupa Sözleşmesi'ne Ek 7. No.lu Protokol Hakkında Genel Bir Bilgilendirme, *Güncel Hukuk Dergisi,* 152, Erişim adresi: https://www.academia.edu/28122179/Avrupa_%C4%B0nsan_Haklar%C4%B1_S%C3%B6zle%C5%9Fmesi_7_nolu_Protokol

◊ Turan, M. (2021). *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması.* Ankara: Seçkin Yayıncılık.

◊ Ünver Y. ve Hakeri, H. (2017). *Ceza Muhakemesi Hukuku.* Ankara: Adalet Yayınevi.

◊ Yerdelen, E. (2013). *Cezanın Belirlenmesi Türk ve Alman Uygulaması.* Ankara: Adalet Yayınevi.

◊ Yılmaz, S. ve Çavuşoğlu, G. F. (2020). *Kişisel Verileri Koruma Hukuku.* Ankara: Yetkin Yayınları.

◊ Anayasa Mahkemesinin 31/05/2017 tarihli, 2017/28 esas sayılı ve 2017/107 karar sayılı kararı. (2017). Erişim adresi: https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2017-107-nrm.pdf

◊ Anayasa Mahkemesinin 26/12/2017 tarihli, 2014/13229 başvuru sayılı kararı. (2017). Erişim adresi: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/13229

◊ Danıştay İdari Dava Daireli Kurulunun 26/10/2020 tarihli, 2019/760 esas sayılı ve 2020/1979 karar sayılı kararı. (2020). Erişim adresi: https://www.lexpera.com.tr/ictihat/danistay/danistay-idari-dava-daireleri-kurulu-e-2019-760-k-2020-1979-t-26-10-2020-1

◊ Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı kararı. (2018). Erişim adresi: https://kvkk.gov.tr/Icerik/4110/2018-10

◊ Kişisel Verileri Koruma Kurulunun 13/09/2018 tarihli ve 2018/106 sayılı kararı. (20189. Erişim adresi: https://www.kvkk.gov.tr/Icerik/5421/2018-106

◊ Kişisel Verileri Koruma Kurulunun 07/11/2019 tarihli ve 2019/332 sayılı kararı. (2019). Erişim adresi: https://www.kvkk.gov.tr/Icerik/6624/2019-332

◊ Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı kararı. (2020). Erişim adresi: https://kvkk.gov.tr/Icerik/6874/2020-71

◊ 6698 Sayılı Kanun Onayı. (2016). Erişim adresi: https://www5.tbmm.gov.tr//develop/owa/kanun_ss.durumu?kanun_no=6684

KİŞİSEL VERİLERİ KORUMA KURULU'NUN MEVZUAT TASLAKLARI HAKKINDA GÖRÜŞ VERME YETKİSİ

Mustafa Koray ALTUN

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "6698 sayılı Kişisel Verilerin Korunması Kanunu'nun Diğer Kanunlarla İlişkisi" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Kişisel verilerin korunması hakkı, bugün geniş bir coğrafyada bir temel hak ve özgürlük olarak tanınmaktadır. Bu anlamda, kişisel verilerin korunması aslında kişinin kendisinin korunmasıdır (Bilir, 2021).

Günümüzde teknoloji devleri şirketler ile bireyler arasında bir teknoloji asimetrisi söz konusudur. Bu durum bireysel otonomiye karşı büyük bir risk teşkil etmekte ve ne okuyacağımıza veya hangi şarkıyı dinleyeceğimize ilişkin en basit seçimlere bile etki edilmesine neden olmaktadır. Yazılım veya cihazlarda yer alan ve bu konuda özel bir uzmanlığa sahip olmayanların işleyişi ve yapabilecekleri hakkında oldukça sınırlı bir bilgiye vakıf oldukları karmaşık algoritmalar ne göreceğimizi, ne yapabileceğimizi ve sonuç olarak ne söyleyeceğimizi belirlemektedir. Dijital ekonomiye katılarak ve küreselleşmiş bir toplumun parçası olmakla zaten savunmasız kalmış bireyler, çağın sunduğu nimetlerden yararlanabilme telaşına dalmışken kendilerini çok daha az güvende ve özgür oldukları bir pozisyonda bulmuşlardır. Bu süreçte asıl sorunlu nokta, *"büyük veriyle ilgilenmesek dahi büyük verinin bizimle ilgileniyor oluşudur"* (Dixon, 2018).

Teknoloji devleri her geçen gün, saat, hatta dakika daha da artan bir ölçekte ve kolaylıkla kişisel verilerimizi elde etmekte, bunlar üzerinde çeşitli tasarruflarda bulunmakta ve üçüncü kişilere aktarmaktadır. Piyasanın işleyişi veya kamu nezdinde olumsuz bir imajın oluşması bu uygulamaları durduramamaktadır. Bu çerçevede, devletler üzerine düşeni yaparak kişisel verilerin korunmasına ilişkin usul ve esasları öngören ve yaptırım mekanizmalarını içeren düzenlemeler yapmaya ve ayrıca kurulan bağımsız denetleyici otoriteler vasıtasıyla bireylerin kişisel verilerinin korunmasını kamu gücüyle sağlamaya başlamışlardır. Diğer bir deyişle devletler, vatandaşlarının özgürleşmeleri için hukuki dayanaklar oluşturmuştur (Dixon, 2018).

Benzer bir anlayışla ülkemizde de uzun yıllar süren bir çalışmanın sonucunda kişisel verilerinin işlenmesi bağlamında bireyleri korumak ve daha öncesinde özel olarak herhangi bir kısıtlamaya tabi olmaksızın ve ortaya çıkan ve/veya çıkabilecek zararı giderici ya da önleyici mekanizmaların yokluğunda gerçekleştirilen kişisel veri işleme faaliyetlerinin hukukiliğine ilişkin sınırların belirlenmesi amacıyla 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKKn) yürürlüğe konulmuştur.

Belirtmek gerekir ki, KVKKn belirli kişisel veri işleme faaliyetleri bakımından herhangi bir ayrıksı düzenlemeyi ihtiva etmemektedir. Aksine, kural olarak her bir kişisel veri işleme faaliyetinin hukuka uygun olarak gerçekleştirildiğinin kabul edilebilmesi için uyulması gereken temel kural ve ilkeleri, söz konusu işleme faaliyetini gerçekleştiren kişi, kurum veya kuruluş tarafından yerine getirilmesi gereken yükümlülükleri ve ilgili kişilerin hukuka aykırı işleme faaliyetlerinin vuku bulması halinde başvurabilecekleri hak arama yollarını öngörmektedir.

Bununla birlikte, belli başlı kişisel veri işleme faaliyetlerine ilişkin usul ve esasları belirleyen sektörel düzeyde birtakım özel düzenlemeler de bulunmaktadır. Bahse konu düzenlemeler, KVKKn'den farklılaşan hükümler içerebilmektedir. KVKKn'nin dördüncü maddesinde kişisel verilerin ancak KVKKn ve diğer kanunlarda öngörülen usul ve esaslara göre işlenebileceğinin hüküm altına alınmıştır. Ayrıca kişisel verilerin imhası ile yurt içinde ve yurt dışına aktarımına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu öngörülmüştür. Bu anlamda, yasa koyucunun sektörel düzenlemelerde yer verilen hükümlerin KVKKn hükümleri karşısında öncelikle uygulanabilmesini sağlamayı amaçladığı anlaşılmaktadır.

Ancak, KVKKn ile kişisel verilerin işlenmesi bağlamında bireylerin temel hak ve özgürlüklerinin korunması hususunda temel güvencelerin belirlendiği dikkate alındığında; KVKKn ile tesis edilen veri koruma rejiminin özel düzenlemelerdeki

hükümler vasıtasıyla zayıflatılmasının önüne geçilmesi gerekmektedir. Bu amaçla, KVKKn'de Kişisel Verileri Koruma Kurulu'na (KVK Kurulu) kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş verme yetkisi tanınarak bir ön kontrol mekanizması oluşturulmuştur. KVK Kurulu, taslağı hazırlayan ilgili kamu kurum veya kuruluşu ile istişare içerisinde KVKKn'de ve KVKKn'ye dayanılarak çıkartılan ikincil düzenlemelerde öngörülen asgari teminatların uygulanabilirliğinin muhafaza edilebilmesi adına mevzuat hazırlama sürecine katılım sağlamaktadır. Dolayısıyla, KVK Kurulu'nun mevzuat taslakları hakkında görüş verme yetkisi ülkemiz veri koruma hukuku uygulaması bakımından önem teşkil etmekte olup KVKKn'nin genel kanun niteliği bağlamında incelenmesinde fayda bulunduğu düşünülmektedir.

Bu kapsamda, çaışmanın ilk bölümünde öncelikle KVKKn'nin yapım süreci ve böyle bir düzenlemeye neden ihtiyaç duyulduğu açıklanmıştır. Ardından ikinci bölümde, KVKKn'nin diğer kanunlar karşısındaki konumu çatışma çözme ilkeleri çerçevesinde belirlenmeye çalışılmıştır. KVKKn hükümlerinin diğer kanun hükümleri karşısında genel norm niteliğini haiz olduğu tespit edildikten sonra üçüncü ve son bölümde ise etkin ve yeknesak bir veri koruma hukuku uygulamasının temininde KVK Kurulunun kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş verme yetkisinin işlevi ve kamu kurum ve kuruluşlarının bu tür mevzuat taslaklarını hazırlarken göz önünde bulundurması gereken hususlar üzerinde durulmuştur. Ayrıca, görüşlerin hazırlanma süreci açıklanmış ve KVK Kurulu'nun söz konusu yetkisinin daha işler hale getirilmesi için öneriler sunulmuştur.

6698 SAYILI KANUN'UN TARİHÇESİ VE KANUN'A DUYULAN İHTİYAÇ

KVKKn, Türkiye Büyük Millet Meclisi (TBMM) tarafından 24 Mart 2016 tarihinde kabul edilmiş olup 7 Nisan 2016 tarihli Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. KVKKn m.1'de Kanun'un amacının kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek olduğu belirtilmiştir. Maddeye ilişkin gerekçede KVKKn ile kişisel verilerin işlenmesinin disiplin altına alınmasının da amaçlandığı ayrıca ifade edilmiştir (Türkiye Büyük Millet Meclisi, 2016a). Diğer taraftan, KVKKn'nin "Kapsam" başlıklı 2'nci maddesinde Kanun hükümlerinin, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanacağı öngörülmüştür. Anılan hükümden görüleceği üzere, KVKKn'nin konu bakımından uygulama kapsamı herhangi bir

sektör sınırlamasına tabi tutulmamıştır. Bu anlamda, "İstisnalar" başlıklı 28'inci madde hükmü saklı olmak üzere KVKKn hükümlerinin kural olarak iştigal alanı fark etmeksizin bütün kişi, kurum ve kuruluşların kişisel veri işleme faaliyetleri hakkında uygulama alanı bulacağı anlaşılmaktadır. Söz konusu maddeye ilişkin gerekçede ise hükümde özel sektör ile kamu sektörü arasında bir ayrım gözetilmediği ve KVKKn'de öngörülen usul ve esasların her iki sektörde de uygulanacağı ifade edilmiştir (Türkiye Büyük Millet Meclisi, 2016a).

Belirtmek gerekir ki her ne kadar KVKKn'ye ilişkin tasarı Başbakanlık'ın 18 Ocak 2016 tarihli yazısı ile TBMM Başkanlığına arz edilmiş olsa da kişisel verilerin korunması alanını sektörler-üzeri bir biçimde düzenleyen genel bir kanun yapımına yönelik çalışmalar 1989 yılına kadar uzanmaktadır (Türkiye Büyük Millet Meclisi, 2016b).

Ülkemizde, yıllar boyunca çeşitli politika belgeleri ve planlarında bireylerin kişisel verilerinin korunmasını güvence altına almaya yönelik hukuki çerçeveyi oluşturma hedefine yer verilmiştir (Şişkin ve Şencan, 2019). Diğer taraftan, kişisel verilerin korunmasına ilişkin bir kanun tasarısı hazırlamak amacıyla ilk defa 13 Eylül 1995 tarihinde bir komisyon kurulmuştur. Ancak söz konusu komisyon çalışmalarını tamamlayamamış ve 18 Eylül 2000 tarihinde ikinci bir komisyon kurulmuştur (Başalp, 2004). Adalet Bakanlığı bünyesinde kurulan ikinci komisyonun çalışmaları neticesinde Avrupa Ekonomik İşbirliği ve Kalkınma Teşkilatı, Birleşmiş Milletler ve Avrupa Konseyi tarafından oluşturulmuş uluslararası belgeler, Avrupa Birliği (AB) mevzuatı ve Almanya başta olmak üzere Avrupa ülkelerinde yürürlükte bulunan ulusal düzenlemeler dikkate alınarak (Öztürk ve Çalışkan, 2018) hazırlanmış bulunan Kişisel Verilerin Korunması Kanunu Tasarısı, 7 Eylül 2003 tarihinde kamuoyu ile paylaşılmış olmakla birlikte (Küzeci, 2019) Başbakanlık'ın 22 Nisan 2008 tarihli yazısı ile TBMM Başkanlığına sunulmuştur (Türkiye Büyük Millet Meclisi, 2008). Ne var ki söz konusu tasarı, seçimler nedeniyle TBMM Genel Kurulu'na sevk edilemeden kadük hale gelmiştir (Küzeci, 2019).

Geçen zaman içerisinde Adalet Bakanlığı bünyesinde kurulan çeşitli komisyonlar tarafından kanun tasarısı hazırlama çalışmaları devam etmiş; ancak 2014 yılına kadar yeni bir tasarı TBMM Başkanlığına sunulamamıştır (Türkiye Büyük Millet Meclisi, 2014). Bununla birlikte, 2014 tarihli tasarıya ilişkin görüşmeler de 2008 tarihli tasarı gibi seçimler nedeniyle tamamlanamamış olup benzer şekilde hükümsüz kalmıştır (Küzeci, 2019). Ardından, bir önceki başlıkta belirtildiği üzere 18 Ocak 2016 tarihinde TBMM'ye sunulan tasarı 24 Mart 2016 tarihinde kabul edilerek yasalaşmıştır.

Kişisel Verilerin Korunması Kanununa Duyulan İhtiyaç

Otuz üç madde ve iki geçici maddeden oluşan KVKKn'de kişisel veri işleme faaliyetlerinde gözetilmesi gereken genel ilkeler, kişisel verilerin işlenme şartları, veri sorumlusunun yükümlülükleri, kişisel verisi işlenen ilgili kişilerin hak arama yolları ve Kişisel Verileri Koruma Kurumu (KVK Kurumu) teşkilatı ile KVK Kurumu'nun görev ve yetkileri düzenlenmiştir. Anılan konularda çerçeve nitelikli hükümleri ihtiva eden KVKKn, ülkemizde doğrudan kişisel verilerin korunması amacına yönelik, kişisel veri işleme faaliyetlerinin hukuka uygun bir şekilde gerçekleştirilebilmesi için uyulması gereken temel usul ve esasları belirleyen ve kapsamı bakımından sektör ayrımı gözetmeyen mevzuat boşluğunu doldurmuştur (Bilir, 2020). Muhtevasında münhasıran kişisel veri işleme faaliyetlerinde riayet edilmesi gereken düzenlemelere yer verilen KVKKn ile kişisel veri işleme faaliyetlerine ilişkin maddi kurallar içeren diğer kanunlar arasındaki ilişkiyi ortaya koyabilmek adına öncelikle neden KVKKn'nin yürürlüğe konulmasına ihtiyaç duyulduğunun anlaşılmasının uygun olacağı ve böyle bir kanuni düzenleme yapılmasında etkili olan ana faktörlerin aşağıda belirtilen üç başlık altında sınıflandırılabileceği değerlendirilmektedir (Kişisel Verileri Koruma Kurumu, 2019).

Bireylerin Temel Hak ve Özgürlüklerine Etkin Biçimde Koruma Sağlama

Teknolojik gelişmeler sonucunda bireylere ilişkin bilgilerin daha kolay toplanabilmesi, özel hayatın gizliliği başta olmak üzere bireylerin temel hak ve özgürlüklerine yönelik tehditlerin farklı bir boyut kazanmasına neden olmuştur. Devletler de *"insan haklarına saygılı bir toplum yaratma ideali"* altında kişisel verilerin korunmasını temin edecek düzenlemeler yapmaya başlamışlardır (Tezcan, 1991). Akıllı cihazların ve internet kullanımının yaygınlığı (Çekin, 2020) ile toplum nezdinde bu alanda bir düzenleme yapılmasına ihtiyacın olduğu yönündeki inanç ülkemizde de kişisel verilerin korunmasına ilişkin bir kanun çıkarılmasını zaruri kılmıştır (Oğuz, 2013). Bu noktada belirtilmesinde fayda görülmektedir ki "kişisel verilerin korunması" şeklinde formüle edilen hukuki güvence sağlama yolu ile esasen bireylerin verilerinin değil; temel hak ve özgürlüklerinin korunması temin edilmek istenmektedir (Şimşek, 2008). Nitekim KVKKn'nin 1'inci maddesinde Kanun'un amacının kişilerin temel hak ve özgürlüklerini korumak olduğu belirtilmiştir (Çekin, 2020).

Bu çerçevede, Anayasa'nın 2'nci maddesinde de belirtildiği üzere insan haklarına saygılı bir hukuk devleti olan ülkemizde kişisel verilerin korunmasına ilişkin temel usul ve esasları belirlemek yoluyla bireylere güvence sağlayacak bir kanuni düzenlemenin hayata geçirilmesi her şeyden önce temel hak ve özgürlüklerin

etkin bir biçimde korunabilmesi için gerekliydi (Küzeci,2019). KVKKn'ye ilişkin genel gerekçede de kişisel verilerin korunması insan haklarının korunması bağlamında ele alınmış olup ülkemizde bu alanı bütüncül olarak düzenleyen bir kanuni düzenlemenin bulunmadığına dikkat çekilmişti (Türkiye Büyük Millet Meclisi, 2016a).

Kişisel Verilerin Korunmasını İsteme Hakkı

Teknolojik gelişmeler sonucunda ortaya çıkan yeni teknik ve teçhizatlar vasıtasıyla kişisel verilerin işlenebilmesi kolaylaşmış ve yaygınlaşmıştır. 20. yüzyılın ikinci yarısından itibaren, kişisel veri işleme faaliyetlerinin herhangi bir insan müdahalesi gerekmeksizin tamamen veya kısmen otomatik yollarla gerçekleştirilmeye başlanmasıyla gerek kamu kurum ve kuruluşları gerek şirketler tarafından daha öncesinde görülmeyen ve her geçen gün artan miktarda kişisel veriye erişim sağlanmaktadır (Küzeci, 2019). Bu kapsamda, devletler tarafından kamu hizmetinin etkin sunumu ve planlama gibi amaçları gerçekleştirmek üzere vatandaşlara ilişkin bilgileri depolayan merkezi veri tabanları kurulurken (Küzeci, 2019); özel kuruluşlar ise iş süreçlerindeki verimliliği artırmak ve müşterilerine yönelik kişiselleştirilmiş mal ve hizmet sunumu sağlamak adına sektörlere göre farklılaşan ve oldukça sofistike işleme faaliyetlerini gerçekleştirmektedir (Türkiye Ekonomi Politikaları Araştırma Vakfi ve Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, 2014).

Belirtmek gerekir ki bilişim teknolojileri alanında yaşanan bu dönüşüm sayesinde yüksek miktarda kişisel verinin elde edilip depolanmasına ilaveten bahse konu veriler üzerinde karmaşık ve ileri düzey işleme tekniklerinin tatbiki ile gerçekleştirilen inceleme ve analizler sonucunda bireyler hakkında çok daha fazla bilgiye sahip olunabilmektedir (Şimşek, 2008). Nitekim Cumhurbaşkanlığı Devlet Denetleme Kurulu'nun "Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları"na ilişkin 27/11/2013 tarihli ve 2013/3 sayılı Denetleme Raporu'nda,

» *"Geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi,*

» *Daha önce dağınık yapılarca toplanan ve birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilmesi,*

» *Verilerin ileri teknolojik imkânlarla ve veri eşleştirme (data matching) ve veri madenciliği (data mining) gibi tekniklerle analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması,*

» *Verilere erişim, paylaşım ve transferin kolaylaşması ve maliyetinin düşmesi,*

» *Kişisel verilerin ticari işletmeler için kıymetli bir varlık ve ticari meta niteliği kazanması neticesinde özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşmış olması,*

» *Yabancı ülke istihbarat birimlerinin, terör ve suç örgütlerinin kişisel verileri ele geçirme veya bu sistemlere zarar verme yönündeki faaliyet ve saldırılarının artması,*

» *Banka ve kredi kartı dolandırıcılıkları başta olmak üzere, kişisel verileri hedef alan veya bunlar kullanılmak suretiyle işlenen suç olaylarının artması"*

şeklinde sayılan gelişmelere dikkat çekilerek kişisel verilerin işlenmesi bağlamında bireylere yönelik tehdit boyutunun ciddiyeti vurgulanmıştır (Cumhurbaşkanlığı Devlet Denetleme Kurumu, 2013, 778-779).

Bilişim teknolojilerindeki değişim ve dönüşüm sürecinin sonraki aşamalarında, daha öncesinde çoğunlukla kamu kurumlarının yönetiminde bulunan merkezi veri tabanları üzerinden gerçekleştirilen kişisel veri işleme faaliyetlerinin daha küçük, düşük maliyetli ve kamu makamları dışında kalan özel kuruluşlar tarafından da temini mümkün bilgisayarlar vasıtasıyla gerçekleştirilmeye başlanmasıyla birlikte bireylerin tehdit algısı önemli boyutlara ulaşmış ve kişisel verilerin korunması taleplerinin *"yurttaşlık hakkı"* bağlamında ifade edildiği yeni bir döneme adım atılmıştır (Şimşek, 2008, 9; Küzeci, 2019). Bu kapsamda, kişisel verilerin korunması bağlamında teknolojinin olumsuz sonuçlarından korunma ihtiyacı (Şimşek, 2008) ile birlikte konunun özel hayatın gizliliğine ve insan haklarına etkisi de ön plana çıkmaya başlamıştır (Küzeci, 2019).

Kişisel verilerin korunması hakkı ilk başlarda özel hayatın gizliliği hakkının özel bir görünümü olarak kabul edilmekle birlikte zaman içerisinde bağımsız bir hakka dönüşmüştür (Küzeci, 2019). Söz konusu dönüşümün pozitif hukuka yansımaları olmuş ve Portekiz ve İspanya anayasalarında kişisel verilerin korunması hakkı güvence altına alınmıştır (Kama Işık, 2020). Benzer bir anlayış ülkemizde de benimsenmiştir. 12 Eylül 2010 tarihinde yapılan halkoylaması sonucunda kabul edilen 5982 sayılı Kanun'un 2'nci maddesi ile Türkiye Cumhuriyeti Anayasası'nın "A. Özel Hayatın Gizliliği" başlıklı 20'nci maddesine,

"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Hükmü eklenerek "kişisel verilerin korunmasını isteme hakkı" anayasal güvenceye kavuşturulmuştur. Değişikliğe ilişkin gerekçede, Anayasa'da kişisel verilerin korunmasına ilişkin dolaylı hükümlerin bulunduğu; ancak yeterli olmadığı ifade edilmiştir (Türkiye Büyük Millet Meclisi, 2010, 9).

Kişisel Verilerin İşlenmesine İlişkin Temel İlkeleri İçerir Bir Düzenleme Yapılması Gereği

Kişisel verilerin kullanımı sonucunda gerek kamusal gerek özel kuruluşlar tarafından önemli derecede katma değer elde ediliyor olsa da kişisel verilerin ölçüsüz, ilgili kişiler bakımından öngörülebilir ve şeffaf olmayan veya ayrımcılığa yol açacak işleme süreçlerine konu edilmesi suretiyle istismar edilmesi ya da uygun güvenlik tedbirlerinin alınmaması sebebiyle kişisel verilere yetkisiz kişi ve kuruluşların erişimi gibi riskler göz önünde bulundurulduğunda; kişisel verilerin ilgili kişiler bakımından güvence teşkil edecek hukuki düzenlemelere tabi olmaksızın işlenebilmesi bireyler nezdinde telafisi imkansız veya çok güç nitelikte olumsuz sonuçlar doğmasına neden olabilecektir. Bu anlamda, Anayasa'nın 20'nci maddesine eklenen üçüncü fikra hükmü, ülkemizde kişisel verilerin korunması alanında bir miladı teşkil etse de kişisel verilerin işlenmesi bağlamında bireylere tam ve etkin koruma sağlama hususunda yeterli olmamıştır. Zira kişisel veri işleyen kuruluşların faaliyetlerini belirli bir çerçevede gerçekleştirmelerini sağlamak, onları denetim altında tutabilmek ve ilgili kişilere etkili hak arama yolları sunabilmek için kanun düzeyinde düzenlemelerin yapılması gerekmektedir. "Soyut" nitelikteki söz konusu temel hak ve özgürlüğün kullanılabilirliği ancak bu yolla sağlanabilecektir (Çekin, 2020, 9). Nitekim Anayasa'nın anılan hükmünde de kişisel verilerin korunmasına ilişkin usul ve esasların kanunla düzenleneceği öngörülmüştür. Bu anlamda kişisel verilerin korunmasına ilişkin usul ve esasları düzenleyen bir kanunun yürürlüğe konulması, hem kişisel verilerin korunmasını isteme hakkına işlerlik kazandırabilmek için gereklilik hem de Anayasa'nın mezkûr hükmü uyarınca yerine getirilmesi gereken bir yükümlülüktür.

Bununla birlikte, Avrupa Konseyi bünyesinde kişisel verilerin otomatik yollarla işlenmesi karşısında temel hak ve özgürlüklere yönelik olarak ortaya çıkan ve

ileride ortaya çıkması muhtemel tehlikelere karşı Sözleşmeci taraflar arasında güvenli bir ekosistem yaratmak adına hazırlanan 108 sayılı Sözleşme 28 Ocak 1981 tarihinde imzaya açılmıştır (Avrupa Konseyi, t.y.). Sözleşme, Türkiye tarafından imzaya açıldığı ilk gün imzalanmasına rağmen imza tarihinden otuz beş sene sonra onaylanmıştır. Sözleşme'de yer verilen ilkelerin iç hukukta uygulanmasını sağlayacak bir kanuni düzenlemenin bulunmaması sebebiyle Sözleşme KVKKn'nin yürürlüğe girmesinden hemen önce onaylanarak ülkemiz bakımından bağlayıcılık kazanmıştır (Küzeci, 2019). Şöyle ki, Bakanlar Kurulu'nun 29/2/2016 tarihli ve 2016/8576 sayılı Kararı ile onaylanan 108 sayılı Sözleşmenin "Tarafların Görevleri" başlıklı 4'üncü maddesinin birinci paragrafi uyarınca Sözleşme tarafları, kişisel verilerin korunmasına ilişkin olarak Sözleşme'de yer verilen temel ilkelere işlerlik kazandırmak amacıyla iç hukukunda gerekli önlemleri almakla yükümlüdür. Yani, 108 sayılı Sözleşme hükümlerinin doğrudan uygulanması mümkün olmayıp bir uygulama kanunu vasıtasıyla Sözleşme'nin öngördüğü düzenlemelerin iç hukuka aktarılması gerekmektedir (Akıllıoğlu, 2004). 108 sayılı Sözleşme'ye ilişkin Açıklayıcı Rapor'da da Sözleşme'nin doğrudan uygulanabilir nitelikte olmadığı ve bu sebeple taraf devletlerin, veri koruma hükümlerini iç hukuklarına dâhil etmekle yükümlü kılındıkları ifade edilmiştir (Avrupa Konseyi, 1981). Dolayısıyla, kişisel verilerin korunması alanındaki temel ilkeleri öngören bir düzenlemenin yürürlüğe konulması 108 sayılı Sözleşme uyarınca ülkemiz tarafından yerine getirilmesi gereken bir yükümlülüktür.

Diğer taraftan, dünyada kişisel verilerin korunması alanındaki düzenlemelere bakıldığında ülkeler tarafından genellikle iki farklı modelin tercih edildiği görülmektedir. Bu kapsamda, Avrupa ülkeleri genellikle kişisel verilerin hem kamu kurum ve kuruluşları hem de özel sektör kuruluşları tarafından toplanmasına, kullanımına ve yayılmasına ilişkin düzenlemeleri bütüncül olarak içeren genel kapsamlı kişisel verilerin korunması yasalarını kabul etmektedirler (Banisar ve Davies, 1999). Diğer taraftan, ABD'nin başını çektiği diğer bazı ülkeler ise herhangi bir ayrım gözetmeksizin bütün kişisel veri işleme faaliyetlerine ilişkin usul ve esasları tek bir mevzuat metninde düzenlemek yerine yalnızca temel hak ve özgürlüklere karşı önemli ölçüde tehlike oluşturduğu kanaatine varılan belli başlı işleme faaliyetlerini düzenleyen sektörel kanunları tercih etmektedirler (Tezcan, 1991). Ayrıca, bazı ülkelerde iki model sentezlenmekte ve sektörel ihtiyaçlar dikkate alınarak kişisel verilerin korunması alanındaki genel kanunlar özel işleme faaliyetlerini düzenleme altına alan diğer kanunlarla desteklenmektedir (Banisar ve Davies, 1999).

Ülkemizde benimsenen sistemin gelişim sürecine bakıldığında ise KVKKn öncesinde de kişisel verilerin korunmasına yönelik birtakım düzenlemelerin bulundu-

ğu görülmektedir. Ancak ülkemiz mevzuatında dağınık halde bulunan söz konusu düzenlemelerin sınırlı uygulama alanları, büyük oranda önleyici değil telafi edici bir niteliğe sahip olması ve kişisel verilerin korunmasına ilişkin temel ilkelerin yokluğunda öngördüğü güvencelerin tam anlamıyla uygulanamaması nedeniyle etkin bir koruma sağlayamadığı ifade edilmiştir (Küzeci, 2019). Hatta bu hususa ilişkin olarak 2008 tarihli kişisel verilerin korunması kanunu tasarısının genel gerekçesinde,

"Kişisel verilerin korunması, çağımızda, insan hakları kavramı ve korunması bilincinin gittikçe gelişmesine paralel olarak önemini artırmaktadır. Bu nedenle bir ülkenin mevzuatında değişik düzenlemeler içinde yer alan farklı hükümlerin, bu konuya özgü felsefeden yoksun olması halinde kişisel verilerin korunması konusunda artan ihtiyaca cevap vermesi mümkün olmamaktadır. Bunun öncelikli sebebi, söz konusu hükümlerin başlı başına yetersiz olmalarından ziyade; bu hükümlerin hukuk sisteminde yer almasının, kişisel verilerin korunması amacı ile değil, ancak her bir hükmün ilgili olduğu sahalarda zamanın ihtiyaçlarına cevap vermesi amacı ile düzenlenmiş olmasıdır. Bundan dolayı hemen tüm modern hukuk sistemlerinde olduğu gibi, ülkemizde de kişisel verilerin korunması amacına yönelik münhasır bir kanunun yürürlüğe girmesi kaçınılmaz hale gelmiştir."

açıklamasına yer verilmiştir (Türkiye Büyük Millet Meclisi, 2008). Özellikle kişisel verilerin korunması hakkının anayasal güvence altına alınmasından sonra yürürlüğe konulan düzenlemelerle kişisel verilerin korunmasından ziyade düzenlemenin ilişkili olduğu alandaki işleme faaliyetlerine dayanak oluşturulmak istendiği anlaşılmaktadır (Küzeci, 2019).

Bahse konu düzenlemeler bankacılık, finans veya sağlık hizmetleri gibi belirli alanlara yönelik sektörel işleme faaliyetleri hakkında hükümler içermekte olup kişisel verilerin korunması bakımından sınırlı düzeyde güvence barındırmaktadır (Gültekin Varkonyi, 2017). Bu bağlamda, KVKKn'nin yürürlükte bulunmadığı dönemde kişisel veri işleme faaliyetlerine özgü kuralları bütüncül olarak öngören kapsamlı bir kanunun yokluğu, zaten tatmin edici bir koruma sağlayamayan sektörel düzenlemelerin bütünüyle etkisiz olmasına sebep olmaktaydı (Gürsel, 2016). Diğer bir deyişle, kişisel verilerin korunması alanı ile ilgili çok yönlü sorunları tam anlamıyla ele alabilecek çerçeve bir kişisel verilerin korunması yasasının olmaması, konuya ilişkin mevcut düzenlemelerin uygulamasındaki belirsizlik ve toplum nezdinde mahremiyet farkındalığının düşük düzeyde olması dikkate alındığında; KVKKn öncesinde kişisel verilerinin işlenmesi bağlamında bireylerin temel hak ve özgürlüklerine yönelik sağlanan sektörel güvence mekanizmalarının yetersiz olduğu tespit edilebilecektir (Küzeci ve Boz, 2017). Yine, yukarıda belirtildiği üzere kamu kurum ve kuruluşlarının görev ve yetkilerinin belirlendiği düzenlemelerde kişisel verilerin toplanmasına dayanak teşkil edecek hükümler bulunmasına karşın işleme faaliyetinin amacı ve kapsamı ile işleme faaliyetine konu kişisel verilerin toplanma şekli, saklanabileceği süreler ve üçüncü kişilere aktarılıp aktarılamayacağı gibi hususlar ile ilgili hükümlerin bulunmaması söz konusu kuruluşların ölçüsüz kişisel veri işleme uygulamalarını engelleyememekteydi (Tene ve Saygın, 2011; Cumhurbaşkanlığı Devlet Denetleme Kurumu, 2013).

Bununla birlikte, KVKKn'ye ilişkin genel gerekçede de açıkça zikredildiği gibi 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135'inci maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesi; 136'ncı maddesinde kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi ve 138'inci maddesinde kanunların belirlediği sürelerin geçmiş olmasına karşın kişisel verilerin yok edilmemesi suç olarak öngörülmüşken, kişisel veri işleme faaliyetinin hukuka uygun olarak gerçekleştirildiğinin kabulü için riayet edilmesi gereken usul ve esaslar bu alana özgü bir kanun vasıtasıyla düzenlenmediği için anılan suçlara esas teşkil eden fiillerin tespitinde zorluklar yaşanmaktaydı (Türkiye Büyük Millet Meclisi, 2016a). Aynı doğrultuda, kişisel veri işleme faaliyetinde bulunan kişi ve kuruluşlar için hukuki öngörülebilirliğin sağlanabilmesi adına da işleme faaliyetlerine ilişkin usul ve esasların belirlendiği bir kanuni düzenlemeye ihtiyaç duyulmaktaydı (Dülger, 2019).

AB ile İlişkiler

10-11 Kasım 1999 tarihlerinde Helsinki'de gerçekleştirilen AB Zirvesi'nde Türkiye'ye adaylık statüsü verilmiştir (Avrupa Birliği Başkanlığı, 2020). KVKKn genel gerekçesinde AB üyelik müzakere fasıllarından dördünün doğrudan kişisel verilerle ilgili olduğu belirtilmiş olup Avrupa Komişyonu'nun KVKKn yürürlüğe girmeden önce ülkemiz hakkında hazırlamış olduğu 2015 tarihli raporda yer alan *"Fasıl 10: Bilgi Toplumu ve Medya", "Fasıl 23: Yargı ve Temel Haklar", "Fasıl 24: Adalet, Özgürlük ve Güvenlik" ve "Fasıl 28: Tüketicinin* ve *Sağlığın Korunması"* başlıkları altında kişisel verilerin korunması hakkında kapsamlı bir çerçeve kanunun yokluğuna dikkat çekilmiştir (Avrupa Komisyonu, 2015). Aynı raporda AB müktesebatı ile uyumlu bir kişisel verilerin korunması kanununun kabul edilmesinin, Vize Serbestisi Diyaloğu kapsamında ve ülkemiz yetkili makamları ile EUROJUST (Bkz. Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, 2021) ve EUROPOL (Bkz. Avrupa Birliği Başkanlığı, 2021) arasında karşılıklı kişisel veri aktarımı yapılması suretiyle terörle mücadele başta olmak üzere adli süreçler ve kolluk faaliyetleri bağlamında işbirliğinin tesis edilmesini sağlayacak operasyonel anlaşmaların akdedilebilmesi için de bir gereklilik olduğu ifade edilmiştir

(Avrupa Komisyonu, 2015). Benzer şekilde KVKKn'ye ilişkin olarak TBMM Adalet Komisyonu'nda yapılan görüşmelerde kişisel verilerin korunması hakkında bir yasanın yürürlüğe konulmasının Vize Serbestisi Diyaloğu kapsamında ülkemiz tarafından yerine getirilmesi gereken taahhütlerden biri olduğu ve bu sebeple çalışmaların ivedi bir biçimde tamamlanmasının önem arz ettiği ifade edilmiştir (Türkiye Büyük Millet Meclisi, 2016c).

Ayrıca ifade edilmesinde fayda görülmektedir ki sadece ülkemiz gibi adaylık statüsüne sahip ülkeler değil ticari ilişkiler başta olmak üzere çeşitli şekillerde AB ile etkileşime giren ülkelerin ekseriyeti, Avrupa standartları ile uyumlu kişisel verilerin korunması yasaları kabul etmeye gayret etmektedir (Banisar ve Davies, 1999). AB veri koruma hukuku uyarınca kişisel verilerin üye devletlerden diğer devletlere veya uluslararası kuruluşlara aktarılabilmesi için ana kural aktarımın yapılacağı ülkede veya uluslararası kuruluş nezdinde yeterli düzeyde koruma sağlandığının Avrupa Komisyonu tarafından verilecek bir kararla tespit edilmesidir. ABAD'ın "Schrems" kararında 95/46/AT sayılı Direktif kapsamında bir ülke tarafından yeterli koruma sağlandığının kabulü için söz konusu ülkenin iç hukuku veya uluslararası yükümlülükleri vasıtasıyla, Direktif'in sağladığı güvenceye temel olarak eşdeğer düzeyde bir güvence sağlaması gerektiği vurgulanmıştır (Avrupa Birliği Adalet Divanı, 2015). Diğer taraftan, GVKT'nin başlangıç hükümlerinin 101 numaralı paragrafında,

"Kişisel verilerin Birlik dışındaki ülkelere ve bu ülkelerden akışı uluslararası ticaretin ve uluslararası işbirliğinin gelişebilmesi için gereklidir. Veri akışındaki artış kişisel verilerin korunması bakımından yeni sınamaları ve endişeleri de beraberinde getirmiştir. Ancak, aktarımın yapıldığı ülke veya uluslararası kuruluşlardan aynı ya da farklı ülke veya uluslararası kuruluşlardaki veri sorumlularına ve veri işleyenlere yapılacak sonraki aktarımlar dâhil olmak üzere, kişisel veriler Birlikten üçüncü ülkelerdeki veri sorumlularına, veri işleyenlere veya diğer alıcılara ya da uluslararası kuruluşlara aktarıldığında gerçek kişilere Birlik içerisinde Tüzükle sağlanan koruma sekteye uğramamalıdır."

ifadelerine yer verilmiştir. Güçlü bürokratik altyapısı, insan haklarını korumak amacıyla katı düzenlemeler yapma yönündeki eğilimi ve büyüklüğü sebebiyle şirketler tarafından vazgeçilmez nitelikte bir tüketici pazarına sahip olduğu da dikkate alındığında (Bradford, 2012); AB'nin gerek mülga 95/46/AT sayılı Direktif gerek GVKT ve ilgili diğer düzenlemeler vasıtasıyla kişisel verilerin korunması alanında "altın standart"ı belirleyerek diğer ülkelerin düzenlemelerini etkilediğini söyleyebilmek mümkündür (Albrecht, 2016, 288). Bu kapsamda, AB, koşulluluk temelinde kendi mevzuatı ile uyumlu veri koruma düzenlemelerini kabul eden ülkelere Avrupa pazarına erişimde veya güvenlikten kamu sağlığının korunmasına kadar çeşitli işbirliği alanlarında imtiyaz tanımış olmaktadır (Akçalı Gür, 2020).

Ülkemizde de bu farkındalıkla AB müktesebatı ile paralel şekilde kişisel verilerin işlenmesine ilişkin temel usul ve esasları içeren müstakil bir veri koruma yasası kabul edilmiş ve bu yasada yer verilen düzenlemeler hazırlanırken o sırada AB'de yürürlükte bulunan 95/46/AT sayılı Direktif esas alınmıştır (Türkiye Büyük Millet Meclisi, 2016a). Bununla birlikte, KVKKn'nin GVKT ile uyumlaştırılması çalışmaları devam etmekte ve özel sektör temsilcileri tarafından kişisel verilerin korunması alanında AB mevzuatı ile tam uyumun sağlanmasının ülkemiz ve AB arasındaki ticari ilişkilerin geliştirilebilmesi bakımından önemli bir etken olduğu ifade edilmektedir (Türk Sanayicileri ve İş İnsanları Derneği, 2021).

Uluslararası İşbirliği ve Ekonomik Faaliyetler

KVKKn genel gerekçesinde ülkemizde kişisel verilerin korunmasına ilişkin çerçeve bir düzenleme bulunmaması sebebiyle Dışişleri Bakanlığı ile yabancı ülke makamları arasında vatandaşların askerlik, vatandaşlık, kimlik ve malvarlığı bilgilerinin karşılıklı paylaşımı hususunda problemlerin bulunduğu belirtilmiştir (Türkiye Büyük Millet Meclisi, 2016a). Bununla birlikte, KVKKn'nin ve 2014 tarihli tasarının genel gerekçelerinde bulunmamakla birlikte 2008 tarihli kişisel verilerin korunması kanunu tasarısının genel gerekçesinde yasal düzenleme yokluğu sebebiyle kişisel verilerin etkin korunmadığı yönündeki algının adli yardımlaşma amacıyla ve gümrük idareleri arasında gerçekleştirilecek kişisel veri aktarımlarını da engellediği dile getirilmiştir (Türkiye Büyük Millet Meclisi, 2008). Yine, Cumhurbaşkanlığı Devlet Denetleme Kurulu Raporu'nda kişisel verilerin korunmasına ilişkin hassasiyetin dünya çapındaki artışına ve bunun sonucunda veri koruma düzenlemelerinin ortaya çıkışına bağlı olarak vergilendirme ile suçun önlenmesi, soruşturulması ve kovuşturulması gibi alanlarda uluslararası işbirliğinin sürebilmesi için ülkelerin benzer nitelikte güvenceleri mevzuatına kazandırmasının bir gereklilik haline geldiği ifade edilmiştir (Cumhurbaşkanlığı Devlet Denetleme Kurulu, 2013).

Diğer taraftan, ülkemizde kişisel verilerin korunmasına yönelik güvenceleri içerir genel bir hukuki çerçevenin yokluğu ticari kuruluşlar tarafından ülkemize yapılacak kişisel veri aktarımlarını kısıtlamakta, söz konusu kuruluşlar bu aktarımları gerçekleştirebilmek adına her bir ülkedeki yetkili otorite nezdinde izin ve/veya yetkilendirme için başvuru yapmak zorunda kalmakta ve aktarım maliyeti artmaktadır (Türkiye Ekonomi Politikaları Araştırma Vakfı ve Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, 2014). Nitekim KVKKn genel gerekçesinde

de gerek yabancı yatırımcılar gerek diğer ülkelerde faaliyet gösteren ülkemiz ekonomik aktörleri tarafından ülkemize kişisel veri aktarımı gerçekleştirilemediğine ve bu durumun ülkemize yapılacak yatırımlar bakımından "caydırıcı" bir etkene dönüştüğüne dikkat çekilmiştir (Türkiye Büyük Millet Meclisi, 2016a).

6698 SAYILI KANUN HÜKÜMLERİNİN DİĞER KANUN HÜKÜMLERİ KARŞISINDAKİ DURUMU VE ÖNCELİKLE UYGULANMA SORUNU

Önceki bölüm altında KVKKn'nin ortaya çıkış süreci ve sürecin bu yönde gelişiminde etkili olan faktörler açıklanmak suretiyle KVKKn'ye ilişkin tarihsel arka plan ortaya konmuştur. Bu bölüm altında ise çalışmanın üçüncü bölümünde, KVK Kurulu'nun kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş verme yetkisinin mahiyeti incelenmeden önce; hukuk kuralları arasında çatışma olması halinde kullanılagelen yorum ilkeleri (Gözler, 2013) açıklanarak teorik bir çerçeve oluşturulmaya çalışılacak ve bu teorik çerçeve ışığında KVKKn'nin diğer kanunlar karşısındaki konumu belirlenecektir.

Hukuk Kuralları Arasında Çatışma Halinde Uygulanacak İlkeler

Öncelikle belirtmek gerekir ki esasen bir hukuk düzenini oluşturan farklı kuralların uyum içerisinde var olduğu ve bu kurallar arasında herhangi bir çelişki veya çatışma bulunmadığı kabul edilir. Ancak bazı hallerde hukuk kuralları arasında "gerçek olmayan" ve üç temel ilke vasıtasıyla çözüme kavuşturulan çatışma hallerinin de ortaya çıkabildiği görülmektedir (Gözler, 2017).

Söz konusu ilkelere ilişkin açıklamalara geçmeden önce bu sözde çatışma halinin varlığının nasıl tespit edileceğinin üzerinde durulmasının yararlı olacağı düşünülmektedir. SÖZER'e göre aynı olaya uygulanabilecek birden çok kuralın bulunması ve bu kuralların uygulanması sonucunda farklı hukuki sonuçların doğması halinde bahse konu kurallar arasında bir çatışma söz konusudur (2008). Bu anlamda, aynı olayın tabi olduğu kurallar arasında bir çelişki yoksa, kurallar birbiriyle bağdaşıyorsa veya örtüşüyorsa, birbirini tamamlıyorsa ya da birbirine alternatif nitelikte ise bir kural çatışması bulunmadığının kabul edilmesi gerekmektedir (Işıktaç ve Metin, 2016).

Üst Kural (*"Lex Superior"*) İlkesi

Kaynağını normlar hiyerarşisinde bulan üst kural ilkesi uyarınca normlar hiyerarşisinde daha üst düzeyde konumlanan bir hukuk kuralı ile daha alt düzeyde konumlanan bir hukuk kuralı arasında çatışma bulunması halinde uygulanma

önceliği üst düzeyde yer alan kurala aittir. Örneğin, bir yönetmelik hükmü ile bir kanun hükmü arasında çatışma varsa uygulamada kanun hükmü esas alınacaktır (Gözler, 2017). Belirtilmesinde fayda görülmektedir ki alt düzeyde yer alan bir kuralın uygulanabilmesi için söz konusu kural, normlar hiyerarşisinde kendisinden yalnızca bir seviye üstte bulunan kurala değil üst düzeylerde bulunan her bir hukuk kuralına uygun olmak zorundadır. Aksi halde alt düzeyde bulunan kural, üst kural ilkesi gereği bir üst düzeyde bulunan hukuk kuralına uygun olsa dahi daha üst düzeyde bulunan kurala aykırılık teşkil etmekte ise uygulanması mümkün olmayacak ve alt düzeyde bulunan kurallarla çelişen üst kural uygulama alanı bulacaktır (Gözler, 2017).

Bu noktada ayrıca ifade etmek gerekir ki ülkemiz hukuk sisteminde diğer bazı ülkelerde olduğu gibi uygulama esasları anayasada belirlenmiş, normlar hiyerarşisinde anayasa ile kanunlar arasında konumlanmış ve kamu kurum ve kuruluşlarının örgütlenişi ile temel hak ve özgürlüklerin kullanımı gibi konuları düzenlemesi öngörülen organik kanunlar bulunmamaktadır (Bakırcı, 2021). Bu bağlamda, her ne kadar temel hak ve özgürlüklerin korunması amacıyla yürürlüğe konulmuş ve konu bakımından herhangi bir ayrım gözetmeden kişisel veri işleme faaliyetlerinde riayet edilmesi gereken ilkeler ile usul ve esasları öngören temel düzenleme niteliğini haiz olsa da KVKKn ile diğer kanunlar arasında normlar hiyerarşisi bağlamında bir altlık-üstlük ilişkisi bulunmamaktadır. Dolayısıyla, KVKKn hükümleri ile diğer kanun hükümleri arasındaki ilişkinin tayininde üst kural ilkesine başvurulması mümkün değildir.

Sonraki Kural (*"Lex Posterior"*) İlkesi

Farklı düzeyde yer alan hukuk kuralları arasında çatışma olabileceği gibi aynı düzeyde bulunan kurallar arasında da çatışma olabilecektir. Böyle durumlarda üst kural ilkesi yetersiz kalmaktadır (Gözler, 2017). Aynı düzeyde bulunan normlar arasındaki çatışmayı çözüme kavuşturmada başvurulabilecek ilk ilke sonraki kural ilkesidir. Bu ilkeye göre farklı tarihlerde kabul edilmiş kurallar arasında bir çatışma ortaya çıkması halinde sonraki tarihli kuralın önceki tarihli kuralı örtülü bir biçimde yürürlükten kaldıracağı ve çatışan düzenlemelerden sonraki tarihli olanın uygulama alanı bulacağı kabul edilir (Işıktaç ve Metin, 2016).

Sonraki kural ilkesinin amacı, yasa koyucunun en güncel iradesinin uygulamada etkili olabilmesidir. Zira yasa koyucu yeni bir kural koyarak uyuşmazlığa konu olay hakkında yeni bir düzenleme getirmekte ve önceki çözümden vazgeçmektedir (Işıktaç, 2004). Ayrıca yakın tarihli düzenlemenin değişen şartlar dikkate alınarak yapılan bir yeniden değerlendirmenin ürünü olduğu ve bu sebeple top-

lumun ihtiyaçlarını daha etkin bir biçimde karşılayabileceği varsayılmaktadır (Sözer, 2008).

Özel Kural (*"Lex Specialis"*) İlkesi

Normlar hiyerarşisinde aynı seviyede bulunan kurallar arasında çıkacak çatışmaların çözümünde kullanılabilecek ikinci ilke ise özel kural ilkesidir. Bu ilke gereğince aynı olaya uygulanacak birden çok kuralın bulunması halinde diğerine kıyasla özel hüküm niteliğini haiz kural öncelikle uygulanacaktır. Özel kural ilkesine göre, çatışan kurallar arasında konuya ilişkin daha fazla düzenleme içeren kurala öncelik tanınması gerekmektedir (Işıktaç, 2004). Çünkü, özel kural konuyu daha yakından ele almakta olup söz konusu olaya özgü şartları dikkate alarak daha etkin bir çözüm sunmaktadır (Işıktaç, 2015).

Aslında yasa koyucu daha özel nitelikte bir kural kabul ederek genel kurala bir istisna yaratmış olmaktadır (Gözler, 2017). Bu anlamda, özel kuralın öncelikle uygulanması da aynen sonraki kural ilkesinde olduğu gibi yasa koyucunun iradesinin tam anlamıyla uygulamaya yansıtılmasının da bir gereğidir (Güneş, 2017).

Diğer yandan, üst kural ve sonraki kural ilkelerinin uygulanması gereken hallerde aralarında çatışma bulunan kuralların niteliğinin tespiti objektif kıstaslarla sağlanabiliyorken özel kural ilkesinin uygulanması gereken durumlarda çatışan iki hükümden hangisinin genel, hangisinin özel nitelikte olduğunun tespiti daha sübjektif kıstaslar çerçevesinde gerçekleştirilebilecektir (Gözler, 2017). GÖZLER'e göre kuralların uygulama alanı, kuralın içeriği ve diğerinin yokluğunda boşluk doldurma kabiliyetine sahip olma genel/özel kural ayrımı yapmada göz önünde bulundurulabilir (Gözler, 2017). Bu kapsamda ilk olarak, genel kural birbiri ile benzer nitelikte birçok hukuksal ilişki türünü veya faaliyeti düzenlemekteyken özel kural bunlar arasından yalnızca bir türe yönelik düzenlemeleri içermektedir (Işıktaç ve Metin, 2016). İkinci olarak, genel kural bütüncül bir düzenleme öngörmekteyken; özel kural düzenleme konusu şeye "yer, zaman, konu ve kişi bakımından" bütüncül düzenlemeden farklı ve spesifik hükümler getirmektedir (Gözler, 2017). Son olarak, genel kural özel kuralın yokluğunda herhangi bir boşluğun ortaya çıkmasını engelleyebilecek niteliktedir (Gözler, 2017). Bu durum, genel kuralın uygulama alanının özel kuralın uygulama alanını da kapsamasının doğal bir sonucudur.

Çapraz Çatışmalar

Aralarında altlık-üstlük ilişkisi bulunan kurallar arasındaki çatışma her hal ve şart altında üst kural ilkesi vasıtasıyla çözülecek olup normlar hiyerarşisinde daha üstte bulunan kurala öncelik tanınacaktır. Bununla birlikte, çatışmanın aynı düzeyde yer alan kurallar arasında çıkması durumunda her zaman sonraki kural veya özel kural ilkelerinden birinin uygulanması ile çözüme ulaşılması mümkün olmayabilir. Şöyle ki kuralların hem kabul tarihlerinin hem de genel veya özel olma niteliklerinin birlikte göz önünde bulundurulması gereken çapraz çatışmalar ortaya çıkabilir.

Çatışmanın farklı tarihlerde kabul edilmiş iki genel kural veya iki özel kural arasında çıkması halinde sonraki kural ilkesi gereğince sonraki tarihli kural uygulanır. Bununla birlikte, önceki tarihli genel kural ile sonraki tarihli özel kural arasındaki çatışmaların çözümü gerek sonraki kural gerek özel kural ilkesi çerçevesinde sonraki tarihli özel kuralın uygulanması ile sağlanır.

Ancak, önceki tarihli özel kural ile sonraki tarihli genel kural arasındaki çatışmanın çözümünde birtakım problemlerle karşılaşılmakta ve çatışma çözümünün sonraki kural ilkesiyle mi yoksa özel kural ilkesiyle mi çözüleceğinin sorgulanması gerekmektedir (Işıktaç, 2004). Bir görüşe göre sonraki tarihli genel kuralın önceki tarihli özel kuralı kaldırması hiçbir şekilde mümkün değilken (Gözübüyük, 2008) diğer görüşe göre hangi kuralın öncelikle uygulanacağının yasa koyucunun amacına bakılarak tespit edilmesi gerekmektedir (Güriz, 2009; Bilge, 2017; Güneş, 2017; Sözer, 2008; Işıktaç ve Metin, 2016). Ayrıca, yapılacak değerlendirmede somut olayın özelliklerinin, uygulanmasına karar verilecek düzenlemeden etkilenecek tarafların menfaatlerinin ve meri hukukun temel ilkelerinin de göz önünde bulundurulması gerektiği savunulmaktadır (Işıktaç ve Metin, 2016).

6698 sayılı Kanun Hükümlerinin Diğer Kanun Hükümleri Karşısındaki Konumu

Yukarıda ülkemizde neden münhasıran kişisel verilerin korunması alanını düzenleyen bir yasaya ihtiyaç duyulduğuna ilişkin açıklamalarda ifade edildiği üzere KVKKn'nin yürürlüğe konulmasının başlıca gerekçelerinden biri sektörel düzenlemelerin bireylerin kişisel verilerinin işlenmesi bağlamında temel hak ve özgürlüklerinin korunmasında yetersiz kalmasıdır. KVKKn, kişisel verilerin korunmasında alana özgü düzenlemelerin sunmuş olduğu sınırlı ve etkin olmayan güvenceler karşısında uygulamada oluşan boşluğu doldurmak amacıyla kabul edilmiştir. KVKKn'deki düzenlemeler, kim tarafından, hangi amaçla ve ne kapsamda gerçekleştirildiği fark etmeksizin bütün kişisel veri işleme faaliyetlerine uygulanabilecek niteliktedir. Bu anlamda, KVKKn'nin çerçeve düzenleme niteliğini haiz olduğu ve kişisel veri işleme faaliyetleri hakkında maddi kurallar içeren

diğer kanunlara göre genel kurallar içerdiği değerlendirilmektedir. Benzer şekilde KVKKn genel gerekçesinde,

"Avrupa Konseyi ayrıca, kişisel verilerin korunmasına yönelik, tıbbi veri bankaları, bilimsel araştırma ve istatistik, doğrudan pazarlama, sosyal güvenlik, sigorta, polis kayıtları, istihdam, elektronik ödeme, telekomünikasyon ve internet gibi çeşitli sektörlerde uygulanacak ilkeleri belirleyen tavsiye kararları da kabul etmiştir. Tasarının hazırlanması sırasında, söz konusu tavsiye kararları göz önüne alınmakla beraber, Tasarının "çerçeve tasarı" niteliği korunmuştur. Tüm sektörlerle ilgili düzenlemelere yer verilmesi halinde, Tasarının hacminin çok genişleyeceği düşünülerek, söz konusu tavsiye kararları Tasarıya alınmamıştır. Bu tavsiye kararlarında yer alan ilkelere, ilerleyen süreçte, değişik sektörlerle ilgili yapılacak düzenlemelerde yer verilebileceği değerlendirilmiştir."

açıklamalarına yer verilmiştir (Türkiye Büyük Millet Meclisi, 2016a, 6). Söz konusu açıklamalardan KVKKn ile sektörler-üstü bir anlayışla kişisel veri işleme faaliyetlerini gerçekleştirirken riayet edilmesi gereken genel nitelikli kuralların getirilmek istendiği ve ihtiyaca göre ilerleyen süreçte belli başlı kişisel veri işleme faaliyetlerine ilişkin özel düzenlemelerin de kabul edilebileceğine ilişkin bir yönlendirme yapıldığı anlaşılmaktadır.

Öte yandan, KVKKn'nin kişisel verilerin imhasına ilişkin usul ve esasları düzenleyen 7'nci maddesinin ikinci fıkrası ile yurt içinde aktarımı düzenleyen 8'inci ve yurt dışına aktarımı düzenleyen 9'uncu maddelerinin son fıkralarında ilgili diğer kanun hükümlerinin saklı olduğu öngörülmüştür. Bu kapsamda KVKKn'de, genel hükümlere yer verilmekte ve önceki veya sonraki tarihli özel düzenlemelerin öncelikle uygulanacağı açıkça belirtilmek suretiyle diğer kanun hükümleri ile bir çatışma ortaya çıkması halinde çatışmanın özel kural ilkesine göre çözülmesi sağlanmaktadır.

Bununla birlikte, AYM'nin, KVKKn'nin, bazı hükümlerinin iptali istemiyle açılan davada vermiş olduğu kararda, KVKKn'nin 7'nci maddesinin ikinci fıkrasında yer alan,

"Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır."

hükmü hakkında,

"Genel kanun niteliğindeki 6698 sayılı Kanun'da kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin her durumun öngörülmesi ve düzenlenmesi mümkün olamayacağı gibi daha sonra ortaya çıkabilecek özel durumlara ilişkin hususların özel kanunlarda daha detaylı düzenlenmesi de gerekebilir. Bu durumda aynı konuyla ilgili olarak genel kanunda ve özel kanunda hüküm bulunması hâlinde özel kanun hükmü uygulanacağından kuralın belirsiz olduğu söylenemez. Ayrıca dava konusu kuralın bazı özel durumlara ilişkin hususların daha ayrıntılı şekilde düzenlenmesini sağlamaya yönelik kamu yararı amacıyla düzenlendiği açıktır. Dava konusu kuralın ulaşılmak istenen amaç için elverişli ve gerekli olduğu, amaç ve araç arasında makul ve uygun bir ilişki kurduğu ve orantılı olduğu anlaşıldığından kuralda ölçülülük ilkesine aykırı bir yön de bulunmamaktadır."

değerlendirmesi yapılmıştır (Anayasa Mahkemesi, 2017). Belirtmek gerekir ki mezkûr kararda, kişisel verilerin yurt içinde ve yurt dışına aktarımına ilişkin olarak diğer kanunlarda yer alan hükümlerin saklı olduğunu öngören 8'inci maddenin üçüncü fıkrası ve 9'uncu maddenin altıncı fıkrası bakımından da aynı değerlendirmenin geçerli olduğu belirtilmiştir (Anayasa Mahkemesi, 2017). Bu kapsamda, KVKKn hükümlerinin genel kural niteliğini haiz olduğu ve diğer düzenlemelerde yer alan özel kuralların KVKKn hükümleri karşısında öncelikle uygulanacağı açıkça ifade edilmiştir.

KİŞİSEL VERİLERİ KORUMA KURULU'NUN MEVZUAT TASLAKLARI HAKKINDA GÖRÜŞ VERME YETKİSİ

KVK Kurulu'nun görev ve yetkileri KVKKn'nin 22'nci maddesinde düzenlenmekte olup anılan maddenin birinci fıkrasının (h) bendinde,

"Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek"

Kurul'un görevleri arasında sayılmaktadır. Söz konusu görüş verme yetkisi bağlamında KVK Kurulu bir *"politika danışmanı"* rolünü üstlenmektedir (Bennett ve Raab, 2017).

KVKKn m.19/4 uyarınca KVK Kurumu'nun karar organı olan Kurul, söz konusu yetkisi ile ülkemiz kişisel verilerin korunması politikası yapım çalışmalarına katkı sağlamakta ve bilhassa kamu kurum ve kuruluşlarının işleme faaliyetlerini yönlendirmektedir. Böylelikle, şikâyet üzerine veya resen inceleme sonucunda tesis edilen Kurul Kararları ile ihlal sonrası bozulan düzeni telafi edici rolüne önleyicilik ekleyerek kişisel verilerin işlenmesi bağlamında temel hak ve özgürlüklerin korunması amacıyla yürütmekte olduğu faaliyetlerin etkinliğini en üst düzeye çıkarmaktadır.

Bir önceki bölümde açıklandığı üzere KVKKn kişisel verilerin işlenmesine ilişkin ayrıksı hükümler barındıran diğer düzenlemeler karşısında genel kural niteliğini haizdir. Dolayısıyla, mevzuatta KVKKn'den ayrışan düzenlemeler öncelikle uygulama alanı bulacaktır. Yasa koyucu, KVKKn'yi çerçeve kanun olarak tasarlayarak işleme faaliyetinin veya işleme faaliyetini gerçekleştiren kişi, kurum ve kuruluşların tabi olduğu düzenlemelerde öngörülen ve alana özgü nitelikteki diğer gerekliliklerin sağlanmasına halel gelmemesini amaçlamıştır. Bununla birlikte, KVKKn ile Anayasa m. 20'nin gereği olarak kişisel verilerin korunması alanında bireylere yönelik temel güvencelerin belirlendiği dikkate alınarak; KVKKn'nin uygulanması hususunda denetleyici yetkilere sahip KVK Kurulu'nun kişisel verilere ilişkin hüküm içeren mevzuat yapım çalışmalarına etkin bir şekilde katılımının temini ve böylece KVKKn'de öngörülen söz konusu koruma mekanizmalarının işlevselliğinin muhafaza edilmesi amaçlanmıştır.

Öte yandan, Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği m.7/1(ı) uyarınca KVK Kurulu; kişisel verilerin işlenmesi, korunması ve güvenliği ile alakalı sektörel düzenleme esaslarını belirlemekle de görevli ve yetkili kılınmıştır. Bu anlamda, belirli kişisel veri işleme faaliyetlerinin alana özgü dinamikleri dikkate alınarak; hem kişisel verilere en üst düzeyde koruma sağlanmaya hem de kişisel verilerden azami miktarda katma değer elde edilmeye çalışılmaktadır. Nitekim, KVK Kurumu'nun misyonu da,

"Anayasada öngörülen özel hayatın gizliliği ile temel hak ve özgürlüklerin korunması kapsamında, Ülkemizde kişisel verilerin korunmasını sağlamak ve buna yönelik farkındalık oluşturarak bilinç düzeyini geliştirmek, aynı zamanda veri temelli ekonomide özel ve kamusal aktörlerin uluslararası rekabet kapasitelerini artırıcı bir ortam oluşturmak."

şeklinde belirlenmiştir (Kişisel Verileri Koruma Kurumu, t.y.).

KVK Kurulu tarafından 2019 yılında 11 (Kişisel Verileri Koruma Kurumu, 2020), 2020 yılında 23 (Kişisel Verileri Koruma Kurumu, 2021) ve 2021 yılında ise 48 (Kişisel Verileri Koruma Kurumu, 2022) adet mevzuat taslağına görüş verilmiştir. Teşkilat Yönetmeliği m.16/1(e) uyarınca mevzuat taslakları hakkında görüş verilmesine ilişkin iş ve işlemler KVK Kurumu Hukuk İşleri Dairesi Başkanlığı'nca takip edilmektedir. Mevzuat taslaklarına ilişkin olarak alınacak Kurul Kararı için gerekli dokümanlar ile görüş ve değerlendirmeleri içerir takrir anılan Daire Başkanlığı tarafından hazırlanmaktadır. Ardından hazırlanan belgeler, Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik m.8/2 uyarınca toplantı tarihinden en az üç gün önce Kurul üyelerine dağıtılmaktadır. Kurul

toplantısında alınan kararlar, KVKKn m.23/5 uyarınca en çok on beş gün içinde yazılmakta ve Kurul Kararı'nda yer verilen değerlendirmeler ve öneriler, Mevzuat Hazırlama Usul ve Esasları Hakkında Yönetmelik'in ekinde yer alan forma uygun olarak mevzuat taslağını hazırlayan ilgili kamu kurumuna iletilerek görüş verme süreci tamamlanmaktadır.

Kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında KVK Kurulu'nun görüşünü almak büyük bir önem arz etmekte olup yargı makamları tarafından ilgili mevzuat taslakları hakkında KVK Kurulu'nun görüşünün alınması zorunlu olarak görülmektedir. Şöyle ki Danıştay 15. Dairesi, 6/7/2017 tarihli ve E. 2016/10500 K. YD. sayılı Kararı'nda,

"(...) genel gerekçe ve Kanun hükümlerine göre, Kişisel Verileri Koruma Kurulu'nun kişisel verilerin korunması konusunda genel nitelikte bir kontrol ve denetim yetkisine sahip olduğu, diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hükümler içeren mevzuat taslakları hakkında Kişisel Verileri Koruma Kurulu'ndan görüş alınmasının şart olduğu, Kişisel Verileri Koruma Kurulu'nun kontrol ve denetiminden geçirilmeksizin hazırlanan ve 20/10/2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren dava konusu düzenlemede bu nedenle mevzuata ve hukuka uygunluk bulunmadığı sonucuna ulaşılmıştır."

ifadelerine yer vermiş ve Karar sonucunda Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in yürütmesini durdurmuştur (Danıştay, 2017). Bu kapsamda, kamu kurum ve kuruluşlarının kişisel veri işleme faaliyetlerine ilişkin usul ve esaslar içeren mevzuat taslaklarını KVK Kurulu'nun görüşüne sunmakla yükümlü kılınmış oldukları söylenebilecektir. Dolayısıyla, kurumların mevzuat yapım sürecinde KVK Kurumu ile istişare içinde olmasında ve Kurul'un görüşlerini azami derecede taslak düzenlemeye yansıtmalarında fayda bulunduğu değerlendirilmektedir.

Kişisel Verilere İlişkin Hüküm İçeren Mevzuat Taslakları Hazırlanırken Dikkat Edilmesi Gereken Hususlar

Daha öncesinde ifade edildiği üzere, kişisel verilerin korunması hakkı, Anayasa'da bir temel hak ve özgürlük olarak tanınmıştır. Söz konusu hakka ilişkin Anayasa hükmünde, kişisel verilerin ancak ilgili kişinin açık rızasının bulunması veya kanunda öngörülmesi halinde işlenebileceği ve kişisel verilerin korunmasına ilişkin usul ve esasların kanunla düzenleneceği hükme bağlanmıştır. Bu kapsamda, KVKKn yürürlüğe konulmuş ve kişisel veri işleme faaliyetlerinde göz önünde bulundurulması gereken temel ilkeler, kişisel verilerin işlenme şartları, haklar

ve yükümlülükler belirlenmiştir. Bu çerçevede, mevzuat taslaklarında KVKKn'de öngörülen temel güvenceleri bertaraf etmeyecek bir yaklaşımın benimsenmesi uygun olacaktır. Ayrıca kişisel verilere ilişkin hüküm içeren her düzenlemenin temel hak ve özgürlüklerin sınırlandırılmasına ilişkin usul ve esasları düzenleyen Anayasa m.13 hükmüne uygun olarak hazırlanması gerekmektedir.

Diğer taraftan, yeknesak ve etkin bir veri koruma hukuku uygulaması temin edebilmek adına mevzuat taslaklarında KVKKn ve KVK Kurulu tarafından çıkartılan ilgili ikincil mevzuat hükümleri ile uyumlu bir terminoloji kullanılmasının uygun olacağı değerlendirilmektedir. Bu bağlamda, veri koruma hukukunun temel kavramlarının ve bunlara ilişkin tanımların mevzuat taslaklarına birebir yansıtılması önem arz etmektedir.

Bununla birlikte, KVKKn'nin çerçeve nitelikli bir düzenleme olması sebebiyle diğer kanunlarla ayrıksı usul ve esaslar öngörülebilecektir. Ancak herhangi bir tereddüde yol açmamak adına KVKKn ve ilgili özel düzenleme arasındaki uygulama alanı farklılığının açık bir şekilde ortaya konmasında fayda bulunmaktadır.

Ayrıca KVKKn'de bireyler bakımından öngörülen hak arama yollarına ilişkin kolaylaştırıcı mekanizmaların ve hesap verebilirlik başta olmak üzere veri işleme faaliyetinde bulunan kişi ve kuruluşlara yönelik sorumluluk rejiminin, taslak düzenlemelerde de azami düzeyde muhafaza edilmesinin uygun olacağı değerlendirilmektedir. Yine, bireylerin haklarının yeterli bir koruma ile güvence altına alınabilmesi için KVK Kurulu'nun kişisel verilerin korunması alanında bir bağımsız idari otorite olarak etkin bir biçimde faaliyet göstermesi gereği dikkate alındığında; KVK Kurulu'nun inceleme ve yaptırım uygulama yetkilerini kısıtlamamaya özen gösterilmesinin yararlı olacağı değerlendirilmektedir.

Mevzuat Taslaklarına Görüş Verme Yetkisine İlişkin Düzenlemelere Yönelik Öneriler

KVK Kurulu, mevzuat taslaklarına verdiği görüşlerle ülkemiz kişisel verilerin korunması politikasına katkı yapmakla beraber, bu alanda uzmanlaşmış bir idari makam olarak KVK Kurulu'nun bahse konu politika yapım çalışmalarına daha aktif ve etkili bir biçimde katılabilmesi için bazı reformların yapılabileceği değerlendirilmektedir.

Öncelikle, yukarıda da ifade edildiği üzere kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş verme yetkisi münhasıran KVK Kurulu'na aittir. KVK Kurulu yetkilerini, Kişisel Verileri Koruma Kurulu Çalışma Usul ve

Esaslarına Dair Yönetmelik'e uygun olarak tesis ettiği Kurul Kararları vasıtasıyla kullanmaktadır. Herhangi bir konu, Kurul gündemine alınmadan önce KVK Kurumu'nun ilgili hizmet birimleri tarafından araştırmalar yapılarak değerlendirmeler ve öneriler oluşturulmaktadır. Ardından hazırlanan bu dokümanlar KVK Kurulu'nun takdirlerine arz edilmektedir. KVK Kurulu ise Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik m.10/1 uyarınca gerçekleştireceği müzakere sonucunda hizmet birimleri tarafından hazırlanan görüş ve değerlendirmelere nihai halini vermektedir. Bu bağlamda, kişisel verilerin korunmasına yönelik olarak günümüzde ortaya çıkan meselelerin karmaşık yapısı da göz önünde bulundurulduğunda; KVK Kurulu tarafından konunun bütün yönlerini dikkate alan bir Karar'ın tesis edilebilmesi için yeterince uzun bir süre tanınması gerekmektedir.

Buna karşılık, Mevzuat Hazırlama Usul ve Esasları Hakkında Yönetmelik m.7/1'de hiçbir ayırım gözetilmeden görüş istenilen bütün kamu kurum ve kuruluşlarının görüşlerini on beş gün içinde bildirmekle yükümlü oldukları ve süresinde görüş bildirmeyen kurumların görüşlerinin olumlu sayılacağı hükme bağlanmıştır. KVKKn m.23/5'te yalnızca Kurul Kararı'nın yazımı için on beş günlük bir süre tanındığı dikkate alındığında; anılan Yönetmelik'teki düzenlemenin KVK Kurulu'nun etkin bir biçimde çalışmasını engelleyebileceği değerlendirilmektedir. Bu noktada belirtilmesinde fayda görülmektedir ki KVK Kurulu, KVKKn m.21/1'de öngörülen,

"Kurul, bu Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz."

hükmü çerçevesinde bağımsız bir biçimde faaliyetlerini sürdürebilmelidir. Bu kapsamda, KVK Kurulu'nun görüş verme yetkisi bağlamında bağımsız hareket edebilmesini ve mevzuat taslakları üzerinde gerekli incelemeleri yapabilmesini temin edecek şekilde, Kurul tarafından yürütülecek işlemlere ilişkin usul ve esasların ayrı bir düzenlemede öngörülebileceği düşünülmektedir.

Öte yandan, Mevzuat Hazırlama Usul ve Esasları Hakkında Yönetmelik m.6/1'de belirli konularla ilgili olarak belirli kamu kurum ve kuruluşlarından görüş alınması zorunlu tutulmuştur. Benzer şekilde, Yönetmelik'in anılan hükmüne eklenecek bir bentle kişisel veri işleme faaliyetlerine ilişkin hüküm içeren mevzuat taslakları hakkında KVK Kurulu'nun görüşünün alınması gerektiğinin düzenlenebileceği değerlendirilmektedir.

SONUÇ

KVKKn, mahiyeti gereği çerçeve düzenleme niteliğindedir. Zaten diğer sebeplerin yanında KVKKn gibi kişisel verilerin işlenmesine ilişkin genel kuralları içerir bir düzenlemenin yürürlüğe konulmasındaki amaç hem kişisel verilerin korunması alanındaki ana iskeleti kurarak özel düzenlemelerde öngörülen kısmi güvencelere işlerlik sağlamak hem de özel düzenleme bulunmayan alanlarda gerçekleştirilen kişisel veri işleme faaliyetlerinden kaynaklanan güvence boşluğunu doldurmaktır. Bu noktada önemle belirtmek gerekir ki KVKKn kişisel verilerin korunması alanındaki temel düzenleme olmakla birlikte gerek kendinden önce gerek kendinden sonra kabul edilen özel düzenlemeleri tamamlayıcı niteliktedir. Diğer bir deyişle KVKKn, kişisel verilerin korunması alanında asli; kişisel verilerin işlenmesine ilişkin usul ve esasları belirleme konusunda ise çerçeve düzenleme olma niteliğine sahiptir.

Çerçeve düzenleme olma niteliği, KVKKn'yi kişisel verilere ilişkin hüküm içeren diğer kanunlar karşısında genel kanun olarak konumlandırmıştır. Bu anlamda, sektörel düzenlemelerde öngörülen ayrıksı hükümler özel kural ilkesi uyarınca öncelikle uygulama alanı bulacaktır. KVKKn'nin bu tasarımı, alana özgü gerekliliklerin yerine getirilebilmesini mümkün kılmaktadır. Fakat aynı zamanda, kişisel verilerin işlenmesinde temel hak ve özgürlüklerin korunması bağlamında KVKKn ile bireylere sağlanan temel güvencelerin zayıflatılması riski bulunmaktadır. Söz konusu riskin asgari düzeye indirilebilmesi adına KVKKn'de kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş verme KVK Kurulu'nun yetkileri arasında sayılmıştır.

KVK Kurulu söz konusu mevzuat taslakları hakkında görüş vererek ülkemizin kişisel verilerin korunması politikası yapım sürecine aktif bir biçimde katılmaktadır. Böylelikle, her ne kadar çerçeve nitelikli bir düzenleme olsa da öngördüğü temel güvencelerin sürekliliği sağlanarak KVKKn'nin ülkemiz veri koruma hukukunun omurgasını teşkil etme niteliği muhafaza edilmeye çalışılmaktadır.◆

KAYNAKÇA

- Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü. (2021). Avrupa Birliğinde Cezaî Konularda Uluslararası Adlî İş Birliği. https://diabgm.adalet.gov.tr/Resimler/SayfaDokuman/12102021113843AB-K%C4%B0TAP-14-09-2021.pdf adresinden 30.09.2022 tarihinde alındı.
- Akçalı Gür, B. (2020). The normative power of the EU: a case study of data protection laws of Turkey, *International Data Privacy Law,* Vol. 10, No. 4. 314-329.
- Akıllıoğlu, T. (2004). İdari Usul ve Kişisel Verilerin Korunması. https://www.idare.gen.tr/akillioglu-idariusul.htm adresinden 16.09.2022 tarihinde alındı.
- Albrecht, J. P. (2016). How the GDPR Will Change the World, *European Data Protection Law Review (EDPL),* Vol. 2, No. 3. 287-289.
- Anayasa Mahkemesi. (2017). 28/9/2017 tarihli ve E. 2016/125 ve K. 2017/143 sayılı Karar. https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2017/143?KelimeAra%5B%5D=6698 adresinden 10.10.2022 tarihinde alındı.
- Avrupa Birliği Adalet Divanı. (2015). 6 Ekim 2015 tarihli ve C-362/14 sayılı Ön Karar. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN adresinden 10.10.2022 tarihinde alındı.
- Avrupa Birliği Başkanlığı. (2020). Türkiye Avrupa Birliği İlişkilerinde Önemli Tarihler. https://www.ab.gov.tr/siteimages/birimler/kpb/kronoloji-trkce-ocak2020.pdf adresinden 24.09.2022 tarihinde alındı.
- Avrupa Birliği Başkanlığı. (2021). Avrupa Birliği ve Üyelik Sürecimiz. https://www.ab.gov.tr/siteimages/2021_05/ab_ve_uyelik_surecimiz_temel_bilgiler_kitabi.pdf adresinden 26.09.2022 tarihinde alındı.
- Avrupa Komisyonu. (2015). Commission Staff Working Document-Turkey 2015 Report. https://www.ab.gov.tr/files/5%20Ekim/2015_turkey_report.pdf adresinden 24.09.2022 tarihinde alındı.
- Avrupa Konseyi. (1981). Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434 adresinden 19.09.2022 tarihinde alındı.

◊ Avrupa Konseyi. (t.y.). Chart of signatures and ratifications of Treaty 108. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 adresinden 10.10.2022 tarihinde alındı.

◊ Bakırcı, F. (2021). Temel Yasalar ve Temel Yasaların Görüşme Yöntemi. F. Bakırcı, M. Çekiç ve B. Dağsalı (Yay. Haz.), *Antik ve Modern Dönemde Yasalar ve Yasa Yapımı Paneli* (59-101) içinde. Ankara: Ankara Barosu Başkanlığı.

◊ Banisar, D. ve Davies, S. (1999). Global Trends İn Privacy Protection: An International Survey Of Privacy, Data Protection, And Surveillance Laws And Developments, *John Marshall Journal Of Information Technology & Privacy Law,* Vol. 18. 1-111.

◊ Başalp, N. (2004). *Kişisel Verilerin Korunması ve Saklanması.* Ankara: Yetkin Yayınları.

◊ Bennett, C. ve Raab, C. (2017). Governance of Privacy. New York: Routledge.

◊ Bilge, N. (2017). *Hukuk Başlangıcı.* Ankara: Turhan Kitabevi.

◊ Bilir, F. (2020). 6698 Sayılı Kişisel Verilerin Korunması Kanunu'na İlişkin Değerlendirme ve İnternet Çağında Kişisel Verilerin Korunması, *Anayasa Yargısı Dergisi,* Cilt 37, Sayı 2. 305-342.

◊ Bilir, F. (2021). Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır, *TRT Akademi,* Cilt 6, Sayı 11. 173-180.

◊ Bradford, A. (2012). The Brussels Effect, *Northwestern University Law Review,* Vol. 107. 1-68.

◊ Cumhurbaşkanlığı Devlet Denetleme Kurulu. (2013). Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları Raporu. https://www.ttb.org.tr/images/stories/file/2015/ddk_rapor.pdf adresinden 12.09.2022 tarihinde alındı.

◊ Çekin, M. S. (2020). *Kişisel Verilerin Korunması Hukuku.* İstanbul: On İki Levha Yayıncılık.

◊ Danıştay. (2017). 15. Daire, 6/7/2017 tarihli ve E. 2016/10500 K. YD. sayılı Karar. https://www.lexpera.com.tr/ictihat/danistay/15-d-e-2016-10500-k-yd-t-6-7-2017 adresinden 10.10.2022 tarihinde alındı.

◊ Dixon, H. (2018). Regulate to Liberate Can Europe Save the Internet?. Foreign Affairs. September/October 2018. https://www.foreignaffairs.com/articles/europe/2018-08-14/regulate-liberate?check_logged_in=1 adresinden 10.10.2022 tarihinde alındı.

◊ Dülger, M. V. (2019). Kişisel Verilerin Korunması Hukuku. İstanbul: Hukuk Akademisi.

◊ Gözler, K. (2013). Yorum İlkeleri. O. Ergül (Yay. Haz.), *Anayasa Hukukunda Yorum ve Norm Somutlaşması* (15-119) içinde. Ankara: Kamu Hukukçuları Platformu ve Türkiye Barolar Birliği Ortak Yayını.

◊ Gözler, K. (2017). *Hukuka Giriş.* Bursa: Ekin Basın Yayın Dağıtım.

◊ Gözübüyük, A. Ş. (2008). *Hukuka Giriş ve Hukukun Temel Kavramları.* Ankara: Turhan Kitabevi.

◊ Gültekin Varkonyi, G. (2017). Evaluation On Turkey's Data Protection Adventure, European Data Protection Law Review (EDPL), Vol. 3, No. 2. 238-243.

◊ Güneş, A. M. (2017). *Hukuk Metodolojisi.* Bursa: Ekin Basım Yayın Dağıtım.

◊ Güriz, A. (2009). *Hukuk Başlangıcı.* Ankara: Siyasal Kitabevi.

◊ Gürsel, İ. (2016). Protection Of Personal Data İn International Law And The General Aspects of the Turkish Data Protection Law, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 18, Sayı 1. 33-61.

◊ Işıktaç, Y. (2004). *Hukuk Normunun Mantıksal Analiz ve Uygulaması.* İstanbul: Filiz Kitabevi.

◊ Işıktaç, Y. (2015). *Hukuk Başlangıcı.* İstanbul: Filiz Kitabevi.

◊ Işıktaç, Y. ve Metin, S. (2016). *Hukuk Metodolojisi.* İstanbul: Filiz Kitabevi.

◊ Kama Işık, S. (2020). *Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış.* İstanbul: On İki Levha Yayıncılık.

◊ Kişisel Verileri Koruma Kurumu. (2019). Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF adresinden 21.08.2020 tarihinde alındı.

◊ Kişisel Verileri Koruma Kurumu. (2020). 2019 Yılı Faaliyet Raporu. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/c325adf5-5337-4567-95c8-b6b953b745aa.pdf adresinden 10.10.2022 tarihinde alındı.

◊ Kişisel Verileri Koruma Kurumu. (2021). 2020 Yılı Faaliyet Raporu. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/60c02fcc-0abf-4c8e-8b9b-514f34a1b0e6.pdf adresinden 10.10.2022 tarihinde alındı.

◊ Kişisel Verileri Koruma Kurumu. (2022). 2021 Yılı Faaliyet Raporu. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/eaf2f71e-efa5-48e2-9326-9b7fa2813193.pdf adresinden 10.10.2022 tarihinde alındı.

◊ Kişisel Verileri Koruma Kurumu. (t.y.) Misyon-Vizyon. https://www.kvkk.gov.tr/Icerik/2074/Misyon---Vizyon adresinden 10.10.2022 tarihinde alındı.

◊ Küzeci, E. (2019). *Kişisel Verilerin Korunması.* Ankara: Turhan Kitabevi.

◊ Küzeci, E. ve Boz, B. (2017). The New Data Protection Act in Turkey and its Potential Implication for E-Commerce, *International Data Privacy Law,* Vol. 7, No. 3. 219-230.

◊ Oğuz, H. (2013). Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum, *Uyuşmazlık Mahkemesi Dergisi,* Sayı 3. 1-38.

◊ Öztürk, B. ve Altınok Çalışkan, E. (2018). Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu, *Fasikül Aylık Hukuk Dergisi,* Cilt 10, Sayı 100. 277-336.

◊ Sözer, A. N. (2008). *Hukukta Yöntembilim.* İzmir: Beta.

◊ Şimşek, O. (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması.* İstanbul: Beta.

◊ Şişkin, D.Ş. ve Çakmak, T. (2019). Türkiye'de Kişisel Verilerin Korunması: 1996-2019 Yılları Arasındaki Bilgi Politikası Belgelerine Yönelik Bir Değerlendirme. B. Yalçınkaya, M. A. Ünal, B. Yılmaz ve F. Özdemirci (Der.), *e-BEYAS 2019: Endüstri 4.0 Sürecinde Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ* (465-481) içinde. Ankara: Ankara Üniversitesi Bilgi Yönetim Sistemleri Belgelendirme ve Bilgi Güvenliği Merkezi.

◊ Tene, Ö. ve Saygın, Y. Privacy and Data Protection in Turkey: (Inching) Towards a European Framework, *Privacy & Security Law Report,* 10. http://ssrn.com/abstract=1941005 adresinden 10.10.2022 tarihinde alındı.

◊ Tezcan, D. (1991). Bilgisayar Karşısında Özel Hayatın Korunması, Anayasa Yargısı Dergisi, Cilt 8. 385-392.

◊ Türk Sanayicileri ve İşinsanları Derneği. (2021). TÜSİAD Kişisel Verilerin Korunması Konferansı, "Doğru Veri Yönetimi ile İşinizi Geleceğe Taşıyın" teması ile gerçekleşti. https://tusiad.org/tr/tum/item/10791-tusi-ad-kisisel-verilerin-korunmasi-konferansi-dogru-veri-yonetimi-ile-i-sinizi-gelecege-tasiyin-temasi-ile-gerceklesti adresinden 26.09.2022 tarihinde alındı.

◊ Türkiye Büyük Millet Meclisi. (2008). Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü'nün 22.04.2008 tarihli ve B.02.0.KKG.0.10/101-902/1812 sayılı yazısı. https://www2.tbmm.gov.tr/d23/1/1-0576.pdf adresinden 13.09.2022 tarihinde alındı.

◊ Türkiye Büyük Millet Meclisi. (2010). Adalet ve Kalkınma Partisi Grup Başkanı İstanbul Milletvekili Recep Tayyip Erdoğan ve 264 Milletvekilinin; 7/11/1982 Tarihli ve 2709 Sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun Teklifi ve Anayasa Komisyonu Raporu (2/656). https://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d23/c066/tbmm23066088ss0497.pdf adresinden 10.10.2022 tarihinde alındı.

◊ Türkiye Büyük Millet Meclisi. (2014). Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü'nün 26.12.2014 tarihli ve 31853594-101-580-5204 sayılı yazısı. https://www2.tbmm.gov.tr/d24/1/1-1009.pdf adresinden 13.09.2022 tarihinde alındı.

◊ Türkiye Büyük Millet Meclisi. (2016a). Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu. https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf adresinden alındı.

◊ Türkiye Büyük Millet Meclisi. (2016b). Adalet Komisyonu Tutanak Dergisi, 2'nci Toplantı, 27 Ocak 2016 Çarşamba. https://www5.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.goruntule?pTutanakId=1439 adresinden alındı.

◊ Türkiye Büyük Millet Meclisi. (2016c). Adalet Komisyonu Tutanak Dergisi, 3'üncü Toplantı, 9 Şubat 2016 Salı. https://www5.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.goruntule?pTutanakId=1468 adresinden 10.10.2022 tarihinde alındı.

◊ Türkiye Ekonomi Politikaları Araştırma Vakfi ve Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü. (2014). Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi. https://www.tepav.org.tr/upload/files/1421853130-9.Turkiyede_Kisisel_Verilerin_Korunmasinin_Ekonomik_ve_Hukuki_Analizi.pdf adresinden 14.09.2022 tarihinde alındı.

ULUSAL HUKUKTA KİŞİSEL VERİLERİN KORUNMASI HAKKINA İLİŞKİN İSTİSNAİ HALLER

Reyhan KARCI

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "Uluslararası ve Ulusal Hukukta Kişisel Verilerin Korunması Hakkına İlişkin İstisnai Haller" başlıklı uzmanlık tezinden alınmıştır.

Kişisel verilerin korunması hakkı temelde bireyi korumasından dolayı insan var olduğundan itibaren arka planda hep varlığını sürdüren "arkaik" bir hak olarak düşünülse de bu hakkın hukuk zemininde karşılık bulması çok daha yakın tarihlidir. Kişisel verilerin korunması hakkı, zamanla gelişen teknoloji çağının hukuki düzenlemelerde bulunmasını zorunlu kıldığı "modern" bir hak olarak ifade edilebilir. Söz konusu "modern" hakkın hukuki zeminde karşılık bulması yine öncelikle toplumsal hayattaki değişimler sonucu olmuştur.

İnsanlığın dünyaya kattığı teknolojik kazanımların ve bunun getirdiği yeniliklerin eriştiği seviye, kişilere ait bilgilerin ekonomik bir değeri olduğunun anlaşılmasını sağlamıştır. Çağlar boyunca ekonomik bir değer varlığının keşfi, insanlar tarafından bu konuya ilişkin hukuki bir düzenleme yapılması ihtiyacını da beraberinde getirmiştir. Bu çerçevede kişisel verilerin korunması hakkının hukukta karşılık bulmasına iten güç yine ekonomi olmuştur. (Kişisel verilerin korunması hakkının uluslararası alanda karşılık bulduğu kabul edilen ilk belge Ekonomik İş Birliği ve Kalkınma Teşkilatı (OECD) tarafından yayımlanan ilkelerdir. Rehber ilkeler, ulusal mevzuatlardaki eşitsizlikler nedeniyle, kişisel verilerin sınır ötesi akışının engellenmemesi, böylece veri akışı sağlanırken kişisel verilerin özel ha-

yatın gizliliği ekseninde korunmasını sağlamak amacıyla yayımlanmıştır.)

"Kişisel veri"nin bir meta olarak ekonomik bir değere dönüştüğü gerçeği kuşkusuz olmakla beraber zamanla ekonomik kuruluşlardan ziyade temel haklara ilişkin kuruluşların katkılarıyla uluslararası belgelerde ve birçok ülkenin anayasasında temel bir hak güvencesine kavuşmuştur. Ancak bir hakkın temel bir hak olarak kabul edilmesi sınırsız olduğu anlamına gelmemektedir.

İstisnai birkaç hak dışında birçok hak çeşitli gerekçelerle sınırlandırılabilir niteliktedir. Bir hakka getirilen sınırlamanın niteliği ve yorumu ile hakkın artık kullanılamaz hale gelmesi mümkün olabilmektedir. Bu anlamda hakkın varlığının tanınmasının yanı sıra hakka getirilen sınırlamaların da önem arz ettiği bir gerçektir. Bu bakış açısıyla hazırlanan çalışmanın temelindeki amaç, modern çağın kazanımı olarak tanımlayabileceğimiz kişisel verilerin korunması hakkının, sınırlanmasına ilişkin ulusal hukuktaki düzenlemeler incelenerek ve yargı mercilerinin yorumları dikkate alınarak ulusal hukukta kişisel verilerin korunması hakkına getirilen yorumlara katkı sağlamaktır. Söz konusu amaçla hazırlanan çalışmanın birinci bölümde hukukta istisna halinin ne anlam ifade ettiği ve bir hakkın sınırlandırılmasına dair bakış açısı açıklanmaya çalışılmıştır. Belirtmek gerekir ki hukuki düzenlemelerde açıkça istisna halinin düzenlemesinin yanı sıra temel bir belgenin kapsam maddesi, o belgenin kapsam dışı bıraktığı alanlara da işaret edeceğinden kapsam dışında kalan durumlar da bir hakka getirilen diğer sınırlama durumu olarak değerlendirilebilir.

Bu çerçevede çalışmada ulusal hukukta kişisel verilerin korunması hakkına dair öncelikle Anayasal düzenlemeye ve Anayasa Mahkemesi içtihatlarına ardından söz konusu hakka ilişkin özel bir kanun olan 6698 sayılı Kişisel Verilerin Korunması Kanununda (6698 sayılı Kanun) yer alan hükümler ile bu hakka getirilen istisna durumları detaylandırılmaya çalışılmıştır. Devamında da AB Genel Veri Koruma Tüzüğü (GVKT, Tüzük) ile 6698 sayılı Kanun karşılaştırmalı olarak değerlendirilerek bir hukuk devleti olmanın gereği olarak ulusal hukukun geliştirilmesi adına gereklilikler ortaya konulmaya çalışılmıştır.

HUKUKTA İSTİSNA HALİ VE KİŞİSEL VERİLERİN KORUNMASI HAKKI

Hukukta istisna hali, hukukun üstünlüğünün kabul gördüğü toplumlarda her zaman dikkat çeken bir unsur olmuş ve tartışmaların odağında yer almıştır. Bu tartışmaların en belirgini istisnaların, olağanüstü hal kavramı ile ilişkilendirilmesi durumunda ortaya çıkmaktadır. Olağanüstü hal, hukukun askıya alındığı hal olarak tanımlanabildiği gibi hukukun askıya alınmasının tamamen yasasız

bir alan yaratmadığı da ifade edilir (Agamben, 2006, s.33).

Bu anlamda, kanunda bir konuya ilişkin istisna halinin söz konusu olması, kanun açısından "olağanüstü hal" olduğu durumlar olarak yorumlanabilir. Bu anlamda istisna hallerinin uygulanması durumlarında, özellikle temel hak ve özgürlüklerin sınırlanmasına ilişkin olarak düzenleme altına alınması durumu söz konusu ise karar vericilerin daha dikkatli bir yaklaşımla değerlendirme yapması gerekir. Bu yaklaşım nasıl olmalıdır sorusuna bir yanıt arandığında da "İstisnalar dar yorumlanır" ilkesi ile karşılaşılmaktadır.

"İSTİSNALAR DAR YORUMLANIR" İLKESİ

İstisnalar dar yorumlanır ilkesi toplumsal hayatın yansıması olan "hukuk"ta yerleşik bir ilke halini almıştır. Bu ilke özellikle temel hak ve özgürlüklerin sınırlanması halinin değerlendirilmesinde daha fazla karşılık bulmaktadır.

Ülkemiz mevzuatında istisnaların dar yorumlanmasına ilişkin bir düzenleme bulunmadığından anılan ilkenin ülkemiz mevzuatı açısından kanuni bir dayanağı olmadığı söylenebilir.

İstisna kavramının, sözlük anlamı itibariyle "olağanın dışı"na hüküm getirmesi şeklinde tanımlandığı dikkate alındığında, olağan dışılığı düzenleyen hükmün nasıl yorumlanacağı sorusuna getirilen yanıt "dar yorum"lanacağı şeklinde kabul görmüştür. Bu bağlamda da dar yorumun ne ifade ettiğinin irdelenmesi gerekir. Ancak dar yorumun ne anlama geldiği noktasında, doktrinde farklı bakış açıları bulunmaktadır. Dar yoruma getirilen bakış açılarını üç başlıkta örneklendirmek mümkündür. Bunlardan ilki, yorumlanacak düzenlemenin metinine yani sözüne dayanılarak yapılan lafzi yorumdur. Bu yorum sözcüklerin etimolojik anlamıyla söylemin yorumlanmasıdır. Diğeri ise düzenlemenin uygulama açısından değerlendirilmesini ve olabildiğince az sayıda olaya uygulanması şeklindedir ve bu bakış açısı devamında kıyasen uygulamanın reddini, kıyas yasağını getirmektedir. Diğer bir bakış açısı ise, kanun yapıcının gerçek düşüncesinin araştırılmasını, kanunun yürürlüğe konulduğu andaki durumun gözetilmesi yani öznel/sübjektif/tarihsel yorumun gerekçesi olarak kullanılması şeklindedir (Yongalık, 2011, s.9). Bu yorumdaki esas alınan ölçüt yasa koyucunun tarihsel iradesidir. Serozan (2015, s.102), bu yaklaşımı artık terk edilmiş bir kavram hukukçuluğu olarak değerlendirerek yasa koyucunun iradesini yorumlanacak bir vasiyetname olarak tanımlar.

İstisnalar dar yorumlanır ilkesine yönelik yaklaşımlardan biri istisna getiren düzenlemelerin kıyasen uygulanamayacağı yaklaşımıdır. Türk hukukunda kabul

edilen görüşün de istisna hükümlerinin kıyasen uygulanamayacağına ilişkin olsa da bu kurala ilişkin genel bir düzenlemeye mevzuatta yer verilmemiştir.

İstisnaların dar yorumlanacağı ve kıyasen uygulanamayacağı kolaylıkla ifade edilen bir kural olsa da, pratikte uygulanması zorluklar barındırabilmektedir. Bu nedenle her somut olay açısından değerlendirme yapılırken geniş veya dar yorumlanması veya kıyasen uygulanma(ma)sına ilişkin gerekçelerin ortaya konularak hareket edilmesi uygun olacaktır.

Diğer taraftan bu ilkenin temel hak ve özgürlükler bağlamında özellikle değerlendirilmesi elzemdir. Temel hak ve özgürlüklere ilişkin düzenlemeler insan haklarının korunması ilkesi gereği ve uluslararası düzenlemelerde yer alan yaklaşımlar ile geniş bir yelpazede ele alınmakta, bu hakların insan yaşamının temeli olduğu düşüncesi ile sınırlayıcı unsurların bu haklara uygulanmasından genel olarak kaçınılmaktadır. Dolayısıyla temel hak ve özgürlüklere ilişkin sınırlamaların ve istisnaların da dar yorumlanması ilkesi benimsenmektedir.

Avrupa İnsan Hakları Sözleşmesinde (AİHS) temel hak ve özgürlüklerin yorumu geniş tutulurken bunlara getirilen istisnalara ise dar yorum metodu uygulanmaktadır. Bu kapsamda, AİHS sisteminde istisnaların dar yorumlanması ilkesi, sınırlanabilen haklar açısından geçerlidir. Diğer bir ifadeyle, kölelik, işkence ve kötü muamele yasağı gibi mutlak haklar sınırlamaya tabi değildir. Bununla beraber Sözleşme metninde düzenlenmeyen içtihatlarla gelişen hakların sınırlanma durumu söz konusu olabileceğinden bu haklara getirilen istisna halleri de dar yoruma tabi olacaktır (Kılınç, 2020, s.600-603).

Kişisel verilerin korunması hakkı açısından değerlendirildiğinde; AİHS'de bu hak açıkça düzenlenmemiş olmakla birlikte geliştirilen içtihatlarla Sözleşmenin 8 inci maddesinde bulunan özel hayata saygı hakkı kapsamında koruma altına alınmıştır. Bu çerçevede Sözleşmenin 8 inci maddesi;

1. *Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.*

2. *Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir."*

şeklinde düzenlenmiştir. Dolayısıyla ikinci fikrada yer alan hususlar özel hayatın korunması hakkına ilişkin getirilen sınırlamalar olarak görülmekle birlikte, söz konusu haller değerlendirilirken dar yorum metodunun uygulandığı çeşitli AİHM kararlarında görülecektir (Klaas vd. v. Almanya, 1978; Rotaru v. Romanya, 2000; Funke v. Fransa, 1992). İstisna hükmü Sözleşme tarafından güvenceye kavuşturulan haklara sınırlama getirdiğinden uygulama alanının da kesin bir şekilde çizilmesi gerekir. Bu anlamda AİHM istisna yorumunu dikkatle geliştirerek dar bir yaklaşım benimsemiştir (Roagna, 2012, s.36).

Kişisel verilerin korunması hakkı, AİHS'in 8 inci maddesi kapsamında korumaya alınan; özel hayat, aile yaşamı, konut ve haberleşmeye saygı gösterilmesini de kapsamına dahil eden ve bu hakkın sınırlandırılması noktasında belirli koşulları ortaya koyan özel hayatın gizliliği hakkının bir parçasıdır (Avrupa Konseyi, "Convention for the Protection of Human Rights and Fundamental Freedoms", Londra, CETS 005). Bununla birlikte özel hayatın gizliliği hakkının ifade özgürlüğü, bilim ve sanat özgürlüğü, bilgi edinme hakkı gibi hak ve özgürlüklerle karşı karşıya gelmesi durumunda diğer hakların korunmasını tehlikeye sokabileceğinde mutlak bir hak niteliğinde değildir. Dolayısıyla AİHM, kararlarında hakların karşılıklı hale gelmesi durumunda bu haklar arasında denge testi yapma yoluna gitmektedir.

ULUSAL DÜZENLEMELERDE KİŞİSEL VERİLERİN KORUNMASI HAKKINA İLİŞKİN İSTİSNAİ HALLER

Türkiye Cumhuriyeti Anayasasında temel hak ve özgürlükler arasında "özel hayatın gizliliği hakkı" Anayasanın 20 nci maddesinde yer bulmuştur. Teklifin genel gerekçesinde, geçen süreçte toplumsal ihtiyaçların karşılanmasını sağlamak amacıyla ve beklentilerin yerine getirilmesi için yeni düzenlemeler yapılması zorunluluğu ile karşı karşıya kalındığı ifade edilmiştir (TBMM, 2010, s. 1271). Bu anlamda, 2010 yılında hayata geçirilen Anayasa değişikliği ile 20 nci maddeye fikra eklenmiş ve kişisel verilerin korunması hakkı, "özel hayatın gizliliği ve korunması hakkı" başlığı altında Anayasal nitelikte güvenceye kavuşmuştur. Anılan maddeye ilişkin 5982 sayılı Kanunla yapılan değişiklik teklifinin gerekçesinde; Anayasada kişisel verilerin korunmasına ilişkin dolaylı nitelikte hükümler bulunsa da bu hükümlerin yeterli olmadığı, karşılaştırmalı hukukta ve taraf olunan uluslararası dokümanlarda kişisel verilerin korunması hakkının öneminin vurgulandığına dikkat çekilmiştir. Aynı zamanda gerekçede, kişilerin, kendileriyle ilgili kişisel verileri üzerinde sahip olduğu hak ve yetkilere ve kişisel verilerinin işlenebileceği haller hükme bağlanırken, kişisel verilerin korunmasına dair usul ve esasların kanunla düzenleneceğinin öngörüldüğü ifade edilmiştir (Yılmazoğlu ve Perdecioğlu, 2019, s.139).

Bu kapsamda hazırlanan *"Kişisel Verilerin Korunması Kanunu Tasarısı"* 26 Aralık 2014 tarihinde TBMM Başkanlığına sunulmuş olup Tasarı 24 Mart 2016 tarihinde kabul edilmiş ve kanunlaşmıştır. Ardından *"6698 sayılı Kişisel Verilerin Korunması Kanunu"* 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

Bu çerçevede çalışmanın bu bölümünde; Anayasa ve uluslararası belgeler ve ilgili mahkeme kararları çerçevesinde, ulusal hukukta kişisel verilerin korunması hakkının sınırlandırılmasına ilişkin hükümlerin nasıl ele alındığı, hangi menfaat ve değer veya amaç için kişisel verilerin korunması hakkının sınırlandırılması yoluna gidildiği hususları ele alınacaktır.

ANAYASA ÇERÇEVESİNDE KİŞİSEL VERİLERİN KORUNMASI HAKKININ SINIRLANDIRILMASI

6698 sayılı Kanun hükümleri açısından kişisel verilerin korunması hakkına getirilen sınırlandırmalara ilişkin değerlendirmelere yer vermeden önce söz konusu hakkın Anayasanın 20 nci maddesinde, "Özel hayatın gizliliği başlığı" altında düzenlenen kişisel verilerin korunmasını isteme hakkının temel bir hak olduğuna dikkat çekmek gerekir.

Kişisel verilerin korunması hakkı kişilere dair verilerin işlenmesinde temel hak ve özgürlüklerini korumasının yanı sıra özellikle bireylerin kendi kişisel verileri üzerinde karar verme özgürlüğünü de korumaktadır (Şimşek, 2008, s.119). Ayrıca hukuka aykırı olarak kişisel verilerin işlenmesi, Anayasanın 17 inci maddesi ile güvenceye alınan kişi dokunulmazlığı, kişinin maddi ve manevi varlığını koruma ve geliştirme hakkının ihlali anlamına da gelmektedir (Kişisel Verileri Koruma Kurumu, 2019, s. 30).

AHİM kararları dikkate alındığında bir gerçek kişinin kişisel verilerinin işlenmesi halinde bireyin kişisel verilerinin korunması hakkının doğrudan sınırlandırıldığını, üst başlık olarak ise özel hayatın gizliliği hakkına müdahale teşkil ettiğini ifade etmek yanlış olmayacaktır (Benzer değerlendirmeler için bkz. S. and Marper v. UK, 2008, par. 67; Leander v. İsveç, 1987, par.48; ABAD, Birleştirilmiş davalar C-293/12 ve C-594/12, Digital Rights Ireland, par. 34-36; Ayrıca bkz. Birleştirilmiş davalar C-92/09 ve C-93/09 Volker und Markus Schecke, 2010, par. 58). Ancak ilgili kişinin özel hayatın gizliliği hakkına müdahale edilmesi durumu, kişisel verinin işlenmesine ilişkin düzenlemeler açısından gerekli hal ve şartları sağlıyorsa müdahalenin hukuka uygun olduğu kanaatine varılabilecektir.

Anayasanın 20 nci maddesinde özel hayatın gizliliği hakkı güvence altına alınmış ve anılan maddede; herkesin *"kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı"*na sahip olduğu, bu hakkın;

> *"kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi"*

kapsadığı, son olarak kişisel verilerin "ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla" işlenebileceği ile "kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla" düzenleneceği belirtilmiştir. Bununla birlikte bu hakka ilişkin özel sınırlama sebeplerine anılan maddede yer verilmemiştir. Ancak kişisel verilerin korunması hakkının ihlaline neden olunmaması için veri işleme faaliyetinin "Temel hak ve özgürlüklerin sınırlandırılması" başlıklı Anayasa'nın 13 üncü maddesine uygun olarak gerçekleştirilmesi gerekecektir.

Anayasanın 13 üncü maddesine göre;

> *"Temel hak ve hürriyetler özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."*

Belirtmek gerekir ki, temel hakların sınırlandırılmasına ilişkin olarak Anayasanın 13 üncü maddesinde 3/10/2001 tarihli ve 4709 sayılı Kanun'la getirilen değişiklikle, AİHS'nde hakların sınırlandırılmasına ilişkin ilkelere paralel olacak şekilde düzenlenme yapılması gerekçesi ile son halini almıştır (Yılmazoğlu vd., 2019, s.69).

Bu bağlamda Anayasa Mahkemesi (AYM) özel hayatın gizliliğinin ihlal edildiğine ilişkin yaptığı incelemelerde belirli bir yöntem geliştirmiştir. Şöyle ki öncelikle, somut olaydaki menfaatin, bu hakkın kapsamına girip girmediği tespitinde bulunulur. İkinci olarak ise hakkın kapsamı dahilinde olan menfaate yönelik bir müdahalenin varlığı araştırılır. Müdahalenin mevcut olduğunun tespiti halinde bu durumun Anayasa'nın 20 nci ve 13 üncü maddesinde düzenlenen şartlara uygun olup olmadığı incelenir. Bu çerçevede, ikinci aşamada müdahalenin kanuni gerekçesinin varlığı, 20 nci maddede belirtilen sınırlama sebeplerinden en az birinin söz konusu olup olmadığı, aynı zamanda 13 üncü maddede yer verilen;

> *"hakkın özüne dokunmama", "demokratik toplum düzeninin gereklerine uygun olma" ve "ölçülülük"*

ilkelerine uyulup uyulmadığı değerlendirilerek inceleme sonuçlandırılır. (AYM, 2014 (a), par. 53).

Dolayısıyla 6698 sayılı Kanun hükümleri söz konusu olmaması halinde de ilgili kişilerin verileri üzerindeki hakimiyeti, hukukun gözetmediği tamamen korumasız bir alana bırakılmamaktadır. Bu anlamda kişisel verilerin korunması hakkının sınırlandırılması *"hakkın özüne dokunmaksızın"* ve *"ancak kanunla"* mümkün olabilmektedir ve aynı zamanda *"Anayasanın sözü ve ruhu", "demokratik toplum düzeninin ve lâik Cumhuriyetin gerekleri"* ve *"ölçülülük"* ilkesi temel ölçütler olarak gözetilmeye devam edilecektir.

Ek olarak Anayasa'nın 13 üncü maddesinde temel hak ve özgürlüklerin sadece Anayasa'nın ilgili maddelerindeki nedenlere bağlı olarak sınırlandırılabileceği ifade edilmiştir. Fakat Anayasa'nın 20 nci maddesinde kişisel verilerin korunmasını isteme hakkına dair sınırlama ve müdahale edilmesi açısından özel bir sınırlama nedenine yer verilmemiştir. Bununla beraber Anayasa Mahkemesinin yerleşik olan içtihadına göre; *"özel sınırlama nedeni öngörülmemiş hak ve özgürlüklerin de o hak ve özgürlüğün doğasından kaynaklanan bazı sınırları"* bulunabilmektedir. Aynı zamanda belirtmek gerekir ki Devletin; *"kişilerin özel ve aile hayatına keyfi olarak müdahale etmemek ve üçüncü kişilerin haksız saldırılarını önlemek"* (AYM, 2014 (a), par. 53) yükümlülüğü de söz konusudur. Buna ek olarak Anayasa Mahkemesi kararlarında, Anayasa'nın diğer maddelerinde düzenlenen hak ve özgürlükler ve devlete yüklenen ödevler açısından bu durumların özel sınırlama nedeni gösterilmemiş olan hak ve özgürlüklere sınır teşkil edebileceğine dair ifadeleri söz konusudur (AYM, 2020 par. 135. Ayrıca bkz. AYM, 2015.) Bu çerçevede Anayasa Mahkemesi bir kararında özel sınırlama nedeni gösterilmemiş olan hak ve özgürlüklerin sınırına ilişkin olarak aşağıdaki tespitlerde bulunmuştur: (AYM, 2020 par. 136).

> *"Anayasa'nın 20. maddesinin üçüncü fıkrasındaki düzenlemelerden kişisel verilerin korunmasını isteme hakkına sınırlama getirilebileceği anlaşılmaktadır. Ancak fıkrada tüketici sayıda bir sebepler ya da meşru amaçlar listesine yer verilmemiştir. Kimliği belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgileri ifade eden kişisel veri kavramının kullanım alanlarının oldukça geniş olması nedeniyle her bir kullanım alanı yönünden farklı sınırlama sebeplerinin ya da meşru amaçların kabul edilmesi kaçınılmazdır. Bu durumda hangi alanda kişisel verilerin korunmasını isteme hakkına yönelik sınırlama getirildiği ya da müdahale edildiğine bağlı olarak sınırlama nedeni ya da meşru amaç değişebilir. Buna göre yapılacak incelemede kişisel verilerin korunmasını isteme hakkının bu hakkın doğasından kaynaklanan bazı sınırlarının bulunduğu dikkate alındığında her dosya ve başvuru kapsamında işin doğasından kaynaklanan sınırlama sebebinin tespit edilmesi ve bunun meşru bir sebep olarak kabul edilip edilemeyeceğinin değerlendirilmesi gerekir. Öte yandan Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin de bu hakka sınır teşkil edebileceği kabul edilmelidir."*

<u>Kanunla sınırlandırılma:</u> Anayasa Mahkemesi kararlarında kanunilik ölçütünü hukuki güvenliğin teminatı olarak değerlendirmektedir. Kanunun şeklen var olması, temel hak ve özgürlüğün sınırlandırılması için yeterli değildir. Bu kapsamda Anayasa Mahkemesi ilgili düzenlemenin keyfiliğe yol açmayacak şekilde, ilgili makama verilen yetkinin sınırlarının ve uygulanmasının belirsiz olmamasını, yetkilerin yeterli düzeyde ve netlikte belirlenmesi gerektiğini zorunlu görmektedir (AYM, 2015, par. 62). Başka bir ifadeyle, AYM hakkın sınırlandırılmasına yönelik kanunun şekli varlığının yanı sıra düzenlemelerin keyfiliğe yol açmayacak şekilde belirli, öngörülebilir ve ulaşılabilir olması gerektiğini vurgulamaktadır (AYM, 2014 (b), par. 89; AYM, 2015, par.62; AYM, 2020 par. 118). Bunun yanı sıra Anayasa'nın 20 nci maddesinin üçüncü fıkrasında;

> *"kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla"* ve *"kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenlenir."*

hükmü yer almaktadır.

Diğer taraftan Anayasa'nın 2 nci maddesinde bulunan hukuk devleti ilkesinin gereği olarak da kanunun niteliği, kanunilik koşulunun sağlanmasının tespit edilmesinde önem arz eder. Nitekim belirlilik ve hukuki güvenlik ilkeleri hukuk devletinin ön koşuludur. Bu anlamda hukuki güvenlik ilkesi hukuki düzenlemelerin öngörülebilir olmasını, kişilerin işlem ve eylemlerinde devlete güven duyulmasını sağlar (AYM, E.2013/39, K.2013/65, 22/5/2013; AYM, E.2014/183, K.2015/122, 30/12/2015, par.5; AYM, 2020, par. 120).

AİHM açısından, kişisel verilerin korunması hakkının 'kanunla sınırlandırılması' ölçütü, ulusal hukuktaki düzenlemelerin AİHS'nin 8 inci maddesinde yer alan güvencelere uygun şekilde kişisel verilerin korunması hakkına ilişkin yeterli güvencelerin sağlanmasını da ifade etmektedir. Bu kapsamda AİHM içtihatları uyarınca ulusal hukuk, kişisel verilerin saklanma amacına uygun şekilde ve amaca uygun gerekli olan süre kadar, yalnızca gerekli olan verilerin muhafaza edilmesini sağlaması gerekir. Ek olarak ulusal hukuk düzenlemesinin, kişisel verilere keyfi ve yetkisiz erişimi engellemek adına uygun önlemleri de içermesi gerekecektir (S. and Marper v. United Kingdom, 2008, par. 103; M.M. v. United Kingdom, 2012, par. 195).

Bu çerçevede 6698 sayılı Kanunun 28 nci maddesi değerlendirildiğinde anılan maddede yer alan hallerin hakkın Kanunla sınırlandırılması ölçütünü yerine getirdiği ifade edilebilir. Ancak bu sınırlama yapılırken temel bir hakkın sınırlandırılmasına dair ölçütleri ortaya koyan Anayasa'nın 13 üncü maddesine de uygun olması gerekir. Dolayısıyla kişisel verilerin korunması hakkı, yalnızca kanunla ve *"demokratik bir toplumda gerekli"* olduğu ölçüde, ayrıca getirilen sınırlama ile *"hakkın özüne dokunulmaksızın"* ve *"Anayasa'nın sözüne ve ruhuna", "demokratik toplum düzeninin gerekliliklerine"* ve *"ölçülülük"* ilkesine aykırı olmamalıdır.

Demokratik Toplum Düzeninin Gereklerine Uygunluk ve Ölçülülük: Anayasa Mahkemesi yerleşik olan içtihatlarında "demokratik toplum"u:

> *"Demokrasiler, temel hak ve özgürlüklerin en geniş ölçüde sağlanıp güvence altına alındığı rejimlerdir. Temel hak ve özgürlüklerin özüne dokunup tümüyle kullanılamaz hale getiren sınırlamalar, demokratik toplum düzeni gerekleriyle uyum içinde sayılamaz. Bu nedenle, temel hak ve özgürlükler, istisnaî olarak ve ancak özüne dokunmamak koşuluyla demokratik toplum düzeninin sürekliliği için zorunlu olduğu ölçüde ve ancak yasayla sınırlandırılabilirler."*

şeklinde betimlemiştir. Bir başka ifadeyle, yapılan müdahale ile hak veya özgürlüğün özüne dokunarak, kullanılmasına engel oluyorsa ya da hakkın kullanımını tamamen güçleştiriyor ve etkisinin bulunmaması haline getiriyorsa aynı zamanda ölçülülük ilkesine aykırı şekilde sınırlamanın amacı ve aracı arasındaki denge gözetilmiyorsa demokratik bir toplumun düzenine aykırılığı söz konusu olacaktır. (AYM, 2004, par. 34. Ayrıca bkz. AYM, E.2006/142, K.2008/148, K.T. 24/9/2008; E.2009/59, K.2011/69, K.T. 28/4/2011; E.2006/142, K.2008/148, K.T. 17/4/2008).

Bu anlamda temel hak ve özgürlüklere ilişkin bir müdahalenin, *"demokratik toplum düzeninin gereklerine uygun"* olarak görülebilmesi için bu müdahalenin zorunlu bir "toplumsal ihtiyaç"ı karşılaması ve ölçülü olması gereklidir. Anayasa'nın 13 üncü maddesinde *"demokratik toplum düzeninin gereklerine aykırı olmama ve ölçülülük ilkesine aykırı olmama"* biçiminde iki ayrı ölçüte yer verilse de iki kriter arasında bütünleşik bir ilişki söz konusudur. Daha açık bir ifadeyle hakka yapılan sınırlamanın amacı ile bu amacı gerçekleştirmek için kullanılan araç arasındaki ilişki ölçülülük ilkesi çerçevesinde şekillenmektedir (AYM, 2020 par. 139, AYM 2018, par. 45).

Ölçülülük ilkesi; "gereklilik", "elverişlilik" ve "orantılılık" olmak üzere üç alt ilkeden oluşmaktadır. Bu çerçevede temel bir hakka yapılan müdahalenin zorunlu olarak toplumsal bir ihtiyacı karşıladığının kabulü için uygulanacak önlemin

amacın sağlanmasına yönelik elverişli ve uygulanabilecek en hafif tedbir olması gerekmektedir. Dolayısıyla hedeflenen amaca dair açık bir şekilde ağır olan bir müdahale; ulaşılmak istenen amaç ile uygulanacak önlem arasında dengesizliğe neden olacağından bu durum orantısız bir müdahale anlamına gelecektir.

Bununla birlikte Anayasa Mahkemesi değerlendirmelerinde kişisel verilerin korunması hakkına ilişkin müdahalelerin "demokratik toplum düzeninin gereklerine uygun" olması için zorunlu bir toplumsal ihtiyacı karşılamasının yeterli olmayacağına da dikkat çekmekte olup Mahkeme, kararında; Anayasa'nın 20 nci maddesinin üçüncü fıkrasında;

> *"Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar."*

denilmesi suretiyle kişisel verilerin korunması hakkına getirilen sınırlamalar açısından ayrıca özel bir takım güvencelere yer verildiği, bunları kişisel verilerin korunması hakkına ilişkin müdahalelerin;

> *"demokratik bir toplum düzeninin gereklerine uygun olabilmesi için Anayasa koyucu tarafından özel olarak belirlenmiş güvenceler"*

mahiyetinde olduğu şeklinde tarif etmiştir (AYM, 2020 par. 142).

Buna ek olarak Anayasa'nın 20 nci maddesinin üçüncü fıkrasındaki kişisel verilerin korunması hakkına dair genel hüküm ile birlikte devam eden cümledeki "... de kapsar" ifadesi çerçevesinde güvencelerin sayılarak tüketilmemiş olması dikkate alınarak Anayasa'nın 13 üncü maddesindeki sınırlama ölçütlerinden demokratik toplum düzeninin gereklerine uygunluk ölçütü kapsamında değerlendirme yapılırken uluslararası belgelerde ve karşılaştırmalı hukuk metinlerinde yer alan ilkeler açısından da her olayın somut koşullara uygun olduğu ölçüde değerlendirmeye alınabileceği sonucuna ulaşılmıştır (AYM, 2020, par. 143). Bu açıdan kişisel verilerin korunması hakkına kamunun müdahalesi halinde belirtilen ek güvencelerin bir kısmının ya da tamamının sağlanması gerektiği vurgulanmıştır (AYM, 2020, par. 114).

Sonuç olarak kişisel verilerin korunması hakkına meşru bir amaç kapsamında kanunla sınırlama getirilmesi halinde özel güvencelere de istisna getirilebilecektir. Ancak böyle bir durumda dahi Anayasa'nın 13 üncü maddesinde tüm temel hak ve özgürlükler yönünden öngörülmüş olan müdahale ölçütlerinin asgari standart-

larına uyulması elzemdir. Başka bir ifadeyle istisna durumları bulunsa dahi sınırlama kanuna dayanmalı, kanun sınırlama nedenlerini barındırmalı veya meşru bir amacı gözetmeli ve demokratik toplum düzeninin gereği olarak zorunlu bir toplumsal ihtiyacı karşılamalı ve ölçülülük ilkesi çerçevesinde değerlendirilmelidir. Bununla beraber bir istisna durumunun varlığı özel güvencelerin tamamının direkt olarak ortadan kalkmasının bir nedeni olmamakla beraber böyle bir istisna halinin varlığı durumunda somut olayın niteliği dikkate alınarak her bir güvence yönünden istisna getirilmesinin zorunlu olup olmadığı da değerlendirilmelidir (AYM, 2020 par. 145).

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA İSTİSNAİ HALLER

Hukuki düzenlemelerde açıkça istisna halinin düzenlemesinin yanı sıra temel bir belgenin kapsam maddesi, o belgenin kapsam dışı bıraktığı alanlara da işaret edeceğinden kapsam dışında kalan durumlar da bir hakka getirilen diğer sınırlama durumu olarak değerlendirilmesi gerekir. Dolayısıyla 6698 sayılı Kanunda kişisel verilerin korunması hakkının açıkça sınırlandığını belirten 28 inci maddenin değerlendirilmesinden önce 6698 sayılı Kanunun kişi, konu, yer, zaman ve yöntem açısından uygulanma alanları ele alınacaktır.

6698 sayılı Kanunun Kapsamı ve Uygulanması

6698 sayılı Kanunun amacı; *"kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek"* olarak belirlenmiştir. Bu amaç çerçevesinde kişisel veri işleyen tüm gerçek ve tüzel kişiler kamu ve özel sektör arasında ayrım gözetmeksizin 6698 sayılı Kanunun hükümlerine uymak ve gerektirdiği yükümlülükleri yerine getirmek zorundadır.

6698 Sayılı Kanunun Kişi Bakımından Uygulanması

6698 sayılı Kanunun "Amaç" başlıklı 1 inci maddesinde, Kanunun amacı kişisel verilerin işlenmesinde uyulacak usul ve esasları belirlemek olduğu ifade edilmiştir. Kanunun "Tanımlar" başlıklı 3 üncü maddesinde de kişisel veri; *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmıştır. Dolayısıyla 6698 sayılı Kanun ile yalnızca gerçek kişilere ilişkin verilerin korunması söz konusu olup tüzel kişilere ilişkin veriler Kanun korumasından yararlanamamaktadır. Ancak, tüzel kişiye ait bir veri aracılığıyla gerçek kişinin belirlenmesi

ya da kişiye ulaşılması söz konusu ise bu veriler de yine gerçek kişiye ilişkin olması ve gerçek kişinin hakkının korunması bakımından Kanunun uygulama alanına girecektir (Kişisel Verileri Koruma Kurumu, 2019, s.37).

Diğer taraftan Kanun, kişisel veri işleme faaliyetinde bulunan kişileri gerçek ve tüzel kişi olmakla sınırlandırmakla birlikte kamu ve özel sektör arasında bir ayrıma gitmemiştir. Dolayısıyla her iki alanda da gerçekleştirilen kişisel veri işleme faaliyetleri açısından bireylerin kişisel verileri koruma altına alınmış olup 6698 sayılı Kanun ile, kamu sektörü karşısında da kişilerin korunması için usul ve esaslar belirlenmiştir.

6698 Sayılı Kanunun Yöntem Bakımından Uygulanması

6698 sayılı Kanunun "Kapsam" başlıklı 2 nci maddesinde;

> *"Kanun hükümlerinin, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında"*

uygulanabileceği belirtilmiştir. Dolayısıyla, Kanunun kapsamında bulunan kişisel veriler tamamen veya kısmen otomatik olan yöntemlerle işlenmesi veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerle işlenmesi gerekir. Sonuç olarak hem bir veri kayıt sistemine dahil olmama hem de otomatik olmayan yollarla işlemenin söz konusu olması halinde, bu kişisel veriler Kanun kapsamına girmemektedir.

6698 Sayılı Kanunun Konu Bakımından Uygulanması

6698 sayılı Kanun, temel itibariyle kişisel verileri ihlal edilen ilgili kişilerin sahip olduğu haklar ve hak arama yöntemlerine ayrıca veri sorumlularının kişisel veri işleme faaliyetinde bulunurken yerine getirmesi gereken yükümlülüklerine ilişkin hükümlere yer verilmektedir. Bunlara ek olarak kişisel verilere dair işlenen suçlar açısından; Kanunun 17 nci maddesi ile; kişisel verilere ilişkin suçlar bakımından 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı maddelerinin, Kanunun 7 nci maddesinde yer alan hükme aykırı olarak kişisel verileri silmeyen veya anonim hâle getirmeyenler bakımından ise Türk Ceza Kanununun 138 inci maddesinin uygulanacağı ifade edilmektedir. Bu anlamda veri sorumlusu sıfatını haiz olmayan kişiler tarafından kişisel verilere ilişkin bir suç işlenmesi halinde kanun kapsamında bir yaptırım uygulanma imkanı bulunmasa da Türk

Ceza Kanunu çerçevesinde kişisel verilerin korunması hakkı ayrıca korunmaya devam edecektir.

6698 Sayılı Kanunun Yer Bakımından Uygulanması

Kanunun yer bakımından uygulanmasına ilişkin olarak 6698 sayılı Kanunda açık bir hüküm bulunmaktadır. Bu anlamda Kanunun 18 inci maddesinde düzenlenen "Kabahatler" maddesi açısından değerlendirme yapılması uygun olacaktır. Bahse konu maddede Kanun 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünün yerine getirmeyenler, 2 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler, 15 inci madde uyarınca Kurul tarafından verilen kararları yerine getirmeyenler ve 16 ncı maddede öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında idari para cezası verileceği hüküm altına alınmıştır. Dolayısıyla Kurul değerlendirme sonucunda verdiği kararların açısından Kabahatler Kanunu uygulanacaktır.

Bu çerçevede Kabahatler Kanunun "Yer bakımından uygulama" başlıklı 6 ncı maddesinde *"5237 sayılı Türk Ceza Kanununun yer bakımından uygulamaya ilişkin 8 inci maddesi hükümleri, kabahatler bakımından da uygulanır. Ancak, kanunlarda aksine hüküm bulunan haller saklıdır."* hükmü yer almaktadır. Atıf yapılan 5237 sayılı Kanun 8 inci maddesine bakıldığında;

"(1) Türkiye'de işlenen suçlar hakkında Türk kanunları uygulanır. Fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde suç, Türkiye'de işlenmiş sayılır.

(2) Suç;

a) Türk kara ve hava sahaları ile Türk karasularında,

b) Açık denizde ve bunun üzerindeki hava sahasında, Türk deniz ve hava araçlarında veya bu araçlarla,

c) Türk deniz ve hava savaş araçlarında veya bu araçlarla,

d) Türkiye'nin kıt'a sahanlığında veya münhasır ekonomik bölgesinde tesis edilmiş sabit platformlarda veya bunlara karşı,

işlendiğinde Türkiye'de işlenmiş sayılır."

maddesi yer almaktadır. Bu anlamda 6698 sayılı Kanunda düzenlenen kabahatler açısından Kabahatler Kanunun atfi dolayısıyla Türk Ceza Kanunun 8 inci maddesinin uygulanması uygun olacaktır.

6698 Sayılı Kanunun Zaman Bakımından Uygulanması

6698 sayılı Kanunun Geçici 1 inci maddesinin üçüncü fikrasında, Kanunun yayımlanmasın önce işlenmiş olan kişisel verilere dair hükme yer verilmiştir. Anılan hükme göre;

"Bu Kanunun yayımı tarihinden önce işlenmiş olan kişisel veriler, yayımı tarihinden itibaren iki yıl içinde bu Kanun hükümlerine uygun hâle getirilir. Bu Kanun hükümlerine aykırı olduğu tespit edilen kişisel veriler derhâl silinir, yok edilir veya anonim hâle getirilir. Ancak bu Kanunun yayımı tarihinden önce hukuka uygun olarak alınmış rızalar, bir yıl içinde aksine bir irade beyanında bulunulmaması hâlinde, bu Kanuna uygun kabul edilir."

Bu itibarla, 6698 sayılı Kanunun yayımı tarihinden önce yürürlükte bulunan mevzuat kapsamında kişisel veriler işlenirken hukuka uygun olarak kişilerden alınmış rızalar, ilgili kişilerce aksi bir beyanda bulunulmadığı sürece yukarıda alıntılanan madde uyarınca Kanuna uygun olduğu kabul edilmiştir. Diğer bir ifadeyle veri sorumlularınca bu şartlar kapsamında alınmış mevcut rızaların Kanunun yayımı sonrasında yeniden alınması veya güncellenmesine gerek kalmamıştır. Ancak ilgili kişiler tarafından Kanunun yayımı tarihinden itibaren bir yıl içerisinde aksine bir irade beyanında bulunulması söz konusu ise bu durumda kişisel verilerin silinmesi veya yok edilmesi gerekmiştir.

6698 Sayılı Kanunun 28 inci Maddesi

6698 sayılı Kanunun 28 inci maddesinde kişisel veri işleme faaliyetinde bulunan veri sorumlularına getirilen yükümlülüklerden ve ilgili kişilerin haklarından istisna tutulan haller düzenlenmiştir. Kanun hükümlerinin ayrım gözetmeksizin uygulanmayacağı haller Kanunun 28 inci maddesinin 1 inci fikrasında, Kanun hükümlerinin kısmen uygulanmayacağı haller ise aynı maddenin 2 nci fikrasında sayılarak belirlenmiştir. Bu çerçevede bahse konu 28 inci maddede sayılan istisna durumlarının ne olduğu ve yorumlanmasına ilişkin açıklamalara yer verilecektir.

6698 sayılı Kanunun "İstisnalar" başlıklı 28 inci maddesinin ilk fikrasında Kanundan istisna tutulan durumlar sayılmak suretiyle belirlenmiştir. Kanunun 28 inci maddesinin ilk fikrasında sayılan hallerde Kanun hükümlerinin bütün

olarak uygulanmayacağı düzenlenmiştir. Bu durumları "tam istisna" olarak nitelendirmek mümkündür. Anılan maddenin ikinci fıkrasında ise belirli koşullar altında Kanunun bazı hükümlerinin uygulanmayacağı durumlar belirlenmiştir. Dolayısıyla belirli hükümlerin uygulanmama durumu söz konusu olduğunda bu durumlar da "kısmen istisna" olarak nitelendirilebilmektedir.

Diğer taraftan somut olayların, Kanunun 28 inci maddesi kapsamına girip girmediği değerlendirilirken öncelikle bahse konu olaydaki verinin, kişisel veri niteliğinde olup olmadığının tespit edilmesi gerekecektir. Diğer bir ifadeyle somut olayda kişisel veri niteliğinin haiz olmaması durumunda Kanunun 28 inci maddesi kapsamında değerlendirmeye gerek kalmaksızın direkt olarak 6698 sayılı Kanun kapsamı dışında bulunmaktadır. Bu anlamda, Kanunun 28 inci maddesi çerçevesinde Kanunun tamamından veya belirli hükümleri açısından kapsam dışında kalan verilerin yalnızca "kişisel veri" olduğu tespit edilen veriler açısından geçerli olduğunun belirtilmesi yerinde olacaktır.

Tam İstisna Halleri

6698 sayılı Kanunun 28 inci maddesinin birinci fıkrasına Kanunun uygulanmayacağı istisna halleri düzenlenmiştir. Bu hükme göre, aşağıdaki başlıklarla yer verilen durumlar tam istisna kapsamına girmekte olup bu haller bakımından Kanun hükümleri uygulanmayacaktır.

Kişisel Verilerin, Üçüncü Kişilere Verilmemek ve Veri Güvenliğine İlişkin Yükümlülüklere Uyulmak Kaydıyla Gerçek Kişiler Tarafından Tamamen Kendisiyle veya Aynı Konutta Yaşayan Aile Fertleriyle İlgili Faaliyetler Kapsamında İşlenmesi

6698 sayılı Kanunun 28 inci maddesi uyarınca;

> *"kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi"*

halinde Kanun hükümleri uygulama alanı bulamayacaktır. Söz konusu madde çerçevesinde belirtilen Kanundan istisna halinin, sadece kişilerin özel veya aile hayatları içerisinde gerçekleştirilen faaliyetlere ilişkin olarak ve dar yorumlanması gerekir. Bununla birlikte söz konusu madde yorumlanırken 108+ sayılı sözleşmede belirtilen Sözleşmenin, bir gerçek kişi tarafından, "tamamen kişisel veya ev içindeki faaliyetler sırasında gerçekleştirilen kişisel veri işleme faaliyetlerine

uygulanmayacağı" maddesi çerçevesinde Avrupa Konseyi tarafından yayımlanan 108+ sayılı sözleşmeye dair açıklayıcı raporda belirtilen hususların dikkate alınması da uygun olacaktır. Buna göre ilgili raporda da belirtildiği söz konusu madde ile de genel olarak kişilere, kendilerine ait özel alanlarda ve özel hayatlarındaki faaliyetlerine ilişkin verilerin işlenmesi halinde uygun olmayan yükümlülüklerden sorumlu tutulmanın önlemeyi amaçlandığı yorumu yerinde olacaktır (Avrupa Konseyi, 2018, s.18). Ayrıca bu faaliyetlerin ticari veya mesleki amacı da söz konusu olmamalıdır. Örneğin özel fotoğrafların, yazışmaların bilgisayarda depolanması, aile üyelerine ait iletişim bilgilerinin listesinin oluşturulması gibi kişisel veya aynı konutta yaşayan aile üyeleriyle ilgili kişisel veri işleme faaliyetleri bu madde kapsamında değerlendirilebilecektir.

Diğer taraftan söz konusu madde metninde de ifade edildiği üzere kişinin kendisiyle veya aynı konutta yaşadığı aile üyeleriyle ilgili faaliyetler kapsamında işlenen kişisel veriler, Kanun kapsamı dışında tutulsa da söz konusu işleme faaliyetinde belirli koşulların aranması söz konusu olabilecektir.

Anılan madde gereğince öncelikle, işleme faaliyetinin gerçek kişi tarafından gerçekleştirilmesi gerekmektedir. Örneğin özel bir günde bir araya gelen aile fertlerinden bir kişinin kendine ait fotoğraf makinesi ile aile üyelerini çektiği fotoğraf kapsamındaki işleme faaliyeti, Kanun kapsamında değilken tüzel kişi bünyesinde hizmet veren bir fotoğrafçı ile anlaşılarak fotoğraf çekimi gerçekleştirilmesi halinde ticari bir faaliyetin de söz konusu olduğu göz önüne alındığında bu işleme faaliyeti kanun kapsamına dahil olacaktır.

Madde kapsamında aranan diğer bir koşul, işlenen kişisel verilerin ilgisiz kişilerin eline geçmemesi ve veri güvenliğine ilişkin yükümlülüklere uyulmasıdır. Veri güvenliğine ilişkin yükümlülüklerden kast edilen Kanunun 12 inci maddesinde düzenlenen yükümlülükler söz konusu olabileceği gibi bunların dışındaki güvenlik tedbirleri de olabilecektir.

Aynı konutta yaşayan aile üyeleriyle ilgili veya tamamen kişisel faaliyetler, bireyin özel yaşamı ile yakından ilişkili olan ve başka kişilerin özel ortamını önemli düzeyde etkilemeyen faaliyetler olarak açıklanabilir. Bu anlamda böyle bir ortamda gerçekleşen işleme faaliyetine ilişkin bir gönderinin, örneğin fotoğrafin internet ortamı gibi çok sayıda kişinin erişimine açık bir ortamda paylaşılması halinde kişisel verilerin üçüncü kişilerle paylaşılması ve kişisel verilerin güvenliğine ilişkin önlemlerin alınmaması hali söz konusu olduğundan Kanundan istisna olmayacaktır (Ayrıca bkz. Lindqvist Kararı, 2003, par 47).

İstisna maddesi kapsamında işleme faaliyetinde aranan diğer bir husus;

> *"tamamen kişisel veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında kişisel verilerin işlenmesi"*dir.

Madde lafzi olarak yorumlandığında; aynı konutta yaşamayan aile üyeleri ve aynı konutta yaşayan ancak aile fertlerinden sayılmayanlar bakımından istisna hükmü geçerli olmayacaktır. Bu anlamda aile kavramına yakından bakıldığında;

> *"evlilik veya kan bağına dayanan, karı, koca, çocuklar, kardeşler arasındaki ilişkilerin oluşturduğu birlik"*

olarak tanımlansa da (TDK) AİHM'in içtihadında da (X, Y ve Z v. Birleşik Krallık, 1997) ifade edildiği gibi, AİHS'nin 8 inci maddesinde aile kavramı sadece evlilik kurumuna dayalı ailelerle sınırlı tutulmamakla birlikte, toplumun değişen yapısı dikkate alınarak başka birlikteliklerin de aile kavramına dahil edilmesi mümkün olabilmektedir. Bu anlamda bir ilişki biçiminin aile hayatına kavramına dâhil olup olmadığına karar verilirken, bazı etmenler göz önünde bulundurulabilir, örneğin; ilişkinin uzunluğu, çiftin birlikte yaşaması ve çocuk sahibi olarak veya başka şekilde kişilerin birbirlerine olan bağlılıklarını kanıtlamaları gibi etmenler (Roagna, 2012, s.27). Dolayısıyla aile fertleriyle ilgili kişisel verilerin işlenmesi hususu değerlendirilirken somut olayın kendine özgü özellikleri de dikkate alınarak karar verilmelidir.

6698 sayılı Kanunun referans düzenlemesi (6698 sayılı Kanunun gerekçesinde anılan düzenlemeye atıfta bulunulduğu görülmektedir. Bkz. 6698 sayılı Kanun Tasarısı Genel Gerekçe, 19. madde ve 21. madde gerekçesi) olan 95/46/AT sayılı Yönerge'de konuya ilişkin hükme bakıldığında da "ev içi faaliyet" ifadesinin kullanıldığı görülmektedir. Dolayısıyla söz konusu istisna hükmünün tamamen özel alanda gerçekleşen faaliyetlerle ilgili işlemelerde kişilere gereksiz yükümlülükler yüklenmemesinin hedeflendiği dikkate alınarak hükmün yorumlanması daha doğru bir yaklaşım olacaktır.

Bu anlamda, faaliyetlerin tamamen kişisel veya aynı konutta yaşayan aile üyelerine (ev halkına) ilişkin olup olmadığı somut olaylara göre değerlendirilmesi gerekir. Örneğin bir kişinin ailesinin evinde güvenliğini veya sağlığını korumak amacıyla yerleştirdiği kamera sistemi aracılığıyla kısmen de olsa kamusal bir alanın görüntülenmesi veya kaydedilmesi halinde özel alan dışına yöneltilme hali söz konusu olacağından tamamen kişisel veya aynı konutta yaşayan aile üyelerine (ev halkına) ilişkin bir faaliyetin söz konusu olduğu kabul edilemeyecektir (Bkz., František Ryneš v. Úřad, 2014). Ek olarak belirtmek gerekir ki bu tür tamamen kişisel veya aynı konutta yaşayan aile halkına ilişkin kişisel verilerin işlenmesi için hizmet veren veya aracılık sağlayanların yürüttüğü veri işleme faaliyetleri de istisna hükmü kapsamında bulunmamaktadır (Avrupa Konseyi, 2018, s.18).

Kişisel Verilerin Resmi İstatistik ile Anonim Hâle Getirilmek Suretiyle Araştırma, Planlama ve İstatistik Gibi Amaçlarla İşlenmesi

6698 sayılı Kanun uyarınca;

> *"kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi"*

halinde Kanun maddeleri uygulama alanı bulamayacaktır. Maddede örnekseyici bir sayım olduğundan benzer amaçlarla yapılacak diğer işleme faaliyetlerinin de anonim hâle getirilmek şartıyla istisna kapsamında sayılabileceği anlaşılmaktadır.

Diğer taraftan istisna hükmünde, kişisel verilerin istatistik amacıyla işlenmesi durumu; resmi istatistik ve anonim hâle getirilmek şartıyla istatistik amacıyla işlenmesi bakımından iki ayrı şekilde karşılık bulmuştur.

Resmi İstatistik Amacıyla Veri İşleme Hali

Bu durum 'resmi' yani devlet bünyesindeki kamu kurumu tarafından istatistik amacıyla işlenen verileri kapsamaktadır. Ülkemizde ihtiyaç duyulan alanlarda verilerin derlenmesini, gerekli istatistiklerin oluşturulmasını, bu istatistiklerin yayımlanmasını yapmakla görevli olan Türkiye İstatistik Kurumu (TÜİK) tarafından yürütülen istatistik faaliyetleri, söz konusu istisna hükmü kapsamındadır. TÜİK'in yanı sıra Resmi İstatistik Programı'nda (Resmi İstatistik Programı; verilerin hangi tanım, yöntem, kapsam ve sınıflama kullanılarak hangi kurum tarafından, hangi sıklıkta derleneceği ve yayınlanacağı ile ilgili bilgileri kapsamaktadır. Erişim: https://www.tuik.gov.tr/Kurumsal/Sikca_Sorulan_Sorular, 06.07.2022.) yer alan kurum ve kuruluşlar tarafından istatistik üretilip, dağıtılıp yayımlanabilmektedir. Bu anlamda, "resmi istatistik"ler, TÜİK ve Programda belirtilen kurum ve kuruluşlar tarafından belirlenen konularda üretilmekte ve yayımlanabilmektedir. Kurum ve kuruluşların, görev alanları ile ilgili resmi istatistiklere ilişkin verileri değerlendirme, derleme ve yayımlama görevi Programda yer alır. Örneğin, 2022-2026 tarihli Resmi İstatistik Programında aşağıda belirtilen kurum ve kuruluşlar resmi istatistik oluşturmada görevleri söz konusudur:

- *"Cumhurbaşkanlığı ve bakanlıklar ile bunların bağlı, ilgili ve ilişkili kuruluşları,*
- *Mahalli idareler ve bunların bağlı ve ilgili kuruluşları ile birlik ve şirketleri,*
- *Türkiye Cumhuriyet Merkez Bankası (TCMB), Borsa İstanbul (BIST) ve üniversiteler de dahil olmak üzere, tüzel kişiliğe haiz enstitü, teşebbüs, teşekkül, birlik, döner sermaye, fon ve sair adlarla kurulmuş olan kurum ve kuruluşlar,*
- *Kamu kurumu niteliğindeki meslek kuruluşları." ("Resmi İstatistik Programı", 2022–2026)*

Vurgulanması gereken bir husus 5429 sayılı Türkiye İstatistik Kanununun 6 ncı maddesinde yer aldığı üzere Programda yer almayan istatistikî konulardaki kurum ve kuruluşların çalışmaları ile özel hukuk tüzel kişiliğine sahip kuruluşlarca veya gerçek kişiler tarafından yapılan araştırma ve sayımlara ait sonuçların resmî istatistik olarak kabul edilmemesidir.

Diğer taraftan istatistik oluşturmada verilerin güvenliği ve gizliliğine dair usul ve esaslar 5429 sayılı Türkiye İstatistik Kanunu'nun 12, 13 ve 14 üncü maddelerinde düzenlenmiş olup 5429 sayılı Türkiye İstatistik Kanunu sadece Türkiye İstatistik Kurumu'nu değil, Türkiye İstatistik Sistemindeki kuruluşların tamamını kapsamaktadır.

Belirtmek gerekir ki, TÜİK'in ve Resmi İstatistik Programında belirtilen kamu kurum ve kuruluşlarının yalnızca resmi istatistik kapsamındaki faaliyetleri Kanunun 28 inci maddesi çerçevesinde istisna hükmüne tabidir. Resmi istatistik haricindeki faaliyet konularına ilişkin olarak kişisel veri işleme faaliyetleri açısından TÜİK ve görev alan diğer kurumlar 6698 sayılı Kanun maddelerine tabi olmaya devam edecektir.

Anayasa Mahkemesinin istatistik amacıyla veri işlemenin konu olduğu ve bu kapsamda Anayasaya uygunluk değerlendirmesi yaptığı kararında (AYM, 2016) başvurucu, Türkiye İstatistik Kurumu (TÜİK) tarafından yapılan Hane Halkı Bütçe Anketi'ne geçerli bir nedeni bulunmaksızın katılmaması nedeniyle idari para cezası uygulanması sebebiyle özel hayata saygı hakkının ihlal edildiği iddiası ile başvuruda bulunmuştur. 6698 sayılı Kanun başvuruya konu idari işlemin tesis edildiği tarihte henüz çıkarılmamış olması nedeniyle başvuru konusu somut olay açısından dikkate alınması mümkün olamamıştır. Bununla birlikte mahkeme somut olayda kişisel verilerin korunması hakkı ve özel hayatın gizliliği hakkına müdahalenin söz konusu olduğunu ancak sınırlamanın 5429 sayılı Türkiye İstatistik Kanunu'na dayandığını, bu anlamda Kanunun "kanunilik" ölçütünü karşıladığını ortaya koymuştur. Ek olarak anılan davada mahkeme;

> *"... somut olayda kamu makamları tarafından başvurucunun; adı, adresi, gelir kaynakları, tüketim alışkanlıkları ve ekonomik durumuna yönelik kişisel verileri"nin talep edildiği ancak söz konusu eyleme dair kanuni bir dayanağın bulunması ve "söz konusu düzenlemelerin, kamu düzeni, ülkenin ekonomik refahı amaçlarına yönelik" olduğu diğer bir ifadeyle meşru bir amacın mevcut olduğu "toplumun tüketim harcamaları ile ekonomik düzeyinin belirlenmesi ve tespit edilen veriler ışığında devletin kamu güvenliği ve planlı kalkınma hususlarında ihtiyaç duyulan tedbirleri alması için hane halklarına yönelik anket yapılmasının demokratik bir toplumda gerekli" olarak görülebileceği belirtilerek "Anayasa'nın 20 inci maddesinde güvence altına alınan özel hayata saygı hakkının ihlal edilmediğine"* karar vermiştir.

Anonim Hâle Getirilmek Suretiyle Araştırma, Planlama ve İstatistik Gibi Amaçlarla Kişisel Verilerin İşlenmesi Hali

Araştırma, planlama ve istatistik gibi amaçlarla kişisel veri işlenmesi halinde bu verilerin anonim hale getirilmesi söz konusu ise işleme faaliyeti Kanundan istisna tutulmuştur.

Kişisel verinin anonim hale getirilmesi, "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"te *"kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi"* olarak tanımlanmaktadır. Bununla birlikte anılan Yönetmeliğin 4 üncü maddesinde imha işlemi de *"kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi"* işlemi olarak tanımlanmıştır. Anonim hale getirme işleminin imha olarak tanımlanma nedeni anonim verinin kişisel veri niteliğini haiz olmamasından kaynaklıdır. Dolayısıyla kişisel verinin mevcut olmadığı bir durumda işleme faaliyetinin, Kanun kapsamında bulunup bulunmadığının değerlendirmesine de gerek kalmayacağı kanaatine varılabilir.

Başka bir anlatımla, anonim veri; *"başından beri belirli bir kişiyle ilişkilendirilmesi söz konusu olmayan veri"*yi ifade ederken, anonim hale getirilmiş veri ise *"daha öncesinde belirli bir kişiyle ilişkilendirilmiş ancak kişiyle bağlantısı kalmamış veri"*yi ifade eder (Kişisel Verileri Koruma Kurumu, 2019, s.51).

Öte yandan 6698 sayılı Kanunun 7 nci maddesinin birinci fikrasında:

"Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir."

maddesine yer verilmektedir. Dolayısıyla anonim hale getirilme işlemi, işleme faaliyetine dayanak teşkil eden işleme şartının ortadan kalkması halinde yapılacak işlemlerden biri olarak sayılmaktadır.

Bu anlamda bir veri sorumlusu tarafından "anonim" olmaksızın araştırma, planlama ve istatistik gibi amaçlarla kişisel verinin toplanması/işlenmesi işlemi gerçekleştirilirken 6698 sayılı Kanun hükümlerine uyulması gerekmektedir. Diğer bir ifadeyle bu amaçlarla veri işlenirken kişisel verilerin anonim hale getirilmesi söz konusu değilse istisna durumu söz konusu olmadığından Kanunun 5 inci maddesinde yer verilen işleme şartlarının mevcut olması gerekmektedir. Dolayısıyla bahse konu amaçlarla ve Kanunda yer alan işleme şartlarına dayanarak işlenen kişisel verilerin sonradan anonim hale getirilmesi durumu söz konusu olduğunda istisna maddesi kapsamına dahil olması mümkün olmakla birlikte Kanunun diğer maddeleri uyarınca kişisel veri işleme faaliyeti sonlandırılabilmektedir. Dolayısıyla söz konusu istisna maddesi açısından maddenin karşılık bulduğu alanların sınırının dar olduğu değerlendirilmesine varılabilmektedir.

Kişisel Verilerin Millî Savunmayı, Millî Güvenliği, Kamu Güvenliğini, Kamu Düzenini, Ekonomik Güvenliği, Özel Hayatın Gizliliğini veya Kişilik Haklarını İhlal Etmemek ya da Suç Teşkil Etmemek Kaydıyla, Sanat, Tarih, Edebiyat veya Bilimsel Amaçlarla ya da İfade Özgürlüğü Kapsamında İşlenmesi

6698 sayılı Kanun uyarınca istisna kapsamına alınan diğer bir husus "sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü" kapsamında kişisel verilerin işlenmesidir. Kişisel verilerin bu amaçlarla işlenmesi hali istisna kapsamında tutulmakla birlikte bu işleme faaliyetlerinin taşıması gereken belirli koşullar söz konusudur. Bu koşullar kişisel veri işleme faaliyetinin;

"millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek"

kaydıyla yapılmasıdır.

6698 sayılı Kanunun diğer maddelerinde ve kıyasen uluslararası düzenlemelerde

"millî savunma", "millî güvenlik", "kamu güvenliği", "kamu düzeni" ve *"ekonomik güvenlik"*i sağlamak adına kişisel verilerin korunması hakkına sınırlama getirilmesinin mümkün olabileceği düzenleniyorken söz konusu maddede farklı olarak sayılan mefhumların ihlal edilmemesi şartıyla belirtilen konularda gerçekleşen işleme faaliyetinin Kanun kapsamında tutulmadığı görülmektedir. Bu anlamda kanun koyucunun kişisel verilerin korunması hakkının sınırlandırılması durumunda dahi sayılan durumların da ayrıca gözetilmesi yoluna gittiği anlaşılmaktadır.

Diğer taraftan madde hükmünde dikkat çeken ilk husus kişisel verilerin "sanat, tarih ve edebiyat veya bilimsel amaçla" işlenmesinin yanı sıra hükmün devamına temel bir hak olarak ifade özgürlüğü kapsamında kişisel verilerin işlenmesi halinin eklenmesidir. Esasında söz konusu maddede yalnızca ifade özgürlüğünün değil Anayasa'nın 27 nci maddesinde yer alan;

"Herkes, bilim ve sanatı serbestçe öğrenme ve öğretme, açıklama, yayma ve bu alanlarda her türlü araştırma hakkına sahiptir."

hükmü çerçevesinde anılan maddede anayasal bir hak olan "Bilim ve sanat hürriyeti" nin de farklı ifadelerle gözetildiği görülmektedir.

Benzer şekilde AİHM de bir kararında ifade özgürlüğü ile birlikte akademisyenlerin çalıştıkları alan hakkındaki düşüncelerini özgür bir şekilde ifade etme özgürlüğü ve sınırlama olmaksızın bilgi ve gerçeği yayma özgürlüğüne sahip olduğunu belirterek bir anlamda söz konusu hakların birbiri ile ilişkisini de ortaya koymuştur. Ek olarak Mahkeme, Avrupa Konseyi Parlamenterler Meclisi'nin akademik ifade özgürlüğünün korunmasına ilişkin 1762 (2006) sayılı Tavsiye Kararına atıfta bulunarak;

"Araştırma ve eğitimdeki akademik özgürlük, ifade ve eylem özgürlüğünü, bilgiyi yayma özgürlüğünü ve araştırma yürütme ve bilgiyi ve gerçeği sınırlama olmaksızın dağıtma özgürlüğünü garanti etmelidir."

değerlendirmesinde de bulunmuştur (Sorguç v. Türkiye, 2009, par. 35).

Bu minvalde, 6698 sayılı Kanunun 28 inci maddesinde de kişisel verilerin korunması hakkı ile bilim ve sanat hürriyeti ve ifade özgürlüğünün karşı karşıya kalma durumunun düzenlendiği ifade edilebilir. Dolayısıyla söz konusu temel haklar ile kişisel verilerin korunması hakkının karşı karşıya gelmesi halinde maddede belirtilen koşulların değerlendirilmesinin yanı sıra, söz konusu haklar arasında

hangi hakkın baskın geleceğinin belirlenmesi amacıyla bir denge testi yapılması yoluna gidilmesinin hak ihlallerinin yaşanmaması uygun olacaktır.

Millî savunma, kamu güvenliği, millî güvenlik, kamu düzeni ve ekonomik güvenlik kavramları açısından değerlendirme yapıldığında, 6698 sayılı Kanunun norm denetiminde bulunduğu Anayasa Mahkemesi, kararında; bu kavramlar soyut ve genel kavramlar olarak görülse de kuralın tamamen belirsiz olduğu anlamına gelmediği, genel ve soyut düzenlemelerin olmasının somut olayın özelliklerine göre yorumlanabilecek çözümler getirilebilmesine de olanak sağlayabileceği ifade edilmiştir (AYM, E.2016/125, K. 2017/143, K.T. 28.9.2017, par. 158). Bu anlamda öncelikle maddede belirtilen amaçlarla kişisel verilerin korunması hakkının sınırlandırıldığı durumlarda ayrıca ihlal edilmemesi gereken koşulların ne anlam ifade ettiğinin açıklığa kavuşturulması gerekmektedir.

Milli Savunma ve Millî Güvenlik

Milli güvenlik, devletin milli savunması ve tüm dış ilişkilerini de kapsamına alan bir kavramdır. Kavram herhangi bir yabancı devlete veya devletler topluluğuna karşı savunma ve askeri üstünlüğü, dış ilişkide üstün bir konumu; dış veya iç menşeli 'düşman'ların örtülü veya açık şekilde yıkıcı eylemlerine karşı savunma durumu/duruşu olarak tanımlanabilir (Amerika Birleşik Devletleri Savunma Bakanlığı, 2001, s.361). Örneğin hükümetin yıkılması veya demokratik düzene karşı saldırılar gibi tehlikelerden korunmayla ilgilidir (Roagna, 2012, s.42). Bu kavramlar AİHM tarafından da bir kişi hakkında gizli bilgi toplanması ve casuslukla ilgili birkaç davada da esas alınmıştır (Örnek kararlar için bkz. Klass v. Almanya, 1993; Leander v. İsveç, 1987).

Kamu Güvenliği ve Kamu Düzeni

Kamu güvenliği ve kamu düzeni kavramları nadiren tek başına değerlendirilmektedir. Bu kavramlar tek başına değerlendirildiğinde dahi AİHM bu amaçlarla beraber suçun önlenmesi, milli güvenlik veya düzenin korunması gibi diğer sebeplere de dayanma eğiliminde olmaktadır (Roagna, 2012, s.42). Güvenlik kavramı ayrıca iç güvenlik ve kamu düzeni kavramları baz alınarak değerlendirilmektedir. Kamu düzeni; toplumsal düzeni ifade etmektedir. Dirlik, güvenlik, esenlik ve sağlık da kamu düzeninin temelleri olarak kabul edilir ve toplumsal barışın bozulmadığı bir durum olarak tanımlanabilir.

Ekonomik Güvenlik

Ekonomik güvenlik, ülkenin refahına ve ekonomik işleyişine ilişkin potansiyel tehlikeler ve ülke ekonomisine yönelik tehditlerle ilgili bir kavramdır. Aynı zamanda devlet güvenliğinin ve refahının bir unsuru olarak değerlendirilmektedir (Krakov, 2008, s.141-142). Örneğin AİHM'de görülen Gillow davasında (Gillow v. Birleşik Krallık, 1992) dengeli bir ekonomik kalkınmanın sağlanması amacıyla devletlerin halkı bölgenin belirli sınırları içinde yerleşmesi ile sınırlı tutulması ihtiyacı ekonomik güvenlik amacı çerçevesinde haklı bulunmuştur. Dolayısıyla kentsel alanların, iş alanları ile gözetilerek nüfus yoğunluğunun buna göre düzenlenmesi yönünde bir gerekçenin, ekonomik güvenlik için haklı bir gerekçe olarak görülmesi mümkün olmuştur.

Özel Hayatın Gizliliği

Özel hayata saygı hakkı, Anayasa'nın 20 nci maddesinde güvenceye alınmıştır. Söz konusu hak kapsamında korunan hukuksal çıkardan biri kişilerin mahremiyet hakkıdır. Ayrıca Anayasa Mahkemesinin de zaman zaman kararlarında atıf verdiği gibi, AİHM tarafından da hiçbir zaman özel hayat kavramına dair açık, net ve belirli bir tanım getirilmemiştir (Örnek AYM Kararı için bkz. AYM, 2022). Mahkemeye göre özel hayat ayrıntılı bir tanımla açıklanamayacak bir kavramdır. Özel hayat kavramına ilişkin açık olansa her bireyin özgür şekilde kişiliğini oluşturduğu ve geliştirdiği, diğer insanlarla ve dış dünya ile ilişkiyi içine alan ve 'mahremiyet'ten daha geniş bir kavram olduğudur (Roagna, 2012, s. 12). AİHS'nin 8 inci maddesinin ilk fikrasında;

> *"Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir."*

hükmü yer alır. Bu anlamda özel hayat kavramı aile hayatı, konut dokunulmazlığı ve haberleşme hürriyeti olmak üzere başlıca üç konuyu içermektedir. Anayasa'nın yapısı dikkate alındığında da benzer bir yaklaşımın söz konusu olduğu görülmektedir. (Anayasanın "IV.Özel hayatın gizliliği ve korunması" başlıklı bölümünde "A.Özel hayatın gizliliği", "B. Konut dokunulmazlığı", "C. Haberleşme hürriyeti" temel haklarına yer verilmiştir.)

Kişisel verilerin korunması hakkı Anayasa'nın "Özel hayatın gizliliği" başlıklı 20 nci maddesinde düzenlendiği dikkate alındığında söz konusu hak, özel hayatın gizliliği hakkının özel bir şekli olarak kişisel verilerin işlenmesi esnasında gerçek kişilerin hak ve özgürlüklerini korumayı amaçlamaktadır. Dolayısıyla kişisel

verilerin korunması hakkı, *"özel hayatın gizliliği hakkının özel bir alt görünümü olduğu"* şeklinde ifade edilebilir. Bu minvalde özel hayatın gizliliğini ihlal eden her durum, kişisel verilerin korunması hakkını ihlal etmese de kişisel verilere ilişkin bir ihlalin özel hayatın gizliliği hakkını ihlal etmeme durumu pek olası görünmemektedir. Benzer şekilde AİHM de kararlarında bir gerçek kişinin kişisel verilerinin işlenmesi ve saklanması durumunun özel hayatın gizliliği hakkına müdahale teşkil ettiğini belirtmiştir. Dolayısıyla 'kişisel verilerin işlenmesi halinde' üst başlık olarak 'ilgili kişilerin özel hayatın gizliliği hakkına müdahale' teşkil ettiğini ifade etmek yanlış olmayacaktır (Benzer değerlendirmeler için bkz. AİHM, S. and Marper v. Birleşik Krallık, 2008, par. 67; Leander v. İsveç, 1987, par. 48 ve ABAD, Birleştirilmiş davalar C-293/12 ve C-594/12, Digital Rights Ireland, par. 34-36; Ayrıca bkz. Birleştirilmiş davalar C-92/09 ve C-93/09 Volker und Markus Schecke, 2010, par. 58).

Bu anlamda 6698 sayılı Kanunun 28 nci maddesinde özel hayatın gizliliğini ihlal etmemek kaydıyla, başkalarının bilim ve sanat özgürlüğü çerçevesinde belirtilen amaçlarla ve ifade özgürlüğü kapsamında kişisel verilerin işlenmesi durumu sorgulanırken somut olayın dinamiklerine göre bir sonuca ulaşılması gerekir. Anılan maddede 'ihlal etmemek kaydıyla' ifadesi kullanılsa da örneğin ifade özgürlüğü ile özel hayatın gizliliği hakkının karşı karşıya gelmesi halinde GVKT'deki düzenlemeye paralel şekilde iki hak arasında denge testi yapılması yolu ile bir kanaate varmak daha uygun bir yaklaşım olacaktır. Nitekim Kişisel Verileri Koruma Kurulu'nun da denge testi yapılması suretiyle kanaate vardığı kararları mevcuttur (Kurulun 22/05/2020 tarihli ve 2020/414 sayılı ve 02/12/2021 tarihli ve 2021/1217 sayılı Kararı).

Kişilik Haklarını İhlal Etmemek

Kişilik hakkı, kişinin, beden bütünlüğü, yaşamı, kişiliğini oluşturan maddi ve manevi değerleri, sözü, fotoğrafi, adı, eseri diğer bir ifadeyle kişiliğini serbestçe oluşturmasını sağlayan öğelerin tümü üzerindeki hakkıdır (Serozan, 2011, s.93). Kişilik hakları, kişiye sıkı sıkıya bağlı haklardan olup bu haklardan vazgeçilmesi ya da hakların devredilmesi mümkün değildir. Kişisel verilerin sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü çerçevesinde işlenmesi halinde somut olayın koşulları göz önünde bulundurularak yine denge testi yapılması suretiyle sonuca ulaşılması uygun olacaktır.

Suç Teşkil Etmemek

Suç, karşılığında ceza veya güvenlik tedbiri yaptırımı olan ceza hukukunun temel

kavramlarından biridir. Yapılan bir haksızlığın suç olup olmadığı her somut olaya ilişkin ilgili kanunda belirtilen unsurları taşıyıp taşımadığına göre belirlenir. Kişisel verilerin tarih, edebiyat, sanat veya bilimsel amaçla ya da ifade özgürlüğü çerçevesinde işlenmesi halinde bu durumun 6698 sayılı Kanundan istisna sayılan hallerden biri olması için bu işleme faaliyetinin kanun uyarınca bir suç teşkil etmemesi de gerekmektedir.

Sanat, Tarih, Edebiyat veya Bilimsel Amaç Kapsamında Kişisel Verilerin İşlenmesi

İstisna hükmü gereğince yukarıda incelenen koşulların ihlal edilmemesi şartıyla tarih, sanat, edebiyat veya bilimsel amaçla veya ifade özgürlüğü kapsamında kişisel verilerin işlenmesi durumunda kanun maddeleri uygulama alanı bulamayacaktır. Bilindiği üzere Anayasa'nın 27 nci maddesinde bilim ve sanat hürriyeti düzenlenmiş olup herkesin;

> *"bilim ve sanatı serbestçe öğrenme ve öğretme, açıklama, yayma ve bu alanlarda her türlü araştırma hakkına"*

sahip olduğu belirtilmiştir.

Sanat, tarih ve edebiyat kapsamında kişisel verilerin işlenmesi halinin somut anlamda karşılığı araştırıldığında öncelikle bu alanların hayatta karşılığını bulan "şey" lere değinmek gerekir. 5846 sayılı Fikir ve Sanat Eserleri Kanununun 2 nci ve devam eden maddelerinde fikir ve sanat eserleri çeşitleri tanımlanmaktadır. İlk olarak "İlim ve edebiyat eserleri" tanımlanmış olup maddede;

> *"Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları*
>
> *Her nevi rakısalar, yazılı koreografi eserleri, Pandomimalar ve buna benzer sözsüz sahne eserleri Bedii vasfı bulunmayan her nevi teknik ve ilmi mahiyette fotoğraf eserleriyle, her nevi haritalar, planlar, projeler, krokiler, resimler, coğrafya ve topoğrafyaya ait maket ve benzerleri, her çeşit mimarlık ve şehircilik tasarım ve projeleri, mimari maketler, endüstri, çevre ve sahne tasarım ve projeleri"*

olarak sıralanmaktadır. İkinci olarak "Musiki eserler" sayılmış olup bunlar da "her nevi sözlü ve sözsüz besteler" olarak tanımlanmıştır. Üçüncü olarak "Güzel sanat

eserleri" belirtilmiş olup bunlar da estetik değere sahip olmak kaydıyla;

> *"Yağlı ve suluboya tablolar; her türlü resimler, desenler, pasteller, gravürler, güzel yazılar ve tezhipler, kazıma, oyma, kakma veya benzeri usullerle maden, taş, ağaç veya diğer maddelerle çizilen veya tespit edilen eserler, kaligrafi, serigrafi, Heykeller, kabartmalar ve oymalar, Mimarlık eserleri, El işleri ve küçük sanat eserleri, minyatürler ve süsleme sanatı ürünleri ile tekstil, moda tasarımları, Fotografik eserler ve slaytlar, Grafik eserler, Karikatür eserleri, Her türlü tiplemeler"*

şeklinde sıralanmıştır. Son olarak ise "Sinema eserleri" ne yer verilmiştir.

Diğer taraftan ülkemizin 07.07.1995 tarihli ve 4117 sayılı Kanun ile en son haline taraf olunan Edebiyat ve Sanat Eserlerinin Korunmasına İlişkin Bern Sözleşmesinin 2 nci maddesinde "Edebiyat ve Sanat Eserleri" deyimi;

"ifade şekli ne olursa olsun, edebiyat, bilim ve sanat alanındaki kitaplar, dergiler ve diğer yazılar; konferanslar, nutuklar, vaazlar ve benzer nitelikteki diğer eserler; dramatik eserler veya dramatik-müzik eserleri; koreografik eserler ve pandomima gösterileri; sözlü veya sözsüz müzikal kompozisyonları, sinema tekniğine benzer bir yöntemle ifade edilen sinematografik eserler; çizim, sulu ve yağlı boya resim, mimarlık, heykel traşlık, oymacılık ve taş basma eserler, fotoğraf tekniğine benzer bir yöntemle ifade edilen fotoğraf eserleri; uygulamalı sanat eserleri; resimlendirmeler, haritalar, planlar, krokiler ve coğrafya, topografya, mimari veya bilimsel üç boyutlu eserler gibi bütün ürünler"

şeklinde belirtilmiştir.

Bu çerçevede 6698 sayılı Kanun lafzı olarak tanımlandığında söz konusu eserlerde belirtilen koşulları ihlal etmemek kaydıyla kişisel verilerin işlenmesi durumunda 6698 sayılı Kanun maddeleri uygulanmayacaktır. Ancak özel hayatın gizliliği hakkı ile madde hükmünde düzenlenen bilim ve sanat özgürlüğünün karşı karşıya gelmesi halinde denge testi yapılması uygun olacaktır. Benzer şekilde kişinin ad ve soyadının maskelenmeden kitapta yer verilmesine ilişkin Yargıtay Hukuk Genel Kurulu, bilim ve sanat özgürlüğü ile özel hayatın gizliliği ve kişisel verilerin korunması hakkının alt başlığı olarak değerlendirilen unutulma hakkı arasında denge testi yapılması yoluna gitmiştir. Mahkeme, Avrupa Birliği Adalet Divanı'nın "Google Kararı"na da atıfta bulunarak kişisel verinin eserde yer almasında üstün bir kamu yararı olduğunu gösteren özel sebepler bulunmaması nedeniyle bilimsel esere alınan belgelerde kişisel verilerin açık bir şekilde yer

almaması gerektiğine kanaat getirerek özel hayatın gizliliğinin ihlal edildiği tespitinde bulunmuştur (Yargıtay Hukuk Genel Kurulu, 2015).

Diğer taraftan sanat, tarih ve edebiyat amacıyla veri işleme halinin yanı sıra bilimsel amaçla veri işleme durumunun da açıklığa kavuşturulması gerekmektedir. Söz konusu madde hükmünde, bilimsel amaçtan kastedilenin bilimsel araştırma olup olmadığı veya araştırma kapsamında olmayan ancak bilimsel bir amaç güden her durumun istisna hükmü kapsamına girip girmediği, bilimsel amaçla veri işleyen kimselerin akademik araştırmacı, kâr amacı güden veya gütmeyen kuruluşlar veya devlet kurumları olup olmayacağı veya bilimsel amacın fen bilimleri veya beşeri bilimleri kapsayıp kapsamayacağı soruları ile karşı karşıya kalınmaktadır. Çoğu zaman sosyal bilimler ile fen bilimleri, ilim, bilim ve fen gibi çeşitli kavramların varlığı ile bilimin tanımı noktasında kavram kargaşası nedeniyle birçok soruya net bir cevap verilememesi sonucunu da doğmaktadır. Dolayısıyla bu kavramlar arasında net bir kanaate varmak için bilimin evrensel özelliği dikkate alınarak, modern dünyada yer alan kullanım ile tutarlı bir şekilde ve bilgi felsefesi de göz önünde tutulmalıdır (Çengel, 2012, s.56).

Madde bu açıdan bir veri sorumlusunun sadece bilimsel bir amaçla kişisel veri işlediği iddiası karşısında yapılacak değerlendirmenin nasıl olacağına ilişkin bir açıklama içermemektedir. Bu açıdan değerlendirildiğinde, istisna maddeleri arasında bulunması nedeniyle kişisel verilerin korunmasına ilişkin 6698 sayılı Kanunda yer alan hak ve yükümlülüklerin sağlanmaması durumu karşısında, maddede "bilimsel amaçla veri işlenmesi" ifadesi sınırları belirli olmayan, genel ve belirsiz bir ifade olarak değerlendirildiğinde ilgili kişiler açısından öngörülemeyen sonuçlar doğurabilecektir. Dolayısıyla uluslararası düzenlemeler de dikkate alınarak somut olay bazında yapılacak değerlendirmelerde esas alınabilecek ölçütlerin ortaya konulması gerekir.

Araştırma veya bilimsel araştırmanın evrensel olarak kabul edilmiş bir tanımı söz konusu değildir. Ancak araştırmanın; bilgi stokunu artıran verilerin toplanması ve analizi de dahil olmak üzere sistematik bir faaliyeti ifade ettiği söylenebilir. Bilimsel araştırma ise fikir, bilgi ve bilgi alışverişine dayanır. Olayları gözlemleme, bu olaylar hakkında bir hipotez elde etme ve hipotezin geçerliliği konusunda sonuca varma yöntemi de bilimsel araştırmanın yöntemidir. Aynı zamanda araştırmanın yürütülmesi esnasında açıklık ve şeffaflık olması bilim ile sözde bilim arasında ayrım yapılmasına da yardımcı olur (Avrupa Veri Koruma Denetmeni, 2020, s. 9-10). Dolayısıyla hükmün sınırlarının bu doğrultuda açıklığa kavuşturulması yerinde olacaktır.

Avrupa Veri Koruma Denetmeni (EDPS), bilimsel araştırmalarda kişisel verilere ilişkin görüşünde AB'nin 2019/790 sayılı Telif Hakkı Direktifine atıfta bulunarak bilimsel araştırmanın hem doğa bilimlerini hem de insan bilimlerini kapsar şekilde ele alındığını ve ticari faaliyet güden kuruluşlar ile diğer kuruluşlar açısından bir ayrım yapıldığını belirtir. Direktifte bilimsel araştırma yapan üniversite, araştırma enstitüsü, hastane gibi araştırma kuruluşlarının çeşitliliği dikkate alındığında söz konusu kuruluşlara karşı ortak bir anlayışa sahip olmanın önemine dikkat çekilir (AB 2019/790 sayılı Telif Hakkı Direktifi, Giriş kısmı, par. 12). Bu anlamda farklı yasal yapılarına rağmen AB üyesi devletlerdeki araştırma kuruluşlarının genel olarak, kar amacı gütmeyen bir temelde ya da Devlet tarafından tanınan bir kamu yararı misyonu bağlamında hareket etmesi ortak bir ölçüt olarak kabul edilmiştir. Bu minvalde yalnızca ticari teşebbüs amacı güden araştırmalar Direktifin amaçları doğrultusundaki araştırma olarak kabul edilmemiştir (Avrupa Veri Koruma Denetmeni, 2020, s. 10).

Bilimsel araştırmanın toplum için yararlı olduğu ve bilimsel bilginin desteklenmesi gerektiği yaygın bir varsayımdır. Ancak bir faaliyetin araştırma olarak kabul edilmesi tamamen sorumsuz bir şekilde kişisel veri işlenmesine dair bir yetki verildiği anlamına da gelmemektedir. Dolayısıyla bir veri sorumlusunun sadece bilimsel araştırma amacıyla kişisel veri işlediği iddiasında bulunması bu kapsama dahil edilmesi için yeterli olmamalıdır. (Giovanni Buttarelli, 2018, s.2).

GVKT resital 157 de araştırmanın rolü, *"birkaç insanın yaşam kalitesini iyileştirebilecek ve sosyal hizmetlerin verimliliğini artırabilecek"* bilgilerin sağlanması olarak belirtilmiştir. Dolayısıyla GVKT teknolojik gelişme, temel ve uygulamalı araştırma ve özel olarak finanse edilen araştırma ve *"halk sağlığı alanında kamu yararına yürütülen çalışmalar"* da dahil olmak üzere geniş bir araştırma anlayışını kabul etmektedir.

29. Madde Çalışma Grubu da rızaya ilişkin görüşünde bilimsel araştırmayı *"ilgili metodolojik ve etik standartlara uygun olarak oluşturulmuş bir araştırma projesi"* olarak tanımlamıştır (29. Madde Çalışma Grubu, 2020, s. 27-30). Ayrıca EDPS de bu yaklaşıma atıfta bulunarak yalnızca yerleşik bir etik çerçeve içinde gerçekleştirilen bilimsel araştırmaların özel veri koruma rejimine giren faaliyetler olarak nitelendirmiştir. Bu nedenle, bilimsel araştırmalar için özel veri koruma rejiminin üç kriterin her birinin sağlanması durumunda uygulanacağı belirtilmiştir.

Söz konusu üç kriter:

1) Kişisel veriler işlenir.

2) Bilgilendirilmiş onay, hesap verebilirlik ve gözetim kavramları da dahil olmak üzere ilgili sektörel metodoloji ve etik standartlar geçerli olmalıdır.

3) Araştırma, özel çıkara hizmet etmek yerine, toplumun kolektif bilgisini ve refahını artırmak amacıyla yürütülmelidir.

şeklinde belirtilmiştir (Avrupa Veri Koruma Denetmeni, 2020, s. 11-12).

Diğer taraftan belirtmek gerekir ki, GVKT'ye göre kişisel verilerin korunması açısından gereklilik ve orantılılık ilkeleri çerçevesinde ve veri minimizasyonu ilkesine uyulması adına, kişisel verileri işlemeden önce bilimsel araştırma yapan kişiler araştırmanın veri işlemeden mümkün olup olmadığını da ayrıca değerlendirmelidir.

Bu anlamda 6698 sayılı Kanun kapsamında bilimsel amaçla kişisel verilerin işlenmesi açısından değerlendirme yapılırken yukarıda yer verilen kriterlerin gözetilmesi uygun olacaktır. Örneğin üniversite bünyesinde akademik araştırma çerçevesinde kişisel verilerin işlenmesi durumunda çalışmanın "konuya özgü" düzenlenmiş olan Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesi çerçevesinde bir çalışma olup olmadığı değerlendirilmelidir.

İfade Özgürlüğü Kapsamında Kişisel Verilerin İşlenmesi

İstisna hükmünde sanat, tarih, edebiyat ve bilimsel amaçlar kapsamında verilerin işlenmesi düzenlenirken bunlara ek olarak ifade özgürlüğü yani temel bir hak ve özgürlük kapsamında kişisel veri işlenmesi hali de belirtilmiştir. Dolayısıyla maddede bilim ve sanat özgürlüğünün yanı sıra kişisel verilerin korunması hakkı ile ifade özgürlüğü hakkının da karşı karşıya gelmesi halinin düzenlendiği yorumunda bulunulabilir.

İfade özgürlüğü Anayasa'nın *"Düşünceyi açıklama ve yayma hürriyeti"* başlıklı 26 ncı maddesi uyarınca düşünceyi açıklama ve yayma özgürlüğü, yalnızca *"düşünce ve kanaate sahip olma"*yı değil, sahip olunan *"düşünce ve görüşü açıklama ve yayma"*, buna bağlı olarak *"haber veya görüş alma ve verme"* özgürlüklerini de kapsamaktadır. Bu çerçevede, AYM'nin de kararlarında vurguladığı gibi "düşünceyi açıklama ve yayma özgürlüğü", bireylerin serbest bir şekilde;

> *"haberlere, bilgilere, başkalarının düşüncelerine ulaşabilmesi", "edindiği düşünce ve kanaatlerden dolayı kınanmaması ve bunları yalnız veya başkalarıyla birlikte çeşitli yöntemlerle serbestçe ifade edebilmesi, anlatabilmesi, savunabilmesi ve yayabilmesi"*

anlamına da gelmektedir (AYM, 2014 (c), par. 40 ve AYM, 2004 par. 29).

Diğer taraftan bilim ve sanat özgürlüğü ile de bağlantılı olarak AİHM, akademisyenlerin çalıştıkları alan hakkındaki düşüncelerini özgürce ifade etme özgürlüğüne ve sınırlama olmaksızın bilgi ve gerçeği yayma özgürlüğüne sahip olduğunu belirtmiştir. Aynı zamanda Mahkeme, Avrupa Konseyi Parlamenterler Meclisi'nin akademik ifade özgürlüğünün korunmasına ilişkin 1762 (2006) sayılı Tavsiye Kararına atıfta bulunarak;

> *"Araştırma ve eğitimdeki akademik özgürlük, ifade ve eylem özgürlüğünü, bilgiyi yayma özgürlüğünü ve araştırma yürütme ve bilgiyi ve gerçeği sınırlama olmaksızın dağıtma özgürlüğünü garanti etmelidir."*

değerlendirmesinde bulunmuştur (Sorguç v.Türkiye, 2009, par. 35).

AİHM kararlarında, ifade özgürlüğünün;

> *"toplumun ilerlemesi ve her insanın gelişmesi için esaslı koşullardan biri olan demokratik toplumun asıl temellerinden birini"*

oluşturduğuna dikkat çekmektedir. AİHM'e göre ifade özgürlüğü, yalnızca lehte ya da zararsız ya da gereksiz olarak nitelenen bilgi veya fikirler için değil, devletin veya kamunun bir bölümü için rahatsız edici, şok edici hatta saldırgan düşünceler için de uygulanmaktadır. Bunlar, demokratik toplum için hoşgörünün, çoğulculuğun ve açık fikirliliğin gerekleridir (AİHM, Handyside v. Birleşik Krallık, 1976, par. 49).

İfade özgürlüğüne ilişkin sınırlamalara ilişkin kamu makamları bir ölçüde takdir yetkisine sahiptir. Ancak bu takdir yetkisi Anayasa Mahkemesinin denetimine de tabi olup hakkın özüne dokunmama, demokratik toplumun gereklerine uygunluk ve ölçülülük kriterleri çerçevesinde denetleme yapmaktadır. AYM yaptığı denetimde genel veya soyut bir değerlendirmeden ziyade ifadenin türü, şekli, içeriği, açıklandığı an ve sınırlama nedenlerinin niteliği gibi çeşitli hususlara göre farklılaşan ayrıntılı bir değerlendirme yapma yoluna gitmektedir (AYM, 2004 par. 33; AYM, 2014 (c), par.48).

Örneğin; basın özgürlüğü ile davacının kişilik hakları arasında bir ihtilaf meydana gelmesi durumunda çatışan söz konusu haklar arasında denge yapılması için başvurunun koşullarına ve bütünselliğine göre olaya uygulanabilecek kriterlerin bazıları şu şekilde sayılmıştır:

i. *"Yayında kamu yararı bulunup bulunmadığı, genel yarara ilişkin bir tartışmaya katkı sağlayıp sağlamadığı,*

ii. *Toplumsal ilginin varlığı ve konunun güncel olup olmadığı,*

iii. *Haber veya makalenin yayımlanma şartları,*

iv. *Haber veya makalenin konusu, bunlarda kullanılan ifadelerin türü, yayının içeriği, şekli ve sonuçları,*

v. *Habere yönelik sınırlamaların niteliği ve kapsamı,*

vi. *Haberde yer alan ifadelerin kim tarafından dile getirildiği,*

vii. *Hedef alınan kişinin kim olduğu, ünlülük derecesi ile ilgili kişinin önceki davranışları,*

viii. *Kamuoyu ile diğer kişilerin kullanılan ifadeler karşısında sahip oldukları hakların ağırlığı."*

(AYM, 2019, par. 33; AYM, 2004, par. 41; AYM, 2015 (a), par. 56; AYM, 2015 (b), par. 58-66; AYM, 2014 (d), par. 66-73).

Temel hak ve özgürlüklerin ihtilafi durumunda hak ve özgürlükler arasında uygun bir dengenin kurularak muhtemel olduğu ölçüde her iki özgürlüğün de gözetildiği bir yöntemin benimsenmesi gerekir. Dolayısıyla iki hakkın karşı karşıya kalması durumunda bu haklar arasında denge testi yapılması yoluna gidilmesi gerekecektir.

Bu anlamda yukarıda yer verilen kriterlerin ve Anayasanın 13 üncü maddesi gereğince hakkın özüne dokunmama, demokratik toplum düzeninin gereklilikleri ve ölçülülük ilkesi de göz önünde bulundurularak somut olayın koşullarına göre kişisel verilerin korunması hakkı ile ifade özgürlüğü arasında makul bir dengenin gözetilmesi dolayısıyla somut değerlendirmeler kapsamında hakkın sınırlandırılması yoluna gidilmesi gerekir.

Örneğin soruşturma çerçevesinde kayıt altına alına alınmış olan telefon görüşmelerinin basına verilmesi ve bu görüşmelerin birçok gazetede yayımlanması sonucunda haberleşme hürriyeti ve özel hayatın gizliliği hakkının ihlal edildiğine yönelik Anayasa Mahkemesine gelen, bir başvuruda (AYM, 2015 (c), par. 70)

özel hayatın gizliğinin bir parçası olan kişisel verilerin korunması hakkı ile ifade özgürlüğünün bir görünümü olan basın özgürlüğü karşı karşıya gelmiştir. AYM değerlendirmesinde; kişinin soruşturma aşamasında haberleşme hürriyetine getirilen sınırlamaları kanunilik, demokratik toplumun gerekleri ve hakkın özüne dokunulması açısından değerlendirmiş ve esas yönünden aykırılık bulmamıştır. Ancak pozitif yükümlülüğü gereğince kamu makamlarının kişisel veriler ile gizli olması gereken haberleşme kayıtlarının açık edilmesini önlemek için ve haberleşmenin gizliliği hakkının etkili bir şekilde korunmasını sağlamak için gerekli hukuki düzenlemelerin yapılması, organizasyonun kurulması, personelin bu konuda eğitilmesini de içeren tüm tedbirleri alması gerektiğinin altını çizmiştir.

Diğer taraftan Mahkeme, ifade özgürlüğü çerçevesinde kamu yararı gözetilerek mahkemelere konu olan ilgili haberlere ve yorumlara basının yer verme görevi bulunduğuna dikkat çekmekle beraber, bu durumun halihazırda görülen davalarda delil olarak kullanılan görüşme kayıtlarının, basın da dâhil olmak üzere üçüncü kişilerin erişimine sınırsız bir şekilde açılacağı anlamına gelmediği, ilgili mahkemenin yargılamaya konu olan kişilerin mahremiyet hakkını ve özel hayatına saygı hakkını koruyucu nitelikte tedbirler alması gerektiği belirtilmiş ve soruşturma aşaması henüz tamamlanmadan görüşme kayıtlarının ifşası nedeniyle kişi hakkındaki iddiaların kamuoyu tarafından öğrenildiği bu nedenle kişinin kendini savunma hakkının da elinden alındığı hususlarına yer verilerek haberleşme hürriyetinin maddi boyutunun ihlal edildiği sonucuna varmıştır.

AİHM de sokakta bulunan kapalı devre kameraların kayıt altına aldığı ve kişinin bileğini kestiğini kayıt altına alan kamera görüntülerinin Belediye tarafından basına verilmesi ile ilgili bir başvuruda, (AİHM, Peck v. Birleşik Krallık, 2003) kişisel verilerin korunması hakkına ilişkin bir müdahale niteliğinde olduğu ve bu müdahalenin başkalarının haklarının korunması ve suçun önlenmesi amaçlarıyla gerçekleştirildiği tespitinde bulunmuştur.

Bununla beraber, kişisel verilerin korunması hakkına müdahalenin demokratik bir toplumda gerekli olmadığı tespitinde bulunarak kişinin özel hayata saygı hakkının ihlal edildiği sonucuna varmıştır.

Sonuç olarak kişilik hakları, sanat ve bilim özgürlüğü de dahil olmak üzere ifade özgürlüğü ile birlikte kişisel verilerin korunması hakkının tehlikede olduğu varsayılarak temel hakların birbiri ile çelişkili olduğu değerlendirilmemelidir. Bunun yerine somut olayın dinamiklerine göre amaç, kişilerin temel hakları ve toplumsal çıkarlar arasında "adil bir denge" aranması başvurulacak yöntem olmalıdır.

Kişisel Verileri Koruma Kuruluna (Kurul) intikal eden şikayetlerde de Kurulun iki hakkın karşı karşıya gelmesi halinde somut olayın özelliklerine göre denge testi yaparak kanaate vardığı görülmektedir. Örneğin ifade özgürlüğü ile kişisel verilerin korunması hakkının karşı karşıya geldiği durumlara ilişkin olarak Kurul, aldığı Kararlarda;

> *"ifade özgürlüğünün bir yansıması olan basın özgürlüğü ile kişilik hakları karşı karşıya geldiğinde haberin; a) Kamu ilgi ve yararı taşıması, b) Gerçek ve güncel olması, c) Özü ile biçimi arasındaki denge, kriterleri kapsamında değerlendirilmesi suretiyle hangi hakka üstünlük tanınması gerektiğinin belirlenmesinin"*

önem arz ettiğine vurgu yaparak denge testi yapılması suretiyle olayları değerlendirmiştir (Kurulun 02/12/2021 tarihli ve 2021/1217 sayılı ve 22/05/2020 tarihli ve 2020/414 sayılı Kararları).

Kişisel Verilerin Millî Savunmayı, Millî Güvenliği, Kamu Güvenliğini, Kamu Düzenini veya Ekonomik Güvenliği Sağlamaya Yönelik Olarak Kanunla Görev ve Yetki Verilmiş Kamu Kurum ve Kuruluşları Tarafından Yürütülen Önleyici, Koruyucu ve İstihbari Faaliyetler Kapsamında İşlenmesi

6698 sayılı Kanun uyarınca millî güvenliği, millî savunmayı, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamak amacıyla yürütülen koruyucu, önleyici ve istihbari faaliyetler kapsamında kişisel verilerin işlenmesi halinde 6698 sayılı Kanun maddeleri uygulanmamaktadır. Ancak bu işleme faaliyetinin "kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından" yapılması gerekmektedir.

6698 sayılı Kanunun gerekçesinde, söz konusu maddeye ilişkin olarak;

> *"Milli İstihbarat Teşkilatı ile diğer istihbarat birimlerinin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik faaliyetleri kapsamında işlediği verilerin Kanun kapsamı dışında tutulduğu"*

ifade edilmiştir. Gerekçenin devamında bu amaçlarla, "suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ve mali suçların araştırılması" konularında yetkili birimler tarafından yürütülen faaliyetler kapsamında işlenen kişisel verilerin de istisna kapsamında olduğu belirtilmiştir. Ek olarak;

"bu konulardaki yetkili birimin; milli savunmayı, milli güvenliği kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olmak üzere mali araştırma yapmak, mali istihbarat elde etmek ve üretmek, veri toplamak, şüpheli işlem bildirimleri ve diğer bildirimleri almak, analiz etmek, değerlendirmek, inceleme yapmak ve ilgili kurumlarla paylaşmak suretiyle işlediği verilerin"

kapsam dışında tutulduğu ifade edilmiştir (6698 sayılı Kanun, m. 28 gerekçesi). Bu anlamda 6698 sayılı Kanun gerekçesinde maddenin kapsamına ilişkin sınırların belirli ölçüde açıklandığı görülmektedir.

Diğer taraftan 6698 sayılı Kanunun söz konusu maddesinde önleyici, koruyucu ve istihbari faaliyetlerin "geniş ve belirsiz bir kavram" olduğu, istisna kapsamına giren konuların sınırlandırılması gerektiği bu anlamda Anayasa'ya aykırı olduğunun ileri sürülmesi üzerine AYM'nin norm denetimi yaptığı kararında mahkeme; "yasa kurallarının genel ve soyut olmasının; somut olayın özelliğine göre değişebilecek tüm çözümleri kuralın bünyesinde barındırma"sından kaynaklı olduğu tespitinde bulunmuştur. Bu doğrultuda Mahkeme hükmün uygulanacağı kamu kurum kuruluşlarına açıklık getirmiş ve aşağıda yer verilen tespitlerde bulunmuştur: (AYM, E.2016/125, K.2017/143, par. 158-159, bkz. 2937 sayılı Kanun'un m.4).

"2559 sayılı Polis Vazife ve Salahiyet Kanunu, 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunu gibi ilgili kuruluş kanunlarında görev ve yetki verilmiş polis teşkilatı ve MİT gibi veya 4208 sayılı Kanun'la kurulan, görev ve yetkileri 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ile yeniden belirlenen Malî Suçları Araştırma Kurulu (MASAK) gibi kamu kurum ve kuruluşlarının dava konusu kuralda yer alan millî güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilen kamu kurum ve kuruluşları olduğu açıktır. Bu kanunlarda, söz konusu kamu kurum ve kuruluşlarının görev ve yetkileri ayrıntılı şekilde düzenlenmiş ve bu düzenlemelerde söz konusu görevlerin Türkiye Cumhuriyeti'nin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve millî gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında millî güvenlik istihbaratını oluşturmak veya suç gelirlerinin aklanmasının önlenmesini sağlamaya yönelik olduğu belirtilerek bu kamu kurum ve kuruluşları tarafından yürütülecek önleyici, koruyucu ve istihbari faaliyetler de düzenlenmiştir. Bu bağlamda dava konusu kuralla düzenlenen "önleyici, koruyucu ve istihbari" faaliyetlerin ilgili kuruluş kanunlarında veya diğer kanunlarda kapsam, sınır ve içeriklerinin ayrıntılı şekilde düzenlenmesi karşısında söz konusu faaliyetlerin kapsamının belirsiz olduğu söylenemez."

Bilindiği üzere kamu düzenini sağlamak idarenin görevinde olup kolluk yetkisinin de varlık nedenini oluşturmaktadır. Kolluk gücü gibi silahlı kuvvetlerinin başta milli güvenlik, milli savunma ve kamu güvenliğinin sağlanmasına ilişkin faaliyetlerinde Kanunla yetki verilmiş birimler tarafından işlenen kişisel veriler Kanun kapsamı dışında tutulmaktadır.

Diğer taraftan AYM, özel hayata dair bilgilerinin yer aldığı istihbari nitelikteki bir raporun, yürütülen soruşturmada delil olarak kullanılması hakkındaki davada; (AYM, 2014 (a)) istihbarat çalışması yoluyla kişilerin özel hayatına dair bilgilerin işlenmesinin ancak demokrasinin gerektirdiği kurumları korumak için ve zorunlu olduğu ölçüde meşru görülebileceğine (Benzer yöndeki AİHM kararı için bkz. Rotaru v. Romanya, 2000, par. 47) dikkat çekerek başvuran kişiye ilişkin bilgilerin yer aldığı istihbarat raporunun 2937 sayılı Kanunun 4 üncü maddesine dayalı olarak hazırlandığı ve Anayasa'nın 20 nci maddesinin ikinci fıkrasında yer alan suç işlenmesinin önlenmesi, kamu düzeni ve milli güvenlik amaçlarına ilişkin olduğunun anlaşıldığı tespitinde bulunmuştur.

Ardından kişinin mesleğiyle ilgili ve olumsuz olarak nitelendirilebilecek değerlendirmelerin kesinlik taşımaması, doğruluğunun sorgulanmamış olması ve kişi hakkında herhangi bir konuya dayanak teşkil etmemiş olmasına rağmen, davanın dosyasına eklenmesinin, duruşmaların kural olarak kamuya açık yürütülmesi nedeniyle bu bilgilerin alenileştirilmesini haklı kılmadığı hususlarını gözeterek kişinin özel hayatına yönelik ağır bir müdahalede bulunulduğu sonucuna varmıştır. Ek olarak kamu davasına konu olmayan kişiye dair verilerin dava dosyasına eklenmesinin demokratik bir toplumda gerekli olarak kabul edilemeyeceği gibi ölçülülük kriterini de taşımadığı belirtilmiştir.

Benzer şekilde AYM başka bir kararında (AYM, B. K. Başvurusu, B. N. 2014/14189, K. T. 25/10/2017) dava dosyasına kişisel verilerin eklenerek duruşma salonunda bulunan kişilere ve davanın taraflarına açık hale getirilmesi halini de özel hayatın gizliliği hakkına bir müdahale olarak değerlendirmiştir. Ek olarak Mahkeme, özel hayatın gizliliği hakkı açısından özellikle önem arz eden kişisel verilerin korunması gereken durumlarda yargı makamlarının da gerekli önlemleri alması ödevinin bulunduğuna dikkat çekmiştir. Bu doğrultuda yargılamanın aleni şekilde yürütülmesindeki kamusal menfaat ile kişinin mahremiyetinin ve özel hayatının korunması menfaati arasında adil bir dengenin kurulması ve varılan kanaatin, hüküm kurulurken yeterli ve ilgili düzeyde gerekçelerin de sunulması gerektiği vurgulanmıştır (AYM, 2017, par. 61).

Anayasa Mahkemesi başka bir kararında; (AYM, Ö.N.M. Başvurusu, B. N. 2014/14751, 15/2/2017) Hava Kuvvetleri Komutanlığı İstihbarat Daire Başkanlığı nezdinde oluşturulan İnceleme Timi tarafından, başka bir kişi ile ilgili yürütülen soruşturma kapsamında incelenen göreve tahsisli e-posta hesaplarında, sivil bir memurun asker kişilerle ilişki yaşadığının tespit edilmesi üzerine görevine son verilmesini değerlendirdiği kararda, somut olayda kişinin alenileşmemiş gönül ilişkisinin milli güvenliğin korunmasına yönelik bir amaca ilişkin askeri istihbaratı ilgilendirmediği, devlet memurluğundan çıkarma cezası ile verilen disiplin soruşturmasında özel hayatın gizliliği hakkına müdahaleye ilişkin haklı ve yeterli bir gerekçe bulunmadığını tespit ederek özel hayatın gizliliği hakkının ihlal edildiğine karar verilmiştir.

Bu bağlamda AYM özel hayatın gizliliğinin ihlal edildiğine dair kararlarında kişisel verilerin korunması hakkına getirilen sınırlandırmanın haklı bir nedeni olup olmadığını değerlendirmiştir. Ancak ek olarak verilerin işlenmesinde haklı bir nedenin varlığı durumunda da işlenen verilerin açıklanmasında, bu durumun ölçülü olup olmadığı ve kişisel verilerin 'kamu'ya duyurulmasında haklı bir neden olup olmadığı hususu da ayrıca değerlendirilmiştir.

AİHM ise kişinin sendika faaliyetlerine ilişkin bilgilerin bulunduğu gizli polis dosyasındaki verilerinin işe alım sürecinde kullanılması nedeniyle yaptığı bir başvuruda (AİHM, Leander v. İsveç, 1987) demokratik bir toplumda, istihbarat birimlerinin varlığının ve kişisel verilerin işlenmesi ve saklanmasının kanuna uygun olabileceğini, ulusal güvenliğin sağlanması veya suç işlenmesinin önlenmesi amaçlarının gözetilmesi koşuluyla kamu menfaatinin, bireylerin menfaatinin önüne geçebileceğini ifade ederek hakkın sınırlandırılmasına ilişkin müdahalenin demokratik bir toplumda ulusal güvenlik gibi bir konuda sosyal ihtiyaçları da göz önüne alarak AİHS'ne aykırı bulmamıştır.

Öte yandan AİHM kararlarında birçok kez kişisel verilerin kolluk veya ulusal güvenlik makamları tarafından işlenmesinin ve saklanmasının AİHS 8 inci maddesinin birinci paragrafına müdahale olduğuna karar vermiştir. Birçok AİHM kararı da anılan nitelikteki müdahalelerin gerekçelendirmesi ile ilgili sonuçlanmıştır (Bkz: Leander v. İsveç, 1987; M.M. v. Birleşik Krallık, 2012; M.K. v. Fransa, 2013; Aycaguer v. Fransa, 2017).

Örneğin B.B-Fransa davasında, (B.B. v. Fransa, 2009) başvuran kişi, 15 yaşında, reşit olmayan kişilerle güven ilişkisi içinde seks suçu işlemesinden dolayı hapis cezası verilmiş ve cezası 2000 yılında sonlanmıştır. Bir yılın ardından söz konusu cezanın sabıka kayıtlarından çıkarılması talebinde bulunmuş ancak talebi kabul

görmemiştir. Ardından 2004 yılında, Fransa Kanunları çerçevesinde ulusal boyutta adli nitelikte seks suçluları veri tabanı oluşturulmuş, ilgili kişiye de bu veri tabanına işlendiğine dair bilgi verilmiştir. AİHM, hüküm giymiş suçlunun ulusal adli nitelikte veri tabanına kaydedilmesini AİHS'nin 8 inci maddesi çerçevesinde bulunduğuna karar vermiş, fakat, ilgili kişinin verilerinin silinmesini talep hakkı, ilgili verilere yetkili erişim gibi yeterli düzeyde koruma tedbirlerinin alınması, nedeniyle somut olayda kamu ve özel menfaat arasında adaletli bir dengenin kurulduğu değerlendirmesinden hareketle AİHS 8 inci maddenin ihlal edilmediğine karar verilmiştir.

Kişisel Verilerin Soruşturma, Kovuşturma, Yargılama veya İnfaz İşlemlerine İlişkin Olarak Yargı Makamları veya İnfaz Mercileri Tarafından İşlenmesi

6698 sayılı Kanunun 28 inci maddesi uyarınca yargı makamlarının ve infaz mercilerinin *"soruşturma, kovuşturma, yargılama veya infaz işlemleri"*ne ilişkin olarak kişisel veri işleme faaliyetleri 6698 sayılı Kanun hükümlerinin uygulanmasından istisna tutulmuştur.

Maddenin lafzından anlaşılacağı üzere hüküm kapsamındaki kişisel veri işleme faaliyetinin 6698 sayılı Kanundan istisna olabilmesi için iki koşulun varlığı aranmaktadır. Bunlardan ilki "kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemleri"ne ilişkin olarak işlenmesi, diğeri ise söz konusu kişisel veri işleme faaliyetinin "bir yargı makamı veya infaz mercii tarafından yerine getirilmesi" ve bu iki şartın varlığının birlikte olmasıdır. Ek olarak vurgulamak gerekir ki söz konusu madde, yargı makamlarını ve infaz mercilerini bütünüyle Kanundan istisna tutmamış, yalnızca bu kurumların soruşturma, kovuşturma, yargılama veya infaz işlemleri kapsamındaki kişisel veri işleme faaliyetleri istisna tutulmuştur.

Anayasanın 9 uncu maddesinde;

> *"Yargı yetkisi, Türk Milleti adına bağımsız ve tarafsız mahkemelerce kullanılır."*

denilerek yargılama yapan makamın bağımsız mahkemeler olduğu belirtilmiştir. Bu doğrultuda Türkiye'deki yargı kolları Anayasanın 146 ncı ile 158 inci maddeleri arasında sayılmakta olup ve bu yargı kolları Anayasa Yargısı (Anayasa Mahkemesi), İdari Yargı (Danıştay), Adli Yargı (Yargıtay), ve Uyuşmazlık Yargısı (Uyuşmazlık Mahkemesi) olarak ifade edilebilir. Bu çerçevede maddede belirtilen yargılama makamlarından kastedilenin de Anayasa'da belirtilen yargı makamları olduğu

değerlendirilmektedir. Diğer bir ifadeyle, anılan maddede istisna tutulan kişisel veri işleme faaliyetleri, mahkemeler ve savcılık makamları tarafından gerçekleştirilen, soruşturma, kovuşturma ve yargılama işlemlerine ilişkin faaliyetlerdir.

5271 sayılı Ceza Muhakemesi Kanunun 2 nci maddesinde soruşturma;

> *"kanuna göre yetkili mercilerce suç şüphesinin öğrenilmesinden iddianamenin kabulüne kadar geçen evre", kovuşturma; "iddianamenin kabulüyle başlayıp, hükmün kesinleşmesine kadar geçen evre"*

olarak tanımlanmıştır. "Yargılama" ifadesinin ise 5271 sayılı Kanunda net bir tanımı bulunmamakla birlikte soruşturma ve kovuşturma aşamalarını da kapsayan üst bir başlık olarak değerlendirilebilir. Bu bağlamda yargılama faaliyetlerine; kesinleşmemiş mahkeme kararlarına karşı gidilen kanun yolları olan itiraz, istinaf ve temyiz işlemleri ve kesinleşmiş kararlara karşı olağanüstü kanun yolları olan kanun yararına bozma, yargılamanın yenilenmesi ve Yargıtay Cumhuriyet Başsavcısı'nın itirazı durumları da dahildir.

Bu doğrultuda söz konusu süreçlerde kişisel verilerin işlenmesi halinde 6698 sayılı Kanun hükümleri uygulanmayacaktır. Örneğin, soruşturma kapsamında Cumhuriyet Savcılığınca şüphelinin kimlik tespitinin yapılması, zimmet suçu kapsamında kişinin banka hesaplarının sorgulanması gibi durumlarda istisna hükmü gereğince 6698 sayılı Kanun hükümleri uygulanmayacaktır.

Maddede düzenlenen diğer bir kişisel veri işleme hali ise infaz işlemleri çerçevesinde yargı makamları veya infaz mercileri tarafından işlenen kişisel verilerdir. Yargılamanın sonucu ile verilen mahkûmiyet hükmü kesinleştikten sonra ceza veya güvenlik tedbirleri infaz olunmaktadır. 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanunda "infaz" ın tanımına yer verilmemekle birlikte infaz işlemi yargılama faaliyeti ile başlayan süreç sonunda verilen kararın uygulanmasına ilişkin işlemler olarak tanımlanabilir.

Hükmün infazına ilişkin olarak; hükümlülerin Ceza İnfaz Kurumlarına alınması ve kayıt işlemleri infaz işlemine örnek olarak verilebilir. İnfaz işlemleri mahkûmiyet hükmünün infazına ilişkin olan işlemlerle sınırlı olarak değerlendirilmelidir. Bu anlamda, Ceza İnfaz Kurumları tarafından gerçekleştirilen her işlemin infaz işlemi olduğu anlamına gelmemektedir. Örneğin Ceza İnfaz Kurumlarının kendi personeli hakkındaki veri işleme faaliyetleri infaz işlemi olarak değerlendirilmemelidir.

Diğer taraftan, yargılama sürecinde kişisel verilerin işlenmesine ilişkin değerlendirmelere dair mahkeme kararları incelendiğinde; dava dosyasında bulunan kanıtların kişisel veri içermesi durumuna ilişkin olarak Yargıtay 4. Ceza Dairesi Kararında (Yargıtay 4. Ceza Dairesi, 2016). Davanın taraflarının, delilleri inceleyerek kaynağını sorgulama, hukukiliği ve inandırıcılığına dair düşüncesini ileri sürme hakkına sahip olduğu, özel durumlar haricinde kanıtların, davanın taraflarından gizlenmesinin, erişiminin engellenmesinin ya da zorlaştırılmasının, sınırlanmasının mümkün olmadığını belirtmiştir. Ancak "kanıtları inceleme hakkı" ile özel hayata ilişkin "kişisel verilerin korunması hakkı" arasında bir dengenin kurulması gerektiği ifade edilerek kişisel veri niteliğindeki bilgi ve belgelerin, Anayasanın 20 inci maddesinin üçüncü fıkrası uyarınca davaya taraf olmayan başka kişilerin bilgi ve belgelere erişimine karşı korunması için örneğin bu belgelerin mühürlü zarf içine bulunması gibi önlemlerin alınması gerektiği belirtilmiştir. Bu itibarla Kararda yargılama faaliyeti kapsamında kişisel veri işlenmesi hali Kanun hükümlerinden istisna olmakla birlikte, haklar arasında denge kurulması yoluna gidildiği görülmektedir.

AİHM, kişisel verilerin yargılama sürecinde dava dosyasına eklenerek davanın tarafları haricinde duruşmaya katılan diğer kişilerin erişimine açık hale getirilmesini özel hayata saygı hakkına bir müdahale olarak değerlendirilmiştir. Bu durumda kişisel verilerin korunması hakkına ilişkin müdahalenin haklı bir nedene dayanıp dayanmadığını irdelemiştir. Örneğin AİHM Panteleyenko-Ukrayna kararında; davaya bakan hâkimin başvurucu kişinin ruh ve sinir hastalıkları hastanesinden bilgilerini temin ederek bunların duruşmada açıklanması ile ilgili olarak, söz konusu verilerin açıklanmasının davanın sonucunu etkilememesi ve soruşturma için önemli nitelikte bilgi olmaması gerekçesi ile ilgisiz bir bilgi olduğunu göz önüne alarak Sözleşme'nin 8 inci maddesinin ihlal edildiğine karar vermiştir (Panteleyenko v. Ukrayna, 2006, par. 61-62). Benzer şekilde, AİHM, L.L. Fransa kararında da dava dosyası içeriğinde sağlık verilerinin bulunmasına ilişkin olarak bu veriler dosyada bulunmadan da aynı sonuca ulaşılabileceğinden kişisel verilerin dosyada bulunmasının bu verilerin alenileştirilmesine neden olduğuna dikkat çekmiştir (L.L. v. Fransa, 2006, par. 46).

Mahkeme kararlarından anlaşılacağı üzere, yargı makamları yargılama esnasında elde ettiği kişisel verilere ilgisiz üçüncü kişiler tarafından erişilmemesine ilişkin gerekli önlemleri almakla yükümlüdür. Bu nedenle görülen davaya ilişkin dosyada davanın esasına etki etmeyecek kişisel verilere gerekli bulunmadıkça yer verilmemelidir (Ocak, 2020, s. 51).

Anayasa Mahkemesi de kararında; dava dosyası içeriğinde göğüs bölgesine ilişkin

fotoğrafların bulunması nedeniyle kişisel verilerine ilişkin gizlilik talebinde bulunan başvurucunun, söz konusu talebinin karşılanmamasını özel hayatın gizliliği hakkının ihlali olarak değerlendirmiştir. Karara konu olayda; mahkeme gerekli yapısal önlemler alınsa da davayı yürüten mahkeme tarafından verilen kararlarda üçüncü kişilerin müdahalelerine karşı kişilerin korunması imkânının sağlanmadığı durumda kişilerin hak ve özgürlüklerinin korunmasız bırakıldığına dikkat çekilmiştir (AYM, 2017, par. 59). Ek olarak, özel hayatın gizliliği hakkı bağlamında kişisel verilerin korunması hakkının gözetilmesinin gerekli olduğu hallerde yargı makamının gerekli önlemleri almaya ilişkin ödevinin bulunduğu, bu doğrultuda yargılamanın aleni yürütülmesine ilişkin kamu menfaati ile kişinin özel hayatının korunması menfaati arasında adaletli bir dengenin kurulması gerektiği ve hüküm kurulurken varılan sonuç hakkında yeterli ve ilgili gerekçelerin de sunulması gerektiği ifade edilmiştir.

Diğer taraftan Anayasa Mahkemesi birçok kararında memur ve kamu görevlilerinin kamu görevlerine atanmasında arşiv araştırması ve güvenlik soruşturması yapılmasına ilişkin kuralları değerlendirmiştir (Kararlar için bkz. AYM, 24/7/2019 tarihli ve E.2018/73, K.2019/65 sayılı, 19/2/2020 tarihli ve E.2018/91, K.2020/10 sayılı, 19/2/2020 tarihli ve E.2018/163, K.2020/13 sayılı, 3/6/2021 tarihli ve E.2020/24, K.2021/39 sayılı ile 16/12/2021 tarihli ve E.2020/41, K.2021/91 sayılı Kararlar). Söz konusu kararlarda kamu görevlileri ve memurların kamu görevine atanmasında bazı koşullara tabi tutulmasının gerekli olduğu, bir kamu görevine atanmadan önce ilgili kişiler hakkında arşiv araştırması ve güvenlik soruşturması yapılmasına yönelik kuralların kanun koyucunun takdir yetkisine bırakıldığı belirtilmiştir (AYM, E.2022/33, K.2022/67, 01/06/2022, par. 12). Ancak kuralda;

> *"güvenlik soruşturması ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler olduğuna, bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenleme" yapılmadığı, "elde edilecek verilerin kullanılmasına ilişkin temel ilkeler belirlenmeksizin kuralla sadece güvenlik soruşturması ve arşiv araştırması yapılması devlet memurluğuna alımda aranacak şartlar arasında sayılması"*

durumunun Anayasa'nın 13., 20. ve 128. maddeleriyle bağdaşmadığı tespit edilerek kuralın iptaline karar verilmiştir (AYM, E.2018/73, K.2019/65, 24/07/2019, par.171-173).

Kısmen İstisna Halleri

6698 sayılı Kanunun 28 inci maddesinin ikinci fıkrasında belirli koşullar altında Kanunun bazı maddelerinin uygulanmayacağı durumlar belirlenmiştir. Söz konusu maddede;

> *"Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla Kanunun veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddelerinin"*

sayılan hallerde uygulanmayacağı ifade edilmiştir. Bu anlamda kural olarak veri sorumluları maddede sayılan durumlarda kanun hükümlerine tabi olmakla beraber yalnızca sayılan maddeler açısından istisna tutulmaktadır. Diğer bir ifadeyle istisna tutulan maddeler haricinde Kanunda getirilmiş olan diğer yükümlülükler uygulanmaya devam edecektir. Ek olarak belirtmek gerekir ki sayılan maddelere ilişkin istisnalar kapsamında kişisel veri işlenmesinin ön koşulu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmaktır.

Bu doğrultuda kişisel verilerin işlenmesine ilişkin ilkeler Kanunun 4 üncü maddesinde yer almakta olup söz konusu madde;

a. "... (2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

b. Hukuka ve dürüstlük kurallarına uygun olma.

c. Doğru ve gerektiğinde güncel olma.

d. Belirli, açık ve meşru amaçlar için işlenme.

e. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

f. İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

hükmünü haizdir. Dolayısıyla kısmen istisna durumu mevcut olsa da veri sorumluları tarafından Kanunun amacına ve yukarıda yer verilen ilkelere uygun olarak kişisel veri işleme faaliyetinde bulunulması gerekir.

Kişisel Veri İşlemenin Suç İşlenmesinin Önlenmesi veya Suç Soruşturması İçin Gerekli Olması

6698 sayılı Kanun çerçevesinde kısmen istisna olarak belirlenen faaliyetlerden ilki;

> *"Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması"*

halidir. Söz konusu madde ile Kanundan tam istisna kapsamında sayılan hallerden olan

> *"kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi"*

hali ile benzerlik teşkil ettiği değerlendirilebilir. Ancak söz konusu kısmen istisna durumunda yalnızca "suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması" durumunda kişisel verilerin işlenmesi hali düzenlenmiş olup veriyi işleyen veri sorumlusunun "kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları" olma şartı aranmamıştır. Bu anlamda söz konusu madde kıyasen daha fazla sayıda veri sorumlusunu kapsamına aldığından yalnızca belirli maddeler açısından Kanun hükümlerinin uygulanmaması yoluna gidildiği değerlendirilmektedir.

Bu çerçevede, suç soruşturması veya suç işlenmesinin önlenmesi için gerekli olması halinde kişisel verilerin işlenmesi durumunda ilgili kişilerin aydınlatılması, ilgili kişinin kişisel verilerine ilişkin bilgi talep etmesi ve ilgili veri sorumlusunun Veri Sorumluları Siciline kayıt yükümlülüğü söz konusu olmayacaktır. Aynı zamanda belirtmek gerekir ki söz konusu kısmen istisna hükmü kendi içinde de bir sınırlamaya gitmiş, yalnızca "gerekli" olduğu ölçüde kişisel verilerin işlenmesi gerektiği hükme bağlanmıştır.

Bunlara ek olarak veri sorumlusunun Kanuna uygun şekilde kişisel verilerin işlenmesi ve temel ilkelere uyum, veri güvenliğine ilişkin yükümlülükleri, belirli şartların gerçekleşmesi halinde kişisel verileri yok etme, silme veya anonim hâle getirme gibi yükümlülüklerinin varlığı da devam etmektedir.

İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Kişisel Verilerin İşlenmesi

6698 sayılı Kanunda *"İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi"* hali kısmen istisna olarak sayılan durumlardan biridir. Ancak ilgili kişi tarafından alenileştirilmiş kişisel veri işlenirken ilgili kişinin alenileştirme iradesinin gözetilmesi gerekir. Diğer bir ifadeyle söz konusu kısmen istisna hali ilgili kişi tarafından alenileştirme yapılma amacı ile sınırlıdır. Örneğin ilgili kişi aracını satmak için telefon numarası bilgisinin kendi iradesiyle alenileştirdiyse, aracın satın alınması ile ilgili olarak işleme faaliyetinde bulunulması mümkündür. Fakat başka bir amaç için telefon numarası bilgisinin kullanılması halinde kısmen istisna halinden yararlanılması mümkün olmayacaktır (Kişisel Verileri Koruma Kurumu, 2019, s. 76. Alenileştirmeye ilişkin Kurul Kararı için bkz. Kurulun 30/06/2020 tarih ve 2020/508 sayılı Karar Özeti ve Kurulun 07/11/2019 tarihli ve 2019/331 Sayılı Karar Özeti).

Kişisel Veri İşlemenin Kanunun Verdiği Yetkiye Dayanılarak Görevli ve Yetkili Kamu Kurum ve Kuruluşları ile Kamu Kurumu Niteliğindeki Meslek Kuruluşlarınca, Denetleme veya Düzenleme Görevlerinin Yürütülmesi ile Disiplin Soruşturma veya Kovuşturması için Gerekli Olması

6698 sayılı Kanunda;

> *"Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması"*

durumunda, Kanunun belirtilen maddelerinden istisna tutulmuştur. İlgili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının yalnızca kişisel verilerin işlenmesinin "denetleme veya düzenleme görevlerinin yürütülmesi" ve "disiplin soruşturma veya kovuşturması" için gerekli olmasına ilişkin işlemleri kanunun belirtilen maddelerinden istisna tutulduğunu vurgulamak gerekir. Başka bir ifadeyle ilgili kurum ve kuruluşların yalnızca söz konusu işlemler haricindeki işlemleri için 6698 sayılı Kanunun tüm maddeleri uygulanmaya devam edecektir.

Örnek vermek gerekirse bir kamu kurumunda çalışan personel hakkında yürütülen idari soruşturma kapsamında ilgili kişinin verilerinin işlenmesi kısmen istisna kapsamında olup ilgili kişi hakkında diğer işlemler açısından istisna hali söz konusu değildir.

Kişisel Veri İşlemenin Bütçe, Vergi ve Mali Konulara İlişkin Olarak Devletin Ekonomik ve Mali Çıkarlarının Korunması için Gerekli Olması

Son olarak 6698 sayılı Kanunda;

> *"Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması"*

durumu sayılan kısmen istisna hallerinden biridir. Örneğin, Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması halinde görevleri aracılığıyla bilgi sahipleri veya bankalar veya finans kuruluşlarının mükelleflerin mali durumları ile ilgili bilgi vermeleri durumunda ilgili kişilerin aydınlatılması, ilgili kişinin kişisel verilerinin aktarılmasına dair bilgi talep etmesi ve ilgili veri sorumlusunun Veri Sorumluları Siciline kayıt yükümlülüğü söz konusu olmayacaktır.

AVRUPA GENEL VERİ KORUMA TÜZÜĞÜ ÇERÇEVESİNDE KİŞİSEL VERİLERİN KORUNMASI HAKKININ SINIRLANDIRILMASI AÇISINDAN 6698 SAYILI KANUNUN DEĞERLENDİRİLMESİ

6698 sayılı Kanun, Türkiye'nin uluslararası anlaşmaları çerçevesinde ve AB'ye uyum süreci gözetilerek hazırlanmıştır. Kişisel verilerin korunmasına ilişkin hukuki bir düzenleme yapılması ve bu hakkın korunmasına dair bağımsız ve denetleyici bir kurumun kurulması 108 Sayılı Sözleşme ve Sözleşmeye Ek Protokol'de yer almaktadır. Bu bağlamda 6698 sayılı Kanun; Avrupa Komisyonu tarafından imzaya açılan 108 sayılı Sözleşme ve 24 Aralık 1995 tarihinde kabul edilen 95/46/AT sayılı Yönerge esas alınarak hazırlanmıştır. Ancak 6698 sayılı Kanuna esas olan 95/46/AT sayılı Yönerge, 25 Mayıs 2018 tarihinde yerini Avrupa Genel Veri Koruma Tüzüğüne bırakmıştır. Bu nedenle AB'ye uyum sürecinde; günümüz itibariyle AB nezdinde kişisel verilerin korunmasına ilişkin güncel düzenleme olan Tüzük dikkate alınmalıdır.

Bu çerçevede kişisel verilerin korunması hakkına getirilen sınırlamalar açısından GVKT ile 6698 sayılı Kanun hükümleri karşılaştırıldığında; öncelikle GVKT uyarınca kişisel verilerin korunması hakkının sınırlandırılması için belirli koşulların sağlanması gerektiği anlaşılmaktadır. Bu çerçevede öncelikle sınırlamanın üye devlet tarafından yasal bir düzenleme ile öngörülmesi gerekmektedir. Ek olarak, sınırlandırma temel hak ve özgürlüklerin özüne saygı duymalı, demokratik bir toplumda gerekli ve orantılı bir önlem olmalıdır ve GVKT'nin 23 üncü maddesinin birinci paragrafında belirtilen gerekçelerden birini veya birkaçını güvence altına alma amacı ile gerçekleştirilmesi gerekmektedir. Bu amaçlar Tüzüğün 23.

maddesinde aşağıdaki şekilde sıralanmaktadır:

> *"a) ulusal güvenlik, (b) savunma, (c) kamu güvenliği, (d) kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların uygulanması, e) mali, bütçesel, vergilendirmeye ilişkin konular, kamu sağlığı ve sosyal güvenlik dahil olmak üzere, özellikle Birlik'in veya bir Üye Devletin önemli ekonomik veya mali menfaatleri gibi Birlik'in veya bir Üye Devletin genel kamu menfaatlerine ilişkin diğer önemli amaçları, (f) yargı bağımsızlığının ve adli süreçlerin korunması, (g) yasal düzenlemeye tabi mesleklerde etik ihlallerinin önlenmesi, soruşturulması, tespiti ve kovuşturulması, (h) (a) ila (e) ve (g) bentlerinde belirtilen durumlarda resmi yetkinin kullanılması ile bağlantılı olarak düzenli bir şekilde olmasa dahi izleme, denetleme veya düzenleme faaliyeti, (i) ilgili kişinin veya başkalarının haklarının ve özgürlüklerinin korunması, (j) medeni hukuktan kaynaklanan taleplere ilişkin kararların icrası"*

Dolayısıyla sınırlamanın gerekçesinin de iyi temellendirilmesi ve açıkça belirli olması öngörülür. Tüm bunlara ek olarak sınırlamalar, Bildirge'de ve Avrupa İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi'nde belirtilen gerekliliklere de uygun olmak zorundadır (GVKT, Resital 73). Diğer taraftan Üye devlet tarafından bu hakka getirilen sınırlandırmaya ilişkin kanunda bulunması gereken zorunlu unsurlara da GVKT'de yer verilmiştir. İlgili madde uyarınca hakka sınırlandırma getiren kanunda;

> *"(a) işleme veya işleme kategorilerinin amaçları, (b) kişisel veri kategorileri, (c) öngörülen sınırlamaların kapsamı, (d) kötüye kullanımı veya hukuka aykırı erişimi veya aktarımı engellemek için öngörülen tedbirler, (e) veri sorumlusu veya veri sorumlusu kategorilerine ilişkin belirleme, (f) işlemenin veya işleme kategorilerinin niteliği, kapsamı ve amaçları dikkate alınarak saklama süreleri ve uygulanacak güvenceler, g) ilgili kişilerin hak ve özgürlüklerine yönelik riskler ve (h) sınırlandırmanın amacı açısından sakınca teşkil etmedikçe ilgili kişilerin sınırlandırma hakkında bilgilendirilme hakkı"na*

ilişkin kurallara yer verilmesi gereklidir (GVKT, m. 23/2). Bu çerçevede GVKT uyarınca kişisel verilerin korunması hakkının sınırlandırılmasının hukuka uygun yapılabilmesi için yukarıda yer verilen gerekliliklerin sağlanması halinde kanunun ilgili kişilerin hakkını sınırlarken yine kişiyi güvenli ve sınırları belirli bir alanda tutacağına ilişkin güvenceler de içermelidir.

Öte yandan ülkemiz mevzuatı açısından kişisel verilerin korunması hakkına getirilen sınırlandırmalar değerlendirildiğinde bu hakkın varlığına ve sınırlandırılmasına ilişkin temel dayanak öncelikle Anayasada karşılığını bulmaktadır.

Anayasa'nın 20 nci maddesinin üçüncü fıkrasında;

> *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir."*

denilmek suretiyle hak, Anayasal güvenceye kavuşmuş ve bunun sonucu olarak temel hak ve hürriyetin sınırlanması açısından Anayasa'nın 13 üncü maddesi açısından hukuki bir koruma altına alınmıştır. Anılan madde uyarınca;

> *"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir."*

Aynı zamanda bu sınırlamaların *"Anayasanın sözüne ve ruhuna," "demokratik toplum düzeninin ve lâik Cumhuriyetin gerekleri"* ve *"ölçülülük ilkesi"*ne aykırı olmaması gerekmektedir.

Bu çerçevede, 6698 sayılı Kanun ile söz konusu temel hakkın kullanımı ve kapsamına dair esas ve usullere yer verilmiş, aynı zamanda Kanunun 28 inci maddesi ile hakkın sınırlandırılacağı hallere ilişkin konular da hükme bağlanmıştır. Anılan maddenin özellikle birinci fıkrasının Kanunda tam istisna halini düzenlemesinden dolayı bu fıkranın ayrıca dikkatle değerlendirilmesi gerekir.

Bu kapsamda Anayasa'nın 13 üncü maddesi gereğince hakkın "kanunla" sınırlandırılma ölçütünün karşılık bulduğu ifade edilebilir. Ancak temel bir hakkın sınırlandırılmasının kanunla yapılması zorunlu olmakla birlikte yeterli değildir. Buna ek olarak, hak sınırlandırılırken özüne dokunulmaması ve; *"Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesi"* ne de aykırı olmaması gerekmektedir. Dolayısıyla 28 inci madde ile kanunla sınırlandırılma ölçütü mevcut olsa da hakkın özüne dokunulmaması diğer bir ifadeyle hakkın kullanımının engellenmemesi, demokratik toplumun ve hukuk devleti olmanın gereği olan ek güvencelerin sağlanması, hak sınırlandırılırken gerekli, elverişli aynı zamanda yeterlilik ölçütünün sağlanması için ek düzenleme ve açıklamaların varlığına ihtiyaç duyulmaktadır. Bu anlamda yalnızca 28 inci maddenin varlığı bahsedilen ölçütleri sağlamakta yetersiz kalabilmekte dolayısıyla kişileri belirsiz ve sınırları belirli olmayan bir alanda bırakabilmektedir.

6698 sayılı Kanunun 28 inci maddesinde hakkın sınırlandırılmasına temel teşkil eden "konu"lara ilişkin hükümlere yer verilse de belirlenen konularda kişisel verilerin işlendiği tespit edildikten sonra öngörülen sınırlandırmanın kapsamı, sınırlandırmaya ilişkin ölçütler ve istisna hükmü kapsamında olup veri sorumlularınca işlenen kişisel verilerin hukuka aykırı erişimini, amacı dışında kullanımını, aktarımını önlemeye yönelik alınabilecek tedbirler konusunda herhangi bir hüküm içermemektedir.

Bu anlamda veri sorumlusu tarafından işlenen kişisel verilerin, Kanunun 28 nci maddesinin birinci fıkrasında olduğunun tespiti halinde ilgili kişiler, haklarını 6698 sayılı Kanun kapsamında ileri sürememekle birlikte kişisel verileri işleniyorken hangi verilerinin hangi veri sorumlusu tarafından işlendiği, işleme faaliyetinin kapsamı, amacı, işlenen verilerinin güvenliği, alınan tedbirler gibi hususlarda bir bilgi sahibi olmasına yönelik herhangi bir düzenlemeye veya sonradan bir düzenleme yapılmasına dair atıf bulunmamaktadır.

Bu minvalde 6698 sayılı Kanun, GVKT ile karşılaştırıldığında; GVKT'den farklı olarak Kanunun 28 inci maddesinin birinci fıkrasında belirtilen amaçlarda kişisel verilerin korunması hakkının sınırlanması haline dair maddeler yer alsa da ilgili maddelerde belirtilen hususlara açıklık getiren, istisnanın sınırlarını, kapsamını, güvenlik tedbirlerini belirleyen herhangi bir hüküm veya hükme atıf 6698 sayılı Kanunda yer bulmamıştır. Dolayısıyla kişilerin, Kanunun 28 inci maddesinin birinci fıkrası çerçevesinde kişisel verilerinin işlenmesi hususunda bir itirazını dile getirmesi halinde değerlendirilecek ölçütlerin mevcut olmaması durumu ile karşı karşıya kalınmamaktır.

Diğer bir ifadeyle ilgili kişilerin veri sorumlusuna karşı 6698 sayılı Kanunun 11 inci maddesinde yer alan haklarını ileri sürememesi ve 6698 sayılı Kanunun diğer hükümleri uygulama alanı bulamasa da kişilerin, Anayasanın da gereği olarak kişisel verilerin korunması hakkını kullanmasının engellenmemesi yani hakkının özüne dokunulmaması gerekir.

Dolayısıyla kişi 6698 sayılı Kanun çerçevesinde haklarını kullanmaktan geri bırakılsa da hakkının sınırlandırılma gerekçeleri, kişisel verilerine hukuka aykırı erişiminin engellenmesi vb. verilerinin güvenliği noktasında belirsiz, durumu meçhul bir alanda bırakılmamalıdır.

Bu minvalde söz konusu belirsizliklerin ortadan kaldırılması adına Anayasa'nın 13 üncü maddesinde yer aldığı üzere bir hakka getirilen sınırlamanın Kanunla yapılması şartı çerçevesinde; GVKT yer alan maddeye benzer şekilde, kişisel verilerin korunması hakkına sınırlandırma getiren kanunun, istisna haline münhasıran olarak düzenlenmesi ve ilgili kanunda hakkın sınırlandırılmasına ilişkin gerekçelerin açıkça belirtilerek istisna halinin kapsamının ve sınırlarının belirlenmesi, işlenen verilerin güvenliğine ilişkin alınacak önlemlerin belirtilmesi vb. düzenlemelere yer verilmesi suretiyle yapılmasının uygun olacaktır.

Diğer taraftan 6698 sayılı Kanunda yer alan kişisel verilerin korunması hakkına getirilen tam istisna maddeleri açısından değerlendirme yapıldığında; 6698 sayılı Kanun yürürlüğe girmesinden itibaren tartışmalara konu olan; *"kişisel verilerin soruşturma, kovuşturma yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi"* haline dikkat çekmek gerekir. AB düzeyinde söz konusu sınırlanma hallerine ilişkin GVKT'den ayrıca ve münhasıran bir düzenleme yapılması yoluna gidilmiştir.

Bu çerçevede, "Avrupa Parlamentosu ve Konseyi'nin 2016/680 Sayılı ve 27 Nisan 2016 Tarihli Kişisel Verilerin Yetkili Otoritelerce Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması veya Cezaların İnfazı Amacıyla İşlenmesiyle İlgili Gerçek Kişilerin Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin Yönerge" GVKT'nin yürürlüğe girmesine paralel olarak kabul edilmiştir.

Bu kapsamda GVKT, bireylerin kişisel verilerinin işlenmesi karşısında korunması ve kişisel verilerinin AB içinde serbest dolaşımı için "genel" düzenlemeler getirirken, 2016/680 sayılı Yönerge, cezai konularda adli ve kolluk iş birliğine ilişkin "özel" düzenlemeler getirmiştir. Dolayısıyla yetkili bir otoritenin, suçların tespit edilmesi, önlenmesi, soruşturulması veya kovuşturulması amaçlarıyla kişisel veri işlemesi halinde 2016/680 sayılı Yönerge uygulama alanı bulmaktadır. Bununla beraber Yönergenin uygulama alanı ulusal düzeyde kişisel verilerin işlenmesinin yanı sıra Üye Ülkelerin kolluk ve adli makamları arasında sınır ötesi işlemlerini, yetkili makamlar tarafından diğer ülkelere ve uluslararası kurumlara yapılan kişisel veri aktarımını kapsamaktadır (2016/680 sayılı Yönerge, Bölüm V.)

6698 sayılı Kanunda ise cezai ve adli konulara ilişkin 28 inci maddenin birinci fıkrasında iki istisna durumu düzenlenmiştir. Bunlar:

> *"kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi" ve "kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi"*

olarak ifade edilmiştir.

Söz konusu iki hal durumunda kişisel verilerin işlenmesi durumunda 6698 sayılı Kanun maddeleri uygulama alanı bulmayacaktır. Ancak söz konusu münhasır alanda hangi düzenlemenin uygulanacağına dair bir husus ulusal hukukta mevcut olmamakla birlikte kişisel verilerin söz konusu iki hükümde yer alan faaliyetler kapsamında işlenmesi halinde Kişisel Verileri Koruma Kurulu'nun yetkilerinin de belirsizliği söz konusudur. Dolayısıyla nicelik itibariyle en yoğun ve hassas nitelikteki kişisel verilerin işlendiği alanlar olan koruyucu, önleyici, istihbarı faaliyetler veya soruşturma, kovuşturma, yargılama faaliyetleri çerçevesinde kişisel verilerin işlenmesi durumuna ilişkin genel ilkeler, veri sorumlusunun yükümlülükleri, veri güvenliğine ilişkin tedbirler, söz konusu verilerin yurtdışına aktarımı gibi hususlarda ulusal mevzuatta düzenlemenin bulunmaması, ilgili kişilerin temel hak ve özgürlüğünün korunması adına gerekliliklerin sağlanamamasının yanı sıra uluslararası kuruluşlarla gerçekleşen adli ve cezai konularda veri aktarımı hususunda sorunlara ve eleştirilere sebep olabilmektedir.

SONUÇ

Hukuk sistemlerinde, kişilere temel bir hakkın tanınmasının önemi kadar hakka getirilen sınırlayıcı düzenlemeler ve bu düzenlemelerin yorumu da önem arz etmektedir. İstisna durumunun hukuk ile siyaset arasındaki dinamiklere göre şekil alan belirsiz bir alan olarak görülebilir. Ancak özellikle temel hak ve özgürlüklerin sınırlanmasına dair istisna halinin söz konusu olması durumunda "istisnalar dar yorumlanır" ilkesinin "hukuk"ta yerleşik bir ilke halini almıştır.

AB Genel Veri Koruma Tüzüğünün yürürlüğe girmesi ile AB nezdinde kişisel verilerin korunması hakkına getirilen sınırlandırmalara ilişkin olarak ortak bir düzenlemeye kavuşulmuştur. GVKT hükümleri uyarınca kişisel verilerin korunması hakkına getirilen sınırlamalar incelendiğinde; Tüzüğün 23 üncü maddesinde sayılan belirli amaçlarla ve aynı maddede belirtilen, sınırlayıcı düzenlemede bulunması zorunlu ve asgari nitelikteki unsurlara yer verilmek suretiyle üye devlet tarafından çıkarılan kanunla hakka sınırlama getirilebileceği düzenlenmiştir. Aynı zamanda AB nezdinde kişisel verilerin korunması alanında genel hükümler getiren Tüzüğün yürürlüğe girmesine paralel şekilde 2016/680 sayılı Yönerge ile cezai konularda adli ve polis iş birliğine yönelik özel düzenlemeler yürürlüğe girmiştir.

Öte yandan ulusal düzenlemeler açısından kişisel verilerin korunması hakkının sınırlandırılması incelendiğinde; Anayasanın 20 inci maddesinde eklenerek anayasal güvenceye kavuşturulan kişisel verilerin korunması hakkının, Anayasa'nın 13 üncü maddesinde belirlenen ölçütlerle sınırlandırılmasının mümkün olduğu AYM kararları ile ortaya konulmuştur. AİHM ve ABAD ile benzer şekilde AYM, içtihatlarında kişisel verilerin korunması hakkına sınırlandırma getirilirken hakkın özüne dokunulmaması, kanunla sınırlandırılması, demokratik toplum düzeninin gereklerine uygunluk ve ölçülülük ilkelerini gözetmiştir. AYM kararlarının bağlayıcılığı dikkate alındığında 6698 sayılı Kanunun 28 inci maddesinde yer alan istisna hükümleri değerlendirilirken AYM yorumları ve gözetilen ilkelerin de dikkate alınması gerekir.

Diğer taraftan 6698 sayılı Kanun hükümleri, AB Tüzüğü ile karşılaştırılarak değerlendirildiğinde, Tüzükten farklı olarak Kanunun 28 inci maddesinin birinci fikrasında belirtilen amaçlarda kişisel verilerin korunması hakkının sınırlanması haline dair maddeler yer almaktadır. Ancak maddede belirtilen hususlara açıklık getiren diğer bir ifadeyle istisnanın sınırlarını, kapsamını, güvenlik tedbirlerini belirleyen herhangi bir hüküm veya hükme atıf 6698 sayılı Kanunda yer almamaktadır. Dolayısıyla kişilerin, Kanunun 28 inci maddesinin birinci fikrası çerçevesinde kişisel verilerinin işlenmesi hususunda bir itirazını dile getirmesi halinde değerlendirilecek ölçütler açıkça bir hukuki düzenleme altına alınmamıştır. Bu minvalde, söz konusu belirsizliklerin ortadan kaldırılması adına Anayasa'nın 13 üncü maddesinde yer aldığı üzere bir hakka getirilen sınırlamanın kanunla yapılması şartı çerçevesinde; GVKT yer alan maddeye benzer şekilde, kişisel verilerin korunması hakkına sınırlandırma getiren kanunun, istisna haline münhasıran olarak düzenlenmesi ve ilgili kanunda hakkın sınırlandırılmasına ilişkin gerekçelerin açıkça belirtilerek istisna halinin kapsamının ve sınırlarının belirlenmesi vb. düzenlemelere yer verilmesi suretiyle yapılmasının uygun olacağı değerlendirilmiştir.

Ek olarak GVKT, bireylerin kişisel verilerinin işlenmesi karşısında korunması ve kişisel verilerinin AB içinde serbest dolaşımı için "genel" düzenlemeler içerirken cezai konularda kişisel verilerin işlenmesi ve adli ve polis iş birliğine yönelik olarak 2016/680 sayılı Yönerge ise "özel" düzenlemeler içermektedir.

Yoğun ve hassas nitelikteki kişisel verilerin işlendiği alanlar olan adli ve cezai faaliyetler kapsamında kişisel verilerin işlenmesi hali 6698 sayılı Kanunun 28 nci maddesi çerçevesinde Kanun kapsamı dışında tutulmaktadır. Bununla beraber bu alanlarda işlenen kişisel verilere özgü olarak hazırlanmış herhangi bir düzenleme mevcut değildir. Dolayısıyla ilgili kişilerin temel hak ve özgürlüğünün korunması adına gerekliliklerin sağlanamamasının yanı sıra uluslararası kuruluşlarla gerçekleşen adli ve cezai konularda veri aktarımı hususunda sorunlara ve eleştirilere sebep olduğu anlaşılmıştır.

Sonuç olarak kişisel verilerin korunmasına ilişkin olarak Türkiye'deki hukuki düzenleme ve uygulamanın, AB düzenlemelerine ve gerekliliklerine uygunluk açısından eksikliklerinin olduğu anlaşılmaktadır. Dolayısıyla Türkiye'nin, AB üyelik sürecinde AB hukuki düzenlemelerine uyumun sağlanması noktasında gerekli standartlara ulaşmayı amaçladığı dikkate alınırsa kolluk ve yargı organlarının faaliyetlerinde kişisel verilerin korunmasına ilişkin münhasır bir düzenleme yapılması yoluna gidilmesinin faydalı olacağı böylece kişilerin istisna maddelerinin uygulama bulduğu durumunda belirsiz ve sınırları belirli olmayan bir alanda bırakılmasının da engellenebileceği değerlendirilmektedir. Buna ek olarak 28 inci maddenin GVKT'de yer alan düzenlemelere benzer şekilde revize edilmesi halinde; kişisel verilerin korunması hakkı belli amaçlar dahilinde Kanunla sınırlanırken, bu sınırlandırmanın gerekçelerini açıkça ortaya koyan, hakkın kullanılmasını engellemeden ve kişileri hukuki güvenlik sınırları içinde tutan belirli kriterlerin oluşturulmasını da mümkün kılacağı kanaatine varılmaktadır. ◆

KAYNAKÇA

- 29. Madde Çalışma Grubu, Guidelines on consent under Regulation 2016/679, WP 259, 7 Haziran, 2018. Erişim: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf .
- Agamben, G. (2006). İstisna Hali. İstanbul: Otonom Yayıncılık.
- Avrupa Konseyi. (2018). Convention 108 + Convention for the protection of individuals with regard to the processing of personal data, Explanatory Report. Erişim: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 .
- Avrupa Veri Koruma Denetmeni (EDPS), "A Preliminary Opinion on data protection and scientific research". Erişim: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf
- Buttarelli, G. (2018). (EDPS) During the Fifth World Congress for Freedom of Scientific research, 12 Nisan 2018, s.2. (Erişim https://edps.europa.eu/sites/edp/files/publication/18-04- 12_fifth_world_congress_freedom_scientific_research_en.pdf 15.05.2022).
- Çengel, Y. (2012). Bilim ve Fen. Bilim ve Teknik Dergisi, Sayı 537, ss. 56-59.
- Kılınç, Ü. (2020). Avrupa İnsan Hakları Sözleşmesinde Sınırlamanın Dar Yorumu İlkesi. Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Sayı 2, ss.599-623.
- Krakov M. (2008). Ekonomik Güvenlik. Uluslararası İlişkiler, Cilt 5, Sayı 18, ss. 125-150.
- KVKK, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi.
- Ocak, A. (2020). İnsan Hakları Açısından Devlet Tarafından İşlenen Kişisel Verilerin Açıklanması. Ankara Baro Dergisi, Sayı 4, ss. 39-74.
- Resmi İstatistik Programı, 2022–2026. Erişim: https://www.resmiistatistik.gov.tr/detail/resmi-istatistik-programinin-kapsami-ve-uygulama-birimleri/https://ms.hmb.gov.tr/uploads/sites/3/2019/02/Resmi_istatistik_Programi_2012-2016Rev.2.pdf , 06.07.2022.

- Roagna, I. (2012). *Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması,* Avrupa Konseyi İnsan Hakları El Kitapları. Avrupa Konseyi.
- Serozan, R. (2011). Kişilik Hakkının Korunmasıyla İlgili Bazı Düşünceler. İstanbul Üniversitesi Mukayeseli Hukuk Araştırmaları Dergisi, Cilt 11, Sayı 14, ss.93-112.
- Serozan, R. (2015). Hukukta Yöntem. İstanbul: Vedat kitapçılık.
- Şimşek, O. (2008). Anayasa Hukukunda Kişisel Verilerin Korunması. İstanbul: Beta Yayınları.
- USA Department of Army. (2010). Department of Defense Dictionary of Military and Associated Terms, Joint Publication. Erişim: https://irp.fas.org/doddir/dod/jp1_02.pdf.
- Yılmazoğlu, Y. E., Perdecioğlu, İ. E. (2019). Türkiye Cumhuriyeti Anayasası (Gerekçeli). Ankara: Anayasa Mahkemesi Yayınları. (Erişim: https://www.anayasa.gov.tr/media/6382/gerekceli_anayasa.pdf, 05/05/2022).
- Yongalık, A. (2011). İstisnalar Dar Yorumlanır Kuralı ve Değerlendirilmesi. Ankara Üniversitesi Hukuk Fakültesi Dergisi, Sayı 60 (1), ss. 1-15.

Mahkeme Kararları

- ABAD, Birleştirilmiş davalar C-293/12 ve C-594/12, Digital Rights Ireland.
- ABAD, Birleştirilmiş davalar C-92/09 ve C-93/09 Volker und Markus Schecke, 9 Kasım 2010.
- ABAD, C-212-13, František Ryneš v. Úřad, 11 Aralık 2014.
- AİHM Rotaru/Romanya, B. N. 28341/95, 4/5/2000.
- AİHM, Aycaguer v. Fransa, No. 8806/12, 22 Haziran 2017.
- AİHM, B.B. v. Fransa, No. 5335/06, 17 Aralık 2009.
- AİHM, C-101/01, Bodil Lindqvist, 6 Kasım 2003.
- AİHM, Funke/Fransa, 25 Şubat 1992, 10828/84.
- AİHM, Gillow-Birleşik Krallık, No. 9063/80 9 Aralık 1992.
- AİHM, Handyside/Birleşik Krallık, B. No: 5493/72, 7/12/1976.
- AİHM, Klass ve diğerleri/Almanya, 6 Eylül 1978, 5029/71.
- AİHM, L.L. v. France, B.N. 7508/02, 10.10.2006.
- AİHM, Leander v. İsveç, No. 9248/81, 26 Mart 1987.
- AİHM, M.K. v. Fransa, No. 19522/09, 18 Nisan 2013.
- AİHM, M.M. v. Birleşik Krallık, No. 24029/07, 13 Kasım 2012.
- AİHM, Panteleyenko v. Ukrayna, B.N. 11901/02, 29.06.2006.
- AİHM, Peck v. United Kingdom, B. N. 44647/98, 28.01.2003.
- AİHM, Rotaru/Romanya, 5 Nisan 2000, 28341/95.
- AİHM, S. and Marper v. United Kingdom, B. N. 30562/04, 30566/04, 4.12.2008.

- AİHM, Sorguç v. Turkey Başvuru no 17089/03 23 Mayıs 2009).
- AİHM, X, Y, ve Z- Birleşik Krallık, (GC), 22 Nisan 1997.
- AYM, Nilgün Halloran Başvurusu, B. N. 2012/1184, 16/7/2004.
- AYM, Abdulkadir Tuncay Başvurusu, B.N. 2019/35343, K.T.30/03/2022.
- AYM, Abuzer Demir ve Aslı Peksezer Başvurusu, B. N. 2016/73556, K.T. 23/10/2019.
- AYM, B. K. Başvurusu, B. N. 2014/14189, K. T. 25/10/2017.
- AYM, Bestami Eroğlu Başvurusu, B.N. 2018/23077, K.T. 17/9/2020.
- AYM, E.2006/142, K.2008/148, K.T. 17/4/2008.
- AYM, E.2006/142, K.2008/148, K.T. 24/9/2008.
- AYM, E.2009/59, K.2011/69, K.T. 28/4/2011.
- AYM, E.2013/39, K.2013/65, 22/5/2013; AYM, E.2014/183, K.2015/122, 30/12/2015.
- AYM, E.2014/177, K.2015/49, 14/5/2015.
- AYM, E.2016/125, K. 2017/143, K.T. 28.9.2017.
- AYM, E.2018/73, K.2019/65, 24/07/2019.
- AYM, Emin Aydın Başvurusu, B. N. 2013/2602, K.T. 23/1/2014.
- AYM, Ercan Kanar Başvurusu, B. N. 2013/533, K. T. 9/1/2014.
- AYM, Ergün Poyraz (2) [GK], B. N. 2013/8503, 27/10/2015.
- AYM, Ferhat Üstündağ, B. N. 2014/15428, 17/7/2018.
- AYM, Güzide Defne Samyeli Başvurusu, B.N. 2014/4399, K.T. 21/9/2016.

◊ AYM, Halime Sare Aysal [GK], B. N. 2013/1789, 11/11/2015.

◊ AYM, İlhan Cihaner (2) Başvurusu, B.N. 2013/5574, K.T. 30.6.2014.

◊ AYM, Kadir Sağdıç Başvurusu B. N. 2013/6617, K.T. 8.4.2015.

◊ AYM, Mehmet Seyfi Oktay Başvurusu, B.N. 2013/6367, 10.12.2015.

◊ AYM, Nilgün Halloran Başvurusu, B. N. 2012/1184, 16/7/2004.

◊ AYM, Ö.N.M. Başvurusu, B. N. 2014/14751, 15/2/2017.

◊ AYM, Tuğba Arslan Başvurusu, B.N. 2014/256, K.T. 25.06.2014.

◊ KVKK, "Bazı avukatların avukat sorgulama siteleri ile ilgili ihbar başvuruları" hakkında Kişisel Verileri Koruma Kurulunun 30/06/2020 tarih ve 2020/508 sayılı Karar Özeti, Erişim: https://www.kvkk.gov.tr/Icerik/6877/2020-508.

◊ KVKK, "Hakkında hüküm verildiği suçtan dolayı cezası infaz edilen ilgili kişiye ait haberin yayımlandığı gazetenin internet sitesinden kaldırılması talebi" hakkında Kişisel Verileri Koruma Kurulunun 22/05/2020 tarihli ve 2020/414 sayılı Karar Özeti, Erişim: https://www.kvkk.gov.tr/Icerik/6915/2020-414, 12/08/2022.

◊ KVKK, "Hakkında hüküm verildiği suçtan dolayı cezası infaz edilen ilgili kişiye ait haberin yayımlandığı gazetenin internet sitesinden kaldırılması talebi" hakkında Kişisel Verileri Koruma Kurulunun 22/05/2020 tarihli ve 2020/414 sayılı Karar Özeti, Erişim: https://www.kvkk.gov.tr/Icerik/6915/2020-414, 10.08.2022.

◊ KVKK, "İlgili kişi anne ve ilgili kişi sıfatını haiz çocuğunun fotoğrafları da kullanılmak suretiyle ilgili kişi hakkında gerçek dışı, şeref ve haysiyet kırıcı bir televizyon haberi yapıldığı iddiası" hakkında Kişisel Verileri Koruma Kurulunun 02/12/2021 tarihli ve 2021/1217 sayılı Karar, Erişim: https://www.kvkk.gov.tr/Icerik/7271/2021-1217, 12/08/2022.

◊ KVKK, "İlgili kişi tarafından alenileştirilen kişisel verinin, alenileştirme amacı dışında işlenmesi" hakkında Kişisel Verileri Koruma Kurulunun 07/11/2019 tarihli ve 2019/331 Sayılı Karar Özeti, Erşim: https://www.kvkk.gov.tr/Icerik/6623/2019-331, 14/08/2022.

◊ Yargıtay 4. Ceza Dairesi, E:2016/1798, K:2016/5371, K.T. 21/03/2016.

◊ Yargıtay Hukuk Genel Kurulu, E.2014/56, K. 2015/1679.

İSTATİSTİKSEL AMAÇLAR DOĞRULTUSUNDA KİŞİSEL VERİLERİN İŞLENMESİ

Safiye PERGEL MAŞACIOĞLU

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "6698 sayılı Kişisel Verilerin Korunması Kanunu ve Avrupa Genel Veri Koruma Tüzüğü Kapsamında Arşivleme, Bilimsel Araştırma, Tarihi Araştırma ve İstatistiki Amaçlar Doğrultusunda İşleme Faaliyetine İlişkin Değerlendirme" başlıklı uzmanlık tezinden alınmıştır.

İstatistik Derneği'nin (Royal Statistical Society) 1834 yılında İngiltere'de kurulmasıyla beraber 'İstatistik' bir bilim dalı olarak kabul edilmiştir. Dernek tarafından istatistik bilimi "İnsanlarla ilgili olguları uygun bir şekilde göstermek için sayılarla ifade edilebilen genel kurallar" olarak ifade edilmiştir ("History", 2022). İstatistik sözcüğünün eskiden yalnızca 'veri' anlamına gelecek şekilde kullanıldığı düşünüldüğünde günümüzde bir bilim dalı olarak tanınması elbette önemlidir. Bugün verinin de ötesinde bir anlam kazanan istatistik, verinin yorumlanması ve ondan sonuç çıkarılması anlamında da kullanılmaya başlanmıştır. İstatistiğin bilim dalı olarak kabulünün ardından standart ögelere sahip olabilmesi adına 1853 yılında Brüksel'de birinci 'İstatistik Kongresi' düzenlenmiş ve sonraki yıllarda da bu kongrenin toplantılarına devam edilmiştir. Söz konusu kongreler ve konu ile ilgili dernekler 1885 yılında 'Uluslararası İstatistik Topluluğu'nun kurulmasına aracılık etmişlerdir (Akdeniz, 2013). İçerisinde bulunduğumuz çağın bilim ve teknoloji çağı gibi adlarla anılıyor olmasında büyük pay sahibi olan istatistik bilimi, yıllar içerisinde geliştirilen ve uygulayıcıları tarafından yaygın olarak kabul edilen standartları sayesinde; doğru, güncel ve güvenilir bilginin elde edilmesine hizmet etmektedir (Akdeniz, 2013; Özsoy, 2014).

Herhangi bir konu özelinde istatistiksel veri ihtiyacının giderilmesine ilişkin farklı yöntemler mevcuttur (Ayrıntılı bilgi için Bkz. "Determine Collection Method", 2022). Örneğin; "Doküman/kayıt incelemesi, anket, soru formu, test, görüşme, odak grup, gözlem, kontrol listesi, etnografya, sözlü tarih, örnek olay incelemesi ve deney" ("Veri Toplama Araçları", 2022) yaygın veri toplama yöntemlerinden yalnızca birkaçıdır. Söz konusu yöntemlerden bazılarının tanımlarına değinmek gerekirse; *verilerin tamsayım yöntemleri ile derlenmesi,* "Kitlede yer alan tüm birimlere ilişkin bilgi derlenmesi tamsayım yöntemi olarak adlandırılır. Kitleye ilişkin en küçük birim bazındaki bilgi tam sayım ile verilir. Ancak, kitlenin çok büyük olması, kitleye ilişkin değişimin çok hızlı gerçekleşmesi, zaman ve maddi olanakların çok kısıtlı olması durumunda tam sayım yönteminin uygulanması zorlaşmaktadır" ("İstatistik Üretiminde İdari Kayıtların Rolü", 2022), örneklem yöntemi ile bilgi derlenmesi, "Uygun örnekleme yöntemi ile kitledeki tüm birimlerin özelliklerini temsil edecek belli sayıdaki birimden derlenen bilgiler ile kitleye ilişkin tahminler elde edilmesine örneklem araştırmaları denir. Tam sayımın zorunlu olmadığı durumlarda veya belirlenen konuda en küçük birim bazında veri derlenmesine ihtiyaç duyulmaması durumunda örnekleme araştırmaları ile veri derlenir" ("İstatistik Üretiminde İdari Kayıtların Rolü", 2022) ve idari kayıtlardan bilgi derlenmesi, "Kurumların kendi iş ve işlemlerini yürütmek amacı ile tuttukları kayıtlar kullanılarak istatistik üretilmesidir. Bir idari kayıt istatistiksel kullanıma uygunsa istatistiksel veri kaynağı olarak kullanılır" şeklinde açıklanmaktadır ("İstatistik Üretiminde İdari Kayıtların Rolü", 2022). Tanımlarına yer verilen bu üç veri toplama yönteminin arasında çeşitli ölçütler çerçevesinde farklılıklar mevcuttur. Örneğin kapsam kümeleri bu farklılıklardan yalnızca biridir. Tamsayım yönteminde ilgili kitlenin tamamı, örneklem araştırmalarında ise bazen kitleden belirli bir kesimin kapsam dışında tutulduğu hal, idari kayıtlar vasıtasıyla veri toplandığı durumlarda ise hedef kitlenin idari ihtiyaçlarına göre kapsam kümeleri belirlenmektedir ("İstatistik Üretiminde İdari Kayıtların Rolü", 2022).

AVRUPA GENEL VERİ KORUMA TÜZÜĞÜ KAPSAMINDA KİŞİSEL VERİLERİN İSTATİSTİKSEL AMAÇLA İŞLENMESİ

Avrupa Genel Veri Koruma Tüzüğü (General Data Protection Regulation/GDPR) kapsamında istatistiksel amaçlarla veri işlenmesi, işlemenin birincil amacının istatistiksel çıktıların üretilmesi olan faaliyetleri ifade etmektedir. İşleme faaliyeti sonrasında bu istatistiksel verilerin bilimsel araştırma da dahil olmak üzere başka amaçlar için kullanılabilmesi mümkündür. Resmi istatistik üretme konusunda yasal yükümlülüğü olan kamu kurum ve kuruluşlarınca ve bunların dışında kalan özel kuruluşlar ile gerçek kişiler tarafından da istatistiksel amaçlarla kişisel veri

işlenebilmektedir. İstatistiksel amaçlarla veri işlenmesi, istatistiksel araştırmaların gerçekleştirilebilmesi ve istatistiksel sonuçların elde edilebilmesi için gerekli olan her türlü kişisel veri işleme faaliyetini kapsamaktadır ("Research Provisions", 2022). Recital'in 162. maddesi ("Recitals", 2022) ile istatistiksel amacın; istatistiksel amaçla veri işlenmesi sonucunun kişisel veri olmadığı toplu veri olduğu (Aggregate Data; toplu veri ifadesi özellikle büyük veri analizlerinde kullanılmaktadır ve anonim veri ile eşdeğer sayılmasına ilişkin tartışmalar mevcuttur. Zira söz konusu veri topluluğunun günümüz teknolojisi ile dahi işlenebilmesi neticesinde ilgili kişilerle ilişkilendirilebileceği değerlendirilmektedir. Ayrıntılı bilgi için Bkz. "Shedding light on the legal approach to aggregate data under the GDPR & the FDPR", 2022; Understanding aggregate, de-identified and anonymous data", 2022) ve bu işleme sonucunun veya kişisel verilerin gerçek kişiyle ilgili önlem veya kararların desteklenmesi için kullanımının mümkün olmadığı ifade edilmektedir. Dolayısıyla toplu verinin kişisel verinin karşıtı olduğu ve kişisel veri içermediği sonucuna varılabilmesi mümkündür ("The Role of Differential Privacy in GDPR Compliance", 2022). Avrupa Veri Koruma Komitesi (European Data Protection Board/EDPB) tarafından yapılan yayınlar ve duyurularda da toplu verinin kişisel veri içermeyeceği ifade edilmiştir ("Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak", 2022). Örneğin EDPB'ye ait çerez politikasında toplu verilerden elde edilmiş olan istatistiklerin hiçbir şekilde kişisel veri içermediği ifade edilmiştir ("EDPB Cookie Policy", 2022). Dolayısıyla toplu veri ifadesi anonim veri ile aynı anlama gelecek şekilde kullanılmaktadır ve gerçek bir kişiyle ilgili önlem ve kararların desteklenmesi için kullanılamamaktadır. Diğer taraftan Recital'in 162. maddesi kapsamında Avrupa Birliği (Birlik) veya Avrupa Birliği Üyesi Devlet (Üye Devlet) hukuku tarafından GDPR'nin sınırları içerisinde; istatistiksel içeriğin, erişim kontrolünün, kişisel verilerin istatistiksel amaçlarla işlenmesine ilişkin özel hallerin ve ilgili kişinin hak ve özgürlüklerini korumak ve istatistiksel gizliliği sağlamak için uygun önlemlerin belirlenmesi gerektiği ifade edilmiştir ("Recitals", 2022).

Kişisel veri işleme faaliyetinin istatistiksel amaçlarla gerçekleştirildiğinin varsayılabilmesi için veri sorumlusunun ya bu faaliyet neticesinde ortaya çıkan sonuçları insanlar hakkında karar veya önlem alınması adına kullanmaması ya da sonuçları artık kişisel veri olmaktan çıkarması ve anonim hale getirmesi gerekmektedir. Ancak anonimleştirilmiş sonuçlarla bağlantı kurulmasına aracılık eden bilgilere sahip olunması ilgili kişileri tekrar belirlenebilir kılabileceğinden gerçek anlamda bir anonimleştirmeden bahsedilemeyecektir. Bu veriler kişisel veri olacaklarından istatistiksel amaçla işlenme şartı gerçekleşmemiş olacaktır. Yine de bu veriler insanlarla ilgili karar veya önlem alınmasını haklı çıkarmak amacıyla kullanılmadıysa istatistiksel işleme geçerli olacaktır. Bilgi Komiserliği Ofisi (Information

Commissioner's Office/ICO) tarafından yayınlanan rehberde veri sorumlularına yol göstermesi amacıyla istatistiksel veri işlemeye ilişkin olarak; aktivitelere, çıktılara ve standartlara yer verilmiştir. Rehberde istatistiksel veri işleme amacıyla gerçekleştirilebilecek aktivitelere örnek olarak "-anket tasarlanması, -örnekleme popülasyonlarının hazırlanması, -verilerin yorumlanması ve analiz edilmesi, - örneklerden popülasyonlar hakkında çıkarımlar yapılması", çıktılara ilişkin olarak "-insanlar hakkında karar veya önlem alınması amacıyla kullanılmaması, -kişisel değil anonim veri kullanılması", standartlara ilişkin olarak "-halihazırda var olan politika ve prosedürlere uyumluluk, -konu ile ilgili davranış kurallara ve düzenleyici çerçevelere bağlı kalınması, -daha geniş bir araştırma projesinin parçası olunması halinde daha önce tanınmış araştırmada dürüst davranmayı düzenleyen standartlara uyum sağlanması" verilmiştir.

Yine ICO tarafından yayımlanan rehberde istatistiksel amaçla veri işlenmesine ilişkin olarak "Bir sağlık kuruluşu tarafından COVID-19 yeniden enfeksiyon oranlarının izlendiği, testi pozitif çıkan kişilerin kişisel verilerinin toplandığı, söz konusu verilerin önceki enfeksiyonla ilgili olduğu, verilerin yeniden enfekte olma oranlarının oluşturulması için istatistiksel amaçla kullanıldığı, başka kurumlar tarafından da bu verilerin gelecekte oluşabilecek yeniden enfeksiyon oranlarının belirlenmesi ve etkilerinin azaltılması amacıyla politika kararlarının alınması amacıyla kullanıldığı, bu işlemenin sonuçlarının anonim olduğu ve herhangi bir kişisel veri içermediği" örneği verilmiş ve her iki durumda da kişisel verilerin istatistiksel amaçla işlenmiş sayılacağı belirtilmiştir ("Research Provisions", 2022).

GDPR kapsamında resmi istatistik kavramına ilişkin açıklamalar Recital'in 163. maddesinde ("Recitals", 2022) yer almaktadır. İlgili maddede Birliğin ve ulusal istatistik kurumlarının resmi Avrupa ve resmi ulusal istatistiklerinin üretimi için topladığı gizli bilgilerin korunması gerektiği belirtilmiştir. Diğer taraftan, Avrupa istatistikleri, Avrupa Birliğinin İşleyişine İlişkin Antlaşmanın 338. maddesinin ikinci fıkrasında belirtilen istatistiksel ilkelere uygun olarak geliştirilmeli, üretilmeli ve dağıtılmalı, ulusal istatistikler de Üye Devlet hukukuna uygun olmalıdır. Avrupa Parlamentosu ve Konseyinin 223/2009 sayılı Tüzüğü (EC) ("Regulation (EC) No:216/2009 of the European Parliament and of the Council", 2022) Avrupa istatistikleri için istatistiksel gizlilik hakkında daha fazla özel hal içermektedir.

GDPR Kapsamında Kişisel Verilerin İstatistiksel Amaçlar Doğrultusunda İşlenmesi Faaliyetine İlişkin Güvenceler ve İstisnalar

GDPR'nin 89. maddesi; "1) Kamu yararına arşivleme, bilimsel veya tarihi araştırma ya da istatistiksel amaçlar doğrultusunda işleme faaliyeti, bu Tüzük uyarınca,

ilgili kişilerin hakları ve özgürlükleri için uygun güvencelere tabidir. Bu güvenceler, özellikle veri minimizasyonu ilkesine uygun hareket edilmesinin sağlanması amacıyla, teknik ve idari tedbirlerin uygulamaya konmasını sağlayacaktır. Bu tedbirler, söz konusu amaçların bu şekilde yerine getirilebilmesi koşuluyla, psödönimleştirmenin kullanımını içerebilir. Bu amaçların ilgili kişilerin teşhis edilmesine olanak tanımayan veya artık olanak tanımamaya başlayan ileri işleme faaliyetleri ile yerine getirilebildiği hallerde, söz konusu amaçlar bu şekilde yerine getirilir; 2) Kişisel verilerin bilimsel veya tarihi araştırma amaçları ya da istatistiksel amaçlar doğrultusunda işlendiği hallerde, Birlik veya Üye Devlet hukuku çerçevesinde, 15, 16, 18 ve 21. maddelerde atıfta bulunulan hakların spesifik amaçlara ulaşılmasını imkânsız hale getirmesinin veya ulaşılmasına ciddi şekilde zarar vermesinin muhtemel olduğu ve istisnaların bu amaçlara ulaşılması için gerekli olduğu ölçüde, bu maddenin 1. fıkrasında atıfta bulunulan koşullar ve güvencelere tabi olarak böylesi haklardan muafiyet sağlanabilir... 4) 2 ve 3. fıkralarda atıfta bulunulan işleme faaliyetlerinin aynı zamanda başka bir amaca hizmet ettiği hallerde, muafiyetler yalnızca bu fıkralarda atıfta bulunulan amaçlara yönelik işleme faaliyetine uygulanır." hükmünü amirdir.

Öncelikle belirtmek gerekir ki madde metni içerisinde düzenlenmiş bulunan dört işleme amacına (kamu yararına arşivleme, bilimsel veya tarihi araştırma ya da istatistiksel amaçlarla veri işlenmesi) ait bir tanım ilgili mevzuatta yer almamaktadır. Buna karşın maddeye ilişkin açıklayıcı nitelikteki gerekçe maddeleri Recital'in 156 ile 163. maddeleri ("Recitals", 2022) arasında düzenlenmiş olup söz konusu maddeler bağlayıcı olmasalar dahi içeriklerinde bu kavramlara ilişkin yol gösterici nitelikte açıklayıcı ifadeler barındırmaktadırlar. Her bir amaç esasen aynı zamanda tek bir amaca hizmet etmektedir ki o da "araştırma"dır. 89. madde başlığı ile beraber değerlendirildiği takdirde görülebilmektedir ki söz konusu düzenleme bünyesinde çeşitli muafiyetleri barındırmakta ancak bu muafiyetler aynı zamanda uygun güvenlik önlemlerinin alınması ile de sınırlandırılmaktadır. Öte yandan gerek ilgili kişinin hakları gerek GDPR'de yer alan veri koruma ilkelerinin tamamından değil de madde metni içerisinde atıf yapılan ilgili hükümlerden muafiyet sağlanması söz konusu düzenlemenin tam manasıyla GDPR'den istisna anlamına gelmediğini göstermektedir.

Dolayısıyla ilgili düzenlemenin istisnai bir veri işleme faaliyeti olarak adlandırılması terminolojik olarak uygun görülmemektedir. Kamu yararına arşivleme, bilimsel veya tarihi araştırma ya da istatistiksel amaçlar doğrultusunda kişisel veri işlenmesinin, bünyesinde veri koruma hukukuna ilişkin çeşitli muafiyetler içeren spesifik veri işleme amaçları olarak nitelendirilmesinin daha doğru olacağı değerlendirilmektedir.

Veri İşleme Şartı mı Amacı mı?

89. madde hem kapsamı bakımından araştırmacıları hem de mevzuatın uygulayıcıları konumunda olmalarından dolayı Üye Devletleri kapsamaktadır. Önemle belirtmek gerekir ki, maddenin veri işleme noktasında tek başına yasal bir temel oluşturduğu doğru bir görüşü yansıtmamaktadır (Svanberg, 2020; "Research Provisions", 2022). Zira, söz konusu haller veri işlemeyi hukuka uygun hale getiren GDPR'nin 6. maddesinde düzenleme altına alınan veri işleme şartları arasında yer almamakta olup yalnızca bu şartlara dayanılarak kamu yararına arşivleme, bilimsel veya tarihi araştırma ya da istatistiksel amaçlarla veri işlenmesi halinde belirli muafiyetlere imkân tanımaktadır.

Dolayısıyla 89. maddede düzenlenen amaçlarla veri işlenecek olması halinde yasal bir temele yani bir işleme şartına ihtiyaç duyulmaktadır. Örnek vermek gerekirse, arşivleme ve araştırma için potansiyel yasal dayanaklar arasında GDPR'nin 6. maddesinin birinci fıkrasının (f) bendinde düzenleme altına alınan veri sorumlusunun meşru menfaatinin yer alması mümkündür ("Research Provisions", 2022; "Secondary use of Personal Health Data: when is it "Further Processing" under the GDPR, and what are the Implications for Data Controllers?", 2022; "EDPB Documenton response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research", 2022).

Veri Koruma Direktifi (Data Protection Directive/DPD) ile Bağlantısı

Konuya DPD geçmişi ile de bakılmasının düzenlemenin geçirdiği değişikliklerin anlaşılmasına yardımcı olabileceği değerlendirilmektedir. DPD'de, GDPR'nin 89. maddesi ile paralel şekilde tarihi, istatistiksel ve bilimsel amaçlarla veri işlenmesine dair hükümler içermektedir. Özel nitelikli veri kategorileri bakımından ise 89. madde ile eşdeğer bir hüküm içermemiş olsa da uygun güvencelerin olması halinde özel nitelikli veri kategorisinde yer alan veriler bakımından kayda değer kamu yararı söz konusu ise 8. maddesinin dördüncü fıkrası gereğince veri işlenebilmesinin mümkün olacağını düzenleme altına almıştır. Burada kayda değer kamu yararı ifadesi özellikle dikkat çekmektedir. Uygulamada bu duruma ilişkin doğrudan bir düzenleme yer almamış, buna karşın 89. maddeye benzer şekilde ulusal düzenlemelerin yapılabilmesi mümkün kılınmıştır. İleri işleme haline ilişkin olarak da düzenlemeye yer verilmiş olup DPD'nin 29 sayılı gerekçesinde kişisel verilerin tarihi, istatistiksel veya bilimsel amaçlarla ileri işlenmesinin Üye Devletlerin uygun güvenlik önlemlerini almaları koşuluyla, genel olarak ilk baştaki veri işleme amaçlarıyla uyumsuz olarak kabul edilemeyeceği ifade edilmiştir. Bu bakımdan ileri işleme faaliyetinin de söz konusu şartların varlığı halinde mümkün olduğu söylenebilecektir (Svanberg, 2020).

Uygulamaya bakıldığında DPD, Üye Devletler arasında uygulama farklılıklarına yol açmaktadır (Örneğin; arşivleme yahut araştırma amacıyla kişisel veri işlemeyi düzenleyen ulusal nitelikli yasalar çoğu tıbbi araştırma ile ilgilenen birçok AB Üyesi devlette mevcuttur ancak DPD'nin uygulandığı bu ülkeler arasında veri koruma gereklilikleri noktasında önemli farklılıklar meydana gelmiştir). Dolayısıyla GDPR, yeknesak bir düzenleme ihtiyacı neticesinde oluşturulmuş ve çoğu konunun daha ayrıntılı düzenlemelerini içermektedir. Bu noktada belirtmek gerekir ki GDPR'nin genelinde rıza gibi konular DPD'ye göre daha sıkı bir şekilde düzenlenmiş olsa da arşivleme ve araştırma faaliyetlerine ilişkin DPD'den daha ayrıntılı bir muafiyet çerçevesinin çizilmiş olması bu durumu yumuşatmaktadır. Zira muafiyet içeren bir düzenlemeye detaylı bir şekilde yer verilmesi suretiyle rıza alınmaksızın veri işlenebilmesinin yolu açılmıştır. GDPR'nin müzakereleri esnasında kişisel verilerin bilimsel araştırma amacıyla işlenmesi esnasında ilgili kişinin açık rızasının (Explicit Concent için Bkz. "EDPB Documenton response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research", 2022) alınıp alınmaması konusu da tartışılagelmiştir. 29 Çalışma Grubu (Article 29 Working Party/WP 29) bu hususta ileri işlemeyi kıstas alarak, sağlık verilerinin tarihi, istatistiksel ve bilimsel araştırma amaçlarıyla 'ileri işlenmesi' durumuna yalnızca ilgili kişilerin açık rızasının alınması halinde veya çok belirli ve sınırlı istisnai hallerde izin verilmesi gerektiğini savunmuştur. Ancak bu görüş GDPR'de yer bulamamıştır (Svanberg, 2020).

Madde Hükmünün Uygulanma Şekli

Veri sorumlusu tarafından öncelikle gerçekleştirilecek veri işleme faaliyetinin GDPR'nin 89. maddesinde düzenlenen hangi işleme amacına hizmet ettiği belirlenmelidir. Tekrar belirtmek gerekir ki bu işleme amaçları, işleme şartları yerine geçmemektedir. Söz konusu maddede, AB yasa koyucusu tarafından uygun güvencelere tabi olması şartıyla özel olarak düzenlenen çeşitli işleme amaçları yer almaktadır. Kamu yararına arşivleme, bilimsel araştırma, tarihi araştırma ya da istatistiksel amaçlar için kişisel veri işlenmesi hallerine bu derece geniş bir muafiyet hali tanınmasının nedeni bu işleme amaçlarının toplum için önem arz etmesi ve mahiyetleri gereği kişisel veri işlenmeksizin gerçekleştirilemeyecek olmalarıdır. Söz konusu hüküm gereğince bu amaçlarla veri işlenmesi esnasında ilgili kişilerin hak ve özgürlüklerinin güvence altına alınabilmesi adına uygun güvencelerin gözetilmesi birinci fıkrasında zorunlu kılınmıştır. Belirtmek gerekir

ki, 89. maddede geçen kamu yararına ifadesi yalnızca arşivleme faaliyetini kapsamakta ve bu nedenle bilimsel veya tarihi araştırma ya da istatistiksel amaçlarla veri işlenmesi durumunda muafiyet kapsamında yer alabilmek için kamu yararı aranmamaktadır. Öte yandan hükmün ikinci ve üçüncü fıkralarında ise ilgili kişilere tanınan çeşitli hakların kullanılamayacağına ilişkin muafiyeti belirten düzenlemelere yer verilmiştir. Maddenin dördüncü fıkrası ise ikinci ve üçüncü fıkralarda belirtilen muafiyet hallerinin yalnızca bu fıkralarda yer verilen işleme amaçları bakımından geçerli olduğu ve başka herhangi bir amaç bakımından uygulama alanı bulunamayacağına ilişkindir (Svanberg, 2020).

Uygun Güvenceler

89. madde kapsamında kişisel verilerin kamu yararına arşivleme, bilimsel veya tarihi araştırma ya da istatistiksel amaçlar doğrultusunda işlenmesi halinde uygun güvenlik önlemlerinin alınması gerekliliği uygulayıcılar açısından bir kafa karışıklığı ortaya çıkarmaktadır. Uygulayıcılar açısından bakıldığında esas problem veri işlenip işlenemeyeceğinin ötesinde, hangi güvencelerin uygulanması gerektiğidir. Bu amaçlardan herhangi birinin ne ölçüde özel kuruluşlar tarafından yerine getirileceğine dair düzenleme yapma yetkisi ulusal mevzuatları kapsamında Üye Devletler'e bırakılmıştır. 89. madde kapsamında veri işleme faaliyeti gerçekleştirilecek veri işleme amaçları bakımından maddede sözü geçen işlemeye dair uygun güvencelerin neler olacağına dair belirleme yetkisi de Üye Devletler'e aittir (Svanberg, 2020; Ayrıntılı bilgi içi Recital no:156 Bkz. "Recitals", 2022).

Belirtmek gerekir ki bu hüküm ile amaçlanan özellikle GDPR'nin 5. maddesinin birinci fıkrasının (c) bendinde bahsi geçen kişisel verilerin "Yeterli, ilgili ve işlendikleri amaçla bağlantılı olarak gerekli olanlarla sınırlı." bir şekilde işlenmesi gerekliliğinin doğurduğu veri minimizasyonunun sağlanması adına teknik ve organizasyonel önlemlerin alınmasıdır. Veri minimizasyonunun sağlanabilmesi adına ilk olarak, araştırmanın kişisel veri işlenmeden yürütülüp yürütülemeyeceğine dair değerlendirme yapılmalıdır. Örneğin anonimleştirilmiş veriler ile araştırmanın gerçekleştirilmesi mümkünse kişisel veri işlenmemelidir. Bu bağlamda 156 sayılı Recital'de anonimleştirmeden bahsedilmekte olup 89. maddenin birinci fıkrasında "İlgili kişilerin tanımlanmasına izin vermeyen veya artık izin vermeyen 'ileri işleme'" hususunda yapılan atfin anonimleştirmeyi kast ettiği şeklinde bir yorum yapılabilmesi mümkündür (Svanberg, 2020). Ancak anonim verinin araştırma amacına hizmet etmemesi durumunda, illaki kişisel veri işlenecekse bu durumda ihtiyaç duyulan minimum kişisel veri miktarının belirlenmesi gerekmektedir. Buna karşın, ihtiyaç duyulduğu kadar bilginin işlenmesi gerekmekte olup daha sonra lazım olur zihniyeti ile fazlası işlenmemelidir ("What are the appropriate safeguards", 2022; "EDPB Documenton response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research", 2022).

Ek olarak 89. maddenin birinci fıkrasında psödönimleştirmeden de bahsedilmektedir. Anonimleştirmenin kullanılamadığı durumlarda psödönimleştirilen verinin kullanılıp kullanılamayacağı da değerlendirilmelidir. Gerçek kişinin veri kümesi içerisinden tanınmasını engelleyecek nitelikte tanımlanmayı sağlayan bilgilerin değiştirildiği veya kaldırıldığı teknikleri ifade eden psödönimleştirme, anonimleştirme ile asla aynı anlama gelmemektedir. Zira psödönim veri, anonim verinin aksine halen kişisel veridir ve veri koruma hukuku kuralları geçerlidir. Bunun sebebi ise psödönim veri kümesi içerisindeki verilerin anahtar kullanılmak suretiyle gerçek kişileri belirlenebilir kılabilecek olmasıdır. Bu nedenle her ne kadar madde içerisinde hangi güvencelerin uygulanacağına ilişkin detaylı bir liste yer almasa da 'anonimleştirme' ve 'psödönimleştirme' kullanımının bu güvencelerden olduğu söylenebilmektedir (Svanberg, 2020; "What are the appropriate safeguards", 2022; "EDPB Documenton response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research", 2022).

89. maddenin birinci fıkrasının en sonunda yer alan 'bu amaçlar bu şekilde yerine getirilecektir' ifadesi büyük ölçüde hangi amaçların izlendiğine bağlı olarak anonimleştirme ya da psödönimleştirmenin zorunlu olduğu algısını yaratabilmektedir. Ancak bu doğru bir yaklaşım olmayacaktır. Belirtmek gerekir ki veri işleme amaçları bakımından korunması için anonim hale getirilen veya psödönimleştirilen verilerin insanlar ve olaylar arasındaki bağı ortadan kaldırması neticesinde işlemenin amacına erişilmesini engelleyeceğinden pek mantıklı olmayacaktır. Anonimleştirme ve psödönimleştirme yöntemlerinin yalnızca işlemin amacını bozmayacağı durumlarda kullanılması gerekmektedir. Yalnızca bu tedbirlerin kullanılabileceği düşüncesi bir yanılgı oluşturmaktadır (Svanberg, 2020; "What are the appropriate safeguards", 2022). Dolayısıyla uygun önlemler işleme amacına bağlı olarak değişebilmektedir. Uygun güvenlik önlemleri ancak işleme amacı ile bağlamının birlikte değerlendirilmesi neticesinde belirlenmelidir ("What are the appropriate safeguards", 2022).

Özel Nitelikli Kişisel Veriler Bakımından

Özel nitelikli kişisel veriler bakımından GDPR'nin 9. maddesinin ikinci fıkrasının (j) bendi; "Gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve ilgili kişinin temel hakları ve menfaatlerinin güvence altına alınmasına

uygun ve belirli tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, 89(1) maddesi uyarınca kamu yararına arşivleme, bilimsel veya tarihi araştırma amaçlar ya da istatistiksel amaçlar doğrultusunda işleme faaliyetinin gerekli olması" hükmünü amirdir (Comandè ve Schneider, 2022). Yukarıda yer verilen hükümden de anlaşılabileceği üzere 9. madde kapsamındaki özel nitelikli kişisel verilerin hassas yapısı, söz konusu hükümde düzenleme altına alınan "Gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve ilgili kişinin temel hakları ve menfaatlerinin güvence altına alınmasına uygun ve belirli tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak" hükmü ile de vurgulanmaktadır (Svanberg, 2020; Comandè ve Schneider, 2022; "An overwiev of the Data Protection Act 2018", 2022).

Söz konusu hükmün uygulanabilmesi için ilk olarak veri işleme amacının GDPR'nin 89. maddesinin birinci fikrasında belirtilen amaçlardan biri ile ilgili olması gerekmektedir. Eğer arşivleme amacıyla işleme söz konusu ise burada arşivleme amacının kamu yararına olması yani bir kamu yararı amacını sağlıyor olması gerekir. Daha önce de bahsi geçtiği üzere yasa gereğince yalnızca arşivleme amacı söz konusu ise kamu yararı şartı aranmaktadır; bilimsel, tarihi araştırma ya da istatistiksel amaçların kamu yararına olması gerekmemektedir. İkinci olarak ise bu amaçların Birlik veya Üye Devlet hukukuna dayanması ve bunlara uygun olması gerekir. Örneğin, arşivleme veya bilimsel araştırma ile ilgili Üye Devlet yasaları gibi (Ancak burada söz konusu hukuki düzenlemelerin genel mi yoksa özel nitelikte mi olması gerektiği tartışmalıdır). Üçüncü şart gereğince ise işleme faaliyeti orantılı olmalı ve veri koruma hakkına saygı göstererek uygun ve özel güvenceler sağlanmalıdır. Bu bağlamda orantılılık verilerin kesinlikle ve yalnızca gerekli olduğu müddetçe işlenmesi anlamına gelir. Madde içerisinde geçen 'veri koruma hakkının özüne saygı duyulması gerektiği' ifadesi yasa koyucunun arşivleme ve araştırma faaliyetleri bağlamında bu hakların korunmasına verdiği önemi göstermektedir. İlgili kişinin temel haklarını korumak adına alınması gereken uygun ve özel önlemler ile ne kast edildiğine ilişkin bir açıklama ise mevcut değildir (Georgieva ve Kuner, 2020; Küzeci, 2021; Yağlıdere, 2022).

İleri İşleme Hali

'İleri işlemenin' söz konusu olması halinde eğer ileri işleme kamu yararına arşivleme, bilimsel veya tarihi araştırma ya da istatistiksel amaçlar doğrultusunda gerçekleştirilecekse 89. maddenin birinci fikrasına uyulması koşuluyla ilk işleme amacı ile bağdaştığı söylenebilecektir (Svanberg, 2020). "Kısacası bu hüküm araştırma amacıyla verilerin ileri işlenmesinde amaçlanan hususun; 89. maddede düzenleme altına alınan araştırma amaçlarından birine dayanması, bu araştırma

amaçlarından birinin gerçekleştirilmesi için gerekli olması, adil ve yasal olması ayrıca uygun güvenlik önlemlerini içermesi" halinde araştırma amacının baştaki işleme amacıyla uyumlu olduğu kabul edilir. Özellikle bir uyumluluk testi aranmamaktadır ("Research Provisions", 2022). Ancak bu doğrultuda 'ileri işleme' yapılabilmesi yine yasal bir işleme şartının varlığıyla mümkündür. Genel olarak araştırma amacıyla gerçekleştirilen işleme faaliyetlerinin işleme şartının temel olarak kamusal bir göreve (işlemenin kamu yararına bir görevin yerine getirilmesi veya kanunda açıkça yeri olan resmi görevler için) veya meşru menfaate (ilgili kişinin kişisel verilerinin korunmasının meşru menfaat ile elde edilebilecek çıkarları geçersiz kılabilecek iyi bir neden olmadıkça işlemenin veri sorumlusunun meşru menfaati açısından gerekli olması veya üçüncü bir tarafının çıkarlarının söz konusu olması durumunda) dayanılabilmesi mümkündür. Burada önemli olan işleme ile güdülen amaca hizmet edecek en doğru işleme şartını dayanak gösterebilmektir. Veri sorumlusunun kamu ya da özel hukuk statüsüne göre bu şartlardan hangisinin doğru bir seçim olacağı değişkenlik arz edecektir. Meşru menfaatin dayanak olarak gösterilmesi halinde genellikle veri işlemeye başlamadan önce bir meşru menfaat değerlendirmesinin yapılması gerekmektedir. Diğer taraftan tüm etik standartlara uyulması suretiyle düzenlemelerde yer alan gerekliliklere de uyularak uygun güvenlik önlemlerinin alınması neticesinde araştırma yapılması, meşru menfaat değerlendirmesinin içerdiği sorunların etkin bir şekilde giderilmeye çalışıldığı anlamına da gelebilmektedir. Meşru menfaate dayalı olarak bu koşullarda veri işlenmesi halinde veri sorumlusu tarafından söz konusu yasal dayanağın geçerli olduğuna güvenilebilmesi mümkündür ("Research Provisions", 2022; "Secondary use of Personal Health Data: when is it "Further Processing" under the GDPR, and what are the Implications for Data Controllers?", 2022; "Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak.", 2022).

Diğer taraftan belirtmek gerekir ki kişisel verilerin ilk işlenmesi esnasında yasal dayanağı rıza ise ileri işleme amacı ne olursa olsun her türlü yeni işleme faaliyeti için yeniden rıza alınması gerekmektedir. Bunun nedeni ise rızanın ilgili kişilere kişisel verileri üzerinde gerçek manada bir seçim ve kontrol hakkı tanıyor olmasıdır. Bundan dolayı da rıza her zaman spesifik ve bilgilendirilmiş şekilde gerçekleştirilmelidir. Ancak işleme faaliyetinin en başında rızaya dayalı olarak toplanmış olsa bile anonim veriler üzerinde araştırma yapılabilmesi mümkündür. Zira anonim veri söz konusu ise veri koruma mevzuatı uygulanmamaktadır. Üzerinde durulması gereken bir diğer husus ise 'geniş rıza'dır (Broad Consent için Bkz. "EDPB Documenton response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research", 2022). Geniş rıza, rızaya dayalı olarak kişisel verilerin bilimsel

araştırma amacıyla işlenmesi durumunda diğer işleme amaçlarında olduğu kadar spesifik bir şekilde rıza alınamama ihtimalinden ötürü geniş kapsamlı rıza alınabilmesi anlamına gelmektedir. Ancak geniş rıza alınıyor olsa dahi genel olarak araştırma alanlarının belirlenmesi gerekmektedir ("Research Provisions", 2022).

Saklama Süresinin Sınırlandırılması

GDPR'nin 5. maddesinin birinci fikrasının (e) bendi; "(e) ilgili kişilerin yalnızca kişisel verilerin işlenme amaçlarının gerektirdiği sürece belirlenmesini sağlayan bir şekilde saklanır; 89 (1) madde uyarınca yalnızca kamu yararına arşivleme, bilimsel veya tarihi araştırma amaçlarına ya da istatistiksel amaçlara yönelik işlendikleri sürece ve ilgili kişinin hak ve özgürlüklerinin güvence altına alınması için bu Tüzük uyarınca gereken uygun teknik ve idari tedbirlerin uygulanmasına tabi olarak, kişisel veriler daha uzun süreler boyunca saklanabilir (saklama süresinin sınırlandırılması)" hükmünü amirdir. Kişisel verilerin saklanmasına ilişkin genel kural gereğince, kişisel verilerin adil bir şekilde ve yasal olarak toplanılması ve kullanılması halinde dahi gerçekte işleme ile amaçlanandan daha fazla tutulmamaları sağlanmalıdır. Bir gün lazım olur düşüncesi ile süresiz bir şekilde depolama yapmak hukuka aykırıdır. Buna karşın yukarıda yer verilen madde 89. maddede düzenlenen amaçlar kapsamında saklama süresinin sınırlanması ilkesine ilişkin bir muafiyet tanımaktadır. Söz konusu hüküm gereğince kişisel verilerin kamu yararına arşivleme, bilimsel veya tarihi araştırma ya da istatistiksel amaçlar doğrultusunda işlenmesi halinde tabiri caizse süresiz olarak saklanabilmesi mümkündür. Ancak burada saklama niyeti verilerin tutulmasındaki yegâne amaç olmalıdır. Bu verilerin başka amaçlarla kullanılabilmesi amacıyla süresiz saklanması mümkün değildir. Diğer taraftan, araştırma amacı da dahil olmak üzere kişisel veriler artık herhangi bir amaçla işlenmiyorlarsa silinmeleri gerekmektedir ("Research Provisions", 2022; "EDPB Documenton response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research", 2022).

GDPR'nin 89/2 Maddesinin Atıf Yaptığı Hükümler

89. madde ile güdülebilen amaçlara ulaşılabilmesi adına aynı maddenin ikinci ve üçüncü fikralarında ilgili kişilerin bazı haklarının kullanımına ilişkin istisnalar tanınmıştır. İlgili kişilerin hak kullanımına ilişkin bu istisnaların uygulanması halinde dahi 89(1)'de düzenlenen korumalar halen geçerlidir. Buna ek olarak istisna uygulanıyor olsa dahi mevzuatta yer alan diğer hükümler de geçerliliğini koruyacaktır.

89(2) ve (3)'te yer alan istisnalar belirli koşullar altında uygulanmaktadırlar. Öncelikle 89(1)'in istisnai hal ne olursa olsun geçerli olduğu ve veri sahiplerinin hak ve özgürlüklerinin korunabilmesi adına uygun güvencelerin alınması gerektiği unutulmamalıdır. İkinci koşul ise istisna fikrasında yer alan haklar ancak "belirli amaçlara ulaşılmasını imkânsız hale getirmeleri veya ciddi şekilde engellemeleri halinde madde ile güdülen işleme amaçlarının yerine getirilmesi için gerekli olması durumunda" ilgili kişilerce kullanılamayacaktır. Bu nedenlerle, Üye Devletlerin istisnai hallerin kapsamını, yalnızca söz konusu hakların kullanılması halinde ilgili veri işlemenin imkânsız hale gelmesi veya ciddi şekilde bozması durumunda uygulanabileceği şeklinde daraltması gerekmektedir. Belirtmek gerekir ki istisnai haller yalnızca söz konusu madde ile hedeflenen işleme amaçları kapsamında geçerlidir. Örneğin bir şirket tarafından bilimsel araştırma yapıldığında bu faaliyet istisna kapsamında yer alacaktır ancak araştırma sonuçları ticari amaçlı kullanılacaksa istisna kapsamında sayılmayacaktır. Uygulamada ise bu ayrımı yapmak bu kadar kolay olmayabilir (Svanberg, 2020; "Research Provisions", 2022; "Exemptions", 2022).

Kısacası, GDPR'nin 89. maddesinin üçüncü fikrası gereğince; bilimsel veya tarihi araştırma ya da istatistiksel amaçlar doğrultusunda işlendiği durumlarda 15, 16, 18, ve 21. maddelerinde yer alan hakların bu işleme amaçlarının gerçekleşmesini imkânsız kılacağı yahut ciddi şekilde bozacağı hallerde bu hakların kullanımına ilişkin muafiyet tanınabilmesi mümkündür. Herhangi bir istisnai hal uygulanıyor olsa dahi 89. maddenin birinci fikrası gereğince ilgili kişinin hak ve özgürlükleri bakımından uygun güvenceler aranmalı ve özellikle veri minimizasyonu ilkesinin gerçekleştirilebilmesi adına teknik ve idari önlemler alınmalıdır (Gonzalez Fuster, 2020).

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA KİŞİSEL VERİLERİN İSTATİSTİKSEL AMAÇ DOĞRULTUSUNDA İŞLENMESİNE İLİŞKİN İSTİSNAİ DÜZENLEME

6698 sayılı Kanunun 28. maddesinde kanun hükümlerinin kısmen veya tamamen uygulanmayacağı hallere iki ana fikra altında sınırlı sayma metodu ile yer verilmiştir. Söz konusu maddenin birinci fikrasında sayılan; "a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi; b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi; c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik

haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi; ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi; d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi." durumlarında 6698 sayılı Kanun hükümleri uygulama alanı bulmayacaktır. Öte yandan "a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması; b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi; c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması; ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması." söz konusu ise 6698 sayılı Kanunun amacına ve yine kanunda düzenleme altına alınan temel ilkelerine uygun ve orantılı olmak kaydıyla aydınlatma yükümlülüğünün düzenlendiği 10. madde, ilgili kişinin haklarının düzenleme altına alındığı 11. madde (zararın giderilmesini talep etme hakkı hariç olmak üzere), veri sorumluları siciline kayıt yükümlülüğünün düzenlendiği 16. madde uygulanmayacaktır (Dülger, 2020).

Bu makale çalışmasının kapsamı bakımından incelenecek olan hüküm; istisna maddesinin birinci fıkrasının (b) bendinde düzenleme altına alınan; "b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi" hükmüdür. Söz konusu maddenin birinci fıkrasının (b) bendi gereğince kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi işlenebilmesi mümkündür (Kaya, 2020; Göçmen Uyarer, 2020; Küzeci, 2021).

6698 Sayılı Kanunun 28/1 Maddesinin (b) Fıkrasına İlişkin İnceleme

Bilindiği üzere, maddenin ilk fıkrasında belirtilen kişisel veri işleme faaliyetleri Kanunun kapsamı dışında kalmaktadır. Bir başka ifadeyle söz konusu kişisel veri işleme faaliyetlerinin gerçekleştirilmesi esnasında 6698 sayılı Kanun hükümleri uygulanmamaktadır.

6698 sayılı Kanunun 28. maddesinin birinci fıkrasının (b) bendi, "Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi." hükmünü amirdir. Madde gereğince kişisel

verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi esnasında Kanun hükümleri uygulanmayacaktır. Belirtmek gerekir ki madde metninin lafzından yola çıkmak suretiyle iki farklı yorumla karşılaşılmaktadır. Birinci yoruma göre madde metni gereğince; kişisel verilerin resmi istatistik yönteminin kullanılması suretiyle anonim hale getirileceği (bir anonimleştirme yöntemi olarak resmi istatistik yönteminin uygulanabileceği) ve kişisel verilerin bu yöntemle anonim hale getirilmesi halinde araştırma, planlama ve istatistik gibi amaçlarla işlenebileceği anlamı çıkmaktadır. İkinci bir yoruma göre ise; madde metni incelendiğinde dört farklı işleme amacını içerdiği görülebilecektir. Bunlar kişisel verilerin; resmi istatistik amacıyla işlenmesi, anonim hale getirilerek araştırma amacıyla işlenmesi, anonim hale getirilerek planlama amacıyla işlenmesi ve anonim hale getirilerek istatistik amaçlarıyla işlenmesidir. Hatta maddenin sonunda 'gibi' ifadesine de yer verilmiştir ki bu durum anonimleştirilmesi halinde kişisel verilerin başka amaçlarla da işlenebileceği anlamına gelebilmektedir (Dülger, 2020).

Söz konusu hükümde karışıklık yaratan olgunun; 'ile' bağlacının sözcüğün sonuna getirilerek birliktelik, beraberlik, araç, neden veya durum anlatan cümle oluşturmaya yarayacak şekilde değil de 've' tümlecinin içerdiği anlamla yani iki kelime veya iki cümle arasına girerek aralarında bir bağ olduğunu ifade eder şekilde kullanılıp kullanılmadığı hususu olduğu değerlendirilmektedir ("Büyük Türkçe Sözlük", 2022). Anlam karışıklığının giderilebilmesi noktasında ipucu vermesi adına 6698 sayılı Kanun Gerekçesi'ne göz atmak gerekmektedir.

6698 sayılı Kanuna ilişkin Tasarı (1/541) ve Adalet Komisyonu Raporu'nda da açıkça gözlemlenebilmektedir ki Tasarı'nın Adalet Komisyonu Raporu'na yer verilen 68. sayfasında *"...Alt Komisyon tarafından kabul edilen metnin 28'inci maddesi (Tasarının 28'inci maddesi), kişisel verilerin resmi istatistik amacıyla işlenebilmesine imkân tanınması ... amacıyla değiştirilerek kabul edilmiştir..."* ifadesi yer almaktadır. Dolayısıyla Alt Komisyon tarafından önerilen madde metninin ilk hali "Kişisel verilerin anonim hale getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi." iken adalet komisyonu tarafından söz konusu metin kişisel verilerin resmi istatistik amacıyla da işlenebilmesi adına "Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi." şeklinde değiştirilerek kabul edilmiştir.

İlgili hükümde istisna kapsamına alınan verilerin niteliğine dair herhangi bir ayrıma gidilmemiş olup madde metninde yer verilen amaç çerçevesinde işlenecek veriler özel nitelikli kişisel veriler olabileceği gibi özel nitelikli olmayan kişisel verilerden de oluşabilmesi mümkündür (Dülger, 2020).

Kişisel Verilerin Resmi İstatistik Amacıyla İşlenmesi

Yukarıda da bahsi geçtiği üzere 28. maddenin birinci fıkrasının (b) bendi kapsamında kişisel verilerin işlenmesi halinde bu işleme faaliyeti 6698 sayılı Kanun hükümlerine tabi değildir. Madde metninin neleri kapsadığının anlaşılabilmesi adına resmi istatistik kavramının irdelenmesinde fayda görülmektedir. Resmi istatistik kavramı, 5429 sayılı Türkiye İstatistik Kanununun (5429 sayılı Kanun) 2. maddesinin (g) bendinde, "Türkiye İstatistik Kurumu veya Programda yer alan konularda istatistik üretecek kurum ve kuruluşlar tarafından derlenen verilerin, kitle özelliklerini ortaya koymak amacıyla işlenmesi ile elde edilen bilgiyi," (5429 sayılı Türkiye İstatistik Kanunu, 1956) şeklinde tanımlanmıştır. Resmi istatistiğin oluşturulması esnasında kullanılan verilerin anketlerden elde edilebilmesinin yanı sıra idari kayıtlardan da üretilebilmesi mümkündür. Bu noktada anket ("Data Collection Methods: Some Tips and Comparisons", 2022; Ayrıntılı bilgi için Bkz. "Açık Veri Açık Bilim", 2022) hususunda malumun ilamına lüzum görülmemekteyse de idari kayıtların kapsamına nelerin girdiğinin açıklanması gerekmektedir. İdari kayıtlar genel olarak, "Devletin diğer kurum/kuruluşların gerek mevzuatlar çerçevesinde tutmakla zorunlu oldukları gerekse kurumsal hizmetlerin yürütülmesinde ihtiyaç duydukları konularda kişi, işletme veya olay bazında düzenlenen rapor, belge ve ölçüm türü gibi dokümanlar" anlamına gelmektedir.

Bu kayıtların aşağıda bahsi geçecek olan ilkeler çerçevesinde standardizasyonu neticesinde oluşturulan sistematik kayıt sistemleri, resmi istatistiksel verileri meydana getirmektedir. Mevzuatımız kapsamında 5429 sayılı Kanunun 9. maddesi gereğince TÜİK tarafından idari kayıtlara erişilebilmesi mümkündür ("RİP 2022-2026", 2022; Küzeci, 2021). İdari kayıt verileri doğrudan veya dolaylı olarak istatistik üretiminde, araştırmalarda, uzun dönemli bilgi kaynağı olarak ve araştırmanın değerlendirilmesinde kullanılabilmektedir (Ayrıntılı bilgi için Bkz. "İstatistik Üretiminde İdari Kayıtların Rolü", 2022).

5429 sayılı Kanunun 2. maddesinin (g) bendine ait metin incelediğinde temelde ardışık iki faaliyet göze çarpmaktadır. Bunlar verilerin derlenmesi ve işlenmesi neticesinde bilgi elde edilmesidir. Biraz daha açmak gerekirse; ilk olarak, Türkiye İstatistik Kurumu (TÜİK) veya veri derleme faaliyetinin gerçekleşeceği dönemi kapsayan Resmi İstatistik Programı (RİP) tarafından belirlenen konularda istatistik üretmekle görevli kurum ve kuruluşların bünyelerindeki verilerin derlenmesi (toplanması), ardından bu verilerin kitle özelliklerinin ortaya konulması amacıyla işlenmesi ve bu işleme faaliyeti neticesinde bir bilgi elde edilmesi gerekmektedir ki bu nihai bilgi resmi istatistik anlamına gelmektedir. Tanımdan da anlaşılacağı üzere resmi istatistik derlenen verilerin (ki bu derlemenin yukarıda

da ifade edildiği üzere anketlerden ve idari kayıtlardan elde edilebilmesi mümkündür) işlenmesi suretiyle elde edilmektedir ki işleme neticesinde istatistiksel sayılar yani veriler elde edilmektedir.

Resmi İstatistik Üretilmesi Esnasında Uyulması Gereken Bazı İlkeler

Resmi istatistik üretiminin disipline edilmesinin amaçlandığı RİP, resmi istatistik üretimi esnasında standardizasyonun sağlanması adına oluşturulmuştur. Bu kapsamda ihtiyaç konusu resmi istatistiğin tutulmasından sorumlu kurum ve kuruluşlar ile bunlar tarafından hangi verilerin hangi yöntemle ve hangi dönemler içerisinde tutulacağı ve bu verilerin yayın dönemleri belirli kılınmaktadır ("Resmi İstatistik Programı", 2022; "İdari Kayıtlar ve Kayıt Sistemleri", 2022).

Kurum ve kuruluşların resmi istatistik verisi işlerken uymaları gereken esasların temelini "Birleşmiş Milletler Ulusal Kalite Güvence Çerçevesi" ve "Avrupa Birliği Avrupa İstatistikleri Uygulama Esasları (Code of Practice- CoP)" ("RİP 2022-2026", 2022) oluşturmaktadır. 5429 sayılı Kanuna, Cop'a uyumun sağlanabilmesi adına gerekli düzenlemeler işlenmiştir. RİP kapsamında resmi istatistik üretimi esnasında Cop'ta yer alan ilkelere uyumlu davranılması zorunludur ve bu zorunluluktan dolayı resmi istatistik kapsamında veri işleyen tüm kurum ve kuruluşlar TÜİK'e karşı sorumludur.

Bu ilkeler; mesleki bağımsızlık, koordinasyon ve işbirliği, veri toplama ve veriye erişim yetkisi ("RİP 2022-2026", 2022), kaynakların yeterliliği, kalite taahhüdü, istatistiksel gizlilik ve veri güvenliği, tarafsızlık ve nesnellik, güvenilir metodoloji, uygun istatistiksel işlemler, cevaplayıcılar üzerindeki yükün azaltılması, maliyet etkinliği, uygunluk, doğruluk ve güvenilirlik, zamanlılık ve dakiklik, tutarlılık ve karşılaştırılabilirlik, erişilebilirlik ve açıklıktır ("RİP 2022-2026", 2022). Yukarıda yer verilen ilkelerden özellikle 'veri toplama ve veriye erişim yetkisi' ve 'istatistiksel gizlilik ve veri güvenliği' ilkeleri doğrudan 6698 sayılı Kanunun özünü yansıtan nitelikte ilkelerdir.

Veri toplama ve Veriye Erişim Yetkisi

Söz konusu ilke yukarıda daha önce bahsedilen resmi istatistik üretiminden sorumlu kurum ve kuruluşların bu amaçları doğrultusunda bilgi toplayabilmeleri adına yasal bir yetkiye sahip olmalarını ve bu yetkinin kanunla düzenlenmesi gerektiğini ifade etmektedir ve bu durum 6698 sayılı Kanunun veri işleme şartlarının düzenleme altına alındığı 5. maddesi kapsamında bir hukuka uygunluk hali anlamına da gelmektedir.

İstatiksel Gizlilik ve Veri Güvenliği İlkesi

İlke, resmi istatistik üretimi ile görevli kurum ve kuruluşların bu görevlerini yerine getirirken gizli verilerin güvenliğini sağlamak adına her türlü önlemi almaları anlamına gelmektedir. Resmi istatistiklerde veri gizliliğine ve gizli verinin güvenliğinin sağlanmasına ilişkin usul ve esaslar 'Resmî İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik' (Gizli Veri Yönetmeliği) kapsamında düzenleme altına alınmıştır. Gizli Veri Yönetmeliğinin 4. maddesinin birinci fikrasının (d) bendi gereğince gizli veri, "İstatistikî birimin doğrudan veya dolaylı bir şekilde sahip olduğu özellikleri ile birlikte tanınabilmesine ve bu şekilde bireysel bilgilerin açığa çıkarılmasına imkân sağlayan bireysel veya tablo hâlinde saklı tutulan veriyi" ifade etmektedir. Söz konusu Yönetmelik kapsamında; gizli verinin istisnaları, tablolaştırılmış verilerde gizliliğin sağlanması, kurum ve kuruluşlarca gizli verinin korunması ile tespitinin sağlanması, gizli/bireysel verinin paylaşım sınırı ile bu verilerin bilimsel amaçlı kullandırılması, personele ilişkin düzenlenen gizliliği sağlama taahhüdü, bilgi taleplerinin karşılanması, istatistiksel birimlerin hakları ve veri gizliliği ihtisas komisyonu da düzenleme altına alınmıştır.

Gizli Veri Yönetmeliği incelendiği takdirde özellikle 6698 sayılı Kanunun 'Veri Güvenliğine İlişkin Yükümlülükler' başlığına sahip 12. maddesinin barındırdığı gerekliliklere uygun düzenlemelerin yer aldığı tespit edilmektedir. Örneğin; 6698 sayılı Kanunun 12. maddesinin birinci fikrası gereğince, "Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." Gizli Veri Yönetmeliği'nin 7. maddesinin birinci fikrası da yukarıda yer verilen düzenleme ile aynı doğrultuda "Kurumların/kuruluşların yetkilileri, Programda belirtilen resmî istatistik çalışmalarının, gizli verilerin açıklanmasına imkân vermeyecek şekilde yürütülmesini sağlar, bu verilerin istatistikî amaç dışında kullanılmaması için her türlü önlemi alır ve istatistik üretiminin her aşamasındaki gizli verinin bulunduğu ortama yetkisiz kimselerin fiziksel veya elektronik yollarla erişiminin engellenmesi için gerek duyulan güvenlik sistemlerini belirler ve kullanır." şeklinde düzenlenmiştir.

Anonim Hale Getirilmek Suretiyle İstatistiki Amaçla Kişisel Verilerin İşlenmesi

İstatistiksel veri, bir derleme ve işleme faaliyeti neticesinde oluşmakta olup kişisel veri içerip içermeyeceği üzerinde uygulanacak analiz yöntemlerine göre değişebilmektedir. Resmi istatistik söz konusu olduğunda bu durum şansa bırakılmamış

ve işleme sonucunda elde edilen veri, kişisel veri içerse dahi Kanundan istisna kapsamında yer almıştır. Ancak resmi istatistik harici veri işlendiği hallerde bu durum kısıtlanmış ve işleme sonucu elde edilecek istatistiksel verinin kişisel veri içermesinin önüne geçilebilmesi amacıyla anonimleştirme şartı getirilmiştir.

Hedefe hizmet ettiği sürece toplanan kişisel verilerin anonim hale getirilmesi suretiyle kullanılması ve sonuca varılması mümkünse, 6698 sayılı Kanunun 28. maddesinin birinci fikrasının (b) bendi gereğince Kanundan tamamıyla muafiyet sağlanabilecektir. Halihazırda anonim veri söz konusu olduğunda 6698 sayılı Kanun zaten uygulanmayacaktır. Burada tam istisna kapsamına alınan halin kişisel verilerin toplanmasından anonim hale getirilmesine kadar olan süreci kapsadığı değerlendirmektedir. Aksi takdirde böyle bir düzenlemeye zaten ihtiyaç yoktur. Dolayısıyla, veri sorumlusunun istatistiksel amaçla topladığı kişisel verileri anonim hale getirmesi durumunda 6698 sayılı Kanun kapsamında istisnaya tabi olması mümkün olacağı düşünülmektedir.

Ancak burada üzerinde durulması gereken iki farklı husus söz konusudur. Bunlardan ilki veri sorumlusu tarafından toplanan verilerin anonim hale getirilmediği tespit edilirse ne olacağıdır. Diğer bir husus ise veri sorumlusunun topladığı verileri ne kadar sürede anonim hale getirmesi gerektiği noktasında ortaya çıkmaktadır. GDPR'nin 89. maddesi kapsamında istatistiksel amaçlarla veri toplanması halinde dahi ilgili kişinin çeşitli haklarından ve veri koruma mevzuatının bazı ilkelerinden muafiyet sağlanmaktadır. GDPR'nin diğer hükümleri ile bağlılık ise devam etmektedir. Ancak 6698 sayılı Kanun anonim hale getirmek suretiyle istatistik amaçlı veri işlenmesi halini tam istisna kapsamına almakta ve Kanunun tamamından muaf tutmaktadır. Dolayısıyla mevcut durumda GDPR düzenlemesi ile paralel bir şekilde ne olursa olsun uygun güvenlik önlemlerinin alınmasından söz edilebilmesi mümkün olmamaktadır.

Belirtmek gerekir ki 6698 sayılı Kanunun veri güvenliği noktasında, GDPR'nin 'aggregate data' algısından daha sağlıklı bir çözüm içerdiği değerlendirilmektedir. Zira daha önce de belirtildiği üzere, Recital'in 162. maddesi ("Recitals", 2022) istatistiksel amacın, istatistiksel amaçla veri işlenmesi sonucunun kişisel veri olmadığı toplu veri olduğunu ("Shedding light on the legal approach to aggregate data under the GDPR & the FDPR", 2022; Understanding aggregate, de-identified and anonymous data", 2022) ve toplu verinin kişisel verinin karşıtı olduğunu dolayısıyla kişisel veri içermediğini düzenlemektedir. Ancak yukarıda da bahsi geçen toplu veriye ilişkin dile getirilen çekinceler ışığında değerlendirildiğinde, istatistiksel verinin bu şekilde toplu veri olarak kabulünün ardından, ilgili kişilerle bağ kurabilecek teknolojilerin gelişmesi halinde, düzenlemenin ilgili kişi

ile ilişkilendirilememesi noktasında bir anlamının kalmayacağı değerlendirilmektedir. Dolayısıyla 6698 sayılı Kanun tarafından resmi istatistik faaliyetinin özellikle faaliyetin yoğunluğu da gözetilerek anonim hale getirme şartı aranmaksızın istisna kapsamında düzenlenmesi ve diğer planlama, araştırma ve istatistik amaçlarıyla veri işlenmesi hallerinin ise doğrudan anonim hale getirilmek suretiyle istisna kapsamında yer alacağına ilişkin ifade, gelecek teknolojilere yönelik olarak herhangi bir muğlaklığa yer vermemesi açısından önemlidir. Zira anonim hale getirme, 'aggregate data'dan daha kesin bir anlama sahip olup kişisel verinin hiçbir şekilde ilgili kişi ile bir bağ kurulamayacak hale getirilmesi anlamına gelmektedir. Buna karşın belirtmek gerekir ki gelişen yapay zekâ teknolojisi ve veri madenciliği tekniklerinin anonim hale getirmenin dahi güvenilirliğini ortadan kaldırabileceği değerlendirilmektedir. Ancak bu durum şimdilik bir soru işaretinden öteye geçmemekte yalnızca gelecek teknolojilere ilişkin endişe ve merak duygularını pekiştirmektedir.

SONUÇ

GDPR'nin 89. maddesi gereğince kişisel verilerin istatistiksel amaçlarla işlenmesi halinde ilgili kişilere tanınan bazı haklardan ve veri koruma hukukuna hâkim olan çeşitli ilkelerden muafiyetler sağlanmıştır. Bunlar; GDPR'nin 89. maddesinin doğrudan atıf yaptığı; ilgili kişinin erişim hakkının düzenlendiği 15. maddesi, düzeltme hakkının düzenlendiği 16. maddesi, işleme faaliyetini kısıtlama hakkının düzenlendiği 18. maddesi ve itiraz hakkının düzenlendiği 21. maddeleridir.

6698 sayılı Kanun'da ise GDPR'nin 89. maddesine benzer nitelikteki istisnai düzenlemelere 28. maddede yer verilmiştir. Maddenin birinci fikrası kanundan tamamen bağışık sayılan halleri düzenlemekte olup, ilgili maddenin birinci fikrasının (b) bendi gereğince kişisel verilerin resmi istatistik ile anonim hale getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi mümkündür. Söz konusu hüküm çerçevesinde veri işlendiği durumlarda 6698 sayılı Kanunun tamamından bağışıklık söz konusudur.

İstatistiksel amaçlarla veri işlenmesi, işlemenin birincil amacının istatistiksel çıktıların üretilmesi olan faaliyetleri ifade etmekte olup sonrasında bu verilerin bilimsel araştırma da dahil olmak üzere başka amaçlar için kullanılabilmesi mümkündür. Kamu kurum ve kuruluşlarınca ve özel kuruluşlar ile gerçek kişiler tarafından da istatistiksel veri işlenebilecektir. İstatistiksel amaçlarla veri işlenmesi, istatistiksel araştırmaların gerçekleştirilebilmesi ve istatistiksel sonuçların elde edilebilmesi için gerekli olan her türlü kişisel veri işleme faaliyetini kapsamaktadır. Recital'in 162. maddesi ("Recitals", 2022) istatistiksel amacın, istatistiksel amaçla veri işlenmesi sonucunun kişisel veri olmadığı toplu veri olduğu ve bu sonucun veya kişisel verilerin gerçek kişiyle ilgili önlem veya kararların desteklenmesi için kullanımının mümkün olmadığını ifade etmektedir. Dolayısıyla toplu verinin kişisel verinin karşıtı olduğu ve kişisel veri içermediği sonucuna varılmaktadır.

6698 sayılı Kanunun 28. maddesi gereğince kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesinde Kanun hükümleri uygulanmayacaktır. Madde metninin lafzı ile özünün birbirine uymadığı değerlendirilmiştir. Zira madde metninin lafzi olarak yorumlanması neticesinde; kişisel verilerin resmi istatistik yönteminin kullanılması suretiyle anonim hale getirileceği (bir anonim hale getirme yöntemi olarak resmi istatistik yönteminin kabul edildiği) ve kişisel verilerin bu yöntemle anonim hale getirildiği takdirde araştırma, planlama ve istatistik gibi amaçlarla işlenebileceği anlamı çıkmaktadır. Hükmün gai (amaçsal) yorumlanması netice-

sinde ise dört farklı işleme amacını ihtiva ettiği görülebilecektir. Bunlar kişisel verilerin; resmi istatistik amacıyla işlenmesi, anonim hale getirilerek araştırma amacıyla işlenmesi, anonim hale getirilerek planlama amacıyla işlenmesi ve anonim hale getirilerek istatistik amaçlarıyla işlenmesidir. Hatta maddenin sonunda 'gibi' ifadesine de yer verilmiştir ki bu durum anonimleştirilmesi halinde kişisel verilerin başka amaçlarla da işlenebileceği anlamına gelebilmektedir. Söz konusu hükümde yer verilen 'ile' bağlacının sözcüğün sonuna getirilerek birliktelik, beraberlik, araç, neden veya durum anlatan cümle oluşturmaya yarayacak şekilde değil de 've' tümlecinin içerdiği anlamla yani iki kelime veya iki cümle arasına girerek aralarında bir bağ olduğunu ifade eder şekilde kullanıldığı değerlendirilmektedir. Bu hal Tasarı'nın 68. sayfasında yer alan *"...Alt Komisyon tarafından kabul edilen metnin 28'inci maddesi (Tasarının 28'inci maddesi), kişisel verilerin resmi istatistik amacıyla işlenebilmesine imkân tanınması ... amacıyla değiştirilerek kabul edilmiştir..."* ifadesi ile de desteklenmektedir. Adalet komisyonu tarafından söz konusu Kanun Tasarısının ilk hali kişisel verilerin resmi istatistik amacıyla da işlenebilmesi adına "Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi." şeklinde değiştirilerek kabul edilmiştir. Söz konusu hükümde istisna kapsamına alınan verilerin içeriğine dair herhangi bir ayrıma gidilmemiştir. Bu veriler özel nitelikli kişisel veriler olabileceği gibi özel nitelikli olmayan kişisel verilerden de oluşabilmektedir.

6698 sayılı Kanunun veri güvenliği noktasında, GDPR'nin 'aggregate data' algısından daha sağlıklı bir çözüm içerdiği değerlendirilmektedir. GDPR kapsamında, istatistiksel verinin bu şekilde toplu veri olarak kabulü neticesinde ilgili kişilerle bağ kurabilecek teknolojilerin gelişmesi halinde, düzenlemenin ilgili kişi ilişkilendirilememesi noktasında bir anlamı kalmayacaktır. 6698 sayılı Kanun tarafından resmi istatistik faaliyetinin özellikle faaliyetin yoğunluğu da gözetilerek anonim hale getirme şartı aranmaksızın istisna kapsamında düzenlenmesi ve diğer planlama, araştırma ve istatistik amaçlarıyla veri işlenmesi hallerinin ise doğrudan anonim hale getirilmek suretiyle istisna kapsamında yer alacağına ilişkin ifadeye yer verilmesi gelecek teknolojilere yönelik olarak herhangi bir muğlaklığa yer vermemesi açısından önemlidir. Zira anonim hale getirme, 'aggregate data'dan daha kesin bir anlama sahip olup kişisel verinin hiçbir şekilde ilgili kişi ile bir bağ kurulamayacak hale getirilmesi anlamına gelmektedir. ◆

KAYNAKÇA

- Açık Veri Açık Bilim. (2022, 27 Eylül). Erişim adresi: https://acikveri.ulakbim.gov.tr/acik-veri-acik-bilim/bolum-2-arastirma-verisi-hazirlama-sureci/2-5-veri-toplamaaraclari/#:~:text=Veri%20toplama%20%C3%A7e%C5%9Fitli%20yollarla%20yap%C4%B1labilmektedir,4%2C %205%2C%206%5D.
- Akdeniz, F. (2013). İstatistikte Yeni Eğilimler ve Yöntemler. TÜİK İstatistik Araştırma Dergisi, 10(3), 35-48.
- An overwiev of the Data Protection Act 2018. (2022, 3 Ekim). Erişim Adresi: https://ico.org.uk/media/for-organisations/documents/2614158/ico-introduction-to-the-data-protection-bill.pdf
- Büyük Türkçe Sözlük. (2022, 21 Eylül). Erişim adresi: https://sozluk.gov.tr/
- Comandè, G. ve Schneider, G. (2022) Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think. German Law Journal, 23, ss.559-596)
- Data Collection Methods: Some Tips and Comparisons. (2022, 27 Eylül). Erişim adresi: https://www.nsf.gov/pubs/2002/nsf02057/nsf02057_4.pdf
- Determine Collection Method. (2022, 27 Eylül). Erişim adresi:http://toolkit.pellinstitute.org/evaluation-guide/collect-data/determine-collection-method/
- Dülger, M. V. (2020). Kişisel Verilerin Korunması Hukuku. İstanbul: Hukuk Akademisi.
- EDPB Cookie Policy. (2022, 7 Ekim). Erişim adresi: https://edpb.europa.eu/about-edpb/legal-notices/edpb-cookie-policy_en
- EDPB Documenton response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research. (2022, 6 Ekim). Erişim adresi:https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf.

◊ Exemptions. (2022, 3 Ekim). Erişim adresi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

◊ Georgieva, L. ve Kuner, C. (2020). Article 9. Processing of special categories of personal data. Kuner, C., Bygrave, L. A., Docksey, C. (Yay. haz.) The EU General Data Protection Regulation (GDPR) A Commentary içinde Oxford: Oxford University Press, Oxford.

◊ Gonzalez Fuster, G. (2020). Article 18. Right to restriction of processing. Kuner, C., Bygrave, L. A., Docksey, C. (Yay. haz.) The EU General Data Protection Regulation (GDPR) A Commentary içinde. Oxford: Oxford University Press, Oxford.

◊ Göçmen Uyarer, S. (2020). Kişisel Verilerin Korunması. Ankara: Seçkin, 2020.

◊ Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak. (2022, 6 Ekim). Erişim adresi: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.

◊ History. (2022, 28 Eylül). Erişim adresi: https://rss.org.uk/about/history/

◊ İdari Kayıtlar ve Kayıt Sistemleri. (2022, 28 Eylül). Erişim adresi:https://www.resmiistatistik.gov.tr/detail/subject/idari-kayitlar-ve-kayit-sistemleri/

◊ İstatistik Üretiminde İdari Kayıtların Rolü. (2022, 27 Eylül). Erişim adresi: https://www.tuik.gov.tr/Kurumsal/Istatistik_Uretiminde_Idari_Kayitlarinin_Rolu

◊ Kaya, M. B. (2020) "Büyük Veri Analitiği ve Kişisel Verilerin Korunması". Ertin, H. ve Sandıkçı, T. (Yay. haz.) Sağlık Alanında Büyük Veri içinde. İstanbul: İsar Yayınları.

◊ Küzeci, E. (2021). Kişisel Verilerin Korunması. İstanbul: Onikilevha.

◊ Özsoy, O. (2014). *İktisatçılar ve İşletmeciler İçin İstatistik.* Ankara: Siyasal Kitabevi.

◊ Recitals. (2022, 9 Eylül). Erişim adresi: https://gdpr-info.eu/recitals/

◊ Resmi İstatistik Programı.(2022, 26 Eylül). Erişim adresi: https://www.resmiistatistik.gov.tr/detail/genel-bilgiler/

◊ Regulation (EC) No:216/2009 of the European Parliament and of the Council. (2022, 29 Eylül). Erişim adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2009%3A087%3ATOC

◊ Research Provisions. (2022, 5 Ekim). Erişim adresi: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/research-provisions/

◊ RİP 2022-2026. (2022, 26 Eylül). Erişim adresi:https://www.resmigazete.gov.tr/eskiler/2021/12/20211231M5-1.pdf.

◊ Secondary use of Personal Health Data: when is it "Further Processing" under the GDPR, and what are the Implications for Data Controllers?. (2022, 6 Ekim). Erişim adresi: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4070716.

◊ Shedding light on the legal approach to aggregate data under the GDPR & the FDPR. (2022, 7 Eylül). Erişim adresi: https://unece.org/sites/default/files/2021-12/SDC2021_Day1_Podda_AD.pdf

◊ Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak. (2022, 7 Ekim) Erişim adresi: https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

◊ Svanberg, C. W. (2020). Article 89. Safeguards and derogations relating to processing for archiving purposes in the publiv interest, scientific or historical research purposes or statistical purposes. Kuner, C., Bygrave, L. A., Docksey, C. (Yay. haz.) The EU General Data Protection Regulation (GDPR) A Commentary içinde. Oxford: Oxford University Press, Oxford.

◊ The Role of Differential Privacy in GDPR Compliance. (2022, 7 Ekim). Erişim adresi:https://cpb-us-w2.wpmucdn.com/sites.gatech.edu/dist/c/679/files/2018/09/GDPR_DiffPrivacy.pdf

◊ Understanding aggregate, de-identified and anonymous data. (2022, 7 Eylül). Erişim adresi: https://www.comparitech.com/blog/information-security/aggregate-vs-anonymous-data/

◊ Veri Toplama Araçları. (2022, 28 Eylül). Erişim adresi:https://acikveri.ulakbim.gov.tr/acik-veri-acik-bilim/bolum-2-arastirma-verisi-hazirlama-sureci/2-5-veri-toplama-

◊ What are the appropriate safeguards. (2022, 5 Ekim). Erişim adresi:https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/the-research-provisions/what-are-the-appropriate-safeguards/.

◊ Yağlıdere, U. E. (2022). KVKK Kapsamında Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme. İstanbul: Platon Hukuk.

◊ 5429 sayılı Türkiye İstatistik Kanunu (1956, 4 Nisan). Resmi Gazete (Sayı: 25997). Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5429.pdf

KOLLUĞUN ÖNLEYİCİ FAALİYETLER KAPSAMINDA KİŞİSEL VERİ İŞLEMESİ

Rifat KARATAY

Kişisel Verileri Koruma Uzman Yardımcısı

"Bu çalışma 14.02.2023 tarihinde kabul edilen Karşılaştırmalı Olarak Kolluk ve İstihbari Faaliyetler Kapsamında Kişisel Verilerin İşlenmesi başlıklı uzmanlık tezinden alınmıştır."

GİRİŞ

Kişisel verilerin korunması 20. yüzyılda gerçekleştirilen uluslararası ve ulusal düzenlemeler ile hukuk sisteminin bir parçası haline gelmiştir. Günümüzde teknolojide yaşanan gelişmelerin de etkisiyle bu düzenlemeler artırılmıştır. Ulusal çapta ise başta 5237 sayılı Türk Ceza Kanunu, 12.09.2010 tarihli Anayasa değişikliği ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) ile kişisel verilerin korunması güvence altına alınmaya çalışılmış olup birçok mevzuat değişikliği ile de bu alana ilişkin düzenlemeler yapılmaya çalışılmıştır.

Kişisel veriler birçok faaliyet alanında kullanılmaktadır. Bu kapsamda, kişisel verilerin korunmasına yönelik gerçekleştirilen düzenleme ve denetleme görevlerindeki en belirgin ayrım kamu kurum ve kuruluşları ile özel kuruluşlar tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinde görülmektedir.

Avrupa Birliği Genel Veri Koruma Tüzüğü (GVKT) ve Kanun tarafından her iki kesim de düzenleme altına alınmaya çalışılmış olmakla birlikte, bazı durumlarda gerçekleştirilecek kişisel veri işleme faaliyetleri bu düzenlemelerden istisna

tutulmuştur. Ancak, her ne kadar söz konusu hususlar bu düzenlemelerden istisna tutulmuş olsa da evrensel hukuk ilkelerinin göz önünde bulundurulması neticesinde dürüstlük ilkesi çerçevesinde işleme faaliyetlerinin gerçekleştirilmesi gerekmektedir. Düzenlemelerden istisna tutulan alanlardan biri de yetkili makamların istihbari amaçla ve suçla mücadele amacıyla gerçekleştirmiş olduğu kişisel veri işleme faaliyetleridir.

AB'de, *"suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla yetkili makamlarca kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımı"* ile ilgili kişisel veri işleme faaliyetlerinde GVKT hükümleri uygulanmamakta olup bu alana yönelik 2008/977/Aİİ sayılı Konsey Çerçeve Kararı (Çerçeve Karar) yerine geçen 27 Nisan 2016 Tarihli 2016/680 Sayılı Avrupa Parlamentosu ve Konsey Direktifi (Direktif) yürürlüğe konulmuştur. Direktif ile yetkili makamların kişisel veri işlerken uyacakları usul ve esaslar belirlenerek hem ilgili kişiler açısından hem de veri sorumluları açısından bir düzen oluşturulmaya çalışılmıştır. Direktif'in AB üye ülkeleri tarafından uygulanabilmesi için iç hukuka aktarılması gerekmektedir. Fakat, iç hukuka aktarım sonucunda her ülkenin ulusal hukukunun bire bir aynı olmaması sebebiyle uygulamada sorunlar doğabileceği ifade edilmiştir.

Öte yandan Kanun, *"kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi ile kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi"* halini istisna tutmuştur. Yine, suç işlenmesinin önlenmesi veya ceza soruşturması için gerekli olması halinde veri sorumlusu, Kanunun 10, 11 ve 16 ncı maddelerinden muaf olacaktır.

Her ne kadar söz konusu faaliyetler Kanundan istisna tutulmuşsa da 2559 sayılı Polis Vazife ve Salâhiyet Kanunu, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu, 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu ve 5271 sayılı Ceza Muhakemesi Kanunu ile yetkili makamların görev alanlarıyla ilgili diğer kanunlarda kişisel verilerin işlenmesine ilişkin hükümlere yer verilerek kişisel veri işleme faaliyeti disiplin altına alınmaya çalışılmıştır. Ancak, AB'de yürürlüğe girmiş olan Direktif benzeri özel alana yönelik genel çerçeve oluşturan bir düzenleme henüz hukuk sistemimizde bulunmamaktadır.

Adli ve idari makamların etkin faaliyet gösterebilmesi için kişisel verilerin korunması alanında meydana gelen güncel gelişmelerin takip edilmesi gerekmektedir.

Zira Türkiye AB üyesi olmasa da üyelik süreci devam etmektedir. Suç ve suçlulukla mücadele, adli iş birliği sözleşmeleri ve ikili ilişkiler kapsamında AB üyesi devletlerden kişisel veri talep edildiğinde bu talebin karşılanması için kişisel verilerin korunması alanına yönelik faaliyetler gündeme gelmektedir.

27 NİSAN 2016 TARİHLİ 2016/680 SAYILI AVRUPA PARLAMENTOSU VE KONSEY DİREKTİFİ

AB hukukunun kaynakları birincil ve ikincil olmak üzere ikiye ayrılmaktadır. Birliğin kuruluş, işleyiş ve organlarına ilişkin temel kuralların yer aldığı kurucu antlaşmalar ile bunlar üzerinde değişiklikler öngören antlaşmalar birincil mevzuat olarak anılırken, birincil mevzuata dayanarak birlik organlarınca çıkarılan tüzük, yönerge, karar, tavsiye ve görüş gibi metinlerse ikincil hukuk kaynakları olarak adlandırılmaktadır (Özer, 2020). Direktifler ise ikincil kaynaklar arasında yer almaktadır. Bununla birlikte, bir direktifte bireylere haklar tanınıyorsa, bu hakların kullanılabilmesi için direktifin iç hukuka aktarılması gerekmektedir (Can, 2020). Çerçeve kararlar üye devletlerin hukuklarının uyumlaştırılmalarını sağlamak için düzenlenmiş olup bunlar direktiflerden farklı olarak üye devletlerin onaylamasına tabi değildir. Ancak, çerçeve kararlar doğrudan etki göstermemektedir. Bu sebeple, çerçeve kararlar, çerçeve kararlardan doğan haklar ve yükümlülüklerle ilgili bir durumu üye devlet vatandaşlarının mahkeme önüne getirme gücünü vermemektedir (Bozbayındır, 2018).

İkincil kaynaklar arasında yer alan Direktif *"suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla yetkili makamlarca kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımı"* ile ilgilidir. GVKT, belirtilen amaçlar çerçevesinde gerçekleştirilen kişisel veri işleme faaliyetleri için uygulanmamaktadır. Bu Direktif ile Çerçeve Karardaki ilkelerin üye devletlerin iç hukukuna aktarılması sağlanarak kolluk ve adli makamların aynı ilkeler kapsamında kişisel veri işleme faaliyeti gösterebilmesi amaçlanmıştır. Çerçeve Karar, cezai konularda üye devletlerin iş birliğini sağlamak için aktarılan veya aktarılmakta olan verilere ilişkindir. Bunun yanında, Çerçeve Kararın amacının, AB ve ABD'de gerçekleşen küresel terör eylemleriyle mücadele olduğu ifade edilmiştir (Can, 2020).

Söz konusu faaliyetlerin doğrudan bağlayıcı olmayan bir düzenleme olan direktif ile korunması, AB üye devletleri arasındaki cezai faaliyetlerde iş birliğine katkı sağlayacak kişisel verilerin kullanım amacından kaynaklanmaktadır. Böylelikle Direktif, yetkili makamlar arasındaki kişisel veri paylaşımını kolaylaştırmaktadır. Direktif kapsamındaki yetkili makamların bahsedilen amaçların dışında bir

hususa ilişkin görevlendirilmeleri halinde, söz konusu kişisel veri işleme faaliyeti GVKT kapsamında ele alınacaktır. Bununla birlikte belirtmek gerekir ki, yetkili makamlar ile sadece adli ve kolluk makamları kastedilmemekte olup Direktifin amaçları doğrultusunda kamu otoritesini ve kamu güçlerini kullanma yetkisine sahip herhangi bir makam yetkili makam olarak değerlendirilebilecektir.

Direktif, olması gereken ilkelerin önceden öngörülerek düzenlenmesi anlayışının bir ürünüdür (Mutlu, 2020). Direktifin temel iki amacı, *"gerçek kişilerin, başta kişisel verilerin korunmasına ilişkin hakları olmak üzere temel hak ve özgürlüklerini korunması ve ilgili mevzuat uyarınca kişisel verilerin yetkili otoritelerce paylaşılmasının gerekli olması durumunda, bu paylaşımın kişisel verilerinin işlenmesiyle ilgili gerçek kişilerin korunmasına ilişkin gerekçelerle sınırlandırılmaması veya yasaklanmaması"*dır. Böylelikle Direktif, özel hayatın gizliliğini aşar nitelikteki kolluk faaliyetleri ile kişisel verilerin korunması arasındaki dengeyi kurmaya çalışmaktadır. Direktif, ilgili alanı düzenlemekte olan Çerçeve Kararın kapsamını genişleterek kişisel verilerin, kamu güvenliğine karşı tehditlerin önlenmesi ile bu tehditlere karşı korunması amaçlı işlendiği hallerde de uygulanmaktadır. Yine, Çerçeve Kararın uygulanacağı alan değiştirilerek, Direktif, sınır ötesi kişisel veri işleme faaliyetleri dışında ulusal seviyedeki kolluk ve adli birimlerce yapılan işlemeler için de uygulanacak şekilde düzenlenmiştir. Kişisel verilerin üçüncü ülkelere aktarımına ek olarak uluslararası organizasyonlarla iş birliği ve bunlara aktarım da Direktif kapsamında düzenlenmiştir.

Üye devletlerden bazıları tek bir düzenleme ile bazıları ise birçok kanunda değişiklik yaparak Direktifi iç hukuka aktarmıştır (Kaya, 2019). EDPB, yayınlamış olduğu kılavuzda Direktifin yürürlüğe girmesinden bu yana gösterilen faaliyetler çerçevesinde Direktifin etkinliği konusunda değerlendirme yapılması için henüz erken olduğunu ifade etmiştir. Ayrıca, Direktifin iç hukuka aktarılması gerektiğinden üye devletlerin hukuk sistemlerindeki mevcut olan farklılıkların Direktif hükümlerinin farklı yorumlanmasına sebep olacağı da belirtilmiştir. Bu da AB açısından zorluklara sebep olabilecektir. Özellikle, Direktifin kapsamı ile Denetleyici Makamların yetkileri açısından zorluklarla karşılaşılabilecektir. Bununla birlikte, AB kurumlarına Direktif hükümleri uygulanmayacaktır. Yine, Denetleyici Makamların çoğunluğu Direktifin soruşturma faaliyetlerini güçlendirdiğini düşünmekte olup sekizi ise Direktifin, bu faaliyetlere ilişkin yetkileri kısıtladığını düşünmektedir. Ayrıca, yargılama faaliyetlerinin denetim dışı olması eleştirilmektedir (EDPB, 2021).

Direktifte, öncelikle üye devletlere ve onların yetkili ulusal makamlarına, kişisel verilerin işlenmesinin ve aktarılmasının gerekli ve orantılı olup olmadığına karar verilmesi hususunda geniş takdir yetkisi tanınmıştır. Bu yetki, veri işleme ve aktarma kategorileri arasında tutarsızlıklara yol açabilir. Ayrıca Direktifin uygulama alanı üye devletlerin adli mekanizmaları ile kendi tarih ve kültürlerine göre farklılıklar arz etmektedir. Buna ilaveten teknolojik yeterlilikleri ile polis ve adalet sistemlerinde yeni teknolojileri kullanma yaklaşımları AB üye ülkeleri arasında farklı uygulamaların da doğmasına neden olabilecektir (Bozbayındır, 2018).

Direktif, risk temelli yaklaşım, yeterli önlemlerin alınması, veri koruma etki değerlendirmesi, veri koruma görevlisi, tasarımdan ve başlangıçtan itibaren veri koruma müesseseleri açısından GVKT ile uyum içindedir (Can, 2020). Tasarımdan ve başlangıçtan itibaren veri koruma müessesesiyle veri minimizasyonuna da atıf yapılmıştır (EDPB, 2018). Kanunda ise risk temelli yaklaşım (KVKK, 2021), veri koruma etki değerlendirmesi ile tasarımdan ve başlangıçtan itibaren veri koruma müesseselerine yer verilmemiştir. Bununla birlikte, Kurumun resmi internet sitesinde yayınlanan 10.12.2021 tarihli "Veri Koruma Görevlisi Hakkında Kamuoyu Duyurusu"nda, kazanılacak olan unvanın kamuoyunda GVKT'de bahsi geçen görev, yetki ve sorumlulukları tanımlanan veri koruma görevlisi ile karıştırıldığı belirtilmiştir. Bu kapsamda, hukuk sistemimizde yer alan veri koruma görevlisi programına ilişkin düzenlemenin Direktif ile tam olarak örtüşmediği anlaşılmaktadır. Diğer taraftan, risk temelli yaklaşımların ve yeterli önlemlerin alınmasının Kanunun 12 nci maddesinde yer alan veri güvenliğine ilişkin yükümlülükler ile aynı mahiyette olduğu değerlendirilmektedir.

Bu noktada belirtilmesi gereken bir diğer konu, Direktif benzeri bir düzenlemeye henüz iç hukukumuzda yer verilmemesinin uluslararası alanda yaratabileceği sorunlardır. Ülkemizde faaliyet gösteren kolluk birimleri Kanun ve tabi oldukları yasal düzenlemeler çerçevesinde faaliyet göstermektedir. AB hukuku ile iç hukukumuz arasındaki farklılıklar Türkiye'nin karşılıklı kişisel veri paylaşımlarına engel oluşturabilmektedir. Türkiye ile Europol arasında 2004 yılında kişisel veri paylaşımına imkân veren anlaşma yerine teknik ve stratejik düzeyde iş birliği anlaşması imzalanmış olup kişisel veri paylaşımına imkân veren anlaşma, o dönemde Türkiye'nin 108 No'lu Sözleşmeye taraf olmaması sebebiyle imzalanamamıştır. Bu durum Europol ile Türkiye arasında veri aktarımını engellemiştir (Can, 2020).

Diğer taraftan, ulusal güvenlik amacıyla kişisel verilerin işlenmesine ilişkin Direktifin resital kısmında yer alan 14 numaralı maddede, Direktifin, AB hukuku kapsamı dışında kalan kişisel veri işleme faaliyetlerini kapsamadığı belirtildiğinden, ulusal güvenlikle ilgili faaliyetlerde Direktif hükümlerinin uygulanmayacağı belirtilmiştir (Kaya, 2019). Bu çerçevede, ulusal güvenliğin Direktif kapsamı dışında bırakılması sebebiyle, istihbari faaliyetlere ilişkin kişisel veri işleme faaliyetlerin-

de Direktif hükümleri uygulanmayacaktır (Can, 2020). Ancak, üye devletlerden biri, ulusal güvenlik alanında da Direktifin uygulandığını ve ulusal güvenlik ile ilgili işlenen kişisel verilerin ayrı bir dosyalama işlemine tabi tutulması gerektiğini ifade etmiştir (EDPB, 2022).

Konsey çerçevesinde kabul edilen düzenlemeler, AB hukukunun aksine ulusal güvenlik alanında da uygulanmaktadır (Bozbayındır, 2018). Bu sebeple, İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşmenin "Özel ve aile hayatına saygı hakkı" başlıklı 8 inci maddesinde yer alan hükümler ulusal güvenlik alanında da uygulanacaktır (EDPB, 2022). AİHM, bu alanda vermiş olduğu ilk önemli kararda ("Klass and Others v. Germany, 5029/71, 06.09.1978".) kişisel veri kavramını kullanmamakla beraber kişiye ilişkin bilgilerin gizli izleme yöntemleriyle toplanması konusunu ele almıştır. AİHM,

> *"istihbarat örgütlerinin gizli izleme yoluyla bireylerin haklarına yönelik gerçekleştirdikleri müdahalelerin etkili bir denetime tabi olması gerektiğini kabul etmiş ve ulusal güvenlikten kaynaklanan ihtiyaçlara her durumda öncelik verilemeyeceğini, AB ülkelerinin casusluk ve terörizmle mücadeleyi gerekçe göstererek uygun gördükleri her türlü tedbiri alamayacaklarını açıklamıştır. Davada, mektupların ve telgrafların okunmasına, telefon görüşmelerinin dinlenmesi ve kaydedilmesine olanak tanıyan bir yasanın AİHS'ye uygunluğunu incelemiştir. AİHM genel olarak gizli izleme yöntemlerine demokratik kurumların korunması için kesinlikle zorunlu olması durumunda başvurulabileceğini kabul etmiş, ancak, bireyin 8 inci maddede güvence altına alınan hakkı kullanabilmesi ile demokratik bir toplumu koruma amacıyla gizli izlemenin yapılmasının gerekliliği arasında bir denge kurulması gerektiğini" belirtmiş olup, "bu konuda devletlerin sınırsız bir takdir yetkisi yoktur. Sınırsız önlemler alınmasına izin veren bir yasa demokrasi için tehdit oluşturur. Gizli izlemeye olanak tanınması durumunda bunun kötüye kullanılmasının engellenmesi için yeterli ve etkili güvencelerin sağlanması gerekir. İzleme ancak başka bir yöntemle bilgilere ulaşılamıyorsa yapılmalı, yazılı izin şartı aranmalı ve belli bir süreyle sınırlı tutulmalıdır. İzlemeyi gerektiren nedenlerin ortadan kalkması durumunda izlemeye son verilmeli, elde edilen veriler başka bir amaç için kullanılmamalı, izlemenin amacının gerçekleşmesi durumunda veriler en kısa süre içinde imha edilmelidir."*

açıklamasına yer vermiştir (Atak, 2010).Yine, ABAD'ın kişisel verilerin işlenmesine ilişkin bireylerin korunmasına ve bu verilerin serbest dolaşımına dair kuralların, sınır ötesi boyutu olsun ya da olmasın güvenliğe ilişkin olması halinde de, uygulanması gerektiği yönünde birçok kararı bulunmaktadır (Bozbayındır, 2018).

Diğer taraftan, Direktifte suç tanımı yapılmamıştır. Kabahatlere ilişkin Direktifin uygulanıp uygulanmayacağı da metinden anlaşılamamaktadır. Bununla birlikte, suç kavramı ABAD tarafından yorumlanacağı için yaptırım belirlenirken, ABAD ile AİHM'nin içtihatlarının dikkat alınması gerektiği belirtilmiştir. Keza ABAD, fiilin suç ya da kabahat teşkil edip etmediğini tespit ederken AİHM kriterlerini esas almaktadır (Can, 2020).

Kanunun 28 inci maddesinin ikinci fikrasının (c) bendi kapsamında, Kurumun yayınlamış olduğu rehberde de *"Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) ile Radyo ve Televizyon Üst Kurulu (RTÜK) gibi düzenleyici denetleyici kurumların; kanunun verdiği yetkiye dayanılarak denetleme veya düzenleme görevlerinin yürütülmesi"* açıklamalarına yer verilmiştir (KVKK, 2019). Uygulamamızda 6112 sayılı Radyo ve Televizyonların Kuruluş ve Yayın Hizmetleri Hakkında Kanununda, idari para cezası yaptırımı öngörülmüş olup bu kapsamda RTÜK tarafından gerçekleştirilecek denetim yetkisi kapsamında tespit edilecek kabahatlere ilişkin gerçekleştirilecek faaliyetlerin kısmi istisna kapsamında olduğu, böylelikle sadece Kanunun 10, 11 ve 16 ncı maddelerinin uygulanmayacağı anlaşılmaktadır (Kaya, 2019). Keza Kurumun, Kanunun 15 inci maddesinde yer alan inceleme yetkisi kapsamında gerçekleştirileceği faaliyetler de kısmi istisnaya tabi olacaktır. Yine, GVKT'nin "Restrictions" başlıklı 23 üncü maddesinde kısıtlamalar öngörülmüştür.

Direktifte yer alan faaliyetlerin yerine getirilebilmesi için GVKT'de yer alan bazı ilkelere yer verilmemiştir. Söz konusu ilkelerin Direktifte bulunması halinde Direktif kapsamında belirtilen faaliyetlerin sekteye uğrayabileceği, soruşturmanın gizliliği ilkesinin zedelenebileceği, şüphelinin kaçabileceği veya delillerin karartabileceği belirtilmiştir.

Direktif, *"kamu güvenliğine karşı tehditlerin önlenmesi ve kamu güvenliğinin bu tehditlere karşı korunması da dahil olmak üzere, yetkili makamlarca suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla, yetkili makamlar tarafından gerçekleştirilecek faaliyetler çerçevesinde kişisel veri işlenmesinin zorunlu olması halinde"* söz konusu faaliyetlerin hukuka uygun olduğunu kabul etmektedir.

Direktifte özel nitelikli kişisel verilere ilişkin koruma getirilmiş olup 1 inci maddede belirtilen amaçlar kapsamında bu verilerin işlenmesi halinde, AB veya üye devlet hukuku izin vermedikçe işlenmiş olduğu amaç dışında kullanılamayacaktır. İşlenme amacı dışında kullanılması durumunda GVKT hükümleri uygulanacaktır. Bir gerçek kişinin hayati menfaatlerinin korunması ya da ilgili kişi tarafından

alenileştirilmiş olması hallerinde de özel nitelikli kişisel veriler işlenebilecektir.

Diğer taraftan GVKT'de, kişisel verilerin işlenebilmesi için ilgili kişilerin açık rızasının alınması gerekliliği öngörülmüşken, Direktifte böyle bir düzenlemeye yer verilmemiştir. Direktifin amaç kısmında belirtilen faaliyetler kamu yararı amacıyla yürütüldüğü için bu faaliyetler ilgili kişilerin açık rızası alınmaksızın gerçekleştirilebilecektir (Can, 2020). Kanun kapsamında tam istisnaya tabi olan işleme faaliyetleri açısından kişisel veri işleme şartı aranmayacak olup kısmi istisnaya tabi işleme faaliyetleri açısından 5 inci ve 6 ncı maddede yer alan işleme şartları aranacaktır (Kaya, 2019). Konumuzla ilgili olarak kişisel verilerin; *"millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi ya da kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından"* işlenmesi halinde Kanun hükümleri uygulanmayacaktır. Bunun yanında kişisel verilerin, suç işlenmesinin önlenmesi veya suç soruşturması çerçevesinde işlenmesi halinde kısmi istisna hükümleri uygulanacağı için Kanunun 5 inci ve 6 ncı maddesinde yer alan hükümler somut olayda aranacaktır.

TÜRK HUKUKUNDA KOLLUK VE KOLLUĞUN KİŞİSEL VERİ ELDE ETMESİ

Devlet teşkilatımızda kolluk yapılanmasında ikili bir yapı oluşturulmuştur. Bunlardan ilki genel kolluk hizmetleri olup ikincisi ise özel kolluk hizmeti faaliyeti göstermek için kurulmuş özel kolluk birimidir (Demir, 2019).

Genel kolluk hizmetleri 3201 sayılı Emniyet Teşkilatı Kanunu kapsamında gerçekleştirilmekte olup (Bilgiç, 2019) Kanunun 3 üncü maddesinde, *"Silahlı bir kuvvet olan (polis) ve (jandarma)dır"* olarak tanımlanmıştır. Devlet tüzel kişiliğinde yer alan Sahil Güvenlik Komutanlığının, 2692 sayılı Sahil Güvenlik Komutanlığı Kanununun "Kuruluş ve Bağlılık" başlıklı 2 nci maddesinde, *"Bu Kanunda belirtilen görev ve hizmetleri yapmak üzere silahlı bir genel kolluk kuvveti olan Sahil Güvenlik Komutanlığı kurulmuştur."* hükmü ile genel kolluk hizmeti niteliği belirtilmiştir. Bunların yanında, 3201 sayılı Kanunun 3 üncü maddesinde özel kolluk, *"Umumi zabıta haricinde kalan ve mahsus kanunlarına göre teşekkül edip muayyen vazifeleri gören zabıta kuvvetleridir."* şeklinde tanımlanmıştır (Gözler, Kaplan, 2014).

Genel kolluk içerisinde yer alan özel kolluk, genel kolluk yapılanması içerisinde yer alan ancak kanuni düzenlemeler ile özel görevler verilen kolluk yapılanmasıdır. Hem merkezi hem de taşra düzeyinde faaliyet göstermektedirler. Aynı

zamanda, genel kolluk görevleri arasında yer alan adli kolluk faaliyetlerini de göstermektedirler. Diğer bir deyişle, özel bir amacı gerçekleştirmeye yönelik faaliyette bulunmak için kurulmuşlardır. Bu kurumlardan, "Milli İstihbarat Teşkilatı, Özel Güvenlik Personeli ve Belediye Kolluğu" öne çıkmaktadır (Denir, 2019). Özel idari kollukların sağlamaya çalıştığı düzen ile kamu düzeni arasında farklılıklar bulunmaktadır. Bu hususa ilişkin olarak, "av, at yarışları, orman, gümrük, turizm, maliye, çevre ve tekel" alanında gerçekleştirilen kolluk faaliyetleri örnek gösterilebilir (Günday, 2013). Yine, RTÜK (Tiryaki, 2002) ve SPK'nin kolluk yetkisine haiz olduğu (Karakurt, 2009) belirtilmiştir.

2559 Sayılı Polis Vazife ve Salâhiyet Kanunun 1 inci maddesinde;

> *"Polis, asayişi amme, şahıs, tasarruf emniyetini ve mesken masuniyetini korur. Halkın ırz, can ve malını muhafaza ve ammenin istirahatini temin eder. Yardım istiyenlerle yardıma muhtaç olan çocuk, alil ve acizlere muavenet eder. Kanun, Cumhurbaşkanlığı kararnameleri ve ilgili mevzuatın kendisine verdiği vazifeleri yapar."*

hükmüne, Ek Madde 7'de,

> *"Polis, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişi sağlamak üzere, ülke seviyesinde ve sanal ortamda istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla iş birliği yapar."*

hükmüne yer verilmiştir. Hukuk sistemimizde adli ve idari kolluk şeklinde teşkilatlanma yapılmamışsa da fonksiyonel yönden bakıldığında böyle bir ayrım söz konusudur (Bayram, 2009). Kurum içerisinde net bir ayrıma gidilmediği için bazı durumlarda polisin hangi kapsamda faaliyet gösterdiği tam olarak anlaşılamamaktadır. AB uygulamasında, söz konusu ayrımın tam olarak tespit edilememesi halinde AB üye devletleri açısından uygulanacak olan Direktifin uygulanıp uygulanamayacağı konusunda üye devletlerin iç hukukuna bakılacağı belirtilmiştir (Can, 2020). Bu kapsamda, kolluk faaliyetlerine ilişkin yasal düzenlemeler çerçevesinde faaliyet amacı tespit edilerek söz konusu ayrımın yapılması gerektiği değerlendirilmektedir. 2559 sayılı Kanunun 2 nci maddesinin birinci fıkrasının (b) bendinde adli kolluğun suç işlendikten sonra 5271 sayılı Ceza Muhakemesi Kanununa tabi olarak faaliyet gösterdiği ifade edilmiştir. Suç soruşturmasında, 5271 sayılı Kanun devreye girmekte ve soruşturmayı başlatmak için "makul şüphe" gerekmektedir (Bayram, 2009).

Bir başka anlatımla, kanunlarda suç olarak sayılan bir fiilin meydana gelmesinden sonra kişisel verilerin toplanması ve değerlendirilmesi ile kamu güvenliğinin sağlanması için genel çerçevede kişisel veri işlenmesinin farklı olduğu ifade edilmiştir. Buna ilişkin olarak özgürlüğün kural olduğu, sınırlamanın istisna olduğu belirtilmiştir (Mutlu, 2020).

5271 sayılı Kanunun "Adlî kolluk ve görevi" başlıklı 164 üncü maddesinde;

> *"(1) Adlî kolluk; 4.6.1937 tarihli ve 3201 sayılı Emniyet Teşkilatı Kanununun 8, 9 ve 12 nci maddeleri, 10.3.1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun 7 nci maddesi, 2.7.1993 tarihli ve 485 sayılı Gümrük Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 8 inci maddesi ve 9.7.1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanununun 4 üncü maddesinde belirtilen soruşturma işlemlerini yapan güvenlik görevlilerini ifade eder."*

hükmüne yer verilmiştir. Adli kolluk, soruşturma aşamasında Cumhuriyet savcısının emri altında görev almaktadır. Bu duruma ilişkin, savcılık ve kolluk fonksiyonlarının birlikte çalıştığı, bunun olması gereken hukuk açısından uygun olmadığı, doğal hukuk kapsamında bilimsel delil araştırmanın Cumhuriyet savcısı kontrolünde ve denetiminde olması, fakat Cumhuriyet savcısının polis olmaması gerektiği belirtilmiştir. Alman Hukukuna göre kolluk, adli görevleri açısından savcının yardımcısı olup bağımsız çalışmaktadır. Ancak savcının yönlendirmesi ile faaliyet göstermektedir (Bayram, 2009).

5271 sayılı Kanunun "Bir suçun işlendiğini öğrenen Cumhuriyet savcısının görevi" başlıklı 160 ncı maddesinde;

> *"(1) Cumhuriyet savcısı, ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hâli öğrenir öğrenmez kamu davasını açmaya yer olup olmadığına karar vermek üzere hemen işin gerçeğini araştırmaya başlar.*
>
> *(2) Cumhuriyet savcısı, maddî gerçeğin araştırılması ve adil bir yargılamanın yapılabilmesi için, emrindeki adlî kolluk görevlileri marifetiyle, şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına almakla ve şüphelinin haklarını korumakla yükümlüdür."*

hükümlerine yer verilmiştir. Anılan maddesinin gerekçesinde de,

> *"Madde, Cumhuriyet savcısının temel görevini belirtmektedir. Cumhuriyet savcısı bir suçun işlendiği görünümünü veren bir hâli öğrenir öğrenmez hemen gerçeği saptamak üzere harekete geçecektir; hedefi kamu davasını açmaya yer olup olmadığına karar vermektir. Demek oluyor ki, ilk iş şüphe karşısında gerçeği belirlemeye çalışmaktır. Bu aşamada kolluk Cumhuriyet savcısının temel yardımcısıdır. Batı hukukunda, kolluğun temelde işi yürüttüğü bu aşamaya araştırma (enquête) denilmektedir..."*

açıklamalarına yer verilmiştir. Her ne kadar, suç işlendiği izlenimi veren halin bulunması durumunda araştırmaya karar verme yetkisi Cumhuriyet savcısına verilmiş olsa da, 5271 sayılı Kanunun, "Yakalama ve yakalanan kişi hakkında yapılacak işlemler" başlıklı 90 ıncı maddesinin ikinci fıkrasında, "Gece yapılacak arama" başlıklı 118 inci maddesinin ikinci fıkrasında, "Arama kararı" başlıklı 119 uncu maddesinin ikinci fıkrasında, "Elkoyma kararını verme yetkisi" başlıklı 127 nci maddesinin birinci fıkrasında gecikmesinde sakınca bulunan haller göz önünde bulundurularak kolluğa istisna olarak bir takım yetkiler tanınmıştır.

Adli Kolluk Yönetmeliğinin 6 ncı maddesinin ikinci fıkrasında da,

> *"Adlî kolluk görevlileri, kendilerine yapılan bir suça ilişkin ihbar veya şikâyetleri; el koydukları olayları, yakalanan kişiler ile uygulanan tedbirleri derhâl Cumhuriyet başsavcılığına ve en üst dereceli kolluk amirine bildirir ve ilgili Cumhuriyet savcısının emri doğrultusunda işin aydınlatılması için gerekli soruşturma işlemlerine başlar."*

hükmüne yer verilmiştir. Almanya mevzuatında acil durumlarda polis resen çalışabilecektir. Hırvatistan, İngiltere, Galler, Kuzey İrlanda ve İrlanda da kolluk organik olarak kendi hiyerarşisinde çalışmaktadır.

Polis, somut tehlikenin varlığında çalışabilmektedir. Klasik bakış açısıyla bakıldığında, polis halen somut bir tehlikenin olduğu durumlarda yetkilidir; yeni bakış açısında ise, *"tehlikenin doğmasını önleyecek tedbir almak da polisin görevi olarak görülmektedir",* bu nedenle, önleyici yetkiler polisin kişilerle ilgili pek çok veriyi toplamasının gerekliliğini doğurmaktadır.

İdari kolluk, kamu düzenine ve kamu güvenliğine yönelik tehlikeleri önlemekle görevlidir. Bu nedenle önleyici kolluk da denilmektedir. Keza, suç işlenmesinin önlenmesi veya istihbarat amacıyla iletişimin dinlenmesi idari niteliktedir. 2529 sayılı Kanunda, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununda, 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda ve ilgili diğer mevzuatlarda bu amaçlar doğrultusunda izleme yapılmasına ilişkin

hükümler bulunmaktadır. Bu yasal düzenlemeler ile yetkilendirilen polis, jandarma, MİT ve diğer yetkili kurum ve kuruluşlar somut ve haklı gerekçeler olmaksızın yalnızca soyut olasılıklara dayanarak işleme faaliyetinde bulunamaz.

SUÇLARIN SORUŞTURULMASI, KOVUŞTURULMASI VE CEZALARIN İNFAZI AMACIYLA KİŞİSEL VERİLERİN İŞLENMESİ

5271 sayılı Kanunun "Tanımlar" başlıklı 2 nci maddesinin birinci fikrasının (e) bendinde soruşturmanın, *"Kanuna göre yetkili mercilerce suç şüphesinin öğrenilmesinden iddianamenin kabulüne kadar geçen evreyi"* kapsadığı, "Soruşturmanın gizliliği" başlıklı 157 nci maddesinde de, *"Kanunun başka hüküm koyduğu hâller saklı kalmak ve savunma haklarına zarar vermemek koşuluyla soruşturma evresindeki usul işlemleri gizlidir."* hükmü belirtilmiştir.

5271 sayılı Kanunun 160 ncı maddesi, "Cumhuriyet savcısının görev ve yetkileri" başlıklı 161 inci maddesinde yer alan;

"(1) Cumhuriyet savcısı, doğrudan doğruya veya emrindeki adlî kolluk görevlileri aracılığı ile her türlü araştırmayı yapabilir; yukarıdaki maddede yazılı sonuçlara varmak için bütün kamu görevlilerinden her türlü bilgiyi isteyebilir. Cumhuriyet savcısı, adlî görevi gereğince nezdinde görev yaptığı mahkemenin yargı çevresi dışında bir işlem yapmak ihtiyacı ortaya çıkınca, bu hususta o yer Cumhuriyet savcısından söz konusu işlemi yapmasını ister.

(2) Adlî kolluk görevlileri, elkoydukları olayları, yakalanan kişiler ile uygulanan tedbirleri emrinde çalıştıkları Cumhuriyet savcısına derhâl bildirmek ve bu Cumhuriyet savcısının adliyeye ilişkin bütün emirlerini gecikmeksizin yerine getirmekle yükümlüdür.

...

(4) Diğer kamu görevlileri de, yürütülmekte olan soruşturma kapsamında ihtiyaç duyulan bilgi ve belgeleri, talep eden Cumhuriyet savcısına vakit geçirmeksizin temin etmekle yükümlüdür..."

hükümleri, "Soruşturmada Cumhuriyet savcısının hâkim kararı istemi" başlıklı 162 nci maddesinin birinci fikrasında yer alan, *"Cumhuriyet savcısı, ancak hâkim tarafından yapılabilecek olan bir soruşturma işlemine gerek görürse, istemlerini bu işlemin yapılacağı yerin sulh ceza hâkimine bildirir. Sulh ceza hâkimi istenilen işlem hakkında, kanuna uygun olup olmadığını inceleyerek karar verir ve gereğini yerine getirir."* hükmü, "Soruşturmanın sulh ceza hâkimi tarafından yapılması" başlıklı 163 üncü maddesinde yer alan;

"(1) Suçüstü hâli ile gecikmesinde sakınca bulunan hâllerde, Cumhuriyet savcısına erişilemiyorsa veya olay genişliği itibarıyla Cumhuriyet savcısının iş gücünü aşıyorsa, sulh ceza hâkimi de bütün soruşturma işlemlerini yapabilir.

(2) Kolluk âmir ve memurları, sulh ceza hâkimi tarafından emredilen tedbirleri alır ve araştırmaları yerine getirirler."

hükümleri, "Soruşturma evresinde yapılan işlemlerin tutanağa bağlanması" başlıklı 169 uncu maddesinin ikinci fikrasında yer alan, *"Her soruşturma işlemi tutanağa bağlanır. Tutanak, adlî kolluk görevlisi, Cumhuriyet savcısı veya sulh ceza hâkimi ile hazır bulunan zabıt kâtibi tarafından imza edilir."* hükümleri soruşturma işlemlerine ilişkin usul ve esaslar içermektedir.

İddianamenin kabulüyle, kamu davası açılmış olur ve kovuşturma evresi başlar. Hükmün verilmesi ile bu evre sona erer. Kovuşturma evresi, *"duruşma hazırlığı evresi, duruşma devresi ve nihayet, son karar devresinden"* oluşmaktadır.

İnfaz kelimesi, *"Bir kararı, bir yargıyı yerine getirme, uygulama, yürütüm"* olarak tanımlanmıştır (TDK, 2022). İnfaz hukuku, hem amaç hem de oluşum bakımından taşıdığı nitelik sebebiyle kendine özgü kurallar içeren bir hukuk dalı haline gelmiştir. Ancak halen ceza hukuku ile ilişkisi devam etmekte olup 5237 sayılı ve 5271 sayılı Kanunda bu alana yönelik düzenlemeler bulunmaktadır. Bununla birlikte infaz için, suç işlediği iddia edilen kişi hakkında hüküm bulunması gerekir. Yine, Avrupa Cezaevi Kurallarının 2 nci bölümünün 14 üncü maddesinde, *"Hiç kimsenin ulusal hukuka uygun geçerli bir mahkeme kararı olmadığı sürece cezaevine konamayacağı gibi buraya kabul dahi edilemez."* hükmüne yer verilmiştir.

Hapis cezalarının infaz edileceği kurumlar, *"Hapis cezaları, 5275 sayılı Kanunun 8 ilâ 15 inci maddelerinde türleri sayılan ve nitelikleri belirtilen ceza infaz kurumlarında infaz olunur."* hükmü ile belirlenmiştir. 5275 sayılı Kanunun "Ceza İnfaz Kurumlarının Türleri" başlıklı ikinci bölümünün 8 ile 15 inci maddesi arasında söz konusu kurumlar, *"Kapalı ceza infaz kurumları, Yüksek güvenlikli kapalı ceza infaz kurumları, Kadın kapalı ceza infaz kurumları, Çocuk kapalı ceza infaz kurumları, Gençlik kapalı ceza infaz kurumları, Gözlem ve sınıflandırma merkezleri, Açık ceza infaz kurumları, Çocuk eğitimevleri"* şeklinde sayılmıştır.

Ceza ve güvenlik tedbirlerinin infazı ile ulaşılmak istenilen temel amaç, *"öncelikle*

genel ve özel önlemeyi sağlamak, bu maksatla hükümlünün yeniden suç işlemesini engelleyici etkenleri güçlendirmek, toplumu suça karşı korumak, hükümlünün; yeniden sosyalleşmesini teşvik etmek, üretken ve kanunlara, nizamlara ve toplumsal kurallara saygılı, sorumluluk taşıyan bir yaşam biçimine uyumunu kolaylaştırmaktır" olarak tespit edilmiştir. Ceza ve güvenlik tedbirlerinin infazına ilişkin kurallar hükümlülerin *"ırk, dil, din, mezhep, milliyet, renk, cinsiyet, doğum, felsefî inanç, millî veya sosyal köken ve siyasî veya diğer fikir yahut düşünceleri ile ekonomik güçleri ve diğer toplumsal konumları"* yönünden ayırım yapılmaksızın ve hiçbir kimseye ayrıcalık tanınmaksızın uygulanır. Ceza ve güvenlik tedbirlerinin infazında zalimane, insanlık dışı, aşağılayıcı ve onur kırıcı davranışlarda bulunulamaz.

Ceza muhakemesi sürecinde yer alan makamlar, *"iddia, savunma ve yargılama makamı"* olmak üzere üç tanedir. Bu makamlar da birtakım süjeler tarafından temsil edilmektedirler. 5271 sayılı Kanunun 160 ıncı maddesi çerçevesinde "*Cumhuriyet savcısı"* ve *"adli kolluğun"* iddia makamını oluşturduğu anlaşılmaktadır. Yine, 5271 sayılı Kanunun 163 üncü maddesi bazı durumlarda *"sulh ceza hakiminin"* de iddia makamını temsil ettiği anlaşılmaktadır.

Bireysel iddia makamı süjesi ise *"mağdur, suçtan zarar gören, vekil ve yasal temsilci"dir (AHBV, 2022). "Şüpheli ve sanık, şüpheli veya sanığın eşi ve yasal temsilcisi, malen sorumlu kişi ile tüzel kişinin temsilcisi"* bireysel savunma makamı süjesidir. 5271 sayılı Kanunun "Tanımlar" başlıklı 2 nci maddesinin birinci fıkrasının (c) bendinde müdafinin, *"Şüpheli veya sanığın ceza muhakemesinde savunmasını yapan avukatı"* kapsadığı ve toplumsal savunma makamı süjesi olduğu ifade edilmiştir. Yargılama makamı ise sadece toplumsal olup *"hâkimler"* ile *"mahkemelerden"* oluşmaktadır (Adalet Bakanlığı, 2022).

Kanunun 28 inci maddesinin birinci fıkrasının (d) bendinde Kanundan istisna hali düzenlenmiştir. Az önce yer verilen açıklamalarda, yargılama makamlarının hakimlik ve mahkemelerden oluştuğu belirtilmişse de, Kanunun ilgili hükmünün kanun sistematiği çerçevesinde yorumlanması neticesinde, soruşturma evresinin de istisnalar kapsamına alınmış olması sebebiyle, Cumhuriyet savcılığının soruşturma faaliyetleri amacıyla yürüttüğü işlemlerin de yargı makamı faaliyeti olarak kabul edildiği, böylelikle, söz konusu makamın yürütmüş olduğu soruşturmalarda gerçekleştirdiği kişisel veri işleme faaliyetlerinin tam istisna kapsamında olduğu değerlendirilmektedir. Diğer taraftan, 5275 sayılı Kanunda belirtilmiş olan infaz mercilerinin infaz işlemlerine ilişkin faaliyetleri de tam istisna kapsamında olacaktır.

Kanunun 28 inci maddesinin birinci fıkrasının (ç) bendi ve ikinci fıkrası ile (a) bendinde yer alan hükümler göz önüne alındığında suç işlenmesinin önlenmesi ve suç soruşturması amacıyla gerçekleştirilecek kişisel veri işleme faaliyetlerinin; *"yetkili makamlar tarafından gerçekleştirilecek önleyici, koruyucu ve istihbari faaliyetler ile soruşturma, kovuşturma, yargılama veya infaz işlemleri"* dışında kalan kişisel veri işleme faaliyetlerini kapsadığı ve bu sebeple kısmi istisnaya tabi tutulduğu değerlendirilmektedir. Yine doktrinde, 28 inci maddenin birinci fıkrasının (d) bendinde belirtilen faaliyetlerin *"yargı makamları ve infaz mercilerince"* yapılması öngörüldüğünden kolluğun bunların dışında kendisine tanınan görev ve yetkisi çerçevesinde özellikle soruşturma sürecinde resen yapacağı işlemlerin tam istisna kapsamında olmayacağı belirtilmiştir. Keza, ulusal güvenliğe ilişkin gerçekleştirilen kişisel veri işleme faaliyetlerinin Direktif kapsamında olmadığı belirtilmiş olup bu doğrultuda, Direktifte belirtilen suçların önlenmesi amacıyla gerçekleştirilen kişisel veri işleme faaliyetlerinde ulusal güvenliğe ilişkin kişisel verilerin işlenmemesinin amaçlandığı değerlendirilmektedir.

Ancak, bu konuların net bir ayrım sağlayacak şekilde düzenlenme altına alınmamış olmasının AB düzenlemeleri ile AİHM içtihatları karşısında devletin düzenlemesi gereken alanı ihmal ettiği, bu durumun devletin pozitif yükümlülüğüne aykırı olduğu ileri sürülmüştür.

AB uygulamasında, *"suçların, önlenmesi, soruşturulması, ortaya çıkarılması, kovuşturulması ile cezaların infazı amacıyla yetkili makamların kişisel veri işlemesi"*nde ikinci bölümde açıkladığımız Direktif hükümleri uygulama alanı bulacaktır. Bu kapsamda, mevcut uygulamamızın aksine söz konusu faaliyetler AB uygulamasında tamamen istisna tutulmamış olup ayrı bir düzenleme ile kişisel verilerin korunması sağlanmaya çalışılmıştır. Yine Direktif, bazı istisnalar dışında GVKT'de sayılan ilkeleri kapsamına alarak *"suçların önlenmesi, soruşturulması, ortaya çıkarılması veya kovuşturulması ya da cezaların infazı amacıyla işlenmesi"* durumunda söz konusu ilkelere uygun olarak kişisel veri işlenmesini sağlamayı amaçlamaktadır.

Kanunda yer alan tam istisna halleri, Anayasada öngörülen kişisel verilerin korunması hakkının bu evrede hiç kullanılamayacak olması sebebiyle eleştirilmiştir. Kanunun tam istisna hallerinde Kanun hükümleri, kısmi istisna hallerinde 11 inci madde hükümleri uygulanmayacaktır (Mutlu, 2020). Direktifin 12 nci maddesinde ilgili kişinin bilgi edinme hakkının soruşturma evrelerinde de kullanılabileceği belirtilmiştir. Bununla birlikte, kişisel verilerin işlenmesine ilişkin temel ilkelerin tüm işleme faaliyetlerinin özünde bulunması gerektiği, bu kapsamda, bir kişisel veri işleme faaliyeti her ne kadar Kanundan tam ve kısmi istisnaya tabi tutulmuş olsa da temel ilkelere uygun ve orantılı olarak bu faaliyetlerin gerçek-

leştirilmesi gerektiği belirtilmiştir (KVKK, 2019).

Her ne kadar soruşturma, kovuşturma ve yargılama evresi Kanundan istisna olsa da 5271 sayılı Kanunda öngörülen usuller çerçevesinde kişisel verilerin işlenmesi gerekmektedir. Böylelikle, 5271 sayılı Kanunda ve ilgili diğer düzenlemelerde öngörülen yargı mercilerinin kararı olmadan kişisel veri işleme faaliyeti gösterilemeyecek olup bu hususlara dayanmadan elde edilen kişisel veriler yargılama faaliyetinde kullanılamayacaktır. Yine, infaz işlemlerinde de 5275 sayılı Kanunun dikkate alınarak kişisel veri işlenmesi gerekmektedir.

ÖN ALAN ARAŞTIRMALARI İLE İSTİHBARAT İLİŞKİSİ VE İSTİHBARAT GEREĞİ VERİ İŞLEME FAALİYETLERİ

Ön alan araştırmasında, kamu düzenini tehdit eden somut tehlike bulunmamasına rağmen kolluğun müdahale alanı öne çekilerek veri toplaması istihbarat olarak nitelendirilmiştir. Toplanan veriler kolluk tarafından saklanıp analiz edilebilmektedir. Bu evrede, önleyici faaliyetin, ceza muhakemesi ile istihbarat faaliyet arasında net bir şekilde konumlandırılamaması sebebiyle yetkinin kimde olduğu konusunda tartışma bulunmaktadır.

Anayasanın 13 üncü maddesi çerçevesinde, ön alan araştırmasına ilişkin yetkilerin kanunla tanınması gerektiği ifade edilmiştir. 5271 sayılı Kanunun "Cumhuriyet savcısının görev ve yetkileri" başlıklı 161 inci ve 161 inci madde ile bağlantısı bulunan "Adlî kolluk ve görevi" başlıklı 164 üncü maddenin bu yetkiyi karşılamadığı, buna karşın, 2559 sayılı Kanunda yer alan gelecekteki tehlikeleri önleme amacıyla öngörülmüş olan polis tedbirlerinin ön alan araştırmaları kavramını oluşturduğu belirtilmiştir (Can, 2020).

Suçun işlenmesinden sonra faili belirlemek amacıyla gerçekleştirilen araştırmalar adli görevler arasındadır. Ancak, bir suç işlenmeden önce suçun işlenmesinin önlenmesi amacıyla gösterilen faaliyetler kolluğun temel görevlerindendir. Örneğin, suç işlemek amacıyla bir örgütün kurulması neticesinde suç işlenmiş ise bu kısım adli alanı ilgilendirmektedir. Bununla birlikte, suç işleme amacıyla örgüt kurulması da bir suç olduğu için o kısım da adli alana girmektedir (Yenisey, 2016). Fakat, örgütün var olup olmadığının araştırılması (Bayram, 2009) veya suç işlemek amacıyla kurulmuş olan örgütün henüz işlemediği suçlar bulunmakta ise bu hususların önlenmesi amacıyla gösterilen faaliyetler kolluğun önleyici görevlerindendir. Bu kapsamda, kolluğun önleyici faaliyetlerini gösterebilmesi için *"bilgi edinme, bilgileri saklama ve analiz etme"* yetkileri doğmuştur.

Suçun önlenmesi amacıyla bilgi toplanması beyaz ve gri alanı kapsadığı için gizlidir. Bu kısım kolluğun istihbarat yetkilerini oluşturur. Bu aşamada başlangıç şüphesi oluşmamaktadır. Başlangıç şüphesi suç işlendikten sonra ortaya çıkmaktadır. Bununla birlikte, suç işlendiği izlenimi veren haller de başlangıç şüphesi kapsamında değerlendirilmektedir. 5271 sayılı Kanunun temel ilkelerinden biri olan resen araştırma ilkesi soruşturma başlamadan önce inceleme yapılmasını zorunlu kılmaktadır. Yapılan inceleme sonucunda soruşturma açılıp açılmayacağı belli değildir (Yenisey, 2016). Sadece araştırmaya değecek şüpheli bir durum vardır. Bilgi elde etmeye yönelik tedbirler içeren ön alan soruşturmalarında, bu tedbirin uygulanması için ne işlenmiş bir suçun aydınlatılması, ne de önlenmesi gereken somut bir tehlikenin bulunması gerekmektedir. Ön alan henüz bir başlangıç şüphesinin ya da somut bir tehlike durumunun bulunmadığı bir zaman dilimini ifade etmektedir (Bayram, 2009).

Suç işleme tahmini için somut olgulara dayalı makul bir şüphe bulunması gerekmektedir. Somut olgulara dayanmayan tahmin ile araştırma yapılmaması gerekmektedir. Suç fiilinin varlığına ilişkin tahminin, hayat tecrübesine veya mesleki tecrübelere yani kriminalistik verilere dayanması gerekir (Yenisey, 2016).

Kolluğa, suç işlemeden önce soyut risklere karşı ve/veya gelecekteki bir ceza muhakemesi için müdahale olanakları verilmesi, aslında polisin zorlayıcı yetkisinin vaktinden önce uygulanması sonucunu doğurur, bu da kolluğun sadece ve doğrudan amacı olan kamu güvenliği ve düzeninin devam ettirilmesi amacını taşır (Bayram, 2009). Kamu güvenliği, bireylerin can ve mallarına zarar verebilecek tehdit ve tehlikelerin yokluğu anlamına gelmektedir (Çetindağ, 2004). İdare hukuku kapsamında kamu düzeni, kolluk eylemlerinin maksat unsuru olarak karşımıza çıkmakta olup kolluk faaliyetlerine yön verici nitelik taşımaktadır. Bireye özgülenmiş olarak, bireysel çıkarlara dayalı bir düzenin kamu düzeni ile ilgisi yoktur. Bu anlamda kamu düzeni toplumun dış ve maddi düzeni olup umuma açık yerlerde bireylerin güvenlik, dirlik, esenlik içinde ve sağlıklı olarak yaşamalarının sağlanması anlamına gelmektedir. Burada belirtilmesi gereken nokta kamu güvenliğinin, kamu düzenin bir unsuru olan güvenlikten ve emniyetten daha sınırlı ve kapsamı daha dar bir olguyu işaret ettiğidir. Kamu güvenliği ve kamu düzeni kavramı literatürde birçok tanımlama çabasına konu olmuş fakat net bir tanımlama asla yapılamamıştır (Işık, 2012).

Ön alan araştırmasının önemli bir unsurunu oluşturan önleme amaçlı iletişimin denetlenmesi henüz suç işlenmeden uygulanmalıdır. Faaliyetin amacı suçun önlenmesi olduğundan önlenmesi istenilen suça ilişkin hazırlık hareketleri başlamadan tedbire başvurulması mümkündür. Önleme amaçlı dinleme için kanun-

larda öngörülmüş bir nedenin varlığı gerekir. Bu nedenin iletişimin dinlenmesi kararında belirtilmesi gerekmektedir. Söz konusu tedbire başvurulabilmesi için bir neden veya suç işleme tehlikesi mevcut olmalıdır. Anayasanın 13 üncü maddesinde öngörülen ölçülülük ilkesi gereği daha hafif bir tedbire başvurulması mümkünse öncelikle ona başvurulması gerekmektedir.

Bu kısımda yer alan araştırmalar 5271 sayılı Kanunun şüphe kategorilerine girmediği için kanun kapsamındaki soruşturma evresini başlatmayacaktır. Soruşturma evresinin başlamayacak olması sebebiyle incelemenin kim tarafından gerçekleştirileceği karmaşası ortaya çıkmaktadır. Hangi organın görevli olduğu tespit edilirken, yapılan incelemelerin ağırlık noktası incelenecektir. Eğer delil elde etme amacıyla araştırma yapılıyor ise adli alanda, suç işlenmesinin önlenmesi amacıyla yapılıyor ise kolluğun önleyici faaliyeti kapsamında değerlendirilmektedir (Yenisey, 2016).

Ön alan araştırması kapsamında bilgi toplama, kolluğun görevinden kaynaklanmaktadır. Bu göreve istihbarat toplama adı verilir. Gizli bilgiler yasal düzenlemeler kapsamında işlenebilmektedir. Ancak, mevcut yasal düzenlemelerin yeterli seviyede olmadığı belirtilerek eleştirilmiştir.

İleride suç işlenmesini önlemek amacıyla polisin bilgi toplama yetkisinin doğması için, *"belli olayların ortaya çıkmış olması ve bunların belli kişiler üzerinde yoğunlaşmış olması"* şart olmalıdır. Çünkü istihbarat yoluyla kişinin, *"özel hayatına, kişisel verilerine, haberleşme özgürlüğüne"* müdahale edilmektedir. Müdahale alanının temel hak ve özgürlük içermesi sebebiyle, Anayasa ve uluslararası sözleşmelere dayanılarak yürürlüğe konulmuş olan kanunlar kapsamında kişisel veriler işlenebilecektir.

Gizli şekilde kişisel veri işlenmesinin müdahale olarak değerlendirilip değerlendirilemeyeceği hususunda bir görüşe göre, ilgili kişi tarafından alenileştirilen kişisel verilerin işlenmesinin müdahale oluşturmayacağı ifade edilmiştir. Burada dikkat edilmesi gereken konu toplanan büyük miktarda veriler ile kişilik ve hareket profili oluşturulmasıdır. Profil oluşturulması halinde sınırın aşılabileceği belirtilmiştir (Bayram, 2009).

Kolluk faaliyetleri idari, adli ve siyasi olarak ayrılmıştır. Bu faaliyetlerden siyasi kolluğun amacı kamu düzeninin sağlanması değildir (Can, 2020). Devletin varlığına karşı içten ve dıştan gelebilecek saldırılara karşı koruma sağlamak amacıyla gerçekleştirilen faaliyetlere gizli kolluk faaliyetleri denilmektedir.

Devletin güvenliği ve milli politikası ile ilgili istihbarat çalışmalarını bir bütün olarak ele almak, istihbarat ile uğraşan kurumlar arasında koordinasyonu sağlamak, devletin milli güvenlik politikası ile ilgili planların hazırlanmasında esas olacak istihbaratı Devlet çapında üretmek amacıyla, 06.07.1965 tarihli ve 644 sayılı Milli İstihbarat Teşkilat Kanunu çıkarılmış olup 22.07.1965 tarihinde yürürlüğe giren bu kanun ile Başbakanlığa bağlı MİT kurulmuştur. 01.11.1983 tarihinde ve 2937 sayılı Kanun çıkarılmış ve MİT doğrudan Başbakana bağlanmıştır. 2017 yılında aynı kanunda yapılan değişiklikle MİT Cumhurbaşkanına bağlanmıştır (MİT, 2022).

Anılan Kanunun, 4 üncü maddesinin birinci fikrasının (a) bendinde MİT'in,

> *"Türkiye Cumhuriyeti ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenliğine, Anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı Cumhurbaşkanı, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmakla görevli olduğu"*

belirtilmiştir.

2937 sayılı Kanununun "Amaç" başlıklı 1 inci maddesinin birinci fikrasında, *"kanunun amacının, Devlet istihbaratının istihsali ve kullanılması ile MİT'in kuruluş, görev ve faaliyetlerine ait esas ve usulleri düzenlemek olduğu"* belirtilmiştir. "Yetkiler" başlıklı 6 ncı maddesinde ise MİT'in, 2937 sayılı Kanun kapsamındaki görevlerini yerine getirirken sahip olduğu yetkiler düzenlenmiştir. Anılan maddenin birinci fikrasının (b) bendinde,

> *"Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilir ve bunlarla irtibat kurabilir. Bu kapsamda talepte bulunulanlar, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamazlar."*

hükmüne, bununla birlikte, Ek maddenin birinci fikrasında ise,

> *"Millî İstihbarat Teşkilatı uhdesindeki istihbari nitelikteki bilgi, belge, veri ve kayıtlar ile yapılan analizler, Türk Ceza Kanununun İkinci Kitap Dördüncü*

Kısım Yedinci Bölümünde yer alan suçlar hariç olmak üzere, adli mercilerce istenemez."

hükmüne yer verilerek MİT tarafından elde edilen verilere ilişkin koruma getirilmiştir. Kanunun 3 üncü maddesinin birinci fıkrasının (h) bendi ve (ı) bendi çerçevesinde, 2937 sayılı Kanun kapsamındaki faaliyetleri yürüten kuruluş olarak MİT'in, az önce yer verilen tanımlar çerçevesinde veri sorumlusu olduğu değerlendirilmektedir. Yine, 2937 sayılı Kanunun "Yetkiler" başlıklı 6 ncı maddesinin birinci fıkrasının (c) bendinde,

"26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun İkinci Kitap Dördüncü Kısım Dört, Beş, Altı ve Yedinci bölümlerinde yer alan suçlara (318, 319, 324, 325 ve 332 nci maddeleri hariç olmak üzere) ilişkin soruşturma ve kovuşturmalarda ifade tutanaklarına, her türlü bilgi ve belgeye erişebilir, bunlardan örnek alabilir."

hükmüne yer verilmiştir. Kanunun 6 ncı maddesinin birinci fıkrasında "ceza mahkumiyeti ile güvenlik tedbirlerine" ilişkin verilerin özel nitelikli kişisel veri olduğu belirtilmiştir. Bu çerçevede, söz konusu bilgi ve belgeler arasında özel nitelikli kişisel verilerin bulunabileceği düşünülmektedir. Ayrıca, 2937 sayılı Kanunun 6 ncı maddesinin birinci fıkrasının (i) bendinde,

"MİT mensupları görevlerini yerine getirirken ceza ve infaz kurumlarındaki tutuklu ve hükümlülerle önceden bilgi vermek suretiyle görüşebilir, görüşmeler yaptırabilir, görevinin gereği terör örgütleri dâhil olmak üzere millî güvenliği tehdit eden bütün yapılarla irtibat kurabilir."

şeklinde ifade edilen hüküm kapsamında da kişisel veri işlenebileceği değerlendirilmektedir.

Diğer taraftan, 2937 sayılı Kanunun 6 ncı maddesinin birinci fıkrasının (d) bendinde, *"Görevlerini yerine getirirken gizli çalışma usul, prensip ve tekniklerini kullanabilir."* hükmü yer almaktadır. Kanunun 6 ncı maddesinin ikinci fıkrasında, *"özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmadan işlenemeyeceği, üçüncü fıkrasında ise sağlık ve cinsel hayata ilişkin veriler dışındaki kişisel verilerin kanunla işlenebileceği"* belirtilmiştir. 2937 sayılı Kanunun 6 ncı maddesinin birinci fıkrasının (d) bendinde belirtildiği üzere faaliyetlerin gizli yürütülmesinin esas olması sebebiyle ilgililerin açık rızası alınmadan kişisel verilerin işleneceği değerlendirilmektedir. Fakat, yetkili kurum ve kuruluşlar tarafından yerine getirilen istihbari faaliyetler Kanundan istisna olduğu için özel nitelikli kişisel verilerin

işlenmesinde 6 ncı maddede yer alan işleme şartlarının aranmayacağı değerlendirilmektedir. Bu değerlendirmeler üzerinde belirtmek gerekir ki, Kurulun, Covid19 Pcr test sonucu ve aşı bilgisi uygulamalarına ilişkin 28.09.2021 tarihli ve 2021/980 sayılı kararı hakkında yapılan kamuoyu duyurusunda yer alan,

"...

Dünya genelinde çeşitli varyantlarının da etkisiyle yayılma hızı giderek artış gösteren Covid-19 virüsünün neden olduğu hastalıklardan korunmak adına, değişen koşulları da dikkate almak suretiyle ülkemizin de aralarında bulunduğu tüm devletler, çeşitli tedbirler almaya devam etmekte olup; karantina, sosyal mesafe ve sosyal izolasyon gibi temel tedbirlerin alınmasının yanı sıra, yapılan bilimsel çalışmalar neticesinde Covid-19 aşıları geliştirilerek kullanıma sunulmuştur. Covid-19 aşısının, koronavirüsün yayılımını önlediği, hastalığın etkilerini de önemli ölçüde azalttığı bilinmekte olup; bu bilimsel gerçeklikten hareketle devletler, kamu sağlığının korunmasını teminen işyerleri de dâhil olmak üzere toplu halde bulunulacak alanlarda, Covid-19 aşı bilgisi ve/veya PCR testi sonuçlarının işlenmesi zorunluluğu getirmektedirler.

Nitekim ülkemizde de İçişleri Bakanlığınca 81 İl Valiliğine gereği, ilgili Bakanlıklara da bilgi için gönderilen 20.08.2021 tarihli yazıda; salgının toplum sağlığı ve kamu düzeni açısından oluşturduğu riskin asgari seviyeye düşürülmesi için konser, sinema, tiyatro ve toplu ulaşım araçları gibi insanların toplu olarak bulunduğu faaliyetlere katılım sağlamak isteyen kişilere Covid-19 aşı bilgisi ve/veya negatif sonuçlu PCR test bilgisinin bildirilmesi zorunluluğu getirilmiştir.

Çalışma ve Sosyal Güvenlik Bakanlığının 81 İl Valiliğine gereği için, ilgili Bakanlıklara da bilgi için gönderdiği 02.09.2021 tarihli yazıda ise işyerlerinde karşılaşılabilecek sağlık ve güvenlik risklerine yönelik koruyucu ve önleyici tedbirler kapsamında; Covid-19 aşısı olmayan işçilerden zorunlu olarak haftada bir kez PCR testi yaptırmalarının işyeri/işveren tarafından istenebileceği ve test sonuçlarının gerekli işlemler yapılmak üzere kayıt altında tutulacağı ifade edilmiştir.

Öncelikle belirtmek gerekir ki; kişilerin tahlil, görüntüleme, test, rapor, aşı durumu gibi sağlık durumlarına ilişkin bilgileri Kanunun 6 ncı maddesine göre kişisel sağlık verisi niteliğini haiz olup, özel nitelikli kişisel veri kategorisinde bulunmaktadır. Bu sebeple, söz konusu bilgilerin Kanunun 6 ncı maddesinde yer verilen işleme şartlarına uygun olarak işlenmesi gerekmektedir. Öte

yandan, Covid-19 salgınının dünya çapındaki gerek sağlık, gerek sosyal hayat gerek ekonomi üzerindeki etkileri dikkate alındığında, bu salgınla mücadele kapsamında aşı durumu ve PCR test sonucu gibi Covid-19'a ilişkin kişisel sağlık verilerinin; kamu sağlığının, kamu güvenliğinin ve kamu düzeninin korunması amacıyla işlenmesi gerekliliğinin ortaya çıkması kaçınılmazdır.

Bilindiği üzere Kanunun 28 inci maddesinin birinci fıkrasının (ç) bendinde, "Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi" halinde Kanun hükümlerinin uygulanmayacağı düzenlenmiştir.

Bu noktadan hareketle salgın hastalık gibi kamu güvenliği ve kamu düzenini tehdit eden durumlarda bu tehdidi ortadan kaldırabilmek amacıyla salgın hastalığın bulaşıcılığının önüne geçilebilmesini teminen kanunla yetki verilmiş kamu kurum ve kuruluşlarınca yürütülen faaliyetler kapsamında kişisel verilerin işlenmesinin de Kanunun 28 inci maddesinin birinci fıkrasının (ç) bendi kapsamında değerlendirilmesi gerektiği düşünülmektedir.

Bu kapsamda Covid-19'un sebebiyet verdiği salgın hastalığın kamu güvenliği ve kamu düzenini tehdit etmesi sebebiyle hastalığın yayılımını engellemek amacıyla Covid-19 aşı bilgisi ve/veya negatif sonuçlu PCR test bilgisinin anılan madde hükmü kapsamına giren kamu kurum ve kuruluşlarınca yürütülen önleyici ve koruyucu faaliyetler kapsamında işlenmesinin önünde bir engel bulunmadığı, dolayısıyla söz konusu kişisel veri işleme faaliyetlerinin Kanunun 28 inci maddesinin birinci fıkrasının (ç) bendi kapsamında gerçekleştirilebileceği, bununla birlikte, Covid-19 salgını kapsamında yürütülen kamu güvenliğini ve kamu düzenini koruma amacına yönelik faaliyetler dışında kalan ya da bu amacı aşan nitelikteki kişisel veri işleme faaliyetlerinin Kanun kapsamında yer alacağı değerlendirilmektedir."

açıklamalarına (KVKK, 2021) yönelik olarak, istihbari faaliyetler ile ön alan araştırmalarının gizli olması sebebiyle, Çalışma ve Sosyal Güvenlik Bakanlığının 02.09.2021 tarihli yazısında (ÇSGB, 2021) bilgilendirme yapılarak işçilerin kişisel verilerinin işlenmesini öngören işleme faaliyetinin önleyici ve istihbari faaliyetler kapsamında olamayacağı değerlendirilmektedir. Kurulun 28.09.2021 tarihli ve 2021/980 sayılı kararında da belirtilmiş olduğu üzere somut olayda kamu sağlığının korunması amacının bulunduğu, bu amaç doğrultusunda Kanunun 6 ncı maddesinin üçüncü fıkrası çerçevesinde uygulamanın büyüklüğüne uygun araçlarla Kanunun 10 uncu maddesinde yer alan aydınlatma yükümlülüğünün yerine getirilmesi ile kişisel verilerin işlenmesi gerektiği değerlendirilmektedir. Bunun yanında, Kanunun 6 ncı maddesinin üçüncü fıkrasında özel nitelikli kişisel verilerin ancak sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kuruluşlar tarafından işlenebileceğinin belirtildiği, sır saklama yükümlülüğü altında olan kişi olarak işverenin Kanunun bu hükmü kapsamında değerlendirilemeyeceği belirtilmiştir (Fiş, 2002). Öncelikle kişi kavramı gerçek kişileri ve tüzel kişileri kapsamaktadır. Bu kapsamda, özel tüzel kişiliklerin "kişi" kavramı içerisinde yer aldığı değerlendirilmektedir. Sır kavramına ilişkin olarak ise, kelime anlamı olarak saklanması gereken bilgiyi ifade ettiği, genel olarak ifade edilecek olursa sırrın, sadece sahibi tarafından bilinen veya sahibi tarafından sınırlı bir çevre dışındaki üçüncü kişilerle paylaşılması istenilmeyen bilgi olduğu, dolayısıyla, sırrın, temelinde gizlilik ile eşdeğer bir kavram olduğu belirtilmiştir (Arkun, 2010). 6331 sayılı İş Sağlığı ve Güvenliği Kanununun "Sağlık gözetimi" başlıklı 15 inci maddesinin beşinci fıkrasında, *"Sağlık muayenesi yaptırılan çalışanın özel hayatı ve itibarının korunması açısından sağlık bilgileri gizli tutulur."* hükmüne yer verilmiştir. Bu hüküm çerçevesinde, aşı uygulaması ve Pcr testi yaptırılması istenen işçilerin işe devam etmesi veya ara verdirilmesine ilişkin bilginin gizli tutulacağı anlaşılmaktadır. Öte yandan, işverenin işçiyi gözetme borcu, işçinin kişiliğinin koruma borcu altında olup işçinin yaşamı, sağlığı, vücut bütünlüğü, onuru, kişisel ve meslek saygınlığı, özel yaşam alanının korunması bu kapsamda yer almaktadır. Bu hususa yönelik olarak 6098 sayılı Kanunun "Kişisel verilerin kullanılmasında" başlıklı 419 uncu maddesinde, *"(1)İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. (2) Özel kanun hükümleri saklıdır."* hükümlerine, 4857 sayılı İş Kanununun "İşçi özlük dosyası" başlıklı 75 inci maddesinde;

"İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır. İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür."

hükümlerine yer verilmiştir (Sümer, 2016). Diğer taraftan, GVKT, yetkili halk sağlığı makamlarının ve işverenlerin, ulusal yasalara uygun olarak ve belirtilen koşullar dahilinde, bir salgın bağlamında kişisel verileri işlemesine izin vermektedir. Kamu sağlığı açısından gerekli olması halinde, GVKT'nin *"Özel kategorilerdeki kişisel verilerin işlenmesi"* başlıklı 9 uncu maddesinin ikinci fıkrasının (i) bendi

kapsamında kişisel verilerin işlenebileceği belirtilmiştir (EDPB, 2020).

2937 sayılı Kanunun 6 ncı maddesinin birinci fikrasının (g) bendinde, *"Telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilir."* hükmü, (h) bendinde, *"Yabancı unsurların ülkenin ve vatandaşların iletişim güvenliğini tehdit eden faaliyetlerinin engellenmesine yönelik çalışmalar yapabilir, ilgili kurum ve kuruluşlardan talepte bulunabilir."* hükmü yer almakta olup bu hükümler kapsamında veri toplanırken, *"bir gerçek kişiyi belirli veya belirlenebilir kılan bir bilgi"* işlenmesi halinde, kişisel veri işleme faaliyetinin gerçekleştirileceği değerlendirilmektedir.

2937 sayılı Kanunun 6 ncı maddesinin birinci fikrasının (i) bendinde, *"MİT'te görev alan veya alacak kişilerin güvenilirliklerini ve uygunluklarını belirlemek için yalan makinası uygulaması dâhil test teknik ve yöntemlerini"* kullanabileceği belirtilmiştir. Bu kapsamda, başta sağlık verisi olmak üzere özel nitelikli kişisel verilerin işlenebileceği değerlendirilmektedir.

2937 sayılı Kanunun 6 ncı maddesi kapsamında yer alan 03.07.2005 tarihli Ek maddede,

> *"Anayasa'da sayılan devletin temel niteliklerine ve demokratik hukuk devletine yönelik ciddi bir tehlikenin bulunması halinde, devletin güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, devlet sırrının ifşasının tespiti, terörist faaliyetlerin önlenmesi için telekomünikasyon yoluyla iletişimin denetlenebileceği"*

belirtilmiştir. Bu denetim kapsamında, *"iletişimin tespiti, dinlenmesi, kayda alınması veya sinyal bilgilerinin değerlendirilmesi"* bulunmaktadır. Ek maddenin devamında ise, istihbari amaçla uygulanacak bu tedbirin sona ermesi halinde dinlemenin içeriğine ilişkin kayıtların en geç on gün içinde yok edileceği ifade edilmiştir (Can, 2020). Bir diğer Ek fikrada,

> *"Kararda ve yazılı emirde, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespite imkân veren kodundan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenler belirtilir. Kararlar, en fazla üç ay için verilebilir; bu süre aynı usûlle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilir. Ancak, casusluk faaliyetlerinin tespiti ve terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir."*

şeklinde ifade edilen hüküm ile iletişim tespit edilirken işlenecek verilerin neler olduğu açıklanmıştır. 2937 sayılı Kanunun 6 ncı maddesi kapsamında yürütülen faaliyetler çerçevesinde, *"elde edilen kayıtların söz konusu kanun dışında kullanılamayacağı, elde edilen bilgi ve kayıtların saklanmasında ve korunmasında gizlilik ilkesinin geçerli olduğu"* ifade edilmiştir. Keza, anılan maddedeki usul ve esaslara aykırı dinlemelerin hukuken geçerli sayılmayacağı, bu şekilde dinleme yapanlara 5237 sayılı Kanun kapsamında işlemlerin uygulanacağı belirtilmiştir.

Az önce bahsedilen hükümlere ve diğer kanunlardaki düzenlemelere bağlı kalmaksızın,

> *"...önleyici istihbarat elde etmek ve analiz yapabilmek amacıyla MİT Başkanı veya yardımcısının onayıyla yurt dışında veya yabancılar tarafından gerçekleştirilen iletişim ile ankesörlü telefonlarla gerçekleştirilen iletişim ve MİT mensuplarının, MİT'te görev almış olanların veya görev almak üzere başvuranların iletişiminin tespit edilebileceği, dinlenebileceği, sinyal bilgilerinin değerlendirilebileceği, kayda alınabileceği..."*

belirtilmiştir.

Anayasa Mahkemesinin 2018/73 E. 2019/65 K. 24.07.2019 tarihli kararında da,

> *" ...*
>
> *167. Anayasa'nın 20. maddesi uyarınca kişisel veriler ancak kanunda öngörülen hâllerde veya kişinin açık rızasıyla işlenebilir. Dolayısıyla kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için bu hakkı ilgilendiren yasal düzenlemelerin açık, anlaşılabilir ve söz konusu hakkın kullanılabilmesine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmî makamların keyfî müdahalelerine karşı korunması mümkün hâle gelebilir.*
>
> *...*
>
> *171. Kuralda güvenlik soruşturması ve/veya arşiv araştırması yapılması memurluğa alımlarda genel şartlar arasında sayılmasına karşın güvenlik soruşturmasına ve arşiv araştırmasına konu edilecek bilgi ve belgelerin neler*

olduğuna, bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına ilişkin herhangi bir düzenleme yapılmamıştır. Diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilen kullanılmasına ilişkin temel ilkeler belirlenmeksizin kuralla sadece güvenlik soruşturması ve arşiv araştırması yapılması devlet memurluğuna alımlarda aranacak şartlar arasında sayılmıştır

172. Güvenlik soruşturması ve arşiv araştırması sonucunda devlet memurluğuna atanmada esas alınacak kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına ve işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesi Anayasa'nın 13., 20. ve 128. maddeleriyle bağdaşmamaktadır.

..."

açıklamalarına yer verilmiştir (AYM, 2019).

Bu noktada belirtmek gerekir ki, Anayasa Mahkemesinin 2018/73 E. 2019/65 K. 24.07.2019 tarihli kararı ile Kanunun 28 inci maddesinin birinci fıkrasının (ç) bendinde, *"faaliyetlerin kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülmesi"* şeklinde belirtilen ifadelerin göz önünde bulundurulması neticesinde faaliyetleri yürütecek kamu kurum ve kuruluşlarının görev ve yetkilerinin şekli anlamda kanunla düzenlenmesi gerektiği, bir başka ifadeyle idarenin düzenleyici işlemleriyle bu görev ve yetkilerin tanınması halinde söz konusu hükmün uygulanmasının mümkün olmayacağı değerlendirilmektedir.

Kanunun 28 inci maddesinin birinci fıkrasının (ç) bendi Kanun kapsamı dışında tutulmuş olup hükme ilişkin gerekçede,

"Bunun gibi kişisel verilerin, milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi istisna olarak düzenlenmektedir. Buna göre Milli İstihbarat Teşkilatı ile diğer istihbarat birimlerinin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik faaliyetler kapsamında işlediği veriler Kanun kapsamı dışında tutulmaktadır. Aynı şekilde belirtilen amaçlarla, suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ve mali suçların araştırılması konusunda; yetkili birim tarafından yürütülen faaliyetler kapsamında işlenen veriler de bu istisna kapsamındadır. Bu konulardaki yetkili birimin; milli savunmayı, milli güvenliği kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olmak üzere mali araştırma yapmak, mali istihbarat elde etmek ve üretmek, veri toplamak, şüpheli işlem bildirimleri ve diğer bildirimleri almak, analiz etmek, değerlendirmek, inceleme yapmak ve ilgili kurumlarla paylaşmak suretiyle işlediği veriler de kapsam dışında tutulmaktadır."

açıklamalarına yer verilmiştir.

Ancak, kişisel verilerin işlenmesine ilişkin temel ilkelerin tüm işleme faaliyetlerinin özünde bulunması gerektiği, bu kapsamda, bir kişisel veri işleme faaliyeti her ne kadar Kanundan tam ve kısmi istisnaya tabi tutulmuş olsa da temel ilkelere uygun ve orantılı olarak bu faaliyetlerin gerçekleştirilmesi gerektiği belirtilmiştir (KVKK, 2019). Bu çerçevede, her ne kadar istihbari faaliyetler açısından Kanun hükümleri uygulanmamakta ise de bu hususun kötüye kullanılmasını önlemek amacıyla kişisel veri işleme faaliyetlerinin denetimini sağlayacak mekanizmaların bulunmasının uygun olacağı değerlendirilmektedir.

Söz konusu istisnalar veri sorumluları için öngörülmemiş olup veri işleme faaliyetleri bakımından düzenlenmiştir. Bu doğrultuda, istihbari olmayan faaliyetler açısından Kanun hükümlerinin uygulanabileceği değerlendirilmektedir.

Ulusal güvenliğe ilişkin kişisel veri işleme faaliyeti AB hukuku dışında tutulmuştur. Bu doğrultuda, ulusal güvenliğe ilişkin kişisel veri işleme faaliyetlerinde GVKT ve Direktif hükümleri uygulanmamaktadır. Uygulama örneği olarak Birleşik Krallık, istihbarat hizmetlerinde AB hukukunun aksine 108 No'lu sözleşmeyi gözeterek "Data Protection Act 2018" kapsamında özel düzenlemeler ile ulusal güvenlik kurumlarına ve bu kurumların gerçekleştireceği kişisel veri işleme faaliyetlerine ilişkin veri koruma usulü sağlamıştır. Bu düzenleme ile istihbari faaliyetler kapsamında gerçekleştirilecek kişisel veri işleme faaliyetlerine ilişkin birtakım ilkeler öngörülmüştür. Ayrıca, ilgili kişilere haklar da tanınmıştır. Bunlar, bilgi edinme hakkı, erişim hakkı, otomatik karar vermeyle yükümlü olmama hakkı, otomatik karar verme sürecinde müdahale hakkı, karar verme hakkında bilgi alma hakkı, işleme faaliyetine karşı çıkma hakkı ile düzeltme ve silme hakkı olarak sayılmıştır (Turan, 2021). Bununla birlikte, ulusal güvenlik için gerekli olması halinde istihbari hizmetlerin düzenlemeden muaf tutulacağı da belirtilmiştir. Aynı zamanda şeffaflık konusunda hükümlere yer verilmiştir (Department for Digital, Culture, Media & Sport, 2018).

SONUÇ

Kişisel verilerin korunması, başta özel hayatın gizliliğinin korunması olmak üzere temel hak ve özgürlükleri güvence altına almayı amaçlamaktadır. Ancak, kolluk ve istihbari faaliyetler söz konusu olduğunda kişisel verilerin işlenmesi disiplin altına almayı amaçlayan 6698 sayılı Kişisel Verilerin Korunması Kanununda yer alan tam ve kısmi istisnalar çerçevesinde Kanun hükümleri uygulanmamaktadır.

AB'de kişisel verilerin korunması, AB düzeyinde sağlanmaya çalışılmış olup bu çerçevede GVKT yürürlüğe konulmuştur. Bununla birlikte, "suçların önlenmesi, soruşturulması, ortaya çıkarılması, kovuşturulması ile cezaların infazı amacıyla" yetkili makamların kişisel veri işlemesine ilişkin ayrı bir düzenleme olarak Direktif, AB bünyesinde yürürlüğe konulmuştur. Bu Direktif ile belirtilen amaçlara yönelik gerçekleştirilecek kişisel veri işleme faaliyetlerinde belli bir sistematik düzen sağlanmaya çalışılmaktadır. Fakat bu Direktifin üye devletlerin iç hukukuna aktarılması gerekmekte olup henüz üye devletlerin tamamı iç hukukuna aktarmamıştır.

Direktif, 1 inci maddesinde belirtilen amaçlar doğrultusunda gerçekleştirilecek olan kişisel veri işleme faaliyetlerinin özel ihtiyaçlarını ve özellikli karakterini dikkate alarak veri koruma ilkelerini ayrıntılı bir biçimde düzenlemiş olup bireylerin hakları ile kolluk sürecinin ve adli sürecingereklilikleri arasında bir denge kurmaya çalışmıştır.

Normlar hiyerarşisinde yer alan normlar her zaman somut olaya uygulanacak normu tayin etmekte yeterli olmamaktadır. Hükümlerin herkese ve her olaya uygulanabildiği hükümleri içeren kanuna genel kanun, belli kişi ve olaylara uygulanan kanunlara ise özel kanun denilmektedir. Bu çerçevede Kanunun, genel nitelikte bir kanun olduğu değerlendirilmektedir.

Kolluk ve istihbari faaliyetler kapsamında, Kanun ve GVKT hükümlerinin birebir uygulanması gösterilen faaliyetlerin gizliliğine zarar verebileceği için bu hükümlerin doğrudan uygulanmaması gerektiği, ancak hukuk sistemimizde, Anayasada yer alan temel hak ve özgürlüklerin korunması ile kişisel verilerin korunması ilkelerinin göz önünde bulundurulması neticesinde de söz konusu alanlara yönelik Direktif benzeri ayrı bir düzenleme yapılması gerektiği değerlendirilmektedir. Keza, gizli bilgilere ulaşılması için de yasal düzenlemeye ihtiyaç bulunduğu açıktır. Böylelikle, faaliyet alanının amacı gözetilerek hem ilgili kişiler açısından hem de veri sorumluları açısında bilinmezlik neticesinde yaşanabilecek hak mahrumiyetlerinin önüne geçilebileceği düşünülmektedir.

Bu hususlar doğrultusunda, Kanunun 28 inci maddesinde yer alan tam ve kısmi istisnaların AB uygulaması ile tam olarak uyuşmadığı, bu çerçevede, mevcut iç hukuk düzenlemelerinin AB uygulaması ile uyumlaştırılabileceği değerlendirilmektedir. ◆

KAYNAKÇA

Dergi Makaleleri için:

◊ 1. BİLGİÇ, A. (2019), Türkiye'de İç Güvenlik Yapılanmasında Çoklu Genel Kolluk Sisteminin Kurumsallaşması, İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi, 6 (2), ss. 287-307, Erişim adresi: https://dergipark.org.tr/en/download/article-file/836917.

◊ 2. BOSTANCI BOZBAYINDIR, G. (2018), Avrupa Birliği Ceza Hukuku'nda Polis ve Ceza Adaleti Otoritelerine Yönelik 2018/680 Sayılı Direktif: Kişisel Verilerin Ceza Adalet Mekanizmalarında Korunmasına Getirilen Standartlar ve Direktife Yönelik Eleştiriler, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2018/2, ss. 51-103. Erişim adresi: https://www.jurix.com.tr/article/18552.

◊ 3. ATAK, S. (2010), Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, TBB Dergisi, Sayı 87, ss.90-120, Erişim adresi: http://tbbdergisi.barobirlik.org.tr/m2010-87-606#:~:text=Bu%20g%C3%BCvenceler%20aras%C4%B1nda%3B%20yaln%C4%B1zca%20ba%C4%9Flant%C4%B1l%C4%B1,dan%20denetlenmesi%20gibi%20g%C3%BCvenceler%20yerhttp://tbbdergisi.barobirlik.org.tr/m2010-87-,606#:~:text=Avrupa%20%C4%B0nsan%20Haklar%C4%B1%20S%C3%B6zle%C5%9Fmesi'nin,g%C3%B6s%2D%20terilmesi%20hakk%C4%B1na%20sahiptir%E2%80%9D.

◊ 4. KARAKURT, A. 2009, Sermaye Piyasası Kanunu Bağlamında İdari Yaptırımlar, TBB Dergisi, Sayı 85, ss. 137-172, Erişim adresi: http://tbbdergisi.barobirlik.org.tr/m2009-85-563.

Kitaplar için:

◊ 5. ÖZER, Y. M. (2020), Kişisel Verilerin Korunmasına Blok Zinciri Modeli: Vaatler ve Hukuki Engeller, Onikilevha Yayıncılık, İstanbul.

◊ 6. MUTLU, M. S. (2020), Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması,Adalet Yayınevi, Ankara.

◊ 7. GÖZLER, K. KAPLAN, G. (2014), İdare Hukukuna Giriş, Ekin Basın Yayın Dağıtım, Bursa.

◊ 8. GÜNDAY, M. (2013), İdare Hukuku, İmaj Yayınevi, Ankara.

◊ 9. SÜMER, H. H. (2016), İş Hukuku, Seçkin Yayıncılık, Ankara.

◊ 10. TURAN, M. (2021), Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, Seçkin Yayıncılık, Ankara.

◊ 11.YENİSEY, F. (2016), Ceza Muhakemesi Hukuku, Ankara: Seçkin Yayıncılık.

Tezler için:

◊ 12. CAN, N. (2020), Kolluk ve Adli Makamlar Tarafından İşlenen Kişisel Verilerin Korunması (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

◊ 13. BAYRAM, Z. (2009), Kolluğun Suç Öncesi ve Sonrası Kişisel Veri Toplama Yetkisi (Yayınlanmamış Yüksek Lisans Tezi), Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

◊ 14. ÇETİNDAĞ, A. F. (2004), Türk Anayasal Sisteminde Temel Hak ve Özgürlüklerin Sınırlanması Bağlamında Kamu Düzeni (Yayımlanmamış Yüksek Lisans Tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

◊ 15.IŞIK, S. (2012), Kamu Hukuku Perspektifinde Türkiye'de Kamu Güvenliği (Yayımlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

◊ 16. FİŞ, B. (2002), Önleyici, Koruyucu Faaliyetler Ve Meşru Menfaatler Bağlamında İşçiye Ait Kişisel Verilerin İşlenmesi (Yayınlanmamış Yüksek Lisans Tezi), Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

◊ 17.SARIHASAN ARKUN, B. (2010), İş Hukukunda İşçinin Sır Saklama Yükümlülüğü, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Elektronik Kaynaklar için:

◊ 18. İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, (AB) 2016/680 Sayılı Avrupa Parlamentosu ve Konsey Direktifi, İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, (AB) 2016/680 Sayılı Avrupa Parlamentosu ve Konsey Direktifi, Erişim adresi: https://itlaw.bilgi.edu.tr/media/2019/7/29/law-enforcement-directive-turkce.pdf, 20.12.2021.

◊ 19. European Data Protection Board, Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, Erişim adresi: https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf, 14.12.2021.

◊ 20. Handbook on European Data Protection Law, 2018, Erişim adresi: https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf, 18.04.2022.

◊ 21. Dijitalleşen Dünyada Kişisel Verilerin Korunması Konferansı, Erişim adresi: https://www.kvkk.gov.tr/Icerik/6947/DijitallesenDunyada-Kisisel-Verilerin-Korunmasi-Konferansi, 16.04.02021.

◊ 22. Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, Erişim adresi: https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf, 17.05.2022.

◊ 23. Örneklerle Kişisel Verilerin Korunması, Erişim adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a23bfe08-9b3a-4c2f8a97-a259dcc0e667.PDF, 07.02.2022.

◊ 24. Aday Memur Hazırlayıcı Eğitimi, Ceza Muhakemesi Hukuku Ders Notu, Erişim adresi: https://edb.adalet.gov.tr/Resimler/SayfaDokuman/26620201539387-CezaMuhakemesi%C4%B0HUKUKU.pdf, 03.04.2022.

◊ 25. Milli Emniyet Hizmeti Riyaseti, Erişim adresi: https://www.mit.gov.tr/ikinci_bolum_F.html#F, 15.02.2022.

◊ 26. Covid-19 Pcr Test Sonucu ve Aşı Bilgisi Uygulamalarına İlişkin Kamuoyu Duyurusu, Erişim adresi: https://www.kvkk.gov.tr/Icerik/7055/COVID-19-PCR-TEST-SONUCU-VE-ASI-BILGISI-UYGULAMALARINAILISKIN-KAMUOYU-DUYURUSU, 03.10.2022

◊ 27. İşyerlerinde iş sağlığı ve güvenliğinin sağlanmasına yönelik olarak 81 İl Valiliğine Covid-19 tedbirleri hakkında gönderilen yazı, Erişim adresi: https://www.csgb.gov.tr/cgm/duyurular/isyerlerinde-is-sagligi-ve-guvenliginin-saglanmasina-yonelik-olarak-81-il-valiligine-covid-19-tedbirleri-hakkinda-yazi-gonderildi/, 03.10.2022.

◊ 28. Statement on the processing of personal data in the context of the COVID-19 outbreak, Erişim adresi: https://edpb.europa.eu/sites/default/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf, 03.10.2022.

◊ 29. Anayasa Mahkemesinin 2018/73 E. 2019/65 K. 24.07.2019 tarihli kararı, Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2019/11/20191129-7.pdf, 10.05.2022.

◊ 30. Data Protection Act 2018 Factsheet-Intelligence Services Processing, Erişim adresi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711233/2018-05-23_Factsheet_4_-_intelligence_services_processing.pdf, 01.04.2022, s.1-4.

BİR HAK ÇATIŞMASI ALANI OLARAK KİŞİSEL VERİLERİN KORUNMASI VE BASIN ÖZGÜRLÜĞÜ

Tülay Selin GÜNER

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "Bir Hak Çatışması Alanı Olarak Kişisel Verilerin Korunması ve Basın Özgürlüğü" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Kişisel verilerin korunmasının bir hak alanı olarak tanınması yakın geçmişte meydana gelmiş olsa da mahremiyet olgusu ile bunun bir uzantısı olarak değerlendirebileceğimiz kişisel verilerin gizli tutulması eğiliminin, insanın toplum içerisinde yaşamaya başlamasından bu yana gündemde olduğu bilinmektedir. Özellikle mesleki yükümlülükler kapsamında kişisel verilerin gizli tutulmasına yönelik uygulamalar ile kimliği belirli ya da belirlenebilir bir bireye ait bilgilerin açığa çıkmaması sağlanmış, kimi zaman ise yasal düzenlemeler sayesinde bu bilgilerin gizli tutulması zorunlu kılınmıştır. Söz konusu düzenlemelerin belli bir alana ya da belli hususlara hasredilmiş olması, kişisel verilerin korunmasına yönelik olarak özel düzenlemelerin getirilmesi ihtiyacını ortadan kaldırmadığından zaman içerisinde kişisel verilerin korunması da ayrı bir hak alanı olarak kabul görmeye başlamıştır.

Diğer taraftan insanın, insan olması sebebiyle duygu, düşünce ya da kanaatlere sahip olmasının bir sonucu olarak bu duygu, düşünce ve kanaatleri farklı bireylere ya da kitlelere aktarma isteği, tarihsel süreç içerisinde birçok engelle karşılaşmıştır. Söz konusu engellemeler neticesinde gerek "ifade"nin gerek ifadenin

özel bir biçimi olarak "basın"ın korunması da gündeme gelmiş; gerek uluslararası gerek ulusal bazda yapılan düzenlemelerle ifade ve basın özgürlüğü koruma altına alınmıştır. Bu sayede toplumun farklı düşünce, kanaat ya da haberlere ulaşabilmesi güvence altına alınmış, ortaya konulan içeriklerin geniş kitlelere yayılması, bireylerin aydınlatılması ya da eleştirel içeriklerle kamusal tartışmalara katkı sağlanması mümkün kılınmıştır. Bununla birlikte; basın ve ifade özgürlükleri kapsamında ortaya konulan içeriklerin, kimliği belirli ya da belirlenebilir gerçek kişileri konu edinmesi halinde içerikte yer alan kişilerin, kişisel verilerinin korunmasını isteme hakkının var olduğunu söylemek ne derece mümkün ise söz konusu içeriğin yayımında ifade ya da basın özgürlükleri kapsamında hareket edildiğini de söylemek aynı derecede mümkün olduğundan yayımlanan bir içerikte kimliği belirli ya da belirlenebilir gerçek kişilere işaret edildiği ya da bu kişilere ilişkin bilgilerin doğrudan içerikte yer aldığı durumlarda, iki temel hakkın karşı karşıya gelmesi söz konusu olmaktadır.

Bu kapsamda, basın özgürlüğü ile kişisel verilerin korunmasını isteme hakkının bir yarışma durumuna yol açıp açmadığının ve yol açması halinde bu yarışmanın ne şekilde çözümlenebileceğinin incelenmesini hedefleyen çalışmada; Türk Hukukunda basın kavramı ve basının kapsamı, ifade ve basın özgürlüğü arasındaki ilişki, 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndan (Kanun) istisna bir hal olarak basın özgürlüğü kapsamında kişisel verilerin işlenmesinin hangi şartlar dahilinde gerçekleşebileceği ve Kişisel Verileri Koruma Kurulu'nun (Kurul) konuya ilişkin yaklaşımının ne şekilde olduğu inceleme konusu edilecektir.

BASIN KAVRAMI İLE KAVRAMIN BASIN ÖZGÜRLÜĞÜ VE İFADE ÖZGÜRLÜĞÜYLE OLAN İLİŞKİSİ

"İletişim", "Kitle İletişimi" ve "Basın" Kavramları

Sosyal bir varlık olarak insan, yaşamını bir topluluk içerisinde sürdürmekte ve sahip olduğu bilgi, duygu, düşünce, istek ve beklentilerini, tabiatı gereği bu topluluk içinde bulunan diğer insanlara aktarmaktadır (Dinçtürk, 2007). Bu bağlamda, üzerinde uzlaşılmış bir tanım verebilmek mümkün görünmemekle birlikte; belirli araçlar kullanarak, bilgi, düşünce ve tutumların karşılıklı aktarılmasını konu edinen faaliyetleri "iletişim" olarak tanımlamak mümkündür (Aziz, 2013).

İnsanlığın var oluşuna dayandırılabilecek kadar eski bir faaliyet olarak iletişim, tarihsel süreç içerisinde pek çok farklı biçimde görünüm kazanmıştır. Örneğin, insanların içinde yaşadıkları doğa ile bütünleştiği ve yaşamını sürdürmeye çalıştığı ilk dönemlerde, doğa kaynaklı etkiler ileti olarak algılanmış ve bu iletiye gösterilen içgüdüsel tepkilerle kendiliğinden bir iletişim kurulduğu kabul edilmiş; insanların birbiriyle iletişim kurma ihtiyacı sonucu duman, ateş, mağara resimleri gibi araçlar kullanarak ya da farklı sesler çıkararak birbirini bilgilendirmesi ya da uyarması faaliyetleri bunu izlemiştir (Gönenç, 2007). İnsanın konuşarak iletişim kurabilmesi ise iletişimde bir dönüm noktası olmuş; yazının bulunması ve akabinde matbaanın icadı, iletişim yöntemlerinin çoğalmasına etki ettiği kadar düşüncenin farklı insanlara ulaşabilmesine de imkân sağlamıştır.

İletişimin tarihsel süreç içerisinde geçirdiği değişim ve yaşanan ilerlemelerde, teknolojik gelişmelerin de büyük etkisi olmuştur. Daha hızlı ve kolay şekilde iletişim kurabilmeye olanak sağlayan telgraf, radyo, telefon, televizyon, bilgisayar gibi pek çok aracın insanlığın kullanımına sunulması, iletişimi yalnızca bireysel temelde gerçekleştirilen bir faaliyet olmaktan çok daha öte bir boyuta taşımış; sözü edilen araçlar, düşüncelerin açıklanması ve başkalarına yayılması bakımından da büyük önem kazanmıştır. Nitekim iletişimde bahse konu araçların kullanımı; bilgi, düşünce ve kanaatlerin geniş kitlelere yayılmasında önemli bir role sahip olmuş ve bilgi, düşünce, tutum ve kanıların, alıcı kesim durumundaki büyük ve dağınık bir kitleye, kitle iletişimi gerçekleştirmek üzere geliştirilmiş araçlarla iletilmesi süreci (Salihpaşaoğlu, 2007) olarak tanımlayabileceğimiz "kitle iletişimi" denilen bir kavramın ortaya çıkmasını sağlamıştır. Kitle iletişiminde kullanılan araçlar gelişen teknoloji ile zaman içerisinde farklılaşmış ve sayıca artmış olsa da kaynak tarafından verilen iletiyi çoğaltmaları bakımından ortak özellik göstermiş ve gazete, dergi, kitap, broşür gibi basılı materyaller ile sinema, film, radyo, televizyon, plak, kaset, video ve benzeri araçların bu kapsamda yer aldığı kabul edilmiştir (Aziz, 2013).

Bu noktada, düşünce ve kanaatlerin kitlelere yayılmasında etkin rol oynayan ve en önemli kitle iletişim araçları arasında yer alan "basın" kavramından da söz etmek gerekmektedir. Sözlük anlamıyla basın, "gazete, dergi gibi belirli zamanlarda çıkan yazılı yayınların bütünü, matbuat; bu tür iş yerlerinde görevli kimselerin tümü" (Türk Dil Kurumu, t.y.) şeklinde ifade edilmektedir. Bununla birlikte basın kavramının; dar anlamda, geniş anlamda ve en geniş anlamda olmak üzere öğretide farklı kullanımlarının bulunduğu görülmektedir. Dar anlamda basının, belirli zaman aralıklarıyla yayınlanan her çeşit haber, yorum ve fikirleri topluma ulaştırma amacıyla basılan gazete, dergi gibi basılmış eserleri; geniş anlamda basının, bunlara ek olarak her türlü yazı, resim, kâğıt ve benzer materyallerden oluşan kitap, el ilanı, broşür, reklam panoları gibi vasıtaları; en geniş anlamda basının ise basının maddi konuları, görevleri, basınla ilgili her tür ödev ve yükümlülükleri, basın özgürlüğü ve basın faaliyetlerini ifade ettiği belirtilmekte (Esendal, 2018) ve bu görüş doğrultusunda basının yazılı, görsel, işitsel ve ben-

zeri şekillerde kategorize edildiği kullanımlara da rastlanabilmektedir. Bununla birlikte öğretide basın kavramı ile kitap, gazete dergi gibi yayımlanmak üzere her türlü basım aracı ile basılan ve basılarak çoğaltılan kitle iletişim araçlarının ifade edildiği genel olarak kabul görmektedir (Akkurt, 2014; Akarcalı, 1989; Salihpaşaoğlu, 2007; Baykan, 2011; Yavuz Yayla, 2019). Öğretide bu kabulün temeline ilişkin olarak; geçmişi daha eskiye dayanan gazete, dergi, kitap gibi yayınların, hukuken korunmalarının farklı zeminlere dayandığı, basın özgürlüğü ve benzeri basın ile ilgili yasal düzenlemelerin bu ayrım gözetilerek yapıldığı ve bu itibarla sözlü/görsel basının, basın kavramı dışında tutulduğu ifade edilmektedir (Esendal, 2018). Bu doğrultuda, basın kavramının günlük hayattaki kullanımı ile bir hak alanı olarak kullanımında bazı farklılıkların bulunduğu anlaşılmaktadır. Bu farklılıklar temelde, bir kitle iletişim aracı olarak basının, düşünce ve kanaatleri kitlelere aktarırken kullandığı yöntem ile ilgilidir. Nitekim yukarıda da ifade edildiği üzere "bilgi, düşünce ve tutumların büyük ve dağınık bir kitleye, bu amaç için geliştirilmiş araçlarla iletilmesi" (Aziz, 2013) olarak tanımlayabileceğimiz kitle iletişimi; yalnızca basılı yayınlar ile sağlanmamakta, teknolojik gelişmeler neticesinde hayatımıza giren radyo, televizyon, internet, videobantları gibi birçok farklı araçla da gerçekleştirilebilmektedir (Esmer, 2014). Bu bakımdan basının, iletişim ve kitle iletişiminin bütününü ifade eden genel bir kavram olarak "medya"nın, yazılı mahiyete sahip olan bir alt başlığı olarak değerlendirildiğini söylemek mümkündür (Yıldız, 2012).

Türkiye Cumhuriyeti Anayasasında Basın ve İfade Özgürlüğü

Genel Olarak

Yukarıda kavramsal çerçevesi ile ortaya çıkış sürecine değinilen, düşüncelerin basılmış eserler yoluyla açıklanması özgürlüğü olarak nitelendirebileceğimiz basın özgürlüğü (Yıldız, 2012; Akkurt, 2014), Anayasa'nın 28. maddesinde düzenleme altına alınmış, yine Anayasa'nın 29. ve 30. maddelerinde süreli ve süresiz yayın hakkı ile basın araçlarının korunması anayasal güvenceye bağlanmıştır. Anayasa'nın, basın özgürlüğüne ilişkin genel düzenlemesi mahiyetini haiz 28. maddesinin birinci fıkrasında; basının hür olduğu ve sansür edilemeyeceği, basımevi kurmanın izin alma ve mali teminat yatırma şartına bağlanamayacağı belirtilmiş, ikinci fıkrasında ise; devletin, basın ve haber alma hürriyetlerini sağlayacak tedbirleri alacağı hükme bağlanmıştır. Düzenlemenin üçüncü fıkrasında basın hürriyetinin sınırlanmasında uygulanacak Anayasa hükümleri gösterilmiş, dördüncü fıkra ve devamında, basın faaliyetleri kapsamında gerçekleşebilecek suçlara ilişkin usul ve esaslar, yayınların toplatılması, zapt ve müsadere edilmesi ile geçici olarak kapatılmasına ilişkin düzenlemelere yer verilmiştir.

Basın özgürlüğünün sınırlama sebeplerine Anayasa'nın 28. maddesinin üçüncü fıkrasında yer verilmiş ise de bu sınırlamanın sınırını, temel hak ve özgürlüklerin sınırlanmasına ilişkin temel düzenleme olan Anayasa'nın 13. maddesi tayin etmektedir. Bilindiği üzere Anayasa'nın "Temel hak ve hürriyetlerin sınırlanması" başlıklı 13. maddesinde; *"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz"* düzenlemesine yer verilerek temel hak ve özgürlüklerin sınırlanmasında riayet edilmesi gereken sınırlar ortaya konulmuştur. Anayasa'nın 28. maddesinin üçüncü fıkrası ise sözü edilen şartlar dahilinde basın özgürlüğünün hangi durumlara dayalı olarak sınırlanabileceğini hüküm altına almakta olup, mezkûr düzenlemede basın özgürlüğünün, Anayasa'nın 26. ve 27. maddesi hükümleri doğrultusunda sınırlanabileceği belirtilmiştir.

Bu sınırlama sebepleri arasında gösterilen, Anayasa'nın "Düşünceyi açıklama ve yayma hürriyeti" başlıklı 26. maddesinde; *"Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet Resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir."* denilerek hakkın kullanımının; millî güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, Devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabileceği hükme bağlanmıştır. Mezkûr düzenlemenin dördüncü fıkrasında ise düşünceyi açıklama ve yayma hürriyetinin kullanılmasında uyulacak şekil, şart ve usullerin kanunla düzenleneceği ifade edilmiştir.

Kişinin dilediği şekil, zaman ve koşulda bir baskı, sınırlama ve zorlamaya maruz kalmadan bilgi ve fikir sahibi olabilme, özgürce düşünebilme, düşündüklerini hiçbir baskı altında kalmadan açıklayabilme, muhatabına iletebilme ve yayma imkânının elinde olması şeklinde tanımlayabileceğimiz (Özkepir, Kocaman ve Kart, 2020), ifade özgürlüğü olarak da bilinen bu özgürlük, gerçeği araştırma hususunda vazgeçilmez bir araç olarak, düşünebilen bir varlık olan insana entelektüel kapasitesini oluşturma ve bunu geliştirme imkânı sunmakta; aynı zamanda karar alma süreçlerine etkin katılım sağlama, ülke yönetiminde söz sahibi olma gibi işlevleri sayesinde demokratik rejimler bakımından önemli bir görev

üstlenmektedir (Uygun, 2014). Bilgiye ya da haberlere özgürce erişebilme, sınırlama ya da yönlendirmelere tabi olmadan kanaat ve fikir sahibi olabilme ve sahip olunan düşünce ya da kanaatleri özgür bir şekilde açıklayabilme ya da yayabilme şeklinde sıralayabileceğimiz üç temel unsurdan oluşan ifade özgürlüğünün kapsamında, sadece ifadenin içeriğinin değil, ifadenin yer aldığı açıklama ya da yayma araçlarının da bulunduğu kabul edilmektedir (Özkepir, Kocaman ve Kart, 2020). Bu bakımdan ifade özgürlüğünün; yalnızca bir fikrin dışa vurulması ile sınırlı olmayan, o fikre ya da bilgiye ulaşma fırsatı ve serbestisi ile birlikte değerlendirilen bir konumda bulunduğunu söylemek mümkündür (Sunay, 2000). Dar anlamıyla bir düşüncenin, fikrin ya da inancın, çeşitli yollarla, herhangi bir engel veya yasakla karşılaşmaksızın başkalarına aktarılmasını, geniş anlamıyla başka düşüncelere ulaşabilmeyi, din ve vicdan hürriyetini, aynı zamanda sahip olunan düşünce doğrultusunda bireysel ya da toplu hareket ve davranışta bulunabilmeyi içeren ifade özgürlüğü (Zarplı, 2008); söz, yazı, müzik, resim, görüntü gibi farklı şekillerde kullanılabilmektedir (Yavuz Yayla, 2019).

Anlaşılacağı üzere ifade özgürlüğü; temel itibarıyla bir düşünce, kanaatin ya da yargının başkalarına açıklanmasını kapsamaktadır. Bununla birlikte sözü edilen açıklama faaliyetinde kullanılan yöntem ve araçların değişkenliği ile ifade özgürlüğünün farklı hak ve özgürlükleri bünyesinde barındıran kapsamlı bir mahiyete sahip olması; ifade özgürlüğünün alt kategorileri olarak da değerlendirilebilecek farklı hakların ortaya çıkışına da zemin hazırlamıştır. Bu bağlamda ifade özgürlüğünün gazete, dergi, kitap gibi basılmış eserler yoluyla kullanılan görünümünün, basın özgürlüğünü ifade ettiğini söylemek mümkündür (Akkurt, 2014; Yılmaz Avcı, 2014). Kanaatimizce basın özgürlüğünün sınırlama sebepleri bakımından ifade özgürlüğüne yapılan yollama da bunun bir sonucudur. Bu yönüyle ifade özgürlüğünün, basın özgürlüğüne kaynak teşkil ettiği ve bu iki özgürlüğün ayrılmaz bir ilişki içerisinde bulunduğu söylenebilir. Bununla birlikte basın özgürlüğünün, mahiyeti gereği ifade özgürlüğünden ayrılan ve özel bir korumayı gerektiren farklı alanlara ve koruma sahalarına sahip olduğunun da ifade edilmesi gerekmektedir. Anayasa'da özel olarak belirtilen ve basın özgürlüğüne ilişkin düzenlemeler arasında yer verilen basımevi kurma, süreli ve süresiz yayın haklarının izin ve mali teminat şartına bağlanamaması, basımevi ve eklentileri ile basın araçlarının suç aleti olduğu gerekçesiyle zapt, müsadere ya da işletilmekten men edilememesi bu kapsamda öngörülen hükümler arasında değerlendirilebilir. Yine; medyada tekelleşmenin önlenmesi, basın çalışanlarının iş güvencesinin sağlanması ve haber kaynağını açıklama hakkı gibi haklar ve düzenlemelerin, bu kapsamda yer aldığı söylenebilecektir. Bu yönüyle basın özgürlüğünün, ifade özgürlüğünün özelleşmiş bir biçimi olduğunu ifade etmek mümkündür (Armağan, 1998). Bununla birlikte Anayasa'da yer alan ve basın özgürlüğüne yönelik olan mezkûr

düzenlemelerin, ifade özgürlüğü bahsi yerine "basın hürriyeti" başlığı altında ya da bu düzenlemenin devamında, ifade özgürlüğünden ayrı bir şekilde ele alınmış olması, Türk hukuku bakımından ifade ve basın özgürlüklerinin tamamen ayrı hak ve özgürlükler olduğu yönünde bir fikri de gündeme getirebilecektir. Bu hususta kanaatimiz; basın özgürlüğünün, ifade özgürlüğünün belli araçlarla kullanılabilen özel bir görünümü olmasına karşın ayrı düzenlemelerle koruma altına alınmış ayrı haklar olduğu yönündedir (Salihpaşaoğlu, 2007).

"Basın Kanunu ile "Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun" Işığında "Basın" Kavramına Yeni Bir Bakış

Bilindiği üzere 5187 sayılı Basın Kanunu, 09.06.2004 tarihinde kabul edilmiş olup, 26.06.2004 tarihli ve 25504 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Basın Kanunu'nun yürürlüğe girdiği tarihten bu yana, Anayasa Mahkemesi'nin (AYM) iptal kararı doğrultusunda mezkûr Kanun'un 9. maddesinde yapılan değişiklik ile 6352 sayılı Kanun ile yargılama süreçlerine ilişkin olarak 19, 26 ve Geçici 3. maddelerinde yapılan değişiklikler haricinde esaslı bir değişiklik geçirmediği bilinmektedir. Buna karşın, 5187 sayılı Basın Kanunu'nun yürürlüğe girdiği 2004 yılından günümüze değin geçen yirmi yıla yakın zaman zarfında teknolojinin yanı sıra basın ve yayın araçlarında da büyük ve köklü değişimler gerçekleşmiş, özellikle basının bilgi, haber ve düşünceleri ortaya koyduğu yöntemlerde meydana gelen değişiklikler; basına, basın araçlarına ve basın mensuplarına bakış açısında bir değişikliğe gidilmesini zaruri kılmıştır.

Bu bakış açısıyla ortaya konulan ve 18.10.2022 tarihli ve 31987 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 7418 sayılı "Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun"un gerekçesinde; teknoloji ve bunun sonuçları arasında yer alan internetin, diğer kitle ve iletişim araçlarını geride bıraktığı, giderek artan kolay erişim ve iletişim yöntemlerinin sosyal medya kavramını toplumsal yaşamın merkezine taşıdığı, internetin, haber ve bilgiye erişimi kolaylaştırmasının ve hızlandırmasının bir sonucu olarak sosyal medya kullanımının da arttığı, sosyal medya platformlarının da çeşitlenmesiyle kişilik hakkı ihlallerinin de yaygınlaştığı vurgulanarak bu ihlallerle mücadele edilebilmesi amacıyla mevcut düzenlemelere ek yeni düzenlemelerin yapılması gerektiği vurgulanmıştır (Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun Teklifi (2/4471) ile Dijital Mecralar Komisyonu ve Adalet Komisyonu Raporları, t.y.). Bu kapsamda, mezkûr Kanun'da kendisine yer bulan en önemli hususlardan biri, konumuz açısından da önem arz eden internet haber sitelerinin durumuna ilişkindir. Nitekim 7418 sayılı Kanun'un yürürlüğe girmesi ile 5187 sayılı Basın Kanunu'nun kapsamına internet haber sitelerinin de eklenmesi sağlanmış, "internet

haber sitesi" kavramı ise mezkûr Kanun'da, "internet ortamında, belirli aralıklarla haber veya yorum niteliğinde yazılı, görsel veya işitsel içeriklerin sunumunu yapmak üzere kurulan ve işletilen süreli yayın" şeklinde tanımlanmıştır. Bu itibarla, teknolojik gelişmelerin izlediği seyir de dikkate alınarak internet haberciliğinin, basın ile olan yakın ilişkisi gözetilerek kanaatimizce isabetli bir şekilde internet haberciliğinin de basın faaliyetleri kapsamında düzenlenen hak ve yükümlülüklere sahip olması amaçlanmıştır.

5187 sayılı Basın Kanunu'nun 7418 sayılı Kanun ile değiştirilmeden önceki halinde; "basın" kavramı ile esasen yazılı ve basılı formatta ortaya konulan, basım araçları ile basılan ve bu yolla çoğaltılabilen kitle iletişim araçları kapsama alınmakta ise de kitle iletişim araçlarının basılı eserlerle sınırlı olmaması, bir diğer ifade ile düşünce, haber ya da kanaatlerin aktarımında "medya" olarak tanımlayabileceğimiz iletişim ve kitle iletişim araçlarının aktif rol oynaması, "basın" kavramının yalnızca yazılı ve basılı eserlerle sınırlı tutulması fikrinin önüne geçmektedir. Özellikle içinde bulunduğumuz dijital çağda bilgiye erişimin ağırlıklı olarak internet, sosyal medya ve diğer dijital platformlar aracılığıyla gerçekleşmesi; gün geçtikçe gazete ve dergi gibi basın araçlarının güç kaybetmesine sebep olmakta, bu durum internet üzerinden ya da başka medya araçlarıyla gerçekleştirilen faaliyetlerin, nitelik itibarıyla basın faaliyeti olarak kabul edilmesinin mümkün olduğu durumlarda "basın" kavramının daha geniş bir kapsamda değerlendirilmesini zorunlu kılmaktadır. Nitekim Türkiye İstatistik Kurumu **(TÜİK)** 2012 yılı verilerine göre sırasıyla 3004 ve 4105 olarak açıklanan gazete ve dergi sayıları, 2021 yılında 2071 ve 2389'a gerilediği gibi, 2020 yılında sırasıyla 2164 ve 2582 olarak açıklanan gazete ve dergi sayıları, bir önceki yıl olan 2020 yılına göre de %6'lık bir azalış göstermiştir (TÜİK, t.y.). Benzer bir durum gazete ve dergilerin yıllık tirajlarında da görülmekte olup, 2020-2021 döneminde gazete ve dergi tirajları arasında %7,2'lik bir fark olduğu TÜİK tarafından açıklanmıştır. (TÜİK, t.y.) Bu istatistiklere paralel olarak; 2011 yılında %42,9 olan "bireylerde internet kullanımı"nın 2021 yılında %82,6'ya ulaştığı, aynı yıl "hanelerin internet erişimi"nin %92 olarak açıklandığı göz önüne alındığında internet haberciliği ve sosyal medyanın basın faaliyetleri bakımından arz ettiği önemi anlamak daha da kolaylaşacaktır. Bu bakımdan; internet haberciliği kapsamında gerçekleştirilen faaliyetlerin, süreli yayın faaliyeti olarak değerlendirilmesini esas alan düzenlemenin yasalaşması ile internet haberciliği ve buna bağlı diğer hususların Basın Kanunu içerisinde açık bir şekilde konumlandırılması sağlanmış olduğundan basının yazılı/görsel/işitsel gibi farklı kategorilere ayrılmasına gerekçe olarak gösterilen fikir ayrılıklarının da büyük ölçüde son bulacağı düşünülebilir. Bununla birlikte Anayasa sistematiği içerisinde basın özgürlüğünün yazılı ve basılı eserlerle ilişkilendirilmesine gerekçe olarak gösterilen "basımevi kurma", "süreli

ve süresiz yayın haklarının izin ve mali teminat şartına bağlanamaması", "basımevi ve eklentileri ile basın araçlarının suç aleti olduğu gerekçesiyle zapt, müsadere ya da işletilmekten men edilememesi" gibi hükümler bağlamında mevcut tartışmaların devam etmesi de ihtimal dahilinde bulunduğundan kanaatimizce konunun ayrı kanunlar ile düzenlenmesi ya da Anayasa'daki mevcut hükümlerin ifade özgürlüğünü de içerecek şekilde daha kapsayıcı bir şekilde kaleme alınması, sorunun kalıcı bir şekilde çözümlenebilmesi adına önemli bir yaklaşım olacaktır.

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU'NDAN İSTİSNA BİR HAL OLARAK İFADE ÖZGÜRLÜĞÜ VE BASIN FAALİYETLERİ

28/1-c Düzenlemesinin Şartları

Kişisel veri işleme faaliyetleri bakımından ana kural; aydınlatma yükümlülüğünün yerine getirilmesi, gerekli teknik ve idari tedbirlerin alınması, bir işleme şartının bulunması ve genel ilkelere riayet edilmesi şartıyla kişisel verilerin işlenebilmesidir. Bununla birlikte kanun koyucu; belirlediği bazı durumlarda gerçekleşecek kişisel veri işleme faaliyetlerini, kısmen ya da tamamen Kanun kapsamı dışında bırakmıştır. Kanun'un 28. maddesinde düzenlenen ve "istisna" olarak ifade edilen bu haller, sınırlı sayıda düzenleme altına alınmış olup faaliyet bazında Kanun hükümlerinin uygulanmasını devre dışı bırakmaktadır. Diğer bir deyişle işleme faaliyetini gerçekleştiren veri sorumlusundan bağımsız olarak, mezkûr düzenlemede gösterilen haller kapsamında gerçekleştirilecek kişisel veri işleme faaliyetlerine Kanun hükümleri uygulanmamaktadır. Anılan düzenlemenin birinci fıkrasının (c) bendi; *"Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi."* hükmünü amirdir. Mezkûr düzenleme ile kişisel verilerin "ifade özgürlüğü" kapsamında işlenmesi halinde, diğer şartların da yerine getirilmiş olması kaydıyla faaliyetin Kanun hükümlerine tabi olmayacağı hüküm altına alınmış olup bu şartlar; milli savunmanın, milli güvenliğin, kamu güvenliğinin, kamu düzeninin, ekonomik güvenliğin, özel hayatın gizliliğinin ya da kişilik hakkının ihlal edilmemesi ile ifade özgürlüğü kapsamında gerçekleştirilen faaliyetin suç teşkil etmemesi olarak öngörülmüştür. Bu bakımdan, sözü edilen kavramların açıklanması anılan düzenlemenin kapsamının anlaşılabilmesi için kritik önem taşımaktadır.

İfade özgürlüğü kapsamında kişisel verilerin işlenmesi durumunda faaliyetin Kanun hükümlerinden istisna tutulabilmesi için uyulması gereken ilk koşul, işleme faaliyetinin milli savunmayı ihlal etmemesi olarak düzenlenmiş olup; "milli sa-

vunma" kavramının anlaşılabilmesi, öncelikle savunma kavramının açıklanmasını gerektirmektedir. Temel itibarıyla savunma ise bir saldırıya karşı koymayı ifade etmektedir (Türk Dil Kurumu, t.y.). Saldırının bir bireye yönelmesi kadar ülkeye yönelmesi de söz konusu olabildiğinden devletler, kendi hakimiyet sahası içerisinde bulunan alanlara yönelik her türlü tehdidi göz önüne alarak bu tehdidin bir saldırıya dönüşmemesi adına gerekli tedbirleri almakta ve uygulamaktadır (Kalyon, 2008). Bu bakımdan bir saldırı tehdidinin ya da saldırının bir ülkeye yönelmesi halinde ilgili devletin, kendi ülke sınırlarını söz konusu saldırıya ya da tehdide karşı koruması "milli savunma" kavramını ifade etmekte olup milli savunma temelde ülkenin dış saldırılara karşı korunmasını konu edinmektedir (Yavuz Yayla, 2018). Bu kapsamda bir ulusa yönelen ya da yönelebilecek olan bir saldırıya karşı hangi tedbirlerin alınabileceği, bu tedbirlerin ne zaman ve nasıl uygulanabileceği, hangi kaynakların, hangi ölçüde, ne kadar ve nasıl kullanılabileceği gibi hususlara yönelik olarak gerçekleştirilecek faaliyetlerin de milli savunma kavramı kapsamında yer aldığı söylenebilecektir (Kalyon, 2008).

Bu noktada "ülke" ve saldırı tehdidi bağlamında "tehdit" kavramlarının da değerlendirilmesi gerekmektedir. Sözlük anlamıyla "ülke", "bir devletin egemenliği altında bulunan toprakların tümü, diyar, memleket" (Türk Dil Kurumu, t.y.) şeklinde tanımlanmakta olup, söz konusu tanımdan da açıkça görüleceği üzere ülke kavramı, devletin hakimiyet sahası ile doğrudan bağlantılı bir konumda bulunmaktadır. Bu yönüyle ülke, devletin hakimiyet sahası içinde yer alan kara sahası, hava sahası, karasuları ve varsa adalarını kapsayan gerçek anlamda ülkeyi ifade etmektedir (Kaya, 2020).

Ülkeye yönelmiş bir saldırı tehdidi bağlamında "tehdit"ten ne anlaşılması gerektiği de bu noktada karşımıza çıkan diğer bir sorudur. Nitekim, her şeyden önce herhangi bir tehlikenin, muhatabı tarafından algılanmadığı sürece "tehdit" olarak değerlendirilmesi fiilen imkân dahilinde değildir. Diğer taraftan ülkeye yönelmiş tehlikenin, ne aşamada tehdit olarak değerlendirilebileceği de söz konusu değerlendirmeyi sübjektif bir hale getirmektedir. Bu bakımdan tehdit kavramının genel geçer bir tanımlanmasının yapılması kanaatimizce mümkün görünmemektedir. Bununla birlikte öğretide Yavuz Yayla, konuyu "güvenlik" kavramı üzerinden ele almakta ve güvenlik kavramını, *"güvensizlik ihtimallerinin ortadan kaldırıldığı kaygı ve tehdidin olmama durumu"* şeklinde tanımlayarak genel güvensizlik halini, tehdit olarak değerlendirmekte, tanım içerisinde yer alan tehdit kavramının ise bir yönüyle gerçek olgu ve olaylara diğer yönüyle algı ve tahminlere dayandığını belirtmektedir (Yavuz Yayla, 2018). Söz konusu tespitlerden yola çıkılarak saldırı tehdidinin, ülkeye yönelik olarak bir saldırının gerçekleşeceğine ilişkin mevcut emarelerin bulunması ya da somut durumun hal ve şartlarının değerlendirilmesi

neticesinde bu yönde bir kanaatin oluşması sonucunda oluşan güvensizlik durumu şeklinde ifade edilmesi mümkündür.

Mezkûr düzenlemede yer verilen ikinci koşul, işleme faaliyetinin milli güvenliği ihlal etmemesidir. Milli güvenlik kavramı, tarihsel olarak devlet kavramı kadar eskiye dayanmakla birlikte, kavrama yüklenen anlamın zamanla farklılaştığı görülmektedir (Yavuz Yayla, 2018). Bu farklılaşmanın temelinde; milli güvenlik kavramının, algılanma biçiminde meydana gelen değişiklikler ile tehditlerin farklı şekiller ve boyutlarda ortaya çıkmasının bulunduğu söylenebilir. Nitekim başta savaşlarla ilgili askeri ihtiyaçlar ve düzenlemeler için "milli savunma" kavramının karşılığı olarak kullanılan milli güvenlik kavramı (Yavuz Yayla, 2018), II. Dünya Savaşı'ndan Soğuk Savaş döneminin sonuna kadar çoğunlukla devlet merkezli olarak ve askeri yaklaşım çerçevesinde dar bir bakış açısıyla ele alınmıştır (Arslan, 2022). Bununla birlikte I. Dünya Savaşı ile evrensel nitelik kazanmaya başlayan milli güvenlik kavramının, II. Dünya Savaşı ve sonrasında bilimsel anlamda ele alınmaya başlayarak mevcut anlamını kazandığı (Yavuz Yayla, 2018) ve kavramın kapsamının suç faaliyetleri, terörizm ve göçü içerecek şekilde genişletildiği kabul edilmektedir (Arslan, 2022).

Bu noktada kavrama dair net bir çerçevenin çizilemediğinin de belirtilmesi gerekmektedir. Öğretide bu duruma gerekçe olarak; kavramın "bilimsel" bir nitelik taşımaması, teknik anlamda hukuki bir kavram olmaması ve kavramın salt askeri bir kavram olarak değerlendirilmesi durumunda, askeri alan dışında kalan unsurlarının dışlanması sebebiyle eksik bir tanımlamada bulunulması, kavramın siyasi, ekonomik ve hukuki olmak üzere çeşitli yönlerinin bulunması gibi sebepler gösterilmektedir (Çınarlı, 2015). Bu bakımdan kavrama ilişkin farklı tanımlamalarda bulunulması yoluna gidildiği ve yapılan tanımlarda milli güvenliğin farklı unsurlarına temas edildiği görülmektedir. Örneğin, öğretide Yavuz Yayla, kavramın yurt içi ve yurt dışı olacak şekilde ülke güvenliğinin sağlanmasını, bu yönüyle özellikle askeri faaliyetleri ve dış güvenliği sağlayacak şekilde gerçekleştirilen eylemleri ifade ettiğini belirtmekte iken (Yavuz Yayla, 2018); Tunç ve Döner, kavramı dar ve geniş anlamda ele alarak dar anlamda milli güvenliğin yalnızca milli savunma ile ilgili sorunları ele aldığını ve olağanüstü hal rejimi sonucunda alınacak önlemleri içerdiğini, geniş anlamda ise toplumsal hayatta karşımıza çıkabilecek her şeyin milli güvenlik konusu kapsamında yer alabileceğini ifade etmektedir (Tunç ve Döner, 1998). Kanaatimizce milli güvenlik kavramının, dar anlamda ele alınarak yalnızca askeri bir kavram olarak tanımlanması, ortaya çıkacak sonuç bakımından "milli savunma" ile "milli güvenlik" kavramlarını eş tutmak anlamına geleceğinden bu noktada "savunma" ile "güvenlik" kavramları arasında bir fark bulunup bulunmadığı meselesine odaklanılması gerekmektedir. Yukarıda, savunmanın te-

mel itibarıyla "bir saldırıya karşı koyma"yı ifade ettiğinden söz edilmişti. Güvenlik ise sözlük anlamıyla "toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu"nu ifade etmektedir (Türk Dil Kurumu, t.y.). Bu bakımdan güvenlik kavramının, savunma kavramına nazaran daha geniş bir kapsama sahip olduğu, diğer bir ifade ile savunmanın, güvenlik kavramının alt başlıklarından birini teşkil ettiği anlaşılmaktadır. Mülga 2945 sayılı Milli Güvenlik Kurulu ve Milli Güvenlik Kurulu Genel Sekreterliği Kanununun ikinci fıkrasının (a) bendinde de kavramın; *"Devletin anayasal düzeninin, milli varlığının, bütünlüğünün, milletlerarası alanda siyasi, sosyal, kültürel ve ekonomik dahil bütün menfaatlerinin ve ahdi hukukunun her türlü dış ve iç tehditlere karşı korunması ve kollanması"* şeklinde tanımlanmış olması, milli güvenlik kavramının sırf askeri bir kavram olmaktan öte bir anlamla yorumlandığı ve farklı boyutlarının olduğu yönündeki yaklaşımları desteklemektedir. Sözü edilen tanım ile "tehdit" kavramının sahip olduğu anlam birlikte değerlendirildiğinde, milli güvenlik kavramının iç güvenliğin sağlanması ve dış güvenliğin sağlanması olmak üzere iki temel meselesinin bulunduğu anlaşılmaktadır. Bu noktada dış güvenlik kavramı, "savaşta ve barışta, dış ülkelerden gelen tehlikelere karşı devlet tüzel kişiliğinin korunması" (Çınarlı, 2015) şeklinde ifade edilecek olursa devletin ülkesine yönelmiş mevcut ya da olası saldırıların önlenmesine yönelik tüm faaliyetlerin bu kapsamda yer aldığı söylenebilecektir. İç güvenlik ise devletin egemenlik sınırları içindeki emniyet ve asayiş durumuna vurgu yapan bir kavram olup; temel itibarıyla ülke sınırları içerisindeki insanların can ve mal güvenliğinin, toplumsal düzenin, temel hak ve özgürlükler ile rejimin temel değerlerinin korunmasını ifade etmektedir (Çınarlı, 2015). Bu bakımdan milli güvenlik kavramının, ülkeye yönelmiş olan somut bir saldırı ya da saldırı tehdidinden bağımsız olarak devletin iç ve dış güvenliğinin sağlanmasına yönelik olarak gerçekleştirilen faaliyetlerin tümünü kapsadığını söylemek mümkündür.

Düzenlemede yer verilen üçüncü koşul, kamu güvenliğinin ihlal edilmemesi olarak ifade edilmiştir. Milli savunma ve milli güvenlik kavramlarına benzer şekilde, kamu güvenliği kavramına ilişkin olarak da üzerinde uzlaşı sağlanmış bir tanım bulunmamakta olup bu durumun sebebine ilişkin olarak "kamu" ve "güvenlik" kavramlarının ne olduğu hakkındaki görüş ayrılıkları gösterilmektedir. Bilindiği üzere güvenlik kavramı, temel olarak tehdit altında bulunmama durumunu ifade etmektedir. Kamu kavramı ise devlet ve devletin organlarını ya da toplumu ifade etmek üzere kullanılabilmektedir. Bu bakımdan güvenlik, topluma yönelik bir tehdidin söz konusu olduğu durumlarda ilgili devlet bakımından çözülmesi gereken bir sorun halini almaktadır. Bu bağlamda kamu güvenliğinin ise; bir ülkede yaşayan insanların başta can ve mal güvenliği olmak üzere temel hak ve özgürlüklerine ya da devletin bizzat kendisine yönelen bir tehlikenin, gerekirse

zor kullanılması suretiyle önlenmesi ve ihlalin meydana gelmesi halinde etkilerinin ortadan kaldırılması amacıyla yapılan devlet faaliyetleri olarak ifade edilmesi mümkündür (Kızılyel, 2014). Bu noktada iç güvenliğin sağlanmasını da kapsamına alan milli güvenlik kavramı ile kamu güvenliği kavramının arasındaki farkın da ortaya konulması gerekmektedir. Bilindiği üzere, üniter yapının korunması ve ulusun tekliği bağlamında karşımıza çıkan sorunların, duruma göre milli güvenlik veya kamu güvenliği meselesi olarak değerlendirilebilmesi mümkün olup bu noktada yönelen tehlikenin boyutunu dikkate almak gerekmektedir (Özdemir, 2016). Anılan değerlere yönelen tehlikenin ancak düzenli askeri birliklerle giderilebilecek noktada olduğu bir durumda milli güvenliğin; bu boyutta olmayan tehlikeye karşı güvenlik tedbirlerinin alınması ihtiyacının doğduğu hallerde ise kamu güvenliğinin söz konusu olabileceği söylenebilir (Özdemir, 2016). Diğer bir ifadeyle milli güvenlik, kamu güvenliğine nazaran daha yoğun ve büyük bir tehlikenin varlığı halinde söz konusu olmakta iken kamu güvenliği, vatandaşların yaşam hakkının korunmasının devamlılığı ve güvenliğinin devlet sorumluluğu altında korunması faaliyeti olarak, kamusal alan ile özel alan arasındaki emniyet hizmetlerini içermektedir (Özdemir, 2016).

İstisna hükümlerinin uygulanması bakımından aranan dördüncü şart, kamu düzeninin ihlal edilmemesi olarak hüküm altına alınmıştır. Kamu düzeni; genel ve soyut bir kavram olarak temel itibarıyla toplum menfaatlerine yönelmiş olan, uyulmasında ve korunmasında toplumun ve devletin menfaatinin bulunduğu kurallar bütününü ifade etmektedir (Bayra, 2020). Bu yönüyle kamu düzeni, göreceli ve değişken bir yapıya sahip ise de toplumsal hayatta düzenin ve barışın hâkim olması ve devletin işleyişini bozması muhtemel unsurların yokluğu kamu düzeninin içeriği bakımından vazgeçilmezdir (Bayra, 2020).

AYM; kamu düzeni kavramına ilişkin olarak bazı değerlendirmelerde bulunduğu bir kararında, öğretide kamu düzeni kavramına ilişkin olarak gerçekleştirilen tanımlamaların incelenmesi sonucunda kamu düzeninin, "toplumun huzur ve sükûnunun sağlanmasını, devletin ve devlet teşkilâtının muhafazasını hedef tutan her şeyi ifade ettiği, bir başka deyimle cemiyetin her sahadaki düzeninin temelini teşkil eden bütün kuralları kapsadığı sonucuna varıldığı"ndan söz ederek "ilk bakışta doğrudan doğruya bir ilgisi görülmeyen birçok konularla birlikte ve memleket güveni de dâhil olmak üzere toplumun her alanda düzenini sağlayan kuralların hedef tutulduğunu" ifade etmiş ve bu kuralların bozulması halinde kamu düzeninin bozulacağını belirtmiştir (Anayasa Mahkemesi Kararlar Dergisi, 1971). Karardan da anlaşılacağı üzere kamu düzeni, oldukça geniş bir kapsama sahip bir kavram olup, kavramın, "bir ülkede yaşayan halkın günlük yaşantısının güvenlik, sağlık, dirlik ve esenlik içinde sürdürülmesi için alınan önlemler ile bu

doğrultuda gerekli koşulların sağlanması" şeklinde tanımlanması mümkündür (Özdemir, 2016).

İstisna hükümlerinin uygulanması bakımından aranan beşinci şart; ekonomik güvenliğin ihlal edilmemesidir. Üzerine farklı tanımlamalar yapılmış olmakla birlikte temel anlamda ekonomik güvenlik, "devletlerin varlığının sürekliliğini ve halkın refahını sağlayan, stratejik ekonomik unsurlarının korunması ile olası tehdit ve risklere karşı hazırlıklı olma hali" şeklinde ifade edilebilir (Kocatepe, 2019). Bu bağlamda söz konusu amaca yönelmiş faaliyetlerin, diğer şartların da sağlanması koşuluyla istisna kapsamında yer alacağı söylenebilir.

Düzenlemede yer verilen altıncı şart ise kişilik haklarının ihlal edilmemesidir. Bu noktada "kişilik hakkı"nın tanımı ve hangi hakların kişilik hakkı kapsamında yer alabileceği, düzenlemenin anlaşılması ve uygulanması bakımından kritik önem taşımaktadır. Bununla birlikte, pek çok düzenlemede kendisine yer bulan "kişilik hakkı" kavramının Türk Medeni Kanunu'nda tanımına yer verilmediğini, mehaz düzenlememiz olan İsviçre Medeni Kanununun da konuya ilişkin bir tanımlamaya gitmediğini belirtmek gerekmektedir. Öte yandan temel olarak kişilik hakkının, "insanın insan olması dolayısıyla ayrılmaz bir biçimde sahip olduğu hakları" şeklinde ifade edilebilmesi mümkündür (Oğuzman, Seliçi ve Oktay Özdemir, 2012). Bu bakımdan "kişilik hakkı"nın, bireyi birey kılan, kişinin kişiliğini oluşturan ve bu itibarla korumaya değer görülen, başta yaşam hakkı olmak üzere kişinin bedensel ve ruhsal bütünlüğü, cinsel dokunulmazlığı, sağlığı, onuru, saygınlığı, özel yaşamının gizliliği, özgürlüğü, sözleri, resmi, ismi gibi insana ait, bireysel ve kişisel değerlerini konu edindiği genel kabul görmektedir (Serozan, 2018; Şimşek, 2008; Oğuzman ve diğerleri, 2012; Dural ve Öğüz, 2018; Akipek, Akıntürk ve Ateş, 2015).

Bu noktada, hem kişilik hakkının bir parçasını oluşturan hem de Kanun'un 28/1-c düzenlemesinde ayrıca ve açıkça sayılarak faaliyetin istisna kapsamında değerlendirilebilmesi için yedinci bir şart olarak aranan özel hayatın gizliliğinin ihlal edilmemesinden ve bu bağlamda "özel hayat" kavramından söz etmek gerekmektedir. Güncel, dinamik ve karmaşık yapıya sahip bir kavram olarak "özel hayat", öğretide farklı yazarlar tarafından farklı şekillerde tanımlandığından kavrama dair üzerinde uzlaşılmış bir tanım verebilmek oldukça güçtür. Bununla birlikte öğretide pek çok taraftar toplayan, Alman hukuku kökenli "Üç Alan" teorisi, konuyu daha basit bir çerçeve ile ele alarak kişinin yaşam alanını "ortak hayat alanı", "özel hayat alanı" ve "gizli hayat alanı" olmak üzere üç sınıf halinde incelemektedir. "Üç Alan" teorisini ileri süren Hubmann'a göre ortak hayat alanı; bireyin, kural olarak herkesin izlemesine ve bilgisine açık olan alanlarda diğer bir ifade

ile kamusal alanlarda yaşadığı olayları içermekte ve bu alan kural olarak kişilik haklarına ilişkin korumadan yararlanamamaktadır (Güntürk, 2012; Akyürek, 2021). Özel hayat alanı ise belli bir grubun ya da belli kişilerin öğrenebildiği ve gözleyebildiği bir alan olup, bu alanın kişilik haklarına ilişkin korumadan yararlandığı kabul edildiğinden özel hayat alanına haksız olarak girilmesi hukuka aykırılık arz etmektedir (Güntürk, 2012). "Giz alanı" ya da "sır alanı" olarak da ifade edilen gizli hayat alanı; kişinin duygusal ya da cinsel hayatının, haberleşmelerinin ve kişisel bilgilerinin yer aldığı alan olup bu alanı özel hayat alanından ayıran temel özellik, özel hayat alanında yakın kişilerle paylaşılan olay ya da bilgilerin, bu kişiler tarafından, kendileriyle aynı kapsamda bulunan diğer kişilere aktarılmasının mümkün olmasına karşın gizli hayat alanına dâhil faaliyetlerin, güvenilen kişiler dışında kalan kişilerce öğrenilmesinin, kişinin açık ya da örtülü iradesiyle engellenmesidir (Güntürk, 2012; Akyürek, 2021). Bu bakımdan özel hayat kavramı; kişinin, ortak hayat alanı dışında kalan, diğer bir ifadeyle kamuya kapalı olan, ancak bireyin rızası üzerine kişinin özel yaşam alanı içerisinde yer alan kimseler tarafından bilinebilen ve bu kişilerle paylaşılabilen etkinlik ve davranışları kapsayan bir kesit olarak ifade edilebilir (Çelik, 2017).

İstisna hükümlerinin uygulanması bakımından aranan sekizinci ve son şart ise işleme faaliyetinin suç teşkil etmemesidir. Bilindiği üzere suç, ceza kanunlarının olumlu veya olumsuz bir emrinin ihlalini ifade etmektedir (Zafer, 2011). Kanun koyucu tarafından yasaklanan fiillerin gerçekleştirilmesi halinde ceza ya da güvenlik tedbiri yaptırımına bağlanmış hukuka aykırı insan fiili olarak karşımıza çıkan suç kavramı, ancak ceza kanunlarında ya da ceza normu içeren diğer kanunlarda düzenlenen hallerde ortaya çıkmaktadır. Bu bakımdan bir fiilin suç teşkil etmesi ile kast edilen; fiilin gerçekleşmesinden önce kanunda emredilmiş olumlu ya da olumsuz emrin, ihlal edilmesi durumunda yaptırım olarak hapis, adli para cezası ya da güvenlik tedbiri uygulanacağının kanunda açık bir hükümle düzenlenmesidir.

Kişisel Verileri Koruma Kurulu Kararları Işığında İfade Özgürlüğü ve Kişisel Verilerin Korunmasını İsteme Hakkının Yarışması

Bilindiği üzere Kanun'un 13. ve 14. maddelerinde, kişisel verileri işlenen ilgili kişilerin; mezkûr Kanun'un 11. maddesinde düzenlenen hususlarda söz konusu işleme faaliyetine ilişkin olarak veri sorumlularına başvurabileceği ve bu başvurunun reddedildiği, başvuruya yeterli cevap alınamadığı ya da hiç cevap verilmediği durumlarda Kurul'a şikâyet hakkının kullanılabileceği hüküm altına alınmaktadır. Yine Kanun'un 15. maddesinde şikâyet üzerine ya da ihlal iddiasının öğrenilmesi halinde resen, Kurul tarafından gerekli incelemenin yapılacağı düzenleme

altına alınmıştır. Bu bakımdan Kurul uygulamasında ifade özgürlüğü ya da basın özgürlüğü ile kişisel verilerin korunması hakkının karşı karşıya geldiği durumlara ilişkin olarak Kurul'un yaklaşımına da yer verilmesi gerekmektedir.

İlk olarak Kurul, metnin lafzi ifadesinde kendisine yer bulan "ifade özgürlüğü" kapsamında basın faaliyetlerinin de bulunduğunu açık bir şekilde ifade ederek basın özgürlüğünün, ifade özgürlüğünün bir yansıması olduğunu kabul etmekte ve demokratik toplumlardaki işlevine dikkat çekmektedir (Kişisel Verileri Koruma Kurumu, 2020a; Kişisel Verileri Koruma Kurumu, 2021; Kişisel Verileri Koruma Kurumu, 2022) Bu bağlamda Kurul'un konuya yaklaşımının, Anayasa'da iki ayrı temel hak ve özgürlük olarak düzenleme altına alınmış olan basın özgürlüğü ve ifade özgürlüğünü, haklar arasındaki bağlantıyı göz önüne almak suretiyle değerlendirmek yönünde olduğu söylenebilir.

Öte yandan Kurul'un, kişilik hakkı ile basın ya da ifade özgürlüğünün karşı karşıya geldiğini değerlendirdiği başvurulara ilişkin olarak öncelikli olarak başvuru konusunun Kanun kapsamında değerlendirilip değerlendirilemeyeceği sorununa odaklandığı görülmektedir. Kurul'un vermiş olduğu kararlar incelendiğinde; haberde yer alan bilgilerin bilinip bilinmemesine ilişkin olarak kamu yararının bulunup bulunmadığı, bu bakımdan içeriğin kamunun haber alma hakkına hizmet edip etmediği (Kişisel Verileri Koruma Kurumu, 2020a), işlenen verinin özel nitelikli olup olmadığı (Kişisel Verileri Koruma Kurumu, 2019), haberle ya da haber metni içeriği ile ilgisi olmayan, diğer bir ifade ile haberin yapılma amacı ile bağdaşmayan ya da bu amacı aşan bilgilerin haberde yer alıp almadığı (Kişisel Verileri Koruma Kurumu, 2020b), haberin doğru olup olmadığı (Kişisel Verileri Koruma Kurumu, 2021) gibi hususları gözeterek öncelikle başvurunun, Kanun hükümlerine tabi olup olmadığını saptamaya çalıştığı anlaşılmaktadır. Söz konusu hususları karşılayamayan, diğer bir ifade ile kişilik hakkının baskın geldiği sonucuna varılan başvurular bakımından, bu başvuruların Kanun'un 28/1-c düzenlemesi kapsamında yer almadığının değerlendirilmesi sebebiyle söz konusu başvurular bağlamında işlenen verinin türüne göre kişisel veri işleme şartları ya da özel nitelikli kişisel veri işleme şartlarının varlığının arandığı, ayrıca işleme faaliyetinde genel ilkelere uyum hususunun da gözetildiği görülmektedir. Bu kapsamda Kurul'a intikal eden bir şikayette, ilgili kişinin kendisi ile ilgili olarak yapılan haber içeriğinde ilgili kişinin babasına ait sağlık verilerine de yer verilmesi durumuna ilişkin olarak Kurul, söz konusu hususun bilinmesinde kamu yararı olmadığı gerekçesiyle konunun Kanun'un 28/1-c düzenlemesi kapsamında değerlendirilemeyeceğinden bahisle habere konu içerikte geçen sağlık verilerinin işlenmesi bağlamında şikayeti inceleme konusu ederek işleme şartının bulunmaması sebebiyle veri sorumlusu gazete hakkında idari para cezası uygulama

yoluna gitmiştir (Kişisel Verileri Koruma Kurumu, 2019). Bir başka şikâyette ise internet gazeteciliği faaliyeti de gösteren veri sorumlusu şirketin, kendilerine gönderilen ihtarnameyi, ihtarname içeriğinde yer alan kişisel veriler de görülecek şekilde haber içeriğinde kullanması inceleme konusu edilmiştir. Konuya ilişkin olarak Kurul, Basın Kanunu'nun 14. maddesi gereğince yapılması gereken düzeltmenin kanundan kaynaklı bir yükümlülük olmasına karşın bu düzeltmenin amaçla bağlantılı, sınırlı ve ölçülü olması gerektiğine vurgu yaparak söz konusu bilgilerin haberle bağlantılı olmadığını ve kişilik haklarının zarara uğramasına sebep olabilecek veriler içerdiğini, bu sebeple şikâyet konusunun Kanun'un 28/1-c düzenlemesi kapsamında değerlendirilemeyeceğini karara bağlamış; söz konusu işleme faaliyetine ilişkin bir işleme şartı bulunmasına karşın işlemenin amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık teşkil etmesi sebebiyle veri sorumlusu hakkında idari para cezası uygulanmasına karar vermiştir (Kişisel Verileri Koruma Kurumu, 2020b). Özetle Kurul, basın faaliyetlerinin icrası neticesinde kişisel verilerin korunması hakkı ile ifade ya da basın özgürlüğünün karşı karşıya geldiği başvurulara ilişkin olarak hangi hakkın üstün geleceği meselesine odaklanmakta; bu noktada ise habere konu içeriğin kamu yararına yönelik olmadığı, haber detayında yer alan kişisel verilerin habere konu olay ile bağlantısız, yanlış ya da yanıltıcı olduğu, haber ile içerikte yer alan kişisel veriler arasında bir dengenin bulunmadığı başvuruları istisna kapsamında tutmayarak Kanun hükümleri bağlamında ayrıca incelemektedir. Basın ya da ifade özgürlüğünün, kişisel verilerin korunması hakkına nazaran üstün geldiği değerlendirilen şikâyetler bakımından ise Kanun hükümleri uygulama alanı bulmadığından, yapılan başvurular bakımından "Kurul tarafından tesis edilecek herhangi bir işlem bulunmadığı" yönünde karar verilmektedir.

Bu noktada Kurul'un basın kavramına ve basın özgürlüğüne yaklaşımına da değinmek gerekmektedir. Kurul'a göre basın; "Kamu yararını ilgilendiren olay ve konularda haber ve bilgi vermek, açıklamalar yapmak, eleştiri ve değer yargıları sunmak suretiyle toplumu aydınlatmak ve kamuoyu oluşturmak" ile görevli olup bu görev sebebiyle basına, haber verme hak ve görevi tanınmaktadır (Kişisel Verileri Koruma Kurumu, 2022). Bununla birlikte Kurul tarafından, habere konu edilen kişilerin, kişisel verilerinin korunmasını isteme hakkı ile basın özgürlüğünün karşı karşıya geldiği durumlarda haberden beklenen yarar ve ilgili kişinin, kişisel verilerinin korunmasını isteme hakkından beklediği meşru çıkarların karşılaştırılması gerektiği, bu karşılaştırmanın temel ölçütünün ise "kamu yararı" olduğu belirtilmekte ve basının görev ve yetkilerini ifa ederken ortaya koyduğu yayının gerçek ve güncel olmasının yanı sıra kamu ilgi ve yararına da mazhar olması, aynı zamanda öz ve biçim arasındaki dengenin de korunması gerektiği ifade edilmektedir (Kişisel Verileri Koruma Kurumu, 2021; Kişisel Ve-

rileri Koruma Kurumu, 2020a). Bu bakımdan Kurul'un "kamu ilgi ve yararının varlığı", "haberin gerçekliği ve güncelliği" ve "öz ve içerik arasında denge bulunup bulunmadığı" olmak üzere üç ana kriter doğrultusunda bir değerlendirme yaptığı anlaşılmaktadır. Bu kriterlerden kamu yararının tespitinde, "yapılan haberin kişilerin merak duygularına ya da yüksek ahlaki ve hukuki değerlerin korunması amaçlarından hangisine hizmet ettiğinin tespit edilmesi gerektiği" belirtilmekte, aynı zamanda "siyasetçiler ya da kamu görevlileri gibi kimseler hakkında yapılan haberlere ilişkin olarak, basın özgürlüğüne yönelecek kısıtlamaların daha dar biçimde yorumlanması gerektiği" ifade edilmektedir (Kişisel Verileri Koruma Kurumu, 2021). Yine benzer şekilde "toplumsal bir ilgi uyandıran, kamuoyunun düşünmesine ve tartışmasına katkıda bulunan, belli bir sorunun aydınlatılması ya da buna ilişkin çözüm yollarının gösterilmesi amacına hizmet eden olayların açıklamasında kamu yararı bulunduğu" kabul edilmektedir (Kişisel Verileri Koruma Kurumu, 2020a). Haberin gerçekliği ve güncelliğine ilişkin olarak ise gerçeklik unsurunun, "haberin verildiği andaki beliriş biçimine uygunluk" biçiminde anlaşılması gerektiği, güncellik unsurunun ise "olayın kamuya açıklandığı zaman diliminde açıklama faaliyetine ilişkin bir kamu yararının bulunması" biçiminde değerlendirileceği, üzerinden geçen zaman sebebiyle açıklanmasının artık kamusal bir yararı içermediği durumlarda kişilik hakkının ön plana çıkacağı belirtilmektedir (Kişisel Verileri Koruma Kurumu, 2021; Kişisel Verileri Koruma Kurumu, 2020a). Son kriter olan biçim ve öz arasındaki dengeye ilişkin olarak ise Kurul, bu unsurun gerçekleşmesi bakımından "haberin dilinin ve haberde kullanılacak ifadelerin, haberin gerektirdiği biçim ve ölçüde bulunması", aynı zamanda "haberin sahip olacağı yasal fonksiyonun yöneldiği amaca ulaşabilmek için en uygun ve elverişli olan araçların seçilmesi ve kullanılması"nı kapsadığını ifade etmektedir (Kişisel Verileri Koruma Kurumu, 2021).

Öte yandan kişiler hakkında yapılan haberlerin, farklı internet siteleri üzerinden arama motorlarına yansıması sonucu bu hususta yapılan silinme taleplerinin de Kurul tarafından inceleme konusu edilerek bu taleplerin, unutulma hakkı kapsamında değerlendirme konusu edildiği görülmektedir. Bu bakımdan basın özgürlüğü ve kişisel verilerin korunmasını isteme hakkı bağlamında ortaya çıkan yarışma alanına; habere konu içeriğin yayınlanmasını takiben, ilgili kişilerce gerçekleştirilecek silinme taleplerinin ve buna bağlı olarak unutulma hakkının da dâhil olduğu anlaşılmaktadır. Bu noktada; iç hukukumuzda "unutulma hakkı" adı ile özel bir düzenlemeye yer verilmemiş olmasına karşın hakkın Türk Hukuku bakımından da tartışma konusu edildiğini ve bu kapsamda yer aldığı değerlendirilen taleplerin de gündeme gelebildiğini ifade etmek gerekmektedir. Özellikle uluslararası gelişmelerle bağlantılı olarak henüz kişisel verilerin korunmasına özgülenmiş bir düzenleme yürürlüğe girmeden önce de unutulma hakkının ülkemizde tartışma konusu edildiğinin, hatta bazı yargı kararlarında "unutulma hakkı" ifadesine açıkça yer verildiğinin, özellikle Yargıtay tarafından unutulma hakkı kavramının farklı kararlarda sıkça kullanıldığının belirtilmesi gerekmektedir. Bu bakımdan Yargıtay'ın bir yüksek mahkeme olarak unutulma hakkını içtihat yoluyla benimsediği ve mahiyeti uygun düştüğü ölçüde Kanun öncesi dönemde de kararlarına konu ettiğini söylemek mümkündür. Ülkemizde unutulma hakkına ilişkin olarak verilen ilk karar olduğu ifade edilen (Yenice Ceylan, 2021) ve Yargıtay Hukuk Genel Kurulu (YHGK) tarafından verilen bir kararda, cinsel taciz suçuna ilişkin olarak yapılan bir yargılama sırasında verilen ilamın temyizi neticesinde Yargıtay tarafından verilen kararın, suçun mağduru ile diğer şahısların ismi rumuzlanmadan akademik bir eserde kullanılması değerlendirme konusu edilmiştir (YHGK, 2015). YHGK, öncelikle sorunun temeline ilişkin bir tespitte bulunarak "Unutulma hakkı ve bunun sonucu olarak kişisel verilerin ve kişilik hakkının korunması ile bilim ve sanat hürriyetinin birbiri karşısındaki sınırların belirlenmesi" gerektiğini ifade etmiş ve bunlar arasında adil bir denge kurulması gerektiğini değerlendirmiştir (YHGK, 2015). Akabinde kişisel verilerin korunması ve kişisel verilerin korunmasının insan haklarıyla olan ilişkisine değinen YHGK; unutulma hakkını "üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanılan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlemesini isteme hakkı" olarak tanımlamış ve unutulma hakkı ile bununla ilgili olduğu ölçüde ve minimum süre ile kişisel verinin tutulması veya depolanması gibi konuların kişisel verilerin korunması hukukunun çatısını oluşturduğunu belirtmiştir (YHGK, 2015). Unutulma hakkının, kişiye geçmişini kontrol etme, belli hususların geçmişinden silinmesini ve artık hatırlanmamayı isteme hakkını tanıdığı; muhataplara da üçüncü kişilerin bu bilgileri kullanmaması ya da hatırlamaması hususunda bir yükümlülük yüklediği, ayrıca Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi kapsamında değerlendirilen mahremiyet hakkının "bireyin kendisi hakkındaki bilgileri kontrol edebilmesi" şeklindeki hukuki çıkarlarını da içerdiği ve kişisel verilerinin mahrem kalması konusunda bireyin hukuki menfaatinin bulunduğu hususu da kararda vurgulanmıştır (YHGK, 2015). Kararı önemli kılan bir diğer husus, unutulma hakkının yalnızca internet ortamında gerçekleşmiş olaylar bakımından değil basılı eserler bağlamında da değerlendirilebilecek bir talep olarak ele alınmış olmasıdır. Nitekim mezkûr kararda unutulma hakkına ilişkin olarak yapılan tanımların dijital veriler için düzenlenmesine karşın hakkın özellikleri ve insan hakları ile ilişkisi göz önüne alınarak unutulma hakkının "kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiği" yönünde bir değerlendirmede bulunulmuştur (YHGK, 2015). Bununla birlikte söz konusu hususa ilişkin olarak öğretide bir birlik bulunmadığı, bazı yazarlar tarafından unutulma hakkının basılı eserleri kapsama-

dığı, yalnızca internet ortamında yer alan içerikler bakımından uygulama alanı bulduğu yönünde değerlendirmelerde bulunulduğu (Ocak, 2018; Nalbantoğlu, 2018; Elmalıca, 2016), bazı yazarlar tarafından ise internet dışındaki mecralarda da kişinin izni olmadan kişisel verilerinin işlenebileceği ve bu durumda unutulma hakkının bulunmadığının kabul edilmesinin hak kaybına yol açabileceğinin ifade edildiği görülmektedir (Çınar, 2022; Akkurt, 2016).

Diğer taraftan unutulma hakkı kapsamında değerlendirilebilecek bazı başvurular, AYM tarafından da inceleme konusu edilmektedir. 27.04.2022 tarihi itibarıyla AYM'nin resmi internet adresi olan üzerinden yapılan taramalara göre bu kapsamda yapılan en eski başvuru, başvurucunun uyuşturucu madde kullandığı iddiasıyla yürütülen kovuşturma neticesinde başvurucu hakkında adli para cezası uygulandığı hususunda yapılan ve ulusal bir gazetenin internet arşivi üzerinden yayınlanan üç ayrı haber başlığının kaldırılması yönündeki talebin reddedilmesi üzerine yapılmış olup, AYM söz konusu hususta Anayasa'nın 17. maddesinin birinci fıkrasında yer alan "şeref ve itibarın korunması hakkı"nın ihlal edildiğine karar vermiştir (AYM, 2016). Konuya ilişkin olarak AYM; kişinin itibarının, kimliğinin ve manevi bütünlüğünün bir parçası olduğunu, bununla birlikte şeref ve itibara yönelen müdahalelerin Anayasa m. 17/1 kapsamında değerlendirilebilmesi için müdahalenin belirli bir ağırlık eşiğini aşması ve öngörülebilir şekilde kişinin kendi eylemleri sonucu ortaya çıkmaması gerektiğini, ulaşılabilirlik, yaygınlık, haber ile fikirlerin depolanması ve muhafazasındaki kolaylık sebebiyle internet ortamının, içeriklerin uzun süre erişilebilir durumda olmasına imkan sağladığını belirterek kişilerin şeref ve itibarını zedeleyebileceği hususuna vurgu yapmıştır (AYM, 2016). Akabinde haberlerin internet ortamında yayınlanmasının kişisel verilerin korunması hakkı ile ilişkili olduğunu belirten Mahkeme, konunun şeref ve itibarın korunması hakkının yanı sıra Anayasa'nın 20. maddesi kapsamında da değerlendirilmesi gerektiğine işaret ederek *"internetin yaygın kullanımı neticesinde basın özgürlüğü ile şeref ve itibarın korunması hakkı arasındaki dengenin, basın özgürlüğü lehine bozulduğunu, bu dengenin yeniden kurulabilmesinin şeref ve itibar yönünden bireylerin unutulma hakkının kabul edilmesi ile mümkün olabileceği"*ni belirtmiştir (AYM, 2016). Unutulma hakkına ilişkin olarak ise Mahkeme, Anayasa'da açıkça düzenlenmemesine karşın hakkın, internet aracılığıyla ulaşılması kolay olan ve dijital hafızada yer alan haberlere erişimin engellenmesine ilişkin olarak Anayasa'nın 5., 17. ve 20. maddelerinin doğal bir sonucu olduğunu, kişilerin manevi varlıklarının geliştirilmesine bir fırsat verebilmek açısından devletin pozitif yükümlülüğünün bulunduğunu; bununla birlikte hakkın, internet gazete arşivlerinde yer alan her türlü haberler için uygulanmasını beklemenin mümkün olmadığını vurgulamıştır (AYM, 2016). Bu noktada bazı kriterler ortaya koyan AYM, yayının internetten kaldırılabilmesi için; yayının içeriği, yayında kaldığı süre, güncelliğini yitirme, tarihsel bir veri olarak kabul edilememe, kamu yararına katkısı (toplumsal açıdan haberin değeri, haberin geleceğe ışık tutan niteliği) habere konu kişinin siyasetçi veya ünlü olup olmadığı, haber veya makalenin konusu, bu bağlamda haberin olgusal gerçekler ya da değer yargısı içerip içermediği, halkın ilgili veriye yönelik ilgisi gibi hususların her somut olay için ayrı ayrı değerlendirilmesi gerektiğini ifade etmiştir (AYM, 2016). Bununla birlikte AYM'nin 2014/16026 (AYM, 2014a) ve 2014/17943 (AYM, 2014b) Başvuru numaralı kararlarında olduğu gibi kimi kararlarda; unutulma hakkının, basın özgürlüğü ile haber ve fikirlere ulaşma özgürlüğünün özüne dokunmadan ve hak sahibinin çıkarlarını koruyacak şekilde kullanılması gerektiği hususuna yer verilmiştir. Bu bakımdan AYM'nin unutulma hakkına ilişkin yaklaşımının, haklar arasında denge kurma prensibi ile hareket edilmesi doğrultusunda şekillendiği ve yayınlanan içerik, içeriğe konu şahsın toplum içerisindeki yeri ya da kamu yararına katkısı gibi hususlarda yapılacak değerlendirmenin bu hususta önem arz ettiği anlaşılmaktadır.

Yukarıda sözü edilen yargı kararlarının verilmesini takiben, Kanun'un yürürlüğe girmesi ve 2017 yılında Kurul'un faaliyetlerine başlamasıyla, unutulma hakkı, idari bakımdan da değerlendirme konusu edilmiştir. Bu kapsamda verilen 23.06.2020 tarihli ve 2020/481 sayılı Kararda, yukarıda yer verilen yargı kararları ile unutulma hakkının uluslararası kaynaklarına yer verilerek iç hukukumuzda hakka açıkça yer verilmemesine karşın hakkı sağlamaya yönelik araçların varlığına vurgu yapılarak Anayasa m. 20, Kanun m. 4, 7 ve 11 düzenlemeleri ile "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" m. 8 düzenlemeleri doğrultusunda *"bu yöndeki taleplerin ayrı bir hak tanımlamasına gerek olmaksızın karşılanabileceği ve unutulma hakkının sağlanmasına ilişkin olarak uygulanacak yöntemin, somut olay kapsamında değerlendirilmesi gerektiği"* belirtilmiştir (Kişisel Verileri Koruma Kurumu, 2020c). Öte yandan anılan kararda; arama motorlarında ad ve soyadı üzerinden gerçekleştirilen taramalar sonucunda kişilerin kendisiyle bağlantılı sonuçlara ulaşılmamasını istemelerinin "indeksten çıkarılma talebi" olarak nitelendirileceği ve *"bu talepler kapsamında arama motorlarının, internette toplanan verilerin işlenmesinde amaç ve vasıtaları belirlemesi sebebiyle KVKK m. 3 gereğince veri sorumlusu sıfatını haiz olduğu ve bu kapsamda arama motoru işletmecisinin gerçekleştirdiği faaliyetlerin mezkûr madde gereği kişisel veri işleme faaliyeti olduğu"* karara bağlanmıştır (Kişisel Verileri Koruma Kurumu, 2020). Yine anılan kararda indeksten çıkarılma taleplerine ilişkin olarak *"ilgili kişilerin temel hak ve özgürlükleri ile kamunun söz konusu bilgiyi edinmesindeki menfaat arasında bir denge kurulması gerektiği"* belirtilerek sınırlı sayım ilkesine tabi olmamak kaydıyla bazı kriterler ortaya konulmuştur. Bu kriterler; *"ilgili kişinin kamusal yaşamdaki rolünün önemi", "ilgili kişinin yasal olarak*

ergin olup olmadığı", "içeriğin doğruluğu ve güncelliği", "bilginin çalışma hayatına ilişkin olup olmadığı", "özel nitelikli kişisel veri içerip içermediği", "içeriğin hakaret, onur kırıcı ifade ya da iftira mahiyetinde bulunup bulunmadığı", "kişi hakkında ön yargıya sebep olup olmadığı ya da kişi açısından risk teşkil edip etmediği", "bilginin ilgili kişi tarafından yayımlanıp yayımlanmadığı", "orijinal içeriğin gazetecilik kapsamında işlenip işlenmediği", "bilgilerin yayımlanmasında yasal bir zorunluluk olup olmadığı" ile "bilginin, ceza gerektiren bir suça ilişkin olup olmadığı" olarak belirtilmiştir (Kişisel Verileri Koruma Kurumu, t.y.).

SONUÇ

2010 yılında yapılan Anayasa değişikliği ile kişisel verilerin korunmasını isteme hakkı bir temel hak ve özgürlük olarak açıkça hukuk sistemimize dâhil edilmiş; mezkûr düzenleme uyarınca çıkarılan Kanun ile söz konusu hakkın kullanımına ilişkin usul ve esaslar düzenleme altına alınmıştır. Bu hususta gerek Anayasa m. 20 düzenlemesi gerek Kanun ve ikincil düzenlemeleri, bireyin özel hayatını ve bireye ait bir değer olarak kişisel verilerin gizliliğini belli şartlar dâhilinde korumaktadır. Anayasa'nın 26. maddesinde düzenlenen ifade özgürlüğü ile 28. maddesinde düzenlenen basın özgürlüğü ise toplumun bilgi edinmesine, haber, bilgi ve düşüncelere ulaşmasını amaçlamakta ve hem bireyin hem toplumun menfaatlerine hizmet eden diğer hak ve özgürlükler olarak karşımıza çıkmaktadır. Her ne kadar söz konusu hak ve özgürlükler Anayasal düzeyde koruma altına alınmış ise de bu haklar bazı durumlarda karşı karşıya gelebilmekte ve ortaya çıkan bu problemin kimin lehine çözümleneceğinin tespit edilmesi gerekmektedir. Sözü edilen bu sorunu, Kanun'un 28/1-c düzenlemesinde öngörülen ve Kanun hükümlerinin uygulanmayacağı haller arasında gösterilen "Kişisel verilerin ifade özgürlüğü kapsamında işlenmesi" durumu daha da karmaşık bir hale getirmektedir. Bu bakımdan öncelikle basın kavramının anlamı ile basın faaliyetlerinin kapsamının belirlenmesi, basın özgürlüğü kapsamında hangi faaliyetlerin bulunacağının tespit edilmesi ve basın özgürlüğü kapsamında yer aldığı değerlendirilen faaliyetin, kişisel verilerin korunmasını isteme hakkı ile yarışması durumunda, hangi hakka üstünlük tanınması gerektiğinin değerlendirilmesi gerekmektedir. Bu hususta "basın" faaliyetinin, iç hukukumuz bakımından, esas itibarıyla yazılı bir formatta olup bu format ile dağıtıma elverişli mahiyete sahip süreli ya da süresiz yayınları kapsamına aldığı ağırlıklı olarak kabul edilmekte ise de basın faaliyetlerinin, teknolojik gelişmelerin etkisiyle geçirdiği değişim ve gerçekleştirilmek istenen faaliyetin mahiyetinin farklılık göstermediği dikkate alınarak faaliyetin kapsamının daha geniş bir şekilde yorumlanmasına bir engel bulunmadığı değerlendirilmektedir. Özellikle kamuoyunun bilgilendirilmesi amacına hizmet edilen faaliyetler bakımından, faaliyetin sırf yazılı/basılı olmayan medya araçlarıyla ya da internet yolu ile yürütülmesi sebebiyle, yürütülen faaliyetin basın özgürlüğü kapsamında yer almadığının değerlendirilmesi, koruma altına alınan hak ve özgürlüğün mahiyetiyle bağdaşmayacaktır. Bununla birlikte Kanun'un m.28/1-c düzenlemesinde "ifade özgürlüğü" bağlamında değerlendirilen haller basın faaliyetleri kapsamında yer alıp almadığına bakılmaksızın kapsam dışı bırakıldığından, sözü edilen faaliyetler, basın özgürlüğü kapsamında yer almadığı kabul edilse dahi, ifade özgürlüğü kapsamında yine himaye göreceğinden esasen bu hususta bir tartışma ortaya çıkmayacaktır.

Öte yandan basın özgürlüğünün sınırlama sebepleri ile ifade özgürlüğünün sınırlama sebepleri büyük ölçüde benzerlik göstermekte olup söz konusu haklar ile özel hayatın gizliliği bağlamında kişisel verilerin korunması hakkı karşı karşıya geldiğinde Kurul uygulamasında iki hak arasında bir denge kurulması yoluna gidildiği görülmektedir. Uygulamada esas itibarıyla yapılan içeriğin kamu yararına katkısı, habere konu kişinin sahip olduğu ünün kaynağı, kamusal bir görevi yerine getirip getirmediği, içeriğin sırf merak duygularının tatmini amacına yönelip yönelmediği gibi hususların gözetildiği, bununla birlikte söz konusu kriterlerin sınırlı sayım suretiyle ele alınmadığı, bu sebeple somut olay şartları dâhilinde farklı kriterler öngörülerek bir değerlendirme yapılması yoluna gidilebildiği görülmektedir. Bu bakımdan uygulamada, basın-yayın araçları ile kamuya açıklanan herhangi bir bilginin, doğrudan "basın özgürlüğü" kapsamında değerlendirilmesi yerine, kamuya açıklanan içeriğin mahiyetinin de gözetildiği ve bu sayede, bir diğer temel hak ve özgürlük olan özel hayatın gizliliği hakkına yönelik koruma alanının devre dışı bırakılmadığı, benzer şekilde, aynı şartlar altında yayımlanan ve kişisel veri barındıran bir içeriğin, peşinen özel hayatın gizliliği kapsamında değerlendirme konusu edilerek kamunun bilgi edinme hakkının engellenmesinin de önüne geçildiği anlaşılmaktadır.

Diğer taraftan basın özgürlüğü ile kişisel verilerin korunmasını isteme hakkının karşı karşıya gelmesi, unutulma hakkı meselesinin de tartışma konusu edilmesini gerektirmektedir. Tarihsel gelişim süreci içerisinde dijital ortamda gerçekleşen ve yapıldığı dönemdeki gerçek durumları yansıtan içerikler hakkında uygulama alanı bulduğu kabul edilen unutulma hakkı, iç hukukumuzda içtihat yoluyla kabul edilmiş ve bazı yargı kararlarında hakkın, yalnızca dijital ortamlar bakımından değil, dijital ortamlar dışında kalan diğer ortamlar bakımından da uygulama alanı bulduğu hususuna yer verilmiştir. Bununla birlikte hakkın ortaya çıkış süreci, kabul ediliş amacı ve dijital ortamlar dışında kalan içeriklere ilişkin taleplerin kabul edilmesi halinde karara ilişkin icraatlarda bulunabilmenin zorlukları göz önüne alındığında unutulma hakkının uygulama alanının dijital ortamlar ile sınırlanması, özellikle uluslararası uygulama ile uyumluluk anlamında daha uygun bir çözüm yolu olacak, verilecek kararların icrası ve bakımından da yeknesaklık sağlayacaktır. ◆

KAYNAKÇA

- Akarcalı, S. (1989). Basının Görevleri ve Basın Özgürlüğü. Ankara Üniversitesi Siyasal Bilimler Fakültesi Dergisi, 44(1), 265-287.
- Akipek, J. G., Akıntürk, T. ve Ateş, D. (2015). Türk Medeni Hukuku- Başlangıç Hükümleri Kişiler Hukuku I. Cilt (Yenilenmiş 12. Baskı). İstanbul: Beta Yayıncılık.
- Akkurt, A. (2014). Basın Özgürlüğünün Kapsamı ve Sınırları (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Akkurt, S. S. (2016). 17.06.2015 Tarih, E. 2014/4-56, K. 2015/2679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı ve Mukayeseli Hukuk Çerçevesinde "Unutulma Hakkı". Ankara Üniversitesi Hukuk Fakültesi Dergisi, 65 (4), 2605-2635.
- Akyürek, G. (2021). Özel Hayatın Gizliliğini İhlal Suçu (3. Baskı). Ankara: Seçkin Yayıncılık.
- Anayasa Mahkemesi. (2014a). 05.10.2017 tarihli ve 2014/16026 Başvuru No'lu G.Y. Başvurusu. https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/16026 adresinden 27.04.2022 tarihinde erişilmiştir.
- Anayasa Mahkemesi. (2014b). 05.10.2017 tarihli ve 2014/17943 Başvuru No'lu Fahri Göncü Başvurusu. https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/16026 adresinden 27.04.2022 tarihinde erişilmiştir.
- Anayasa Mahkemesi. (2016). 03.03.2016 tarihli ve 2013/5653 Başvuru No'lu N.B.B. Başvurusu. https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/5653 adresinden 27.04.2022 tarihinde erişilmiştir.
- Anayasa Mahkemesi Kararlar Dergisi (1971). E:1962/128; K:1964/8 sayılı ve 28.01.1964 tarihli Karar, https://www.anayasa.gov.tr/media/4921/kd_02.pdf 19.02.2023.
- Armağan, S. (1998). Basın Hürriyeti ve Sınırları. Gazi Üniversitesi Hukuk Fakültesi Dergisi, 2(2) https://dergipark.org.tr/tr/download/article-file/789921 , 28.02.2022.

◊ Arslan, U. (2022). Milli Güvenlik Kavramı ve Kavramın Türkiye'de Hukuksallaşması Süreci. Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, 5 (1), 183-212.

◊ Aziz, A. (2013). Televizyon ve Radyo Yayıncılığı (Giriş), İstanbul: Hiperlink Yayınları. (https://books.google.com.tr/books/about/Televizyon_ve_Radyo_Yaync%C4%B1l%C4%B1%C4%9F%C4%B1_Giri.html?id=6TdwDwAAQBAJ&redir_esc=y adresinden 31.01.2022 tarihinde erişilmiştir.)

◊ Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun Teklifi (2/4471) ile Dijital Mecralar Komisyonu ve Adalet Komisyonu Raporları. (t.y.). https://www5.tbmm.gov.tr/sirasayi/donem27/yil01/ss340.pdf adresinden 08.08.2022 tarihinde erişilmiştir.

◊ Baykan, M. (2011). Avrupa İnsan Hakları Mahkemesi Kararlarında Basın Özgürlüğü. Ankara: Adalet Yayınevi.

◊ Bayra, A. E. (2020). Hak ve Özgürlükleri Sınırlandıran Kavramların Tasnifi ve Derecelendirmesi-I: Kamu Düzeni ve Kamu Düzeni ile İlgili Kavramlar. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 7 (2), 45-72.

◊ Çelik, Y. (2017). Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı. Türkiye Adalet Akademisi Dergisi, Sayı 32, 391-410.

◊ Çınar, A. (2022). Unutulma Hakkının Ortaya Çıkış Serüveni ve Kapsamının Değerlendirilmesi. Türkiye Adalet Akademisi Dergisi, Sayı 49, 551-584.

◊ Çınarlı, G. (2015). Anayasal Bir Kurum Olarak Milli Güvenlik Kurulu (Yayımlanmamış Yüksek Lisans Tezi). Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

◊ Dinçtürk, Ö. (2007). 5187 Sayılı Yeni Basın Kanunu Kapsamındaki Basın Düzenine Yönelik Suçlar (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

◊ Dural, M. ve Öğüz, T. (2018). Türk Özel Hukuku Cilt II Kişiler Hukuku (19. Baskı). İstanbul: Filiz Kitabevi.

◊ Elmalıca, H. (2016). Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı. Ankara Üniversitesi Hukuk Fakültesi Dergisi, 65 (4), 1603-1636.

◊ Esendal, N. (2018). Basın Yolu ile Kişilik Haklarının İhlali. Ankara: Seçkin Yayıncılık.

◊ Esmer, M. (2014). Avrupa İnsan Hakları Sözleşmesi ve 1982 Anayasası'nda İfade ve Kitle İletişim Özgürlüğü (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

◊ Gönenç, E. Ö. (2007). İletişimin Tarihsel Süreci. İstanbul Üniversitesi İletişim Fakültesi Dergisi, Sayı 28, 87-102.

◊ Güntürk, M. S. (2012). Türk Yüksek Mahkemeleri ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Özel Hayatın Gizliliğinin Korunması. Ankara: Seçkin Yayıncılık.

◊ Kalyon, L. (2008). Cumhuriyet Dönemi Savunma Politikaları (Yayımlanmamış Doktora Tezi). Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

◊ Kaya, B. (2020). Uluslararası Sözleşmelerde Mülkilik İlkesi. İktisadi ve İdari Yaklaşımlar Dergisi, 2 (1), 31-59.

◊ Kızılyel, S. (2014). Temel Hak ve Özgürlüklerin Kısıtlanmasında Kamu Güvenliği Ölçütü (Yayımlanmamış Doktora Tezi). Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara.

◊ Kişisel Verileri Koruma Kurumu. (2019).09.12.2019 tarihli ve 2019/372 sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/6663/2019-372 adresinden 21.02.2023 tarihinde erişilmiştir.

◊ Kişisel Verileri Koruma Kurumu. (2020a). 22.05.2020 tarihli ve 2020/414 sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/6915/2020-414 adresinden 22.08.2023 tarihinde erişilmiştir.

◊ Kişisel Verileri Koruma Kurumu. (2020b).18.02.2020 tarihli ve 2020/145 sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/6888/2020-145 adresinden 21.02.2023 tarihinde erişilmiştir.

◊ Kişisel Verileri Koruma Kurumu. (2020c). 23.06.2020 tarihli ve 2020/481 sayılı Kararı. https://www.kvkk.gov.tr/Icerik/6776/2020-481 adresinden 27.04.2022 tarihinde erişilmiştir.

◊ Kişisel Verileri Koruma Kurumu. (2021). 30.09.2021 tarihli ve 2021/989 sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/7143/2021-989 adresinden 22.08.2023 tarihinde erişilmiştir.

◊ Kişisel Verileri Koruma Kurumu. (2022). 06.01.2022 tarihli ve 2022/13 sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/7179/2022-13 adresinden 18.04.2022 tarihinde erişilmiştir.

◊ Kişisel Verileri Koruma Kurumu. (t.y.). Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına İlişkin Değerlendirmede Dikkate Alınacak Kriterler. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/68f1fb19-5803-4ef8-8696-f938fb49a9d5.pdf adresinden 22.11.2022 tarihinde erişilmiştir

◊ Kocatepe, M. (2019). Türk Vergi Hukukunda Mükellefin Vergi Mahremiyeti Hakkı (Yayımlanmamış Yüksek Lisans Tezi). Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

◊ Nalbantoğlu, S. (2018). Bir Temel Hak Olarak Unutulma Hakkı. Türkiye Adalet Akademisi Dergisi, Sayı 35, 583-605.

◊ Ocak, A. (2018). Hakları Dengelemek: Unutulma Hakkı İfade Özgürlüğüne Karşı. Türkiye Adalet Akademisi Dergisi, Sayı 33, 507-518.

◊ Oğuzman, K., Seliçi, Ö. ve Oktay Özdemir, S. (2012). Kişiler Hukuku- Gerçek ve Tüzel Kişiler (12. Bası). İstanbul: Filiz Kitabevi.

◊ Özdemir, A. (2016). "Kamu Düzeni" ve "Kamu Güvenliği" Kavramlarına Analitik Bir Yaklaşım (Toplantı ve Gösteri Yürüyüşü Hakkının Sınırlandırılması Örneği. International Journal of Legal Progress, 2 (2), 78-115.

◊ Özkepir, R., Kocaman, S. Z. ve Kart, E. H. (2020). Sosyal Medya ve Basın Hukuku. Ankara: Seçkin Yayıncılık.

◊ Salihpaşaoğlu,Y. (2007). Türkiye'de Basın Özgürlüğü. Ankara: Seçkin Yayıncılık.

◊ Serozan, R. (2018). Medeni Hukuk- Genel Bölüm/Kişiler Hukuku (8. Bası). İstanbul: Vedat Kitapçılık.

◊ Sunay, R. (2000). Avrupa İnsan Hakları Sözleşmesinde ve Türk Anayasasında İfade Hürriyetinin Korunması. Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 8(1-2), 527-544.

◊ Şimşek, O. (2008). Anayasa Hukukunda Kişisel Verilerin Korunması. İstanbul: Beta Yayıncılık.

◊ Tunç, H. ve Döner, A. (1998). MGK ve Milli Güvenlik Kavramı. Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi, Sayı 1, 3-22.

◊ TÜİK. (t.y.). https://data.tuik.gov.tr/Bulten/Index?p=Yazili-Medya-ve-Uluslararasi-Standart-Kitap-Numarasi-Istatistikleri-2021-45833 adresinden 12.08.2022 tarihinde erişilmiştir.

◊ Türk Dil Kurumu. (t.y.). https://sozluk.gov.tr/ adresinden 29.01.2022 tarihinde erişilmiştir.

◊ Türk Dil Kurumu. (t.y.). https://sozluk.gov.tr/ adresinden 17.02.2023 tarihinde erişilmiştir.

◊ Türk Dil Kurumu. (t.y.). https://sozluk.gov.tr/ adresinden 17.02.2023 tarihinde erişilmiştir.

◊ Türk Dil Kurumu. (t.y.). https://sozluk.gov.tr/ adresinden 18.02.2023 tarihinde erişilmiştir.

◊ Uygun, O. (2014). Devlet Teorisi. İstanbul: On İki Levha Yayıncılık.

◊ Yargıtay Hukuk Genel Kurulu. (2015). 17.06.2015 tarihli ve E: 2014/56; K. 2015/1679 sayılı Kararı. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ adresinden 25.04.2022 tarihinde erişilmiştir.

◊ Yavuz Yayla, E. (2018). Milli Güvenlik Kavramının Hukuki Boyutu. Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, 6 (12), 29-78.

◊ Yavuz Yayla, E. (2019). Basın Özgürlüğü ve Milli Güvenlik Kapsamında Sınırları. Ankara: Adalet Yayınevi.

◊ Yenice Ceylan, Ö. (2021). Unutulma Hakkının Basın Özgürlüğü Karşısındaki Konumu. Kişisel Verileri Koruma Dergisi, 3 (2), 1-14.

◊ Yıldız, F. (2012). Türk Anayasa Hukukunda Basın Özgürlüğü (Yayımlanmamış Yüksek Lisans Tezi). Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

◊ Yılmaz Avcı, K. (2014). İnsan Hakları Hukukunda İfade Özgürlüğü Bağlamında Basın Özgürlüğünün Sınırlandırılması Sorunu ve Türkiye Örneği (Yayımlanmamış Yüksek Lisans Tezi). Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü, Trabzon.

◊ Zafer, H. (2011). Ceza Hukuku Genel Hükümler- TCK m.1-75, (2. Bası). İstanbul: Beta Yayıncılık.

◊ Zarplı, Ç. (2008). İfade Özgürlüğü: İçeriği ve Sınırları (Yayımlanmamış Yüksek Lisans Tezi). Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü, Kütahya.

BİR SORUMLULUK ŞEKLİ OLARAK ORTAK VERİ SORUMLULUĞU

Burak ÖZER

Kişisel Verileri Koruma Uzmanı

"Bu çalışma 14.02.2023 tarihinde kabul edilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 4857 sayılı İş Kanunu Kapsamında Kişisel Verilerin Korunması başlıklı uzmanlık tezinden alınmıştır."

GİRİŞ

Ulusal ve uluslararası düzeyde toplumsal entegrasyonun artması ve teknolojinin çok hızlı bir şekilde ilerliyor olması, veri kavramının önemini gün geçtikçe daha da artırmaktadır. Veriye kolay ulaşmanın hayatın olağan akışı içerisinde çeşitli avantajları olduğu aşikârdır. Kamu sektöründen özel sektöre, hizmet sağlayıcılarından hizmetten faydalananlara kadar birçok kişi ya da kurum bu avantajlardan istifade etmektedir. Veriyi işlemenin, kullanmanın ve manipüle etmenin bu denli kolay olduğu bir ortam veri işleme kaidelerinin ve veriyi korumanın nasıl ve ne şekilde yapılacağı, işlemeden kimin sorumlu tutulacağı fikrini de ön plana çıkarmaktadır. Bu noktada, veri sorumlusu kavramı ortaya çıkmaktadır.

Veri sorumlusu, kişisel veri işleme faaliyetinin amaç ve araçlarını belirleyen gerçek veya tüzel kişidir. Veri sorumlusu, veri koruma düzenlemelerine intibak sağlanması ve kişisel verileri işlenen gerçek kişilerin hukuki düzenlemeler kapsamındaki taleplerinin muhatabı olması hasebiyle kişisel verilerin korunması hukukunda kritik öneme haizdir. Veri sorumlusu işleme faaliyetinin asli sorumlusu konumu ile yükümlülük altında bulunmaktadır. Veri sorumlusu kavramı

içerisinde gerçek veya tüzel kişi olma, tek başına veya başkalarıyla birlikte hareket etme gibi birtakım unsurlar barındırmakla birlikte veri sorumlusunun asıl unsuru veri sorumlusunun bağımsız olarak karar alma yeterliliğini veya kapasitesini gösteren işlemenin amaç ve araçlarını "belirleme" yetkisidir. Bu yetki kanunlardan, sözleşmeden veya kamu otoritesinin bildirimden kaynaklanabileceği gibi genellikle fiili olguların bir sonucudur.

Ortak veri sorumlusu kavramını ise veri sorumluluğunun özel bir türü olarak nitelendirilebilmek mümkündür. Ortak veri sorumluluğu işlemenin amaç ve araçlarının birden fazla veri sorumlusu tarafından birlikte belirlenmesini ifade eder. Bu çalışmada, ortak veri sorumlusu kavramı genel hatlarıyla ortaya konulacaktır.

VERİ SORUMLUSU KAVRAMI

Ortak veri sorumlusu kavramının anlaşılabilmesi için kısaca veri sorumlusu kavramına da değinmek gerekir. Zira kişisel verilerin korunması ile alakalı düzenlemelere uyumun sağlanması ve kişisel verileri işlenen kişilerin hukuki düzenlemeler kapsamındaki hak ve taleplerinin muhatabı öncelikli olarak veri sorumlusudur. Veri sorumlusu, kişisel veri işleme faaliyetinin amaç ve araçlarını belirleyen gerçek veya tüzel kişidir. Veri sorumlusu kavramı ile kişisel verilerin korunması hakkı arasındaki ilişki 1960'lı yıllardan bugüne büyük bir değişim göstermiş ve veri sorumluları zaman geçtikçe kişisel verilerin korunması bakımından farklı yükümlülük ve sorumluluklar ile yüzleşmek zorunda kalmıştır (Halıcıoğlu, 2019). Veri sorumlusunun tespiti 1990'lı yılların başında çok daha kolayken, bilgisayar teknolojisinin gelişimi ve internet kullanımının yaygınlaşması, ticari ilişkilerin ve haberleşme yöntemlerinin değişimi ve daha kompleks bir hal alması, kişisel veri işlemenin küreselleşmesi, veri işleme yöntemindeki karmaşıklığın artması sebepleriyle, bu belirgin durum daha bulanık bir hal almış, ilişkilerin ve yapıların karmaşıklaşması veri sorumlusu kavramının tespiti ve veri işleyen ile veri sorumlusu kavramı arasındaki çizginin belirgin şekilde çizilmesi çok daha zorlaşmıştır (Kuner, 2007).

Günümüzde pek çok kişisel veri işleme faaliyetinde birden fazla aktörün yer aldığı pek çok senaryo karşımıza çıkmaktadır. Buna örnek vermek gerekirse ülkemizde e-devlet uygulaması ele alındığında söz konusu uygulamanın kurulmasından ve yönetilmesinden sorumlu kurum ve kuruluşlar ile birlikte bu uygulama kapsamında vatandaşlara elektronik ortamda hizmet veren pek çok kurum bulunmaktadır. Dolayısıyla e-devlet uygulaması kapsamında gerçekleşen veri işleme faaliyetinde birden fazla aktörün varlığı veri sorumlusu tespitini zorlaştırmaktadır.

Veri sorumlusunun tespiti için kavramın temel esasları yol gösterici olmaktadır. Tanım ayrı ayrı analiz edilebilecek beş yapı taşı içermekte olup bunlar;

» Gerçek veya tüzel kişi, kamu kurum kuruluşu veya herhangi bir organ
» Belirleyen
» Tek başına veya başkalarıyla birlikte
» Amaç ve araçlar
» Kişisel verilerin işlenmesi şeklindedir.

Gerçek veya Tüzel Kişi, Kamu Kurum Kuruluşu veya Herhangi Bir Organ

Veri sorumlusu tanımının ilk unsuru kişilik unsurudur. Kimin veri sorumlusu sıfatına haiz olacağı yasal düzenlemelerden kaynaklanan yükümlülüklerin yerine getirilmesi bakımından önem taşımaktadır. 95/46/EC sayılı Direktif (Direktif) ve Avrupa Birliği Genel Veri Koruma Tüzüğü (Tüzük) gibi metinlerde "gerçek veya tüzel kişi, kamu kurum kuruluşu veya herhangi bir organın" veri sorumlusu sıfatını haiz olabileceği belirtilmiştir. Prensipte, gerçek veya tüzel, özel hukuk ya da kamu hukukunda yer almasına bakılmaksızın geniş bir çerçevedeki kişi veya kişi gruplarının veri sorumlusu olarak kabul edilebilmesi mümkün hale gelmektedir. Tüzel kişilerde bizatihi tüzel kişiliğin kendisi veri sorumlusu sıfatını taşımakta olup tüzel kişiliğin personeli, organı, yetkilisi veya tüzel kişilik nezdinde veri işleme faaliyetleri ile görevlendirilen kişi ve birimler veri sorumlusu olarak tavsif edilmemektedir.

Belirleyen

Veri sorumlusu tanımının bir diğer önemli unsuru veri işleme faaliyeti üzerindeki karar verme gücü/etkisidir. Veri sorumlusunu işleme faaliyetinde yer alan diğer paydaşlardan ayırmak için gerekli unsurları içerir ve veri sorumlusunu tayin edici en önemli unsur kişisel verilerin işlenmesinin amaç ve araçlarının belirlenmesidir. "Belirleme" yetkisi, veri sorumlusunun bağımsız olarak karar alma yeterliliğini veya kapasitesini gösterir. Bu yetki; kanunlardan, sözleşmeden veya kamu otoritesinin bildiriminden kaynaklanabileceği gibi genellikle fiili olguların bir sonucu da olabilmektedir (Avrupa Veri Koruma Kurulu, 2021). Madde 29 Çalışma Grubu ve Avrupa Veri Koruma Kurulu bir işleme faaliyetinde veri sorumlusunun anlaşılabilmesi için "İşlemenin neden yapıldığı", "Belirli bir amacın yerine getirilebilmesi için işlemenin yapılması gerektiğine kimin karar verdiği", ve "İşlemeyi kimin başlattığı" sorularının cevaplarının araştırılması gerektiğini öne sürmüştür (Madde 29 Çalışma Grubu, 2010, Avrupa Veri Koruma Kurulu, 2021).

İşlemenin karar verici tarafi genellikle yasal veya fiili olgulara bağlı olarak kolay bir şekilde tespit edilebilmektedir. Bazı durumlarda açık yasal bir yetkinin kullanılması veya doğrudan kanun tarafından veri sorumlusu da tayin edilebilmektedir. Nitekim, Tüzüğün veri sorumlusunu tanımlayan ilgili maddesinde buna vurgu yapılmıştır. Kamu kurum, kuruluşları görevleri kapsamında gerçekleştirdikleri kişisel veri işleme faaliyetlerinde veri sorumlusu olmaktadır. Öte yandan, yasal bir yetkinin yokluğunda veri sorumlusunun tespit edilmesi, işlemeyi çevreleyen tüm fiili koşulların değerlendirilmesi sonucu sağlanır. İşleme ile alakalı tüm şartlar göz önünde bulundurularak işleme üzerinde hangi tarafin karar verici etkisinin olduğu anlaşılmaya çalışılır. Ancak belirtmek yerinde olacaktır ki değerlendirme her bir spesifik işleme faaliyetinin kendine özgü şartları dikkate alınarak yapılmalıdır. Zira, bir işleme faaliyeti için veri sorumlusu olarak hareket eden tarafin başka bir işleme faaliyetinde veri işleyen şeklinde tavsif edilmesi de mümkündür. Bu hususdaki yaygın örneklerden biri muhasebe şirketleridir. Muhasebe şirketleri kendi çalışanları ile ilgili işleme faaliyetlerinde veri sorumlusu sıfatını taşırken hizmet verdiği müşteri ile alakalı verileri bakımından veri işleyen olarak kabul edilebilmektedir.

Veri sorumlusunun belirlenmesinde işlemenin tarafları arasında akdedilen sözleşme hükümlerinin değerlendirilmesi de faydalı olabilmektedir. İşleme için taraflar arasındaki sözleşmede direkt bir veri sorumlusu ataması yapılmasa da işlemenin amaç ve araçlarının belirlenmesinde kimin karar verici olduğu ilgili hükümlerin tetkik edilmesi ile ortaya çıkarılabilir. Şayet sözleşmede veri sorumlusu olan taraf açık bir şekilde belirtilmişse fiili durumu gerçekten yansıtıp yansıtmadığı kontrol edilmelidir. Tarafların sorumluluktan kaçınmak için aralarında akdedilen sözleşmeyi istedikleri şekilde tanzim etme imkânları bulunduğundan akdin fiili durum ile uyuşması önem arz etmektedir. Örneğin, işlemenin amaç ve araçları üzerinde belirleyici etkisi olan taraf sözleşmede veri işleyen olarak tavsif edilmişse de fiiliyatta veri sorumlusu olarak kabul edilmesi gerekmektedir (Avrupa Veri Koruma Kurulu, 2021).

Tek Başına ya da Başkaları ile Birlikte

Direktifte ve Tüzükte veri sorumlusu için işlemenin amaç ve araçlarına tek başına veya başkaları ile birlikte belirleyen ifadesi kullanılmıştır. Birden fazla tarafin veri sorumlusu olarak hareket edebileceği ihtimalini öngören daha net bir söyleyiş ile ortak veri sorumluluğuna kapı aralayan bu ifade çalışmamıza vücut veren ortak veri sorumluluğunun kaynağı olarak ilerleyen bölümlerde ele alınacaktır.

Amaç ve Araçlar

İşlemenin amaç ve araçlarının belirlenmesi ise işlemenin “neden” ve “nasıl” gerçekleştirileceği sorunudur bu nedenle bu iki faktör üzerindeki hangi etki düzeyinin bir kişi veya kuruluşun veri sorumlusu olarak nitelendirilebilmesi için yeterli olduğunun tespit edilmesi önem arz etmektedir. Amaç ve araçların belirlenmesi söz konusu olduğunda önemli olan bir gerçek veya tüzel kişinin veri sorumlusu sıfatını alabilmesi için hangi düzey ve ayrıntıda amaç ve araçları belirlemesi gerektiğidir. Bu nedenle, işleme faaliyetinin hukuka uygunluğu için gerekli ve önemli konularda örneğin işlemenin neden yapılacağı, hangi amaçların elde edilmesinin planlandığı, verilerin ne kadar süre ile saklanacağı, olası veri işleyen veya üçüncü kişilerin işleme faaliyetinde nasıl bir rol ve yetkiye sahip olacakları gibi hususlarda karar alınması veri sorumlusunun bir niteliği olup, buna ilişkin kararları alanlar fiili olarak veri sorumlusudur ve veri sorumlusunun yükümlülüklerine tabidir.

Araçların belirlenmesi ise sadece kişisel verilerin işlenmesinin teknik yollarını değil aynı zamanda hangi verilerin işleneceği, verilere kimlerin erişebileceği soruları gibi işlemenin nasıl yapılacağını gösterir teknik ve organizasyonel konuları da içeren daha geniş bir tanımlamadır. Ancak, bu her durumda veri sorumlusuna atfedilmiş bir nitelik olmayıp, veri sorumlusu hangi donanım veya yazılımın kullanılacağı gibi bazı teknik ve organizasyonel konulara ilişkin alınacak kararları veri işleyene devredebilmektedir. Araçların belirlenmesi kimi zaman veri sorumlusunun tespiti için yetersiz kalabilmektedir. Bu nedenle, hangi verilerin işleneceği, ne kadar süreyle işleneceği ve verilere kimlerin erişebileceği benzeri işleme faaliyetinin temel hususlarının belirlenmesi veri sorumlusunun kontrolüne bırakılmalıdır.

Önemle belirtilmelidir ki amaçları belirleyen olmak münhasıran veri sorumlusuna ait ise de araçları belirleme konusunda veri işleyen de veri sorumlusunun lehine hareket etmek koşuluyla temel olmayan araçları belirleyebilecektir. Eğer bir veri işleyen amaçların belirlenmesinde söz sahibiyse ve veriyi kendi menfaatleri adına işlerse veri sorumlusu olarak değerlendirilebilecek ve veri sorumlusunun yükümlülükleriyle bağlı olacaktır (Madde 29 Çalışma Grubu, 2010).

Kişisel Verilerin İşlenmesi

Veri sorumlusu tarafından belirlenen amaç ve araçlar ise kişisel verilerin işlenmesi ile alakalı olmalıdır. Tüzükte, kişisel verilerin işlenmesi veriler veya veri setleri üzerinde gerçekleştirilen herhangi bir işlem veyahut işlemler dizisi olarak

tanımlanmaktadır. Şu hâlde, veri sorumluluğu tek bir işleme faaliyeti için geçerli olabileceği gibi birden fazla işleme için de geçerli olması mümkün bulunmaktadır. Ancak işlemenin tamamı yerine belirli bir kısmı ile sınırlı kalmasına da engel teşkil etmemektedir.

ORTAK VERİ SORUMLULUĞU

Avrupa Genel Veri Koruma Tüzüğünün ortak veri sorumluluğunu düzenleyen 26'ncı maddesinde "joint controllers" tabiri kullanılarak kavram "İki ya da daha fazla sayıda veri sorumlusunun işleme amaçları ve araçlarını ortak bir şekilde belirlediği hallerde, bu veri sorumluları ortak veri sorumlularıdır. Ortak veri sorumluları, veri sorumlularının ilgili sorumlulukları veri sorumlusunun tabi olduğu Birlik veya üye devlet hukuku çerçevesinde belirlenmedikçe ve belirlendiği sürece, özellikle ilgili kişilerin haklarının kullanımı ve 13 ve 14. maddelerde atıfta bulunulan bilgi sağlama görevleri ile ilgili olarak bu Tüzük kapsamındaki yükümlülüklere uygunluğa ilişkin sorumluluklarını aralarındaki bir düzenleme vasıtasıyla şeffaf bir şekilde belirler. Düzenleme çerçevesinde ilgili kişilere yönelik bir irtibat noktası belirlenebilir." şeklinde tanımlanmıştır.

"Joint" sözcüğü Türkçe'ye ortak, ortaklaşa, müşterek ya da birlikte anlamlarında çevrilebilir. Bu sözcükler anlamsal olarak kavramı doğru karşılamakla birlikte Kişisel Verileri Koruma Kurulunun "ortak" sözcüğünü tercih ettiği anlaşılmaktadır (Kişisel Verileri Koruma Kurulu, 2021).

Kavram genel tanımı itibariyle bir işleme sürecinde işlemenin amaç ve araçlarının birden fazla paydaş tarafından birlikte/ortaklaşa belirlenmesini ifade etmektedir. Ortaklaşa belirleme ile karar alma süreçlerinin sadece işlemeye katılan tek bir veri sorumlusu tarafından tayin edilmediği, tersine işlemeye katılan tüm tarafların ortak iradesinin bir eseri olarak belirlendiği kast edilmektedir. Böyle bir durumda, her bir veri sorumlusu verileri işlenen kişilerin haklarının korunması için kanunların getirdiği yükümlülüklere bağlı hareket etmelidir. Ancak işleme sürecine birden fazla tarafın dahil olduğu her durumda ortak veri sorumluluğunun var olduğunu iddia etmek doğru bir yaklaşım değildir.

Teknolojinin günlük hayatta daha çok yer etmesiyle kişisel verilerin işlenmesi çeşitlenerek karmaşık bir görüntü almıştır. Farklı paydaşların kişisel verileri üzerinde aynı anda veya farklı zamanlarda ve aşamalarda farklı işlem veyahut işlem grupları gerçekleştirmesi mümkün hale gelmiştir. Ortak veri sorumluluğun tespitinde temel yaklaşım kişisel veri işleme sürecinin amaç ve araçlarının birden fazla paydaş tarafından belirlenip belirlenmediğine odaklanmaktır. Eğer işlemenin

amaç ve araçlarını tek bir taraf belirliyorsa burada ortak veri sorumluluğundan söz edilemez. Tarafların ortak karar alma sürecine katılımı farklı şekillerde olabilir ve taraflar arasında eşit söz hakkı, eşit sorumluluk vb. hususlarda her zaman eşitlik olmasına da gerek yoktur. İşlemenin amaç ve araçları tamamen ortak belirlenebilir, sadece amaç veya araç ortak belirlenebilir ya da bunlar kısmen ortak belirlenebilir. Ancak olası varyasyonların çokluğu ve işleme ortamlarının görece karmaşıklığı nedeniyle ortak veri sorumluluğu tipolojisinin kapsamlı ve detaylı bir şekilde sınıflandırılması mümkün olmamakta ancak müşterek birtakım fiili unsurlar aracılığıyla ortak veri sorumluluğunun bazı örnek ve kategorileri anlaşılabilmektedir. Mevcut işleme faaliyetlerinin artan karmaşıklığına karşı taraflar arasında akdedilen sözleşme hükümleri de ortak veri sorumluluğunun belirlenmesinde faydalı olmaktadır ancak sözleşme hükümleri her zaman fiili durum ile birlikte değerlendirilmelidir.

ORTAK VERİ SORUMLULUĞUNUN SONUÇLARI

Tüzüğün ortak veri sorumluluğunu düzenleyen 26'ncı maddesi uyarınca ortak veri sorumluluğunun birtakım sonuçları bulunmaktadır. Bunları değerlendirmek gerekirse öncelikle ilgili maddeye göre taraflar Tüzük kapsamındaki yükümlülüklerine uyum konusunda sorumluluklarını belirleyebilirler. Daha öz bir ifade ile ortak veri sorumluları kimin hangi işlemi yürüteceğini, kimin hangi işlem özelinde sorumlu olacağını netleştirmelidirler. Bu bilhassa birden fazla tarafın dahil olduğu karmaşık işleme ortamlarında yetki çatışmasının önlenmesi, veri koruma kurallarına tam uyumun ve kişisel veriler üzerindeki korumanın sağlanması açısından önem arz etmektedir. Aksi halde belirsizliğin getireceği karmaşa veri koruma yükümlülüklerinin ihlaline yol açabilecektir. Fiili koşullar da dikkate alınarak tüm görev ve sorumluluklar taraflar arasında açık ve şeffaf bir şekilde paylaşılmalıdır. Bunun yanı sıra ilgili kişilerin talep ve şikâyetlerinin kim tarafından cevaplanacağı da iç ilişkide kararlaştırılabilir. Ancak tarafların bu yöndeki kararından bağımsız olarak Tüzüğün 26'ncı maddesinin üçüncü fıkrası uyarınca ortak veri sorumlularından herhangi birine başvuruda bulunabilir. Bir diğer önemli husus ise ortak veri sorumlularının yükümlülükleri sadece Tüzüğün ortak veri sorumluluğunu düzenleyen maddesinde yer alan hususlar ile sınırlı kalmamakta veri sorumluları için Tüzükte düzenlenen genel veri koruma ilkelerinin uygulanması, işlemenin yasal dayanağının sağlanması, güvenlik önlemlerinin alınması, ihlal halinde denetim makamlarına ve ilgili kişilere bildirimde bulunma gibi tüm yükümlülüklere uymaları gerekmektedir.

Mevcut işleme faaliyetlerinin artan karmaşıklığına karşı görev ve sorumlulukların belirlenmesi ve paylaşılması noktasında Tüzük ortak veri sorumlularına

bir miktar hareket esnekliği sağlamıştır. Taraflar işlemenin Tüzük hükümlerine uyumluluğunu sağladıkları sürece görev ve sorumluluklarını belirlemelerinde bir engel bulunmamaktadır. Avrupa Veri Koruma Kurulu görev ve sorumlulukların belirlenmesinde hangi tarafın ilgili kişilerin taleplerini karşılayabileceği, işleme sürecinin farklı bölümleri için kimin daha yetkin olduğunun belirlenmesi benzeri iş bölümü ile alakalı konulara yanıt verecek bir iç analiz yapılarak kayda geçirilmesinin yararlı olacağını belirtmiştir.

Ortak veri sorumlularına ayrıca bir yükümlülük getirilerek Tüzükte yer alan yükümlülüklerinin bilhassa ilgili kişilerin bilgilendirilmesinin sağlanması hususundaki yükümlülüğün veri sorumluları arasında yapılacak sözleşme ile açık bir şekilde düzenlenmesi gerektiği ifade edilmiştir. Her ne kadar Tüzükte sözleşmelerin yasal şekli belirlenmese ve taraflara bu konuda serbestlik tanınsa da hesap verilebilirlik ve şeffaflık ilkelerinin bir gereği olarak Tüzük sözleşmelerin veri sorumlularının, ilgili kişilere karşı görev ve ilişkilerini net bir şekilde ortaya koymalarını beklemektedir (Dülger, 2019). Ayrıca, sözleşmenin özünün de ilgi kişilere sunulması gerektiği belirtilmiştir. Sözleşmenin özünden kasıt açıklanmamış olmakla birlikte Avrupa Veri Koruma Kurulu Tüzüğün 13 ve 14'üncü maddelerindeki hususlara değinecek şekilde asgari işlenen kişisel veri kategorileri, işlemenin amacı, ilgili kişilerin haklarını kullanabilmeleri için başvuru usul ve yollarını, alınan teknik ve idari tedbirleri, varsa veri işleyenleri, veri sorumlularının görev ve sorumluluk paylaşımı konularında ilgili kişilere bilgi sağlanabileceği görüşündedir (Avrupa Veri Koruma Kurulu, 2021).

Taraflar arasında akdedilecek böyle bir anlaşma/sözleşme vasıtasıyla sorumlulukların net bir biçimde dağıtılması uygulayıcılar açısından da kolaylık sağlayacaktır. İlgili kişiler ortak veri sorumlularının arasındaki anlaşma ile ortak veri sorumlularının üstlendikleri roller ve sorumluluklar hakkında bilgilendirilmelidir. Bununla birlikte, bilgilendirme yapılmış olsa dahi ilgili kişilerin ortak veri sorumlularının her birine de ilgili kişi hakları kapsamında başvuruda bulunmalarına mâni bir durum yoktur. Bu sebeple ilgili kişilerin veri sorumlularının her biri ile temasa geçebilmesinin de önü açılmalıdır.

SORUMLULUĞUN PAYLAŞILMASI

2018 yılında yürürlüğe girerek Direktifi mülga eden Tüzük, beraberinde veri sorumluları ve veri işleyenler arasındaki sorumluluk rejimini düzenleyen birtakım değişiklikler getirmiştir. Tüzüğün 82'nci maddesine göre veri sorumlusu halen veri işleme sürecinin asli sorumlusu olmakla birlikte veri işleyen de artık yaptırımların muhatabı ve Tüzüğün ihlal edilmesi durumunda ilgili kişilere karşı sorumlu tutulmuştur. İşleme sürecine birden fazla veri sorumlusu ve işleyen iştirak ettiğinde iştirakçilerin her birinin oluşan zararın tamamından sorumlu olacağı hükme bağlanmıştır.

Tüzük ile birlikte veri sorumlusuna yeni yükümlülükler getirilmiş ve veri sorumlusunun mevcut yükümlülükleri ağırlaştırılmış olsa da Tüzükteki veri sorumlusu için belirlenen sorumluluk rejimi temelde Direktifte veri sorumlusuna çizilen sorumluluk modeli ile aynı kalmıştır. Tüzüğe göre hukuka aykırı işleme nedeniyle ortaya çıkacak zarardan veri sorumlusu mesuldür. Şahsi kusurunun bulunmadığını ispatlaması da bu durumu değiştirmemektedir. Buna göre veri sorumlusunun kusursuz sorumluluğunun Tüzükte de devam ettiğini ifade etmek mümkündür. (Mesarcik, 2021). Veri sorumlusu adına hareket eden veri işleyenin hukuka aykırı eylemlerinin mesuliyeti de veri sorumlusu üzerindedir. Bu çerçevede, veri sorumlusunun mesuliyeti genel itibari ile devam etmekte ise de veri sorumlusu zarara neden olan olaydan sorumlu olmadığını ispat ederse yaptırımlardan kurtulabilmektedir. Veri sorumlusunun zarara neden olan olaydan sorumlu olmaması yani zararın kontrolünün ötesindeki olayların bir sonucu şeklinde vuku bulması ilgili kişinin kusuru veyahut mücbir sebep kaynaklı olabilmektedir (Alsenoy, 2016).

İşleme sürecine birden fazla tarafın dahli halinde ayrı veri sorumlusu şeklinde hareket eden veri sorumluları kendi tasarrufları altındaki işleme faaliyetleri bakımından mesuliyet taşımaktadır. Ortak veri sorumluluğu noktasında ise Tüzük ortak veri sorumlularının özellikle ilgili kişilere karşı görev ve sorumluluklarını aralarında yapacakları bir sözleşme ile belirlemelerine cevaz vermektedir. Ancak yukarıda değinildiği üzere Tüzüğün 82'nci maddesi uyarınca işlemeye dahil olan her veri sorumlusu ilke olarak zarardan sorumludur. Dolayısıyla tarafların aralarında akdettikleri anlaşma ile sorumluluk paylaşımında bulunmaları ilgili kişilere karşı zararın tümünden doğan sorumluluklarına engel teşkil etmemekte ve zararı meydana getiren olaya sebebiyet vermediklerini kanıtlamadıkları müddetçe sorumluluktan kurtulamamaktadırlar.

AVRUPA BİRLİĞİ ADALET DİVANI KARARLARI

Ortak veri sorumluluğu kavramının ve uygulamada kavramın nasıl yorumlandığının anlaşılması adına Avrupa Birliği Adalet Divanının (ABAD) geçtiğimiz yıllarda yayınlanan ortak veri sorumluluğu ile alakalı üç kararının tetkik edilmesi yerinde olacaktır. Bahse konu ABAD kararları sırasıyla 5 Haziran 2018 tarihli Wirstshaftsakademie ve Facebook İrlanda Kararı, 10 Temmuz 2018 tarihli Yehova Şahitleri Kararı ve 29 Temmuz 2019 tarihli Fashion ID ve Facebook Kararıdır.

Wirstshaftsakademie ve Facebook İrlanda Kararı

Wirstshaftsakademie ve Facebook İrlanda Kararı ABAD'ın ortak veri sorumluluğu hakkında vermiş olduğu ilk karardır. Wirstshaftsakademie, Facebook'ta kurduğu fan sayfası üzerinden eğitim hizmeti sunmaktadır. Fan sayfaları kişiler veya işletmeler tarafından Facebook'ta açılabilen kullanıcı hesaplarıdır. Fan sayfası yöneticileri, Facebook'a kayıt olduktan sonra Facebook tarafından tasarlanan platformu kullanarak kendini sosyal ağın kullanıcılarına ve fan sayfasını ziyaret eden kişilere tanıtabilmekte ve platformdaki her türlü iletişim imkânından yararlanabilmektedir. Facebook'un "Facebook Insights" adı verilen bir fonksiyonu sayesinde fan sayfası yöneticileri sayfa ziyaretçileri ile ilgili anonim istatiksel verileri elde edebilmektedir. Bahse konu hizmet Facebook'un değiştirilemeyen kullanım koşulları altında ücretsiz olarak sunulmaktadır. Bu veriler, sayfayı ziyaret edenlerin bilgisayarının sabit diskine ya da diğer medya araçlarına yerleştirilen ve her biri benzersiz bir kullanıcı kodu içeren çerezler vasıtasıyla Facebook tarafından toplanmaktadır. Çerezler iki yıl boyunca etkinliklerini koruyabilmektedir. Facebook'ta kayıtlı kullanıcıların bağlantı bilgileriyle eşleştirilebilen kullanıcı kodu fan sayfası yüklendiğinde toplanmakta ve yüklenmektedir. Wirstshaftsakademie ve Facebook İrlanda tarafından çerezlerin yüklenmesi ve işlevi ya da sonraki işleme süreci ile alakalı herhangi bir bilgilendirme yapılmamıştır (ABAD, 2018).

Dava konusu olay uzun yargısal süreçlerin ardından nihayetinde Alman Federal İdare Mahkemesi tarafından ABAD'a intikal ettirilmiştir. ABAD 13 Mayıs 2014 tarihli Google Spain kararına atıf yaparak veri sorumlusu kavramının kişilerin tam ve etkin korunmasının sağlanabilmesi adına geniş bir şekilde yorumlanması gerektiğini ifade etmiş olup sonrasında ise veri işleme faaliyetleri bakımından tarafların veri sorumlusu sıfatını kazanıp kazanmadıklarını değerlendirmiştir. ABAD'ın değerlendirmesine göre esas veri işleme faaliyeti Facebook tarafından fan sayfasını ziyaret eden kişilerin bilgisayarlarına veya diğer cihazlarına çerez yerleştirilmesi suretiyle gerçekleştirilmektedir. Ziyaretçiler Facebook hizmetlerini veya Facebook şirketler grubu tarafından sunulan hizmetleri kullandığında cihazlarına yerleştirilen bu çerezler yoluyla Facebook kişisel verileri elde etmekte, işlemekte ve kayıt edebilmektedir. Ayrıca, Facebook iş ortaklarının, üçüncü tarafların bu çerezleri reklam amaçlı kullanabileceği belirtilmiştir. Facebook çerezler vasıtasıyla elde ettiği verileri kendi sistemini iyileştirmek için kullanmakta ve fan sayfası yöneticilerine sayfalarını ziyaret eden kişilerle alakalı istatistiki veri sağlamaktadır. Örneğin, sayfalarını beğenenlerin veya sayfadaki uygulamaları kullananların profil bilgilerini vermekte böylece bu kişilerin ilgisini çekebilecek içeriklerin üretilmesine katkı sağlamaktadır. Salt Facebook gibi bir sosyal medya platformunu kullanmak kullanıcıyı işlenen veriler bakımından Facebook ile birlikte sorumlu yapmamakla birlikte fan sayfası yönetimi Facebook'ta sayfa açarak; Facebook'a ziyaretçilerin bilgisayar veya diğer cihazlarına Facebook hesabı olsun ya da olmasın çerez yükleme fırsatı tanımaktadır (ABAD, 2018).

ABAD Başsavcısı Yves Bot, dava ile alakalı mütalaasında veri sorumlusu kavramının şekli bir kavramdan ziyade işlevsel bir kavram olduğunu ve sorumluluğun tespitinde somut şartların ve fiili etkinin göz önüne alınması gerektiğini belirtmiştir. Bot'a göre veri sorumlusunun belirlenmesinde işlemenin neden ve nasıl yapıldığı sorgulanmalıdır. Bu hususta tayin edici unsur ise tarafların aralarındaki sözleşme çerçevesinde belirlenmiş rolleri yerine gerçekteki işlevlerinin/faaliyetlerinin tetkik edilmesidir. Bot, fan sayfası yönetiminin kişisel verilerin Facebook tarafından nasıl işleneceği konusunda baskın bir role sahip olduğu, işlemenin amaç ve araçlarının belirlenmesine katılım sağladığı; dolayısıyla işleme üzerinde fiilen etkisinin bulunduğunu ileri sürmüştür (Bot, 2018). Ayrıca, Wirstshaftsakademie ve Facebook'un işlemede yakın ilişkili amaçları bulunmaktadır. Wirstshaftsakademie, istatistiki veri elde etmeyi hedeflemekteyken Facebook reklam hizmetlerini geliştirme fırsatı yakalamaktadır. Bot, kişisel verilerin Facebook tarafından toplanması faaliyeti özelinde Wirstshaftsakademie'nin Facebook ile birlikte sorumlu olduğu sonucuna varmıştır. Her iki şirketin de Facebook tarafından gerçekleştirilen faaliyet bakımından sorumluluk taşımakta olduğu ancak bu sorumluluğun eşit sorumluluk anlamına gelmediği vurgulanmıştır.

Başsavcı Bot'un görüşü veri sorumlusunun amaçsal bir yorumu şeklinde anlaşılabilir çünkü defaten vurgulandığı üzere Avrupa Birliği hukukunun birinci önceliği kişisel verilerin dolayısıyla kişilerin temel hak ve özgürlüklerinin koruma altına alınmasıdır. ABAD da başsavcının görüşleri ile aynı doğrultuda Wirstshaftsakademie'nin Facebook'un kullanım koşulları ve çerez politikasını kabul ettiğini ifade etmiştir. Bu bağlamda Wirstshaftsakademie, Facebook tarafından kendisine sunulan parametreler vasıtası ile hangi hedef kitlenin verilerinin toplanacağı, toplanacak veri kategorileri gibi kriterleri belirleyerek Facebook'un veri işleme faaliyetine ve daha sonra hangi amaçlar için kullanılacağının belirlenmesine dahil olmaktadır. Wirstshaftsakademie'nin belirlediği kriterlere göre Facebook ziyaretçilerin verilerini toplayarak istatistik verisi haline getirmektedir. Bu çerçevede, Wirstshaftsakademie Facebook ile birlikte işlemenin amaç ve aracını belirlemekte ve her iki taraf ortak veri sorumlusu sıfatını almaktadır (Ronthkegel, Strassmeyer, 2019). ABAD, Wirstshaftsakademie gibi bir fan sayfasının Facebook'un sunduğu platform ve hizmetlerden yararlanmasının onu kişisel verilerin korunması ile alakalı yükümlülüklerden muaf tutmadığını değerlendirmektedir. Yine ortak veri sorumluluğu her durumda eşit sorumluluk anlamında ele alınmamalıdır. Zira birden fazla tarafın işlemenin farklı aşamalarında ve seviyelerde işlemeye

dahil olması olasıdır. Bu yüzden tarafların sorumluluğu somut olayın ilgili tüm koşulları dikkate alınarak tayin edilmelidir. Somut olayda, fan sayfası Facebook kullanıcı hesabı bulunmayan kişiler tarafından da ziyaret edilebildiğinden söz konusu kişilerin kişisel verilerinin işlenmesi bakımından Wirstshaftsakademie'nin sorumluluğu daha ağır basmaktadır (ABAD, 2018).

Yehova Şahitleri Kararı

ABAD'ın Wirstshaftsakademie ve Facebook kararından sonraki bir diğer önem arz eden kararı Yehova Şahitleri kararı olmuştur. Karara konu hadisede, Finlandiya'daki Yehova'nın Şahitleri Topluluğu üyeleri dini propaganda aracı olarak kapıdan kapıya iletişim yöntemini kullanmaktadır. Üyeler yaptıkları görüşmeler sırasında görüşme yaptıkları kişiler ile alakalı çeşitli bilgileri not almakta, kişilerin isimleri, adresleri, aile durumları ve dini inançları gibi bilgileri kayıt altına alınmaktadır. Söz konusu bilgiler sonraki ziyaretler için de saklanmaktadır.

ABAD, bir önceki Wirstshaftsakademie ve Facebook kararında yer alan görüşlerini aynen yineleyerek bunlara ilave olarak işlemenin amaç ve araçlarının belirlenmesi sürecinin veri sorumlusunun yazılı emir veya talimatları doğrultusunda yürütülmesine yönelik Direktifte herhangi bir şart olmadığını kişisel verilerin işlenmesine kendi amaçları için etki eden ve işleme faaliyetinin amaç ve araçlarının belirlenmesi sürecine katılan her gerçek veya tüzel kişi veri sorumlusu olarak tavsif edilebileceğini, ortak veri sorumluluğunun kabulü için işlemeye katılan tarafların verilere erişiminin bulunmasının gerekmediğini açıklamıştır (ABAD, 2018). ABAD, somut olayda ziyaret edilen kişilerden kişisel verilerinin toplanmasının ve sonraki işleme faaliyetlerinin Topluluğun inancını yayma maksadıyla kullanıldığını ve Topluluk üyelerinin Topluluğun çıkarları doğrultusunda hareket ettiğini belirtmiştir. Diğer yandan, Topluluk üyeleri ziyaret ettikleri kişilerle ilgili hangi durumlarda kişisel veri toplayacaklarını, hangi veri kategorilerinin toplanacağını ve sonrasında bu verilerin nasıl işleneceğini belirleyebilmektedir. Buna ilişkin koordinasyon, organizasyon ve teşvik Topluluk tarafından yürütülmektedir. Topluluk, veri işlemenin amaç ve araçları hususunda üyelerine gönderdiği yazılı talimatlar ile net ve kesin bir sınır ve kurallardan ziyade genel bir çerçeve belirlemekte üyeler de kendileri için belirlenen sınırlar dahilinde özgürce hareket ederek ziyaret edilen kişilerin hangi bilgilerinin ne şekilde toplanacağını belirleyerek inanışın yayılması amacına katılmakta ve aktif katkıda bulunmaktadır. Bu doğrultuda, işlemenin amaç ve araçlarının belirlenmesi sürecinde ortak hareket eden Yehova Şahitleri Topluluğu ve Topluluk üyelerinin ortak veri sorumlusu haline geldiği kabul edilmiştir (ABAD, 2018).

Fashion ID ve Facebook İrlanda Kararı

ABAD tarafından ortak veri sorumluluğu konusunda verilmiş son karar 2019 tarihli Fashion ID ve Facebook İrlanda kararıdır. Fashion ID online satış yapan bir Alman giyim perakende şirketidir. Fashion ID, internet sitesine Facebook tarafından sağlanan "beğen" butonunu üçüncü kişi eklentisi olarak yerleştirmiştir. Eklenti site ziyaretçilerine Fashion ID'nin hizmetlerini beğenme ve Facebook'ta yayınlama fırsatı tanımakla birlikte ziyaretçilerin ip adresleri, kullandıkları tarayıcının özellikleri ve beğendikleri içerik bilgileri Facebook'a iletilmektedir. Bunun için ziyaretçilerin Facebook hesaplarının olması veya "beğen" butonuna tıklamaları da gerekmemekte siteyi ziyaret etmeleri yeterli olmaktadır (Globocnik, 2019). Alman Tüketiciyi Koruma Derneği (Verbraucherzentrale-NRW) site ziyaretçilerinin bilgileri ve rızaları olmaksızın kişisel verilerin Facebook'a aktarımının hukuka aykırı olduğunu öne sürerek konuyu yargıya taşımıştır. Fashion ID yerleştirilen eklenti marifetiyle ziyaretçilerin kişisel verilerinin toplandığından ve Facebook'a iletildiğinden bilgisinin olmadığını zira söz konusu verilere erişemediğini ve işlemenin amaç ve araçlarını belirleyemediğini ileri sürmüştür. Facebook ise ziyaretçilerin ip adreslerinin jenerik hale getirildiği ve bu şekilde saklandığını ifade etmiştir. Nihayetinde, konu hakkındaki görüşlerini almak üzere Düsseldorf Bölge Yüksek İdare Mahkemesi (Oberlandesgericht Düsseldorf) tarafından ABAD'a başvurulmuştur.

ABAD Başsavcısı Michal Bobek dava ile ilgili mütalaasında Fashion ID'nin veri sorumlusu statüsüne ilişkin görüşlerini açıklamıştır. Fashion ID her ne kadar Facebook tarafından işlenen verilere erişemediğini ve bu çerçevede işlemenin amaç ve araçlarını belirleyemediğini iddia etse de başsavcı Bobek Fashion ID'nin Facebook'un ziyaretçilerin kişisel verilerini sitede yer alan eklenti sayesinde elde etmesini mümkün kıldığını ifade etmiştir. Buna ek olarak, Fashion ID'nin eklentiyi gönüllü olarak internet sitesine entegre ettiğini, eklentinin internet sitesine yerleştirilmesi işlemi ile toplanacak kişisel verilerin parametrelerinin belirlendiğinin söylenebileceğini ve ortak veri sorumluluğu için verilere erişimin şart olmadığını belirtmiştir (Bobek, 2019). Fashion ID ve Facebook kişisel verilerin ticari kullanımı için karşılıklı veya tamamlayıcı amaçlarla hareket etmektedir. Ancak tarafların ortak veri sorumluluğu işlemenin amaç ve araçlarının birlikte/ortaklaşa belirlendiği faaliyet ile sınırlı kalmaktadır. O halde Fashion ID, ziyaretçilerin kişisel verilerinin toplanması ve Facebook'a iletilmesi faaliyetinde Facebook ile birlikte ortak veri sorumlusu olarak kabul edilmelidir. Ancak Fashion ID'nin sorumluluğu verilerin Facebook'a iletiminin ardından gerçekleştirilecek işleme faaliyetlerini kapsamamaktadır. Bobek son olarak, kişisel verilerin toplanması ve Facebook'a iletilmesinden önce zamanında ve etkin korumanın sağlanabil-

mesi için ziyaretçilerin rızalarının alınması ve işlemeyle ilgili bilgilendirilmesi görevinin/sorumluluğunun Fashion ID tarafından yerine getirilmesi gerektiği üzerinde durmuştur.

ABAD, kararında ilk olarak internet sitesine eklentiyi yükleyen Fashion ID'nin Facebook'a iletilen veriler üzerinde herhangi bir etkiye sahip olmamakla birlikte eklentinin sağlayıcısı Facebook ile birlikte veri sorumlusu sıfatını alıp alamayacağı sorusuna cevap aramıştır. ABAD bu sorunun çözümü için Wirstshaftsakademie ve Facebook İrlanda ile Yehova Şahitleri kararlarındaki çizgisini devam ettirmiştir. Direktifin gayesinin kişilerin temel hak ve özgürlüklerinin en yüksek düzeyde korunması olduğu, söz konusu hedefin sağlanabilmesi için Direktifte veri sorumlusu kavramının geniş bir bakış açısıyla ele alındığı belirtilmiştir.

ABAD'a göre somut olayda Fashion ID hangi verilerin toplanarak Facebook'a aktarılacağı ve sonrasında yürütülecek işleme faaliyetleri konusunda herhangi bir rol almamakla birlikte Facebook eklentisini sitesine ekleyerek ziyaretçi verilerinin toplanmasına ve Facebook'a aktarılmasında bilinçli bir etkisi olmuştur. Zira Fashion ID'nin katkısı olmadan Facebook'un kişisel verileri elde etme ve işleme olanağı bulunmamaktadır. Fashion ID sitesine Facebook'un "beğen" butonunu ekleyerek ziyaretçilerin kişisel verilerinin toplanacağının ve Facebook'a iletileceğinin tamamen farkındadır. Öyleyse Fashion ID sitesine Facebook eklentisini yerleştirerek verilerin toplanması ve iletilmesi işlemleri üzerinde belirleyici bir etkiye sahip olmaktadır. Bu bağlamda sonuç olarakFashion ID internet sitesini ziyaret edenlerin kişisel verilerinin toplanması ve Facebook'a iletilmesi işlemlerinde Fashion ID ve Facebook işlemenin araçlarını birlikte belirlemektedir. İşlemenin amaçları için bakıldığında ise Fashion ID Facebook'un "beğen" butonunu internet sitesine yükleyerek ürünlerini sosyal medya mecrasında daha görünür kılarak bilinirliğini artırma gayesindedir. Ürünlerinin artan bilinirliği sayesinde Fashion ID ticari avantaj sağlayacaktır.

Bu nedenle site ziyaretçilerinin verilerinin toplanması ve Facebook'a iletilmesini kabul etmiş görünmektedir. Facebook da kendi sisteminin optimize edilmesi veya reklam/tanıtım faaliyetleri için söz konusu verileri kullanabilecektir. Sonuç olarak, bu işleme faaliyetleri hem Fashion ID hem de Facebook'un ekonomik çıkarları için gerçekleştirilmektedir. ABAD bu şartlar altında Fashion ID ve Facebook'un işlemenin amaçlarını da birlikte belirlediğini ifade etmiştir. Fashion ID'nin "beğen" butonu yoluyla toplanan ve iletilen verilere erişiminin olmamasının ortak veri sorumluluğuna engel teşkil etmediğini çünkü bir tarafın ortak veri sorumlusu olarak kabul edilebilmesi için gerekli şartın işlemenin amaç ve araçlarının birlikte belirlenmesi olduğunu vurgulamıştır (ABAD, 2019).

ABAD, Fashion ID gibi bir internet sitesinin Facebook hesabı olan veya olmayan tüm kişilerin erişimine açık olduğunu bu son durumda kişisel verilerin işlenmesinden Fashion ID'nin sorumluluğunun özellikle Facebook hesabı bulunmayan ziyaretçiler açısından daha fazla olduğunu açıklamıştır. ABAD'a göre verilerin toplanması ve iletilmesi öncesinde ziyaretçilerin rızalarının alınması gerekmektedir. İnternet sitesini ziyaret dolayısıyla kişisel veri işleme süreci başladığından ziyaretçilerin rızalarının alınması yükümlülüğü Fashion ID'nin üzerindedir. Rızanın işlemeye daha sonra dahil olan Facebook tarafından alınması ziyaretçilerin haklarının tam ve zamanında korunmasına engel teşkil edecektir. Bununla birlikte ABAD rızanın işlemenin amaç ve araçlarının Fashion ID tarafından belirlendiği işlemler için geçerli olacağını yani iletim sonrasında Facebook tarafından gerçekleştirilecek işlemeleri kapsamayacağını belirtmiştir. Ziyaretçilerin bilgilendirilmesi yükümlülüğü de ziyaretçiler ile ilk elden muhatap olduğu için Fashion ID üzerindedir. Ancak yine Facebook tarafından gerçekleştirilecek sonraki işlemleri kapsamayacaktır zira Fashion ID'nin bu işlemler ile alakalı bilgi sahibi olması beklenmemektedir (ABAD, 2019). Tüm açıklamalar ışığında ABAD internet sitesi ziyaretçilerinin kişisel verilerinin toplanması ve Facebook'a iletilmesi işlemi özelinde Fashion ID ve Facebook'un ortak veri sorumlusu oldukları sonucuna varmıştır.

ABAD Kararlarına İlişkin Değerlendirmeler

Yukarıda detayları aktarılan ABAD kararlarının arkasında yatan mantığın daha iyi anlaşılabilmesi ve ortak veri sorumluluğunun tespitine sistematik bir yaklaşım getirilebilmesi için veri koruma kanunlarında; özellikle Tüzükte tanımlanan veri sorumlusu kavramının temel unsurlarının irdelenmesi gerekmektedir. Öncelikle ortak veri sorumluluğundan bahsedebilmek için işlemede rol alan tarafların veri sorumlusu sıfatını taşıması zorunluluğu bulunmaktadır. ABAD, 2014 yılındaki Google Spain kararında, daha sonraki kararlarını da etkileyecek temel prensibini ortaya koymuştur. ABAD, Direktifin amaçsal yorumu yoluna giderek temel hedefin kişilerin temel ve hak özgürlüklerinin tam ve etkin korunması olduğunu, bunun temini için ise veri sorumlusu kavramının geniş bir şekilde ele alınması gerektiğini belirtmiştir (ABAD, 2014). Dolayısıyla, ortak veri sorumluluğu kavramının da aynı şekilde geniş bir perspektifte yorumlandığını söylemek mümkündür.

İşlemeye dahil olan tarafların veri sorumlusu sıfatını taşıyıp taşımadıklarının tespitinde çoğu durumda somut olayın koşulları dikkate alınmaktadır. İşlemenin amaç ve araçlarına karar veren taraf veri sorumlusu olarak hareket etmekte buna karşın işleme sürecinin esaslı unsurları üzerinde karar yetkisi bulunmayan taraf ise veri işleyen sıfatını almaktadır. Şartların gerektirmesi halinde işlemenin araç

yönü veri işleyen vasıtası ile dış kaynaklı sağlanabilir ancak veri sorumlusunun işleme üzerinde fiili kontrolü devam ettiği sürece bu onun veri sorumluluğunu engellememektedir (Hess, 2019).

İşleme sürecine birden fazla veri sorumlusu dahil olduğunda ortak veri sorumluluğu ihtimali değerlendirmeye alınmalıdır. Ortak veri sorumluluğu işlemede yer alan tarafların işlemenin amaç ve araçlarını birlikte belirlemeleri şartı ile geçerlilik kazanmaktadır. Ancak Ortak veri sorumluluğu kavramı sistematik bir konsept olmadığından uygulamadaki sorunların çözüme kavuşturulabilmesi için ABAD kararlarında da çok kez vurgulandığı üzere somut olaydaki tüm ilişkili faktörler bütüncül bir yaklaşım ile ele alınmalıdır.

Ortak veri sorumluluğunun belirlenmesinde temel kriter işlemenin amaç ve araçlarının işlemeye dahil olan taraflar tarafından birlikte belirlenip belirlenmediğidir. Burada belirtilmelidir ki işlemenin amaç ve araçlarının belirlenmesinde hangi düzeydeki etkinin ortak veri sorumluluğu için yeterli olduğu cevaplanması gereken kritik bir sorudur. Fakat, yasal düzenlemelerde bu etkinin ne düzey ve detayda olması gerektiği hükme bağlanmamıştır. Bu nedenle, böyle bir değerlendirme yapılabilmesi için ana odak noktası genellikle fiili olgular olmaktadır. ABAD, her işleme sürecinin aşama aşama incelenmesini ve işlemeye ortak veri sorumlusu olarak dahil olan taraflar arasında eşit düzeyde etkinin gerekli olmadığını, bunun yerine her bir tarafın bilinçli ve aktif münferit katkısının değerlendirmeye alınmasını salık vermiştir. Fashion ID kararında, sayfasına Facebook'un beğen butonunu entegre etmesinin işlemenin amaç ve aracının belirlenmesi için yeterli katkıyı sağladığını; dolayısıyla internet sitesinin Facebook ile birlikte ortak veri sorumlusu olduğuna hükmetmiştir. Bu görüşe göre ortak veri sorumluluğu amaç ve aracın tarafların birlikte belirlediği belirli işlem veya işlem dizileri için geçerli ve sınırlı olmaktadır. Dolayısıyla tarafların sorumluluğu da bu amaç ve araçları birlikte belirlenmiş belirli işlem veya işlemler dizisi çerçevesinde kalmaktadır. Fashion ID kararında Fashion ID'nin sorumluluğu verinin toplanması ve Facebook'a aktarılması işlemleri ile sınırlı kalmaktadır. Verilerin Facebook'a aktarımından sonra Facebook'un veriler üzerinde gerçekleştireceği işlemler özelinde Fashion ID'nin bir sorumluluğu bulunmamaktadır.

İşlemenin neden yapıldığı, işlemeyi hangi tarafın başlattığı ve işlemeden doğrudan kimin fayda sağladığı sorularına cevap aranması değerlendirmeye yardımcı olabilecek hususlardır. Bu hususlardan bir veya birkaçının belirli bir veri işleme faaliyeti için geçerli olması halinde ortak veri sorumluluğu ihtimali kuvvetlenmektedir. Örneğin bir tarafın işlemeden fayda sağlayıp sağlamadığı değerlendirilirken sunulan bir hizmetin karşılığı olarak ticari kazanç elde edilmesi tek

başına veri sorumluluğu için yeterli olmayacaktır. Çünkü bu durum sundukları hizmet için kazanç elde eden veri işleyenlerin ortak veri sorumlusu olarak kabul edilmeleri sonucunu doğurur ki ortak veri sorumlusu sıfatını alabilmek için ilgili işlemin doğrudan bir değer meydana getirmesi gerekmektedir.

İşlemenin amaç yönü bakımından ise taraflar işlemenin amaçlarını birlikte belirledikleri sürece farklı amaçlar gütmelerinde bir engel bulunmamaktadır. Tarafların amaçları aynı, farklı, birbirine yakın veya birbirini tamamlayıcı nitelikte olabilirler. Şu husus vurgulanmalıdır ki amaçlar belirli, açık ve meşru olmalıdır. Wirtshaftsakademie ve Fashion ID kararlarında Facebook kendi hizmetlerinin kalitesini artırma diğer internet siteleri ise ürünün tanıtımı, bilinirliğini artırma, ziyaretçi profilleri hakkın bilgi temin etme gibi kendi bağımsız amaçlarını takip etmektedir. Nihayetinde veri sorumluları kişisel verileri ticari amaç gibi genel bir hedefle işlemektedir. Ancak ortak veri sorumluluğundan bahis açabilmek için salt soyut düzeyde işlemenin amaçlarının belirlenmesi yeterli gelmemektedir. Araçların da birlikte belirlenmesi şartı aranmaktadır. Wirtshaftsakademie ve Fashion ID kararlarında olduğu gibi bir tarafın sunduğu işleme aracının, alt yapının kullanılması, tercih edilmesi; Yehova Şahitleri kararında belirtildiği gibi hangi verilerin toplanacağı, saklanacağı gibi işlemenin esaslı unsurlarının belirlenmesi bu mahiyette kabul edilmiştir. Ayrıca belirtmek yerinde olacaktır ki; örneğin bir tarafın diğer tarafların kişisel verileri belirli bir amaç için işlemesine olanak tanıyan bir uygulamayı diğerlerinin kullanımına sunması ortak veri sorumluluğuna yol açmamaktadır. Bunun için, işlemenin amaç ve araçları üzerindeki etkinin tüm ortak veri sorumluları tarafından bilinen veri setlerine yönelik olmasına bakılmalıdır. İşlenecek veri kümesine/kümelerine karar verilmesi veya önceden belirlenen işleme amaçlarının diğer veri sorumlusuna sunulması gibi işlemler ortak veri sorumluluğunu gündeme getirebilmektedir (Rothkegel, Strassmeyer, 2019). Bu sayede belirli bir veri kümesine ilişkin işleme amaçlarını önden belirleyen taraf diğerlerinin aynı veri kümesi üzerinde gerçekleştirecekleri işleme faaliyetine etki etmektedir.

Fiili işleme üzerinde herhangi bir etkide bulunmadan sadece tamamlanmış bir işleme faaliyetinden faydalanmak ortak veri sorumluluğuna neden olmamaktadır. Ortak veri sorumluluğu sadece söz konusu belirli bir veri işleme faaliyeti üzerinde etkinin uygulandığı durumlarda var olabilir. Daha önceden tamamlanmış bir işlemeden elde edilen sonuçların veya bilgilerin paylaşılması çoğu kez ayrı veri sorumluları arasında veri aktarımı şeklinde görülebilir. Ancak işleme öncesinde veya işleme sırasında planlayıcı, karar verici ya da teşvik edici bir etkide bulunulursa bu durum değişebilir (Rothkegel, Strassmeyer, 2019).

SONUÇ

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 26'ncı maddesinde ortak veri sorumluluğu özel olarak düzenlenmiştir. Ortak veri sorumluluğu, iki veya daha fazla veri sorumlusunun işleme sürecinin amaç ve araçlarını birlikte belirlemeleri halinde ortaya çıkan veri sorumluluğunun özel bir türüdür.

Uygulama açısından bakıldığında ortak veri sorumluluğuna dair şu iki temel nokta veri koruma otoriteleri ile işleme sürecinden etkilenen ve faydalanan kişiler için sorunlu gözükmektedir. Bunlardan ilki ortak veri sorumluluğunun tespitinin günümüzün karmaşık teknoloji dünyasında görece zor olması ve bu tespite imkân tanıyacak yeterli somut kriterlerin eksikliğidir. Esasında, ortak veri sorumluluğunun tespiti için tek bir kriter bulunmaktadır. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün ilgili maddesinin lafzından anlaşıldığı üzere ortak veri sorumluluğu işlemenin amaç ve araçlarının birden fazla veri sorumlusu tarafından belirlenmesi halinde ortaya çıkmaktadır. Burada önemli nokta işleme amaç ve araçlarının işlemeye dahil olan veri sorumluları tarafından birlikte belirlenmesidir. Ancak bu "belirleme" yetki veya kapasitesinin hangi ayrıntı ve düzeyde olması gerektiği netliğe kavuşturulmamıştır. Madde 29 Çalışma Grubu ve Avrupa Veri Koruma Kurulu yayınladığı dokümanlar ile konuya açıklık getirerek uygulamaya yön vermeye çalışmışsa da konu hakkında halen kısıtlı sayıda kaynak ve uygulama örneği bulunmaktadır. Avrupa Birliği Adalet Divanının bir önceki bölümde tafsilatıyla izah edilmeye çalışılan üç kararı bu konuda literatürdeki en temel başvuru kaynaklarıdır.

Avrupa Birliği Adalet Divanı, kararlarındaki mantığını kişilerin temel hak ve özgürlüklerinin tam ve etkin korunması gayesi üzerine inşa etmiş olup kararlar bu çerçeveden ele alınmalıdır. Kişilerin temel hak ve özgürlüklerinin korunması da veri sorumlusu kavramının dolayısıyla ortak veri sorumlusu kavramının geniş yorumuyla mümkün hale gelmektedir. Böylelikle işlemede yer alan tarafların veri işleme sürecinin tamamına yayılmaksızın belirli bir aşama veya aşamalarına aktif ve bilinçli katkıda bulunmaları ortak veri sorumluluğunun mevcudiyeti için yeterli kabul edilmiştir. Farklı veri sorumluları kişisel veriler üzerinde aynı anda veya farklı zaman ve aşamalarda, farklı işlem veya işlem grupları gerçekleştirebildiğinden tarafların belirleme sürecine katılımları da değişkenlik gösterebilir, yani taraflar arasında eşit söz hakkı, eşit sorumluluk vb. konularda her zaman eşitlik bulunmasına gerek yoktur. Aksine Avrupa Birliği Adalet Divanı kararlarında da görüldüğü üzere bir tarafın daha baskın olması mümkündür. Söz konusu kararlar işlemenin amaç ve araçları yönünden yorumlandığında, amaç ve aracın bir bütün halinde değerlendirilmesi gerektiği yani işlemenin hem amaçlarına hem de araçlarına dair birlikte karar alınması gerektiği söylenebilir. Karar alma düzeyi bir tarafın sunduğu altyapı, sistem veya işlem parametrelerinin kullanılması, kabul edilmesi, münferit veya ortak hedeflere ulaşılabilmesi için bir tarafın veri işlemesine olanak verilmesi, rıza gösterilmesi gibi mutlak eşitlik ve hakimiyet gerektirmeyen durumları kapsayabilmektedir. Ayrıca bir kez daha belirtilmelidir ki tarafların ortak belirlemeleri kaydıyla işlemede farklı, aynı, yakınsak veya birbirini tamamlayan amaçlar gütmelerinde bir sakınca bulunmamaktadır. Amaç unsurunun bu denli çeşitlilik gösterebilmesi nedeniyle ortak veri sorumluluğunun tespitinde araç unsuruna daha fazla dikkat gösterilmelidir.

Uygulama açısından zorluk arz eden ikinci husus ise taraflar arasında sorumluluğun ne şekilde belirleneceği ve paylaştırılacağıdır. Tüzükte ortak veri sorumlularına bilhassa ilgili kişilere karşı görev ve sorumluluklarını, aralarında akdedecekleri bir sözleşme ile belirlemelerine izin verilmiştir. Bir zararın ortaya çıkması halinde Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 82'nci maddesi uyarınca işlemeye dahil olan her bir veri sorumlusu ilke olarak zarardan sorumlu olmaktadır. İlgili kişi, taraflar arasındaki sözleşmeden bağımsız olarak her bir veri sorumlusuna karşı haklarını tatbik edebilmektedir. Bu bakımdan ortak veri sorumlularının ilgili kişilere karşı müteselsil sorumluluğunun bulunduğu söylenebilir. Fakat idari yaptırımlar söz konusu olduğunda Avrupa Birliği Genel Veri Koruma Tüzüğü'nde sorumluluğun belirlenmesi ve paylaştırılması sarih bir düzenleme ile açıklığa kavuşturulmamıştır. Avrupa Birliği Adalet Divanı, sorumluluğun tespitinde aşama temelli bir yaklaşım getirmiştir. Veri işleme sürecinin karmaşık yapısı dikkate alınarak uygulanan bu yaklaşımda, veri sorumluları amaç ve aracın birlikte belirlendiği işleme safhalarındaki sorumlulukları oranında değerlendirmeye tabi olmaktadır. Dahil olmadıkları işleme süreçleri bakımından taraflarına herhangi bir sorumluluk atfedilmemektedir. Ortak veri sorumlularına ilişkin sorumluluk ve kusur miktarlarının belirlenmesi açısından her halükârda olay bazında veri işleme süreçlerinin ve koşullarının incelenmesi gerekmektedir. ◆

KAYNAKÇA

- Alsenoy, B. V. (2016). The Allocation Of Responsibility And Risk Among Actors Involved In Personel Data Processing, (Doktora Tezi), Leuven Üniversitesi Hukuk Fakültesi, Leuven
- Avrupa Veri Koruma Kurulu/ European Data Protectıon Board (EDPB), (2021). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.0. Erişim adresi: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf
- Avrupa Birliği Adalet Divanı/Court Of Justıce Of The European Unıon (CJEU), Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. C-131/12. 2014. Erişim adresi: https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en
- Avrupa Birliği Adalet Divanı/Court Of Justıce Of The European Unıon (CJEU), Patrick Breyer vs Bundesrepublic Deutschland. C-582/14, 2016. Erişim adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0582
- Avrupa Birliği Adalet Divanı/Court Of Justıce Of The European Unıon (CJEU), Unabhangiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtshaftsakademie Schleswig-Holstein GmbH, Facebook Ireland Limited. C210/16. 2018. Erişim adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62016CJ0210
- Avrupa Birliği Adalet Divanı/Court Of Justıce Of The European Unıon (CJEU), Jehovan Todistajat - Uskonnollinen Yhdyskunta. C-25/17. 2014.Erişim adresi: https://curia.europa.eu/juris/document/document.jsf?docid=203822&doclang=EN
- Avrupa Birliği Adalet Divanı/Court Of Justıce Of The European Unıon (CJEU), Fashion ID GmbH & Co.KG Verbraucherzentrale NRW Ev, Facebook Ireland Ltd. Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen C-40/17. 2019. Erişim adresi: https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&doclang=EN

- Dülger, M. V. (2019). Avrupa Birliği Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması, Yaşar Üniversitesi Hukuk Fakültesi Dergisi, 1(2), 71-174
- Globocnik, J. (2019). On Joint Controllership for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID, International Review of Intellectual Property and Competition Law, (IIC) 50, 1033–1044
- Halıcıoğlu, M. (2019). Türk Hukukunda Veri Sorumlusu Kavramı, (Yüksek Lisans Tezi), Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara
- Kuner, C. (2007). European Data Protection Law, Corporate Compliance and Regulation, United Kingdom, Oxford University Press
- Madde 29 Çalışma Grubu/Artıcle 29 Workıng Party, (2010) Opinion 1/2010 on the Concepts of “Controller” and “Processor”, WP 169. Erişim adresi: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf
- Madde 29 Çalışma Grubu/Artıcle 29 Workıng Party, (2007) Opinion 4/2007 On The Concept of Personal Data, WP No: 136. Erişim adresi: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
- Mesarcîk, M. (2021) The Great Escape? Liability Of Public Authorities In The Data Protection Area, Institute of State and Law, Czech Academy of Sciences, 11,158-177
- Hess, S. (2019). The GDPR: Joint Controllership anda Independent Controllership Should the SWIFT Criteria Determine the Difference?, (Yüksek Lisans Tezi), Tilburg University, Tilburg
- Kişisel Verileri Koruma Kurulu, 23.12.2021 tarihli ve 2021/1303 sayılı Araç kiralama programları yazılımcısı ve satıcısı firmalar tarafından, ilgili kişilerin verilerinin işlenmesi ve bu verilerin araç kiralama firmaları arasında paylaşılmasını sağlayan bir kara liste programı oluşturulması hakkında Kararı.
- Rothkegel, T., Strassemeyer, L. (2019). Joint Control in European Data Protection Law-How to make Sense Of the CJEU’s Holy Trinity, Computer Law Review International, 20, 162-168

MAHREMİYET KORUMALI VERİ PAYLAŞIMI VE AÇIK VERİ

Mert VAROL

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen " Mahremiyet Korumalı Veri Paylaşımı ve Açık Veri " başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Günümüzde büyük miktarda veri gerek kamu kurumları gerekse özel şirketler tarafından toplanıp depolanmakta, işlenmekte ve fayda sağlayan bir kaynak konumuna gelmesiyle giderek daha çok alanda kullanılmaktadır. Dijital devrimle birlikte, veri ekonomide merkezi bir rol almaya başladı. Bununla birlikte, verilerin tam potansiyeline ulaşmak, onların nasıl sunulduğuna bağlı olmaktadır. Veriler değerleri kaybolmadan farklı şekillerde fayda sağlayacak biçimde kullanılmalıdır. Bu, verileri doğru biçimde ve doğru zamanda kullanılması ve ona değer katmak ve veriden değer yaratmak isteyen herhangi bir tarafa sunulması anlamına gelmektedir. Verileri paylaşmak ve açmak, birçok karar vericinin analizini geliştirebilmek için gerekli verileri çevrimiçi olarak kullanılabilir hale getirmek anlamına gelmekle birlikte aynı zamanda insanların zamandan tasarruf etmelerini veya her türlü sektörde daha bilinçli kararlar almalarını mümkün kılmaktadır.

Veri ve içerik bağlamında açık veri, herkesin herhangi bir amaç için özgürce erişebileceği, kullanabileceği, değiştirebileceği ve paylaşabileceği veri anlamına gelmektedir. Kamu kurumları tarafından açık hale getirilen ve kullanılabilecek veya yeniden kullanılabilecek birçok veri türü mevcuttur. Bunlar başlıca kültür, bilim ve araştırma, finans, istatistik, hava durumu ve çevre ile ilgili verileri içerebilir.

Verilerin açık veri olarak yayınlanması son yıllarda artış göstermektedir. Gittikçe daha fazla veri seti halka açılmış; vatandaşların, araştırmacıların veya uygulama geliştiricilerin gerçek zamanlı verilerden yararlanabilmesi için API'ler tasarlanmış ve bu verilere dayalı yeni uygulamalar geliştirilmiştir.

Kamu kurumları doğası gereği veri açısından oldukça zengindir. Verilerin kamu kuruluşları tarafından açılması, kamu sektörü verilerinin kullanıma sunulduğu ve böylece diğer veri kaynaklarıyla birleştirilebildiği ve vatandaşlar tarafından kamu hizmetlerinin iyileştirilmesi, ticari yeniliklere ilham verilmesi ve şeffaflığın sağlanması dahil olmak üzere çeşitli amaçlar için kullanılabileceği yeni bir olgudur. Temelde açık veri kamu sektörü tarafından açıklık ve şeffaflık çerçevesinde benimsenen bir yaklaşım olarak ön plana çıkmıştır. Bunun yanında verilerin yayınlanması ve yayınlanan verilerin analiz edilmesiyle verilerden yeni faydalar elde edilmesi de açık verinin kullanımını giderek yaygınlaştırmaktadır. Örneğin; hava durumunu kontrol etmeye, gidilecek adres için en iyi rotayı bulmaya veya gayrimenkul değerlerini karşılaştırmaya yönelik uygulamaların tümü açık verilerin kullanılabilirliğine bağlıdır. Bu örnekler, verilerin açık veri olarak yayınlanmasının vatandaşların günlük yaşamlarını nasıl iyileştirebileceğine örnek teşkil etmektedir. Benzer şekilde, işletmeler açık veri olarak yayınlanan devlet verileri sayesinde yeni hizmetler geliştirmenin yeni yollarını bulmaktadırlar.

Bununla birlikte tüm bu faydaların yanında verilerin açık olarak yayınlanması, farklı kaynaklardan elde edilebilecek verilerin eşleştirilmesi yoluyla bireylerin yeniden tanımlanması riskini de beraberinde getirebilir. Artan yeniden tanımlama riski, yararlı verilerin serbest bırakılması bakımından zorluklar yaratır ve dikkatli bir şekilde dengelenmiş bir yaklaşım gerektirir. Söz konusu verilerin niteliğine ve değerine bağlı olarak bazı yeniden tanımlama riskleri açık veri yayınlamada göz önünde bulundurulmaktadır.

AÇIK VERİ KAVRAMI

Açık veri; her türden kullanıcı için herhangi bir kısıtlama olmadan erişilebilen, paylaşılabilen, kullanılabilen ve yeniden kullanılabilen verilerdir. Open Definition'a göre açık veri; herhangi bir amaç için herkes tarafından serbestçe kullanılan, değiştirilen ve paylaşılan; en fazla kaynağı ve açıklığı koruyan önlemlere tabi olan veriler olarak tanımlanmaktadır (Monina ve Sedkaoui, 2016). Açık veri tanımı aşağıda yer alan spesifik ögeleri içerir:

Kullanılabilirlik ve Erişim: Verilerin bir bütün ve rahatlıkla herkesçe erişilebilir olmasıdır.

Yeniden Kullanım ve Yeniden Dağıtım: Verilerin yeniden kullanımının ve yeniden dağıtımının diğer veri kümeleriyle birleştirme olasılığı da dahil olmak üzere mümkün kılacak şekilde kullanılabilir hale getirilmesidir.

Evrensel Katılım: Verileri herkesin kullanabilmesi, yeniden kullanabilmesi ve yayabilmesidir.

Verilerin açıklığı ise iki boyutta düşünülmektedir:

Yasal Olarak Açıklık: Yasal olarak açıklık, verilerin herkesçe erişilebilir, yeniden kullanılabilir ve dağıtılabilir olmasını sağlayan açık bir lisansa sahip olmasıdır. Veriler minimum kısıtlamalara tabi olarak açık hale getirilmelidir.

Teknik Olarak Açıklık: Teknik olarak açıklık; verilere herkesin ortak, ücretsiz olarak kullanılabilen yazılım araçları ile erişebilmesi ve bu verilerin kullanılabilmesi için makine tarafından okunabilen ve tescilli olmayan elektronik formatlarda yayınlanmasıdır. Veriler herkese açık olmasının yanında teknik olarak açıklığı sağlayabilmesi için parola veya güvenlik duvarı kısıtlamaları olmaksızın herkese açık bir sunucuda erişilebilir olmalıdır (The World Bank, 2022).

Açık veri, veri setlerinin ortak bir alanda olmasını veya açık bir lisans aracılığıyla dağıtılmasını gerektirmektedir. Veriler bir bütün olarak, ücretsiz ve tercihen internet üzerinden indirilebilir ve açık lisans koşullarına uymak için olabilecek ek bilgiler de dahil olarak sağlanmalıdır (Van Loenen, Vancauwenberghe ve Crompvoets, 2018).

Açık veri özel sektör ya da kamunun dijital verisidir. Belirli bir yönteme göre yapılandırılmış bir şekilde ve ücretsiz erişimi garanti eden açık bir lisans ile teknik, yasal veya finansal kısıtlamalar olmadan herkesin yeniden kullanma olasılığına sahip olarak yayılır. Açık veriyi oluşturan bir dizi kaynak ve veri türü bulunur. Bu kaynaklar; her seviyeden kamu organı tarafından toplanan tüm verileri içeren kamu verileri, bilimsel araştırmalardan, özellikle de kamu tarafından finanse edilen araştırmalardan elde edilen veriler ve doğru teşvikler ve gizlilik korumaları ile kamuya açılabilecek özel sektör verileridir (Monina ve Sedkaoui, 2016). Açık veri hareketinin arkasındaki felsefe, temelinde vatandaşı merkeze alır. Bu anlamda, verilere ücretsiz erişim, demokratik kurumların vatandaş açısından geliştirilmesine katkıda bulunur. Bu etkinlik demokratik tartışmaları zenginleştirmeye, kamusal yaşamı canlandırmaya ve kamu hizmetlerinin yenilenmesine katkıda bulunmaya yardımcı olmalıdır. Açık veri süreci, inovasyonda ve kamusal faaliyetlerin geliştirilmesinde şeffaflık üzerine inşa edilmiş bir süreçtir. Açık veri aynı zamanda

kamu sektörünün verilerin bekçisi olma rolünden vazgeçtiği ve bunun yerine özel ve kamu sektörleri arasında güç dinamiklerinin yeniden düzenlenmesine yol açan bir veri ve bilgi sağlayıcısı rolüne geçiş yaptığı anlamına gelebilir. Bu açıklık; şeffaflığı, yeni uygulamaların geliştirilmesini ve veri zenginleştirilmesine bireysel katılımı teşvik ederek veriler etrafında devlet, şirketler ve vatandaşlar arasında ilişkiler kurmayı mümkün kılacaktır. Açık verilerin odak noktası ile ilgili herhangi bir kısıtlama bulunmamakla birlikte her türlü sosyoekonomik, iş, kültürel, çevresel veya bilimsel araştırmalar açık veri olarak kullanım alanı bulsa da, bugüne kadarki odak genel olarak yüksek kamu politikasına ve ekonomik, ulaşım ve mekânsal veriler gibi ticari yeniden kullanım değerine sahip verilerin açılması olmuştur.

Açık Veri İlkeleri

Açık veri, kamu sektörünün verilerin koruyucusu rolünü bırakması ve yerine yeni bir bilgi ve veri sağlayıcısı rolü koyarak kamu ve özel sektör arasındaki güç dinamiklerinin yeniden düzenlenmesini sağlaması açısından önemlidir. Verilerin açık veri olarak paylaşılması belirli ilkelere bağlıdır. Açık veri ilkeleri, hangi verilerin kamuya açık olması gerektiğini belirleyen bir kriter değildir. Mahremiyet, güvenlik ve diğer yasal kısıt ve endişeler veri setlerinin halkla paylaşılmasını engelleyebilir. Açık veri ilkeleri kamuya açık verilerin açık veri olarak kabul edilmesi için karşılaması gereken koşulları belirtir (Open Government Working Group, 2007). Açık veri ilkelerine ilişkin literatürde birbirinden farklı görüşler bulunsa da genel olarak kabul görmekte olan ilkeler ve açıklamalarına çalışmada yer verilmiştir:

Verilerin Eksiksiz Olması (Complete): Tüm kamuya açık veriler kullanıma sunulmalıdır. Kamuya açık veriler; geçerli gizlilik, güvenlik veya ayrıcalık sınırlamalarına tabi olmayan verilerdir. Veriler mümkün olan en yüksek ölçüde dijital olarak paylaşılmalıdır.

Verilerin Birincil Olması (Primary): Veriler mümkün olan en yüksek ayrıntı düzeyi ile birleştirilmiş ya da değiştirilmiş formlarda değil, kaynaktan ilk toplandığı gibi olmalıdır.

Verilerin Güncel Olması (Timely): Verilerin değerinin korunması için gerektiği kadar çabuk kullanıma sunulmalıdır.

Verilerin Erişilebilir Olması (Accesible): Veriler en geniş amaç ve kullanıcı yelpazesinde internette erişilebilir hale getirilmelidir.

Verilerin Makinelerce Okunabilir Olması (Machine Processable): Veriler, otomatik işlemeye izin verecek şekilde yapılandırılmalıdır. Verilerin yaygın olarak kullanılabilmesi, verilerin uygun şekilde kodlanmasını gerektirir. Serbest biçimli metin, tablo ve normalleştirilmiş kayıtların yerini tutmaz. Benzer şekilde bir metnin görüntüleri metnin kendisinin yerine geçmez. Normalleştirilmiş veri öğelerinin veri formatı ve anlamları hakkında yeterli belgeler, veri kullanıcıları için mevcut olmalıdır.

Verilerin Ayrımcı Olmaması (Non-Discriminatory): Veriler herhangi bir kayıt gerektirmeksizin herkesçe kullanılabilmelidir.

Verilerin Tescilli Olmaması (Non-Proprietary): Veriler, üzerinde hiçbir varlığın özel denetimi olmayan bir formatta kullanılmalıdır. Tescilli formatlar, verileri kimlerin kullanabileceği, nasıl kullanılabileceği ve paylaşılabileceği ve verilerin gelecekte kullanılabilir olup olmayacağı konusunda gereksiz kısıtlamalar ekler.

Verilerin Lisanssız Olması (License Free): Veriler herhangi bir telif hakkı, patent, ticari marka veya ticari sır düzenlemesine tabi olmamalıdır. Yalnızca makul gizlilik, güvenlik ve ayrıcalık kısıtlamalarına izin verilebilir. Devletlerin bünyesindeki bilgiler, kamuya açık kayıtlar, kişisel veriler, telif hakkıyla korunan çalışmalar ve diğer açık olmayan verilerin bir karışımı olduğundan, hangi verilerin mevcut olduğu, hangi lisanslama, hizmet koşulları ve yasal kısıtlamaların geçerli olduğu konusunda net olmak önemlidir. (The Annotated 8 Principles of Open Government Data, 2022)

AÇIK VERİ VE MAHREMİYET İLİŞKİSİ

Açık verilerden elde edilecek faydalar, kamu kurumları ve işletmelerin sahip oldukları verileri açık lisanslarla yeniden kullanılabilir formatlarda yayınlanmasını teşvik etmektedir. Ayrıca, hem tek başlarına hem de diğer veri setleriyle birlikte bu verilerin yeniden kullanımlarını artırmak için veriler bulunabilir ve diğer veri setleriyle birlikte çalışabilir hale getirilmeye çalışılmaktadır (Davies, Walker, Rubinstein ve Perini, 2019). Açık veriler şeffaflığın artması, kamu kurumlarının verimliliğinin artırılması, vatandaşların yönetime katılımlarının teşviki ve yeniliğin teşvik edilmesi dahil olmak üzere birçok amaca hizmet eder. Bunun yanında kamu kurumların topladığı, depoladığı ve işlediği veriler kişilerle ilgili bilgileri de içerebilir. Bu nedenle mahremiyet, açık verilerin yayımlanmasında dikkate alınması gereken bir konudur. Mahremiyet ile ilgili endişeler, ana kaynağı veri olan teknolojilerden büyük veri analitiği, yapay zekâ ve makine öğrenimi gibi alanlarda öne çıkmaktadır. Açık hükümet verileri bu yeni teknolojilerde ve sü-

reçlerde kullanılabilir, ancak bu durum mahremiyet endişelerini daha önemli hale getirmektedir Açık veri kümelerinin kişisel veri içermesi durumunda ortaya çıkabilecek mahremiyet zararlarına ek olarak, mahremiyetle ilgili endişeler, vatandaşları daha az veri paylaşmaya yöneltebilir. Birbirinden farklı kaynaklardan gelen verileri kullanarak birbirinden farklı veri setlerinden bireylerin yeniden tanımlanması potansiyeli, mahremiyet ve açık verilerle ilgili endişeleri daha keskin hale getirdi (Davies ve diğerleri, 2019). 2015 yılında kabul edilen Uluslararası Açık Veri Sözleşmesi verilerin açık veri olarak yayımlanmasından önce, kamu kuruluşlarının bu veriler için kişilerin mahremiyetine yönelik hassasiyeti ve riskleri değerlendirmesi gerektiğini, bireylerin kimliklerinin tespit edilememesi için açık verilerin varsayılan olarak uygun anonimleştirmeyi içermesi gerektiğini özellikle kabul eder (Open Goverrnment Partnership, 2015). Açık veri yayınlamada mahremiyet konusu, yayımlanacak veri setlerinin kişisel veri içerip içermediği dikkate alınarak ele alınmalıdır. Yeniden tanımlanma riskleri, verilerini açmaya niyetli kuruluşların verileri açık veri haline getirmeye yönelik isteklerinin azalmasına neden olabilir. Mahremiyet risklerinin ele alınması söz konusu olduğunda açık verilerin belirli zorluklar sunan bazı özellikleri vardır. Örneğin; açık verinin ideal karakteristiği, herhangi bir amaç için herkes tarafından özgürce kullanılabilen, değiştirilebilen ve paylaşılabilen veriler olmasıdır. Buna ticari amaçlar da dahildir. Açık verilerin, özellikle büyük veri ortamında ticari olarak yeniden kullanılması ve dağıtılabilir olması mahremiyet risklerini artırabilir.

Mahremiyetin açık veri yayımlanmasında önemli bir konu olduğuna şüphe yoktur. Vatandaş güveni, kuruluşların kendileriyle paylaşılan kişisel bilgileri uygun şekilde koruma yeteneklerine bağlı olmakla kalmaz, kişisel veriler gelişigüzel bir şekilde paylaşılırsa bireyler mahremiyet zararlarına maruz kalabilir. Kamu bilgileri ve verileriyle ilgili olarak mahremiyeti şeffaflıkla dengeleme ihtiyacı, açık veri hareketinden önce gelir. Bazı durumlarda, şeffaflığa yönelik kamu yararı, kişisel verilerin açık veri olarak ifşa edilmesini haklı kılabilir. Mahremiyet, bir ülkeden diğerine ve belirli bir ülkedeki alt gruplar arasında dahi değişebilen bir kavramdır. Ayrıca, her iki hedefin göreli önemine bağlı olarak, mahremiyet/şeffaflık dengesi de farklı şekillerde kurulabilir.

Hızla gelişen büyük veri ve yapay zekâ çağı, açık verilerin yeni kullanımlarına yol açmıştır. Bu teknolojiler aynı zamanda farklı kaynaklardan gelen anonimleştirilmiş verilerin eşleştirilmesi yoluyla bireylerin yeniden tanımlanması riskini de artırabilir. Bu artan yeniden tanımlama riski, faydalı açık verilerin paylaşılması için zorluklar yaratır ve dikkatli bir şekilde dengelenmiş bir yaklaşım gerektirir. Söz konusu verilerin niteliğine ve değerine bağlı olarak, bazı yeniden tanımlama riskleri kabul edilebilir. Açık veri yayıncıları potansiyel mahremiyet sorunlarını

belirlemek ve ele almakla uğraşırken, aynı zamanda, büyük veri çağından önce geliştirilen politikalara dayalı olarak hükümetler tarafından rutin olarak büyük miktarda kişisel veri yayımlanabilir. Kamuya açık kişisel veriler, mahkeme ve mahkeme kararlarında bulunabilir, seçimler, satın alma, kamu sektörü maaşları vb. ile ilgili çeşitli şeffaflık yasaları ve politikaları kapsamında yayımlanabilir (Davies ve diğerleri, 2019). Kamu verilerinin bu kategorileriyle ilgili olarak mahremiyete ilişkin riskler, bu tür verilerin kamuya nasıl açık hale getirildiğinin yeniden değerlendirilmesini gerektirecektir.

Açık verilerin yayınlanmasında mahremiyet ve şeffaflığı dengelemek, eğitim ve kaynak gerektirecek ve hükümetlerin bu kaynakları sağlama taahhüdü, dengenin nasıl sağlanacağı üzerinde önemli bir etkiye sahip olacaktır. Veri setleri kişisel veriler içerdiğinde, veri setlerini yayımlamayı reddetmek, yeniden kullanım için verilere erişimi sınırlayacaktır. Bunun yerine, açık verilerin paylaşılması teşvik edilirken mahremiyeti korumak için verilerin yeterince anonim hale getirilip getirilemeyeceğinin belirlenmesi önem arz etmektedir.

Gizlilik Riskleri ve Yeniden Tanımlama

Verilerin varsayılan olarak açık olması kurumların kendi verilerini proaktif olarak paylaşması, çevrimiçi olarak erişilebilir biçimlerde yayınlanması açık veriden elde edilecek faydalar açısından önemlidir. Açık verilerin önemli ekonomik, demokratik ve sosyal faydaları olsa da verilerin açık veri olarak yayınlanması, örneğin açık veriler kişisel verileri içerdiği takdirde, bireyin mahremiyetine yönelik tehdit oluşturacaktır. Bu verilerin yayınlanmasında mahremiyete yönelik birincil risk, bireylerin yeniden tanımlanabilecek olmasıdır. Bu, kişisel veri olan veya diğer bilgilerle kolayca bağlantı kurarak kişisel verilere dönüştürülebilen verileri içeren veri setlerini serbest bırakmaktır. Bir veri setinin açık veri olarak yayınlanmasında bir bireyin yeniden tanımlanması gibi olumsuz sonuç ortaya çıkabilir. Örneğin; bir kişi için aşağılanmaya, utanmaya veya endişeye neden olabilecek sağlık verilerinin serbest bırakılmasından, bireyin hassas bir sağlık durumu için tedaviye eriştiği sonucuna varılabilir. Veya verilerin açık veri olarak yayınlanması bireylerin istihdam veya ilişkilerine, birey hakkında verilen kararlar veya sigorta gibi hizmetlere erişimlerinde problemler, mali kayıplar ya da bir şiddet mağduru ya da suç tanığının kimliğinin belirlenmesi gibi güvenlik riski gibi zararları ortaya çıkarabilir. Bu zararların niteliği, kapsamı ve etkileri yayınlanan verilerin türlerine ve bireylerin kimliklerinin kapsamlarına bağlı olacaktır. Kamu verilerinin açılması ile ortaya çıkabilecek kimlik belirleme riskleri iki gruba ayrılabilir: Bir kişinin kimliğinin kasıtlı olarak bir girişim olmaksızın yeniden tanımlanması ve serbest bırakılan veri setinden bir kişiyi yeniden tanımlamaya yönelik kötü

niyetli ve kasıtlı bir girişim. Bu serbest bırakılan veri kümelerindeki verilerin diğer açık veri setleriyle ya da yasal olmaya yollarla başka şekillerle elde edilen veri setlerindeki bilgilerle eşleştirilmesiyle gerçekleşebilir (Privacy Committee of South Australia, 2014). Verilerini varsayılan olarak açık hale getiren kurumlar, aynı zamanda yayınladığı verilerde mahremiyet korunmasına da önem vermelidir. Verilerin yayınlanmasında bireylerin kimliklerinin yeniden belirlenmesi riskinin değerlendirilmesi, bir kurumun verileri yayınlama kararı almasında bu riskleri kabul edilebilir düzeye indirmek için atılması gereken adımlardan biridir (Article 29 Data Protection Working Party, 2013). Bir veri setinin açık olarak yayınlanmasında gizlilik risklerini yönetmenin ilk adımı, bu verileri kamuya açık hale getirme riskinin ilk değerlendirmesini yapmaktır. Bu risklerin değerlendirilmesi, yayınlanacak verilerin de ayrıntılı bir şekilde değerlendirilmesini gerektirecektir. Gizlilik riskinin seviyesi, verilerin yayınlanmasından ve bu tür bir yayının sonuçlarından kimlik tespit etme olasılığına bağlı olacaktır. Çoğu durumda en çok kullanılan mahremiyeti koruyucu risk azaltma tekniği, verileri hassas bilgilere kadar izleyebilecek her türlü tanımlayıcıyı ortadan kaldırarak kimliksizleştirmektir (Ethical and Responsible Use of Open Government Data, 2022).

Kimliksizleştirme

Giderek artan bir şekilde özellikle kamu kuruluşları çeşitli konularda veri setlerini halka açık hale getirmektedirler. Açık veri paylaşımı kapsamında yayınlanacak verilere örnek olarak, altyapı projelerine yapılan devlet harcamalarının bir tablosu veya kamu tesisleri için coğrafi kodlardan oluşan bir veri kümesi verilebilir. Bununla birlikte, serbest bırakılması amaçlanan diğer kamu verileri, kişisel olmayan ve kişisel veriler arasında bu kadar net bir ayrıma sahip olmayabilir ve kimliksizleştirilmiş kişisel verileri içerebilir. Kişisel verilerin kimliksizleştirilmesi, belirsiz kişisel tanımlayıcıların ve kişisel verilerin veri setlerinden kaldırılmasıdır, böylece bilgilerin konusu olan bireylerin tanımlanması riski minimuma inecektir. Kişisel veri içeren veri setleri için, kurumlar genellikle veri setlerini açık olarak paylaşmadan önce bu kişisel verileri veri setinden kaldırır. Kimliksizleştirme kişisel verilerin toplanan, kullanılan, arşivlenen ve paylaşılan verilerden kaldırılmasını tanımlamak için kullanılan bir terimdir (National Institute of Standards and Technology, 2022). Kimliksizleştirme tek bir teknik değil, farklı etkinlik düzeylerine sahip farklı veri türlerine uygulanabilecek yaklaşımlar, algoritmalar ve araçlar topluluğudur. Genel olarak, bir veri kümesinin yayınlanmasının yarattığı mahremiyet riski, daha agresif kimliksizleştirme teknikleri kullanıldıkça azalır, ancak bu durumda veri kalitesinin de düşme ihtimali ortaya çıkacaktır. Kamu kurumlarının elindeki verilere olan talep arttıkça, kurumlar kişisel verileri yayımlamak için bazı mahremiyet koruyucu süreç ve teknikleri uygulamalıdır. Bu

bağlamda önemli bir araç kimliksizleştirmedir. Kimlik gizleme, kişisel verilerin bir kayıttan veya veri setinden çıkarılması işlemi için kullanılan genel terimdir. Kimlik gizleme, bireylerin mahremiyetini korur, çünkü bir kez kimliksizleştirildikten sonra bir veri setinin artık kişisel veri içermediği kabul edilebilir. Bir veri seti kişisel veri içermiyorsa, paylaşımı, yayımlanması, yeniden kullanılması bireylerin mahremiyetinin ihlal edilmesi riskini olabilecek en düşük seviyeye indirecektir. Böylece mahremiyet koruma düzenlemeleri ile ilgili hükümler, bu tip veri paylaşımları için geçerli olmayacaktır. Veri setinin yeniden tanımlanması riskini sıfıra indirmediğini belirtmek önemlidir. Bunun yerine bu süreçle, yeniden tanımlama riskinin çok küçük olduğu veri setleri üretilir.

Kimliksizleştirilmiş veri setlerini serbest bırakmanın ana nedenlerinden biri, başkalarına araştırma amacıyla ham verilerin değerlerini ve özelliklerini inceleme fırsatı sağlamaktır. Bu nedenle, kimliksizleştirme, bireylerin mahremiyetini korurken, bilgilerde mümkün olduğunca fazla fayda sağlamaya çalışmalıdır. Açık veri girişimleri, proaktif olarak veri setlerini serbest bırakarak ve bunları herkesin kullanımına ve yeniden yayımlamasına ücretsiz olarak sunarak kamu kurumlarının şeffaflığını ve hesap verebilirliğini artırmayı amaçlar. Kimliksizleştirmenin bu amacı, onu açık veri paylaşımı için dikkate alınması gereken önemli bir araç haline getirir. Bu girişimlerin sağladığı artan bilgi miktarı ve kullanılabilirliği göz önüne alındığında, kurumların veri setlerini bireylerin mahremiyetini koruyacak şekilde yayınlamaları önemlidir. Açık veri girişimleri ayrıca araştırmayı, inovasyonu ve yeni uygulama ve hizmetlerin geliştirilmesini teşvik etmeye çalışır. Açık veri kümelerinin faydası ne kadar büyük olursa, kamu verilerini kullanmak isteyen araştırmacılar, yeni kurulan şirketler ve girişimciler için başarı şansı o kadar iyi olur (Information and Privacy Commissioner of Ontario, 2016). Kamu kurumları, veri setlerini içerisinde yer alabilecek kişilerin mahremiyetinden ödün vermeden araştırmacılara ve kullanıcılara açık hale getirmek için kimliksizleştirme yöntemini kullanabilir. Mahremiyet duyarlı veri setlerini açık veri setlerine dönüştürmek için kimliksizleştirmeyi kullanmak isteyen kurumlar; kimliksizleştirmeyi, veri yayımlamayı ve yayım sonrası izlemeyi desteklemek için uygun sürdürülebilir yönetişim yapıları oluşturmaya özen göstermelidir. Kimliksizleştirme işlemi kişisel verilerin mahremiyet koruyucu teknolojiler vasıtasıyla kişiyi belirlenebilir kılan özelliklerinden ayrılması olarak tanımlanmakta ve başta veri anonimleştirme olmak üzere bulanıklaştırma, şifreleme, anahtar kodlama olmak üzere, pek çok farklı kimliksizleştirme metodu kimliksizleştirme için uygulanmaktadır. Verilerin anonimleştirilmesi, kişisel verilerle ilgili veriler için geçerli olan, bir bireyin bu veri kümesinden doğrudan veya dolaylı olarak, bu verileri diğer veri kümeleriyle birleştirerek bile tanımlanamadığı dönüştürücü bir süreçtir. Bu, istenmeyen kişisel verilerin ifşa edilme risklerini azaltmaya yardımcı olurken,

verilerin verileri paylaşmak için katılımcılar arasında yeniden kullanılabilmesini, dağıtılabilmesini ve böylece açık verinin amaçlarına uygun olarak kullanılmasını sağlayacaktır (Dang, Küng, Takizawa ve Chung, 2020). Açık veri yayınlamada temel endişelerinden biri, kişisel verilerin izinsiz olarak paylaşılmasıdır. Bu sorun, veriler anonimleştirilerek giderilebilir diğer bir deyişle, veri setlerinde yer alan kişisel tanımlayıcıların, bir bireyin herhangi bir şekilde tanımlanmasını engelleyecek ölçüde kaldırılmasını ve verilere erişen tarafların verileri anonimleştirmeye çalışmasını engelleyecek ölçüde kaldırılmasını gerektirmektedir. Veriler mahremiyeti korumak için uygun şekilde anonimleştirildiği takdirde, araştırma amacıyla indirilebilir, kullanılabilir, paylaşılıp ve analiz edilmesi için serbestçe kullanılabilir olacaktır (Al Ryalat ve Momani, 2019).

SONUÇ

Açık veri herkes tarafından, herhangi bir yerde, herhangi bir amaç için özgürce kullanılabilen, paylaşılabilen veriler olarak tanımlanmaktadır. Açık veriler tanımı ve özellikleri gereği herkesin serbestçe erişebileceği ve herhangi bir kısıtlama olmaksızın kullanabileceği ve manipüle edebileceği şekilde yayınlanan veriler olarak ifade edilir. Verilerin açık veri niteliğinin olması için; veriler bütün olarak mevcut, kolayca erişilebilir, yeniden kullanılabilir, yeniden dağıtılabilir ve evrensel olmalıdır (yani herkesçe erişebilir, yeniden kullanabilir veya yeniden dağıtabilir). Genel olarak verilerin açık veri olarak kabul edilebilmesi için, başkaları tarafından kullanılması, birleştirilmesi, yeniden yayımlanması ve üzerine inşa edilmesi amacıyla açık, izin verilen bir lisans altında makine tarafından okunabilir bir biçimde yayınlanması gerekmektedir.

Veri temelli ekonomide açık veri kullanımının yaygınlaşması; inovasyonun teşvik edilmesi, iş süreçlerinin, ürünlerin ve hizmetlerin iyileştirilmesine yönelik katkı sağlaması, yeni ürün ve hizmetlerin geliştirilmesi gibi faydalarından dolayı kaçınılmaz bir durumdur. Ekonomik faydasının yanında kamu kurumları açısından daha fazla şeffaflık, demokratik hesap verilebilirlik, yönetime daha fazla vatandaş katılımı, devlete karşı güven yaratılması gibi faydalar açık verinin sağladığı önemli faydalar arasında yer alır.

Verilerin açık veri olarak hiçbir kısıtlama olmaksızın yayınlanarak yeniden kullanımının ve serbestçe erişilebilirliğinin, daha fazla şeffaflık ve ekonomik faydalar getireceği söylenebilir. Ancak bununla birlikte, açık veri yayınlaması sonucunda verilere kolayca erişilebilmesi, kullanılabilmesi, yeniden kullanılıp dağıtılabilmesi, kişiler açısından bir mahremiyet riski unsurunu da berberinde getirecektir. Mahremiyetin ve kişisel verilerin korunmasının söz konusu olduğu tüm durumlarda dengeli bir yaklaşım izlenmelidir. Çünkü açık verilerin doğası gereği kısıtlama olmaksızın herkesçe erişilebilir, serbeste paylaşılabilir ve herhangi bir amaç için özgürce kullanılabilir veriler olması, kişisel verilerin ilgili düzenlemelerde öngörülen şartlar ve ilkelerle işlenebilmesi, aktarılabilmesi gibi sebeplerle açık veri olarak yayınlanmasının önünde bir zorluk ve mahremiyete yönelik de bir risk unsuru ortaya çıkarmaktadır. Bu yüzden veriler her zaman için mahremiyetin ifşası riski de göz önünde bulundurularak ve bu risk minimuma indirildikten sonra açık veri olarak yayınlanmalıdır. Özellikle kamu kurumları tarafından açık veri portalları veya diğer platformlar aracılığıyla açık veri ve verilerin yeniden kullanım girişimleri, kişisel veriler yerine anonimleştirilmiş verilerin yeniden kullanım için kullanılabilir hale getirilmesi amaçlanmalıdır. Bu yaklaşım veri mahremiyetinin sağlanması ve korunması ile şeffaflık arasında bir denge sağlanması bakımından

daha güvenilir bir yol olacaktır. Bu yüzden açık veri yayınlama için veriler uygun tekniklerle anonimleştirilmelidir. Anonimleştirme, kişisel bilgiler içeren verilerin ifşasının önlenmesi amacıyla mahremiyet koruyucu modeller ve teknikler vasıtasıyla bireyi tanımlayıcı öznitelikler üzerinde yapılan kimliksizleştirme işlemidir. Anonimleştirme tamamen veya ağırlıklı olarak teknik bir faaliyet olarak görülebilir ancak; verileri güvenli bir şekilde paylaşmanın en iyi yolu olarak anonimleştirme seçildikten sonra, bir sonraki adım uygun bir istatistiksel modeli seçmek gibi görünebilir. Tüm bunlarla birlikte anonimleştirme; araştırma, yasal ve etik değerlendirmeler, risk analizi ve testlerini içeren bundan daha derinlemesine bir süreçtir. Veri setleri anonimleştirildiğinde, yeniden tanımlama riskinin değerlendirilmesi gereklidir ve yeniden tanımlama testi yapmak iyi bir uygulama olabilir. Anonimleştirmeyle, verinin biçimi ve tipi korunarak paylaşılmış büyük veri setlerinde yer alan bireylerin tanımlayıcı bilgileri ve hassas verilerinin ifşa edilmesi riski en aza indirilebilir ya da tamamen engellenebilir. Fayda sağlayacak içerikten yoksun bırakılmış verileri açık veri olarak yayınlamanın bir anlamı olmayacaktır. İdeal olarak, anonimleştirme, veriyi fayda amaçlı kullanacak tarafların ihtiyaçlarını karşılamak için yeterli faydayı korurken yeniden tanımlama riskini minimuma indirecek şekilde uygulanmalı ve yöntemler buna göre seçilmelidir. Bu yüzden açık veri paylaşımında veri mahremiyeti sağlanırken bu çalışma kapsamında da açıklanmış olan diferansiyel mahremiyet gibi yenilikçi veri mahremiyeti yaklaşımları maliyet uygulanabilirlik çerçevesinde uygulanmalıdır.

Son olarak ülkemizde açık veriye yönelik herhangi bir yasal düzenleme bulunmadığı görülmüştür. Bu konuya ilişkin olarak ilgili kurumlarca çalışmalar yapılması gerekliliği ve yapılacak yasal düzenleme çalışmalarının günümüzde hemen hemen her alanda bireylerin faaliyetleri neticesinde üretilen veriden fayda sağlamaya yönelik yaklaşım olan açık veri paylaşımının, veri mahremiyeti göz ardı edilmeden, aralarında bir denge oluşturularak mevcut düzenlemeler ile birlikte ele alınması gerektiği düşünülmektedir.

KAYNAKÇA

- Alryalat S. S., Momani, S. M. (2019) A Beginner's Guide to Using Open Access Data, CRC Press.
- Dang, T. K., Küng, J. , Takizawa, Chung, Makoto Tai M., der., (2020). Future Data and Security Engineering Big Data, Security and Privacy, Smart City and Industry 4.0 Applications, Singapore: Springer Singapore,
- Data Europa, "Ethical and Responsible Use of Open Government Data", 2022, https://data.europa.eu/sites/default/files/report/2015_ethical_and_responsible_use_of_open_government_data.pdf, 10.09.2022.
- Davies, T., Walker, S. B., Rubinstein, M., Perini F. (2019) The State of Open Data Histories and Horizons, Cape Town: African Minds and International Development Research Centre.
- IPC, "De-identification Guidelines for Structured Data", 2022, https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf, 13.09.2022.
- Monino, J-L, Sedkaoui, S. (2016), Big Data, Open Data and Data Development, Londra: ISTE Ltd.
- NIST, "De-Identifying Government Datasets", 2022, https://csrc.nist.gov / csrc/media/ publications/sp/800-188/draft/documents/sp800_188_draft2.pdf, 10.09.2022.
- Opendatacharter, "Principles", 2022, https://opendatacharter.net/, 04.04.2022.
- Opendatatoolkit, "Open Data Essentials", 2022, http://opendatatoolkit.worldbank.org/en/essentials.html, 04.04.2022.
- Opengovdata, "The Annotated 8 Principles of Open Government Data", 2022, https://opengovdata.org/, 30.03.2022.
- Privacy and Open Data Guideline, Privacy Committee of South Australia, 22.02.2020.

◊ Public Resource, “Open Government Data Principles”, 2022, https://public.resource.org/8_principles.html, 23.03.2022.

◊ Van loenen, B., Vancauwenberghe G., CROMPVOETS, J. (2018) .Derleyen: Open Data Exposed, Lahey: T.M.C. ASSER PRESS.

YAPAY ZEKÂ SİSTEMLERİNDE VERİ KORUMA YAKLAŞIMLARI

Begüm Tuğçe BURHAN

Kişisel Verileri Koruma Uzmanı

“Bu çalışma 14.02.2023 tarihinde kabul edilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 4857 sayılı İş Kanunu Kapsamında Kişisel Verilerin Korunması başlıklı uzmanlık tezinden alınmıştır.”

GİRİŞ

Yapay Zekâ (YZ) uygulamaları, insanın bilişsel süreçlerine uyumlu bir şekilde çalışmasıyla beraber hayatımızda önemli bir yer edinmeye başlamıştır. Bilginin dijital ortama aktarılarak gelişen teknolojiler kapsamında kullanım süreçlerinde; bir iş modelini değiştirmek, yeni gelir ve değer üreten firsatlar sağlamak amaçlı kullanımı sonucu dijitalleşme yaygınlaşmaya başlamıştır. Dijitalleşmeyi, büyük verinin kullanımını, bulut teknolojilerinin yaygınlaşmasını ve nesnelerin internetinin kullanımını kapsayan Yapay Zekâ sistemlerinin kullanımı, yaşamı kolaylaştırarak birçok yeniliğin ortaya çıkmasına olanak sağlamaktadır. Yapay Zekâ teknolojisi ile beraber bilgi işlem gücünün artmasıyla teknolojiler ucuzlayıp hızlanmakta ve organizasyonlarda daha az insani iş gücüne ihtiyaç duyulmaktadır. Tüm bu faktörler yeni teknolojilerin kullanımına ilişkin ve Yapay Zekânın etkinliğini arttırmaya yönelik teşvik edici nitelik taşımaktadır.

Yapay Zekaya ilişkin yaşam döngüleri verilerin toplanması ile başlamakta olup, bu verilerin analizi ve çıktıların değerlendirilmesi ile bilgilerin sentezlenerek süreçlerin başlamasına dayanmaktadır. Bu durum veri ekonomisine değer katmakta

olup, çalışmalarla beraber hayal etmesi güç eylemlerin bile teknoloji ile gerçekleşebilmesini mümkün kılmaktadır. Bu teknolojilerin kullanımı ile hizmetlerde iyileşme gerçekleşmesi ve verimliliğin artması sağlanmaktadır. Öte yandan verilerin YZ teknolojileri makine öğrenmesi süreçlerinde kaynak olarak kullanılması ile; bilgiye erişilmesi, toplanması, değerlendirilmesi ve çıktıların alınması kaçınılmazdır. Bilgi işleme süreçlerinin bulut bilişim ile etkileşimi sayesinde büyük miktarda veri toplanarak çeşitli yerlerde depolanabilmektedir.

Konu, ilgili kişilerin mahremiyeti ve özel hayatın gizliliği açısından değerlendirildiğinde; verilerin işlenme amacı dışında kullanılması, kişilerin davranış modellerinin ve karakter analizinin tespit edilerek profilleme gerçekleştirilmesi, veri yanlılığı sonucu YZ uygulamaları tarafından önyargı içeren kararlar alınması, öneri sistemleri ile bireylerin yönlendirilmesi gibi durumlarda etik ve hukuki problemlerin doğarak mahremiyet ihlallerinin ortaya çıkabildiği görülmektedir. Uygulama geliştirme sürecinde kullanılan verilerin doğru ve güvenilir olmadığı veya algoritmik kararların adil olmadığı durumlar, kişilerin hak ve özgürlüklerinin zarar görmesine veya ekonomik kayıplara neden olabilmektedir. Bahse konu araçlar kullanılarak yaşamın kolaylaştırılması sağlansa da diğer yandan pek çok hususta oluşturabileceği muhtemel risk ve tehlikeler ile de farklı disiplinler için tartışma konusu olabilmektedir.

Ancak Yapay Zekânın insanlık için çok önemli ve büyük bir yenilik olduğunu göz ardı etmemek, bu konudaki gelişimleri engellememek büyük önem taşımaktadır. Bu noktada teknolojinin gelişimi ile dengeli bir biçimde, insan haklarının korunması çerçevesinde hukuki ve etik düzenlemeler yapılarak ve çeşitli teknik ve idari tedbirler alınarak kişisel verilerin korunması kapsamında kişilerin temel hak ve özgürlüklerinin korunması ihtiyacı doğmaktadır. YZ kullanımında, veri yönetişimi stratejisi uygulanırken kaynakların yalnızca yapay zekâ ürün geliştirmeye odaklanmak yerine mahremiyeti artırmaya yönelik, kullanımda mahremiyet odaklı olunması, güvenliğin ve sistemlerin takibinin de sağlanması gerekmektedir.

Bu kapsamda, veri koruma ilkelerine uyumlanmasına yönelik düzenlemeler ile

1. Sistemlerin demokratik ve anayasal denetiminin sağlanması,
2. Eşitlik, adalet, hakkaniyet şeffaflık, mahremiyet ve hesap verebilirlik gibi değerlerin korunması,
3. YZ sistemleri ve uygulamaları için standart kalite seviyesi geliştirilmesi,
4. Bu sistemlerin uygun ve orantılı bir biçimde kullanılması,
5. İlgili kişiler ve kullanılan veriler açısından şeffaflığın sağlanması,

6. Taraflar için yükümlülüklerin ve sorumlulukların belirlenmesi,
7. Verilerin kullanımının ilgili kişilerin mahremiyeti ve yönlendirilmesi açısından oluşturabileceği risklerin azaltılması,
8. Geliştirilen sistemlerde oluşabilecek hataların kolaylıkla belirlenip ayıklanabilir olabilmesi

gerekmektedir (Hoffmann-Riem, 2019). İlgili düzenlemelerin ise veri koruma ilkelerine uygun bir biçimde, şeffaf, etkin, teknolojik gelişmelerin artışını destekleyici, gelişmeleri kapsayacak ve çeşitli alanları düzenleyebilecek şekilde esnek, meşru ve yeterli olması gerekmektedir (Baldwin, 2011).

Bu konuda düzenlemeler yapılırken ayrıca, YZ teknolojisini kullanmanın yararlarından ve zararlarından kimin veya neyin sorumlu olduğu ve güvenilir yapay zekâ için gereksinimlerin neler olduğu sorularına değinmek gerekmektedir.

YZ teknolojilerinin makine ve derin öğrenme ile insan beynini model alarak insanlar tarafından gerçekleştirilen muhakeme, özerklik, yaratıcılık vb. faaliyetleri gerçekleştirdiği görülmektedir. Makine öğrenmesi ile YZ uygulamaları çok hızlı bir biçimde öğrenme ve değişim gerçekleşmekte, dinamik olarak kendi alt hedeflerini belirleme kapasitesine ve harici sensör bilgileri veya güncellenmiş girdi verileri aracılığıyla yerel koşullara uyum sağlama yeteneklerine sahip olmaktadır. Aynı zamanda, makine öğrenme sistemleri, önceden programlanmayan yollarla alternatifler arasında seçim yapan bağımsız kararlar alarak ve bunu herhangi bir insan müdahalesi olmadan gerçekleştirecek şekilde tasarlanmıştır. (CoE, 2019)

Faaliyetleri değerlendirilerek yapay zekânın gelişmişlik düzeyi göz önüne alındığında, veri sorumlusunun robot olarak kabul edilmesi durumunda kişiliğinin belirsizliği problemi ortaya çıkmaktadır. Doktrinde yer alan görüşlerde YZ'ye kölelik statüsü verilmesi, tüzel kişilik benzeri bir kişilik tanınması gerektiği, ya da öngörülebilirlik ve şeffaflık sorunlarının ortadan kaldırılması adına yapay insan statüsü, elektronik kişi olarak kabul edilmesi görüşleri yer almaktadır.

Konuya ilişkin olarak, gelişmiş otonom robotların elektronik kişi statüsü edinmesi ile, robotların özerk karar alabilecekleri durumlarda veya üçüncü taraflarla bağımsız olarak iletişim sağladıkları hallerde neden olabilecekleri muhtemel hasarlarda, robotlara elektronik kişilik statüsü verilerek sorumluluk almaları gerektiği görüşleri de mevcuttur. (European Parliament, 2015) Bu yaklaşımla, yapay zekâ sistemlerine bir tür yasal statü verilmesinin, yapay zekayı geliştiren veya başlatan şirketten ayırarak, yapay zekanın neden olduğu kayıp ve hasar için belirli bir tazminat planının yapay zekanın kendisi için oluşturulmasını sağlaya-

cağı öngörülmektedir. YZ teknolojisinin dinamik yapısı gereği, bu teknolojinin gelişimi ile birlikte, iş süreçleri ve tüketicilere ilişkin ilgili yeni hesap verebilirlik ve sorumluluk biçimlerine ihtiyaç duyulacağı açıktır.

Ancak YZ sistemlerine doğrudan sorumluluk yüklemek yerine mevcut sistemler ve uygulamaların değerlendirilmesi gerekmekte olup, ele alınan YZ sistemlerinin henüz kendilerine ve geçmişlerine ilişkin bilince sahip olmamaları durumunda bu sistemlere doğrudan sorumluluk yüklemek uygun olmayacaktır. (Erdoğan, 2021) Ayrıca insan üretimi ile ortaya çıkan YZ'ye sahip varlıklara kişilik atfedilmesi durumunda, üretimi yapanın ve kullanıcının sorumluluğunu zayıflatmak gibi, olası sorunları ortadan kaldırmaktan çok yeni sorunlar ortaya çıkarması muhtemeldir. (Akyol, 2021) Bu noktada belirtmek gerekir ki, yaşamımızı etkileyen her alanda olduğu gibi bu YZ'nin uygulamalarının kullanımında ortaya çıkan hukuki, insan hakları ihlallerini önleyecek, etkili ve meşru düzenleyici mekanizmalara ihtiyaç duyulmaktadır.

Tüm yasal düzenlemelerin yanısıra yapay zekâ uygulamalarının geliştirme süreçlerinden itibaren, YZ'nin dinamik yapısı gereği gelişmelere uyum sağlayabilecek, siber tehditlere karşı koruma sağlayabilecek, düzenlemelere ve mahremiyetin korunmasına yönelik gelişmelere adapte olabilecek çeşitli teknik ve idari tedbir, yöntem ve araçlara ihtiyaç duyulmaktadır. Ortaya çıkan düzenleme ve yönlendirme gereksinim ile birlikte konuya ilişkin birçok ülke tarafından rehber veya açıklayıcı nitelikli rehberler sunulmuştur.

Bu hususta ülkemizde, Kişisel Verileri Koruma Kurumu tarafından "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler" başlıklı rehber düzenlenmiştir. (KVKK, 2021) Rehberde, YZ teknolojileri geliştirilirken insanlara hizmet edecek şekilde tasarlanmasını sağlamak üzere; geliştiriciler, üreticiler, servis sağlayıcılar ve karar alıcılara yönelik tavsiyeler sunulmakta olup, gerçekleştirilen çalışmalar çerçevesinde kişisel verilerin korunması hususunda açıklık sağlanması hedeflenmektedir. Rehberde, YZ sistemlerinin geliştirilme ve uygulama süreçlerinde ilgili kişilerin temel hak ve özgürlüklerine saygı gösterilmesinin gerekliliği vurgulanmaktadır. Aynı zamanda YZ sistemleri geliştirilirken ilgili kişiler üzerinde ayrımcılık, önyargı gibi istenmeyen etkiler yaratmasından kaçınılmasının önemi belirtilmektedir. Bu kapsamda, demokrasinin işleyişini, sosyal ve etik değerleri göz önünde bulunduran yaklaşımın gerekliliğinin üzerinde durulmaktadır. Ayrıca, konuya ilişkin genel ve taraflar için tavsiyeler sunulmuş olup, tasarımdan itibaren veri koruma ilkesine uygun bir biçimde teknolojik gelişmelerin gerçekleştirilmesine yönelik alınabilecek olan teknik ve idari tedbirler sunulmaktadır. Bu kapsamda YZ sistemleri geliştiricilerinin, üreticilerinin, servis sağlayıcılarının

ve karar alıcılarının; YZ teknolojilerinin yaşam süreçleri boyunca genel kapsamlı bu rehberden faydalanmaları konuya ilişkin çalışmalarında veri güvenliğini sağlamaları hususunda önem arz etmektedir.

YAPAY ZEKÂ UYGULAMARINDA KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK ALINABİLECEK TEKNİK TEDBİRLER

Yapay Zekâ uygulamaları, sosyal yaşam, ekonomik gelişim, toplum refahı ve güvenliğinin iyileştirilmesine yönelik birçok yenilik sunmaktadır. Ancak bu teknolojilerin yayılması ile birlikte veri miktarının ve çeşitliliğinin artmasına sebep olan süreçlerde kişisel verilerin de kullanılması bireyler için risk teşkil edebilmektedir. Bilindiği üzere, Kanun'da veri sorumlularının yükümlülükleri arasında "kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak" yer almaktadır. Bu kapsamda veri sorumlusu gerekli tüm teknik ve idari tedbiri almak zorundadır.

Kişisel verilerin kullanıldığı, işlendiği, depolandığı; öğrenme, çıkarsama, uygulama süreçleri için büyük veriye ve algoritmanın büyük verilerle eğitiminin sonucu olarak veri modeline ihtiyaç duymaktadır. Bu uygulamaların veya sistemlerin kişisel verileri de içerebilecek olmaları sebebi ile uygulama geliştiriciler veya sağlayıcıların veri mahremiyetini sağlamaları gerekmektedir.

Sürekli değişmekte ve gelişmekte olan YZ uygulamalarının kullanımına ilişkin süreçlerde ortaya çıkabilecek risklere ilişkin olarak uygulanabilecek tedbirlerin konu özelinde değerlendirilmesi gerekmekle birlikte, uygulanabilecek güvenlik tedbirleri çalışmada örneklendirilmiştir. YZ sistemlerinin geliştirildiği ve devreye alındığı süreçlerde süreç boyunca mahremiyet değerlendirilmesi yapılmasına yönelik, eğitim verisi ihtiyacını azaltmaya yönelik, temel veri kümesini azaltmadan veri korumasını desteklemeye yönelik ve kara kutu sorununu önlemek için tasarlanmış yöntemler kullanılmaktadır. Bu yöntemler süreçlerle ilişkilendirilerek örneklendirmek mümkündür;

1. **Tasarım Gereği ve Varsayılan Ayarlarla Mahremiyet İlkeleri:** Tasarım gereği ve varsayılan ayarlarla mahremiyet kavramının amaçları; mahremiyeti sağlamak, kişilerin kendilerine ilişkin bilgileri üzerinde kontrolünün olmasını sağlamak ve kuruluşlar için sürdürülebilir bir rekabet avantajı elde edebilmelerini sağlamaktadır. (Cavoukian, 2011) Risk odaklı yaklaşımlara dayanan ilkelere uyum ile yapay zekanın oluşturabileceği tehditler önceden ele alınarak minimum düzeye indirilmesi hedeflenir. Bu ilkelerin YZ teknolojisinin

her aşamasında göz önünde bulundurulması; herhangi bir sistemin, hizmetin, ürünün veya sürecin tasarım aşamasında ve daha sonra yaşam döngüsü boyunca veri koruma konularının dikkate alınmasını sağlar ve belirli amaca ulaşmak için yalnızca gerekli olan verilerin işlenmesini gerektirir.

2. **Veri Koruma Etki Değerlendirmesi:** Modernize Edilen 108 sayılı Sözleşme'nin 10(2) maddesinde; veri sorumlularının ve veri işleyenlerin "bu tür bir işleme faaliyeti başlamadan önce, amaçlanan veri işlemenin, ilgili kişilerin temel hak ve özgürlükleri üzerinde oluşabileceği muhtemel etkisini incelemenin ve değerlendirmenin ardından, veri işleme faaliyetini bu faaliyete bağlı riskleri önleyecek veya bu riskleri en aza indirecek şekilde tasarlanmaları gerektiği" belirtilmiştir.

   Bu durum AB mevzuatında GDPR madde 36 uyarınca, "veri işleme faaliyetlerinin bireylerin hak ve özgürlükleri için yüksek risk oluşturabileceği durumlarda etki değerlenmesi yapılması gerekmektedir" biçiminde ele alınmıştır.

   Yapay Zekâ teknolojilerinin gelişimiyle beraber karmaşıklaşan veri işleme faaliyetleri gözlemlendiğinde, veri sorumlularının sürecin doğasını, kapsamını, bağlamını, yeni teknolojilerinin etkisini ele alarak, veri işlemenin gerekliliği, orantılılığı ve ilgili kişilerin hak ve özgürlüklerine ilişkin oluşabilecek riskleri değerlendirmeleri gerekmektedir. Veri koruma etki değerlendirmesi yapılarak, kişisel verilerin işlenmesinden önce mahremiyete ilişkin risklerinin ve bu yönde alınabilecek tedbirlerin belirlenmesi ve risklerin en aza indirilmesi sağlanabilir.

3. **Kişisel Verilerin Anonim Hale Getirilmesi:** YZ sistemlerinin eğitim ve işleyiş verilerine ilişkin anonimleştirme gerçekleştirildiği durumlarda, kayıtların sonradan ayırt edilememesi sayesinde ilgili kişilerde daha fazla güven duygusu uyandırarak daha fazla veri paylaşımı sağlayarak, yapay zekâ sistemlerinin performansının önemli ölçüde iyileştirilmesi sağlanabilecektir. Anonimleştirmenin ilgili YZ öğrenme sürecinde YZ sistemlerinin işlevlerini gerçekleştirmesine engel olması durumunda ise takma adlandırma (Pseudonymisation) ile, bir bireyin adı gibi benzersiz bir tanımlayıcının yerine başka bir değer atanması ile gizliliğin arttırılması sağlanabilmektedir. Her iki yöntemde de temel amaç yalnızca gerekli olan verilerin muhafaza edilmesi ile kişisel verilerin muhafaza edilme süreçlerinde meydana çıkabilecek riskleri en aza indirmektir.

4. **Çekişmeli Üretici Ağ:** Çekişmeli Üretici Ağlar gerçek verilerin yerine geçebilecek, yeni, sentetik veri örnekleri oluşturmak için iki sinir ağı kullanan algoritmik mimarilerdir. Bu yöntem ile makine öğrenim süreçlerinde, eğitim seti gerçek verilerle uyumlu istatistiklerle yapay veri üreterek yeni veriler oluşturmaktadır. Günümüzde asıl kullanım alanı görüntü üretimine yönelik olmakla beraber, pek çok alanda büyük hacimli yüksek kaliteli, yapay eğitim verileri üretmek için bir yöntem olma potansiyeline de sahiptir. Bu durum, gerçek kişisel bilgileri içeren büyük miktarda veriyi kullanmaya gerek kalmadan büyük hacimli verilere olan ihtiyacı karşılayacaktır. (Goodfellow, 2014)

   Bu teknoloji sayesinde etkili bir biçimde anonimleştirme gerçekleştirilebilmektedir. Yapay olarak oluşturulan ve gerçek olaylardan kaynaklanmayan sentetik veriler üretilmesi sağlanmaktadır. Bu nedenle veriler gerçek olmadığı için kişisel veri olarak kabul edilemez. Ancak bu yöntemin Deepfakes teknolojisinin temelini oluşturduğunu ve kullanım durumuna bağlı olarak, ilgili kişinin mahremiyetini riske atabileceği veya mahremiyeti koruyucu bir tedbir olabileceği unutulmamalıdır.

5. **Federe Öğrenme:** Federe öğrenme yöntemi kullanılarak, veri veya modellerin güvenilmeyen cihazlarda depolanması, güvenilmeyen kanallar üzerinden iletim veya güvenilmeyen hizmetlerde hesaplama problemlerine ilişkin çözüm sağlamak amaçlanmaktadır. (OVIC, 2019)

   Federe öğrenme dağıtık öğrenme prensibine dayanmaktadır. Bu makine öğrenmesi yönteminin ana özelliği, yerel bir veri kümesine sahip merkezi olmayan cihazlara veya sunuculara dayalı paylaşılan istatistiksel modellerin eğitmesine olanak sağlamasıdır. Eğitim verileri yerelde tutularak, kullanıcı verilerinin, kullanıcıların cihazlarından hiç çıkmadan, eğitim sürecinin birçok kullanıcı arasında dağıtılarak işbirlikçi bir süreç izlenmektedir.

   Başka bir deyişle, verileri tek bir konumda bir araya getirme ihtiyacını ortadan kaldırarak makine öğrenimini merkezden uzaklaştırır. Bunun yerine model, farklı konumlarda birden çok yinelemede eğitilir. Daha genel anlamda bu yöntem, makine öğrenimi algoritmalarının farklı konumlarda bulunan çok çeşitli veri kümelerinden deneyim kazanmasına olanak tanır. Tüm bu avantajların yanısıra bu yöntemin kullanımı, ham verilerin merkezi bir sunucuya geri iletilmesi ve ardından sonuçların cihaza geri gönderilmesi nedeniyle oluşan zaman gecikmesini azaltmaktadır. Tahmin cihazın kendisinde gerçekleştiği için gerçek zamanlı tahmini mümkün kılmaktadır.

   Veri güvenliği açısından değerlendirilecek olursa; federe öğrenme tasarım ge-

reği ve yapısal olarak veri minimizasyonunu içermektedir. Yöntemin çalışma prensibinde anlatıldığı üzere veri toplama ve birleştirme, federe yaklaşımda birbirinden ayrılamaz. Müşteri verilerinin amaca özel dönütleri, analistlerin müşteri başına mesajlara erişimi olmadan, anında birleştirme için toplanmaktadır. Ayrıca ele alınan makine öğrenmesi ve analiz hedefleri, anonim olarak veri toplama hedefiyle uyumludur. Makine öğrenme sürecinde amaç, eğitim için kullanılan verileri fazla ezberlemeden tüm kullanıcılar için doğru tahminde bulunan bir modeli eğitmektir.

6. **Matriks Kapsülleri:** Matriks kapsülleri, sinir ağlarının yeni bir çeşididir ve öğrenme faaliyeti için daha az veri gerektirmektedir. Kapsüller, bir katmandaki tüm aktivasyon olasılıkları ve kapsüllerin pozlarını bir sonraki katmandaki aktivasyon olasılıkları ve pozlarına dönüştüren çok daha karmaşık bir sistem kullanmaktadır. Temel bir hesaplama birimi oluşturabilmektedir.

7. **Diferansiyel Mahremiyet:** Diferansiyel mahremiyet yöntemi, veri setinde yer alan kişilerin bilgilerini anonim hale getirirken, grupların kalıplarını tanımlayarak veri kümesi hakkındaki bilgileri herkese açık olarak paylaşmak için kullanılan bir sistemdir. Bu sayede veri sorumlusu orijinal verileri bünyesinde tutarken, veri setini yayınlama esnasında veri kümesinin anonimleştirilmiş görünümlerini oluşturabilmektedir.

Bu yöntem ile, istatistiksel veri tabanları üzerine yapılan analizlerde gürültü ekleme metodu kullanılarak sistemin yaşam döngüsünde girdi, model ve çıktı süreçlerinde koruma sağlanmaktadır.

Kişisel verilerin kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi durumu olan anonimleştirmeyi sağlamak, orijinal veriler kullanılarak gerçekleştirilen model veya analizin kullanımına göre daha düşük seviyede doğruluk sunabilmektedir. Ancak verilerin korunması kapsamında diferansiyel mahremiyet yönteminin kullanılması ile, veri setine gürültü eklenmesi gibi yöntemlerle araştırmacılar gerçek verinin gürültü eklenmiş halini kullanmaları sonucu gerçek veriye yaklaşık değerler elde etmiş olacaklardır. (Canbay ve Sağıroğlu,2020)

Konuyu örneklendirmek gerekir ise, gerçek kişilere ilişkin bilgileri içeren bir veri tabanından bilgi alındığında yanıt, veri tabanındaki kişiler hakkında bilgi alınmasını sağlayan, ancak belirli bireyler hakkında kesin ayrıntılar içermeyen, kasıtlı olarak oluşturulmuş “gürültü” içerecektir. Bu yöntemde veri kümesinin baskın eğilimleri veya özellikleri değişmeyecektir ve kişisel verilerin kapsamlı olarak korunması sağlanabilmektedir. (Ji, Lipton ve Elkan, 2014)

Veri koruma perspektifinden bakıldığında bu yöntemin kullanılması esnasında karşılaşılması muhtemel en büyük zorluk, gerçek cevaplara eklenecek uygun miktarda gürültü üretilmesi sonucu hem ilgili kişilerin mahremiyetini sağlayıp hem de paylaşılan cevapların kullanışlılığının korunmasıdır. Ayrıca veri tabanlarının bağlantılarının takip edilmesi ile sorgu sonuçlarının kombinasyonunun, gizli olması amaçlanan bilgilerin ifşa edilmesine yol açabilecek olması sebebiyle her sorgunun bağımsız olarak ele alınması önem taşımaktadır. (Madde 29 Çalışma Grubu, 05/2014 Görüşü)

8. **Homomorfik Şifreleme:** Homomorfik şifreleme, kullanıcıların şifrelenmiş verileri üzerinde şifresini çözmeye ihtiyaç duymadan işlem yapmasını sağlayan bir şifreleme türüdür. Homomorfik şifreleme ile mahremiyeti koruma odaklı dış kaynaklı depolama ve hesaplama işlemleri yapılabilmektedir. Bu durum, veri setinin kullanım olanaklarını sınırlamadan gizliliğin korunabileceği anlamını taşımaktadır.

Geleneksel bir şifreleme modelinde, veriler üzerinde değişiklik yapılmak istenirse bulut konumundan indirilmeli, şifresi çözülmeli, okunmalı veya düzenlenmeli, yeniden şifrelenmeli ve ardından yeniden yüklenmelidir. Dosyaların boyutları genişledikçe, bu görevler giderek daha külfetli hale gelebilmektedir ve veri setinin güvenliğini sağlamak zorlaşmaktadır.

Öte yandan, homomorfik olarak şifrelenen veriler, hala sunucudayken şifre çözülmesine gerek olmaksızın üzerlerinde sınırlı işlemler gerçekleştirilebilmektedir. Ardından, nihai olarak şifrelenmiş ürün, mesajın şifresini çözmek için anahtarını kullanan kullanıcıya gönderilir. Bu yöntem uçtan uca şifrelemeye benzemektedir, şifresi çözülen mesaja yalnızca alıcı erişebilir.

Örneğin, sağlık verileri gibi özel nitelikli kişisel veriler için mahremiyeti sağlamak amacıyla, veri paylaşımını engelleyen gizlilik engellerini kaldırarak veya mevcut hizmetlerin güvenliğini artırarak yeni hizmetleri etkinleştirmek için homomorfik şifreleme kullanılabilir. Bu kapsamda yapılan çalışmalarda, sağlık hizmetlerinde tahmine dayalı analitiğin tıbbi veri gizliliği endişeleri nedeniyle üçüncü taraf hizmet sağlayıcı aracılığıyla uygulanması sorun teşkil edebilmektedir. Ancak tahmine dayalı analitik hizmet sağlayıcısının gerçek veriler yerine şifreli veriler üzerinde çalışabilmesi durumunda, mahremiyete ilişkin endişeler azalabilmektedir. Ayrıca bu yaklaşım ile, hizmet sağlayıcının sisteminin ele geçirilmesi durumunda verilerin güvende kalması sağlanacak-

tır (Bos, Lauter ve Naeherig, 2014).

Konuya ilişkin mevcut gelişmeler takip edildiğinde, homomorfik şifrelemenin sınırlamaları görülmesi sebebiyle, bu şifrelemeyi kullanan sistemlerin düşük verimlilik oranında çalışacağı anlamına gelmektedir. Ek güvenlik yöntemlerine ihtiyaç duymayan birçok işletme için kullanımı maliyetli ve düşük verimli olmakla beraber, özel nitelikli veriler barındıran sektörler için bu yöntem oldukça kullanışlı olabilmektedir. Bu kapsamda çözümler geliştirilmesine yönelik aktif çalışmalar devam etmektedir.

9. **Transfer Öğrenme:** Öğrenme süreçlerinde her zaman modelleri sıfırdan geliştirmeye ihtiyaç duyulmamaktadır. Bir diğer yöntem olarak, benzer görevleri çözen mevcut modelleri kullanmaktır. Transfer öğrenme kullanılarak, bir makine öğrenimi modeli bir tür problem üzerinde eğitilir ve daha sonra yeni görevini öğrenirken zaten sahip olduğu bilgiden yararlanarak farklı ancak ilgili bir problem üzerinde kullanılır. İşleme faaliyetini bu mevcut modellere dayandırarak, aynı sonuca daha az veri ile ve daha kısa sürede ulaşmak çoğu zaman mümkün olmaktadır. Bu yöntemin kullanım süreçlerinde, önceden eğitilmiş modelleri içeren kütüphaneler kullanılmaktadır (Datatilsynet, 2022).

Pratik açıdan değerlendirildiğinde, yeni görevlerin öğrenilmesi için önceden öğrenilen görevlerden bilgilerin yeniden kullanılması veya aktarılması, pekiştirmeli öğrenme süreçlerinde verimliliği önemli ölçüde iyileştirme potansiyeline sahiptir (Karimpanal, Bouffanais ve Roland, 2019). Transfer öğrenme, ürün geliştiricilerin çok miktarda yeni veri ihtiyacını ortadan kaldırmasına olanak tanımaktadır. Etiketlenmiş eğitim verilerinin bulunduğu bir görev üzerinde önceden eğitilmiş bir model, çok daha az veri ile yeni ve benzer bir görevi gerçekleştirebilecektir. Ayrıca önceden eğitilmiş bir model kullanmak genellikle modelin yeni bir görevde eğitilmesi sürecini hızlandırır ve genel olarak daha doğru ve etkili bir ürünle sonuçlanabilmektedir.

Öte yandan, önemli karar verme uygulamalarında giderek daha fazla kullanılması sebebiyle, diğer küresel teknolojiler gibi derin öğrenme modelleri de, kötü niyetli kişilerin hedefi haline gelebilmektedir. Bu kapsamda, transfer öğrenme süreçlerinde taraflar arasında makine öğrenme süreçlerini hızlandırmak üzere paylaşılan veriler üzerinde değişiklik yapılmasının önlenmesi ve verilerin korunmasına ilişkin diferansiyel mahremiyet, homomorfik şifreleme gibi yöntemlerden destek alınması gerekmektedir.

10. **Blokzinciri:** Blokzinciri, verilerin bloklar halinde gruplanmasına dayanan, işlemleri güvenli, kurcalamaya karşı dayanıklı, dağıtık (yani merkezi bir otorite olmadan) ve verimli bir şekilde düşük maliyetle kaydeden merkeziyetsiz bir dijital hesap teknolojisidir (Tatar, Gökçe ve Nussbaum, 2020). Blokzincirinde yer alan her düğüm, ağın bir kullanıcısını temsil ederek veritabanının ayrılmaz bir kopyasını saklar ve veritabanını bağımsız olarak güncelleyebilir (EPRS, 2019).

Zincirde yer alan kullanıcı kimlikleri metin olarak, hash değeri tutularak veya takma adlandırma kullanılarak kaydedilebilmektedir. Dolayısıyla, metin verilerinin ilgili kişiler doğrudan belirlenebilmektedir. Hash fonksiyonlarının kullanımıyla da kişilerin tanımlanabilirliğine ilişkin çeşitli görüşler olmakla beraber; yaygın görüşte ilgili kişiyi doğrudan tanımlanın mümkün olmadığı ancak çıktıların kıyaslanarak gerçek kişiyle ilişkilendirilebilir olması nedeniyle, bu fonksiyonların takma adlandırılan veriler kategorisi altında bulunduğu kabul edilmektedir. (AEPD, 2019) Bu sebeple verilerin ilgili kişilerle ilişkilendirilebilir olmasıyla zincirde yer alan veriler, kişisel veri kategorisine girebilmektedir.

Blokzincirinde yer alan veriler merkezi olmayan bir şekilde toplanır, saklanır ve işlenir. Blok olarak kaydedildikten sonra işlemler kronolojik olarak sıralanarak değiştirilemez biçimde tutulmaktadır (Iansiti ve Lakhani, 2017). Gerçekleşen tüm işlemlerin takma adlandırılmış, sahipliğini doğrulanabilir ve sürdürülebilir bir şekilde kaydederek belgeleyip, onaylamaktadır. Bazı görüşlerce takma adlandırma veri güvenliği açısından bir güvenlik önlemi olarak sayılmaktadır. Ancak belirtmek lazım ki, blok zincirler, verilerin eklenebildiği, fakat yalnızca olağanüstü durumlarda kaldırılabildiği hesaplardır.

Blok zinciri, Bitcoin ve diğer kripto para birimlerinin altında yatan teknoloji olmakla beraber Yapay Zekâ teknolojisiyle bir arada kullanımı ile, sağlık, finans, tedarik gibi birçok alanda oldukça etkin bir güvenlik mekanizması sağlamak mümkündür. Örneğin sağlık sektöründe blokzinciri sayesinde oldukça kapsamlı ve çok miktarda verinin blokzinciri ile tutulması durumunda hastanın tedavisine ilişkin süreç birçok doktor tarafından takip edilebilecek, istenmesi durumunda izne tabi olarak doktorlar tarafından düzenlenebilecektir. Şifrelenmiş blokzinciri sayesinde aynı zamanda verilerin güvenliği de sağlanmış olacaktır. Bu zincirde yer alan kayıtlarının paylaşımının, düzenlenmesinin izne tabi olması ise kullanıcıların kişisel verilerinin ne kadarını paylaşacaklarına karar vermelerine olanak sağlamaktadır. Ayrıca, blokzinciri değiştirilemez yapısı gereği ilgili kişilere ilişkin bilgileri, kişilerin kararlarını

yansıtırken güvenilirlik ve şeffaflık sağlamaktadır.

Öte yandan blokzincir teknolojisi tarafından kullanılan merkezi olmayan veri yönetişim modeli ve verilerin işlenmesine dahil olan çok sayıda taraf bulunması nedeniyle, dağıtık yapısı gereği bu sistemlerde veri sorumlusunu tayin etmek güçleşmektedir. Bu çerçevede veri sorumlusu belirlenirken, zincire yazma hakkına sahip olan ve madencilerin doğrulaması için veri göndermeye karar veren katılımcıların veri sorumlusu olarak kabul edilebileceğini görüşü savunulmaktadır. (CNIL ,2018)

Bu teknolojinin kullanımıyla ortaya çıkan bir diğer problem ise; dağıtık defterlerin, yeni veriler eklendikçe sürekli büyüyen, yalnızca ekleme yapılan veri tabanları olmasıdır. Bu durum hem veri minimizasyonu ilkesine uymamakta hem de ilgili kişilerin verilerinin silinmesini veya unutulmasını talep etmeleri durumunda taleplerinin yerine getirilememesine sebep olmaktadır. (EPRS, 2019) Ayrıca bu teknolojinin yapısı gereği değiştirilemez olması sebebiyle zincire eklenen verilerin muhafaza süresi kısıtlanamamaktadır. Bu durum da süresiz olarak verilerin muhafazası durumuyla karşı karşıya kalınabilmektedir.

11. **Açıklanabilir Makine Öğrenimi:** Açıklanabilir Makine Öğrenimi alınan tüm otomatik kararların açıklanabilir olması gerektiği fikrine dayanmaktadır. Böylece şeffaflık ve hesap verebilirlik sağlanmaya çalışılmaktadır. Ayrıca bu öğrenme ile yapay zekâ destekli sistemleri kullanıcılara, zihinsel modelleri geliştirerek ve kavram yanılgılarını ortadan kaldırarak, daha etkili performans sunmayı hedeflemektedir (Alizadeh, 2021).

    Konuya ilişkin P. Jonathon Phillips vd. tarafından "Açıklanabilir Yapay Zekânın Dört İlkesi Raporu"nda, insan-makine etkileşiminin araştırılabilmesi ve kullanıcıların sistem hakkında daha kapsamlı bilgiye sahip olmasının sağlanması ile daha güvenli bir ortam yaratılması adına 4 temel ilke tanımlamıştır. Bu ilkeler:

    - Sistemler, tüm çıktılar için kanıt veya sebep(ler) sunarak açıklama üretmeli,
    - Sistemler, kullanıcılar için anlaşılabilir açıklamalar sağlamalı,
    - Açıklama, sistemin çıktı üretme sürecini doğru bir şekilde yansıtmalı,
    - Sistemin yalnızca tasarlandığı koşullar altında veya sistem çıktısında yeterli güvene ulaştığında çalışması ile bilgi sınırları tanımlanmalı.

Açıklanabilir Makine Öğrenimi kullanımında amaç, kararlarını anlaşılır bir şekilde açıklayabilen, YZ eylemlerinin dayandığı bilgileri ortaya koyabilen ve sistemi kullanma konusunda güveni artıran bir yapay zekâ yaratmaktır. (Rieg,Frick, Baumgartl ve Buettner, 2020) Bu özellikler mevcut bilgiyi doğrulamayı, mevcut bilgiyi sorgulamayı ve yeni varsayımlar üretmeyi mümkün kılmaktadır. Bu yaklaşıma yüksek doğruluk payının ve geri bildirimin önem taşıdığı savunma, sağlık ve hukuk gibi alanlarda daha belirgin ihtiyaç duyulmaktadır.

Bu kapsamda önlemlerin YZ teknolojileri geliştiricileri, veri sorumluları ve/veya dağıtım sürecinde yer alan taraflarca değerlendirilerek ihtiyaç duyulduğu durumlarda birbirlerini destekleyecek bir biçimde bir arada uygulanması önerilmektedir.

SONUÇ

Yapay Zekâ sistemlerinin kullanıldığı süreçlerin bütüncül olarak ele alınması gerekmektedir. Yenilikler meydana gelirken kişisel verilen korunmasına ilişkin hukuki düzenlemelerin de bu teknolojinin dinamizmine ayak uyduracak bir biçimde gerçekleştirilmesi elzemdir. Bu açıdan Yapay Zekâ teknolojilerinin geliştirilmesinde temel hedef bireylere hizmet etmesi olmakla beraber, yeniliklerin kişilerin temel hak ve özgürlükleri çerçevesinde kişisel verilerin korunmasını isteme hakkı açısından yönetilmesi gerekmektedir. (Baldwin, Cave ve Lodge, 2011) Bu sebeple hukuki düzenlemelerin; şeffaf, etkin, teknolojik gelişmelerin artışını destekleyici, gelişmeleri kapsayacak ve çeşitli alanları düzenleyebilecek şekilde esnek, meşru ve yeterli olması gerekmektedir. Aynı şekilde kişisel verilerin veri sorumluları tarafından çeşitli teknik ve idari tedbirler ile korunması, adil bir şekilde kullanılması, kişiler için haksız veya olumsuz etkiler oluşturmayacak biçimde işlenmesi önemlidir. Bu kapsamda Yapay Zekâ Uygulamalarına yönelik çalışmalar gerçekleştirilirken mevcut yasal düzenlemeler takip edilerek, onlara uyum sağlanarak rol ve sorumlulukların belirlenmesi önem arz etmektedir.

Ancak vurgulamak gerekir ki güvenli yapay zekâ kullanım süreçleri için tüm paydaşlara görevler düşmektedir.

» Yapay zekâ sistemlerini araştıran, tasarlayan ve/veya geliştiren ürün geliştiricileri ve üreticiler teknolojiyle uyumlu, dinamik, yeterli teknik ve idari önlemleri almalıdır. YZ sistemlerinin çok çeşitli olmaları gereği tasarım aşamasından itibaren şeffaf, açıklanabilir ve denetlenebilir olması gerekmektedir.

» Ürün ve hizmetleri kullanan kuruluşlar olan dağıtıcılar, kullandıkları sistemlerin ve sundukları ürün ve hizmetlerin gereksinimleri karşılamasını sağlamalıdır.

» YZ sistemlerini kullanan, sistemlerden doğrudan veya dolaylı olarak etkilenen ve karar verme aşamasında beklenen davranışı göstermesini sağlaması için talimat veren kullanıcılar taraflarınca alınabilecek önlemler hakkında farkındalığa sahip olmalı, gereklilikler hakkında bilgilendirilmeli ve bunların yerine getirilmesini talep edebilmelidir. ◆

KAYNAKÇA

◊ AEPD. (2019) Introduction To The Hash Functıon As A Personal Data Pseudonymisation Technique. https://edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf adresinden 18.08.2022 tarihinde alınmıştır

◊ Akyol, A. (2021). Yapay Zekânın Cezai Sorumluluğu. Editörler. Balcı, M. ve Aydın, H. (Ed.), s.174. Ankara.

◊ Alizadeh,F.(2021). I Don't Know, Is AI Also Used in Airbags?: An Empirical Study of Folk Concepts and People's Expectations of Current and Future Artificial Intelligence, https://doi:10.1515/icom-2021-0009

◊ Article 29 Data Protection Workıng Party. (2014). Opinion 05/2014 on Anonymisation Techniques,. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf adresinden alınmıştır.

◊ Baldwin, R., Cave, M., Lodge, M. (2011). Best Practices Setting Targets and Detecting Vulnerabilities, Policy Quarterly. 3(3), s. 26-31.

◊ Bos, J.W., Lauter K. ve Naehrig M. (2014). Private Predictive Analysis On Encrypted Medical Data. Journal of Biomedical Informatics 50, s. 234-243.

◊ Cavoukian, A. (2011). Privacy by Design The 7 Foundational Principles. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf adresinden alınmıştır.

◊ CNIL. (2018). Solutions for a responsible use of the blockchain in the context of personal data. https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf adresinde 18.02.2022 tarihinde erişim gerçekleştirilmiştir.

◊ CoE. (2019). A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework.https://rm.coe.int/responsability-and-ai-en/168097d9c5 adresinden alınmıştır.

◊ Datatilsynet. (2018). Artificial Intelligence And Privacy., ss.27, https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf adresinden 24.04.2022 tarihinde alınmıştır.

◊ European Parliament Legislative Observatory. (2015/2103(INL). Civil Laws for Robotics. https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1473044&l=en&t=D adresinden alınmıştır.

◊ EPRS | European Parliamentary Research Service. (2019). Blockchain and the General Data Protection Regulation. Panel for the Future of Science and Technology . https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445 adresinden alınmıştır.

◊ Erdoğan, Ö. Yapay Zekânın Cezai Sorumluluğu. Editörler. Balcı, M. ve Aydın, H. (Ed.), s.133. Ankara.

◊ Goodfellow, I.J. ve ark. (2014). Generative Adversarial Nets.

◊ Hoffmann-Riem, W. (2019). Artificial Intelligence as a Challenge for Law and Regulation, Regulating Artificial Intelligence, s.11

◊ Iansıtı M., Karim R. L. (2017).The Truth About Blockchain. Harvard Business Review. https://hbr.org/2017/01/the-truth-about-blockchain adresinden 17.08.2022 tarihinde erişilmiştir.

◊ Karimpanal, G., Thommen- Bouffanais, R.(2019) Self-organizing maps for storage and transfer of knowledge in reinforcement learning. Adaptive Behavior, 27 (2), s. 111–126.

◊ Kişisel Verileri Koruma Kurumu. (2021). Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf adresinden alınmıştır.

◊ Tatar, Ü., Gokce, Y. Ve Nussbaum, B. (2020) Law versus technology: Blockchain, GDPR, and tough tradeoffs. Computer Law & Security Review, 38, s.1-11.

◊ Rieg, T. ve ark. (2020). Demonstration of the potential of white-box machine learning approaches to gain insights from cardiovascular disease electrocardiograms.

◊ OVIC. (2019). Closer To The Machine. https://ovic.vic.gov.au/wp-content/uploads/2019/08/closer-to-the-machine-web.pdf adresinden 10.04.2022 tarihinde alınmıştır.

NESNELERİN İNTERNETİ (IOT) UYGULAMALARINDA KİŞİSEL VERİ GÜVENLİĞİ VE MAHREMİYET

Büşra YILMAZ

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "IoT (Nesnelerin İnterneti) Uygulamalarında Kişisel Veri Güvenliği ve Mahremiyetin Korunması" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Teknolojik gelişmelerle iletişim hep daha kolay, pratik ve hızlı hale getirilmeye çalışılmıştır. Endüstri 4.0 olarak bilinen Sanayi Devrimiyle birlikte artık nesneler arasındaki iletişim de gündeme gelmiş olup "Nesnelerin İnterneti (internet of things/IoT)" kavramı ortaya çıkmıştır.

Nesnelerin interneti için birçok tanım yapılmış olup aslında temelde fiziksel obje ve nesnelerden oluşan bir ağ olarak ifade edilebilir. Bu ağı oluşturan nesneler ise; bilgi toplayan sensörler, verinin kaynağını tanımlayan tanımlayıcılar, verileri analiz etmek için yazılım ve iletişim sağlanması, bilgilendirme/uyarı yapılması için internet bağlantısı ile güçlendirilmiştir (Rayes ve Salam, 2022). Nesnelerin interneti kavramı ilk kez Kevin Ashton tarafından 1999 yılında kullanılmış ve bu yeni teknolojiyle tedarik zincirinde RFID (Radio Frequency Identification/Radyo Frekansıyla Tanımlama) etiketlerinin ve sensörlerinin ürünler üzerinde kullanılması amaçlanmıştır. IoT günümüzde sadece sanayi için değil insanların günlük yaşantısında da kullanılmakta olan bir teknoloji haline gelmiştir.

İnternet, sadece bilgisayarlardan oluşan bir ağ olmayıp artık bilgisayarların yanında her boyuttan ve her türden cihazdan oluşan bir ağ olarak evrilmiştir. Günümüzde internet ağı, nesnelerin internetiyle birlikte bilgisayar, akıllı telefon, tablet, kameralar, binalar, ev aletleri, endüstriyel sistemler, araçlar, tıbbi cihazlar ve giyilebilir teknolojiler gibi çeşitli bileşenlerden oluşmaktadır. Bu kapsamda IoT teknolojileri tarımdan sağlık sektörüne, akıllı binalardan akıllı şehirlere, enerjiden endüstriye gibi uygulama alanı bakımından geniş bir yelpazeye sahiptir.

IoT sistemlerinin insanların günlük yaşantısına girmesiyle ve kişisel amaçlarla kullanımlarının artmasıyla birlikte bu sistemler ile toplanan verilerin miktarı ve çeşitleri de günden güne artmaktadır. IoT cihazlarının ve sensörlerinin kendi çevrelerinden topladığı verilerin ise kişisel veri içermesi oldukça kaçınılmaz bir duruma gelmiştir. Özellikle, giyilebilir teknolojilerin kullanılması hassas ve ayrımcılığa sebebiyet verebilecek verilerin, sağlık bilgisine, uyku düzenine, gerçekleştirilen spor ve egzersiz aktivitelerine ilişkin verilerin toplanması anlamına gelirken, günlük hayatta kullanılan akıllı ev aletleri ve akıllı araçlar ile kişinin rutinine, alışkanlıklarına, davranışlarına ve sık gittiği yerlere ilişkin kişisel verilerin toplanması ve işlenmesi anlamına gelmektedir. Akıllı şehirlerde kullanılabilen gürültü ölçer, güvenlik kamerası vb. gibi IoT cihazları ile ilgili kişinin görüntüsü ve/veya sesi de işlenebilmektedir.

IoT teknolojileriyle bireylerin kişisel verileri ile mahremiyetlerine ilişkin veriler toplanabilmektedir. Çok sayıda ve çok çeşitte gerçek zamanlı olarak toplanan bu veriler ile de büyük veri olarak ifade ettiğimiz devasa boyuttaki veriler elde edilmektedir. Bilindiği üzere içerisinde kişisel verilerin de bulunduğu söz konusu veriler IoT cihazları ve sistemleri üzerinden işlenerek siber dünyaya dahil olmaktadır. Siber teknolojiler her zaman getirmiş olduğu yeniliklerin yanında siber tehditleri de beraberinde getirmektedir. Bu noktada, IoT sistemleri ve teknolojileri için de siber tehditlerin varlığı söz konusudur. IoT siber tehditleri nedeniyle bireylere ait kişisel verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin ihlal edilmesi riski bulunmaktadır. Kişisel veriler üzerinde risk oluşturan unsurlar da kullanılan sistem, uygulama ve cihaz vb. üzerindeki açıklık ve zafiyetler olarak detaylandırılabilir. Mahremiyetin ihlaline sebebiyet veren hususlar ise temel olarak profilleme yapılması, kimliğin belirlenmesi, izleme ve konum bazlı takip gerçekleştirilmesi, veriler arasında bağlantı kurulması, yaşam döngüsü geçişleri ve envanter saldırıları şeklinde sıralanabilir.

Bilindiği üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında veri sorumlularının kişisel veri güvenliğinin sağlanmasına yönelik yükümlülüğü bulunmaktadır. Bu sebeple, IoT uygulamalarında kişisel veri güvenliğinin sağlanabilmesi için veri sorumlularının ve veri işleyenlerin işleme faaliyeti gerçekleştirdikleri veriler üzerinde kontrolü sağlamaları ve gerekli teknik ve idari tedbirleri almaları gerekmektedir.

NESNELERİN İNTERNETİ KAVRAMI

"Nesnelerin interneti" kavramına ait tek bir tanım bulunmamaktadır. İngilizce dilinde "Internet of Things (IoT)" olarak geçen kavram "internet" ve nesneler/şeyler anlamına gelen "things" kelimelerinden oluşmaktadır. Nesnelerin interneti; her türlü nesnenin ve cihazın kablolu veya kablosuz internet üzerinden bağlı olduğu bir sistem olarak tanımlanabilir (Tawalbeh, Muheidat, Tawalbeh ve Quwaider, 2020). Ortaya çıkan bu yeni teknolojiyle internete bağlanan nesnelerin başlangıç olarak üretimde kullanılması amaçlansa da IoT, artık insanların günlük hayatında pek çok yerde kullandığı bir teknoloji haline gelmiştir.

Nesnelerin interneti; insanların farklı bilgisayar türleriyle, giyilebilir teknolojik ürünlerle, akıllı hale getirilmiş sistemlerle internete bağlandığı, buna ek olarak nesnelerin de internete bağlanıp nesnelerin birbirleriyle, insanlarla, insanların kullandığı sistemlerle veri paylaşımı yapabildiği bir sistemdir (Yıldız, 2020).

Nesnelerin interneti, birbirleriyle ve başka sistemlerle iletişime geçebilen nesnelerden oluşan ağda karşılıklı veri paylaşımının yapılabildiği ve akıllı bir şekilde davranış gösteren bir sistem olarak tanımlanabilir. Bu tanım biraz daha açılırsa; otomatik düzenleme, bilgi, veri ve kaynaklarını paylaşabilme, ortaya çıkan yeni durumlar, olaylar ve ortamdaki değişimler karşısında uygun şekilde tepki verme ve hareket edebilme kapasitesine sahip açık ve kapsamlı bir akıllı nesne ağı olarak ifade edilebilir (Madakam, Ramaswamy ve Tripathi, 2015).

2023 yılı Ekim ayı itibariyle dünya çapındaki aktif internet kullanıcı sayısı bir yıl öncesine göre yaklaşık %3.7 artarak 5.30 milyara ulaşmıştır. (DataReportal, 2023). Bu sayı her geçen gün artarak yeni kullanıcılar internete dâhil olmaktadır. İnternetin başta iletişim olmak üzere çeşitli alanlarda kullanımının artmasıyla birlikte nesnelerin internetinin hem popülerliği büyümekte hem de kullanım oranı da artmaktadır. Enerji yönetimi, sağlık, trafik yönetimi, ev aletleri ve uygulamaları, üretim, lojistik vb. gibi birçok alanda uygulama bulan nesnelerin interneti günümüz dünyasının kaçınılmaz teknolojisi haline gelmiştir.

Nesnelerin İnterneti Uygulama Alanları

Nesnelerin interneti, her şeyi her yerde ve her an kontrol edebildiğimiz ve her

şeyi birbirine bağlayabildiğimiz yeni bir paradigmadır (Sundareswaran, Mahesh, Rajesh ve Salmon, 2018). Bu kapsamda, nesnelerin interneti teknolojisi uygulama alanı bakımından giderek hayatımızda daha da geniş bir yer edinmektedir. Akıllı şehir uygulamaları, akıllı ev uygulamaları, güvenlik uygulamaları, taşımacılık uygulamaları, sağlık uygulamaları, günlük kullanıma yönelik uygulamalar, enerji sektörüne yönelik uygulamalar, ticaret ve imalat uygulamaları gibi çeşitli alanlarda nesnelerin interneti teknolojisiyle karşılaşabilmek mümkündür.

IOT TEKNOLOJİLERİNİN GÜNÜMÜZDEKİ YERİ, ÖNEMİ VE GELECEĞİ

Ashton (2009), bilgisayarların; veriler için insana ihtiyaç duymadan veri elde edebilmesi durumunda tıpkı internetin dünyada meydana getirdiği değişim gibi IoT teknolojisinin de birçok değişim meydana getireceğini düşünmektedir. Bu değişimler, artık insanların günlük yaşantılarına yansımaktadır. IoT teknolojilerindeki gelişmelerle birlikte özellikle evlerimizde ve iş yerlerimizde akıllı cihaz kullanımı artmış ve günlük yaşama bu cihazlar dahil olmuştur ve olmaya da devam etmektedir.

Aktif olarak internet kullananların sayısı giderek artmakta ve buna bağlı olarak da nesnelerin internetinin yaygınlaşmasında gelişme yaşanmaktadır. Elektronik cihazlar, taşıtlar, günlük ve iş hayatımızda kullandığımız aletler ve araçların da internete bağlanmasıyla mevcut nesnelerin interneti popülasyonu da artacaktır. İlerleyen zamanda internete bağlanan ve her bir cihazın kendi verisini ürettiği daha fazla sayıda akıllı cihaz ve elektrikli alet hayatımızda yer edinecek olup söz konusu cihazlarda devamlı olarak fazla miktarda veri iletilip toplanacaktır (Alkan, Menteş ve İnceefe, 2021). 2021 yılı için 10 milyardan fazla IoT cihazının bulunduğu, bu sayının da 2030 yılında 25.4 milyarı aşacağı tahmin edilmektedir (Jovanovic, 2023).

Günümüzde artık nesnelerin internetinin kullanımına yönelik örneklerin yansımalarını daha fazla görmekteyiz. Örneğin, Güney Kore'de deniz doldurularak yapılan Songdo yeni yerleşimli bir kent olup bu kent baştan itibaren akıllı olacak şekilde geliştirilmiştir. 2009'da oturuma açılan Songdo şehri, akıllı şehirler için ön koşul olarak kabul edilebilen nesnelerin interneti teknolojisini tam destekleyen bir altyapıyla karşımıza çıkmaktadır. Apartmanlar, kamu tesisleri, endüstriyel binalar, kamuya dair her türlü nesnenin ortak bir ağa entegre edildiği ve şehirde yaşayanların anlık olarak bu sistemler üzerinden veri ürettiği bir yaşam alanı ortaya çıkmıştır (Karma, 2021). Şehirdeki evlere yerleştirilen sensörler sayesinde tüketilen enerji miktarı hakkında bilgi alınabilmektedir. Bununla birlikte vatandaşlara ısıtma, aydınlatma gibi işlemlerde enerji tasarrufuna yönelik tavsiyeler

mobil uygulamalar üzerinden verilebilmektedir. Sıcaklığın kontrol edilmesi, elektronik cihazların kapatılıp açılması gibi eylemlerin uzaktan telefon ile tek bir dokunuşla yapılması mümkündür.

Bir diğer akıllı şehir örneği İspanya'da bulunan Santander şehridir. Avrupa'nın sensör başkenti unvanını 20.000 sensör ile kazanan bu şehirde sokak aydınlatmaları, enerji sistemleri, çöp konteynerleri, otobüs vb. toplu taşıtlar gibi çeşitli nesneler sensörlerle donatılmıştır (Yıldız, 2020).

Günlük hayatta kullanılan çeşitli giyilebilir cihazlar da aslında birer IoT cihazıdır. Giyilebilir cihazlara; akıllı bileklik, akıllı saat, akıllı gözlük gibi teknolojiler örnek verilebilir. Bu cihazlarla insan vücudu üzerinden anlık olarak veri toplanmakta ve verilerin analiz edilmesiyle cihazların kullanım amacına göre veriler işlenmektedir. Örneğin, ebeveynler tarafından güvenlik için çocuklarının konum takibinin yapılması amacıyla bileklik şeklindeki GPS takip cihazları kullanılmaktadır. Kandaki nikotin miktarını ölçerek fitnes izleyici özelliğe sahip olan giyilebilir teknolojiler ile gün içerisinde ne kadar koşulduğu, yüründüğü ve uyunduğu, kalp atış hızı, stres seviyesi gibi çeşitli veriler toplanmaktadır. Bu veriler sensörler sayesinde bir mobil uygulamada toplanarak analiz edilebilir. Yapılan analizlere göre kullanıcıyı yönlendirebilir ya da kullanıcının belirlemiş olduğu otomasyon sistemini harekete geçirilebilir. Bir doğa yürüyüşçüsünün akıllı saat kullanmasıyla hayatta kaldığı olay bu otomasyona örnek verilebilir. Doğa yürüyüşçüsünün sert bir şekilde düşmesiyle akıllı saati acil yardım numarasını aramasıyla düştüğü yerden kurtulmuştur. Aramadan önce kullanıcının onayını isteyen akıllı saat, eğer kullanıcı bir dakika içerisinde hareketsiz kalırsa otomatik olarak aramaktadır.

Akıllı mağazalarda insanların ürünleri sepetlerine koymalarıyla birlikte bu ürünlerin fiyatları otomatik olarak kendi telefonlarıyla entegre edilen hesaplarından düşürülmesiyle insanlar kolay, hızlı bir şekilde kasa sırası beklemeden alışveriş yapabileceklerdir.

Akıllı ulaşımı sağlamak adına nesnelerin interneti, trafik yoğunluğunun tespit edilmesine, yol güvenliği durumunun takip edilmesine, kaza tespit eden sistemlere ve otomatik ücret ödeme sistemlerine çözüm olarak kullanılmaktadır.

Teknolojinin gelişmesiyle birlikte nesnelerin internetinin kullanım alanı giderek çeşitlenmektedir. IoT teknolojisi, günlük basit işlerden kritik alanlara kadar oldukça geniş bir yelpazede kullanılabilmekte olup geleceğin önem arz eden kaçınılmaz teknolojilerinden biri haline gelmiştir.

IOT GÜVENLİĞİNİN KİŞİSEL VERİ GÜVENLİĞİ VE MAHREMİYET AÇISINDAN ÖNEMİ

Siber tehditlerin giderek arttığı süreçte IoT kullanıcılarının mahremiyeti ile kişisel verilerinin hem de IoT cihazlarının güvenliğini sağlamak için IoT sistemlerinin güvenliğinin önemi de artmaktadır. Bu noktada güvenliğe yönelik tedbirler hem teknik olarak hem de idari olarak alınması gerekmektedir.

Nesnelerin interneti sistemlerinde veri akışı oldukça fazladır. Veri akışına dahil olan veriler, ilgili kişiler hakkında mahrem ve hassas bilgilerin de dahil olduğu kişisel verileri barındırabilmektedir. Bu sebeple, veri akışındaki verilerin bütünlüğünün korunması, gizliliğinin sağlanması ve erişilebilirliğinin korunması amacıyla IoT siber güvenliği sağlanmalıdır. IoT siber güvenliğinin amacı IoT bileşenlerinin ve mahremiyetin korunarak kuruluşlar ve kullanıcılar için siber güvenlik riskini azaltmaktır (Lee, 2020).

IoT uygulamalarında güvenliğin sağlanamaması sonucu ilgili kişilerin mahremiyetleri ve kişisel verileri ihlale uğrayabilmektedir. Bu noktada, ihlaller sebebiyle ilgili kişiler üzerinde maddi ve/veya manevi olmak üzere olumsuz sonuçlarla karşılaşılabilmektedir. Söz konusu yaşanan veri ihlalleriyle de ilgili kişilerin veri sorumlularına duymuş olduğu güven sarsılmakta ve veri sorumlularının itibarı zedelenmekte olup uzun vadede veri sorumluları için de kişisel veri ihlalleri olumsuz sonuçlar oluşturmaktadır. Bu sebeple 6698 sayılı Kanun kapsamındaki veri güvenliğinin sağlanmasına yönelik yükümlülüklerin yerine getirilmesi noktasında hassas davranılması oldukça önemlidir.

2016 yılında Mirai olarak bilinen saldırı ile IoT cihazları hedeflenmiştir. Global olarak gerçekleştirilen DDoS saldırısından aralarında ülkemizin de bulunduğu birçok ülke etkilenmiş olup bu ülkelerin etkilenen cihaz sayısına göre sırayla Tayvan, Vietnam, Çin, Brezilya, Türkiye, Rusya ve Hindistan olduğu belirtilmiştir (Holub, 2020).

Yakın geçmişte yaşanan bir başka siber saldırıda, ilgili IoT cihazında güvenlik sağlanamadığından ilgili kişilerin olumsuz sonuçlarla karşılaşmasına neden olunmuştur. Bu kapsamda, IoT ev güvenlik cihazlarından biri olan akıllı kameraya siber saldırı gerçekleştirilmiştir. Ev içerisinde ebeveynler tarafından küçük çocukların kontrol edilmesi, kapı zillerinde güvenlik sağlanması amacıyla kullanılan akıllı kameralar ile siber saldırganlar insanların mahremiyetlerine müdahil olmuşlardır. The Guardian (Paul, 2020) tarafından yapılan habere göre siber saldırı kapsamında kameradaki karşılıklı konuşma özelliği aracılığıyla; çocuk odasında korku müziği çalınması, oturma odasında izlenen televizyon programına yorum yapılması, insanların tehdit ve taciz edilmesi gibi birçok olay yaşandığı, bu kapsamda davalar açıldığı ifade edilmektedir. Veri sorumlusu, bu tür ihlalleri önlemek adına kullanıcılara güçlü parola ve çift faktörlü kimlik doğrulaması kullanılmasını önermiştir. Bununla birlikte, Şirket tarafından da açıklıkların kapatılmasına yönelik tedbirler alındığı belirtilmiştir.

Akıllı kamera ve kapı zillerine ilişkin yaşanan olaylardan da anlaşılacağı üzere nesnelerin interneti uygulamalarında kişisel veri güvenliğinin sağlanması ve mahremiyetin korunması adına IoT güvenliğinin sağlanması gerekmektedir. IoT güvenliği sağlanırken tedbirlerin tek taraflı olarak değil; kullanıcılar, veri sorumluları ve veri işleyenler ile diğer IoT paydaşları tarafından da alınması gerekmektedir.

IOT UYGULAMALARINDA VERİ GÜVENLİĞİNİN SAĞLANMASI VE MAHREMİYETİN KORUNMASI

6698 sayılı Kanun kapsamında veri sorumlularının birtakım yükümlülükleri yerine getirmesi gerekmektedir. Bu yükümlülüklerden veri güvenliğine ilişkin yükümlülükler Kanunun 12 nci maddesinde düzenlenmiştir. Buna göre veri sorumlusu;

a. Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
b. Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
c. Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. IoT uygulamaları kapsamında da kişisel veri işleme faaliyetleri gerçekleştirildiğinden veri sorumluları tarafından veri güvenliğine ilişkin yükümlülüklerin yerine getirilmesi gerekmektedir.

Veri Mülkiyeti ve Veri Koruma Yükümlülüğü Açısından Veri Sorumlusu - Veri İşleyen İlişkisi

Kişisel verilerin korunmasına yönelik ulusal ve uluslararası mevzuatlarda veri sorumlusuna ve veri işleyene hükmedilen yükümlülüklerde farklılıklar bulunabilmektedir. Nesnelerin interneti teknolojisi; sensörler, çeşitli araçlar ve protokoller, bluetooth, kablosuz, uydu ve hücresel gibi farklı iletişim teknolojileri ile heterojen yapıya sahip olup IoT sistemlerindeki her bir cihazın amaç ve güvenlik açısından farklı gereksinimleri vardır. Bu gereksinimlerin kimler, yani hangi aktörler tara-

findan ele alınacağı ise belirsizlik oluşturmaktadır.

Siber dünyanın tehlikelerle dolu olduğu dikkate alındığında IoT sistemleri için de gerekli önlemlerin alınması ve siber güvenliğin sağlanması gerekmektedir. Özellikle günümüzde kişisel verilerin korunması daha fazla önem arz etmeye başlayan bir konu olup IoT sistemlerinde de özel nitelikli kişisel veriler de dahil olmak üzere pek çok kişisel veri türü işlenmektedir. Söz konusu veri işleme faaliyetleri ilgili ülkelerin kişisel verilerin korunması mevzuatlarına uygun şekilde gerçekleştirilmelidir.

Eğer IoT sistemlerine yönelik gerekli tedbirler alınmazsa siber saldırganlar tarafından nesnelerin zafiyetleri ve açıklıkları sömürülerek bu durumdan faydalanılabilir. IoT sistemindeki verilere erişen saldırganlar verilerde çarpıtma ve değişiklik yapabileceği gibi küresel IoT ağı üzerinden sistemleri bozabilecektir (Lu ve Xu 2019). Ayrıca hem ilgili kişiler hem de kuruluşlar açısından itibar kaybı ve mali kayıp olabileceği gibi ilgili kişilere ait kişisel verilerin, günlük yaşantılarına dair alışkanlıkların ve mahremiyetin ifşa edilmesi söz konusu olabilir. Bu kapsamda, veri sorumluları tarafından kişisel veri güvenliğinin sağlanması adına gerekli tedbirler alınmalıdır. Ancak, birden fazla sayıda aktör IoT sistemini oluşturan parçaların üretim ve geliştirme sürecine dahil olmaktadır. Bununla birlikte, veri mülkiyeti/sahipliği veri sorumlusunda olabileceği gibi veri sorumlusu tarafından veriye sahip olunması şart değildir (Wright, 2019). Veri sorumlusu veri işleyen arasında bir sözleşme ile ilgili faaliyetler yürütülebilmektedir. Article 29 Data Protection Working Party - Madde 29 Çalışma Grubu'nun IoT alanındaki gelişmelere ilişkin görüşünde (2014a) IoT sistemlerindeki söz konusu aktörleri cihaz üreticileri, sosyal platformlar, üçüncü taraf uygulamalar, IoT cihazını ödünç verenler veya kiralayanlar, veri komisyoncuları (data brokers) veya veri platformları şeklinde sınıflandırmıştır. Bu kapsamda örneğin; bir şirket tarafından tasarımı yapılan IoT cihazının, başka bir şirket tarafından üretimi yapılabilmekte, yazılım desteği sağlanabilmekte, bir başka şirket tarafından da cihazın dahil olduğu ağ işletilebilmekte ve bir başka şirket tarafından da cihaz dağıtımının yapılabildiği bir süreç dikkate alındığında güvenliğe ilişkin alınacak kararların kimin sorumluluğunda olacağı (Restuccia, D'Oro, ve Melodia, 2018) ve veri sorumlusu-veri işleyen rollerinin kime veya kimlere ait olduğu belirsizlik içerisindedir.

Bu sebeple, IoT uygulamalarındaki karmaşık paydaş ağı, paydaşların IoT sistemlerine dahil oldukları ölçütte kişisel verilerin işlenmesine yönelik yasal yükümlülüklerin hassas bir şekilde dağıtılmasını gerektirmektedir (Article 29 Data Protection Working Party, 2014a).

IoT Uygulamaları ve Tehditler

Teknolojik gelişmelerin amacı insanlığa hizmet ederek insan hayatını daha kolay ve pratik hale getirerek yaşam kalitesini artırmak olarak ifade edilebilir. Günden güne teknoloji alanında yapay zekâ, makine öğrenmesi, büyük veri, artırılmış ve sanal gerçeklik, blokzincir gibi birçok gelişme ve inovasyonlara şahit olmaktayız. Nesnelerin interneti de insan hayatına büyük bir ivme ile giren teknolojilerden biridir. Günümüzde akıllı şehirler gibi kompleks IoT uygulamalarına çok yaygın olarak rastlanmasa da IoT cihazlarının sayısının 2030 yılına kadar 25.4 milyara ulaşacağı tahminleri göz önüne alındığında gelecekte akıllı şehirler gibi daha büyük çapta olan IoT uygulamaları daha fazla hayat bulacaktır.

Teknoloji alanındaki gelişmeler birbirlerini desteklemekte ve birbirlerinin gelişmelerini tetiklemektedir. Özellikle büyük veri, yapay zekâ gibi unsurlarla nesnelerin interneti arasında ayrılmaz bir bağ bulunmaktadır. Büyük veri ile yapay zekâ arasındaki iki yönlü ilişki aynı şekilde hem yapay zekâ ve nesnelerin interneti (Dülger, 2019), hem de büyük veri ve nesnelerin interneti arasında mevcuttur.

Nesnelerin interneti uygulamaları; çeşitli nesnelerin çevresinden toplamış olduğu birtakım verileri istenilen bir zamanda istenilen yere bir ağ üzerinden iletmesi olarak tanımlanabilir. Bir diğer ifadeyle, IoT teknolojisi, cihazların birbirleriyle iletişime geçerek öngörülen veya yapılması gereken işleri yapmasıdır (Ülker, Canbay ve Sağıroğlu, 2017). Bu kapsamda, IoT sistemindeki nesnelerin akıllı olması gerekmekte ve nesneler, birbirleriyle koordineli şekilde çalışma özelliğine sahip olmalıdır.

Uygulama alanı açısından nesnelerin interneti ilk olarak endüstri alanında kullanılması amacıyla ortaya çıkmıştır. Ancak, endüstri ve üretim amacının yanında enerji, tarım, akıllı ev ve binalar, akıllı şehirler, giyilebilir teknolojiler ve lojistik gibi oldukça geniş bir yelpazede uygulama bulmaktadır. Yakın geçmişte yaşamış olduğumuz ve az da olsa etkileri devam eden Covid-19 salgınıyla birlikte uzaktan erişim sağlama ve komut verme gibi temassız ve sosyalliği azaltan eylemlerin ve hizmetlerin önemi artmıştır. Özellikle sağlığın daha çok gündemde olduğu bu süreçte giyilebilir teknolojiler daha çok tercih edilmektedir. Giyilebilir teknolojiler olarak akıllı saat, bileklik vb. gibi çeşitli cihazlarla kalp atış hızı, glikoz miktarı, kandaki oksijen miktarı ölçülebilmektedir. Anlık olarak vital değerleri ölçen bu akıllı cihazlar tarafından toplanan veriler bir telefondaki uygulama ile takip edilebilmektedir. Hastanın vital değerlerinde herhangi bir sorun olması durumunda telefon üzerinden ilgili sağlık kuruluşuna alarm verilebilir. Sağlık kuruluşu da gerekli görmesi halinde ambulans gibi acil yardım hizmet çağrısı

yapabilecektir. Bu derecede kritik veriler üzerinden de hizmet veren IoT uygulamalarının önemi giderek artmaktadır. Ancak bununla birlikte, IoT cihazlarının bir ağ ortamında var olması güvenlik açısından riskleri de getirmektedir (Ülker, Canbay ve Sağıroğlu, 2017). Bu cihazlar üzerinden menfaat elde etmek ya da bireylere ya da kuruluşlara zarar vermek isteyen üçüncü kişiler tarafından IoT uygulamalarındaki ve cihazlarındaki açıklıkları kullanma, kurcalama vb. tehditler ile verilere erişilmesi, elde edilmesi, ifşa edilmesi veya erişiminin engellenmesi söz konusudur. Kısaca gerçekleştirilen saldırılar verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin ihlal edilmesiyle sonuçlanabilmektedir.

IoT uygulamalarına yönelik birçok tehdit aktörü bulunmakta olup günden güne de yeni tehditler ortaya çıkmaktadır. IoT sistemlerindeki yazılımların ve cihazlardaki açıklıklarının kullanılması ve siber saldırı gerçekleştirilmesi bunlardan biridir. IoT ağının ortadaki adam saldırısı ile dinlenerek verilere ulaşılması, DoS/DDoS saldırılarıyla IoT hizmetlerinin engellenmesi, zararlı yazılımlarla verilere erişilmesi, değiştirilmesi ve erişimin engellenmesi gibi birçok siber tehdit bulunmaktadır. İşlenen veriler üzerinden profilleme yapılarak ilgili kişiler hakkında mahremiyete yönelik bilgi elde edilebilir, kimlik belirleme yapılabilir, ilgili kişiler bu cihazlar üzerinden izlenebilir ve takip edilebilir. Bir diğer yöntemle ise işlenen verilerin başka veri setleriyle eşleştirilerek ilgili kişiler hakkında diğer kişisel verilere ve mahremiyete yönelik bilgi elde edilebilmektedir. Yaşam döngüsü geçişleri olarak adlandırılan süreçte ilgili kişilerin artık kullanmadıkları IoT cihazlarını atmaları, satışa çıkarmaları ya da kiralamaları gibi elden çıkarma yöntemlerinde de cihazı kullanan ilgili kişi hakkında birçok bilgi edinilebilmektedir. Envanter saldırısı gerçekleştirilmesiyle ağ üzerinden sorgulanabilen cihazlarla ilgili kişilerin cihaz listesi çıkarılabilmekte ve eşya-envanter listesiyle ilgili kişiler hakkında bilgi çıkarımı yapılabilmektedir. En basit örnek olarak spesifik bir alanda sağlık için (örneğin glikoz veya parkinson takibinin yapılması amacıyla) kullanılan bir IoT cihazının varlığının tespit edilmesi durumunda ilgili kişinin hangi hastalığa sahip olduğu hakkında bilgi edinilebilmektedir.

IoT Uygulamalarında Mahremiyet ve Veri Koruma Yaklaşımlı Çözümler

IoT uygulamalarında veri ihlallerinin yaşanmasını önlemek adına IoT paydaşları ve kullanıcılar tarafından tedbirler alınması gerekmektedir. Bu noktada, IoT cihazlarının bireylerin mahremiyeti dikkate alınarak tasarlanması gerekmekte olup tasarımdan itibaren mahremiyet ve varsayılan mahremiyet yaklaşımları temel alınmalıdır. Varsayılan mahremiyet ile IoT sistemlerinin ayarlarının ve varsayılan özelliklerinin mahremiyeti korumaya yönelik düzenlenmiş olması oldukça önem arz etmektedir.

IoT sistemlerinde hangi cihazların sisteme dahil olduğu hakkında bilgi sahibi olunmalı, cihazlarda kimlik doğrulama ve yetkilendirme sistemleri kullanılmalıdır. Yazılım ve donanım yazılımlarında olası açıklık ve zafiyetlere karşı korunmak için düzenli olarak güncellemelerin geciktirilmeden yapılması gerekmektedir. IoT ağında ve iletişimdeki güvenlik sağlanmalı ve ağdaki verilerin açık metin şeklinde kullanılmamasına dikkat edilmelidir. Kriptografik yöntemlerle şifrelemelerin tercih edilerek bu sistemlerdeki verilerin okunması engellenmelidir.

Makine-insan, insan-makine, insan-insan ya da makine-makine iletişimlerin olduğu IoT ağlarında bağlantılar kablolu veya kablosuz çözümlerle yapılabilmektedir. İletişimin ağa gömülü olduğu bu sistemler, siber saldırganlar tarafından ilgi odağı haline gelmiştir. Siber güvenliğin sağlanması adına gelişmiş protokoller ve yazılım/donanım gibi anomali tespiti yapan çözümlerin de kullanılmasında fayda bulunmaktadır.

IoT cihazlarının günlük hayata dahil olmasıyla birlikte sağlık, akıllı ev, akıllı şehir, akıllı üretim gibi birçok alanda bu teknolojiler kullanılmaktadır. IoT sistemlerinde sayısız akıllı cihaz birbirlerine bağlanarak veri toplamaktadır. Akıllı cihazların toplamış oldukları veriler sebebiyle ilgili kişiler açısından mahremiyet ve güvenlik riskleri söz konusu olup işlenen verilerin özel nitelikli kişisel veri içermesi ve bu verilerin ifşa edilmesi veya özensiz şekilde işleme faaliyetlerine maruz kalması ilgili kişileri oldukça olumsuz etkileyebilecektir. Özellikle, büyük veri analitiği gibi veriler arasında bağ kuran teknolojilerin kullanımıyla IoT verileriyle ilgili kişilere ilişkin detaylı bilgi çıkarımı, davranış analizi vb. yapılabilmektedir. 6698 sayılı Kanunda düzenlenen kişisel verilerin işlenmesine ilişkin şartların tamamının ortadan kalkması durumunda kişisel veriler resen veya ilgili kişinin talebi doğrultusunda veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir. Bu kapsamda ilgili kişilerin hassas verilerinin, özel nitelikli kişisel verilerinin ve mahremiyetinin korunması adına işlenen veriler ile ilgili kişi arasındaki bağ koparılarak anonimleştirme tekniklerinden faydalanılabilmekte olup (Ren ve arkadaşları, 2021) IoT sistemleriyle işlenen verilerde, anonimleştirme kullanılması veri güvenliği ve mahremiyetin sağlanması için etkin yöntemlerden biridir.

Bir başka veri koruma temelli yöntem olan takma ad kullanımında; kişisel verilerin, yapay tanımlayıcılar oluşturularak bu tanımlayıcılar ile ilgili kişilerin kimliğini belirleyen verilerin yer değiştirmesiyle veri mahremiyeti amaçlanmaktadır. Veri üzerinde başarılı bir şekilde takma ad kullanımı veri mahremiyetini garantilemektedir (Voigt & von dem Bussche, 2017). Bununla birlikte, takma ad kullanma yöntemiyle ilgili kişi ile kişisel verisinin ilişkilendirilememesi, IoT sistemlerinde profilleme yapılmasına karşı koruma sağlayacaktır (Vasilomanolakis ve arkadaşları, 2015).

İlgili kişilere ait bilgilerin takma adlarla yer değiştirilmesi sonucu veri ihlali yaşansa bile ek bilgiler olmadan ilgili kişiye ait veriler ilgili kişinin kendisiyle ilişkilendirilemez. Ancak, ilgili kişi ile takma adlandırma uygulanan veri arasında ilişki kurulması ihtimali her zaman vardır. Bununla birlikte, anonimleştirilmiş veriler kişisel veri koruma düzenlemeleri kapsamına girmezken Madde 29 Çalışma Grubu (2014b) tarafından belirtildiği üzere takma ad kullanma yöntemi ilgili kişinin belirlenmesi ihtimaline izin vermekte ve bu nedenle söz konusu kişisel veriler yasal anlamda veri koruma rejimi kapsamında kalmaktadır. Kişisel Verileri Koruma Kurumu'nun "6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar - 2" rehberinde de takma ad kullanma yöntemiyle, kişisel verilerin anonim hâle getirilmemiş olması sebebiyle, kişisel veri niteliğini haiz olan bu verilerin Kanuna tabi olduğu belirtilmiştir.

Veri mahremiyetinin sağlanması adına gerektiği kadar veri işlenmesine dikkat edilmeli ve veri minimizasyonu esas alınarak veri işleme faaliyetleri gerçekleştirilmelidir. Yaşanabilecek veri ihlallerindeki sızdırılan, yetkisiz erişilen, elde edilen verilerin sınırlandırılması önceden uygulanan veri minimizasyonu yöntemiyle mümkündür. Sezgisel olarak, akıllı cihazlar tarafından toplanacak, muhafaza edilecek ve paylaşılacak veri ne kadar az olursa, ilgili kişilerin kişisel bilgilerinin korunması da o kadar kolay olacaktır (Qu, Nosouhi, Cui ve Yu, 2019). Veri minimizasyonuyla, veriler üzerinden keşif yapılarak ilgili kişiler üzerinde olumsuz etki oluşturulması ihtimali en aza indirgenmiş olacaktır. Veri minimizasyonunun iç ve dış tehditlere yönelik riskleri azaltan veri korumanın temel ilkelerinden birisi olduğu (Alkan, Menteş ve İnceefe, 2021) göz önünde bulundurulduğunda IoT sistemlerinde de veri güvenliği açısından oldukça önemlidir.

Bununla birlikte, kişisel veri güvenliğinin sağlanması ve mahremiyetin korunması için üretici ve hizmet sağlayıcılar tarafından mahremiyet etki değerlendirmesi ve risk değerlendirmelerinin yapılması oldukça önemlidir. Özellikle, IoT sistemlerinin geliştirilmesinde fazla sayıda aktör rol almakta olup veri sorumlusu ve veri işleyenlerin netleştirilmesi, veri güvenliğinin sağlanması adına yükümlülüğü bulunan veri sorumlularının sorumluluğu üstüne alması ve uygun güvenlik düzeyini sağlaması gerekmektedir. Bu kapsamda, IoT cihaz ve sistemlerinde güvenliğe yönelik teknik ve idari tedbirler alınmalıdır.

IoT sistemlerine yönelik tehditler sadece uygulama, yönetim hizmetleri ve ağ katmanlarına yönelik tehditlerden oluşmamakta olup fiziksel katman olan sensör/algılayıcı katmana yönelik tehditler de söz konusudur. Fiziksel katmana yapılan saldırılar cihazın güç bağlantısının kesilmesi, cihazın devre dışı hale getirilmesi, cihazın çalınması veya cihaza ait bir parçanın çıkarılması, değiştirilmesi gibi çeşitli şekillerde gerçekleştirilebilmektedir. Aynı şekilde siber saldırganlar tarafından IoT cihazlarının iç bileşenlerine, bağlantı noktalarına ve devrelere erişmek için IoT cihazları fiziksel olarak açılabilir ve ardından tüm ağa bağlanılabilir. Bu kapsamda, veri sorumluları tarafından veri güvenliğinin sağlanması ve mahremiyetin korunması adına fiziksel önlemlerin de alınması gerekmektedir.

Fiziksel güvenlik kapsamında, IoT cihazlarını geliştirme sürecinin sonunda kullanılan fiziksel portlar ve bağlantı noktalarının kaldırılması gerekmektedir. Bununla birlikte, IoT cihaz üreticileri tarafından cihazların varsayılan şifreleri, modeli, markası, üreticisi gibi çeşitli bilgiler içeren etiketler cihazların üstüne veya altına yapıştırılabilmektedir. Bu durum da kötü niyetli kişiler tarafından kullanılarak cihazın açıklıklarının tespit edilerek sömürülmesine ve yetkisiz erişim gerçekleştirilmesine neden olabilir. Veri sorumluları tarafından kurcalama saldırısı vb. tehditlere karşı mümkünse cihazların üzerinde varsa bilgi içeren etiketlerin kaldırılması veya cihazların kasa ya da kutulara yerleştirilmesi gibi önlemler alınmalıdır.

İlgili kişilerin kullandıkları IoT cihazları, kullanım süreleri boyunca bireylere ilişkin verileri ve etraflarındaki çeşitli verileri işleyebilmektedirler. İlgili kişiler, kullanıcılar tarafından kullanılan IoT cihazları artık kullanılmak istenmeyerek atılabilir, kiralanabilir veya satışa çıkarılabilir. Böyle bir durumda, söz konusu cihazlarla kullanım süresi boyunca toplanan verilerle kişilerin alışkanlıkları, rutinleri, tercihleri belirlenebilir ve profil çıkarılması gibi bir sonuçla karşılaşılabilir. Bu gibi durumların önüne geçmek için cihaz mülkiyeti değişecekse IoT Güvenlik Kuruluşu (IoT Security Foundation-IoTSF)'na ait IoT Güvenlik Teminatı Çerçevesi'nde yer verilen hususlardan faydalanılabilir.

Tablo 1. Sistemlerinde Veri Güvenliği ve Mahremiyetin Korunmasına Yönelik İlgili Kişiler Tarafından Alınabilecek Özet Tedbir Tablosu

İlgili Kişiler Tarafından Alınabilecek Tedbirler
• Ağda kullanılan varsayılan kullanıcı adı ve parolalar değiştirilmelidir.
• Parolalar belirlenirken güçlü parola özellikleri tercih edilmeli, parola güvenliği sağlanmalıdır.
• Düzenli olarak yazılım ve donanım yazılımları güncellenmelidir.
• IoT ağına erişirken halka açık Wi-Fi bağlantıları kullanılmamalıdır.
• Misafirler ve ziyaretçiler için misafir ağı oluşturulmalıdır.
• Wi-Fi üzerindeki iletişimlerin şifrelenmesine yönelik yönlendiricideki özellikler aktifleştirilmelidir.
• Kullanılmayan süreçlerde; Wi-Fi ağı kapatılmalı veya IoT cihazı ağdan çıkarılmalıdır.
• IoT cihaz ve sistemlerine erişimlerde çok faktörlü kimlik doğrulama kullanılmalıdır.
• Yeni nesil güvenlik duvarları kullanılmalıdır.
• IoT cihazlarında ve yönlendiricilerde kullanılmayan özellik ve fonksiyonlar pasif hale getirilmelidir.
• Fiziksel yetkisiz erişimleri önlemek adına IoT cihazlarında fiziksel güvenlik sağlanmalıdır.
• Gizlilik politikaları, hizmet şartları, kullanım koşulları ve kullanıcı sözleşmeleri dikkatli okunmalı, okunmadan kabul edilerek IoT uygulamaları kullanılmaya başlanmamalıdır.

Kişisel veri güvenliği için sadece veri sorumluları ve veri işleyenler tarafından güvenlik tedbirlerinin alınmasıyla %100 veri güvenliğinin sağlandığı söylenemez. Siber saldırganlar, IoT cihazlarının geliştirilme sürecindeki açıklık ve zafiyetler dışında kullanıcıların zayıflıklarına da yönelmektedir. Bu kapsamda, kullanıcılar nezdinde de kullanılan ağ bağlantılarının güvenli hale getirilmesi, parola güvenliğinin ve cihaz güvenliğinin sağlanması gibi çeşitli yönlerden güvenlik önlemlerinin alınması gerekmektedir. Bu noktada, ilgili kişiler tarafından dikkat edilmesi gereken hususlar (Tablo 1) bulunmaktadır. Ağ güvenliği, parola güvenliği, ağın segmente edilmesi gibi tedbirler alınmalı ve kullanılan IoT cihazlarının gizlilik sözleşmeleri, kullanım koşulları ve aydınlatma metinleri gibi dokümanlar dikkatlice okunmalı ve hangi verilerin kim tarafından ne amaçla işlendiği, nerelere aktarıldığı gibi konularda bilgi sahibi olunmalıdır.

NESNELERİN İNTERNETİNE YÖNELİK HUKUKİ DÜZENLEMELER VE STANDARTLAR

IoT sistemlerinin kullanımı giderek artmakta ve gelecekte de günlük hayatımızın birçok alanında kullanılacağı gerçeği kaçınılmazdır. Geleceğin teknolojisi olarak kabul gören IoT teknolojisi etrafından ve bireylerden fazla miktarda ve çeşitte veri toplamasıyla mahremiyet ve kişisel veri güvenliği endişelerine yol açmaktadır. Avrupa Veri Koruma Kurulu (2021), güvenlik kurallarının, politikalarının ve standartlarının siber güvenlik ve bilgi güvenliği yönetiminin bel kemiğinin oluşturduğunun altını çizmiş olup, bu sebeple de nesnelerin interneti ve ilgili hizmetlerin siber güvenliğinin sağlanması için güvenlik kuralları oluşturma stratejisi kullanılmasını önermektedir. Aynı zamanda, bu endişeleri gidermek adına IoT sistemlerine yönelik yasal çerçeveler getirilmesi birçok riski azaltacaktır. Bununla birlikte IoT pazarındaki veri akışı ve birçok açıdan işleyiş de düzenlenmiş olacaktır.

IoT teknolojilerindeki mahremiyet ve kişisel veri güvenliği endişeleri yakın dönemde ortaya çıktığından bazı ülkeler tarafından yasal düzenlemeler yapılmışken bazıları tarafından henüz yapılmamıştır. IoT'ye yönelik güvenlik ve mahremiyete ilişkin standartların bir kısmı yayımlanmış olup bazı standartlar ise geliştirme aşamasındadır. Buna örnek olarak Uluslararası Standart Organizasyonu'nun ISO/IEC 27400 Siber Güvenlik – IoT Güvenliği ve Mahremiyeti (Cybersecurity — IoT security and privacy) standardı verilebilir. Tablo 2 ve Tablo 3'te bazı ilgili standartlara ve düzenlemelere yer verilmiştir.

Tablo 2. IoT'ye Yönelik Bazı Yasal Düzenlemeler

Ülkeler	Düzenlemeler
ABD	The IoT Cybersecurity Improvement Act of 2020
ABD, Oregon	Relating to security measures required for devices that connect to the Internet
Avrupa Birliği	The Cybersecurity Act (Regulation (EU) 2019/881 of 17 April 2019)
Birleşik Arap Emirlikleri – Telecommunication Regulatory Authority	Regulatory Policy Internet of Things (IoT)
İngiltere	DCMS Code of Practice for Consumer IoT Security (Rapor)
Kaliforniya	SB-327 Information privacy: connected devices

Tablo 2. IoT'ye Yönelik Bazı Standartlar

Kurum/Kuruluş/Organizasyon Adı	Standart
International Telecommunication Union	Open data application programming interface (API) for IoT data in smart cities and communities (ITU Y.API4IOT)
International Telecommunication Union	Data Processing and Management Framework for IoT and Smart Cities and Communities
International Organization for Standardization (ISO)	ISO/IEC 27400 Cybersecurity - IoT security and privacy - Guidelines
International Organization for Standardization (ISO)	ISO/IEC TS 27570:2021 Privacy protection - Privacy guidelines for smart cities
European Telecommunications Standards Institute	ETSI TS 103 645 - Cyber Security for Consumer Internet of Things

ENISA - The European Union Agency for Network and Information Security (2022) tarafından IoT operatörlerine, akıllı altyapı sektörünün ve IoT sektörlerinin risk değerlendirmelerini yaparken rehber olması adına web tabanlı çevrimiçi bir araç geliştirilmiştir. Çalışmada, temel IoT güvenliği, akıllı hastaneler, akıllı şehirler, akıllı havalimanları, akıllı araçlar ve Endüstri 4.0 temelinde IoT sistemi ele alınmıştır.

IoT'ye yönelik spesifik yasal düzenlemeler de (Tablo 2) bulunmakta olup Avrupa Birliği'nde IoT cihazlarıyla toplanan veriler GVKT hükümlerine tabi olarak kabul edilmektedir. Bu kapsamda, IoT sistemlerinde herhangi bir veri güvenliği ihlali gerçekleşmesi durumunda GVKT hükümlerinin uygulanması gerekmektedir.

IoT teknolojileriyle kişisel verilerin işlenmesi söz konusu olduğundan ilgili sektördeki veri sorumluları ülkemizde 6698 sayılı Kanuna tabidir. Bununla birlikte, ülkemizde IoT teknolojisine yönelik spesifik bir düzenleme bulunmamakla birlikte T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin yayımlamış olduğu Bilgi ve İletişim Güvenliği Rehberinde "Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği" başlığı altında cihaz güvenliğine yönelik tedbir listeleri ve denetim sorularına da yer verilmiştir.

SONUÇ

Kullanıcılar verilerini toplayan, işleyen ve muhtemelen bilinmeyen üçüncü taraflara gönderen çok sayıda cihazlarla çevrilidir (Barati ve Rana, 2019). Söz konusu IoT cihazları aracılığıyla operasyonel ve kişisel veriler ile birlikte kullanıcıların rutini, davranışları, eylemlerine ilişkin veriler de işlenmektedir. Bu kapsamda, IoT teknolojisinin getirmiş olduğu yenilikler ve avantajlar kişisel veri güvenliği ve mahremiyet sorunlarını da beraberinde getirmektedir.

Kullanıcıların bu yeni teknolojiye olan ilgisi sebebiyle IoT cihazlarının kullanımı giderek artmakla birlikte cihazların bilinçsiz bir şekilde kullanılması söz konusudur. Bu nedenle, veri sorumluları için IoT sistemlerinde veri güvenliğine yönelik yeterli tedbirlerin yetkili makamlarca belirlenmesi, ilgili kişilerin alabilecekleri tedbirler hakkında bilgilendirilmesi ve IoT cihazlarında veri güvenliğinin önemine yönelik farkındalıklarının artırılması sağlanmalıdır.

Bilindiği üzere IoT sistemlerinde cihaz üreticileri, sosyal platformlar, üçüncü taraf uygulamalar ve geliştiricileri, IoT cihazını ödünç verenler veya kiralayanlar, veri komisyoncuları (data brokers) veya veri platformları gibi birden fazla aktör bulunmaktadır. IoT sistemlerinde veri güvenliğinin sağlanması adına ilk olarak yükümlülüğün kimde olduğuna karar verilmesi, veri sorumlusu-veri işleyen ilişkilerinin netleştirilmesi ve daha sonra geliştirme aşamasına geçilmesi gerektiği düşünülmektedir. İlerleyen süreçlerde ise veri sorumlusu, veri işleyen ve üçüncü taraflar arasındaki ilişkilerdeki değişikliklerin takip edilmesi, veri sorumlusu olmayan kişiliklerin veri sorumlusuna dönüşmesi durumunda veri işleme faaliyetlerinin kişisel verilerin korunması mevzuatına uygun olarak yürütülmesi gerekmektedir.

IoT teknolojisindeki kişisel verilere ve mahremiyete yönelik tehditleri bertaraf edebilmek adına tedbirler alınması gerektiği, bu noktada IoT donanım ve yazılımların geliştirilmesi aşamasında tasarımdan itibaren mahremiyet, varsayılan ayarlarla mahremiyet ilkeleriyle birlikte 6698 sayılı Kanun'da kişisel verilerin işlenmesinde uyulması zorunlu olan ilkelerin esas alınması gerektiği değerlendirilmektedir. Geliştirilecek IoT uygulamaları için mahremiyet etki değerlendirmesi ve risk değerlendirmelerinin de yapılması oldukça önemlidir. Öte yandan, cihaz keşfi ve yönetimi, kimlik doğrulama ve yetkilendirme, anonimleştirme tekniklerinden faydalanılması, yama yönetimi stratejisi geliştirilmesi ve güncellemelerin yapılması, ağ güvenliğinin sağlanması ve fiziksel önlemler gibi teknik tedbirler de alınmalıdır. IoT paydaşları tarafından alınması gereken tedbirlerin yasal bir altyapıya dayandırılması veri güvenliğinin sağlanması ve mahremiyetin korunması hususunda en azından belirlenen bir düzeyde güvence sağlayacaktır. Günümüzde global olarak baktığımızda bazı ülkelerde IoT uygulamalarına yönelik düzenlemeler mevcut olsa da bu alandaki düzenlemeler oldukça az sayıdadır. Aynı şekilde ülkemizde de konu özelinde henüz bir düzenleme bulunmamaktadır. Ancak, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin yayımlamış olduğu Bilgi ve İletişim Güvenliği Rehberindeki "Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği" başlığı ile IoT alanında güvenliğe yönelik çalışmaların ilk adımları atılmıştır. Bu kapsamda, IoT'ye yönelik olarak düzenlemeler yetersiz olduğundan sektöre özgü düzenlemeler, tavsiye niteliğinde rehberler ve kılavuzlar hazırlanması için çalışmalar yapılmasının gerektiği ve/veya var olan ilgili düzenlemelerde de IoT'ye yönelik değişiklikler yapılarak güncellenmesi gerektiği değerlendirilmektedir. IoT özelinde veri sorumluları tarafından alınması gereken temel tedbirlerin tanımlanması gerekmekte olup ulusal bir yasal altyapı ile desteklenmelidir. Oluşturulacak yasal alt yapıların, IoT teknolojisinin gelişmesini engellemeyecek şekilde geliştirilmesi konusunda hassas davranılarak veri koruma ile teknolojinin gelişmesi arasında uygun bir denge sağlanması gerektiği değerlendirilmektedir. ◆

KAYNAKÇA

- Alkan, M., Menteş, T. ve İnceefe, M. A. (2021). Kişisel Verileri Koruma El Kitabı - Teknik Uygulama ve Uyumluluk. Ankara: Nobel Akademik Yayıncılık.
- Article 29 Data Protection Working Party. (2014a). Opinion 05/2014 on Anonymisation Techniques. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf adresinden alınmıştır.
- Article 29 Data Protection Working Party. (2014b). Opinion 8/2014 on the on Recent Developments on the Internet of Things. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf adresinden alınmıştır.
- Ashton, K. (2009). That 'Internet of Things' Thing. RFID Journal. http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf adresinden alınmıştır.
- Avrupa Veri Koruma Kurulu. (2021). Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive. https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf adresinden alınmıştır.
- Barati M., Rana, O. (2019). Barati, M., & Rana, O.F. (2019). Enhancing User Privacy in IoT: Integration of GDPR and Blockchain. International Conference on Blockchain and Trustworthy Systems. Singapur: Springer, 322-335. DOI: 10.1007/978-981-15-2777-7_26
- DataReportal. (2023). Digital Around the World, https://datareportal.com/reports/digital-2023-october-global-statshot adresinden alınmıştır.
- Dülger, M. V. (2019). Kişisel Verilerin Korunması Hukuku, İstanbul: Hukuk Akademisi.
- Holub, A. (2020). The Future is Here – Assaulting the Internet with Mirai. https://umbrella.cisco.com/blog/future-assaulting-internet-mirai adresinden alınmıştır.
- Jovanovic, B. (2023). Internet of Things statistics for 2023 - Taking Things Apart. https://dataprot.net/statistics/iot-statistics/ adresinden alınmıştır.

- Karma, J. (2021). Songdo. https://www.aboutsmartcities.com/songdo-smart-city/ adresinden alınmıştır.
- Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12(9), 157. DOI: 10.3390/fi12090157
- Lu, Y. ve Xu L. D. (2019). Internet Of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. IEEE Internet of Things Journal, 6(2), 2103-2115. DOI: 10.1109/JIOT.2018.2869847
- Madakam, S., Ramaswamy, R. ve Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 3, 164-173. DOI: 10.4236/jcc.2015.35021.
- Paul, K. (2020). Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs. The Guardian. https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats adresinden alınmıştır.
- Qu, Y., Nosouhi, M. R., Cui, L. ve Yu, S. (2019). Chapter 6 - Privacy Preservation in Smart Cities, Rawat, D. B. ve Ghafoor, Z. K. (Der.), Smart Cities Cybersecurity and Privacy, (85), Amsterdam: Elsevier.
- Rayes, A. Salam, S. (2022). Internet of things (IoT) overview. Internet of Things from Hype to Reality, Springer, Cham, 1-34. DOI:10.1007/978-3-030-90158-5_1
- Ren, W., Tong, X., Du, J., Wang, N., Li, S., Min, G., ve Zhao, Z. (2021). Privacy Enhancing Techniques in the Internet of Things Using Data Anonymisation. Information Systems Frontiers. DOI:10.1007/s10796-021-10116-w
- Restuccia, F., D'Oro, S. ve Melodia, T. (2018). Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. IEEE Internet Of Things Journal, 5(6), 4829-4842. DOI: 10.1109/JIOT.2018.2846040
- Sundareswaran, V., Mahesh K., Rajesh M. ve Salmon, S. (2018). The Survey on Smart Agriculture Using IoT. International Journal of Innovative Research in Engineering and Management (IJIREM), 5(2), 63-66.

◊ Sundareswaran, V., Mahesh, K., Rajesh, M. ve Salmon, S. (2018). The Survey on Smart Agriculture Using IoT, International Journal of Innovative Research in Engineering and Management (IJIREM), 5(2), 63-66.

◊ Tawalbeh, L., Muheidat, F., Tawalbeh, M. ve Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions, Applied Sciences, 10(12), 4102. http://dx.doi.org/10.3390/app10124102 adresinden alınmıştır.

◊ The European Union Agency for Cybersecurity. (2022). Good practices for IoT and Smart Infrastructures Tool. https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool adresinden alınmıştır.

◊ Ülker, M., Canbay, Y. ve Sağıroğlu, Ş. (2017). Nesnelerin İnternetinin Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Açısından İncelenmesi. Türkiye Bilişim Vakfi Bilgisayar Bilimleri ve Mühendisliği Dergisi, 10(2), 28-41. https://dergipark.org.tr/tr/pub/tbbmd/issue/33390/335496 adresinden alınmıştır.

◊ Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., ve Kikiras, P. (2015). On the Security and Privacy of Internet of Things Architectures and Systems. 2015 International Workshop on Secure Internet of Things (SIoT), 49-57. DOI:10.1109/siot.2015.9

◊ Voigt, P., ve von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). Cham: Springer International Publishing, 16. DOI:10.1007/978-3-319-57959-7

◊ Wright, S. A. (2019). Privacy in IoT Blockchains: with Big Data comes Big Responsibility. IEEE International Conference on Big Data (Big Data), Los Angeles. DOI: 10.1109/BigData47090.2019.9006341

◊ Yıldız, M. (2020). E-Devlet Alanının Geleceği, Yıldız, M. ve Okur, M. R. (Haz.), Bilgi Toplumu ve E-devlet (136-267). Eskişehir: Anadolu Üniversitesi Yayınları.

BULUT BİLİŞİM ORTAMLARINDA KİŞİSEL VERİ GÜVENLİĞİ TEDBİRLERİ

Sefer AKTAŞ

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "Bulut Bilişim Ortamlarında Mahremiyet Sorunları ve Çözüm Önerileri" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Verilerin elektronik ortamlarda işlenebilir hale gelmesi, hayatımıza birçok kolaylıklar sağlamakla birlikte bazı sorunları da beraberinde getirmiştir. Bu sorunlardan bir tanesi sanal ortamda işlem yaparken güvenliğin nasıl sağlanacağıyla ilgilidir.

Bilgi ve iletişim teknolojilerindeki gelişmeler ile birlikte özellikle internetin kullanımında verilerin bulutta depolanması ihtiyacı doğmuştur. İnternetle beraber hayatımıza giren bulut bilişim ortamını kullanmak yürütmekte olduğumuz işlerimizi kolaylaştırsa da internetin dinamik ve dağıtık yapısı sebebiyle kişisel verilerimizi korumak daha da zorlaşmıştır. (BTK, Kişisel Veriler ve Kişisel Bilgi Güvenliği, 2021) Her ne kadar kişisel veriler kanunlarla ve uluslararası sözleşmelerle korunuyor olsa da içerik paylaşımının artarak devam ettiği internet üzerinde kişinin temel güvenliğini ve gizliliğini öncelikle kendisi sağlamalıdır.

Günümüzde işletmeler ve kullanıcılar tarafından kişisel verilerin sanal ortamda depolanması ve paylaşılmasındaki artış mahremiyetin ve güvenliğin sağlanmasına yönelik endişeleri de beraberinde getirmektedir. Bu sebeple bir bulut sağlayı-

cısından hizmet alındığında güvenliğin sağlanması açısından belirli gereksinimleri karşılaması beklenmektedir. Söz konusu gereksinimler arasında; anonimlik, yetkilendirme, kullanılabilirlik, gizlilik, bütünlük ve süreklilik bulunmaktadır.

Bulut bilişim, bir ağ üzerinde hizmet olarak sunulan bilgi işlem kaynaklarının kullanımı olarak kısaca tanımlanabilir. Son yıllarda kullanımı artarak devam eden bilgisayar teknolojilerinden birisi olarak görülen bulut bilişim ile birlikte verilerin, dünyanın herhangi bir noktasında işlenebilir hale gelmesi sonucu ilgili kişilerin güvenliğinin ne şekilde sağlanması gerektiği sorusunu akıllara getirmektedir. Bulut bilişim teknolojisi; düşük maliyeti, yüksek performansı, esnekliği ve kullanım kolaylığı ile kullanıcılara birtakım avantajlar sağlamaktadır. Söz konusu avantajların yanı sıra bazı dezavantajları da bulunmaktadır. Bunlar arasında; bulut hizmetinin genelde internet aracılığıyla erişilebilir olması, internet bağlantısı hızı, siber saldırılara açık olması gibi bazı dezavantajları bulunmaktadır.

Diğer taraftan veri güvenliği, verilerin yetkisiz kişilerce erişilmesine karşı korunması olarak kısaca tanımlanmakla birlikte kötü niyetli saldırıları ve verilerin kötüye kullanılmasını önlemek için her türlü teknik ve idari tedbirleri almayı hedeflemektedir. Alınan güvenlik tedbirleri sayesinde verilerin doğru, güvenilir ve yetkili kişilerce erişilebilir olması sağlanmaktadır. (Berqnet, 2021)

BULUT BİLİŞİM VE GENEL YAPISI

NIST (ABD Ulusal Standartlar ve Teknoloji Enstitüsü) tarafından ifade edilen bulut bilişim tanımına göre; “Bulut bilişim, yapılandırılabilir bilişim kaynaklarından oluşan ortak bir havuza, uygun koşullarda ve isteğe bağlı olarak her zaman, her yerden erişime imkân veren bir modeldir.” (BTK, Bulut Bilişim, 2013) Belirtilen tanımın yanı sıra kısaca bulut bilişim, farklı kaynakların internet üzerinden sunulması olarak ifade edilebilir. Söz konusu kaynaklar; veri depolama, sunucular, veri tabanları, ağ iletişimi, yazılım gibi araçları ve uygulamaları içerirler.

Bulut Bilişim Servis Modelleri;

Yazılım Servisi (SaaS), bir bulut sağlayıcısının uygulamaları barındırdığı ve bunları internet üzerinden son kullanıcıların kullanımına sunduğu bir bulut bilişim servis modelidir. Bu servis modelinde bulut kullanıcıları, uygulamanın üzerinde çalıştığı bulut altyapısını ve platformu yönetemezler. Kurulum gerektirmediğinden bir internet tarayıcısı ve bir ağ bağlantısı yazılım servisini kullanmak için yeterlidir. Yazılım servis sağlayıcılarına örnek olarak: Microsoft Office365, Google Apps, GT Nexus, Marketo, TradeCard Onlive ve Netflix verilebilir.

Platform Servisi (PaaS), bulut sağlayıcılarının internet üzerinden kullanıcılara donanım ve yazılım araçları sağladığı bir bulut bilişim modelidir. PaaS modeli, uygulama geliştiricilerini yeni bir uygulama geliştirmek veya uygulamaları çalıştırmak için kurum içi donanım ve yazılım yükleme zorunluluğundan kurtarır. PaaS sağlayıcılarına örnek olarak: AWS Elastic Beanstalk, Cloud Foundry, Force.com, OrangeScape verilebilir. Altyapı Servisi, bulut aracılığıyla işletmelere ve bireylere talep üzerine kaynaklar sunan, neredeyse sonsuz ölçeklenebilir bilgi işlem kaynaklarının isteğe bağlı olarak kullanılabilirliğini sağlayan bir bulut bilişim servis modelidir. IaaS servis modeli; bireysel sunuculardan özel ağlara, mesajlaşma sistemlerinden alan adı sunucularına, e-posta sunucularından çeşitli depolama aygıtlarına kadar çok geniş çapta araç ve özelliği kapsayabilir. IaaS sağlayıcılarına örnek olarak Amazon Cloud Formation, Amazon EC2, Microsoft Azure, Google Cloud verilebilir.

Bulut Bilişim Dağıtım Modelleri;

Bulutun kullanım şekli kuruluşların yapısına ve büyüklüğüne göre değişim göstermektedir. Her kuruluşun bir bulutta hangi hizmetlere erişmek istediği ve ortam üzerinde ne kadar kontrol sahibi olmak istediği konusunda kendi gereksinimleri vardır. Genel, özel, topluluk ve karma bulut modellerinden oluşur.

Genel Bulut (Public Cloud), genel olarak her kesimden kullanıcıya açık, verileri iletmek için yüksek bant genişliğine sahip ağ bağlantısına dayanan tamamen sanallaştırılmış bir ortam olmakla birlikte; sanal makineler, uygulamalar veya depolama gibi kaynakları kullanıcılara uzaktan sunan standart bir bulut bilişim dağıtım modelidir.

Özel Bulut (Private Cloud), yalnızca bir kuruluş için işletilen, kuruluş veya üçüncü bir tarafça yönetilen ve şirket içinde veya şirket dışında var olan bir bulut altyapısı olarak tanımlanır. Özel bulutlar kullanımı açısından genel bulutlardan farklıdır. Çünkü özel bir bulutla ilişkili altyapı genellikle tek bir kuruluşa tahsis edilirken başka hiçbir kuruluşla paylaşılmaz.

Topluluk Bulutu (Community Cloud), Kavramsal olarak özel bulut ile genel bulut arasında bir yerde bulunan topluluk bulutu, birden fazla şirket tarafından kullanılan ve paylaşılan bir altyapıyı tanımlamaktadır.

Karma Bulut (Hybrid Cloud), şirket içi bir veri merkezini (özel bulut) bir genel bulutla birleştiren, verilerin ve uygulamaların aralarında paylaşılmasına izin veren bir bilgi işlem ortamıdır.

BULUT SİSTEMLERİNDE KİŞİSEL VERİ GÜVENLİĞİ İÇİN DİKKAT EDİLMESİ GEREKEN UNSURLAR

Doğru Bulut Hizmetini ve Bulut Sağlayıcısını Seçme

Bulut kullanıcılarının ihtiyaçlarını gidermek için çok çeşitli bulut hizmetleri mevcuttur. Kullanıcıların çeşitli bulut hizmetlerini kullandıklarında birtakım riskler ortaya çıkmaktadır. Kullanıcının uyum sağlaması gereken bir bulut hizmetini kullanmak yerine belirli işlem için tasarlanmış kullanıcının ihtiyacına uygun bir bulut hizmeti kullanmak daha makul olabilir. Doğru bulut sağlayıcısını seçmek; bulut sağlayıcısı yönünden, sahip olduğu kişisel veri güvenliğine verdiği öneme dair bir değerlendirme olacaktır. Değerlendirme neticesinde veri sorumlusunun kişisel veri güvenliğine verdiği önem ortaya çıkacak ve bulut sağlayıcılarının sıkı tedbirler alması gerektiği konusunda bulut sağlayıcılarında farkındalık oluşacağı için sunulan hizmetin kalitesi de artacaktır. (Keskin, 2020)

Bulut sağlayıcıları, hizmetlerinin geliştirilmesi konusunda farklı yöntemler kullanarak belirli pazar sektörlerini de hedefleyebilmektedirler. Örneğin, bazı bulut hizmetleri genel tüketicilere yönelikken, bazıları ise belirli kuruluşların talebi üzerine oluşturulmuş özel hizmetler şeklinde olabilmektedir. (Keskin, 2020)

Veri sorumlularının, bulut hizmeti ile ilgili uygulamaya koyduğu düzenlemeler hakkında son kullanıcılarını bilgilendirmek için uygun adımları atması gerekir. Veri sorumlusu oluşturmuş olduğu bilgilendirme mekanizması ile söz konusu konuya ilişkin son kullanıcılara yönelik mümkün olduğunca açık bir şekilde bilgi vermelidir. (EDPS, 2021)

Bulut Sağlayıcısı Güvenliği Değerlendirme

Genellikle bir veri işleyen tarafından kullanılan güvenlik önlemlerini değerlendirmenin en etkili yollarından biri, veri sorulusunun veri işleyen tesislerini yerinde incelemek olacaktır. ICO (Information Commissioner's Office), özellikle genel bulut ortamı için denetlemenin çeşitli lojistik nedenlerle uygulanabilir olma ihtimalinin düşük olduğunu ifade etmektedir. Ayrıca bir bulut sağlayıcısının, olası ve mevcut müşterilerinin her birinin bir denetim yapmak üzere tesislerine girmesine izin vermesi de mümkün gözükmemektedir. (EDPS, 2021)

Bulut sağlayıcıları verdikleri hizmetin güvenlik denetimini yürütmesi için bir kontrol mekanizması oluşturulmalı ve üçüncü bir tarafça bir değerlendirmeden geçirilmelidir. Daha sonra değerlendirmenin sonucu veri sorumluları ile paylaşıldığında ilerde meydana gelecek sorunların üstesinden gelmek daha kolay hale gelecektir. Bulut sağlayıcısının güvenliğinin uygun olup olmadığı konusunda veri sorumlusunun bilinçli bir seçim yapabilmek için söz konusu değerlendirmenin yeterince ayrıntılı olması gerekir. Ayrıntılı bir değerlendirme raporu veri sorumlusunun veya bulut kullanıcısının veri koruma yükümlülüklerine uymasına yardımcı olacaktır. Aynı zamanda bahse konu değerlendirme içerisinde mevcut fiziksel, teknik ve idari güvenlik önlemlerinin yanı sıra planlanan ilave tedbirlere ilişkin bilgilendirmeler de yer almalıdır. (Investopedia, Cloud Computing, 2021)

Ayrıca bulut sağlayıcısı veri sorumlularına uygun güvenlik önlemlerini uygulanmaya devam ettiğini gösteren düzenli güncellemeler ve geri bildirimler sağlayabilmelidir. Veri sorumlusu da elde ettiği geri bildirimler neticesinde bulut sağlayıcısının sağladığı kullanılabilirlik, gizlilik ve bütünlük garantilerini gözden geçirmeli ve takibini sağlamalıdır. (Azure, 2021)

Sözleşmeler

Bulut hizmeti satın alırken bulut sağlayıcısı ile yapılan sözleşme maddelerine dikkat etmek gerekir. Yazılı bir sözleşmenin mevcudiyeti, bulut sağlayıcısı tarafından kullanıcı bilgisi ve onayı olmadan sözleşmenin süresi boyunca veri işleme şartlarını değiştiremeyeceği anlamına gelmektedir.

Veri sorumluları, bir bulut sağlayıcının pazarlık fırsatı olmadan "kullan veya kullanma" koşulları sunması durumunda dikkatli olmalıdır. Sözleşmelerin zoraki kullanım şartlarıyla hazırlanması, veri sorumlularının veya kullanıcıların veri koruma yükümlülüklerini yerine getirmek için veriler üzerinde yeterli kontrolü elinde tutmasına izin vermeyebilmektedir. Bu nedenle; veri sorumluları, oluşabilecek riskleri göz önünde bulundurarak bir bulut sağlayıcısının sunabileceği hizmet şartlarını dikkatli bir şekilde kontrol etmesi gerekmektedir. (EDPS, 2021)

Bulut hizmeti alt hizmet sağlayıcıları aracılığıyla da alınabilmektedir. Alt hizmet sağlayıcılarının aracı olduğu durumda bulut sağlayıcısı ile alt hizmet sağlayıcıları arasındaki sorumluluk ilişkisinin belirlenmesi gerekmektedir. Bulut hizmeti verilirken sistemin yavaşlaması, arızalanması veya herhangi bir sebeple veri kaybına sebep olma durumu gibi riskler göz önünde bulundurulmalıdır. Söz konusu problemlerle karşılaşıldığında sorumluluğun kime ait olduğuna ilişkin hükümlere dikkat etmek gerekmektedir. (EDPS, 2021)

Veri merkezlerine verilerin aktarılması ve verilerin işlenmesi gibi hususların sözleşme metni içerisinde ayrıntılı olarak değerlendirilmesi ve ele alınması gerek-

mektedir. Verilerin ve verilerin tutulduğu sistemdeki alanın sözleşme bitiminden sonra ne gibi işlemlerden geçirileceği konusu gizlilik şartları açısından önem arz etmektedir. Verinin saklandığı ve yedeklendiği yerler, bulut sağlayıcının bulunduğu yerler, kullanıcıların ikamet ettiği yerler farklı ülkelerde olması sebebiyle uygulanacak mevzuatın kararlaştırılması da ayrıca önem arz etmektedir. (Startuphukuku, 2021)

Buluta geçiş yapmayı düşünen herhangi bir işletme, uygun bir bulut sağlayıcı kullandığından emin olmak için ihtiyaçlarını ve yükümlülüklerini net bir şekilde ortaya koymalıdır. Ayrıca veri sorumlusunun yapacağı sözleşmede geçen yükümlülüklere hâkim olarak ileride meydana gelecek istenmeyen durumlara karşı da önceden önlemini alması gerekir. (Cora, 2022)Veri sorumlusu, bulut sağlayıcısı ile yapılan sözleşmeye özen göstermeli, aksi takdirde ortaya çıkacak olan olumsuz durumlardan dolayı sorumlu tutulacağı unutulmamalıdır.

Riskleri Değerlendirme

Veri sorumlusu, kendisi için hangi bulut hizmetinin veya bulut sağlayıcısının uygun olduğunu belirlemeden önce, bulut sağlayıcısının kişisel verileri bulutta nasıl işleyeceğini göz önünde bulundurmalıdır. Veri sorumlusu elinde tuttuğu kişisel verileri bulutta nasıl işlemesi gerektiğini planladığını netleştirdiğinde riskleri değerlendirebilir durumda olur ve daha sonra söz konusu riskleri azaltmak için uygun adımları atabilir. (EDPS, 2021)

Büyük veya karmaşık bulut hizmetlerinde kişisel verileri işlemek isteyen veri sorumluları veya bulut kullanıcıları, herhangi bir gizlilik endişesini değerlendirmek, belirlemek ve bunları erken bir aşamada ele almak için bir gizlilik etki değerlendirmesi yaparak bundan fayda sağlayabilir. Gizlilik etki değerlendirmesi; yeni bir ürün, hizmet veya teknoloji geliştirirken ortaya çıkacak olan olumsuzluklara karşı olası gizlilik sorunlarını belirlemek ve sorunlar ortaya çıkmadan önce gerekli önlemleri almak için bir kılavuzdur. (Takçı & Pelin, 2017)

Buluta Taşınacak Verilerin Seçimi

Bir bulut kullanıcısının veya veri sorumlusunun tüm verilerini buluta veya aynı bulut hizmetine taşımaması gerektiğini bilmesi gerekir. Bireylerin belirli türdeki kişisel verilerinin işlenmesi, kişilerin güvenlik ve mahremiyeti üzerinde daha büyük bir etkiye sahip olabilmektedir. Söz konusu durumu göz önünde bulundurması gereken bulut kullanıcısı, işlediği kişisel verileri gözden geçirmeli ve buluta konulmaması gereken herhangi bir veri olup olmadığını belirlemelidir. Çünkü

bulut sağlayıcısı kişisel verileri toplarken belirli güvenceler vermiş olsa da kullanıcılar buluta aktaracağı kişisel verilerin daha sonra ortaya çıkabilecek olumsuzlukları da göz önünde bulundurarak önem durumunu kendileri belirlemeli ve ona göre işlem yapmalıdır. (EDPS, 2021) Aksi takdirde oluşabilecek herhangi olumsuz bir durum kullanıcıların kişisel veri güvenliğini olumsuz yönde etkileyebilecektir.

Çoğu zaman üzerinde durulması gereken şey, kişisel verilerin buluta yerleştirilmesi gerekip gerekmediği değil, veri koruma risklerinin neler olduğu ve bu risklerin azaltılıp azaltılamayacağı şeklinde olması önem arz etmektedir. Bulut kullanıcısı, buluta taşımayı planladığı veri kategorileri hakkında net bir kayıt oluşturmalıdır. (Kyoceradocumentsolutions, 2022)

Bulut kullanıcısı, bulut hizmetlerini kullanırken daha fazla kişisel verinin toplanmasına yol açabileceğini de unutmamalıdır. Örneğin, kullanıcıların kullanım istatistikleri veya işlem geçmişleri kaydedilebilmektedir. Söz konusu meta veriler, belirli durumlarda kişisel veriler de olabilmektedirler. Böyle bir durum söz konusu olursa, bulut kullanıcısı hangi verilerin toplandığını bilmeli, toplanan verilerin gerekli olup olmadığını belirlemeli ve kendilerine bu konuda bir gizlilik politikası aracılığıyla yeterli bilgi verilip verilmediğini kontrol etmelidir. (Cora, 2022)

Veri Kullanılabilirliği

Veri merkezinde meydana gelebilecek su baskını, yangın, sabit disk veya ağda oluşabilecek arızalar gibi beklenmedik durumlarla karşılaşılabilir. Bulut hizmet sağlayıcısının beklenmedik durumlara karşı almış olduğu önlemler doğrultusunda son kullanıcının verilerine ulaşabilmesi ve verilerini doğrulayabilmesi verinin kullanılabilirliğine etki etmektedir.

Sınır ötesinde bulunan sunucular üzerinde veri depolama sorunu kullanıcılar için ciddi bir endişe kaynağı olmaktadır. Bulut hizmeti sağlayıcısının verileri hangi ülkede işlediğine bakılmaksızın verinin güvenliğini, gizliliğini ve bütünlüğünü sağlaması gerekmektedir. Kafalarda oluşabilecek tüm endişeleri kullanıcılarıyla paylaşmalı ve bu bağlamda güven ilişkisi kurmalıdır. Ayrıca, veri güvenliği için garanti sağlamalı ve müşterilere bulunduğu yerin yasalarına ilişkin uyması gereken kurallar hakkında açıklamada bulunarak şeffaf olmalıdır. Son kullanıcının kendisine ait verilere istediği zaman ulaşabilmesini sağlamak ve verilere erişimdeki karmaşıklığı ortadan kaldırmak kullanıcıların buluta olan güvenlerini artırmaktadır. (Sun, 2014)

Bulutta depolama işlemi kullanıcılar için bulutun karmaşıklığını azaltabilen şeffaf depolama hizmeti sağlasa da aynı zamanda kullanıcıların veri depolama

üzerindeki kontrol yeteneğini de azaltmaktadır. (Mindcentric, Keeping Cloud Computing Confidential, 2022) Genel olarak sabit sürücüler bulut sisteminde ana depolama ortamı olarak kullanılırlar. Bulut sisteminde her ne kadar fiziksel sabit sürücüler kullanılsa da bu sabit sürücüler veri merkezlerinde ölçeklenebilirliği sağlamak ve maliyet tasarrufu sağlamak amacıyla sanal sabit sürücülere ayrılmaktadır. Birden fazla fiziksel sabit sürücünün bulunduğu sistem tek bir fiziksel sabit sürücüymüş gibi ayarlanarak daha sonra birden fazla sanal sabit sürücüye ayrılabilmektedir. Sanal olarak oluşturulan sabit sürücüler kullanıcılara tahsil edildiğinde kullanıcılar birden fazla fiziksel sabit sürücünün belirli bir depolama alanını kullanıyor olmaktadır. Bu sebeple, kullanıcı verileri sadece bir fiziksel sürücüyü kullanmadıkları için sabit disklerin güvenilirliği ve yedekli olması bulut depolamanın temelini oluşturmaktadır. Sabit sürücülerin yazılımsal ve donanımsal hataları bulut sağlayıcısı tarafından göz önünde bulundurulmalı ve beklenmedik arızalar gerçekleştiğinde kullanıcının depolamış olduğu verilerde kayıp olmayacak şekilde önlemler alması gerekmektedir. (Sun, 2014)

Veri Bütünlüğünün Korunması

Veri bütünlüğü, herhangi bir bilgi sistemindeki en kritik unsurlardan biridir. Verilerin yetkisiz olarak silinmesini, değiştirilmesini veya korunmasını önlemeyi amaçlamaktadır. Tüzel kişiliğin belirli kurumsal kaynaklara sahip haklarını yöneterek değerli olarak görülen verilerin ve hizmetlerin kötüye kullanılmasını veya çalınmasını önler. (Talend, 2021)

Bulut sistemindeki veri bütünlüğü, bilgi bütünlüğünün korunarak yetkisiz kullanıcılar tarafından erişilemez veya değiştirilmez durumunu ifade etmektedir. Bulut sistemlerinde veri bütünlüğünü sağlamak; SaaS, PaaS ve IaaS gibi bulut bilişim hizmetlerinin sağlıklı işleyebilmesi için bulut güvenliğinin temelini oluşturmaktadır. Bulut bilişim sistemleri, büyük ölçekli verileri depolamasının yanı sıra, genellikle söz konusu verileri işleme hizmetini de sağlamaktadır.

Bulut sistemlerinde veri bütünlüğü RAID benzeri stratejiler ve dijital imza gibi tekniklerle de elde edilmektedir. (Digitalguardian, 2021) RAID, tek bir sürücünün performansını artırmak için birden çok sabit sürücüyü birleştiren, onu bir veya daha fazla mantıksal birimde adreslenebilir hale getiren ve böylece veri depolamanın güvenilirliğini ve işlevselliğini artıran bir sanallaştırma teknolojisidir. (Turhost, 2022) Dijital imza ise; elektronik ortamdaki bir belgeyle, bahse konu belgeyi imzalayanı güvenilir bir şekilde ilişkilendiren kimlik doğrulama metodudur. Belge veya mesaja eklenen ıslak imzalara benzer şekilde söz konusu belge ve mesajlara elektronik ortamda eklenen bir kod olarak düşünülebilir. (Innova, 2022)

Yetkilendirme

Yetkilendirme, veriye erişimi denetlemek için kullanılan bir erişim politikası tanımlama işlemi olmakla birlikte bir sistemin, kimliği doğrulanmış belirli bir kullanıcının sistem tarafından denetlenen kaynakları güvence altına almak için hangi erişim düzeyine sahip olması gerektiğini belirleyen bir mekanizmadır. (Economictimes, 2021)

Yetkilendirme, bulut ortamındaki çok sayıda varlık ve erişim noktası sayesinde, yalnızca yetkili varlıkların verilerle etkileşim kurabilmesini sağlamak için çok önemlidir. Veri sorumluları izleme mekanizmaları ile yetkisiz erişimi önleyerek veri bütünlüğünü korumada daha fazla güven sağlayabilirler. Söz konusu izleme mekanizmaları, verilerin veya sistem bilgilerinin kimler veya neler tarafından değiştirilmiş olabileceğini belirlemede açıklık getirdiğinden veri bütünlüğünü potansiyel olarak etkilemektedir. Bulut bilişim sağlayıcıları veri bütünlüğünü ve doğruluğunu koruduklarını ifade ettiklerinde veri sorumluları tarafından farklı kontrol mekanizmalarına başvurulmadan sağlayıcılar güvenilir kabul edilebilmektedir. Ancak, kullanıcılar ve bulut hizmeti sağlayıcılarının almış olduğu güvenlik önlemlerinin yanı sıra üçüncü taraf denetim mekanizmasını da oluşturmak yetkilendirmenin sağlıklı işletilebilmesi için gereklidir. (Sun, 2014)

Uyumluluk Gereksinimi ve Veri İşleme

Bulut bilişim kullanımı, çevrimiçi uygulama kurallarında ifade edilen kişisel verilerin toplanması, saklanması ve kullanılmasıyla ilgili sorumluluklara ek olarak, bir veri sorumlusunun daha önce karşılaşmamış olabileceği bazı uyumluluk gereksinimlerini beraberinde getirebilmektedir. (EPDS, 2021)

Bulut bilişim, herkese uyan tek bir çeşit ürün olmamakla birlikte çoğu durumda bir kurum veya kuruluşun özel ihtiyaçlarına göre uyarlanabilmektedir. Uyarlama sırasında ortaya çıkabilecek uyumluluk sorunları, bulut hizmetinin türüne bağlı olarak değişkenlik gösterebilir. (Cora, 2022)

Kişisel Verileri Koruma Kanunu'nun 4. maddesine göre kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygunluğu, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesinin zorunluluğu belirtilmiştir. (KVKK, 2016)

Bahse konu Kanuna göre bulut hizmeti alan veri sorumluları, bulut sağlayıcısının

kişisel verileri yalnızca belirtilen amaçlar doğrultusunda işlemesini sağlamakla yükümlüdür. Bir şirket veya kuruluş, işlediği kişisel verileri barındırmak ve gerekirse buna göre hareket etmek için bir bulut hizmeti sağlayıcısıyla anlaşma yapabilir. Bu durumda bulut hizmeti sağlayıcısı, yalnızca barındırma hizmetleri sağladığı, kendi adına herhangi bir kişisel veri işlemediği ve veri denetleyicisinin talimatlarına uygun hareket ettiği için veri işleyen olarak hareket edecektir. (KVKK, 2016)

Hizmetin Kötüye Kullanılması

Hizmetin kötüye kullanımı, saldırganların bulut hizmetini kötüye kullanarak verileri ele geçirebileceği veya kullanıcıların çıkarlarını yok edebileceği anlamına gelmektedir. Bunun yanı sıra sadece saldırganlar tarafından değil diğer kullanıcılar tarafından veya hizmet sağlayıcısı çalışanlarınca da hizmetin kötüye kullanılabilme durumu söz konusudur. (Sun, 2014)

Bulut hizmet sağlayıcıları bulutta depolama işlemlerini gerçekleştirirken tekilleştirme teknolojisini kullanabilirler. Tekilleştirme teknolojisi (Deduplication Technology) bulut depolama alanında yaygın olarak kullanılmakla birlikte verilerin genellikle bir kez depolandığı ancak birden fazla farklı kullanıcı tarafından paylaşıldığı anlamına gelir. Söz konusu teknoloji, depolama alanında tasarruf sağlayarak bulut hizmeti sağlayıcılarının harcama maliyetini azaltır. Ancak tekilleştirme teknolojisi kullanıldığında saldırganların depolanan dosyaların hash kodunu öğrenerek verilere erişebilme ihtimalleri göz önünde bulundurulduğunda buluttaki hassas verileri sızdırmak mümkün hale gelebilir. (Sun, 2014) Bu nedenle, bulut kullanıcılarının kimlik doğrulamasını kontrol etmek için Sahiplik Kanıtı Yaklaşımı (Proof of Ownership) önerilmektedir. (Dave, 2021) Sahiplik Kanıtı Yaklaşımı (PoW), bulut depolama sunucularına istemcilerin yalnızca sahip oldukları dosyaları yüklemelerini ve indirmelerini garanti etme olanağı sağlayarak depolama gereksinimlerini azaltmaya yönelik etkili bir tekilleştirme tekniği olarak düşünülmektedir. (Gonzalez-Manzano, 2016)

Ayrıca bulut hizmeti sağlayıcısının sistemi yöneten ve teknik işlemlerini yapan çalışanları arasındaki gereksiz yetkilendirmeler kullanıcıların kişisel veri güvenliği için risk oluşturabilmektedir. Özellikle yönetici konumunda olanların, altında çalışan teknik personelden ayrıcalıklı sistem yönetim haklar istemesi durumunda kullanıcı verilerine yetkisiz erişim hakkına sahip olmasına neden olmaktadır. Bu durumun önüne geçebilmek için, her ne kadar güvenilir personel çalıştırıldığı düşünülse de sistemdeki hareketlerin takip ve kontrolünün düzenli bir şekilde yapılması ve mümkünse farklı personel tarafından izlenmesi ve rapor edilmesi gerekir.

Kimlik Yönetimi

Kişisel veriler, bilgisayar ağları içerisinde kontrolsüz şekilde erişilebilir olduğunda güvenlik endişelerini de artırmaktadır. Uygun ve yeterli koruma mekanizmalarının eksikliği durumunda, veriler üçüncü kişiler tarafından erişilebilir hale gelebilir. Kimlik yönetimi, kullanıcılarla ilgili bilgilerin kontrolü işini yürütmektedir. Kullanıcının kimlik onayı, erişim durumu, yürütmeye yetkili olduğu işlemler, kullanıcının tanımlayıcı bilgisi, söz konusu bilgiye kimin, nasıl erişebileceği veya değiştirebileceği bilgisini içerdiği için kişisel veri güvenliği endişelerini en aza indirmeyi sağlar. (E.Burr, 2017)

Kullanıcıların kişisel verilerini nasıl bir şekilde yöneteceklerinin kararını vermelerine yardımcı olmak önemli bir konu haline gelmiştir. Kullanıcıların işlerini kolaylaştırmak için bulut sağlayıcıları, bulut yapısı içerisinde kimlik yönetimi sistemini sıkı bir şekilde kullanırlar. Söz konusu sistem, kullanıcıların servis tabanlı hizmetler yoluyla kimliklerini doğrulayarak, kullanıcıya kendi kişisel verilerine erişme izni vermektedir. (ICO, 2021)

Performans İzleme ve Erişim Kontrolü

Bir bulut sağlayıcısını seçtikten sonra işlemin sona ermeyeceğinin farkında olmak veri sorumlusunun dikkat etmesi gereken durumları arasındadır. Bulut hizmetinin beklenen şekilde ve sözleşmeye dayalı anlaşmanın şart koştuğu şekilde çalıştığından emin olmak için sürekli bir izleme, inceleme ve değerlendirme döngüsünde bulunması gerekmektedir. (ICO, 2021) Bulut sağlayıcısı katmanlı hizmetler söz konusu olduğunda, bulut hizmetinin sağlanması sırasında meydana gelen alt işleyen zincirindeki değişiklikler hakkında bulut müşterisini bilgilendirmelidir. (STM, 2022)

Bulut hizmetinin faydalarından biri, verilere herhangi bir yerden erişebilme yeteneğine sahip olmamızı sağlamasıdır. Söz konusu erişim, bulut kullanıcılarının internet erişimi olduğu sürece verilerine herhangi bir yerden farklı cihazlarla ulaşması anlamına gelir. Ancak veri sorumlusunun verilere yetkisiz erişimi önlemek için yeteri kadar önlem alındığından emin olması gerekir. Örneğin, bulut hizmeti, kullanıcı adı ve parola sistemi kullanarak kimlik doğrulama süreci sunuyorsa, bulut kullanıcılarının her birinin kendisine ait tekil hesapları olmalıdır. Ayrıca, kullanıcı hesapları oluşturmak, güncellemek, askıya almak veya silmek, işletmeden ayrılan çalışanların erişimini kaldırmak veya unutulan, kaybolan, çalınan kimlik bilgilerini sıfırlamak için bir sistemin de mevcut olması gerekir. (Investopedia, Cloud Computing, 2021)

Verilerin Şifreli Korunması

Şifreleme; veri sorumlularının sorumlu olduğu kişisel verilere yalnızca doğru anahtara sahip yetkili taraflarca erişilebilmesini sağlamasına olanak tanıdığı için bulut bilişim güvenliğinde önemli bir kavramdır. Öncelikle verilerin aktarımı sırasında uç noktalar arasında iletişim güvenli olmalı ve müdahaleye karşı korunmalıdır. Uçtan noktalar arasındaki iletişimi koruma şifreli bir protokol yöntemi kullanılarak gerçekleştirilir. İletişimde kullanılan söz konusu şifreleme algoritması rastgele değil tanınan endüstri standartlarını karşılaması gerekir. (ICO, 2021) Bulut sağlayıcısı iletişimi sağlarken, bulut hizmetinde coğrafi olarak ayrılabilen veri merkezleri arasında aktarılan verilerin uygun şekilde güvenli olarak aktarıldığına dair güvence verebilmelidir. (Investopedia, Cloud Computing, 2021)

Veri sorumlusu, bulut hizmeti içinde depolanan veriler için de şifreleme kullanmanın uygun olup olmadığını da değerlendirmelidir. Şifrelemenin kullanım durumu, kişisel verilerin niteliğine ve bulutta gerçekleştirilen işleme türüne göre değişiklik gösterebilir. Özellikle özel nitelikli kişisel veriler işlenirken hem iletişimde hem de depolamada şifreleme kullanmak veri güvenliğinin korunması açısından önemli bir husus olarak değerlendirilmektedir. (ICO, 2021)

Kişisel veri güvenliğinin ve gizliliğin korunmasını sağlamak için teknik bir önlem olarak şifreleme kullanılıyorsa, şifreleme için kullanılan anahtarın güvenliğinin de ayrıç sağlanması gerekir. Bu bağlamda, sağlam bir anahtar yönetimi düzenlemesi, şifrelemenin sunabileceği koruma düzeyini sürdürebilmek için çok önemlidir. Aksi takdirde anahtara sahip olan üçüncü kişilerin verilere erişim hakkına sahip olacağı ve bir şifreleme anahtarının kaybı verileri işe yaramaz hale getirebileceğinden kişisel verilerin yanlışlıkla imha edilmesi anlamına gelecektir. (Forcepoint, 2022)

Veri Saklama, Kopyalama ve Silme

Veriler temel depolama ortamlarından silindiğinde bazı ek işlemler yapılmadıkça nadiren tam olarak kaldırılırlar. Ayrıca bir bulut sağlayıcının daha güvenilir bir hizmet sağlamak amacıyla birden çok yerde depolanan verilerin birden çok kopyasına sahip olması da olasılık dâhilindedir. Söz konusu verilerin depolandığı yerler, yedekleme bantları veya doğrudan buluta bağlı olmayan diğer depolama ortamları olabilir. Bir bulut hizmetinde saklanan kişisel verilerin kopyaları verilerin aynısı gibi değil de farklı uzantılarla veya farklı dizin yapıları gibi başka biçimlerde de saklanabilir. (Investopedia, Cloud Computing, 2021)

Büyük ölçekli bulut sağlayıcıları tarafından veri kopyalama işlemi yapılırken genellikle fiziksel sunucularda ve farklı bölgelerde bulunan üç kopya tercih edilir. Bahse konu tercih edilen yöntem farklı bölgelerdeki kullanıcılara daha hızlı ve daha dağıtık hizmetler sunduğu için yaygın olarak kullanılmaktadır. Bulut hizmet sağlayıcısı tarafından veri kopyalama (replikasyon) stratejisine göre veriler güncellenirken güncelleme işleminin diğer kopyalara nasıl ve ne zaman yansıyacağı veri sorumlusu ile paylaşılmalıdır. Bulut sağlayıcısının planladığı büyük ölçekli bir güncelleme söz konusu olduğunda, güncelleme işlemi sırasında farklı bir sunucudaki verilerin bir kopyasına erişmeye çalışan bir kullanıcı için iyi bir yöntem oluşturulmalıdır. (ICO, 2021)

Veri sorumlusu, bulut sağlayıcısının kendi silme planına uygun bir zaman ölçeği içinde kişisel verilerin tüm kopyalarını silebilmesini sağlamalı ve gelecekte bulut sağlayıcısı bulut hizmetinden herhangi bir sebeple çekilmeye karar verirse kullanıcıların kişisel verilerine ne olacağı veya ne gibi işlemler yapılacağı hakkında bilgi sahibi olmalı ve söz konusu çekilme sonrası yapılacağı beyan edilen işlemlerin sözleşmede yer aldığından emin olması gerekir. Aynı şekilde veri sorumlusu bulut sağlayıcısı ile arasındaki sözleşme süresi sona erdiğinde veya sözleşme feshedildiğinde yapılacak işlemlerin sözleşmede yer almasını ve sonrasında takibini sağlaması gerekir. (Beyondtrust, 2022)

Sağlayıcı Erişimi ve Personel Eğitimi

Bulut sağlayıcısı, bilgi işlem kaynaklarını veri sorumlusu veya bulut kullanıcısı adına yönettiğinden dolayı verilere ve verilerin kopyalarına erişmesi muhtemeldir. Destek hizmetlerinin sağlanması gibi eylemler için de sistem erişiminde yetki sahibi olabilmektedir. Ancak kendisine verilen yönetim yetkisiyle yetkisiz erişime neden olursa kişisel verilerin uygun olmayan şekilde ifşa edilmesine, silinmesine veya değiştirilmesine yol açabilir. (Checkpoint, 2022)

Bulut sağlayıcısının işlediği kişisel verilere erişebileceği koşulları belirlemek için yürürlükte olan açık politikalar ve prosedürler olmalıdır. Söz konusu politika ve prosedürler; yetkisiz erişim, silme veya değişiklik meydana geldiğinde neler yapılacağına ilişkin bulut müşterisini uyarmalı ve yapılacak işlemlere ilişkin bilgilendirme sağlamalıdır. (ICO, 2021)

Veri sorumlusu, bulut bilişim hizmeti alırken istekleri doğrultusunda yeni bir dizi veri koruma riskine yol açabileceğini de göz ardı etmemelidir. Bulut sağlayıcısı, veri sorumlusunun almış olduğu bulut hizmetinin güvenlik ayarlarını yapılandırması için denetim mekanizması oluşturabilir. Veri sorumlusunun söz

konusu güvenliği sürdürebilmek için uygun eğitime ve prosedürlere sahip olması gerekir. (ICO, 2021)

Çoklu Kiracılı Ortam

Bir bulut sağlayıcısı, birçok veri sorumlusu için bir veri işleyen görevinde olabilmektedir. Söz konusu bulut sağlayıcısının veri sorumlusuna hizmet sunan bir veri işleyen olmasının yanı sıra çok sayıda bulut kullanıcısına da hizmet verebilmektedir. Bulut bilişimin sunmuş olduğu bu çeşitli yapı ile bilgi işlem kaynaklarının verimli kullanımı bulut sağlayıcısı açısından maliyet tasarrufunu ortaya çıkarmaktadır. Ancak bulut sağlayıcılarının söz konusu maliyete yönelik tasarruflu çalışma durumu sebebiyle veri sorumluları ve kullanıcıları, kendi verilerinin diğer bulut sağlayıcılarının müşterilerinin verileriyle aynı sistemlerde işlenmesi durumuyla karşılaşabilir. Bulut sağlayıcısı, bir bulut müşterisinin diğer bulut müşterisinin kişisel verilerine erişme olasılığına karşı koruma sağlamak için sağlam bir dizi güvenlik önlemine sahip olmalı ve bir bulut müşterisinin faaliyetinin diğerlerinin faaliyetlerini etkilememesi için tedbirler alması gerekecektir. (IBM, 2022)

Güvenilirlik, Dayanıklılık ve İlgili Kişi Hakları

Veri sorumlusu, hizmet aldığı bulut sağlayıcısı tarafından çevrimdışına alınarak büyük bir kesintiye maruz kalması durumunda meydana gelecek sonuçları dikkate almalıdır. Kendini kanıtlamış bir bulut sağlayıcısının seçilmesi, daha güvenilir ve dayanıklı bir hizmet sağlayacağı için hizmet kesintilerine karşı da ciddi önlemler almış olacağından önem arz etmektedir. Ayrıca veri sorumlusunun, kesintinin etkisini en aza indirebilmek için verilerinin bir kopyasını alternatif bir yerde depolaması uygun olacaktır. (ICO, 2021)

Veri sorumlusu, bir bulut hizmetine geçmeden önce bulut sağlayıcısının ilgili kişilerin haklarını kullanmasına izin verdiğinden emin olmalıdır. Örnek olarak; ilgili kişiler kişisel verilerine erişim hakkına ve kişisel verilerinin belirli amaçlar dışında işlenmesine itiraz etme hakkına sahip olması verilebilir. (Netser, 2022)

SONUÇ

Bulut bilişimin; kullanım kolaylığı, esnekliği, uygun maliyeti, verilere hızlı ve istenilen yerden erişim imkânı sağlaması sayesinde günümüzde kullanımı artarak devam eden bir teknoloji olarak kabul edilmektedir. Söz konusu kullanım artışıyla birlikte kişisel verilerin güvenliğine gösterilen hassasiyetin artması da kullanıcılar tarafından önem arz eden bir konu haline gelmiştir. Verilerin depolandığı sunucular için alınan güvenlik önlemleri ve sunucuların hangi ülkede bulunduğu gibi konularda kullanıcılar kontrol sağlayamadıkları için birtakım endişelere sahip olmaktadırlar. Söz konusu endişeleri ortadan kaldırmak için kullanıcıların, alınan güvenlik önlemleri hakkında, verilerin işlenmesi ve aktarımı gibi konularda bilgilendirilmeye ihtiyaçları vardır. Bu sebeple veri sorumluları bulut hizmetini satın alırken; çalışanlar, müşteriler, kullanıcılar ve diğer üçüncü kişiler açısından bu gibi hususlara dikkat etmeleri gerekmektedir.

Veri sorumlusunun kişisel verilerin kötüye kullanılmasından dolayı sorumlu tutulacağı için sözleşme yaptığı bulut sağlayıcısının ve bağlı alt sağlayıcılarının uygun güvenlik hizmetini sunabildiğine emin olmalıdır. Verilerin güvenliği konusunda yeterli bilgi vermeyen ve güvence sağlayamayan herhangi bir bulut hizmet sağlayıcısı tercih edilmemelidir. Veri sorumlusu riskleri değerlendirmek ve belirli bir bulut sağlayıcısına güvenilip güvenilmeyeceğine karar vermek zorunda olduğu için almış olduğu kararlardan dolayı da sorumlu tutulacağını unutmamalıdır. Bulut hizmet sağlayıcılarının, bulut bilişim hizmetlerine olan güveni artırmak için araştırmalara, standardizasyon ve belgelendirme programlarına, yasal ve düzenleyici çerçeve çalışmalarının uyarlamalarına daha fazla önem göstermesi gerekir. Veri sorumluları, gerekirse güvenilir üçüncü tarafların yardımıyla, bulut bilişim sistemini kullanmadan önce uygun risk değerlendirmelerini ve gizlilik etki değerlendirmelerini yapmalıdır. Bulut bilişim sistemlerine yapılan saldırılarla verilerin üçüncü kişilerin eline geçmemesi için yukarıda belirtilen gerekli güvenlik önlemlerinin alınması ve verilerin şifrelenmiş bir şekilde bulutta saklanması önerilmektedir. Verileri şifrelemek, güvenlik ve gizlilik söz konusu olduğunda atılması gereken en önemli adımlardan biridir. Bulut bilişimde şifrelemeye yönelik konu Kişisel Verileri Koruma Kurulu tarafından yayınlanan kılavuzlarda açıkça ele alınmaktadır. ◆

KAYNAKÇA

- Azure. (2021, 12 06). *Top benefits of cloud computing.* https://azure. microsoft.com: https://azure. microsoft.com/en-us/overview/what-is-cloud-computing/#cloud-deployment-types adresinden alınmıştır.
- Berqnet. (2021, 06 11). *Veri Güvenliği Nedir? İşletmeler Nasıl Önlem Alabilir?* https://berqnet.com: https://berqnet.com/blog/veri-guvenligi-nedir adresinden alınmıştır.
- Beyondtrust. (2022, 03 20). *Effective Privilege Management for the Cloud: The 3 Keys.* https://www.beyondtrust.com: https://www.beyondtrust.com/blog/entry/effective-privilege-management-for-the-cloud-the-3-keys adresinden alınmıştır.
- BTK. (2013). Bulut Bilişim. Ankara: BTK.
- BTK. (2021, 02 11). *Kişisel Veriler ve Kişisel Bilgi Güvenliği.* https://internet.btk.gov.tr: https://internet.btk.gov.tr/kisisel-veriler-ve-kisisel-bilgi-guvenligi adresinden alınmıştır.
- Checkpoint. (2022, 01 13). *What is Cloud Security?* https://www.checkpoint.com: https://www.checkpoint. com/cyber-hub/cloud-security/what-is-cloud-security/ adresinden alınmıştır.
- Cora. (2022, 04 09). *Understanding the Determinants of Cloud Computing Adoption for High Performance Computing.* https://cora.ucc.ie: https://cora.ucc.ie/bitstream/handle/10468/5269/paper0490.pdf?sequence=1&isAllowed=y adresinden alınmıştır.
- Dave, J. (2021, 11 22). *Secure and Efficient Proof of Ownership for Deduplicated Cloud Storage.* https://www.researchgate.net: https://www.researchgate.net/publication/320075845_Secure_and_Efficient_Proof_of_Ownership_for_Deduplicated_Cloud_Storage adresinden alınmıştır.
- Digitalguardian. (2021, 11 12). *A Definition Of Data Integrity.* https://digitalguardian.com/: https://digitalguardian.com/blog/what-data-integrity-data-protection-101 adresinden alınmıştır.
- E.Burr, W. (2017). Information security. NIST (s. 31-37).

- Economictimes. (2021, 12 21). *What is 'Authorization'.* https://economictimes.indiatimes.com: https://economictimes.indiatimes.com/definition/authorization adresinden alınmıştır.
- EDPS. (2021, 11 01). *Guidelines on the use of cloud computing services by the European institutions and bodies.* https://edps.europa.eu: https://edps.europa.eu/sites/default/files/publication/18-03-16_cloud_computing_guidelines_en.pdf adresinden alınmıştır.
- EPDS. (2021, 11 01). *Guidelines on the use of cloud computing services by the European institutions and bodies.* https://edps.europa.eu: https://edps.europa.eu/sites/default/files/publication/18-03-16_cloud_computing_guidelines_en.pdf adresinden alınmıştır.
- Forcepoint. (2022, 01 20). *Bulut Güvenliği nedir?* https://www.forcepoint.com: https://www.forcepoint. com/tr/cyber-edu/cloud-security adresinden alınmıştır.
- Gonzalez-Manzano, L. (2016). ase-PoW: A Proof of Ownership Mechanism for Cloud Deduplication in Hierarchical Environments. L. Gonzalez-Manzano içinde, *Security and Privacy in Communication Networks* (s. 412-418).
- IBM. (2022, 03 12). *Çok Kiracılı Ortamlar.* https://www.ibm.com: https://www.ibm.com/docs/tr/cognos-analytics/11.0.0?topic=guide-multitenant-environments adresinden alınmıştır.
- ICO. (2021, 12 18). *Guidance on the use of cloud computing.* https://ico.org.uk: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf adresinden alınmıştır.
- Innova. (2022, 04 14). *Dijital İmza nedir, nasıl kullanılır?* https://www.innova.com.tr: https://www.innova.com.tr/tr/blog/dijital-donusum-blog/dijital-imza-nedir-nasil-kullanilir adresinden alınmıştır.
- Investopedia. (2021, 01 12). *Cloud Computing.* https://www.investopedia.com: https://www.investopedia.com/terms/c/cloud-computing.asp#toc-what-is-cloud-computing adresinden alınmıştır.

◊ Investopedia. (2021, 12 12). *Cloud Computing.* https://www.investopedia.com: https://www.investopedia.com/terms/c/cloud-computing.asp#toc-what-is-cloud-computing adresinden alınmıştır.

◊ Investopedia. (2022, 02 05). Cloud Computing. https://www.investopedia.com: https://www.investopedia.com/terms/c/ cloud-computing.asp adresinden alınmıştır.

◊ Keskin, N. (2020). Çok Ölçütlü Karar Verme Yöntemleri İle Bulut Bilişim Hizmet Sağlayıcısı Seçimi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi,* 52-73.

◊ KVKK. (2016, 03 24). 6698 *Sayılı Kişisel Verilerin Korunması Kanunu.* 6698 Sayılı Kişisel Verilerin Korunması Kanunu. Resmi Gazete.

◊ Kyoceradocumentsolutions. (2022, 03 12). *Veriler buluta nasıl taşınır?* https://www.kyoceradocumentsolutions.com.tr: https://www.kyoceradocumentsolutions.com.tr/tr/smarter-workspaces/business-challenges/the-cloud/cloud-data-migration-guide.html adresinden alınmıştır.

◊ Mindcentric. (2022, 04 28). *Keeping Cloud Computing Confidential.* https://www.mindcentric.com: https://www.mindcentric.com/blog/data-security-in-cloud-computing#:~:text=Data%20availability%20is%20a%20term,ranging%20from%20normal%20to%20disastrous adresinden alınmıştır.

◊ Mindcentric. (2022, 04 28). *Keeping Cloud Computing Confidential.* https://www.mindcentric.com: https://www.mindcentric.com/blog/data-security-in-cloud-computing#:~:text=Data%20availability%20is%20a%20term,-ranging%20from%20normal%20to%20disastrous. adresinden alınmıştır.

◊ Netser. (2022, 03 12). *Bulut İletişim Çözümleri.* https://www.netser.com.tr: https://www.netser.com.tr/tr/cozumlerimiz/bulut-iletisim-cozumleri, adresinden alınmıştır.

◊ Startuphukuku. (2021, 10 16). *https://startuphukuku.com.* Bulut Bilişimin Hukuki Boyutu ve Bulut Bilişim Sözleşmesi: https://startuphukuku.com/bulut-bilisim-sozlesmesi-hukuki-boyutlar/ adresinden alınmıştır.

◊ STM. (2022, 02 01). *Bulut Bilişim Güvenliği.* https://thinktech.stm.com.tr: https://thinktech.stm.com.tr/uploads//docs/1646651618_stmbulutbilisimguvenligi.pdf? adresinden alınmıştır.

◊ Sun, Y. (2014). Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks,* 1-8.

◊ Takçı, H., & Pelin, C. (2017). Kişisel verilerin korunmasında öznitelik tabanlı gizlilik etki değerlendirmesi yöntemi. *Mühendislik Mimarlık Fakültesi Dergisi,* 1301-1310.

◊ Talend. (2021, 04 28). *What is data integrity?* https://www.talend.com: https://www.talend.com/resources/what-is-data-integrity/ adresinden alınmıştır.

◊ Turhost. (2022, 04 14). *Raid Nedir?* https://www.turhost.com: https://www.turhost.com/blog/raid-nedir/ adresinden alınmıştır.

VERİ KORUMA HUKUKU AÇISINDAN BLOK ZİNCİR TEKNOLOJİSİNE BAKIŞ

Hande ÖZTÜRK

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "KVKK Kapsamında Blok zincir Teknolojisi" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Merkezi bir otorite ihtiyacını ortadan kaldırarak eşlerin birbirleriyle doğrudan işlem yapmalarını sağlayan eşler arası bir defter sistemi olarak tanımlanan blok zincirinin hem veri depolama hem de bilgisayar kodlarının çalıştırılması için kullanılabilen genel amaçlı bir teknoloji olma özelliği, farklı bağlamlarda farklı hedeflere ulaşmak için çeşitli aktörlerin şu anda bu teknolojiyi neden denemekte olduğunu açıklamaktadır. Blok zincir teknolojisinin merkezi olmayan, şeffaf ve güven odaklı olma özellikleri nedeniyle günümüz teknoloji faaliyetlerindeki kaygılara bir çözüm olarak sunulabileceği öngörülmektedir (Diri, 2022).

Çalışmanın ilk kısmında blok zincir teknolojisi genel anlamda teorik olarak ele alınmış olup tanımı ve tarihçesi ile başlanarak teknolojinin karakteristik özellikleri, türleri, yönetim yapısı ile teknolojide kullanılan şifreleme yöntemlerine değinilmiş olup alışmanın ikinci kısmında ise blok zincir teknolojisi kullanımında söz konusu olabilecek kişisel veri işlemelerin veri koruma hukuku kapsamında nasıl ele alındığı konusu detaylandırılmıştır. Bu kapsamda ilk olarak blok zincir ağında tutulabilecek kişisel veri türleri ele alındıktan sonra ilgili teknolojide veri sorumlusu ve veri işleyen tanımını karşılayacak aktörlerin kimler olabileceği ko-

nusu irdelenmiştir. Sonrasında blok zincir teknolojisinin veri koruma hukuku kapsamında ilişkilendirilebileceği kişisel veri işleme şartlarına yer verilmiş olup burada blok zincir ağında gerçekleştirilebilecek veri işleme faaliyetlerinin veri işleme şartlarına göre işlenebilme durumu ele alınmıştır. Daha sonra ise blok zincir teknolojisinde kişisel veri işlenmesine dair diğer önemli kavramlar arasında veri minimizasyonu ilkesi, saklama süreleri, yurt dışına kişisel veri aktarımı ve ilgili kişi haklarına yer verilmiştir. Çalışma dahilinde ilgili konu başlıkları altında ve ayrıca sonuç kısmında blok zinciri teknolojisinin veri koruma hukuku ile ilişkisine dair görüş ve öneriler de yer almaktadır.

BLOK ZİNCİR TEKNOLOJİSİ

Tanım ve Tarihçe

Blok zincir merkezi bir otorite ihtiyacını ortadan kaldırarak eşlerin birbirleriyle doğrudan işlem yapmalarını sağlayan eşler arası bir defter sistemidir. Özünde blok zinciri; bir işleme ilişkin bilgileri, değiştirilmesini zorlaştıran veya imkânsız hale getiren, merkezi olmayan yeni bir yolla kaydetme sistemidir. Bu işlemler, ağın katılımcıları arasında paylaşılan bir dijital defterdeki sayfalarda veya bloklarda saklanır. İşlemler üzerindeki fikir birliği eşler arası ağı anlaşmaya (mutabakata) vardırır. Üzerinde anlaşmaya varılan işlem blokları değişmez deftere kaydedildiğinde "güven" kavramı sistemin temel bileşeni haline gelir.

Müzik paylaşım siteleri uçtan uca ağ oluşturma hakkında ilk ışığı yakmıştır. Telif ihlali bir yana bırakıldığında müzik paylaşım şirketlerinin ana hedefi dosya bütünlüğünün sağlanması idi.

2000'lerin başında birbirinden bağımsız iki proje olan eDonkey ve BitTorrent, tam olarak internet üzerinde hiç tanımadığımız ama iletişime geçebileceğimiz diğer kişiler, daha doğrusu makineler üzerinden verinin paylaşılması için geliştirilmiş, uçtan uca "Peer to Peer- P2P" olarak isimlendirilen bir tür veri depolama çözümü olarak karşımıza çıkmışlardır. Bu sistemlerde veri, tek bir merkezde değil sayısı milyonları bulabilecek makineler üzerinde dağıtılmış veya paylaşılmış şekilde bulunur. Bu makinelerden bazıları verinin tamamını, bazıları ise kısmen belli bir parçasını içerebilir. Ulaşmak istediğinizde sistem size bu veriyi, sunulabilecek en hızlı düzenlemeyle, farklı makinelerden çekecek şekilde yönlendirir. Siz veriyi kendi bilgisayarınıza çekerken, aldığınız veri karşılığında aynı zamanda diğer kullanıcılara bir veri kaynağı olarak hizmet edersiniz. Sistemin kullanıcıları, sisteme verdikleri destek süreci ile doğru orantılı olarak sistemden faydalanabilirler. Bu platformlar, bulutun ötesinde bir çözüm sunmakla birlikte, içeriğin şifrelenmesi, verinin nerelerde saklanacağına dair seçenek sunmaması gibi nedenlerden dolayı, kurumsal veya mahremiyet içeren kişisel veriler için güvenli bir depolama çözümü değildir. Bu yaklaşım ile Distributed Ledger Systems ("Dağıtık Kayıt Defterleri") adı verilen çözümler ortaya çıkmıştır ve blok zincir teknolojisi de bu çözümün farklı bir uygulaması olarak değerlendirilebilir (Usta ve Doğantekin, 2019).

Değerin İnterneti, bugün bilginin hareket ettiği hızda değerin değiş tokuşunun gerçekleştirildiği bir dünyayı temsil etmektedir. İnternet şu anda da bu yeni teknolojilerin işlem gördüğü temel platform olma özelliğini taşımaktadır. Kripto paraların, anahtarların, şifrelerin ve diğer blok zincir özelliklerinin yönetimine yardımcı olmak adına yeni Web 3.0 tarayıcıları yapım aşamasındadır.

İnternetin yarattığı gibi bir etkiye sahip olabilecek blok zincir teknolojisini anlamaya da aşina olduğumuz bir örnekle başlanılabilir. Bir e-postaya bir Word belgesi, Excel sayfası veya PDF dosyası gibi bir belge eklediğimizde orijinali gönderilmez. Aslında alıcıya bir kopyası gönderilir ve bu bilginin dolaşımı açısından iyi bir yol olarak karşımıza çıkar. Ancak konu para, hisse senetleri ve tahviller, sadakat puanları, fikri mülkiyet, bir oyun veya konser biletleri olduğunda o zaman bu belgelerin bir kopyasının gönderilmesi birdenbire kötü bir fikir halini almaktadır. Örneğin, birine bir konser bileti gönderdiğimizde o kişiye bu biletin kopyasını göndermememiz önemlidir. O kişi artık biletin orijinaline sahip olmalıdır ve biz artık bu bileti kullanamamalı veya satamamalıyızdır. Aynı şekilde birine bir para gönderdiğimizde bu paraya artık biz sahip olmamalıyız veya bir başkasına gönderememeliyiz. Bu iki örnek de "çifte harcama problemi' ne (Dijital para birimi kavramıyla ortaya çıkan teknik bir sorun, birisinin dijital parayı çoğaltma ve aynı anda iki veya daha fazla yerde harcama yeteneğidir. Bu 'çifte harcama' sorunu, Bitcoin gibi blok zinciri tabanlı kripto para birimlerinde, Emeğin İspatı (PoW) olarak bilinen bir mutabakat mekanizması kullanılarak önlenir. Emeğin İspatı, yalnızca blok zincirinin defterindeki geçmiş işlemlerin doğruluğunu güvence altına almakla kalmayıp aynı zamanda çifte harcamayı tespit eden ve önleyen merkezi olmayan bir "madenciler" ağı tarafından gerçekleştirilir.) işaret eder ve blok zincir teknolojisi ile bu duruma çözüm getirilebilir ("How Does Block Chain Prevent Doublespending Bitcoins", 2022). Bu teknoloji ile biletten paraya ve müziğe kadar her türlü varlık, aracı olmaksızın saklanabilir, taşınabilir, takas edilebilir ve işlem görebilir. Her yerde insanlar, iş birliği ve kriptografi kullanarak eşler arası işlem yapabilir ve birbirlerine güvenebilir. Bu güven ve iş birliğine nasıl gelindiği noktasında ise gerçek kimliği hala bilinmeyen Satoshi Nakamoto'nun 2008'de yayınladığı Bitcoin olarak bilinen elektronik paranın eşler arası versiyonunu tanıttığı teknik incelemesine işaret edilir (Nakamoto, 2008). Bununla

birlikte blok zincir teknolojisine ait kavramsal temel ve bileşenler sadece Satoshi Nakamoto'nun makalesine özgü değildir. Bu bileşenler, ilk olarak 90'lı yıllarda kaleme alınan üç farklı makale ile karşımıza çıkmaktadır. Stuart Haber ve W. Scott Stornetta tarafından hazırlanan 1991 yılına ait makalede, belgelerin zaman damgası ile birlikte kripto imzalarla nasıl kullanılacağı anlatılmaktadır (Haber ve Stornetta,1991). Ross Anderson'ın hazırladığı 1996 yılına ait bir makalede ise, kaydedilen güncellemelerin silinemeyeceği, merkezi olmayan bir veri depolama sistemi tanımlanır (Anderson, 1996). Bruce Schneier ve John Kelsey tarafından hazırlanan 1998 yılına ait bir makale (Schneier ve Kelsey, 1998) ise, güvenilmeyen makineler üzerinde tutulan günlük dosyalarının içerdiği hassas bilgilerin korunması için şifrelemenin nasıl kullanılacağını açıklar (Usta ve Doğantekin, 2019).

Blok zincir, sürekli büyüyen dijital bir veri kayıtları listesidir. Bu liste, kronolojik sıraya göre düzenlenmiş ve kriptografik kanıtlarla bağlanmış ve güvence altına alınmış birçok veri bloğundan oluşur. Haber ve Stornetta'nın çalışmaları Dave Bayer, Hal Finney ve diğer birçok bilgisayar bilimci ve kriptografi meraklısının çalışmalarına ilham vermiştir ve bu da ilk merkezi olmayan elektronik nakit sistemi (ya da sadece ilk kripto para birimi) olarak Bitcoin'in yaratılmasına yol açmıştır ve nihayetinde Bitcoin hakkındaki resmi rapor da 2008 yılında Satoshi Nakamoto takma adı altında yayınlanmıştır ("Blockchain", 2022).

Blok zincir tarihçesi esasında muhasebenin tarihçesi ile sıkı sıkıya bağlıdır. Üçlü kayıt sistemi, dış tarafların da dahil olduğu tüm muhasebe girişlerinin üçüncü bir giriş tarafından kriptografik olarak kapatılarak bu şekilde geleneksel çift kayıt sistemine yapılan bir iyileştirmedir. Borç ve alacak kaydına ek olarak tüm geçmiş borç ve alacaklara bir bağlantı da bulunur. Üçlü kayıt sistemi defteri Nakamoto'nun 2008 yılındaki teknik incelemesinde karşımıza çıkar. Blok zinciri, bir işlem bağlamında deftere kaydedilen bir varlığımızın olduğu üçlü kayıt sisteminin ilk uygulamasıdır. Üçlü kayıt sistemindeki üçüncü giriş, defterde kalıcı ve değişmez bir şekilde saklanan işlemin kriptografik bir hesabına sahip olmamızı sağlayan kriptografidir.

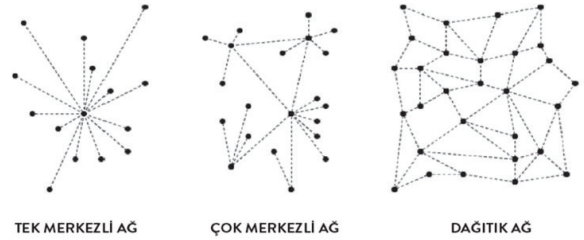
Blok zincir Teknolojisinin Özellikleri

Dağıtık Defter Yapısı

Bir defter, varlıkların değil işlemlerin bir koleksiyonudur. Varlıklar işlemin bir parçasıdır, ancak defter işlemi kaydeder. Dijital olarak dağıtılmış bir defter veya blok zincirinde, defterin bir sahibi olmaz. Defter, hepsi aynı blok zinciri protokollerini çalıştıran ağdaki katılımcılar arasında dağıtılır. Ağdaki her düğümde/

bilgisayarda defterin özdeş bir kopyasının bulunması nedeniyle ağ merkezi değildir. Nakamoto'nun teknik incelemesinin yayınlanmasıyla Bitcoin, halka açık bir blok zinciri defterine ilk varlık transferini kaydederek blok zincir teknolojisinden yararlanan ilk uygulama olmuştur.

Merkezi olmayan bir defter, farklı konumlar ve kişilerin merkezi bir otoriteye olan ihtiyacı ortadan kaldıran merkezi olmayan ağı tarafından desteklenen herhangi işlemler veya sözleşmelerin defteri olarak tanımlanabilir. Bir kayıt yapıldığında, her katılımcı bu kayıttan haberdar edilir. Katılımcılar, artık o ağdaki diğer tüm düğümlerle aynı olacak şekilde işlemlerin kaydının özdeş bir kopyasına sahiptirler.



Şekil 1. Dağıtık ağ

Uçtan uca (Eşler arası) Ağ Yapısı

Defter, uçlardan oluşan bir ağ tarafından depolanır, güncellenir ve korunur. Düğümler; bir blok zinciri ağının altyapısını oluşturur, bir blok zincirinin varlığını sağlamak üzere blok zinciri verilerini depolar, yayar ve korurlar. Bir ağdaki tüm düğümler aynı işlem kurallarını veya protokolleri takip eder ancak düğümlerin farklı rolleri vardır. Tam bir düğüm, blok zinciri protokolünün bir kopyasını ve blok zincirinin işlem geçmişini içerir, ayrıca blok zincirinin bakımına yardımcı olur. Kullanıcı düğümü, defter ile etkileşime girer. Blok zinciri teknolojisi ile bir merkezi otoritenin eksikliği eşler arası bir ağ yapısı ile değiştirilmiş olur.

Çok Taraflılık (Aracının Kaldırılması)

Geleneksel merkezi defter sistemlerinin bazı zayıf tarafları vardır. Örneğin doğruluk, merkezi defterin detaylarını değiştirebilen aracılara bağlıdır. Defterden elde edilen veriler ayrı yere alınarak kötü amaçlı olarak kullanılabilir. Merkezi olmayan dağıtık defterler, verileri manipüle edebilecek olan aracılara bağımlı

değildir. Veriler güvenli ve müdahaleye karşı dayanıklıdır.

Konsensus (Mutabakat)

Blok zinciri eşler arasında paylaşılan, senkronize bir geçmiş defteri olarak tasarlanmıştır, resmi kayda neyin dahil edilip edilmeyeceği konusunda bir noktada nihai bir karar verilmesi gerekir. Blok zinciri merkezi olmadığından, bir blok zinciri bloğunun içeriğini onaylayacak ve son haline getirecek bir "üst otorite" yoktur. ("Blockchain Consensus and Fault Tolerance In a Nutshell", TY) Satoshi Nakamoto, kimsenin aynı Bitcoin'i iki kez harcamamasını sağlamak için Bitcoin ağı için PoW-Proof of Work ("Emeğin İspatı") adlı fikir birliği algoritmasını oluşturmuştur. O zamandan sonra, farklı kullanım durumlarına uyacak şekilde birkaç başka mutabakat algoritması da icat edilmiştir. Bunlara PoS-Proof of Stake ("Sahipliğin İspatı"), DPoS-Delegated Proof of Stake ("Yetkilendirilmiş Sahipliğin İspatı"), PBHT ("Pratik Bizans Hata Toleransı") ve PoET-Proof of Elapsed Time ("Geçen Süre İspatı") dahil edilebilir. En yaygın kullanılan mutabakat algoritmaları Emeğin İspatı ve PoS-Proof of Stake ("Sahipliğin İspatı") olarak bilinmektedir.

Emeğin İspatı'nda, blok zinciri ağındaki bir sonraki bloğu oluşturmak isteyen kullanıcılar olan madenciler bir blok madenciliği hakkını kazanmak için "zor" bir kriptografik probleme kabul edilebilir bir çözüm bulmak için yarışırlar ("Blockchain Consensus and Fault Tolerance in a Nutshell", TY). Emeğin İspatı mutabakatının güvenliği, hiç kimsenin bir blok zincirin madencilik ağının hesaplama kaynaklarının yarısından fazlasını kontrol etmediği varsayımına dayanmaktadır. Madencilik çabasının %51'ini bir kuruluş kontrol ediyorsa, mutabakatı o kontrol eder. Kontrolü ele geçirmek; ekipman ve enerjiye, sistemi dolandırmaktan elde edilecek olandan daha büyük bir yatırım gerektirecektir.

Sahipliğin İspatı, Emeğin İspatı sistemlerine bir dizi iyileştirme getirir. Daha az enerji gerektirir ve blok oluşturmak için özel bir donanım gerekmediğinden daha düşük giriş engeline sahiptir. Sahipliğin İspatı, bir sonraki bloğu oluşturan düğümün seçildiği blok zincirini doğrulamak ve blok eklemek için kullanılan başka bir yöntemdir ("Proof of stake versus proof of work", 2022). Bu mutabakat modelinde bir düğüm sistemde ne kadar hisseye sahip olduğuna dayanarak blokları ekler ve doğrular. Böylece, sahiplik(mülkiyet) aktörlerin dürüst davranmasına yol açacaktır, aksi takdirde dürüst olmayan davranışlarda bulunurlarsa hisselerini kaybedeceklerdir (Faber, Michelet, Weidmann, Mukkamala ve Vatrapu, 2019).

Etheryum Toronto'dan bir Rus-Kanadalı girişimci ve programcı olan Vitaly Dmitriyevich "Vitalik" Buterin'in teknik incelemesinde tanıtılmıştır (Buterin, 2014).

Uzun süre Emeğin İspatı mutabakat modelini kullanmıştır. Buterin, Bitcoin kodunu "çatalladığı" veya kopyaladığı, iyileştirmeler yaptığı ve Etheryum blok zincirini yarattığı zaman ikinci en büyük kripto para birimini hayal etmiştir. Bu yeni blok zinciri sadece bir para birimi değişim sistemi değil, aynı zamanda Etheryum Sanal Makinesi ile birlikte programcılar tarafından geliştirilmeye açık, birbirine bağlı, Turing tamlığına sahip bir bilgisayardır. Akıllı sözleşmelerin yürütülebileceği ve üzerine uygulamaların oluşturulabileceği bir platform oluşturur. Etheryum her zaman Emeğin İspatı mutabakat mekanizmasından uzaklaşmayı planlamıştır ve nitekim 2022'de "Birleşme" ("The Merge") olarak adlandırılan olayda, Etheryum tüm ağını değişim ve iyileştirme vaatleriyle birlikte gelen Sahipliğin İspatı mekanizmasına geçirmeyi planlamıştır. "Birleşme", Sahipliğin İspatı'na geçişte ilk adım olup tamamen Sahipliğin İspatı tabanlı bir ağ olarak işlemlerine devam edebilmesi için önünde başarılı bir şekilde gerçekleşmesi gereken sırasıyla "Surge" (Kaynaştırma), "Verge" (Sınırlandırma), "Purge" (Temizleme) ve "Splurge" (Tamamlanma) adımları bulunmaktadır (Kurt, 2022).

Şifreleme (Kriptoloji)

Şifreleme (kriptografi), blok zincirindeki bilgilerin güvenilir olmasını sağlamak için blok zincir teknolojisi ile birleştirilir. Daha önce verdiğimiz gerçek dünyadan örneğimizdeki müzik paylaşım şirketleri yalnızca telif hakkı ihlalinden kaynaklanan yasal sorunlar yaşamakla kalmayıp aynı zamanda veri bütünlüğü sorununu da çözememişlerdir. Bu platformlardan indirilen müzik, ancak onu saklayan ve gönderen anonim kişi kadar güvenilir olmuştur. Verilerin bütünlüğü yoktu. Kriptografi ve blok zinciri, bir şeyin doğru olduğunu kanıtlamanın güvenli bir yolunu sunar. Burada üçüncü taraflara güvenmek yerine, verilen bir onayın kaynağını ve gerçekliğini kanıtlayan kriptografik algoritmalara güven duyulur.

Blok zincir Teknolojisinde Kullanılan Şifreleme Türleri

Açık Anahtar Şifreleme

Açık anahtar kriptografisi, farklı görevleri gerçekleştirmek için bir açık anahtar ve bir özel anahtar çifti kullanır. Açık anahtarlar yaygın şekilde dağıtılırken, özel anahtarlar gizli tutulur. Bir kişinin açık anahtarını kullanarak bir mesajı şifrelemek mümkündür, böylece yalnızca özel anahtara sahip kişi şifresini çözebilir ve okuyabilir. Özel anahtar kullanılarak dijital imza oluşturulabilir, böylece ilgili açık anahtara sahip olan herkes mesajın özel anahtarın sahibi tarafından oluşturulduğunu ve o zamandan beri değiştirilmediğini doğrulayabilir.

Sıfır Bilgi Kanıtları

Sıfır bilgi kanıtları (ZKP), özel bilgilerin çevrimiçi ortamda yaygın olarak iletilmesine gerek kalmadan tarafların kimliklerini doğrular. ZKP, bir tarafın (kanıtlayıcı) başka bir tarafa (doğrulayıcı) herhangi bir ek bilgi iletmeden belirli bir ifadenin doğru olduğunu kanıtlamasına olanak tanıyan bir kriptografik yöntemdir.

Özet Değer Fonksiyonları

Bu şifreleme türü anahtar kullanmaz. Sabit uzunlukta bir özet değeri oluşturmak için bir şifre kullanır. Fonksiyon, boyutu önemli olmayan düz bir metni sabit boyutlu bir özet değere dönüştürür. Düz metnin içeriğinin şifreli metinden bulunması neredeyse imkansızdır. Bunu bir parmak izinden bir insanı yeniden yaratmaya çalışmak gibi düşünürsek, bir parmak izi, insanın boyutu ne olursa olsun bir insanı benzersiz bir şekilde temsil eder ve insanı yeniden yaratmak için bir parmak izini tersine mühendislik yapılamaz.

Merkle Ağaçları

Blok zincirlerini depolamak için verileri sıkıştıran veya paketleyen müdahaleye karşı dayanıklı bir bileşene sahip bir veri depolama tekniğidir. Merkle ağaçları, müdahaleye dayanıklı bir veri depolama modeli oluşturmak için her bir özet değerin bir sonraki özet değerin bir parçası haline geldiği özet değer ilkeleri üzerine inşa edilmiştir.

Şeffaflık ve Değişmezlik

Merkezi sistemlerde şeffaflık yoktur, deftere ait bilgiler tek bir otorite tarafından kontrol edilir. Bir blok zincirinde, paylaşılan veya dağıtık defterde gerçekleşen tüm işlemler görülebilir. Bir blok zinciri, ilk transferden bu yana gerçekleşen her işlemin ayrıntılarını saklar. Blok zinciri, tüm geçmişi görünür ve değiştirilemez olacak şekilde tasarlanmıştır. Blok zincirindeki işlemler oluşturulduktan sonra değiştirilemez ve tüm geçmişleri herkese açık olarak görülebilir. Bu, blok zincirinin bütünlüğünün herhangi bir kullanıcı tarafından kolayca doğrulanabilir olması gibi faydalı bir özelliğe sahip olan tamamen şeffaf bir veri yapısı olduğu anlamına gelir.

Programlanabilir Olma

Bazı blok zincirler, sisteme mantık kavramını aşılayan ek bir özellik olarak **"akıllı sözleşmeleri"** sunar. Bitcoin blok zincirini finansal işlemleri kaydeden bir hesap makinesi olarak düşünürsek bu blok zincirleri de bilgisayarlar olarak düşünebiliriz. Bu blok zincirlerden ilki olan Etheryum, dijital anlaşmalar veya akıllı sözleşmeleri uygulama yeteneğine sahip olan EVM'yi (Etheryum Sanal Makinesi'ni) çalıştırır. Akıllı sözleşme, sözleşmeye dayalı anlaşmaları uygulayabilen bir blok zinciri üzerinde çalışan bir programdır. Tipik olarak, belirli bir dizi kuralı uygulayan dijital anlaşmalar olarak çalışırlar. Bu kurallar, tüm ağ düğümleri tarafından çoğaltılan ve çalıştırılan bilgisayar kodu tarafından önceden tanımlanmıştır. Blok zincir akıllı sözleşmeleri, güvenilir olmayan protokollerin oluşturulmasına izin verir. Bu, iki tarafın birbirini tanımak veya güvenmek zorunda kalmadan blok zinciri aracılığıyla taahhütlerde bulunabileceği anlamına gelir. Şartlar yerine getirilmezse sözleşmenin uygulanmayacağından emin olabilirler. Bunun dışında akıllı sözleşmelerin kullanılması, aracılara olan ihtiyacı ortadan kaldırarak işlem maliyetleri önemli ölçüde azaltabilir.

Blok Zincir Türleri

Genel ve İzinsiz Blok zincirler

Halka açık blok zincirleri, ağ üzerinde kimsenin kontrol sahibi olmadığı merkezi olmayan blok zincirlerdir. Bu değişmez ve sansüre dirençli ağlar, birbirine güvenmeyen, ancak yine de bir ağda etkileşime giren ve fikir birliğine katılan katılımcılar için idealdir. Halka açık blok zincirler izinsizdir. Herhangi biri etkin bir şekilde blok zincir ağına katılabilir. Kimsenin katılması yasak değildir. Bitcoin ve Etheryum, halka açık ve izinsiz blok zincirlerinin örnekleridir.

Özel ve İzinli Blok zincirler

Özel blok zincirler, bir kullanıcının kabul edilmeden önceki ağ üzerindeki haklarını tanımlar. Deftere kimlerin yazabileceği ve hangi işlemlere katılabilecekleri gibi faaliyetlere kısıtlamalar getirilir. İzinli bir blok zincirinde, katılıma bir kuruluş veya bir kuruluşlar konsorsiyumu tarafından izin verilir. Bu yetkilendirilmiş kurum, ağ üzerindeki belirli işlemlere ve mutabakata kimlerin katılabileceğini tanımlar.

Hyperledger ve Corda blok zincirleri özel ve izinli blok zincirlerine örnektir.

Blok Zincirde Yönetim

Bitcoin'de Yönetim

Bitcoin, madencileri ağa blok eklemeye teşvik etmek için Emeğin İspatı modelini kullanır. Bu, blok zincirinin işlemlerini yönetir. Ancak değişiklik yapılması gerektiğinde ne olur? Bunlar nasıl uygulamaya konur? Bitcoin topluluğu üç ana oyuncudan oluşur: geliştiriciler, madenciler ve kullanıcılar. Bu katılımcıların hiçbiri beklenmedik durumlar ortaya çıktığında acil durum kararları alma yeteneğine sahip değildir. Bitcoin, kararların geliştiriciler, madenciler ve kullanıcılar tarafından dengelendiği zincir dışı yönetim modelini kullanır. Blok zincirinde, geliştiriciler blok zincirini değiştirmek için kodu yazmalıdır. Madencilerin ve kullanıcıların onayı olmadan, geliştiricilerin değişikliği uygulamak için hiçbir yolu yoktur. Madenciler ve kullanıcılar yeni yazılım değişikliklerini uygulamayı seçmelidir.

Etheryum'da Yönetim

Bitcoin gibi, Etheryum'un üç ana oyuncusu (geliştiriciler, madenciler ve kullanıcılar) işlevselliği geliştirmek için kodu güncellemelidir. Ethereum Improvement Proposals (EIPs), Etheryum için potansiyel yeni özellikleri veya süreçleri belirten standartlardır ("EIP's", 2023). EIP'ler önerilen değişiklikler için teknik özellikler içerir ve topluluk için gerçeğin kaynağı ("source of truth") olarak hareket eder. Etheryum Yorum Talebi ERC-20 ("Ethereum Request for Comment"), Etheryum protokollerine dayalı olarak blok zincirinde yardımcı program belirteçleri ("utility token") yayınlama standartlarını tanıtmıştır ("ERC-20.",2023). The Beacon Chain ("The Beacon Chain", 2023), Sahipliğin İspatı mutabakat modelini ve parçalama ("sharding") kavramını tanıtmıştır. Parçalama, ağdaki tıkanıklığı hafifletmek için paralel yan zincirler çalıştırma kavramıdır. The Berlin Hard Fork ("The Berlin Hard Fork", 2021) ve The London Fork ("The London Fork.", 2019) madencilere ödenen ücretleri stabilize etmek için yapılan iyileştirmelerdir, böylece bu ücretler Ether fiyatı ile dalgalanmaz.

Nihayetinde Etheryum, blok zinciri yönetiminin "ömür boyu hayırsever diktatör modeli"ni kullanır. Etheryum için kullanıcı girdileri ve geliştirme ekibinden gelen girdiler memnuniyetle karşılanırken, Vitalik Buterin Etheryum yol haritasına ilişkin kararlarda nihai yetkilidir.

Hyperledger'da Yönetim

Hyperledger, Linux Vakfi tarafından onaylanan açık kaynaklı bir blok zinciri projesi olarak tanıtılmıştır. ("Hyperledger", 2016) Brian Behlendorf tarafından yönetilen projenin misyonu, dağıtılmış defter teknolojisini kurumsal düzeyde teşvik etmek için topluma araçlar ve eğitim sağlamaktır. Hyperledger çerçeveleri, Hyperledger ortamına ilişkin teknik kararlar almak için "Açık Yönetim" modelini kullanır.

Hyperledger Teknik Yönlendirme Komitesi (The Hyperledger Technical Steering Committee-TSC) ("Leadership", 2022) Hyperledger'daki teknik kararlar için nihai otoritedir. TSC her yıl Hyperledger ortamının aktif katkıda bulunanları ve uygulayıcıları arasından seçilir. Katkıda bulunanlar ve uygulayıcılar kendilerini on beş kontenjan için potansiyel aday olarak sunabilir ve kontenjanlar aynı grup tarafından yapılan oylamaya göre doldurulur. Bu model, Hyperledger geliştirme topluluğunda aktif bir role sahip olanların, bu topluluğun nasıl yönetileceği konusunda söz sahibi olmalarını sağlamak üzere tasarlanmıştır.

Corda'da Yönetim

Corda iş dünyası için tasarlanmış açık kaynaklı bir blok zinciri projesidir ("Corda", 2022). Kurumsal bir blok zincir yazılım firması olan R3 tarafından 200'den fazla teknoloji ve endüstri ortağı ile iş birliği içinde geliştirilmiştir. Corda platformu 2017 yılının Eylül ayında başlatılmıştır. Corda ayrıca blok zincirinin geleceğine ilişkin teknik kararlar almak için bir "Açık Yönetim" modeli kullanmaktadır. "Corda Ağı Yönetim Kurulu", Corda ağındaki tüm kullanıcıların çıkarlarını temsil etmek üzere seçilmiştir (Linux Foundation, 2022).

KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN BLOK ZİNCİR TEKNOLOJİSİ

Blok zinciri ve veri koruma hukuku arasındaki gerilim noktalarının çoğu iki ana faktörden kaynaklanmaktadır. Birincisi, veri koruma hukuku, her bir kişisel veri noktasıyla ilgili olarak, ilgili kişilerin ilgili veri koruma yasası kapsamındaki haklarını kullanmak için başvurabilecekleri en az bir gerçek veya tüzel kişi veri sorumlusu olduğu varsayımına dayanmaktadır. Bu veri sorumluları ilgili yasaların yükümlülüklerine uymak zorundadır. Ancak blok zincirleri, genellikle tek bir aktörün yerine birçok farklı oyuncuyu koyarak ademi merkeziyetçiliği sağlamaya çalışan dağıtık veri tabanlarıdır. Veri sorumluluğunun (ortak veya değil) nasıl tanımlanması gerektiği konusunda fikir birliği olmaması, sorumluluk ve hesap verebilirliğin tahsisini engellemektedir (Avrupa Parlamentosu Araştırma Dairesi

[EPRS], 2019). İkinci olarak, veri koruma hukuku yasal gerekliliklere uymak için gerekli olduğunda verilerin değiştirilebileceği veya silinebileceği varsayımına dayanmaktadır. Ancak blok zincirleri, veri bütünlüğünü sağlamak ve ağa olan güveni artırmak adına verilerin tek taraflı olarak değiştirilmesini bilinçli olarak zor hale getirmektedir. Bunun yanında blok zincirleri, veri ekonomisinin mevcut biçiminde veri minimizasyonu ve amaç sınırlaması gerekliliklerine uymanın zorluklarının altını çizmektedir.

EPRS'in bu konudaki çalışması Avrupa veri koruma çerçevesini incelemekte ve bu gerilimleri belgelemek amacıyla blok zinciri teknolojilerine uygulamaktadır. Ayrıca blok zincirinin veri koruma yasasının bazı hedeflerinin ilerletilmesine yardımcı olabileceği gerçeğini de vurgulamaktadır. Bu analiz temelinde somut politika seçenekleri geliştirilmektedir (EPRS, 2019).

Dağıtık defterler ve veri koruma hukuku arasındaki uyumluluk, ilgili blok zincir olayının özel teknik tasarımı ve yönetişim kurulumunu dikkate alan ancak detaylı bir olay bazlı analiz temelinde değerlendirilebilir. Sonuç olarak öğretide blok zincirlerin tamamı ile veri koruma hukuku ile uyumlu veya uyumsuz olduğu şeklinde genel bir sonuca varmanın mümkün olamayacağı, bu şekilde bir sonuca varılabilmesi için daha ziyade teknolojinin her kullanımının kendi esasları dahilinde incelenmesi gerektiği ifade edilmiştir. Bununla birlikte, özel ve izinli blok zincirlerini AB veri koruma yasasıyla uyumlu bir şekilde tasarlamak, genel ve izinsiz ağlara göre daha kolaydır. Bunun nedeni, izinli ağlardaki katılımcıların birbirleri tarafından biliniyor olması ve bu sayede örneğin sorumluluğun uygun bir şekilde dağıtılmasını sağlayan sözleşmeye dayalı ilişkilerin tanımlanabilmesidir. Ayrıca, bu ağlar, genel ve izinsiz ağların aksine, ağ üzerinde kontrol sağlayacak şekilde tasarlanmış ve hangi aktörlerin verilere erişebileceği üzerinde bir kontrol söz konusudur (EPRS, 2019).

Blok zincirleri, güvenilir bir merkezi aracıya ihtiyaç duymadan veri paylaşımını mümkün kılacak şekilde tasarlanabilir, verilere kimin eriştiğine dair şeffaflık sunar ve ayrıca blok zinciri tabanlı akıllı sözleşmeler veri paylaşımını otomatikleştirerek işlem maliyetlerini de azaltabilir. Bu özellikler, örneğin kurumlar arası veri paylaşımını kolaylaştırarak veri pazarlarını desteklemek, ki bu da yapay zekanın gelişimini destekleyecektir, çağdaş veri ekonomisine daha geniş çapta fayda sağlayabilir. İlgili kişilerin kendilerini doğrudan veya dolaylı olarak ilgilendiren kişisel verileri üzerinde daha fazla kontrol sahibi olması gibi veri koruma yasalarının ulaşmaya çalıştığı bazı amaçlarını desteklemesi adına bu teknolojilere güvenilebilir. Bu gerekçe, ilgili kişilere kişisel verileri ile ilgili diğer kişilerin ne yaptıkları ve kendi kişisel verileri ile ilgili olarak kendilerinin ne yapabileceği üzerinde kontrol

sahibi olmalarını sağlayan erişim hakkı (Bkz. GVKT Madde 15) veya veri taşınabilirliği hakkı (Bkz. GVKT Madde 20) gibi ilgili kişi hakları temelinde gözetilebilir.

Blokların kendileri, blokta yer alan tüm işlemlerin bir özet değerini ('parmak izi'), bir zaman damgasını ve sıralı blok zincirini oluşturan önceki bloğun bir özet değerini içeren farklı veri türlerinden oluşur (Antonopoulos, 2017, s. 25). Bu verilerin bazıları veri koruma yasasının amaçları doğrultusunda kişisel veriler olarak nitelendirilir. Bloklar sürekli olarak eklendiği ancak asla kaldırılmadığı için bir blok zinciri yalnızca eklenebilir veri yapısı olarak değerlendirilir. Kriptografik özet zincirleme logu, şeffaflığı ve hesap verebilirliği arttıracak şekilde "müdahaleye karşı korumalı" (tamper-evident) hale getirir (Felten, 2018). Gerçekten de bir bloğu diğerine bağlayan özet değer nedeniyle bir bloktaki değişiklikler o bloğun yanı sıra sonraki tüm blokların özet değerini de değiştirir. Dağıtık defter teknolojilerinin ("DDT") yalnızca ekleme özellikli yapıları nedeniyle, veri koruma yasalarının gereklerinden olan verilerin değiştirilmesi ve silinmesi hususları bazı koşullar altında doğrudan uygulanamayacaktır. Blok zinciri ağları kopyalayarak çoğaltma yoluyla dayanıklılık(direnç) elde eder. Defterin verileri aynı anda birçok düğümde depolandığı için dayanıklıdır, böylece bir veya birkaç düğüm başarısız olsa bile veriler etkilenmez. Bu tür bir kopyalama, donanım düzeyinde merkezi bir arıza veya saldırı noktası olmamasını sağlar. Bloklarda depolanan kopyalanmış veriler, merkezi bir kontrol noktasının yokluğunda dağıtık ağın defterin mevcut durumu üzerinde anlaşmaya varmasını sağlayan bir mutabakat protokolü aracılığıyla senkronize edilir. Bu süreç ile veriler, sıradaki blokları değiştirmeden verileri değiştirmeyi zorlaştıracak bir şekilde kronolojik olarak sıralanır.

Blok zincirleri yalnızca veri depolarken, bu veriler temsil ettiğine inandığımız ve kabul ettiğimiz her şeyi temsil edebilir. Bitcoin esasında değerli olan bir veridir çünkü insanlar böyle olduğuna inanmaya başlamıştır. Benzer şekilde, zaman içinde bir mal, hizmet veya hakkı temsil etmek üzere alınan ham veriler olan diğer dijital varlık biçimleri ortaya çıkmıştır. Blok zinciri tabanlı varlıklar tamamen zincir içi değere sahip olabilir (Bitcoin'de olduğu gibi) ya da gerçek dünyadaki bir varlığın bir avatarı olabilir, ister bir mal (örneğin bir bisikleti temsil eden bir token), bir hizmet (saç kesimi için bir kupon gibi) veya bir hak (yasal bir hak gibi) (Cortese, 2016). 2018 yılında Avrupa Parlamentosu tarafından yapılan bir araştırmaya göre 2035 yılına kadar vergi raporlaması, e-kimlik veri tabanları, oylama planları blok zinciri veya başka bir DDT biçimi üzerinde çalışabilir.

Blok zincirleri, merkezi olmayan bir şekilde güncellenen kopyalanmış bir veri tabanı (örneğin kripto varlıklardaki işlemleri kaydetmek veya bilgileri kaydetmek için kullanılabilen) ve aynı zamanda yazılımın merkezi olmayan bir şekilde ça-

lıştırılması için bir altyapı sunar. Örnekler arasında akıllı sözleşmeler veya 'merkezi olmayan uygulamalar' (altta yatan ağın merkezi olmayan yapısını yansıtan uygulamalar) yer almaktadır. Bu uygulamalar çok çeşitli şekillerde olabilir ve çok çeşitli kullanım durumları sunabilir. Buna ek olarak, merkezi olmayan uygulamaların oluşturulması ve sürdürülmesi için kendi protokollerini hayata geçiren merkezi olmayan uygulama çerçeveleri gibi ara katmanlar da olabilir. Verilen bir blok zincirin GVKT ile uyumluluğu değerlendirileceği zaman, örneğin bu çeşitli katmanlarda farklı veri sorumluları yer alabileceğinden bu çok katmanlı yapı akılda tutulmalıdır (Avrupa Parlamentosu [AP], 2018a).

Teknolojinin yıkıcı doğasına ilişkin tahminlere rağmen, şu anda bu konuda çok az somut uygulama bulunmaktadır ve blok zinciri teknolojisinin gelecekte pratik bir etkiye sahip olup olmayacağını, nerede ve ne şekilde olacağını tahmin etmek zordur. Şu anda blok zincirleri ciddi teknik ve prosedürel sınırlamalardan mustarip oldukları için olgunlaşmamış durumdadır. Bu eksiklikler arasında en belirgin olanı, geniş çaplı kullanım için gerekli olan ölçeklenebilirlik eksikliğidir. Blok zincirlerinin, her tam düğümün her işlemi işlemesi ve tüm mevcut durumun bir kopyasını tutması gerektiğinden tasarım olarak verimsizdir. Bu süreç tek hata noktasını ortadan kaldırıp güvenlik avantajları sunsa da verimi düşürmekte ve işlemleri yavaşlatmaktadır. Bu sorunun dağıtık defterlerin boyutu büyüdükçe de artması muhtemeldir. Ölçeklenebilirlik, her yeni işlemin ağın büyümesine neden olduğu, sadece ekleme yapılabilen ve dolayısıyla sürekli büyüyen bir veri tabanında önemli bir endişe kaynağı oluşturmaktadır (EPRS, 2019).

Blok zincirde Tutulan Kişisel Veri Örnekleri

Açık Anahtarlar

Blok zinciri bağlamında, açık anahtarlar GVKT'nin 30'uncu maddesi kapsamında bahsedilen türden tanımlayıcılar olarak hizmet vermektedir. Blok zincirleri asimetrik şifreleme ile iki aşamalı bir doğrulama sürecine dayanır. Her kullanıcı, kullanıcıyı temsil eden harf ve rakamlardan oluşan bir dizi şeklinde bir genel anahtara sahiptir. Bu anahtar işlemleri yapmak için başkalarıyla paylaşılan bir hesap numarası olarak düşünülebilir. Buna ek olarak, her kullanıcı yine harf ve rakamlardan oluşan bir dizi olan bir özel anahtara sahiptir. Bu da başkalarıyla asla paylaşılmaması gereken bir şifre olarak düşünülebilir. İki anahtar arasında da özel anahtarın genel anahtar tarafından şifrelenmiş verilerin şifresini çözebildiği matematiksel bir ilişki vardır.

İşlemsel Veriler

'İşlemsel veriler', blok zincirlerinde kullanılabilecek ancak açık anahtar olmayan diğer veri kategorileri için kullanılan terminolojidir. Fransa Veri Koruma Otoritesi CNIL'e göre bu, bir diploma veya mülk tapusu gibi bir işlem dahilindeki verileri ifade eder (Commission Nationale de l'Informatique et des Libertés, [CNIL], 2018). Örneğin, işlemsel kişisel veriler belirli bir işlemin yükünde (payload) bulunan ad, adres veya doğum tarihi olabilir.

İşlemsel verilerin GVKT'nin kişisel veri tanımını karşılayıp karşılamadığını belirlemek için olay bazında bir analiz yapılmalıdır. Bazı durumlarda, işlemsel veriler açık bir şekilde kişisel veri olarak nitelendirilemez. Örneğin, blok zincirlerinin veri paylaşımı için kullanılan bir veri altyapısı olarak hizmet verdiği durumlarda katılımcılar arasında uzaydan gelen iklim sensörü verileri, kişisel veri olmayabilir. Ayrıca, A'dan B'ye aktarılan bir kripto varlığın satın alınan ürün veya hizmeti tanımlayan ek bilgilerle birleştirilerek kimliğin belirlenmesine yol açabildiği durumlar haricinde kişisel veri olarak nitelendirilmesi olası değildir (Bacon, Michels, Millard ve Singh, 2017). Ancak örneğin, bir grup bankanın "Müşterinizi Tanıyın" (KYC) verilerini paylaşmak için DDT kullandığı durum gibi bazı diğer durumlarda, bu tür veriler kişisel veri olarak nitelendirilebilir.

CNIL'e göre bir blok zinciri aşağıda sıralanan iki kategoride kişisel veri içerebilir: **katılımcıların ve madencilerin tanımlayıcıları ile ek veriler (yük).** Her katılımcının bir dizi alfa numerik karakterden oluşan bir tanımlayıcısı vardır. Bunlar rastgeledir ve katılımcının hesabının açık anahtarını oluşturur. Bu açık anahtar yalnızca katılımcı tarafından bilinen bir özel anahtarla bağlantılıdır. Blok zincirleri mimarisinde bu tanımlayıcılar her zaman görünürdür, çünkü bunlar onun düzgün şekilde işlemesi için gereklidir. Bu nedenle CNIL, bu verilerin daha fazla minimize edilemeyeceği ve bunların saklama sürelerinin özleri itibariyle blok zincirinin yaşam süresiyle uyumlu olduğu kanaatindedir. Katılımcıların tanımlayıcılarının yanı sıra, blok zincirinde depolanan ek veriler, potansiyel olarak katılımcılar ve madenciler dışındaki bireylerle ilgili olabilecek kişisel veriler içerebilir. Tasarımda mahremiyet ilkesi (Bkz. GVKT Madde 25.), veri sorumlusunun bireylerin hak ve özgürlükleri üzerinde en az etkiye sahip formatı seçmesini gerektirir.

CNIL, kişisel verilerin tercihen bir taahhüt şeklinde blok zincirine kaydedilmesi gerektiğini düşünmektedir. Burada "taahhüt", bir kişinin verileri, her iki taraf için de ek bilgilerle neyin dondurulduğunu kanıtlamanın ve sadece bu "taahhüt" kullanılarak bu verileri bulmanın veya tanımanın imkânsız olduğu bir şekilde

"dondurulmasını" sağlayan kriptografik bir mekanizmadır. Bu mümkün değilse, veriler bir anahtar ile bir özet değer fonksiyonu kullanılarak oluşturulan bir özet değer şeklinde veya en azından yüksek düzeyde gizlilik öngören bir şifreleme şeklinde kaydedilebilir. Bu çözümlerden bazılarının altında yatan ortak özellik, herhangi bir veriyi blok zincirinin dışında açık metin olarak saklamak (örneğin, veri sorumlusunun bilgi sistemi gibi) ve blok zincirinde yalnızca verilerin varlığına dair bir kanıt saklamaktır (örn. taahhüt, özet değer anahtarlı bir özet değer fonksiyonundan üretilen bir özet değer, vb.). İşleme amacı tarafından gerekçelendiriliyorsa ve bir Veri Koruma Etki Değerlendirmesi (DPIA) kalan risklerin kabul edilebilir olduğunu kanıtlamışsa, kişisel veriler istisnai olarak blok zincirinde, geleneksel bir parmak izi şeklinde (anahtarsız) veya hatta açık metin olarak saklanabilir. Esasında, bazı veri sorumlularının bazı bilgileri saklama süresi olmaksızın kamuya açık ve erişilebilir yapmak için yasal yükümlülüğü olabilir: bu özel durumda, kişisel verilerin halka açık bir blok zincirinde depolanması, DPIA'nın ilgili kişilere yönelik risklerin asgari düzeyde olduğu sonucuna varması koşuluyla öngörülebilir.

Blok zincir Tabanlı Kişisel Veri İşlemede Veri Sorumluları ve Veri İşleyenler

Özel ve/veya İzinli Blok Zincirlerinde

Özel ve/veya izinli DDT'de, kişisel veri işleme araçlarını ve çoğu durumda amaçlarını da belirleyen genellikle belirli bir tüzel kişilik (örneğin bir şirket veya konsorsiyum) bulunur. Bu durumda, bu kuruluş veri sorumlusu olarak nitelendirilir. Ancak bu tür durumlarda ortak veri sorumluları da olabilir. Wirtschaftsakademie Schleswig Holstein davası ile uyumlu olarak, bu tür bir altyapıyı kendi amaçları için kullananların ortak veri sorumlusu oldukları iddia edilebilir. Wirtschaftsakademie Schleswig-Holstein davasında özel bir eğitim kurumu Facebook'u kullanarak sözde bir hayran sayfası oluşturmuştur (Wirtschaftsakademie Schleswig-Holstein, 2018). Kullanıcılar bu sayfayı ziyaret ettiklerinde, Facebook veya okul tarafından bu konuda bilgilendirilmeksizin bilgisayarlarına bir çerez yerleştirilmiştir. Sonuç olarak, yerel veri koruma otoritesi, okula hayran sayfasını devre dışı bırakması talimatını vermiştir. Mahkeme, kararında ilgili kişilerin etkili ve eksiksiz bir şekilde korunmasını sağlamak adına ortak veri sorumluluğunun geniş bir şekilde yorumlanmasının önemini vurgulamıştır (Wirtschaftsakademie Schleswig-Holstein, 2018). Buna bir örnek, aynı tedarik zincirinin parçası olan birçok aktör arasında kurulan bir konsorsiyum blok zinciri olabilir. Konsorsiyum tarafından oluşturulan tüzel kişiliğin, veri işleme amaç ve araçları üzerinde önemli bir kontrole sahip olduğu göz önünde bulundurulduğunda bir veri sorumlusu olacağı açıktır. Bununla birlikte, konsorsiyuma katılan ve daha sonra altyapıyı

kendi amaçları için kullanan ve dolayısıyla DDT'nin yeni kişisel veriler işlemesine yol açan şirketlerin her biri de ortak veri sorumlusu olarak nitelendirilebilecektir. Bir grup katılımcı ortak bir amaçla veri işleme faaliyetlerini gerçekleştirmeye karar verdiğinde, veri sorumlusunun önceden belirlenmesi tavsiye edilmektedir. Örneğin katılımcılar dernek veya ekonomik çıkar grubu şeklinde bir tüzel kişilik oluşturabilir. Ayrıca, grup adına karar verecek bir katılımcı belirlemeyi ve söz konusu katılımcıyı veri sorumlusu olarak atamayı da seçebilirler (EPRS, 2019).

Akıllı sözleşmelere ilişkin olarak, herhangi bir yazılımda olduğu gibi, algoritma geliştiricisi sadece bir çözüm sağlayıcısı olabilir veya söz konusu algoritma geliştiricisi işlemeye katıldığında, işlemenin amaçlarını belirlemedeki rolüne bağlı olarak bir veri işleyen veya veri sorumlusu olarak nitelendirilebilir.

Halka Açık ve İzinsiz Blok Zincirlerinde

Veri sorumlusunun kimliğinin benimsenen bakış açısına bağlı olduğunu vurgulamak önemlidir. Makro düzeyde bakıldığında, işlemenin amacı 'ilgili hizmeti sağlamak' (Bitcoin işlemi gibi) iken 'araçlar' düğümler ve madenciler tarafından kullanılan yazılımla ilgilidir. Mikro açıdan bakıldığında (bireysel işlem açısından) işlemenin amacı 'belirli bir işlemi blok zincirine kaydetmek' iken araçlar 'blok zinciri platformunun seçimine' atıfta bulunmaktadır. Veri koruma hukuku belirli kişisel veri öğeleriyle ilgilendiğinden, mikro düzey daha uygun bir yaklaşım olarak değerlendirilebilir (Bacon ve diğerleri, 2017). CNIL' e göre, **zincir üzerine yazma hakkına sahip olan katılımcılar** ve madenciler tarafından doğrulanmak üzere veri göndermeye karar verenler veri sorumlusu olarak kabul edilebileceklerdir. Esasında, blok zinciri katılımcıları işleme amaçlarını ve işleme araçlarını (veri formatı, blok zinciri teknolojisinin kullanımı, vb.) tanımlar. Daha açık bir ifadeyle**, katılımcının gerçek bir kişi olması ve kişisel veri işleme faaliyetinin profesyonel veya ticari bir faaliyete ilişkin olması (faaliyet kesinlikle kişisel olmadığında)** ile **katılımcının tüzel kişi olması ve kişisel verileri bir blok zincirine kaydetmesi** durumlarında veri sorumlusu olabileceği değerlendirilmektedir.

Örneğin, bir noter müşterisinin mülk tapusunu bir blok zincirinde kaydederse, söz konusu noter bir veri sorumlusudur. Buna ek olarak, eğer bir banka müşteri yönetimi işlemlerinin bir parçası olarak bir blok zincirine müşterisinin verilerinin girişini yapıyorsa bir veri sorumlusudur.

Madenciler protokolü çalıştırır, paylaşılan deftere veri ekleyebilir ve defterin (genellikle tam) bir kopyasını makinelerinde saklayabilir. Madencilerin etkilerinin işlemenin 'amaç ve araçlarını' belirleyecek kadar ileri gidip gitmediği konusunda

bir tartışma vardır. Madenciler, protokolün hangi versiyonunun çalıştırılacağını seçerek araçlar üzerinde önemli bir kontrol uygulamaktadır. Ancak, araç kriterinin 'amaç' kriterine göre ikincil konumda olması ve madencilerin belirli bir işlemin amaçlarını belirlemediği düşünüldüğünde, veri sorumlusu olarak nitelendirilmeleri olası değildir. Bu konuda CNIL görüşüne baktığımızda, madenciler yalnızca katılımcılar tarafından gönderilen işlemleri onaylar ve bu işlemlere dahil olmazlar. Bu nedenle, işleme faaliyetinin amaçlarını ve araçlarını tanımlamazlar. Ayrıca, "tamamen kişisel veya hane halkı faaliyeti " olan faaliyetleri hariç tutan GVKT Madde 2'ye uygun olacak şekilde, blok zincirine mesleki veya ticari bir faaliyete işaret etmeyen kişisel verileri giren gerçek kişiler veri sorumlusu kabul edilmeyecektir (CNIL, 2017).

Örneğin, kendi adına Bitcoin alan veya satan bir gerçek kişi veri sorumlusu değildir. Ancak, bu işlemlerin diğer gerçek kişiler adına profesyonel veya ticari bir faaliyetin parçası olarak gerçekleştirilmesi halinde söz konusu kişi bir veri sorumlusu olarak kabul edilebilecektir.

Düğümler bir blok zincirinin tam ya da kısmi bir kopyasını saklayan ve yeni blokların doğrulanmasına katılan bilgisayarlardır. Düğümlerin belirli bir blok zinciri ağını seçmede (veya başlatmada) eşit etki ve özgürlüğe sahip oldukları göz önünde bulundurulduğunda ortak veri sorumluları olarak değerlendirilebilirler ve örneğin gerekli çoğunluk ile bir Fork("Çatal") aracılığıyla kuralları değiştirebilmeleri de ortak kontrolün bir işaretidir (Wirth ve Kolain, 2018).

KVKK Madde 3(1)(1)'de "veri sorumlusu" kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen ve buna ek olarak veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmaktadır. Fakat blok zincir ağının kurulması ve yönetilmesi tek bir elde gerçekleşmemekte, dağıtık bir ağ yapısından söz edilmektedir. Diğer taraftan KVKK dahilinde hali hazırda GVKT'de bulunan **"ortak veri sorumlusu"** kavramı bulunmadığı için tüm katılımcıları ortak veri sorumlusu olarak nitelendirmek de mümkün olamayacaktır (Çekin, 2019). Öte yandan olay bazında yapılan değerlendirmeler sonucunda birden fazla veri sorumlusu tayin etmenin önünde herhangi bir engel bulunmadığı gibi bu durumu destekleyecek şekilde Kişisel Verileri Koruma Kurumu tarafından yayınlanan bir karar da bulunmaktadır (Kişisel Verileri Koruma Kurulu (KVKK), 2021).

Yazılım güncellemeleri söz konusu blok zincirinin madenciler, düğümler veya sikke ("coin") sahipleri gibi diğer aktörleri tarafından kararlaştırılan yönetişim yapısına bağlıdır. Buna göre **yazılım geliştiricilerin** işleme araçlarının belirlenmesinde sınırlı bir rolü vardır ve genellikle belirli bir kişisel veri işleme faaliyetinin amaçları üzerinde hiçbir etkiye sahip değildir. Çünkü yalnızca başkalarının kendi amaçlarını gerçekleştirmek için kullanabilecekleri bir altyapıyı kullanıma sunmaktadırlar. Belirli bir kullanım durumuna ait özel koşullar bu varsayımları değiştirmediği sürece, yazılım geliştiricilerin veri koruma hukuku kapsamında (ortak) veri sorumlusu olarak nitelendirilmesi mümkün görünmemektedir.

DDT kullanıcılarının en azından bazı durumlarda GVKT kapsamında veri sorumlusu olarak kabul edileceği konusunda geniş bir fikir birliği vardır. Bu bağlamda CNIL görüşüne göre iki senaryo ayırt edilmelidir. Bir kullanıcının başkalarının verilerini mi yoksa kendi verilerini işlediği hususlarına bakılması gerekir (EPRS, 2019).

DDT' ye dayanan bir operasyondaki belirli bir kişisel veri işlemeye ilişkin olarak bir **veri işleyen** olup olmadığını tespit etmek için ayrıntılı bir olay bazında değerlendirme yapılmalıdır. Bazı senaryolarda, örneğin harici bir hizmet sağlayıcının blok zinciri altyapısını kullanan bir şirketin veya kamu kurumunun olması durumunda, bir veri işleyenin varlığı muhtemeldir. Bu alt yapı eğer işleme amaç ve aracını belirleyen bir veri sorumlusunun isteklerine uygun olarak kullanılıyorsa bu durumda harici sağlayıcının yalnızca bir veri işleyen olduğundan bahsedilebilir (AP, 2018b). Ayrıca, **kullanıcılar** "deftere yükledikleri kişisel veriler" için veri sorumlusu olarak kabul edilebilecekken "kendi bilgisayarlarında defterin tam bir kopyasını saklamak" suretiyle de veri işleyen sayılabileceklerdir.

Veri işleyenlere örnek olarak dış kaynak kullanan kurumların veri ambarları, bulut hizmet sağlayıcıları veya hizmet olarak yazılım, platform veya altyapı sağlayanları verilebilir ('SaaS', 'PaaS' veya 'IaaS'). Barındırma("hosting") hizmetleri sağlayan internet hizmet sağlayıcıları("ISP") da veri işleyen olarak kabul edilir. Ancak ISP'ler bu tür kişisel verileri kendi amaçları doğrultusunda daha fazla işlemeleri durumunda bir veri sorumlusu haline gelecektir (Madde 29 Veri Koruma Çalışma Grubu, 2010). Dolayısıyla buradan, bir hizmet olarak blok zincirini ('BaaS') sunan şirketlerin de veri işleyen olarak nitelendirilebileceği çıkarımı yapılabilecektir.

Veri sorumlusu-veri işleyen konusuna ilişkin olarak EU Observatory and Forum'un ilgili raporunda da veri sorumlularının ve veri işleyenlerinin tanımlanabildiği ve yükümlülüklerine uyabildiği birçok durum olsa da özellikle blok zinciri işlemleri ilgili kişilerin kendileri tarafından yazıldığında, bir veri sorumlusunu tanımlamanın zor ve belki de imkânsız olduğu durumların da olduğu ifade edilmiştir (EU Blockchain Observatory and Forum, 2018).

CNIL'e göre ise GVKT kapsamında veri işleyenler şunlar olabilir: Veri sorumlusu

katılımcı adına kişisel verileri işleyen akıllı sözleşme geliştiricisi ve bir blok zincirinde kişisel veri içeren işlemi doğrulayan madenciler. Halka açık blok zincirleri konusuna ilişkin olarak ise CNIL'in derinlemesine bir inceleme yürütmekte olduğu katılımcılar/veri sorumluları ile madenciler arasındaki sözleşmeye dayalı ilişkileri ele alacak çözümlerin geliştirilmesini teşvik etmekte olduğu bilinmektedir (CNIL, 2018).

Blok Zincirde Gerçekleşebilecek Kişisel Veri İşleme Faaliyetlerinin Kişisel Veri İşleme Şartları Dahilinde Ele Alınması

KVKK "Tanımlar" başlığı altında Madde 3(1)(a)'ya göre **açık rıza** kavramı, "belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızayı ifade etmektedir. Burada ilgili kişinin yeterince bilgilendirilmesi ve bilgilendirme sırasında kişisel verilerin hangi amaçlarla işleneceği, kimlerle paylaşılacağı gibi hususların somut şekilde belirtilmesi gerekmektedir. Blok zincir ağında ise kimlerin veri işlediği bilinmemektedir. Özünde dağıtık defter teknolojisinin amacı internette anonim kalmak olduğundan verinin kimler tarafından işlendiği ve kimlere aktarılacağı gibi bilgilere ulaşmak, blok zincir teknolojisinde imkânsız görünmektedir. Bununla birlikte, gelecekte ağa katılacak kişilerin belirsiz oluşu ve katılımcıların farklı hukuk düzenlerine tabi olması durumu da mümkündür. Dolayısıyla söz konusu belirsizlikler sebebiyle ilgili kişilerden belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür irade ile açıklanan bir açık rıza alınması yoluna gidilmesi mümkün görünmemektedir. Açık rızanın geri alınması halinde ağda mevcut olan kişisel verilerin silinmesi de blok zincirin yapısal özelliği gereği işlemlerde geçmişe dönük değişiklik yapılamadığı için mümkün görünmemektedir (Çekin, 2019).

Açık rıza haricinde veri işlemenin dayanabileceği şartlardan biri de KVKK Madde(5)(2)(c) 'de belirtilen **"bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması"** hükmüdür. Bu noktada "akıllı sözleşmeler" kapsamında işlenen kişisel verilerin bu işleme şartı bağlamında değerlendirilebileceği mümkün görünmektedir. Ancak ilgili hüküm uyarınca işlenebilecek kişisel veriler yalnızca sözleşmenin taraflarına ait kişisel verilerdir. Ancak blok zincir ağında kişisel veriler sadece sözleşmeye taraf olan düğümlerce değil tüm düğümler ve veri madencilerince işlenmektedir nedenle, akıllı sözleşmeler için bu işleme şartına dayanılabilmesi için bu hükmün geniş yorumlanarak kişisel verilerin, yalnızca sözleşmenin taraflarına ait olanlarla kısıtlanmaması gerekecektir.

Kişisel veri işleme aynı zamanda **'veri sorumlusunun hukuki yükümlülüğünü yerine getirmesinin zorunlu olduğu'** durumlarda da gerçekleşebilir. Bu durum GVKT (6)(1)(c) ve KVKK Madde 5(2)(ç) bentlerinde düzenlenmektedir. 'Örneğin, KYC ve Kara Para Aklamayı Önleme (AML) gereklilikleri ile uyumlu olma adına kişisel veriler düzenli olarak işlenmektedir. Blok zinciri bağlamında da bu durum örneğin AML ve KYC gereklerine uyum gerektiren kripto varlık işlemleri veya alternatif olarak vergi hukukuna uygunluk için belirli kişisel veri türlerinin işlenmesinin gerekliliği söz konusu olduğunda karşımıza çıkabilecektir (EPRS, 2019).

KVKK Madde 5(2)(f) ye göre veri işlemenin dayandırılabileceği şartlardan biri olan **meşru menfaat** kavramı da Kanunda *"ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"* şeklinde yer almaktadır. Blok zincir teknolojisindeki kişisel veriler, onlara ihtiyaç duyulmasa da sistemde kayıtlı kalmaya devam edecektir. Yapılan işlemlerin tarafi olmayan kişisel verilerin dahi sistemde sürekli şekilde kayıtlı kalmaya devam etmesi durumunun veri sorumlusunun meşru menfaatiyle bağdaşır yanı görülemediğinden ilgili işleme şartının bu teknoloji kapsamında kullanılmasının mümkün olmadığı değerlendirilmektedir.

Kişisel Veri İşlenmesine İlişkin Diğer Tespitler

Kişisel verilerin işlenmesinde uyulması gereken genel ilkeler arasında KVKK Madde (4)(1)(ç)'de, kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü şekilde işlenebileceği ifade edilmiştir. Bu, **veri minimizasyonu ilkesi** gereği veri sorumlusunun yalnızca amacı için gerekli olan kadar veriyi işlemesi gerektiği anlamına gelmektedir. Blok zincirlerinin iki yapısal özelliği veri minimizasyonu açısından bir endişe kaynağı oluşturabilir. Bunlardan ilki bu tür veri tabanlarının sürekli büyüyen yapısıdır. Dağıtık ağ yapılarında veriler yalnızca olağanüstü durumlarda değiştirilebilir veya kaldırılabilir ve eski veriler kaldırılamaz. İkinci olarak ise, bu gibi dağıtık ağlarda her bir düğümde tüm veri tabanının bir kopyasının tutuluyor oluşu nedeniyle verilerin çoğaltılmış yapısının mevcut oluşu ilgili kişisel verilerin birçok kopyasının oluşmasına yol açmaktadır (EPRS, 2019). KVKK Madde 4(2)(d)'de kişisel verilerin işlenmesinde **"ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme"** ilkesine de yer verilmektedir. GVKT Madde (5)(1)(e)' de de aynı doğrultuda "eski" verilerin silinmesinin zorunlu tutulduğu görülmektedir. Kişisel verilerin gerekenden daha uzun süre tutulmaları için veri sorumluları tarafından silme veya periyodik gözden geçirme için zaman sınırlarının belirlenmesi gerekmektedir. Burada amaç sınırlaması doğrultusunda verilerin ne zaman "eski" hale geleceği konusu gündeme gelmektedir. Bu ilgili işlemin tamamlandığı zamana işaret edebilir ya da bu işlem sonrasında dahi ilgili mutabakat protokolü kapsamında söz konu-

su verilerin sıradaki işlem için de gerekli olması durumu ve bu noktada devam eden bir saklamanın var olduğu da iddia edilebilir. Veriler yalnızca en olağanüstü durumlarda blok zincirlerden çıkarılabilir bu da bu tür ortamlarda saklama süresi sınırlamasına uyulacağı konusunu soru işaretinde bırakmaktadır. Bu konuya ilişkin olarak, verilere artık ihtiyaç duyulmadığında blok zincirlerden verilerin kaldırılabilmesi amacıyla geliştiriciler **budama("pruning") teknikleri** üzerinde çalışmaktadır. Bu çalışma genellikle zincirin boyutunu azaltarak performansını arttırma fikri doğrultusunda yapılmaktadır (EU Blockchain Observatory and Forum, 2018).

Yurt dışına kişisel verilerin aktarılması konusu GVKT 'da 44 ila 50'nci maddelerde, KVKK 'da ise 9'uncu madde altında hükme bağlanmıştır. Bir blok zincir ağında katılımcılar AB dışında da bulunabileceğinden AB dışına yapılabilecek kişisel veri aktarımlarında GVKT ve KVKK' ya uyum konuları gündeme gelecektir. Kapalı ve izin gerektiren blok zincir ağlarında veri aktarımına ilişkin olarak bağlayıcı şirket kuralları ve veri işleme davranış kuralları gibi uygun güvenlik önemlerinin alınması mümkün olabilecekken halka açık ve izin gerektirmeyen blok zincir ağlarında veri sorumlusu madencilerin kontrolünü etkin şekilde yapamayacağından söz konusu önlemlerin alınabilmesi bu ağlarda mümkün görünmemektedir. Bu konu kapsamında verilerin hangi üçüncü ülkeye aktarımının yapıldığı ve bu ülkelerde yeterli korumanın sağlandığının nasıl tespit edileceği sorularına çözüm aranması gerekmektedir.

Söz konusu teknoloji kapsamında bazı **ilgili kişi hakları**nın etkili bir şekilde kullanılması sorunlu görünmese de silme hakkı, düzeltme hakkı ve itiraz hakkının bir blok zincirine uygulanması daha derinlemesine bir analiz yapmayı gerektirmektedir. İlgili kişilerin bilgi edinme hakkı konusunda veri sorumlusu kişisel verileri doğrulama için madencilere göndermeden önce ilgili kişilere veri sahibi için kolay erişilebilir ve açık terimlerle formüle edilmiş özlü bilgiler sağlamalıdır. Aynı durum erişim hakkı ve taşınabilirlik hakkı için de geçerlidir. CNIL tarafından bu hakların kullanımının blok zincirlerinin teknik özellikleriyle uyumlu olduğu görüşü savunulmaktadır. Veriler bir blok zincirine kaydedildiğinde bir ilgili kişi tarafından yapılan silme talebini yerine getirmenin teknik olarak imkânsız olduğunu belirtilmektedir (CNIL, 2018). Ancak, blok zincirine kaydedilen veriler bir taahhüt, anahtarlı bir özet değer fonksiyonu tarafından üretilen bir özet değer veya son teknoloji algoritmalar ve anahtarlar vasıtasıyla elde edilen bir şifreli metin olduğunda, veri sorumlusu verileri pratik olarak erişilemez hale getirebilir ve dolayısıyla veri silme etkilerine yaklaşılmış olur. Örneğin, bazı taahhüt şemalarının matematiksel özellikleri (Bir taahhüt şeması mükemmel bir şekilde gizlendiğinde, şahidin (belirli bir değerin belirli bir taahhüte bağlandığını

doğrulayan öğe) ve taahhüt edilen değerin silinmesi taahhüdü artık kişisel veri olarak kabul edilemeyecek şekilde anonim hale getirmek için yeterlidir.) doğrulanmasını sağlayan unsurların silinmesinin ardından, hangi bilginin taahhüt edildiğini kanıtlamanın veya doğrulamanın artık mümkün olmayacağını garanti edebilir. Dolayısıyla taahhüdün kendisi gizlilik açısından artık herhangi bir risk oluşturmayacaktır. Bilginin işlenmek üzere saklandığı diğer sistemlerde de silinmesi gerekecektir. Başka bir örnek olarak, anahtarlı özet değer fonksiyonunun gizli anahtarının silinmesi de benzer etkilere sahip olacaktır. Hangi bilginin özetlendiğini kanıtlamak ya da doğrulamak artık mümkün olmayacaktır. Uygulamada, özet değer bir gizlilik riski oluşturmayacaktır. Aynı şekilde, bilginin işlenmek üzere depolandığı diğer sistemlerde de silinmesi gerekecektir. Yine silme hakkı kapsamında veri koruma hukuku gerekliliklerine uyulabilmesi adına yukarıda sözü edilen budama("pruning") işlemi de uygulanabilecek yöntemler arasında yer almaktadır.

Ek olarak Blockchain Observatory and Forum'un girişimciler ve yenilikçilere sunduğu blok zincir ve kişisel veri ilişkisine yönelik önerileri şu şekilde olmuştur: i) Büyük resimle başlanılmalıdır. Kullanıcı değerinin nasıl yaratılacağı, verinin nasıl kullanıldığı ve gerçekten blok zincirine ihtiyaç olup olmadığı sorularına cevap verilmelidir. ii) Kişisel verileri blok zincirinde saklamaktan kaçınılmalıdır. Verileri anonimleştirmek için veri gizleme, şifreleme ve birleştirme tekniklerini kullanılmalıdır (Blockchain Türkiye, 2022). iii) Kişisel veriler zincir dışında veya blok zincirinden kaçınılamıyorsa özel ve izinli blok zincir ağları üzerinde toplanmalıdır. iv) Yenilik üretmeye devam edilmelidir ve kullanıcılarla mümkün olabildiğince açık ve şeffaf olunmalıdır (EU Blockchain Observatory and Forum, 2018).

SONUÇ

Blok zincirleri, güvenilir bir merkezi aracıya ihtiyaç duymadan veri paylaşımını mümkün kılacak şekilde tasarlanabilir, verilere kimin eriştiğine dair şeffaflık sunar ve ayrıca blok zinciri tabanlı akıllı sözleşmeler veri paylaşımını otomatikleştirerek işlem maliyetlerini de azaltabilir. Bu özellikler, örneğin kurumlar arası veri paylaşımını kolaylaştırmak suretiyle veri pazarlarını destekleyerek çağdaş veri ekonomisine daha geniş çapta fayda sağlayabilir. 2018 yılında Avrupa Parlamentosu tarafından yapılan bir araştırmaya göre 2035 yılına kadar vergi raporlaması, e-kimlik veri tabanları ve oylama planları gibi uygulamaların blok zinciri veya başka bir dağıtık defter teknolojisi biçimi üzerinde çalışabileceği öne sürülmüştür. Özel sektörde DDT, çeşitli dijital para türleri (Bitcoin gibi) ve mobil bankacılığı biçimlerine olanak tanımak, uluslararası ticarette malları takip etmek, yazılım lisanslarını yönetmek, makineden makineye elektrik piyasalarını güçlendirmek ve merkezi paylaşım ekonomisi platformlarını değiştirmek için denenmiştir. Kamu sektörü de aynı şekilde teknolojiyi denemektedir. Ek olarak, AB tarafından uluslar üstü bir blok zinciri altyapısı geliştirme seçeneğinin araştırıldığı bir Avrupa Komisyonu çalışmasının da bulunduğu görülmüştür.

Dağıtık defter teknolojileri geleneksel olarak “genel ve izinsiz” ve “özel ve izinli” olmak üzere iki kategoride gruplandırılır. Öğretide özel ve izinli blok zincirlerini veri koruma yasalarıyla uyumlu bir şekilde tasarlamanın genel ve izinsiz ağlara göre daha kolay olduğu görüşü savunulmaktadır. Bunun nedeni, izinli ağlardaki katılımcıların birbirleri tarafından biliniyor olması ve bu sayede sorumluluğun uygun bir şekilde dağıtılmasını sağlayan sözleşmeye dayalı ilişkilerin tanımlanabilmesidir. Ayrıca, bu ağlar, genel ve izinsiz ağların aksine, ağ üzerinde kontrol sağlayacak şekilde tasarlanmış ve hangi aktörlerin verilere erişebileceği üzerinde bir kontrol söz konusudur. Genel ve izinsiz ağlar için ise bu hususlarda farklı görüşlerin ortaya konulabildiği gözlemlenmiştir.

Blok zincirleri, merkezi olmayan bir şekilde güncellenen kopyalanmış bir veri tabanı (örneğin kripto varlıklardaki işlemleri kaydetmek veya bilgileri kaydetmek için kullanılabilen) ve aynı zamanda yazılımın merkezi olmayan bir şekilde çalıştırılmasına yönelik bir altyapı sunar. Örnekler arasında yer alan akıllı sözleşmeler veya ‘merkezi olmayan uygulamalar’ (tabandaki ağın merkezi olmayan yapısını yansıtan uygulamalar) çok çeşitli şekillerde olup çok çeşitli kullanım durumları sunabilir. Ek olarak merkezi olmayan uygulamaların oluşturulması ve sürdürülmesi için kendi protokollerini hayata geçiren merkezi olmayan uygulama çerçeveleri gibi ara katmanlar da olabilir. Verilen bir blok zincirin veri koruma yasaları ile uyumluluğu değerlendirileceği zaman, örneğin bu çeşitli katmanlarda farklı veri sorumluları yer alabileceğinden blok zinciri teknolojisinin bu çok katmanlı yapısı da akılda tutulmalıdır.

Şu anda blok zincirleri ‘ciddi teknik ve prosedürel sınırlamalar’ sebebiyle tam olarak olgunlaşmamış durumda görülmektedir. Bu eksiklikler arasında en belirgin olanı, geniş çaplı kullanım için gerekli olan ölçeklenebilirlik eksikliğidir. Blok zincirlerinin, her tam düğümün her işlemi işlemesi ve tüm mevcut durumun bir kopyasını tutması gerektiğinden bu tasarımları verimsiz bulunmaktadır. Bu süreç tek hata noktasını ortadan kaldırmak suretiyle güvenlik avantajları sunsa da verimi düşürmekte ve işlemleri yavaşlatmaktadır. Bu sorunun dağıtık defterlerin boyutu büyüdükçe de artması muhtemeldir. Ölçeklenebilirlik, her yeni işlemin ağın büyümesine neden olduğu, sadece ekleme yapılabilen ve dolayısıyla sürekli büyüyen bir veri tabanında önemli bir endişe kaynağı oluşturmaktadır.

Öğretide yer alan ve tarafımca da katıldığım görüşlere göre, veri koruma yasalarının yorumlanması ve uygulanması sırasında yenilikçi bir yaklaşım ortaya konmalı, amaçsal yorum ilkesi olabildiğince benimsenerek blok zinciri modeline yeterli bir hareket alanı bırakılmalıdır. Blok zinciri modelinin, kişisel verilerin korunmasına ilişkin potansiyelini gerçekleştirip gerçekleştiremeyeceği ancak bu şekilde görülebilecektir (Özer, 2019). Ayrıca günümüze kadar kabul görmüş hukuk uygulamaların dikkate alınarak teknolojik, sosyolojik ve ekonomik menfaatlerin iyi analiz edilerek hukuk düzenimizin şekillendirilmesi isabetli olacaktır (Çekin, 2019). Bu çalışma kapsamında yapılan inceleme ve değerlendirmeler ışığında blok zincir teknolojisinin veri koruma hukuku kapsamında değerlendirilebileceği düşünülen hususlar dahilinde kişisel verilerin korunması mevzuatına uyumu anlamında olumsuz yanların bulunduğu gözlemlenmiş olsa da veri koruma yasaları ile tamamen uyumlu veya uyumsuz olduğu şeklinde genel bir sonuca varmanın doğru olmayacağı daha ziyade teknolojinin her kullanıldığı durumun ilgili teknik ve bağlamsal faktörleri (yönetişim çerçevesi gibi) dikkate alınarak kendi esasları dahilinde (olay özelinde) incelenmesi gerektiği öngörülmektedir. ◆

KAYNAKÇA

- Anderson, R.J. (1996). The Eternity Service, Pragocrypt.
- Antonopoulos, A.M. (2017), Mastering Bitcoin, O'Reilly
- Avrupa Parlamentosu (AP) (2018a), 2035'e Doğru Küresel Trendler-Ekonomi ve Toplum. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/627126/EPRS_STU(2018)627126_EN.pdf adresinden alınmıştır.
- Avrupa Parlamentosu Araştırma Dairesi (EPRS). (2019), Blockchain and the GDPR- Can distributed ledgers be squared with European data prptection law?, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf adresinden alınmıştır.
- Avrupa Parlamentosu (AP) (2018b), Report on Blockchain: a forward-looking trade policy. https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html adresinden alınmıştır.
- Bacon, J., Michels, J.D., Millard, C. ve Singh, J. (2017), Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218 adresinden alınmıştır.
- BitFury Group (2022), Proof of stake versus proof of work, http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1. 0.2.pdf adresinden alınmıştır.
- Blockchain (2022). https://academy.binance.com/tr/glossary/blockchain?utm_campaign=googleadsxacademy&utm_source=googleadwords_int&utm_medium=cpc&gclid=CjwKCAjw9LSSBhBsEiwAKtf0n1jHlofSxtr-3mO89mlQUjlZ2vVEuWdT7ZJ2NI3g1BXXRzvRIwzyaSBoC-KIQAvD_BwE adresinden alınmıştır.
- Blockchain Türkiye (2022), Kişisel Verilerin Korunması Hukuku ve Blok zinciri Teknolojisi Raporu. https://bctr.org/bctr-rapor-kisisel-verilerin-korunmasi-hukuku-ve-blokzinciri-teknolojisi-raporu-27977/ adresinden alınmıştır.

- Buterin, V. (2014), Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf adresinden alınmıştır.
- Commission Nationale de l'Informatique et des Libertés (CNIL) (2018), Blockchain and the GDPR: Solutions For A Responsible Use Of The Blockchain İn The Context Of Personal Data
- Corda. (2022). https://www.corda.net/ adresinden alınmıştır.
- Cortese, A. (2016). Blockchain Technology Ushers in The Internet of Value. Cisco
- Çekin, M.S. (2019), Borçlar Hukuku ile Veri Koruma Hukuku Açısından Blockchain Teknolojisi ve Akıllı Sözleşmeler: Hukuk Düzenimizde Bir Paradigma Değişimine Gerek Var Mı? İstanbul Hukuk Mecmuası, 315-341.
- Diri, N. (2022). Blok zincir Uygulamasında Kişisel Verilerin Tutulması (Yüksek Lisans Tezi). Marmara Üniversitesi, İstanbul.
- EIP's (2023). https://ethereum.org/en/eips adresinden alınmıştır.
- ERC-20 (2023). https://ethereum.org/en/developers/docs/standards/tokens/erc-20/ adresinden alınmıştır.
- EU Blockchain Observatory and Forum (2018), Blokchain and the GDPR Tematik Raporu. https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf adresinden alınmıştır.
- Faber, B., Michelet, G., Weidmann, N., Mukkamala R. R. ve Vatrapu, R., BPDIMS: A Blockchain-based Personal Data and Identity Management System. https://www.researchgate.net/publication/332085440_BPDIMSA_Blockchain-based_Personal_Data_and_Identity_Management_System adresinden alınmıştır.
- Felten, E. (2018), Blockchain:What is it good for?. https://freedom-to-tinker.com/2018/02/26/blockchain-what-is-it-good-for/ adresinden alınmıştır.

◊ Haber, S. ve Stornetta, W.S. (1991). How to Time-Stamp a Digital Document, In Advances in Cryptology – Crypto '90 Lecture Notes in Computer Science v 537, Springer-Verlag, 437–455.

◊ How Does Block Chain Prevent Doublespending Bitcoins (2022) https://www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-bitcoins.asp adresinden alınmıştır.

◊ Hyperledger. (2016). https://www.hyperledger.org/ adresinden alınmıştır.

◊ Kişisel Verileri Koruma Kurumu (KVKK) (2021), Araç Kiralama Programları Yazılımcısı ve Satıcısı Firmalar Tarafından, İlgili Kişilerin Verilerinin İşlenmesi Ve Bu Verilerin Araç Kiralama Firmaları Arasında Paylaşılmasını Sağlayan Bir Kara Liste Programı Oluşturulması" Hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 Tarihli Ve 2021/1303 Sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/7288/2021-1303 adresinden alınmıştır.

◊ Kurt, C.A. (2022), Ethereum Merge Gerçekleşti, https://www.btchaber.com/son-dakika-ethereum-merge-gerceklesti/ adresinden alınmıştır.

◊ Leadership. (2022). https://www.hyperledger.org/about/leadership adresinden alınmıştır.

◊ Madde 29 Veri Koruma Çalışma Grubu (2010), Opinion 1/2010 on the concepts of "controller" and "processor", https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf adresinden alınmıştır.

◊ Massessi, D. (TY), Blockchain Consensus and Fault Tolerance In a Nutshell. https://medium.com/coinmonks/blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03 adresinden alınmıştır.

◊ Nakamoto, S. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf adresinden alınmıştır.

◊ ÖZER, Y.M. (2019). Kişisel Verilerin Korunmasında Blok zinciri Modeli (Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi, İstanbul.

◊ Schneier, B ve Kelsey, J. (1998), Cryptographic Support for Secure Logs on Untrusted Machines. https://www.schneier.com/wp-content/uploads/2016/02/paper-secure-logs.pdf adresinden alınmıştır.

◊ The Beacon Chain (2023). https://ethereum.org/en/upgrades/beacon-chain/ adresinden alınmıştır.

◊ The Berlin Hard Fork. (2021). https://www.coindesk.com/tech/2021/04/15/berlin-hard-fork-is-now-live-on-ethereum/ adresinden alınmıştır.

◊ The Linux Foundation (2022), Blockchain Understanding Its Uses and Implications. https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS170x+2T2021/block- v1: LinuxFoundationX+LFS170x+2T2021+type@sequential+block@4ee4f8bc0dad4e09ad99b376b061b0c9/ adresinden alınmıştır.

◊ The London Fork. (2019). https://eips.ethereum.org/EIPS/eip-1559 adresinden alınmıştır.

◊ Usta, A. ve Doğantekin, S. (2018). Blockchain 101 v.2, 18. https://bkm.com.tr/wp-content/uploads/2019/08/15082019_kitap.pdf adresinden alınmıştır.

◊ Wirth, C., Kolain, M. (2018), Privacy by Blockchain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data, https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf adresinden alınmıştır.

◊ Wirtschafsakademie Schleswig-Holstein,No. C-210/16 C-210/16 [2018] EU:C:2017:796, para.16

KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN DİJİTAL PARMAK İZİ

Şükran KOÇAK

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "Kişisel Verilerin Korunması Açısından Dijital Parmak İzi" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Tarayıcıların cihaz bağımsız olarak çalışabilmesi; kullanıcı deneyimini iyileştirme, zengin içerik görüntüleme firsatları sunma açısından olumlu etkileri olsa da bu işlevleri gerçekleştirme amacıyla tarayıcılara eklenen özellikler, kullanıcının web üzerinde anonim kalabilmesini zor bir hale getirmiş ve kişinin çevrim içi takibine imkân tanımıştır. Tarayıcıların, bir web takip teknolojisi olarak sınıflandırılan çerezlere karşı daha sıkı önlemler almasıyla beraber, çevrim içi hizmet sunumunda çerezlere alternatif teknoloji arayışı başlamış ve dijital parmak izi kullanımı ortaya çıkmıştır (Madde 29 Veri Koruma Çalışma Grubu, 2014c).

Avrupa Birliği Hukukunda çerez ve benzeri teknolojiler, "2009/136 sayılı Direktif" ile "2002/58/AT sayılı Direktifi"nin ("E-Gizlilik Direktifi") bazı maddelerinde yapılan değişiklik ile özel olarak düzenlenmekle beraber "Avrupa Birliği Genel Veri Koruma Tüzüğü"nde de düzenleme alanı bulmaktadır. "E-Gizlilik Direktifi"nin 24'üncü maddesinde ajan yazılımlar, web açıkları, gizli tanımlayıcılar ve diğer benzer teknolojiler olarak bahsedilen web takip teknolojileri; mevcut "E-Gizlilik Tüzüğü Taslağı"nın 20'nci maddesinde daha açık bir şekilde yer almaktadır. Söz konusu Tüzük'ün 20'nci maddesi hükmünde; ajan yazılımlar, web açıkları

("bugs"), gizli tanımlayıcılar, takip çerezleri veya diğer istenmeyen takip araçları kullanıcı cihazı bilgisine erişme veya gizli bilgi depolama ve aktivitelerinin takibi amacıyla kullanıcı cihazına erişebildiği, kullanıcı cihazına ilişkin bilginin ise tanımlama ve takip amacıyla uzaktan toplanabildiği, cihaz parmak izi gibi bu tür tekniklerin genellikle kullanıcının bilgisi dahilinde yapılmadığı ve son kullanıcıların mahremiyetini ciddi bir şekilde ihlal edebildiği belirtilmektedir. Böylelikle cihaz parmak izi yani dijital parmak izi bizzat taslak halde olan "E-Gizlilik Tüzüğü"nde ele alınmış bulunmaktadır.

Literatürde cihaz parmak iziyle ilişkili olarak tarayıcı parmak izi, dijital parmak izi olarak farklı terimler kullanılmakta olup bu terimler teknik anlamda birbiriyle yakından ilişkilidir. "Cihaz parmak izi", genellikle uzak bir bilgi işlem cihazından toplanan yazılım veya donanım ayarlarının kompakt bir özeti olarak tanımlanırken "tarayıcı parmak izi" sunucuya gönderilen her bir HTTP talebindeki bilgilerin birleşimini ifade etmektedir. Bu çalışmada, cihaz parmak izi veya tarayıcı parmak izini ifade eden geniş anlamıyla "dijital parmak izi" terimi kullanılacaktır. Dijital parmak izi çıkarma, *"bir sitenin ziyaretçi kullanıcıyı, kullanıcının kullandığı tarayıcı veya cihazı, yapılandırma tercihleri veya diğer gözlemlenebilir özellikleri aracılığıyla tanımlama veya tekrar tanımlama kabiliyeti"* olarak tanımlanabilecektir ("Mitigating Browser Fingerprinting in Web Specifications", 2019). Dijital parmak izi çıkarma, durumsuz ("stateless") bir çevrim içi takip yöntemi olarak karşımıza çıkmaktadır. Durumsuz takip, doğası gereği kullanıcının terminal cihazında bir tanımlayıcı depolayan durum bilgisi tutan yani denetlemeli ("stateful") takip yöntemlerine göre daha az gözlemlenebilirdir.

İlk olarak 1994 yılında kullanıldığı bilinen çerezler o dönemlerde mahremiyet istilacısı olarak adlandırılmıştı (Acar, Eubank, Englehardt, Juarez, Narayanan ve Diaz, 2014). Tarayıcıların çerezler gibi durum bilgisi tutan tanımlama yöntemlerine karşı gittikçe daha sıkı önlemler almasıyla beraber çevrim içi takip yöntemleri kullanıcılar ve araştırmacılar için daha az gözlemlenebilir ve hatta görünmez bir hal almaya başlamıştır. Edward Felten'in 2009 tarihli "Eğer Beni Takip Edeceksen Lütfen Çerez Kullan" isimli yazısında çerezlerin kontrol edilebilir olduğu, tarayıcıların sınırlı kapasitede ve sınırlı sayıda çerez muhafaza edebildiği, çerezleri görüntüleme, engelleme ve kaldırma araçlarının mükemmel olmadığı, ancak en azından mevcut olduğu ve diğer izleme yöntemlerinin, kullanıcıları neredeyse savunmasız bıraktığı belirtilerek çerezden farklı izleme teknolojilerin varlığına dikkat çekmiştir (Felten, 2009)

Bir araştırma raporunda; web takip teknolojilerinin risk oranları gözlemlenebilme, sıfırlanabilme ve engellenebilme olmak üzere üç kritere göre sınıflandırılmış

olup bu sınıflandırmaya göre; dijital parmak izi yüksek riskli olarak nitelendirilmiştir (Johnston ve Culnane, 2020). Dijital parmak izi; birçok veri noktasının, özellikle IP adresi gibi benzersiz tanımlayıcılarla birleştirilmesinde ve işlemenin amacı; kişiyi zaman içinde farklı web siteleri üzerinden tanımlamak olduğunda (örneğin davranışsal reklamcılık gibi), bu tür bir faaliyet kişisel veri işlenmesini gerektirdiğinden veri koruma kanunlarıyla uyum sağlanması gerektiği değerlendirilmektedir. Kullanıcının farkındalık düzeyi ve dijital parmak izi kullanımının tespit etme güçlüğü dikkate alındığında, dijital parmak izi çevrim içi davranış takibinde oldukça görünmez bir teknik olarak değerlendirilebilecektir. Çevrim içi bir hizmetin kullanılması esnasında web sunucusuna gönderilen bilgilerin ne amaçla toplandığı ve hangi kişisel veri işleme şartı dahilinde işlenmesi gerektiği hususları ile hukuka aykırı kişisel veri işlenip işlenmediğinin tespiti de zor olacaktır.

Çalışmanın birinci bölümünde dijital parmak izi ve diğer takip teknolojileri ele alınacak olup ikinci bölümünde dijital parmak izinin hukuksal açıdan değerlendirilebilmesini teminen, dijital parmak izi teknolojisinin teknik boyutu açıklanacaktır. Üçüncü bölümde dijital parmak izinin hangi amaçlarla kullanılabileceği hususuna değinilecektir. Dördüncü bölümde AB ve Türk Hukukunda dijital parmak izine ilişkin düzenlemeler hakkında bilgi verilerek beşinci bölümde; dijital parmak izi çıkarılmasının oluşturduğu mahremiyet riskleri ortaya konulacak ve bunlara yönelik olarak ilgili kişi tarafından alınabilecek önlemler ile veri sorumluları, geliştirici ve üreticiler için Kanun'a uyum konusunda çözüm önerileri sunulacaktır.

DİJİTAL PARMAK İZİ VE ÇEVRİM İÇİ DİĞER TAKİP TEKNOLOJİLERİ

Kişinin çevrim içi takibini mümkün kılan çoğu teknoloji aslında kişinin benzersiz bir tanımlayıcı aracılığıyla zaman içinde kullanıcının tanımlanması esasına dayanmaktadır. Özellikle reklam endüstrisi, kişi hakkında detaylı profiller oluşturulabilmek ve davranışsal olarak kişilere reklam sunabilmek amacıyla kişilerin çevrim içi olarak ayırt edilebilmesini sağlayan bazı teknolojiler kullanmaktadır. Bu teknolojilerin kullanımı yalnızca reklamcılık amacıyla sınırlı değildir. Çevrim içi izlemenin oluşturduğu en ciddi risk, bireylerin gözetimi için küresel bir araç haline gelmesi olup bu gözetimin amacı; güvenlik, politik veya ticari olabilmektedir. Çevrim içi takip edilen bireyler hakkında profilleme yapılması bireylere hizmet verilmesinde ayrımcılığa neden olmaktadır. Profilleme faaliyetinin sonucu olarak ürün veya hizmetin kişiye özel fiyatlandırılması (örneğin profiline uygun beğenebileceğin ürünün sana daha yüksek fiyattan sunulması) ya da yalnızca kişinin profiline göre kişisel içerikler sunulması nedeniyle bireyler, çevrim içi içe-

rik bakımından bir fanus içinde sınırlı bilgiye erişmek durumunda kalmaktadır (European Network and Information Security Agency, 2012). Cambridge Analytica skandalı, bizlere çevrim içi takibin bireyler üzerindeki etkisinin hangi boyuta ulaşabileceği hakkında bir öngörü yeteneği kazandırmıştır. Bu dava sürecinde Mark Zuckerberg'e Facebook'un üyesi olmayanlar hakkında profil oluşturup oluşturmadığı sorulduğunda, Zuckerberg gölge profillerin ("shadow profiles") kendisine tanıdık bildik bir şey olarak gelmediği, ancak Facebook kullanıcıların güvenliği için üye olmayanların da bazı bilgilerinin toplandığını itiraf etmiştir (Molitorisz, Meese ve Hagedorn, 2021).

Kullanıcının çevrim içi takip edilmesi amacıyla herhangi bir yöntem ile veri toplanması, verilerin birleştirilmesi veya analiz edilmesi kişisel veri işlenmesini de gerektirecektir. Bununla birlikte, takip teknolojilerinin gözlemlenebilme ve engellenebilme gibi özellikleri göz önünde bulundurulduğunda mahremiyet açısından her zaman aynı riski ihtiva etmeyecektir. Web'de takip teknolojileri; durum denetlemeli takip (*stateful tracking*) ve durumsuz takip (*stateless tracking*) olmak üzere iki kategoride tasnif edilmektedir. Durum denetlemeli takip yaklaşımı; bir tanımlayıcının kullanıcı tarayıcısının veya cihazının herhangi bir yerinde depolanması ve daha sonra bu tanımlayıcının geri çağırılması suretiyle kullanıcının web oturumları sırasında takip edilmesine dayanmaktadır. Gizli form alanları, çerezler, *web beacon* (piksel etiketleri), yerel paylaşılan nesneler (*local shared objects* veya diğer adıyla *Flash* çerezler), yerel depolama, tarayıcı önbelleği, cihaz tanımlayıcıları, *eTag* ve son değiştirilme tarihleri (*last modified date*), açık web yetkilendirme gibi teknolojiler durum denetlemeli takipte kullanılmaktadır (Johnston ve Culnane, 2020).

Durumsuz takip teknolojileri ise belirli bir tanımlayıcının kullanıcı tarayıcısında veya cihazında depolanmasına dayalı değildir. Durumsuz takipte, çevrim içi takip için gerekli tanımlayıcı değerini oluşturan kullanıcı cihazı veya kullanıcının davranışlarıdır. Ancak çevrim içi takip teknolojilerinin dayandığı temel prensip olan kişiyi benzersiz olarak tanımlayacak bir değer oluşturulması, durumsuz takip teknolojileri de geçerlidir. Bu ihtiyaç duyulan değer ise kişinin veya kullandığı cihazın veya uygulama örneğinin özelliklerine dayalı olarak oluşturulmaktadır.

Durumsuz takip teknolojileri arasında yer alan dijital parmak izi RFC 6973'te; *"Bir parmak izi (fingerprint); bir cihazı veya uygulama örneğini tanımlayan bilgi öğeleri kümesi"* olarak tanımlanmaktadır (Cooper, Tschofenig, Aboba, Morris, Hansen ve Smith, 2013). Parmak izi çıkarma (fingerprinting); *"gözlemci veya saldırgana iletilen birçok bilgi öğesine dayalı olarak bir gözlemci veya saldırganın bir cihazı veya uygulama örneğini benzersiz (yeterli bir yüksek olasılıkla) olarak tanımlaması sürecidir."* (Cooper ve diğerleri, 2013). Tarayıcı veya cihaz parmak izi çıkarma birbiriyle ilişkili kullanılan iki tekniktir. Tarayıcı parmak izi çıkarma; her bir web tarayıcısının sağladığı bilgilere dayalı olarak bir web tarayıcısını tanımlama yöntemidir.

Cihaz parmak izi çıkarma; kullanılan cihazın (masa üstü bilgisayarı, diz üstü bilgisayarı veya mobil cihazı) özelliklerine dayalı olarak cihazın tanımlanmasıdır. Cihaz parmak izi, kullanıcı farklı tarayıcılar kullanması halinde dahi takibi mümkün kılmaktadır (Nottingham, 2020). Dünya Çapında Ağ Birliği (The World Wide Web Consortium ya da kısaca W3C), tarayıcı parmak izi çıkarma kavramını; *"bir sitenin ziyaretçi kullanıcıyı, kullanıcının kullandığı tarayıcı veya cihazı, yapılandırma tercihleri veya diğer gözlemlenebilir özellikleri aracılığıyla tanımlama veya tekrar tanımlama kabiliyeti"* olarak tanımlanmıştır ("Mitigating Browser Fingerprinting in Web Specifications", 2019). Tarayıcı veya cihaz parmak izi çıkarma her ne kadar birbiri yerine geçecek şekilde kullanılsa da cihaz parmak izi çıkarma, cihazın yapılandırma tercihlerine dayalı olması ve daha az değişkenlik göstermesi nedeniyle kullanıcıyı tanımlamak için tarayıcı parmak izine göre daha stabil bir yöntemdir. Bu çalışmada her iki tekniği kapsar biçimde "dijital parmak izi" terimi kullanılacaktır.

Günümüzde 4 milyar bilgisayar, akıllı telefon ve diğer terminallerin olduğu tahmin edilmekle birlikte, bu cihazlara dair yeterli düzeyde ayırt edici veri kümesi sayesinde dijital parmak izi çıkarmak suretiyle herhangi bir internet sitesine bağlanan terminal cihazını sunucuda sonsuza kadar benzersiz olarak tanımlamak mümkündür (Agencia Española Protecciòn Datos (AEPD), 2019). Ancak bir dizi özellik kümesine göre çıkarılan parmak izinin, cihazı veya tarayıcıyı benzersiz olarak tanımlamasının bir derecesi bulunmaktadır. Bir cihazı veya tarayıcıyı benzersiz olarak tanımlamanın derecesi, Bilgi Teorisinde yer alan entropi ile ölçülmektedir. Entropi, rasgele bir olayın bit olarak belirsizlik derecesi veya bilgi miktarıdır. Bilgi miktarı arttıkça bireyleri benzersiz tanımlama riski artacaktır (Madde 29 Veri Koruma Çalışma Grubu, 2014c). Bir kişi hakkında yeni bir gerçek öğrendiğimizde bu gerçek, kişinin kimliğinin belirlenmesi için gerekli olan entropi miktarını belirli bir miktarda azaltmaktadır.

DİJİTAL PARMAK İZİ VE BENZERSİZ OLARAK TANIMLAMASI

Günümüze kadar dijital parmak izinin araştırılması hakkında geniş çapta üç büyük çalışma gerçekleştirilmiştir. Pierre Laperdrix ve arkadaşlarının 2019 yılında yayımladığı bir raporda; dijital parmak izi alanında yapılan üç büyük çalışmada toplanan parmak izlerinin kaçının benzersiz olduğuna ilişkin bir karşılaştırma

yapılmıştır (Laperdrix, Bielova, Baudry ve Avoine, 2020). 2010 yılında Peter Eckersley tarafından gerçekleştirilen Panopticlick projesinde (Mevcut internet adresi olan https://coveryourtracks.eff.org/ (eskiden panopticlick.eff.org) sitesinden proje için oluşturulan web sayfasına ulaşılabilmekte olup benzersiz bir dijital parmak iziniz olup olmadığı test edilebilmektedir.) mahremiyet farkındalığı ortalama düzeyde olan kullanıcı grubu üzerinden yapılan ölçüm aracılığıyla 470.161 adet parmak izinin %94,2'sinin kişiyi benzersiz olarak tanımlayabildiği tespit edilmiştir (Eckersley, 2010).

2016 yılında Laperdrix ve arkadaşları tarafından gerçekleştirilen *AmIUnique* (https://amiunique.org/ sitesinden proje için oluşturulan web sayfasına ulaşılabilmekte olup benzersiz bir dijital parmak iziniz olup olmadığı test edilebilmektedir.) projesinde ise masaüstü bilgisayar kullanan kişilerden 105.829 adet parmak izi toplanmış olup bunların %89,4 kullanıcıları benzersiz olarak tanımladığı, mobil tarayıcılardan toplanan parmak izlerinin ise %81'inin kişiyi benzersiz olarak tanımladığı tespit edilmiştir (Laperdrix, Rudametkin ve Baudry, 2016)

2018 yılında Gómez-Boix ve arkadaşları tarafından gerçekleştirilen *Hiding In The Crowd* projesinde veriler, en çok ziyaret edilen Fransız web siteleri arasında ilk 15'te yer alan daha küresel bir kitleyi hedefleyen bir ticari platformda toplanmıştır. Anılan diğer iki çalışmada, mahremiyet farkındalığı olan veya ortalama bir kullanıcıdan daha temkinli olabilen ziyaretçileri açıkça hedefleyen web sitelerinde toplanmıştır. *Hiding In The Crowd* projesinde toplanan parmak izi sayısı diğer iki çalışmaya göre daha fazladır, benzersiz tanımlama oranı ise daha düşüktür (Gómez-Boix, Laperdrix ve Baudry, 2018).

Araştırmacıların farklı sonuçlar elde etmesinin nedeni, tespit yöntemleri ve kriterleri, araştırma grubunun farklı olması şeklinde yorumlanabilecektir. Gómez-Boix ve arkadaşlarının da (2018) dile getirdiği gibi ölçüm için hedeflenen kitlenin demografik yapısı dijital parmak izinin etkinliğinde büyük değişkenlik oluşturmaktadır. Ayrıca daha eğitimli ve tarayıcı ayarlarını yapılandırmayı bilen kullanıcılardan oluşan bir örneklem üzerinde daha çok sayıda benzersiz dijital parmak izinin varlığı hususuna kendi araştırması kapsamında cevap bulamamış, ölçüm için farklı yönlerin göz önünde bulundurulmasının dijital parmak izinin takip ve tanımlamadaki gerçek etkinliği anlamada önemli olduğu ifade edilmiştir (Gómez-Boix ve diğerleri, 2018).

DİJİTAL PARMAK İZİNİN KARARLILIĞI

Dijital parmak izi, kullanıcının cihazının ve ortamının doğrudan bir yansıması olduğundan, sistem bileşenleri değiştirildiğinde, yapılandırıldığında veya güncellendiğinde değişebilmektedir. Tarayıcı veya eklentisinin güncellenmesi, yeni bir yazı tipi eklenmesi veya harici bir monitör bağlanması sonucu ekran çözünürlüğünün değişmesi gibi nedenlerden dolayı dijital parmak izi değişebilmektedir. Dijital hakları savunma amacıyla kurulan sivil toplum kuruluşu olan Electric Frontier Foundation (EFF) tarafından yürütülen ve 2010 yılında başlatılan *"Panopticlick"* projesi kapsamında test amaçlı oluşturulan bir internet sitesinde modern tarayıcıların dijital parmak izi çıkarmaya maruz kalma derecesi araştırılmıştır. *Panopticlick* projesi için 2010 yılında hazırlanan raporda; çerezleri kabul eden kullanıcılar arasında dijital parmak izinin değişim oranı %37,4 gibi bir oranla yüksek olduğu değerlendirilmiştir. Kullanıcının belirli bir çerez ile iki ziyareti arasında yaklaşık 5 gün olması halinde parmak izindeki değişim %50 üzerine çıkmaktadır (Eckersley, 2010). Uzun vadeli izlemeyi mümkün kılmayı amaçlayan bir kişinin, bu değişiklikleri anlama ve tahmin etme becerisine sahip olması gerekmektedir (Laperdrix ve arkadaşları, 2020).

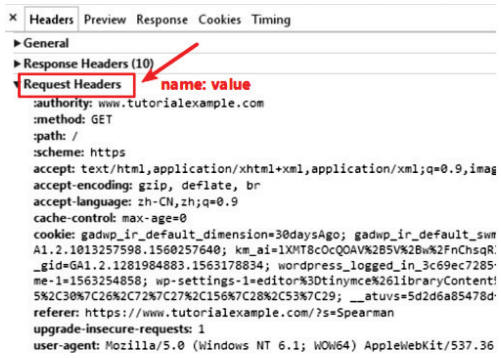
EFF tarafından yeterli düzeyde mahremiyet farkındalığı olan kullanıcı örneklemi ve 40,671 tarayıcı üzerinden yürütülen ölçümde; tarayıcı uzayının %83,6'sının benzersiz parmak izine sahip olduğu, Adobe Flash veya Java Sanal Makinesi aktif olan tarayıcılarda bu oranın %94,2'ye çıktığı, parmak izlerinin hızlı değişen doğası gereği yeni parmak izinin atası olan parmak izinin tahmini için oluşturdukları algoritma ile parmak izi aracılığıyla takibin stabil hale getirildiği belirtilmiştir. Peter E. tarafından 2010 yılında hazırlanan söz konusu projenin dönemsel sonuçlarını değerlendirdiği raporda *"Panopticlick"* projesi kapsamında tarayıcı parmak izlerinin kararlığı için bir algoritma oluşturulduğundan bahsedilmektedir. Bu algoritma ile Adobe Flash ve Java kurulu olmayan sistemleri hariç tutmak üzere, çeşitli sebeplerden dolayı değişen parmak izinin atasını tespit etmek için iki parmak izi arasındaki benzerlik analizi yapılmış ve benzerliğin belirli bir eşik değeri üzerinde olması halinde iki parmak izi arasında bağlantı sağlanabildiği değerlendirilmiştir (Eckersley, 2010).

DİJİTAL PARMAK İZİ ÇIKARMA TEKNİKLERİNİN SINIFLANDIRILMASI

Dijital parmak izi aracılığıyla kullanıcı tanımlanma sürecinde pasif ve aktif parmak izi yöntemlerinin birlikte kullanılması söz konusu olmaktadır (Englehardt ve Narayanan, 2016).

Pasif Olarak Dijital Parmak İzi Çıkarma

Pasif olarak dijital parmak izi çıkarma yönteminde, web taleplerindeki gözlemlenebilir özelliklerden faydalanılmaktadır. Aktif parmak izinden ayıran temel özelliği, istemci tarafı herhangi bir kod çalıştırılmamasıdır ("Mitigating Browser Fingerprinting in Web Specifications", 2019). Pasif parmak izi çıkarmada çerez tanımlayıcıları, HTTP taleplerinde yer alan HTTP talep başlık bilgisi, IP adresi ve diğer ağ seviyesinde bilgiler kullanılmaktadır ("Mitigating Browser Fingerprinting in Web Specifications", 2019). Kullanıcı aracısı dizesi, bir HTTP talebinin başlığında yer almakta olup tarayıcı, renderer, versiyon ve işletim sistemi bilgisini içermektedir. Aktif parmak izi çıkarma sürecinde; istemci tarafında çalışan Javascript kodları kullanıldığından pasif parmak izine göre tespit edilebilirliği daha kolaydır. Şekil 1'de örnek bir HTTP talebinde yer alan başlık bilgileri gösterilmekte olup, accept, accept encoding, dil bilgisi, çerezlerin bilgisi, referer başlık bilgisi, kullanılan kullanıcı aracısı gibi bilgiler sunucuya gönderilmektedir.



Şekil 1. Web talebi başlık bilgisi örneği ("An Easy Guide to Get HTTP Request Header List for Beginners – Python Web Crawler Tutorial", 2019)

Bir özelliğin tasarlanması için en makul yöntem olmadığı sürece, yani bir özellik başka bir makul bir yöntem ile tasarlanamadığı sürece pasif parmak izi çıkarmaya katkı sağlayan durumlardan kaçınılması gereklidir. Zira daha önce de bahsedildiği üzere, pasif parmak izi ile kullanıcıyı tanımlamak daha kolaydır ve bu yöntem oldukça ulaşılabilir bir yöntemdir, bunun yanı sıra pasif parmak izi kullanımını tespit etmek üzere eklenti gibi harici algılama ve kontrol sistemlerini kullanma fırsatı da bulunmamaktadır ("Mitigating Browser Fingerprinting in Web Specifications", 2019).

Aktif Olarak Dijital Parmak izi Çıkarma

İstemci tarafında çalışan Javascript kodları aracılığıyla elde edilen bilgiye dayanmaktadır. Tarayıcılardan Javascript kullanımı kısıtlanabildiğinden pasif parmak izine göre önlenmesi daha kolay olsa da bu kısıtlama kullanılabilirlik bakımından olumsuz etki doğurmaktadır. Dijital parmak izi çıkarma amacıyla yaygın olarak kullanılan Uygulama Programlama Ara Yüzleri (API); ses bağlamında API (Audio Context API), Web RTC API, Batarya Durumu API, Canvas API, WebGL API'dir.

HTML 5 kütüphanelerinden olan *"Audiocontext"*, ses sinyalini işleme süreci için kullanılmaktadır. Sistemin donanım veya yazılım özelliğine göre ses sinyali işlemede küçük farklar ortaya çıkabilmekte olup, işleme sürecindeki bu farklılıklar dijital parmak izi çıkarımına katkı sağlamaktadır. Ses bağlamında parmak izinin işleyişi, *canvas* parmak izine benzerlik göstermekle beraber ses bağlamında parmak izinde, canvas'tan farklı olarak görsellerden öte sesin işlenmesindeki farklılıklara dayalı olarak dijital parmak izi oluşturulmaktadır.

Web Gerçek Zamanlı İletişim (Web Real-Time Communication, kısaca Web RTC), tarayıcılar ve mobil uygulamalarda uçlar arası (P2P) multimedya iletişimleri için kullanılan bir teknolojidir. Web RTC herhangi bir eklenti olmaksızın sesli arama, video görüşme ve uçlar arası dosya paylaşımı sağlayan ve 2011 yılında Google tarafından geliştirilen bir teknolojidir. Günümüzde Chrome, Firefox ve Safari gibi tarayıcılar WebRTC'yi desteklemektedir.

WebRTC ile iletişim sağlanırken, cihazlar arası en iyi rotayı belirleme amacıyla yereldeki IP adresleri ve dış IP dahil olmak üzere toplanan bilgiler uygulamaya erişilebilir kılınmaktadır (Englehardt ve diğerleri, 2016). Kullanıcının yerel IP adresinin uygulamaya erişilebilir kılınması ile öğrenilen yerel IP adresi ve dış IP adresi, kullanıcı cihazını tanımlamak üzere tutarlı bir tanımlama faktörü olarak karşımıza çıkmaktadır. Steven Englehardt ve Arvind Narayanan'ın (2016) 2016'da 1 milyon internet sitesi üzerinden yaptıkları ölçüm çalışmasında, WebRTC ile "createDataChannel" ve "createOffer" metotlarının çağrılması ve "onicecandidate" olay işleyicisine (event handler) erişilmesi durumunda yerel IP adreslerinin (0 yanlış pozitif değerle) getirildiği manuel olarak tespit edilmiş, bununla beraber diğer parmak izi çıkarma tekniklerinin de bulunması halinde kullanılan *Javascript* kodunun takip yaptığı kabul edilmiştir.

Bu çalışmadaki sonuçlar; 1 milyon siteden 715 sitenin kullanıcı etkileşimi olmaksızın yerel IP adreslerinin keşfedildiği ve bu kod parçacıklarının 99 ayrı konumdan olmak üzere 659'unun ziyaret edilen site dışı kaynaklı script olduğu ve 625'inin

takip için kullanıldığı tespit edilmiş ve gözlemlenen bu sciptlerin URL'leri de çalışma kapsamında yayımlanmıştır (Englehardt ve diğerleri, 2016).

İspanya Veri Koruma Otoritesi tarafından yapılan 2018 tarihli bir çalışmada ise, yine 2016'da yapılan çalışmada yararlanılan araç olan OpenWPM ile web sitelerine dair gözlem çalışması yürütülerek 2.503 adet alan adına tekabül eden 5.006 adet URL analiz edilmiş olup, bu çalışmaya göre; %10,1 oran ile parmak izi çıkarmada en çok kullanılan teknik olarak ikinci sırada WebRTC yer almıştır (https://browserleaks.com/webrtc adresinden tarayıcınızın, WebRTC kaynaklı olarak kamera ve mikrofona izin verdiğiniz ya da vermediğiniz durumda hangi verilerinize erişilebilir kıldığı kontrol edilebilmektedir.) (AEPD, 2019.).

Bununla birlikte web siteleri, Batarya Durumu API'si sayesinde, bataryaya sahip bir mobil cihazın veya bir diz üstü bilgisayarın batarya durumuna erişebilmektedir. Söz konusu API aracılığıyla cihazın batarya seviyesi bilgisi, enerji tasarrufu veya yüksek performans modunda olduğu bilgisi kullanıcının izni ve bilgisi olmadan işlenebilmektedir. *Navigator.getBattery* yöntemini çağıran bir *Javascript* kodunun yer aldığı bir web sitesi; bataryanın seviyesi, dolum zamanı veya batarya boşalma zamanı gibi özelliklerine erişebilmektedir. Bu sayede hem birinci taraf hem de üçüncü taraflar bu bilgiye erişim sağlayabilecektir (Olejnik, Acar, Castelluccia ve Diaz, 2016). Cihazların benzer nitelikleri ve IP adreslerini paylaştığı kurumsal bir ağda, batarya bilgisi NAT arkasında olan cihazları ayırt etmek amacıyla kullanılabilmektedir (Olejnik ve diğerleri, 2016).

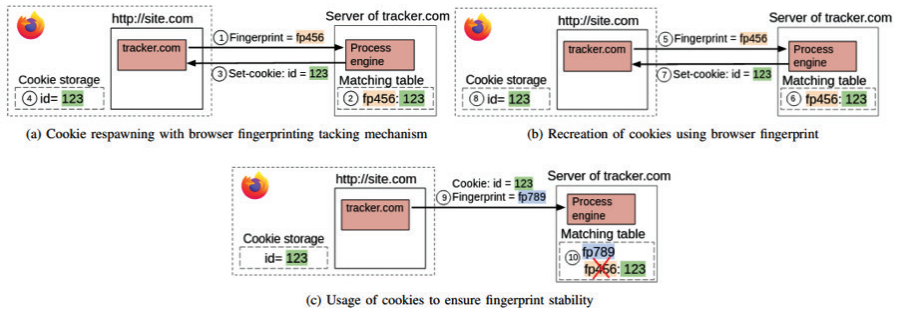
Canvas API aracılığıyla dijital parmak izi çıkarımında ise bu kütüphanenin kullanılması sonucunda oluşan görselin işlenmesindeki farklılıklarından faydalanılmaktadır. Canvas kütüphanesi kullanılarak oluşturulan metin veya grafiklerin işlenmesinde işletim sistemi, yazı kütüphaneleri, cihazın grafik kartı, grafik sürücüsü veya tarayıcısına dayalı olarak bazı farklılıklar meydana gelebilmektedir. Dijital parmak izi çıkaran Javascriptler Canvas kütüphaneleri aracılığıyla; canvas elementinin genelde *"toDataURL"* yöntemi aracılığıyla Base64 karşılığını almak ve bir hash fonksiyonu aracılığıyla özet değerini çıkarmak suretiyle dijital parmak izi oluşturmaktadır. Daha önce de belirtildiği üzere Canvas API aracılığıyla elde edilen parmak izi diğer tekniklerle elde edilen entropi ile birleştirilebilmektedir (Acar ve diğerleri, 2014).

Web GL API sayesinde tarayıcılar ile interaktif üç boyutlu nesneler görüntülenebilmekte ve Javascript aracılığıyla değiştirilebilmektedir. Bu işleme süreci cihazların donanımdaki ve yazımlarındaki farklılıklar nedeniyle aynı değildir. Bu farklılara dayalı olarak dijital parmak izi çıkarılabilmektedir. Yinzhi Cao, Song Li ve Erik Wijmans'ın tarayıcılar arası dijital parmak izi oluşturulmasına yönelik yapmış oldukları çalışmada, cihazın donanımsal ve işletim sistemleri özelliklerine yönelik bilgi toplamak için ağırlıklı olarak WebGL API'ye dayanan bir parmak izi çıkarma tekniği uygulamışlardır. Bu çalışmada 1.903 cihaz üzerinden yürütülen bu çalışmada tek tarayıcı kullanıldığında %99,24 oranla, tarayıcılar arası %91,44 kararlılıkla %83,24 benzersiz olarak tanımlama gerçekleştirilmiştir (Cao, Li ve Wijmans, 2017). Söz konusu API kullanımı ile cihaz özelliklerine dayalı olarak dijital parmak izi çıkarıldığından, daha tutarlı bir tanımlama mekanizması olduğu değerlendirilmektedir.

Çerez Benzeri Dijital Parmak İzi Çıkarma

Bu teknik aslında durum denetlemeli ve durumsuz takip teknolojilerin kesişim noktadır. Zombi (kendini yenileyen) çerezler silinse de çeşitli web depolama alanları aracılığıyla kendini yenileyebilmektedir ("Mitigating Browser Fingerprinting in Web Specifications", 2019). Öte yandan dijital parmak izi aracılığıyla kişinin takibinde kararlılık sorunu ortaya çıkabilse de herhangi bir depolama alanına gerek duyulmaksızın benzersiz parmak izi oluşturma imkânının bulunmaması ve dijital parmak izi kullanımının kişi tarafından kolayca engellenememesi hususları takip için bir avantaj olarak karşımıza çıkmaktadır. Durum denetlemeli takip teknolojisi olarak yer alan çerez teknolojisinde ise; kullanıcı tarafından çerez silindiği ve çerezin oluşturulmasında kullanılan diğer web depolama alanlarını temizlendiği takdirde, çevrim içi takibin devamı için çerezin yeniden oluşturulması ihtiyacı doğmaktadır (Fouad, Santos, Legout ve Bielova 2021).

Çerez benzeri dijital parmak izi çıkarma ile söz konusu iki teknoloji birleştirilerek birbirinin avantajlarından faydalanılmaktadır. Şekil 2'de gösterildiği üzere, takip yapan taraf, dijital parmak izi çıkarma tekniğiyle ilk önce bir tanımlayıcı oluşturabilecek ve bu tanımlayıcı değerini bir çerezde saklayabilecektir. Kişi çerezi temizlese dahi, tanımlayıcı değeri dijital parmak izi aracılığıyla tekrar oluşturulabilecektir. Diğer taraftan, dijital parmak izi zaman içinde değişse bile çerezde saklanan tanımlayıcı sayesinde, eski parmak iziyle kullanıcının yeni parmak izinin eşleşmesi sağlanabilecek ve çevrim içi takip söz konusu iki teknik aracılığıyla daha uzun vadede gerçekleştirilebilecektir.



Şekil 2. Dijital parmak izinin çerez teknolojisi ile birlikte kullanımına bir örnek (Fouad ve diğerleri, 2021)

DİJİTAL PARMAK İZİNİN KULLANIM AMAÇLARI

Dijital parmak izi, web takip teknolojisi olarak değerlendirilmesine rağmen uygulamada birçok amaçla kullanılabilmektedir kullanım amaçları negatif ve yıkıcı ile pozitif ve yapıcı olarak sınıflandırabilmektedir (Lapedrix ve diğerleri, 2019):

Negatif ve yıkıcı amaçlar:
» Kullanıcının açık rızası olmaksızın takibi,
» Bilinen bir zafiyeti tespit ederek kullanıcı cihazına saldırmak

Pozitif ve yapıcı amaçlar:
» Kullanıcıların, cihazlarının güncel olmaması durumunda belirli güncellemelerin önerilmesi
» Kullanıcı ara yüzü uyumlaştırma
» Web sitesi performansının iyileştirilmesi
» Çevrimiçi hizmetlerin güvenliği, bir cihazın orijinal olduğunu ve sistem tarafından bilindiğini doğrulama yoluyla da güçlendirme (Anomali tespiti, kullanıcı kimlik yönetimi)

Çevrim içi takip (tracking); davranışların gözetimi (monitoring) kavramıyla ilişkili ele alınmaktadır. Avrupa Veri Koruma Kurulu (EDPB) tarafından, Genel Veri Koruma Tüzüğü'nün (GVKT) bölgesel kapsam maddesinde yer alan AB'dekilerin davranışlarının gözetimi hususunun değerlendirilmesinde, gözetim kavramının GVKT'de açık bir tanımı olmadığından 24'üncü gerekçe maddesi göz önünde bulundurulmaktadır (European Data Protection Board, 2019a). Anılan gerekçe maddesinde:

> *"...Bir işleme faaliyetinin ilgili kişilerin davranışlarını gözetlenmesi olarak değerlendirilip değerlendirilemeyeceğini belirlemek için, özellikle onu ilgilendiren kararlar alınması veya tercihlerinin, davranışlarının ve bakış açısının tahmini ve analizi amacıyla kişinin profillemesini içeren kişisel veri işleme faaliyeti tekniklerinin potansiyel sonraki kullanımı dahil gerçek kişinin internette takip edilip edilmediğinin (tracking) belirlenmesi gereklidir."* ifadesi yer almaktadır.

Bireyin "gözetimi" konusunda, veri sorumlusunun bir bireyin davranışına ilişkin ilgili verileri toplama ve daha sonra yeniden kullanma amacında olması gerekmektedir (European Data Protection Board, 2019a). Düzenli ve sistematik gözetim faaliyetlerine; bir telekomünikasyon ağının işletilmesi, telekomünikasyon hizmetinin sağlanması, e-posta yeniden hedefleme (Yeniden hedefleme; bir tarayıcının veya cihazın herhangi bir bağlı olmayan web etki alanı veya uygulamasındaki etkinliği hakkında veri toplama veya bu verilerin bir reklamın farklı, bağlantılı olmayan bir web etki alanında veya uygulamada veya ayrı bir cihaz üzerinde özelleştirme amacıyla kullanılmasıdır (Network Advertising Initiative, 2021)), veri-güdümlü pazarlama faaliyetleri, risk değerlendirmesi amacıyla profilleme ve puanlandırma (örneğin; kredi puanlandırma, sigorta primlerinin belirlenmesi, dolandırıcılığın önlenmesi, kara para aklamanın tespiti), konum takibi (örneğin mobil uygulamalar aracılığıyla), sadakat kartları, davranışsal reklamcılık, giyilebilir cihazlar aracılığıyla zindelik, fitness ve sağlık verilerinin izlenmesi, kapalı devre kamera (CCTV), bağlı cihazlar (örneğin akıllı sayaçlar, akıllı arabalar, ev otomasyonu vb.) örnek verilebilir (Madde 29 Veri Koruma Çalışma Grubu, 2017a). Takip faaliyetlerinin oluşturduğu en büyük risk küresel gözetim mekanizması olarak kullanılmasıdır. Gözetim faaliyetleri güvenlik ya da politik sebeplerle hükümetler tarafından gerçekleştirilebileceği gibi ticari amaçlarla şirketler tarafından da gerçekleştirilebilmektedir. Gözetim faaliyetleri kimi zaman ekonomik fayda getirse de kişisel verilerin korunması açısından riskleri de beraberinde getirmektedir (European Union Agency For Cybersecurity (ENISA), 2012). Dijital parmak izi aracılığıyla gözetimin amaçları arasında; konum takibi, davranışsal reklamcılık, dolandırıcılığın önlenmesi gibi amaçlar yer almaktadır.

Konum Takibi

Konum tabanlı servisler iç mekân ve dış mekân olmak üzere ikiye ayrılmaktadır. Dış mekânda kullanılan konum tabanlı servis yöntemi genellikle yüksek doğruluk ve kapsayıcılık nedeniyle Küresel Konumlandırma Sistemi ("Global Positioning System", GPS)'dir. Öte yandan dış mekânda olduğu gibi iç mekânda yüksek doğrulukla GPS ile konum takibi yapılamamaktadır. İç mekânda duvarlar, mobilyalar

ya da elektromanyetik dalga yayınımı engelleyecek diğer faktörler nedeniyle GPS sinyali gücü ciddi bir şekilde düşmektedir.

Konum parmak izi olarak adlandırılan yöntem ile konum tespiti, iki aşamalı olarak gerçekleştirilmektedir. İlk aşama olan eğitim aşaması ya da kalibrasyon aşaması, diğer aşama ise konum tespiti aşamasıdır (Kim,S., Yoo ve Kim, J. (2017). Kalibrasyon aşamasında, parmak izi için haritalar ya ölçüm işlemlerinde deneysel olarak kurulmakta ya da analitik olarak hesaplanmaktadır (Farid, Nordin ve İsmail, 2013). Sinyal parmak izleri olarak adlandırılan RSS ("Received Signal Strength", RSS), sinyal açıları, sinyal yayılma süresi gibi çeşitli radyo sinyali özellikleri ile belirli koordinatlar kalibrasyon aşamasında eşleştirilerek bir veri tabanı oluşturulmaktadır. İkinci aşama olan konum tespiti aşamasında, kullanıcı cihazı bilinmeyen noktadaki sinyal özelliklerini ölçerek bir sunucuya iletir ve mevcut ölçülen sinyal gücü değerleri, bir veri tabanı diğer bir tabir ile radyo haritası ile karşılaştırılarak en uyumlu sinyal parmak iziyle eşleşme sağlandığında bilinmeyen noktanın koordinatları için bir çıkarım sağlanmaktadır (Kim ve diğerleri, 2017). Google Haritalar Android API konumlama sistemi, üçü iç ortamlar ve biri dış ortamlar için olmak üzere dört farklı konum belirleme yöntemine dayanmakta olup iç mekân konumlandırma için parmak izi konumlandırma yöntemi kullanılmıştır (Farid ve diğerleri, 2013). Örneğin, giyilebilir cihazların ilgili kişilere yakın mesafede olması, ilgili kişinin konum takibine izin veren bir parmak izi oluşturulmasında yararlı olan diğer cihazların MAC adresi gibi birtakım tanımlayıcılara ulaşılmasına neden olmaktadır. Birçok sensör cihazın MAC adresinin toplanması benzersiz parmak izleri ve IoT paydaşlarının belirli bireylerle ilişkilendirilebildiği daha stabil tanımlayıcılar oluşturacaktır. Bu parmak izleri ve tanımlayıcılar konum analitiği veya kişilerin ve kitlenin hareket kalıplarının analizi dahil birtakım amaçlar için kullanılabilmektedir (Madde 29 Veri Koruma Çalışma Grubu, 2014b).

İç mekân konumlandırma sistemlerinde; eğer kullanıcı kaydı gerekiyorsa servis sağlayıcısı kullanıcıları, kullanıcı kimlikleri aracılığıyla tanımlayabilmektedir. Kayıt gerekmediği durumlarda ise kullanıcılar, akıllı telefonlardaki benzersiz tanımlayıcılar (IMEI, IMSI, MAC adresi) sayesinde ayırt edilebilmektedir. Bu çerçevede, belirli bir kullanıcının davranış desenlerini belirleme amacıyla veriler bir araya getirebilmektedir. Örneğin belirli MAC adresine sahip kullanıcı A mağazasını bu hafta içinde 5 kez ziyaret etti (Kim ve diğerleri, 2017). Şunu da hatırlatmak gerekir ki, GVKT çerçevesinde bir güvenlik önlemi olarak MAC adreslerinin özet değerleri muhafaza edilse dahi söz konusu özet değerler de GVKT uyarınca kişisel veri olarak kabul edilmektedir (Madde 29 Veri Koruma Çalışma Grubu, 2017b).

Davranışsal Reklamcılık

Davranışsal reklamcılık, bireylerin davranışlarının zaman içinde gözlemlenmesine dayalı olarak yürütülen bir reklamcılık modelidir. Bu modelde; kişi hakkında belirli bir profil oluşturmak ve kişiye özel reklamları sağlamak amacıyla kişilerin hareketleri (site ziyaretleri, etkileşimleri, kullandıkları arama kelimeleri, çevrim içi içerik üretimi gibi) aracılığıyla davranış özellikleri araştırılmaktadır (Madde 29 Veri Koruma Çalışma Grubu, 2010b). Davranışsal reklamcılıkta, kişilerin görüntüledikleri web sayfaları ve görüntüleme süreleri, makaleleri veya diğer öğeleri ne kadar süreyle hangi sırayla görüntüledikleri vb. hususlarda reklamcılara bilgi sağlanarak kişinin çevrim içi yaşamının çok ayrıntılı bir resmi oluşturulmaya çalışılmaktadır.

Çevrim içi davranışsal reklamcılıkta tüm ekosistem, çevrim içi tanımlayıcıların kullanımı üzerine kuruludur. FTC Tüketici Koruma Birimi yöneticisi Jessica Rich (2015) tarafından, dijital parmak izinin başlangıçta yasa dışı kopyalama ve sahtekarlık önleme amacıyla geliştirildiği, ancak daha sonrasında şirketlerin internete bağlı cihazları benzersiz olarak tanımlamak ve bunları kullanan bireyler hakkında detaylı profiller oluşturmak amacıyla kullanmaya başladığı belirtilmiştir. Bu profiller, üçüncü taraf çevrim dışı kaynaklar ile desteklenerek daha detaylı ve kişisel hale getirilmektedir (Rich, 2015).

ICO'nun 2018-2021 Teknoloji Stratejisinde; gizli kişiselleştirme, büyük veri, nesnelerin interneti, görünmez işleme gibi risklere dikkat çekilmiştir. Stratejide; bir dizi alternatif çevrim içi izleme yönteminin (örneğin cihaz parmak izi, tarayıcı parmak izi ve canvas parmak izinin) ortaya çıkması ve bunların daha yaygınlaşmasının çerez kullanımını azaltmadığı belirtilmiştir. Ayrıca, teknoloji stratejisinde daha fazla cihazın internete bağlanmaya ve bireylerin çevrim içi aktivitelerinde daha çok cihazı kullanmaya devam etmesinin olası olduğu; cihaz parmak izi, tarayıcı parmak izi ve canvas parmak izinin yaygınlaştığı ve çevrim içi davranışsal reklamcılık dahil, sistematik izleme ve bireylerin takibinde daha fazla risk oluşturduğu ifade edilerek bu teknolojilerin beraber kullanımındaki müdahalecilik stratejik öncelik olarak ele alınmıştır (Information Commissioner's Office (ICO), 2019.).

Bot ve Dolandırıcılık Önleme

Günümüzde evlerden şehirlere kadar geniş bir kullanım alanına sahip olan IoT cihazlar, *Mirai* (Kelime anlamı olarak Japoncada gelecek adına anlamına gelen Mirai, bir tür zararlı yazılımdır.) gibi ciddi siber saldırıların da hedefi haline

gelmiştir. Ağa bağlı cihazlarda herhangi bir kötücül amaçlı bir cihazın bulunup bulunmadığını tespit etmek birçok durumda ağ güvenliği ve kişisel veri ihlali yaşanmaması adına önemli olabilecektir. Bu konuda önlem alınabilmesi amacıyla IoT cihazlarda anomali tespiti yapılması gerekecektir. IoT anomali tespiti, ağa bağlı cihazların tanımlanması sayesinde yapılabilmektedir. Yeni tanıtılan bir cihaz benzersiz bir şekilde tanımlanabiliyorsa, mevcut IoT cihaz profilleriyle karşılaştırılabilecek, ardından cihaz normal, güvenliği ihlal edilmiş, yetkisiz veya arızalı olarak tanımlanabilecektir. IoT ağ trafiğinin analiz edilmesiyle ağa yeni bağlanan cihazlar olmak üzere tüm cihazların parmak izinin çıkarılması, anomali tespitinde önemlidir (Falola, 2020).

Mobil uygulama mağazaları ve web hizmetleri sahte yüklemeler, sahte incelemeler, spam yorumlar, kazıma istekleri ve diğer sentetik etkileşimler için meşru müşteri kılığına giren saldırganların otomatik kötüye kullanımıyla karşı karşıyadır. Çevrim içi hizmetler sunanlar hizmete talep yapanın bot mu yoksa gerçekten insan mı olduğunu anlama amacıyla çok yaygın olarak *Captcha* (Captcha kelimesinin açılımı *"Completely Automated Public Turing test to tell Computers and Humans Apart"* olarak ifade edilmekte olup Türkçe karşılığı Bilgisayarları ve İnsanları Ayırmak için Tamamen Otomatik Halka Açık Turing testidir.) sistemlerini kullanmaktadır. En fazla kullanılan ise Google'ın *Recaptcha* sistemidir. Bu sistem dijital parmak izi doğrulamasını kullanmaktadır. "Ben robot değilim" olarak işaretlendiğinde eğer sistem, parmak izine dayalı olarak kullanıcının güvenilir olduğunu tespit edebilirse ekstra güvenlik önlemi olan istenilen öğenin yer aldığı resim seçme işlemini uygulamamaktadır (Segers, 2021).

Kimliği doğrulanmış bir kullanıcı için yalnızca çerezin veya çerezle birlikte IP adresinin ilişkili olarak muhafaza edilmesi, oturum çalma saldırılarında veya özellikle hareketli ortamdaki mobil networklerde dinamik IP'lerin sık değişimi hem kullanıcıya iyi bir deneyim sunmayacak hem de saldırganın meşru bir kullanıcıyla aynı IP adresine sahip olduğu durumlarda saldırı tespitini de zorlaştıracaktır (Segers, 2021). Bu tür durumlar göz önünde alındığında dijital parmak izi dolandırıcılığın önlenmesinde risk bazlı bir doğrulama yöntemi olarak kullanılmaktadır (Segers, 2021).

Siber Saldırı Amaçlı Olarak İstihbarat Toplama

Kötücül reklamcılık (malvertising) tekniği aracılığıyla kötücül bir yazılımın hedef cihazlara dağıtımı yapılabilmektedir. Bir reklam bandının sayfaya yüklenmesi sessiz sayfa yönlendirmeleri ile kötücül yazılım yüklenmesine neden olabilmektedir. Saldırganlar reklam ağlarını bu şekilde istismar ederek sahte reklam verenler

olarak hedeflerine saldırabilmektedir. Kötü amaçlı reklamcılık nedeniyle meşru web sitelerini ziyaret eden masum kullanıcıları kötü amaçlı yazılımlara maruz kalabilmektedir. Kötü amaçlı yazılımın hedefe yüklenmesi için bir reklamı tıklamak gibi kullanıcı etkileşimine gerek duyulmamaktadır. Siber suçlular, parmak izi tekniğini kullanarak hangi bilgisayarlara kod parçacığını gönderebileceklerini belirleyebilmektedir. Kötü amaçlı yazılımları tespit etmek için kurulan bal küpleri veya reklam denetimi doğrulaması gerçekleştiren güvenlik şirketleri gibi uygun olmayan hedefler bu şekilde hızla elenebilmekte bunlara sıradan reklamlar gösterilmekte ancak daha savunmasız hedefler suçluların hedefi olabilmektedir (Malwarebytes ve GeoEdge, t.y.).

Kullanıcı Kimlik Yönetimi

Dijital parmak izi kullanıcı kimlik yönetiminde kullanılabilmektedir. Kullanıcı adı ve şifre girmek suretiyle kimliği doğrulamanın yanı sıra dijital parmak izi; kimlik doğrulamada ikinci bir faktör olarak kullanılabilmektedir (Madde 29 Veri Koruma Çalışma Grubu, 2014c). Örneğin, bir dijital parmak izi alma sistemi, ek bir kimlik doğrulama faktörü sağlayarak cihaza dair parmak izini oluşturabilmekte ve bu parmak izine daha önce rastlanıp rastlanmadığını tespit edebilmektedir. Kullanılan kimlik doğrulama sistemi, bu parmak izi daha önce görüldüyse eğer ek kimlik doğrulama faktörünün başarılı olduğunu belirten bir kimlik doğrulama jetonu göndermektedir. Eğer parmak izi daha önce görülmediyse kimlik doğrulama sistemi ek faktör olarak tek seferlik bir şifre doğrulaması yapmaktadır. Söz konusu doğrulama sağlanırsa, bu cihaza dair parmak izi, ek bir faktör olarak gelecekteki kimlik doğrulaması için kullanıcı cihazıyla ilişkili olarak saklanmaktadır (Grajek, Liu, Quach ve Lo, 2018).

Web Analitiği

Dijital Analitik Birliği'nin (eski adıyla Web Analitiği Birliği) resmî tanımına göre web analitiği; ölçüm elde etme, analiz etme ve web deneyimini anlama ve iyileştirme amacıyla internetten toplanan verinin raporlanmasını ifade etmektedir (Bekavac ve Praničević, 2015). Ölçüm; sayılar, oranlar ve anahtar performans göstergeleri (key performance indicator-KPI) şeklinde ifade edilir (Web Analytics Association, 2010). Herhangi bir kuruluşun KPI göstergesi web iş modeline göre değişkenlik gösterecektir. İş modeli; belirli bir kuruluşa gelir oluşturan ürün veya hizmete yeni bir değer katan yöntem olarak tanımlanmaktadır. Temel Web iş modelleri; (1) Simsarlık (brokerage), (2) Reklam modeli (3) Bilgi temsilcisi modeli, (4) Ticari model, (5) Üretim modeli, (6) Bağlı kuruluş/ortak çalışma modeli, (7) Sanal topluluk modeli, (8) Abonelik modeli ve (9) Yardımcı/fayda hizmetler

olarak sıralanmaktadır (Bekavac ve diğerleri, 2015).

Web analitiği hakkında yapılan bir araştırma kapsamında 570 katılımcının *"Kuruluşunuzda bir işlev olarak web analitiğinin amacı nedir? (Birden fazla yanıt verilebilmekteydi.)"* sorusuna vermiş olduğu cevaplar neticesinde ortaya çıkan sonuçlar;

- Web sitesi işlevselliğini ve dönüşümünü optimize etme (yüzde 79,7),
- Geçmiş performansın analizi (yüzde 73,7),
- Pazarlama kampanyalarının performansını ve dönüşümlerini optimize etme (yüzde 67,3),
- A/B ve çok değişkenli testler yoluyla en iyi yaratıcı uygulamaları belirleme (yüzde 49,8),
- Sitenin yeniden tasarımı için temel bilgiler (yüzde 48,6),
- Gelecekteki pazarlama kampanyalarını geliştirmek için tahmine dayalı metrikler (yüzde 41),
- Yaklaşan iş hedefleri için bütçeleme ve planlama (yüzde 32,7),
- Diğer (yüzde 5,6)

olarak sıralanmıştır (Web Analytics Association, 2011).

Web analitiğinde, bir sunucunun log dosyaları analizi veya web sayfalarının *javascript* komut dosyaları aracılığıyla etiketlenmesi sonucunda veri elde edilebilmekte olup bu yöntemlerden ikincisi daha popüler olarak kullanılmaktadır (Bekavac ve diğerleri, 2015).

Profesyoneller tarafından yaygın olarak kullanılan web analitik araçlarının ilk dokuzunda sırasıyla, Google Analitik, Mixpanel, Kissmetrics, Adobe Analitik, Matomo, Open Wn Analytics, Woopra, Hotjar, HubSpot araçlarının yer aldığı görülmüştür ("Top 12+ web analytics tools to improve your site and grow your business", 2023). Web Analitiği Derneği Görünüm Raporunda tüm web analitiği endüstrisinin yüz yüze geldiği sorunlar arasında 4. sırada "mahremiyet" yer almaktadır (Web Analytics Association, 2011). Mahremiyet odaklı analitik araçların özellikleri arasında; açık kaynak kodlu olması, bir günlük bir süre diliminde kullanıcıyı benzersiz olarak tanımlaması gibi özellikler sayılabilmektedir. Analitik ölçümde, örneğin IP bilgisinin, kullanıcı aracısı bilgisinin ve günlük olarak oluşturulan bir salt değerinin toplu olarak özet fonksiyonundan geçirilmesi gibi benzeri yöntemlerle her bir kullanıcının bir önceki günkü tanımlayıcısı arasında bağlantı kurulmasının önlenmesi, IP bilgisi veya kullanıcı aracı bilgisinin loglar dahilinde, veri tabanında veya diskte saklanmaması gibi önlemlerle mahremiyetin korunması amaçlanabilir (Plausible, t.y.).

Her ne kadar bazı analitik araçlar mahremiyet odaklı olarak çalıştığında, kullanıcıyı tanımlama süresi bakımından bir sınırlılıkla hareket etse de performans odaklı analitik araçları kullanmayı hedefleyen bir kuruluşun daha doğru bilgi elde etme amacıyla kullanıcıları daha uzun süre benzersiz olarak tanımlamayı talep etmesi işletmenin performans hedefinin doğal bir sonuç olarak karşımıza çıkabilecektir. Dijital parmak izi de özelliği bakımından sürekli bir tanımlayıcı olabildiği ve farklı tarayıcılar arası takibi mümkün kıldığı göz önünde bulundurulduğunda, analitik amaçlı olarak kullanılmasının performansı arttırması beklenebilir. Bazı çevrim içi hizmetler tarafından, AB hukuku kapsamında çerezlerin analitik ölçüm amaçlı olarak kullanımında rıza almaktan kaçınmak için çerezlere alternatif olarak dijital parmak izi çıkarma yönteminin kullanılması önerilmiştir (Madde 29 Veri Koruma Çalışma Grubu, 2014c). Bu durum, çerez kullanımında rıza almaktan kurtulmak ve dijital parmak izi kullanarak görünmez bir şekilde amacın gerçekleştirilmesi olarak yorumlanabilecektir.

Güncelleme

Cihazlarda gerekli güncellemelerin yapılması için dijital parmak izi teknolojisi kullanılabilmektedir. Bu yöntem sayesinde, basit bir güvenlik taramasıyla, ağ üzerinde binlerce farklı konfigürasyonu idare eden sistem yöneticileri, kolaylıkla eski bileşenlere sahip cihazları tanımlayarak düzeltmeleri ve güncellemeleri çok hızlı bir şekilde ilgili cihazlara uygulayabilecektir (Laperdrix ve diğerleri, 2020).

Örneğin, finansal kuruluşlar çevrim içi işlemlerin güvenliğini sağlamak üzere, sunucu güvenliği için ciddi anlamda güvenlik önlemi almaktadır. Bunun yanı sıra kullanıcı cihazının güvenliğini de göz önünde bulundurmak amacıyla alınan önlemler kapsamında dijital parmak izi kullanılabilmektedir. Örneğin; artık desteklenmeyen IOS işletim sistemine sahip bir cihaz, ortaya çıkan zafiyetler için güncelleme alamayacaktır. Bu durumda kurumlar dijital parmak izi aracılığıyla güncel olmayan sistemlerin tespitini yaparak kullanıcıları bu konuda bilgilendirebilecek veya işlem güvenliği için bu cihazlarda uygulamaların kullanımını kısıtlayabilecektir (Segers, 2021).

Kullanıcı Ara Yüzü Kontrolü

Dijital parmak izi, masa üstü bir bilgisayardaki web tarayıcısının yapılandırma ayarlarıyla sınırlı değildir. Ayrıca, bu teknoloji belirli bir protokole bağlı olmayıp mobil cihazlar, akıllı televizyonlar, oyun konsolları, e-kitap okuyucular, internet radyoları, araç içi sistemler, akıllı sayaçlar gibi birçok çeşitte internete bağlı ci-

hazda dijital parmak izi kullanımı mümkündür (Madde 29 Veri Koruma Çalışma Grubu, 2014c).

Çoğu durumda web sitesinde yer alan içeriklerin cihazın teknik özelliğine göre uyumlulaştırılması gerekmektedir. Örneğin; bir web sitesi içeriğine bir tablet veya bir akıllı TV aracılığıyla ulaşılması durumuna göre web sitesinin görüntüleneceği ekran boyutu birbirinden farklı olacaktır. Bir web sitesi veya bu web sitesinde yer alan içerikler nedeniyle ziyaret edilen web sitesi operatörü dışındaki bir taraf, kullanıcı cihazının teknik özelliklerini sorgulayabilmektedir (Madde 29 Veri Koruma Çalışma Grubu, 2014c). Bu teknik özellikler, aynı zamanda dijital parmak izi çıkarılmasında kullanılan nitelikler, veri noktaları olarak da karşımıza çıkabilecektir. Bu öz niteliklerin takip amaçlı kullanılıp kullanılmadığının tespitinde, elde edilen veri noktalarının sayısı ve elde edilen veri noktalarının kullanım amacıyla bağlantılı ve ölçülü olup olmadığı değerlendirilebilecektir.

KARŞILAŞTIRMALI HUKUKTA DİJİTAL PARMAK İZİNE İLİŞKİN ÇEŞİTLİ DÜZENLEMELER

Dijital Parmak İzinin Kişisel Veri Niteliği

Dijital parmak izinin kişisel veri olarak değerlendirilmesi açısından bazı belirsizlikler gündeme gelebilecektir. Reklam ekosistemindeki taraflar dijital parmak izi gibi çevrim içi tanımlayıcıların kişisel veri kapsamı içinde yer almadığı iddia edebilir, ancak çoğu ülke; mevzuatında, emsal kararlarında veya rehberlerinde cihaz tanımlayıcılarını açık olarak kişisel veri olarak tanımaktadır (Sallinger Privacy, 2020). Dijital parmak izi çıkarılmasını kapsayan işleme faaliyetlerine kişisel veri koruma kurallarının uygulanması bakımından, bu merkez unsurun analizi önem arz etmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (Kanun) temel aldığı 95/46/AT sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Birliği Konseyi Direktifi'nin (Direktif) ikinci maddesinin (a) bendinde kişisel veri tanımlanmaktadır. Direktif'te yer alan kişisel veri tanımında; (i) Kişisel verinin kimliği belirli veya belirlenebilir gerçek kişiye ilişkin herhangi bir bilgi olduğu, (ii) Kimliği belirlenebilir gerçek kişinin doğrudan veya dolaylı olarak kimliğinin belirlenebileceği, (iii) Özellikle kimlik numarasıyla veya onun fiziksel, psikolojik, ruhsal, ekonomik, kültürel veya sosyal kimliğine özgü bir veya birden fazla etmen ile kimliğinin belirlenebileceği ifade edilir. Bir kişi ismi ile direkt veya telefon numarası araba plakası, sosyal güvenlik numarası, pasaport numarası aracılığıyla dolaylı olarak tanımlanarak veya dâhil olduğu gruptaki insanlar yaş, mesleği, ikametgâhı gibi verilerle daraltılmasını sağlayan bir kritere göre tanımlanabilir.

Somut olayda tanımlayıcıların, tanımlama durumu değişken olabilmektedir. Örneğin; çok sık rastlanan bir soyadı bir ülke içinde kişiyi tanımlamak için yeterli olmaz iken bir sınıf içerisinde tanımlamak için yeterli olabilmektedir. Trafik ışıklarında bekleyen siyah takım giymiş adam tabiri dahi trafik ışıklarında bekleyen adamı tanımlamak için kullanılabilir. Bu yüzden kişiyle ilişkili bilginin bir kişiyi tanımlayıp tanımlamaması durumu somut olayda değişkenlik göstermektedir (Madde 29 Veri Koruma Çalışma Grubu, 2007).

2011 yılında www.youronlinechoices.eu adresindeki internet sitesinde çoğu durumda, reklam gösterimi amacıyla toplanan bilginin kişisel veri olmadığı, söz konusu bilginin kişiyi tanımlamadığı iddia edilmiş olsa da Madde 29 Çalışma Gurubu'nun 02/2010 sayılı Görüşünde, davranışsal reklamcılığın, çerez veya cihaz parmak izi gibi benzersiz tanımlayıcıların işlenmesini kapsadığı ifade edilmiştir (Madde 29 Veri Koruma Çalışma Grubu 2010b). Bu tür benzersiz tanımlayıcılar, IP adresi silinse veya anonim hale getirilse dahi kullanıcıların takibine imkân tanımakta, yani bu tanımlayıcılar aracılığıyla davranış takibi amacıyla kullanıcı tekilleştirilmektedir, dolayısıyla benzersiz tanımlayıcılar kişisel veri olarak nitelendirilmektedir (Madde 29 Veri Koruma Çalışma Grubu, 2011). Benzersiz tanımlayıcıların kişinin kimliğini belirlemediği iddiaları veri koruma kuralları kapsamından çıkmak amacıyla üretilse de başarıya ulaşamamıştır.

www.youronlinechoices.eu isimli sitenin Birleşik Krallık için hazırlanan güncel durumuna ulaştığımızda, çerez veya dijital parmak izi gibi benzeri teknolojiler aracılığıyla davranışsal reklam sunulmasında, kişisel veri işlenmediği yönünde herhangi bir açıklamanın yer almadığı gözlemlenmektedir. Ancak aynı sitenin Türkiye için hazırlanan versiyonuna ulaştığımızda, davranışsal reklamcılık için *"kişisel bilgilerin toplanmadığı, isim, adres veya e-posta adresi gibi hiçbir bilgi kullanılmadığı ve gerçek dünyadaki kimliğiniz tespit edilmediği, sistemde web tarama aktivitenize ilişkin veriler anonim olarak toplandığı ve analiz edildiği"* ifadelerine rastlanmaktadır.

Madde 29 Veri Koruma Çalışma Grubunun 2/2010 sayılı "Çevrim İçi Davranışsal Reklamcılık Hakkında Görüşü"nde; davranışsal reklamcılık yöntemlerinin, IP adreslerinin toplanmasını ve benzersiz tanımlayıcıların, örneğin dijital parmak izinin, işlenmesini gerektirdiği ifade edilmiştir (Madde 29 Veri Koruma Çalışma Grubu, 2010b). Ancak, IP adresleri dinamik olarak zaman içinde değiştiği için kullanıcı takibinde benzersiz tanımlayıcılardan faydalanılarak yapılan çevrim içi takip daha stabil hale getirilmektedir. Söz konusu görüşte; ilgili kişilerin gerçek ismi bilinmese dahi, benzersiz tanımlayıcılar aracılığıyla bireylerin "tekil hale getirildiği" ifade edilmiştir (Madde 29 Veri Koruma Çalışma Grubu, 2010b).

95/46/AT sayılı Direktif'in kişisel veri tanımı içerisinde doğrudan çevrim içi tanımlayıcılar yer almasa da Madde 29 Çalışma Grubunun cihaz parmak izine 2002/58/AT sayılı Direktif'in uygulanmasına ilişkin görüşünde; cihaz parmak izinin kişisel veri olabileceği, örneğin birkaç bilgi öğesi, özellikle IP adresi gibi benzersiz tanımlayıcılar birleştirildiğinde ve işlemenin amacı kullanıcıları zaman içinde ve siteler arası tanımlamak olduğunda (örneğin; davranışsal reklamcılık) veri koruma kurallarına uyum sağlanması gerektiği açıkça ifade edilmiştir (Madde 29 Veri Koruma Çalışma Grubu, 2014c).

Ayrıca, davranışsal reklamcılık kapsamında elde edilen bilgi, bir kişi hakkında olduğundan kişiyle içerik kriteri bakımından ilişkilendirilmektedir. Zira bu kapsamda elde edilen bilgi belirli bir kişinin özellikleri ve davranışlarıdır. Ayrıca elde edilen bu bilgi belirli bir kişiyi etkilemek amacıyla kullanılarak amaç kriteri bakımından ilgili kişiyle ilişkilendirilmektedir (Madde 29 Veri Koruma Çalışma Grubu 2010b).

Öte yandan, herhangi bir zamanda ilgili kişi tarafından sağlanan doğrudan tanımlayıcı bilgi ile kullanıcı profillerinin ilişkilendirilme olasılığı da bulunmaktadır. Örneğin dijital parmak izi aracılığıyla kullanıcıyı çevrim içi takip eden bir sosyal ağda kişi bir üyelik hesabı oluşturduğunda veya mevcut üyelik hesabına giriş yaptığı durumda kişinin kimliğinin belirlenmesi söz konusu olacaktır. Kişinin kimliğinin belirlenme olasılığı yalnızca bununla sınırlı değildir; şirket birleşmeleri, veri ihlali sonucu oluşan veri kayıpları, internete açık kişisel veriye ulaşılabilirliğin artması gibi nedenler de sayılabilecektir (Madde 29 Veri Koruma Çalışma Grubu 2010b).

AB Genel Veri Koruma Tüzüğü (GVKT) kişisel veri kavramını 4'üncü maddesinin birinci fikrasında tanımlanmış olup, Direktif ve GVKT'de yer alan kişisel veri tanımına baktığımızda; Direktif'ten farklı olarak GVKT'de konum verisi, çevrim içi tanımlayıcı aracılığıyla ve genetik olarak gerçek kişinin kimliğinin belirlenebileceği ifade edilmektedir. GVKT'nin 26'ncı resitaline göre; gerçek kişinin kimliğinin belirlenebilir olup olmadığını belirlemek örneğin tekil hale getirme (single out) (Bir kişiyi bir grup insan içinden seçip ayırmak, tekilleştirmek GVKT'de "single out" terimi ile karşımıza çıkarken aynı anlamda "individuation" terimi de kullanılabilmektedir.), yani bir kişiyi bir grup insan içinden kişiyi direkt veya dolaylı olarak belirlemek, amacıyla veri sorumlusu veya başka bir kişi tarafından kullanılabilecek makul muhtemel tüm araçlar göz önünde bulundurulmalıdır. Söz konusu araçların kişiyi tanımlamak amacıyla kullanılmasının makul olarak muhtemel olup olmadığını belirlemek için işlemenin gerçekleştiği sıradaki ulaşılabilir teknoloji ve teknolojik gelişmeler ile kimlik belirleme için ihtiyaç duyulan zaman ve maliyet gibi tüm objektif etmenlerin birlikte değerlendirilmesi gerekmektedir. GVKT'nin çevrim içi tanımlayıcılar hakkındaki 30'uncu gerekçe maddesinde ise; kişiler cihazları, uygulamaları, araçları ve protokolleri tarafından sağlanan çevrim içi tanımlayıcılar aracılığıyla kişilerle (IP adresleri, çerez tanımlayıcıları gibi diğer tanımlayıcılar) ilişkilendirilebildiği ifade edilmektedir. GVKT'nin 30'uncu gerekçe maddesinin devamında; bu durumun özellikle sunuculara iletilen benzersiz tanımlayıcılar ve diğer bilgilerle birleştirildiğinde, gerçek kişilerin profillerini oluşturmak ve onların kimliğini belirleme kullanılabilecek izler bırakabildiği belirtilmektedir.

Dijital ekonominin gerçekleri, kimliği belirlenebilir bireyin mahremiyetine zarar verileceği varsayımına meydan okumaktadır. Bir kitle içinde belirlenenler, kimliği bilinmese veya bilinebilir olmasa dâhi birey düzeyinde çevrim içi olarak takip edilmekte, profillenmekte, hedeflenmekte, iletişim kurulmakta veya kişi üzerinde etkileri olan bir karara ya da davranışa maruz bırakılmaktadır (Johnston, 2020). GVKT'nin açıklayıcı maddelerinde (resitallerinde) tekil hale getirme kavramına yer verilmesi veya kişisel veri tanımı kapsamında çevrim içi tanımlayıcı kavramına yer verilmesinin kişinin kimliğinin belirlenebilir olmasının dar yorumlanmaması gerektiğinin bir göstergesi olduğu anlaşılmaktadır.

2018 tarihli Birleşik Krallık Veri Koruma Kanunu'nun (DPA) 3'üncü maddesinin ikinci fikrasında kişisel veri; kimliği belirli veya belirlenebilir yaşayan bir bireye ilişkin bilgi olarak tanımlanmaktadır. Aynı maddenin üçüncü fikrası uyarınca, ilgili kişi; "(a) bir isim, kimlik numarası, konum verisi veya çevrimiçi tanımlayıcıyı veya (b) bireyin sosyal, kültürel, ekonomik, ruhsal, genetik, psikolojik, fiziksel kimliğine özgü bir veya birden fazla etmen"i referans alarak direkt veya dolaylı olarak kimliği belirlenebilir yaşayan bir birey olarak tanımlanmıştır. Bu tanım GVKT'nin kişisel veri tanımıyla uyuşmakla beraber, GVKT'de gerçek kişi kullanılırken DPA 2018'de kişisel veri tanımında yaşayan birey kavramına yer verilmiştir.

Birleşik Krallık Veri Koruma Ofisi ICO tarafından çerez benzeri teknolojiler arasında sayılan dijital parmak izi; belirli bir cihazı benzersiz şekilde tanımlamak amacıyla bir dizi bilgi öğesini birleştirmeyi içeren bir teknik olarak tanımlamaktadır (Information Commissioner's Office, t.y.b). Bir cihazın konfigürasyonundan elde edilen veriler, belirli ağ protokollerinin kullanımıyla açığa çıkan veriler, CSS bilgisi, Javascript nesneleri, HTTP başlık bilgisi, saat bilgisi, TCP yığın varyasyonu, yüklü yazı tipleri, tarayıcıda yüklü eklentiler, herhangi bir API'nin kullanımı gibi veri noktalarıyla sınırlı olmamak üzere bu veri noktalarından veri türetilerek oluşturulan dijital parmak izi; kişiyi, tarayıcı veya cihazı tekilleştirmede, ilişkilendirmede, çıkarım yapmada kullanılabilmektedir (Madde 29 Veri Koruma Çalışma Grubu, 2014c), (Information Commissioner's Office, t.y.b).

Dijital parmak izi çıkarımında toplanan bilgi öğelerini daha önce de ele aldığımız gibi IP adresleri veya çerezler vb. diğer bilgilerle birleştirmek de mümkündür. ICO da GVKT'nin 30'uncu gerekçe maddesinde açıklanan çevrim içi tanımlayıcıları göz önünde bulundurarak DPA 2018'i uygulamaktadır. Dijital parmak izi çevrim içi tanımlayıcılar arasında yer almakta olup kişisel veri olduğu belirli durumlarda veri koruma kuralları uygulanmaktadır. Örneğin kullanıcının hesabına giriş yaptığı bir durumda kimlik doğrulanması amacıyla dijital parmak izi kullanıldığı takdirde, dijital parmak izi aracılığıyla kişisel veri işlenmesi gündeme gelebilecektir. Çevrim içi tanımlayıcıların tek başına veya mevcut olabilecek diğer verilerle birlikte bir kullanıcıyı diğerinden ayırt etmek için kullanılıp kullanılamayacağının hususunda değerlendirme yapmak suretiyle kişinin kimliğinin belirlenebilir olup olmadığının kontrol edilmesi tavsiye edilmektedir. (Information Commissioner's Office, t.y.a).

Dijital parmak izi için elde edilen veri noktalarının sayısı ve entropi miktarının kullanıcıyı benzersiz olarak tanımlamak açısından önemli olduğunu dile getirmiştik. Bir çevrim içi hizmetin alınması esnasında, veri sorumlusuna açıklanan veri kümesi sayesinde dijital parmak izi çıkarılabilecektir. Dijital parmak izi aracılığıyla kişi, çevrim içi olarak tekilleştirilerek kişiyle oluşturulan tanımlayıcı değeri kişiyle ilişkilendirilebilecek veya kişi hakkında çıkarım yapılması söz konusu olabileceğinden, kişisel veri işlenmesi gündeme gelecektir.

Veri Sorumlusu – Veri İşleyen

95/46/AT sayılı Direktif'te veri sorumlusu; kişisel verilerin işlenmesinin amaçlarını ve araçlarını tek başına veya başkalarıyla birlikte belirleyen gerçek veya tüzel kişi, kamu otoritesi, kurum veya diğer herhangi bir organ olduğu ifade edilmektedir.

Kişisel verilerin işleme amacını ve vasıtasını tek başına veya birlikte belirleyen tüzel veya gerçek kişilerin veri sorumlusu olabilmesinin belirtilmesi 95/46/AT sayılı Direktif döneminde de ortak veri sorumluluğunun kabul edildiği anlamına gelmektedir. Direktif döneminde Madde 29 Çalışma Grubunun veri sorumlusu ve veri işleyen hakkında görüşünde; Direktif'te yer alan veri sorumlusunun ortak olarak kişisel veri işleme amaç ve yöntemlerini belirlenmesine ilişkin olarak; sorumluluğun eşit olarak paylaşılmasına gerek olmadığı, işlemenin tüm amaç ve yöntemlerinin belirlenmesinde çok yakın bir ilişki olabileceği gibi örneğin, yalnızca amaçları veya araçları veya bunların bir kısmını paylaşmak gibi daha sıkı olmayan bir ilişki içerisinde olabileceği ifade edilmiştir (Madde 29 Veri Koruma Çalışma Grubu, 2010a).

Bununla birlikte, kişisel verilerin işlenmesinde farklı tarafların iş birliği yapması, her durumda ortak veri sorumlusu oldukları anlamına gelmemektedir. Ortak bir amaç veya araç paylaşmadan iki taraf arasındaki veri alışverişi vuku bulması, yalnızca ayrı veri sorumluları arasında bir veri aktarımı olarak düşünülmesi gerekmektedir.

Ortak veri sorumluluğu için içtihat oluşturan önemli kararlardan birisi de Avrupa Adalet Divanı tarafından verilen Fashion ID Kararıdır. Fashion ID kararındaki taraflar arasında yer alan Fashion ID GmbH & Co. KG, moda ürünleri satan bir çevrim içi perakendeci olup web sitesine Facebook beğen butonunu yerleştirmiştir. Bir kullanıcı Fashion ID'nin web sitesine girdiğinde, o kullanıcı hakkında IP adresi ve tarayıcı dizisi bilgileri (Yüksek Mahkeme IP ve tarayıcı dizesinin tek başına veya birlikte mi kişisel veri olup olmadığını tartışmamış, bu değerlendirmeyi ulusal mahkemeye bırakmıştır.) Facebook'a aktarılır. Bu aktarım, kullanıcının "Beğen" düğmesini tıklayıp tıklamadığına ve bir Facebook hesabına sahip olup olmadığına bakılmaksızın Fashion ID'nin web sitesi yüklendiğinde otomatik olarak gerçekleşmektedir (Avrupa Birliği Adalet Divanı (ABAD), 2018).

Fashion ID'nin web sitesine "beğen" butonu yerleştirmesindeki amaç Facebook sosyal ağı aracılığıyla ürünlerinin görünürlüğünü arttırmaktı. Veri, sonraki kendi ticari amaçları için Facebook İrlanda'ya aktarılmıştır (ABAD, 2018). Bu yüzden Fashion ID, üçüncü taraf eklentiyi internet sitesine yerleştirmek suretiyle kullanıcının kişisel verini toplanmasına ve iletilmesine neden olmuş ve veri sorumlusu olarak değerlendirilmiştir. Öte yandan bu veri sorumlusunun (ortak) sorumluluğu kişisel verilerin işlenme amacı ve yöntemini etkin bir şekilde birlikte karar verildiği faaliyetler için sınırlıdır. Rıza ve bilgilendirme yükümlülükleri, Fashion ID'nin dahil olmadığı ve mantıksal olarak herhangi bir araç veya amaç belirlemediği veri işlemenin sonraki aşamalarını kapsamamaktadır (ABAD, 2018).

Aktif dijital parmak izi çıkarılması yöntemi kapsamında bir internet sitesine veya uygulamaya yerleştirilen bir javascript kodu aracılığıyla veya HTTP paketi kapsamında kullanıcı cihazı veya uygulama örneğinin belirli özelliklerini üçüncü bir tarafa iletilmesi yoluyla benzersiz bir tanımlayıcı oluşturulması ile bu tanımlayıcı sayesinde kişinin belirlenmesi, bu yöntemlerle kişinin cihazı hakkında bilgi toplanması kişisel veri işleme faaliyeti olarak değerlendirilebilecektir. Burada verilerin iletilmesi noktasında reklam geliri gibi ekonomik fayda gören web sitesi yayımcısının verilerin üçüncü tarafa iletilmesi konusunda veri sorumlusu olabileceği değerlendirilebilecektir. Bu noktada, bu kod parçacığı aracılığıyla reklam ağına iletilen veri işlenmeye devam edecek olup reklam ağı sahibi de veri sorumlusu olabilecektir. Söz konusu işleme faaliyetleri "ortak bir amaç" olarak

davranışsal reklamcılık ve "ortak bir araç olarak" ise dijital parmak kullandığı çıkarımı yapılabileceği değerlendirilmektedir. İki tarafın da bu konuda iş birliği gerektiğinden, ortak veri sorumluluğu gündeme gelecektir. Bununla birlikte web sitesi operatörünün hizmet satın alması ile işlemenin temel amaç ve yöntemlerine tek başına karar verdiği durumda, veri sorumlusu olarak web sitesi operatörünün bir veri işleyenden hizmet satın alımı yapıldığı değerlendirilebilecektir. Böyle bir senaryo, bir web sitesi tarafından analitik ölçüm hizmetlerinin kullanılması halinde söz konusu olabilecektir.

İşleme Şartları ve Genel İlkeler

Çevrim içi takip teknolojilerinin kullanılması söz konusu olduğunda, AB hukukunda öncelikle elektronik haberleşme hizmetlerinde kişisel verilerin korunmasına ilişkin düzenleme olan 2002/58/AT sayılı Direktif, GVKT öncesinde 95/46/AT sayılı Veri Koruma Direktifi, mevcutta ise Genel Veri Koruma Tüzüğü'ne uyumluluk gözetilmelidir. AB üyeleri ülkeler, 2002/58/AT sayılı Direktifi, iç hukuklarında ilgili veri koruma kanunlarına kapsamında veya ayrı özel bir kanun olarak uygulamaya koymaktadır.

2002/58/AT sayılı E-Gizlilik Direktifi'nin 24'üncü giriş hükmünde;

- Ajan yazılımlar, web bugs, gizli tanımlayıcılar veya diğer araçların; bilgiye erişmek, bilgi depolanması veya kullanıcının hareketlerinin izlenmesi amaçlarıyla kullanıcının terminal cihazına kullanıcının bilgisi dışında giriş yapabileceği ve kullanıcının mahremiyetine ciddi bir şekilde zarar verebileceği,

- Bu tür araçların kullanımına ilgili kullanıcıların bilgisi dahilinde, yalnızca meşru amaçlarla izin verileceği, belirtilmektedir.

2002/58 sayılı E-Gizlilik Direktifi'nin 25'inci giriş hükmünde ise;

- Örneğin "çerezler" olarak adlandırılan bu tür araçların, örneğin web sitesi tasarımının ve reklamın etkinliğinin analiz edilmesinde ve çevrim içi işlemlerde bulunan kullanıcıların kimliğinin doğrulanmasında meşru ve faydalı bir araç olabileceği,

- Bu tür araçların, bilgi toplumu hizmetlerinin sağlanmasını kolaylaştırmak gibi meşru bir amaç için tasarlandığı durumlarda, 95/46/AT sayılı Direktif uyarınca kullanıcılara açık ve kesin bilgiler sağlanması koşuluyla kullanımlarına izin verilmesi gerektiği,

- Kullanıcılar, terminal ekipmanlarında bir çerez veya benzeri bir aracın saklanmasını reddetme fırsatına sahip olması gerektiği,

- Kullanıcının terminal ekipmanına kurulacak çeşitli cihazların aynı bağlantı sırasında kullanımı için ve ayrıca bu cihazların sonraki bağlantılarda daha sonraki kullanımlarını da kapsayacak şekilde bilgi ve reddetme hakkının bir kez sunulabileceği,

- Bilgi verme, reddetme hakkı sunma veya izin isteme yöntemleri mümkün olduğunca kullanıcı dostu olması gerektiği,

belirtilmektedir.

Direktif'in işleme şartlarıyla ilgili olan maddesi olan 5'inci maddesinin üçüncü fıkrası uyarınca;

- Elektronik iletişim ağı üzerinden bir iletişimin gerçekleştirilmesi ya da kolaylaştırılması veya

- Abone veya kullanıcı tarafından açıkça talep edilen bir bilgi toplumu hizmetini sağlamak için kesinlikle gerekli olan herhangi bir teknik depolama veya erişim hariç olmak üzere, diğer depolama ve erişim faaliyetleri için veri sorumlusu tarafından işleme amaçları ve söz konusu işlemeye itiraz etme hakkı tanınarak 95/46/AT sayılı Direktif ile uyumlu olarak yalnızca ilgili abone veya kullanıcıya açık ve kapsamlı bilgi sağlanması koşuluyla kullanıcı veya abone tarafından izin verilmesi durumunda gerçekleştirilebileceği,

düzenlenmiştir.

2002/58/AT sayılı Direktif'in 5'inci maddesinin üçüncü maddesi ile elektronik haberleşme şebekesinin kullanımı, kullanıcının terminal cihazına bilgi depolamak veya depolanan bilgiye erişimi belirli şartlar altında kullanıcı rızası olmaksızın gerçekleştirilebilmektedir. Bu durumlar haricinde kullanıcının rızası zorunlu kılınmıştır. Madde 29 Veri Koruma Çalışma Grubu'nun dijital parmak izi çıkarımı hakkındaki görüşü (2014c) ile söz konusu maddenin dijital parmak izine uygulanması benimsenmiştir. Ancak dijital parmak izi çıkarımı, doğrudan kullanıcı cihazına erişerek bilgi toplanması suretiyle gerçekleşebildiği için aslında bir depolama faaliyeti, buna bağlı olarak depolanan bilgiye erişimi gerektirmemektedir. Dijital parmak izi tekniğinin bu özelliği göz önünde bulundurulduğunda, E-Gizlilik Direktifi'nin 5'inci maddesinin üçüncü fıkrasının bu açıdan yeniden ele

alınması gerektiği değerlendirilmektedir. Madde 29 Veri Koruma Çalışma Grubu tarafından dijital parmak izi kullanımının öncelikle 2002/58/AT sayılı Direktif'in uygulama alanına girdiği hususuna açıklık getirilmiştir (Madde 29 Veri Koruma Çalışma Grubu, 2014c). Örneğin dijital parmak izi çıkarımı yapan web sitesi yayımcısı bakımından da E-Gizlilik Direktifi kişisel veri işlenmesine bakılmaksızın geçerli olacaktır. Bu Direktif'in 5'inci maddesinin üçüncü fıkrasında belirtilen istisnalar dışında kalan dijital parmak izi kullanımları için de kullanıcının açık rızası gerekli olacaktır. Eğer dijital parmak izi aracılığıyla kullanıcı cihazında bilgi depolama veya buna erişim gerçekleşmesi sonucunda toplanan bilgi kişisel veri olarak değerlendiriliyorsa, Direktif'in 5'inci maddesinin üçüncü fıkrasına ek olarak GVKT de uygulama alanı bulacaktır.

E-Gizlilik Direktifi'nin 17'nci giriş hükmünde; bu Direktif'in amaçları doğrultusunda, kullanıcı veya abonenin rızasının, 95/46/AT sayılı Direktif'te tanımlandığı ve ayrıca belirtildiği şekilde ilgili kişinin rızası ile aynı olduğu ifade edilmektedir. Kullanıcı bir internet sitesine girdiği zaman dijital parmak izi oluşturulması amacıyla bilgiye erişim mevcutsa, E-Gizlilik Direktifi uyarınca, söz konusu Direktif'in 5'inci maddesinin üçüncü fıkrasında belirtilen istisna hallerdeki kullanımlar dışında, kullanıcının veya abonenin rızasının özgürce ve bilinçli bir şekilde alınması gereklidir. Örneğin, benzersiz dijital parmak izi çıkarımına katkı sağlayan bazı niteliklere web sitesi yayımcısı veya alt şirketleri tarafından kimlik doğrulama amacıyla erişim sağlandığı takdirde, bu kullanım E-Gizlilik Direktifi kapsamında sayılan istisna haller içinde yer alabileceğinden, kullanıcının rızası olmaksızın dijital parmak izi çıkarımı yapılması uygun olabilecektir. Diğer taraftan, davranışsal reklamcılık amacıyla dijital parmak izi kullanımı söz konusu ise henüz dijital parmak izine katkı sağlayan erişim işlemleri gerçekleştirilmeden önce E-Gizlilik Direktifi kapsamında kullanıcının rızasının alınmasının gerekli olduğu değerlendirilmektedir.

Alınacak rızanın özgürce verilmesi, belirli bir konuda olması ve kullanıcının neye rıza gösterdiği hakkında bilgilendirilmiş olması gerekli olup verilen rızanın geri alınabilir olması da sağlanmalıdır. Bu anlamda tarayıcı ayarlarından verilen rıza ise geçerli bir rıza olarak değerlendirilmemektedir. En sık kullanılan tarayıcılarda dijital parmak izi kullanımı için bir önlem sayılabilecek "beni takip etme" seçeneği varsayılan olarak pasif gelmektedir. Tarayıcı ayarlarından ortalama bir kullanıcının bu seçeneği bulup işaretlemesi ve bunun farkında olmasını beklemek makul değildir (Madde 29 Veri Koruma Çalışma Grubu, 2010b). Ayrıca tarayıcılarda yer alan "beni takip etme" seçeneğinin seçilmesi halinde bile web sitesi operatörleri iş birliği içinde olmaksızın parmak izi çıkarmaya devam edebilecektir. Bununla birlikte, tarayıcı ayarlarıyla verilen rızanın toplu bir rıza olduğu dikkate alındığında, web sitesi bağlamında dijital parmak izi kullanımının amaçları hakkında bilgi verilmeksizin rıza alınması durumunun ortaya çıkmasına neden olacaktır (Madde 29 Veri Koruma Çalışma Grubu, 2010b).

Taslak durumda olan Elektronik Haberleşmede Özel Hayata Saygı ve Kişisel Verilerin Korunması ile İlgili ve 2002/58/AT Sayılı Direktifi Yürürlükten Kaldıran Taslak Tüzük'ün 8'inci maddesinin birinci fıkrası ile;

> *"Terminal cihazın işleme ve depolama yeteneklerinin kullanımı, yazılım ve donanım da dahil olmak üzere son kullanıcıların terminal cihazından ilgili son kullanıcı dışında bilgi toplanması, aşağıdaki durumlar hariç olmak üzere yasaklanmıştır:*
>
> *a. elektronik bir iletişimin bir elektronik iletişim ağı üzerinden iletiminin gerçekleştirilmesi amacıyla gerekli olması veya*
> *b. son kullanıcının rıza vermesi veya*
> *c. son kullanıcı tarafından talep edilen bir bilgi toplumu hizmetinin sağlanması için gerekli olması, veya*
> *d. Son kullanıcı tarafından talep edilen bilgi toplumu hizmetinin sağlayıcısı tarafından bu ölçümün yapılması şartıyla, web izleyici ölçümü için gerekli olması halinde."*

düzenlenmiştir. Taslak durumda bulunan Tüzük'te yer alan madde hükmünün yukarıda yer verildiği şekilde kabulü halinde, söz konusu hüküm dijital parmak izi çıkarma tekniğine uygun hale getirilmiş olacaktır.
E-Gizlilik Tüzüğü Taslağı'nın 20'nci gerekçe maddesinde ise;

> *"- Son kullanıcının cihazıyla ilgili bilgiler, genellikle son kullanıcının bilgisi olmadan, 'cihaz parmak izi çıkarma' gibi teknikler kullanılarak, tanımlama ve izleme amacıyla uzaktan da toplanabilir ve bu bilgiler, genellikle son kullanıcının bilgisi olmadan, kullanıcının mahremiyetine ciddi bir şekilde zarar verici nitelikte kullanılabilirliği, kullanıcıların hareketlerinin gözetimi gerçekleştirilebildiği,*
> *- Çevrim içi davranışlarının izlenmesi veya cihazın konumunun takibi veya terminal cihazın işleyişini bozması son kullanıcılarına mahremiyetini tehdit ettiği"*

ifade edilmiştir. "E-Gizlilik Tüzüğü Taslağı"nın 20'nci gerekçe maddesi ile doğrudan dijital parmak izine atıf yapılarak bu tekniğin tanımlama ve gözetim amacıyla kullanılmasının mahremiyet açısından risk oluşturduğu vurgulanmıştır.

E-Gizlilik Direktifi'nin AB'de özel hayata saygının ve haberleşme gizliliğinin korunmasının verimliliği etki analizi ile değerlendirilmiştir. Etkinlik ve verimlilik adına bu Direktif'in hedefleri tamamıyla karşılamadığı sonucuna varılmıştır. Direktif'te bazı hükümlerin net bir şekilde yazımı ve yasal kavramlardaki belirsizlik, uyumlaştırmayı tehlikeye atmış, bu yüzden şirketlerin sınır ötesi faaliyetinde güçlükler ortaya çıkmıştır. Direktif'teki rıza kuralı ile son kullanıcıların ne olduğu hakkında bir fikir sahibi olmaksızın izleme çerezlerini kabulünün talep edildiği, hatta bazı hallerde kullanıcı rızası olmaksızın çerezlerin terminal cihazda oluşturulması gibi nedenlerle Direktif'in amacına ulaşamadığı değerlendirilmiştir. Rıza alınmasının gerektiği durumlarda, mahremiyetle ilgisiz uygulamaların da kapsama dahil edilmesi nedeniyle rıza alma kapsamının geniş olduğu ve cihazda erişim veya depolamaya gerek duyulmayan takip tekniklerinin (örnek olarak; dijital parmak izi çıkarma) Direktif'te açıkça yer almaması bakımından eksik olduğu değerlendirilmiştir (Ayrıca bkz. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN).

Öte yandan, E-Gizlilik Direktifi'nden farklı olarak taslak durumda olan E-Gizlilik Tüzüğü'nün 8'inci maddesinin birinci fıkrası ile, son kullanıcı tarafından talep edilen bilgi toplumu hizmetinin sağlayıcısı tarafından bu ölçümün yapılması şartıyla, analitik ölçüm amaçlı olarak dijital parmak izi kullanımını da rıza gerektirmeyen istisna haller kapsamına alınması öngörülmektedir. E-Gizlilik Direktifi'nde ise böyle bir istisna duruma cevaz verilmemektedir. Taslak Tüzük'e ise web ölçümü ayrıca bir istisna hükmünün eklemesi öngörülmektedir. Taslak Tüzük çerçevesinde analitik amaçlı olarak bilgi toplumu hizmeti sağlayıcı tarafından dijital parmak izi kullanımı mevcut ise kullanıcı rızasına gerek olmadığı savunabilecektir. Halen uygulamada olan 2002/58/AT sayılı Direktif'in yerine geçmesi beklenen E-Gizlilik Tüzüğü hakkında ise henüz mutabık kalınamamıştır.

Dijital parmak izi kullanımında toplanan benzersiz dijital parmak izlerinin kişisel veri niteliği göz önünde bulundurulduğunda, GVKT de uygulama alanı bulacaktır. Bu çerçevede, konum takibi tabanlı reklamcılık veya davranışsal reklamcılık, profilleme faaliyetleri için dijital parmak izi kullanımı varsa hem 2002/58/AT sayılı Direktif hem de GVKT açısından rıza alınmasının gerekli olduğu anlaşılmaktadır.

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU

Kişisel Veri

6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre kişisel veri; *"kimliği belirli veya belirlenebilir gerçek kişilere ilişkin her türlü bilgi"*dir. Kanun büyük ölçüde

95/46/AT sayılı Direktif'e dayalı olarak hazırlanmış olup kişisel veri kapsamı oldukça geniş tutulmuştur. Kişisel veri kavramının yorumlanması açısından kanun koyucunun iradesini anlamak amacıyla incelenen Adalet Komisyonu Raporunda; kişisel veri kavramının kapsamı itibarıyla çok geniş bir alanda tezahür ettiği belirtilmektedir. Kanun'un ana unsuru olan kişisel verinin kapsamını yorumlarken teknolojinin değişen gerçeklerini göz önünde bulundurarak Kanun koyucunun iradesinin zamana göre yorumlanması doğru olacaktır. Bireyleri dijital ortamda takip etmek amacıyla kullanılan benzersiz bir tanımlayıcının eğer onlar üzerinde bir etkisi varsa kişiselleştirilmiş içerik sunuluyorsa, birey için ortaya çıkan herhangi bir etkisi varsa ya da muhtemelse ya da birey bakımından herhangi bir sonuca yol açıyorsa bu tanımlayıcının ve bu tanımlayıcı ile ilişkili toplanan bilgilerin kişisel veri olarak ele alınması gerektiği değerlendirilmektedir.

Davranışsal reklamcılık, satış veya pazarlama veya analitik amacıyla izleme, güvenlik, kimlik doğrulama vb. amaçlarıyla dijital parmak izi çıkarımında kullanıcının belirli bir kesinlik derecesiyle benzersiz olarak tanımlanması gereklidir. Kişinin dijital parmak izi aracılığıyla bir kitle içinde tekil hale getirilmesi ile kişi hakkında çıkarım yapılması ya da kişiye belirli bir şekilde davranılması kişisel veri işlenmesini de gerektirecektir. Dijital parmak izi aracılığıyla toplanan bilgiler, kişi bakımından sonuç doğurabilecek veya içerik bakımından bu kişi hakkında olabilecektir. Hatta dijital parmak izi aracılığıyla takip edilen kişi hakkında elde edilen bilgiler kişinin kimliğinin belirlenmesine yol açabilecektir. Benzersiz dijital parmak izleri ile kişinin tekilleştirilmesi, kişi hakkında bilgi toplanması ve hakkında çıkarım yapılmasının, Kanun kapsamında kişisel veri işlenmesini gerektireceği yönünde değerlendirilmesi yanlış olmayacaktır.

Veri Sorumlusu – Veri İşleyen

Web hizmetlerinin verilmesi esnasında üçüncü taraf içeriklerin bulunması nedeniyle kişinin profil bilgilerine göre reklamların gösterimi amacıyla çevrim içi takibe imkân veren web sitesi yayımcısı, web hizmetini kullanan ilgili kişinin kişisel verilerini üçüncü tarafa aktarmaktadır. Üçüncü taraf diğer sitelerde kullanıcıyı takip ederek elde ettiği verileri, çevrim dışı elde ettiği diğer veriler ile birleştirebilmektedir. Bu sayede kişiye profiline göre içerik gösterilebilmektedir. Bu türlü bir gözetimin farklı amaçları olabilecektir. Web hizmetlerinin sunumu esnasında tarafların birlikte yakınsak kararlar verdiği sürece ortak veri sorumluluğu meydana gelebilecektir.

*"Kurulun 23.12.2021 tarihli ve 2021/1304 sayılı Kararı"*nda (2021); yazılım olarak bulut servisi veren araç kiralama için yazılım sunan şirket ile araç kiralama hiz-

meti veren şirketlerin ortak veri sorumlusu olduğu değerlendirilmiştir. Karara konu olayda araç kiralama yazılımı hizmeti sunan firma teknik destek ve yazılımın bakımı konularında araç kiralama şirketlerine destek vermektedir. Araç kiralama şirketlerinin yalnızca içerik yani veri girişi yapma ve kaydetme bakımından denetim yetkisine sahip olduğu ve araç kiralama yazılımı sunan şirketin bu elde ettiği verileri işleyerek diğer araç kiralama firmalarına aktarabildiği ve "kara liste" mekanizması aracılığıyla verinin işleme amacında araç kiralama şirketlerinin ve yazılım firmasının sonucundan her iki tarafın da fayda gördüğü veri işleme süreciyle ilgili kararlar aldığı ve iş birliği içinde hareket ettiği göz önünde bulundurulduğunda taraflar ortak veri sorumlusu olarak yorumlanmıştır. Kararda, araç kiralama şirketlerince kullanılan söz konusu programa veri girişi yapıldığı ve yazılım şirketinin "kara liste" oluşturulmasında araç kiralama şirketlerinin girmiş olduğu bu verilerden faydalandığı, "kara liste" uygulamasından programı satın alan tüm şirketlerin faydalanabildiği hususu açıklanmıştır.

Davranışsal reklamcılıkta reklam gösterimi amacıyla dijital parmak izi kullanımı söz konusu olduğunda, web hizmetini sunan web sitesi yayımcısı tarafından ilgili kişi verileri üçüncü tarafa iletilecektir. Böyle bir durumda, web sitesi yayımcısının üçüncü tarafa aktarılan kişisel veriler bakımından üçüncü tarafla birlikte hareket etmesi söz konusu olacağı için üçüncü tarafla birlikte ortak veri sorumlusu olması gündeme gelebilecektir. Web sitesi yayımcısının bu sorumluluğunun, kişisel verilerin işlenme amacı ve yöntemini etkin bir şekilde birlikte karar verdiği faaliyetler için sınırlı olduğu değerlendirilmektedir.

Teknik destek amacıyla bir hizmet sağlayıcıdan dijital parmak izi çıkarımı yapan ürünler satın alınabilmektedir. Örneğin bankacılık hizmeti veren bir şirketin satın aldığı güvenlik çözümünde dijital parmak izi doğrulama mekanizması kullanılmaktadır. Bu güvenlik çözümünü sağlayan şirket, sadece teknik destek verdiği ve hizmet sağladığı işletmelerden aldığı verileri kendi amaçları doğrultusunda kullanmadığı ve üçüncü taraflarla paylaşmadığı sürece veri işleyen olması gündeme gelebilecektir.

İşleme Şartları

Dijital parmak izi kullanımıyla ilişkili olarak 5809 sayılı Elektronik Haberleşme Kanunu (EHK) yer almakta olup 2002/58/AT sayılı Direktif'in 5'inci maddesinin üçüncü fikrası ile EHK'nin 5'inci maddesinin üçüncü fikrası arasında kısmi bir uyum gözetildiği değerlendirilmektedir. Çerezde olduğu gibi dijital parmak izi kullanımında da EHK kapsamında bazı yükümlülükler doğabilecektir. Bu yüzden Kanun ile EHK arasındaki ilişkinin ortaya konulması, kişisel veri işleme şartı ve

genel ilkelere ilişkin olarak doğru tespit yapma imkânı sağlayacaktır. Bu konudaki görüşlerden birisi EHK'nin öncelikli olarak ele alınması gerektiği, ancak Kanun'un getirdiği yükümlülüklerin de uygulanmaya devam edilmesi gerektiğidir (Çekin, 2019).

EHK'nin 51'inci maddesine baktığımızda; *"(3) Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir. (...)"* şeklinde düzenlendiği görülmektedir. Söz konusu madde E-Gizlilik Direktifi'nin 5'inci maddesinin üçüncü fikrası ile kısmen uyumlu olsa da maddenin uygulama alanının işletmecilerle sınırlandığı ve web sitesi yayımcılarının kapsam dışında bırakıldığı anlaşılmaktadır.

Bununla birlikte, EHK'nin işletmeciler için özel kanun niteliğinde olması nedeniyle işletmeciler tarafından dijital parmak izi kullanımı söz konusu olduğunda, öncellikli olarak EHK'nin uygulanabileceği düşünülmekle beraber, kişisel veri işlenmesi noktasında ise Kanun'un uygulanarak kişisel veri işleme şartları bakımından,

- Açık rıza veya
- Veri sorumlusunun dijital parmak izi aracılığıyla kişisel veri işleme faaliyeti için Kanun'un 5'inci ve 6'ncı maddelerinde sayılan diğer veri işleme şartlarının

göz önünde bulundurulmasının uygun olacağı değerlendirilmektedir. Haberleşmenin sağlanması noktasında işletmeci tarafından dijital parmak izi aracılığıyla kişisel veri işlendiği durumda, Kanun'un 5'inci maddesinin ikinci fikrasında yer alan "Kanunlarda açıkça öngörülmesi" işleme şartı dahilinde kişisel verilerin işlenmesi gündeme gelebilecektir. Ancak, Kanun'un 4'üncü maddesi dahilinde "amaçla bağlantılı, sınırlı ve ölçülü" ve "hukuka ve dürüstlük kuralına uygun" ve "ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkelerine uygunluk gözetilmelidir. Örneğin; dijital parmak izi aracılığıyla konum verilerinin toplanması gibi bir durumda elektronik haberleşme mevzuatındaki saklama sürelerine uygunluk gözetilmelidir.

Web hizmetleri söz konusu olduğunda hizmet sağlayıcı tarafından bir web sitesinde/uygulamasında birçok hizmetin bir arada verilmesi sık rastlanan bir durumdur. Kişi tarafından açıkça talep edilen bir çevrim içi hizmetin sunulması için

kesinlikle gerekli olarak dijital parmak izi çıkarımı söz konusu olduğunda, kişisel verilerin sözleşmenin (örneğin üyelik sözleşmesi veya satış sözleşmesi) kurulması veya ifası için taraflara ait kişisel verilerin işlenmesinin zorunlu olması işleme şartı dahilinde işlenmesi gündeme gelebilecektir.

KİŞİSEL VERİLERİN KORUNMASI AÇISINDAN RİSKLER VE ÖNLEMLER

Web'in kuruluş fikirlerinden birisi de herhangi birinin, cihazdan bağımsız olarak büyük çaptaki makineler ağına erişebilmesiydi. Makinelerin birbirileri arasında iletişim kurmasının evrensel bir yoluna ihtiyaç duyulmasından kaynaklı olarak 1990'ların başında HTTP ve HTML standartları ortaya çıkmış, bunun akabinde bu standartları destekleyen tarayıcılar geliştirilmiştir. Bu süreçte platformlar ve tarayıcılar, yeni eklenen özelliklerin tümünü desteklemediler. Ortaya çıkan uyumluluk sorunlarını önlemek amacıyla ise HTTP protokolüne kullanıcı-aracısı-başlığı *(user-agent-header)* eklenmiştir. Kullanıcı aracısı başlığı, geliştiricilerin tarayıcı sınırlamalarını dikkate almasını sağlayan cihazlar arasındaki farklılıkları belirten ilk bilgi parçası olarak kabul edilebilir. 90'lı yılların ortalarında web sayfalarını daha dinamik yapmak amacıyla *JavaScript* olarak adlandırılan *script* programlama dili kullanılmaya başlandı. Böylelikle örneğin tarayıcı, doğrudan kullanıcı cihazının işletim sisteminin zaman dilimi bilgisine ulaşabildi. Tarayıcılar birçok modern *API*'nin kullanılmasıyla beraber, multimedya içerikleri de uyumlu bir şekilde görüntülemeye başlamışlardır (Laperdrix ve diğerleri, 2020).

Tarayıcıların cihaz bağımsız olarak çalışabilmesi, kullanıcı deneyiminin iyileştirilmesi, zengin içerik görüntüleme firsatlarını sunabilmesi kullanım açısından olumlu olsa da eklenen özelliklerin kullanıcı mahremiyetini etkilediği ve kullanıcının Web'te anonim kalabilmesini zor bir hale getirdiği söylenebilecektir. İşlevsellik ve mahremiyet arasındaki dengenin kurulabilmesi kullanıcının mahremiyetinin korunması açısından önemlidir. Dijital parmak izi çıkarımının, kişi için görünmez ve anlaşılması zor bir teknik olduğu açıktır. Bu yüzden, dijital parmak izi aracılığıyla kişisel verilerin işlenmesi hususunda farkındalığın oluşturulması ve kişisel veri güvenliğinin sağlanması açısından önlemler konusunda kişilerin bilgilendirilmesi gerekmektedir. Bu konudaki mevcut risklerin somut bir şekilde ortaya koyularak bu risklere karşı alınabilecek önlemlerin tartışılmasının veri sorumluları, ilgili kişiler, teknoloji geliştiriciler ve üreticileri, politika yapıcılar adına faydalı olacağı değerlendirilmektedir.

Dijital Parmak İzi Teknolojisi Bakımından Kişisel Veri Koruma Riskleri

Aktif veya pasif dijital parmak izi aracılığıyla kullanıcının tekil hale getirilerek

internet tarama alışkanlarının izlenmesi yoluyla elde edilen bilgiler, çevrim içi veya çevrim dışı olarak başka verilerle birleştirilebilmektedir. Veri komisyoncuları, kişisel verileri toplayarak ve verilerin ticaretini yaparak veri setlerinin birleştirilmesinde rol oynamaktadır.

Tomasz Bujlow ve ark. tarafından kişinin çevrim içi olarak takibinin değerli olduğu, bu oluşturulan dijital kimliğin kişinin adı soy adı, sosyal güvenlik numarası gibi bilgilerle eşleştirilmesi sonucunda takip edilen bir kişinin kimliğinin belirlenmesinin ise daha kârlı olduğu belirtilmiştir (Bujlow, Carela-Español, Solé-Pareta, ve Barlet-Ro, 2017). Toplanan veriler birçok yolla başka verilerle birleştirilerek satış ve pazarlama dahil olmak üzere çeşitli amaçlarla kullanılabilmektedir. Bunlar arasında üçüncü taraf servisler, üçüncü taraf sitelere bilgi sızıntısı, veri ihlalleri, şirket birleşmeleri olarak sıralanabilmektedir.

Google, Facebook, Youtube gibi dijital platformlara üyelik bulunması halinde, dijital platformun tutmuş olduğu veriler ile çevrim içi diğer tanımlayıcı ile toplanan bilgiler birleştirilebilmektedir. Dijital platforma henüz hesabına girişi olmayan bir kullanıcı için dijital platform tanımlayıcısı dışında herhangi bir tanımlayıcı ile kullanıcıyı takip ettiğini ve onun hakkında bilgi topladığını düşünelim, kullanıcı daha sonrasında dijital platformdaki hesabına giriş yaptığında ise bu tanımlayıcı aralığıyla halihazırda toplanan bilgiler ile dijital platform nezdinde var olan bilgiler birleştirilebilecektir.

Öte yandan, bir internet sitesinde bulunan üçüncü taraf reklamlar, analitik servisler gibi gömülü içerikler aracılığıyla HTTP başlıkta *(HTTP header)* yer alan referans alanı (referrer field) (Mevcut istek yapılan siteye hangi siteden yönlendirildiği bilgisini içerir.) için tanımlanan politika sebebiyle üçüncü taraflara kişisel veri sızıntısı olabilmektedir. Bir kişi A internet sitesinde bulunan bir bağlantı aracılığıyla B internet sitesine ulaştığında, B internet sitesinde bulunan analitik servis, referans alanı için tanımlanan politika sebebiyle referans alanı bilgisine sahip olabilmektedir. İnternet sayfasında gömülü olan üçüncü taraftan alınan resim, iframe (Bir internet sayfasına doküman, video ve interaktif medya yerleştirmenizi sağlar. Örneğin Youtube'da bir videoyu internet sitesine yerleştirmeniz halinde, Youtube bu videoyu size iframe öğesi içinde sağlar ve bu öğeyi sitenizin uygun bölümüne gömebilirsiniz.) veya *javascriptler* nedeniyle ve referans politikasına bağlı olarak web talepleri ile beraber referans alanı bilgisi üçüncü taraf sunucuya iletilebilmektedir. A sitesine bulunan kişiye özel hedefli bir reklam nedeniyle ilgili reklam sunucusundan reklam alanında yer alan nesnenin getirilmesi için talep oluşturulduğunda, Şekil 3'te görüldüğü gibi kullanıcı e-postası da referans alanıyla beraber üçüncü taraf olan reklam sunucusuna iletilebilecektir.

Şekil 3. Bir internet sitesinde bulunan hedefli reklam için reklam sunucuna yapılan web talebinin başlığı ("HTTP referer explanation", t.y.)

Şekil 4 ile referans alanında yer alan URL ile ne tür bilgi sızıntıları olabileceğine örnekler verilmiş olup bunlar; ne tür müzik dinlendiğin, ilgi alanların, hastalıkların, kullanıcı adın, e-posta adresin veya parola sıfırlama bağlantın olabilecektir.

Şekil 4. Referans alanında bilgi sızıntılarına örnekler ("Referer and Referrer-Policy best practices", 2021.)

Referans alanı politikaları arasında "referans bilgisi yok *(no-referrer)*", "düşük gizlilikte referans bilgisi yok *(no-referrer-when-downgrade)*", "aynı kaynak *(same-origin)*", "origin (kök)", "sıkı kök *(strict-origin)*", "çapraz kök olduğunda kök *(origin when cross origin)*", "çapraz kök olduğunda sıkı kök *(strict origin when cross origin)*", "güvensiz adres *(unsafe url)*" bulunmaktadır ("Mitigating Browser Fingerprinting in Web Specifications", 2019). Politika "referans bilgisi yok" olarak tanımlanırsa referans alanında bilgi gönderilmez, "same-origin" olarak tanımlanırsa, yalnızca kaynağı aynı taleplerde (kaynağın bağlantı tipi ile aynı olması lazım) URL bilgisinin tamamı gönderilir.

Diğer bir risk ise birinci tarafların, üçüncü taraflara bilgi satması olacaktır. Örneğin bir reklam verisi sağlayıcısı olan *Datalogix* isimli şirket, pazarlama kuruluşlarından tüketicilerin isimleri, posta kodları, e-postaları ve demografik ve davranışsal bilgilerini içeren bilgilerini satın alarak profil çıkarma amacıyla kullanmıştır (Bujlow ve diğerleri, 2017). Datalogix'in topladığı bilgiler arasında IP adresi, tarayıcı çeşidi, servis edilen reklamlar ve bunların tarihlerinin de bulunduğu açıklanmıştır (Bujlow ve diğerleri, 2017), (Torres, Jonker ve Mauw, t.y.).

Bir diğer davada ise FTC tarafından, "LeapLab" isimli veri simsarının mali açıdan sıkıntılı tüketicilerin adları, adresleri, telefon numarası, işverenin yanı sıra sosyal güvenlik ve banka hesap numaraları dahil olmak üzere yüzbinlerce tüketicinin hassas bilgisini satın aldığı, daha sonra bu hassas bilgileri meşru bir amacını olmadığı bildiği pazarlamacılara sattığı iddia edilmiştir. Davaya konu alıcılar arasında tüketicilere e-posta, kısa mesaj veya telefon görüşmesi yoluyla istenmeyen satış teklifleri yapan pazarlamacılar ve tüketicilerin hesaplarından izinsiz olarak milyonlarca dolar çekmek için kullanan internet tüccarları olduğu ifade edilmektedir (Fedaral Trade Commission, 2016).

Cihaza dayalı özellikler sayesinde dijital parmak izi aracılığıyla kişinin farklı siteler arası takibi söz konusu olabilecektir. Dijital parmak izi, kişinin cihazının herhangi bir veya birden fazla depolama alanındaki tanımlayıcıyı silmesi sonucunda kurtulabileceği bir tanımlayıcı özelliği göstermemektedir. Dijital parmak izi ile takip yapan tarafların engellenebilmesi için daha fazla çaba gerekmektedir. Kişinin dijital parmak izi aracılığıyla stabil şekilde benzersiz olarak tanımlanmasının sağlanması halinde, farklı tarayıcılar kullanılsa bile takibin engellenememesi ve kişinin farklı tarayıcılar arası internet tarama kullanım bilgilerini ilişkilendirilebilmesi söz konusudur.

Hem araştırmacılar hem de kullanıcılar, dijital parmak izi çıkarımının şeffaf olmayan bir şekilde yapılması sebebiyle kullanımını tespit etmekte güçlük çekmektedir. Araştırmacılar aktif olarak dijital parmak izi çıkarılıp çıkarılmadığının tespiti için bir web sayfasının kaynak kodunda yer alan scriptleri sınıflandırma yoluna gitmişlerdir. Scriptler benzer içerikte olsa dahi iki scriptin kullanım amacı değişebilmektedir. Bu yüzden, bir scriptin, dijital parmak izi çıkarma amacıyla mı, yoksa başka bir amaç için mi kullanıldığının ayrımının yapılmasında güçlük çekilmektedir. Yapılan bir araştırmada bir scriptin dijital parmak izi çıkarımında kullanıldığının göstergeleri arasında; belirli fonksiyonlara erişim durumu, erişilen bilgi miktarının fazla olması, belirli API'lerin kullanımı ve belirli API fonksiyonlarına erişim ve erişim sırası, farklı parametreler ile değer döndürme, bir scriptin döndürdüğü değerlerin tek bir nesnede saklanması, özet fonksiyonları aracılığıyla değer üretimi, scriptin cihazdaki herhangi bir depolama alanında tanımlayıcı değerleri oluşturması, kod gizleme ve minimizasyonu yapılması sayılmaktadır (Laaperdrix ve diğerleri, 2019).

Mevcut Risklere Karşı Alınabilecek Önlem Önerileri

Üreticiler ve geliştiriciler, ilgili kişiler, veri sorumluları ve düzenleyici kurumlar tarafından mevcut risklere karşı çeşitli teknik önlemler ve politika önlemleri alınabilecektir. Mevcut riskler karşısında dijital parmak izinin mahremiyet odaklı ve meşru kullanılabilmesi için teknoloji üreticileri ve geliştiricilerine de bazı sorumluluklar düşmektedir. Teknoloji üreticileri tarafından dijital parmak izi çıkarılan yüzeyin dengelenmesi, tespit edilebilirliğin sağlanması, standardizasyon sağlanarak homojen parmak izlerinin oluşturulması, bütüncül silme imkânının sağlanması gibi önlemler çerçevesinde web teknolojilerinin mahremiyet odaklı şekilde tasarlanması ve üretilmesi gereklidir. Web spesifikasyonu yazarları, düzenli olarak yeni işlevsellik ve dijital parmak izi yüzeyi arasında bir denge kurmaya çalışır. Örneğin sürüm veya versiyon numaralandırması hata ayıklama açısından her ne kadar katkı sağlasa da ayrıntılı numaralandırmalar

dijital parmak izi yüzeyinin artmasına neden olacağından takip amaçlı olarak kullanılmasına olanak sağlayabilmektedir ("Mitigating Browser Fingerprinting in Web Specifications", 2019). Herhangi bir fonksiyonellik devreye alınırken dijital parmak izi yüzeyine katkı sağlayıp sağlamadığı ile işlevsellik yönünden ne kadar önemli olduğu hususunun değerlendirilerek tasarımdan itibaren mahremiyetin korunması önemlidir. Özellikle, pasif cihaz parmak izi çıkarılmasına katkı sağlayan özelliklerden kaçınılması mahremiyetin korunması açısından önemlidir. Daha önce de bahsedildiği üzere, pasif olarak dijital parmak izinin çıkarımının tespit ve kontrol firsatı yoktur diyebiliriz. Pasif olarak dijital parmak izi çıkarımına katkı sağlayan bir özellik başka bir şekilde tasarlanamayacaksa eğer, bunun devreye alınması yani son yöntem olarak ele alınması tavsiye edilmektedir. Dijital parmak izi çıkarımına katkı sağlayan özelliklerin kod tarafında işaretlenmesi ve alınabilecek önlemlerin belirtilmesi iyi bir uygulama örneği olabilecektir.

Veri minimizasyonu ilkesiyle API tasarlanması belirli bir işlevsellik için gerekli entropi miktarına erişim sağlayabilecektir. Örneğin, Tor Browser, bir *"browser.display.max_font_attempts"* tercihiyle sorgulanabilecek yazı tipi sayısını sınırlamaktadır. Entropiyi azaltmak amacıyla talep sonucu döndürülen bilginin ayrıntı düzeyi veya kesinliği en aza indirilebilecektir. Örneğin, Pil Durumu API'sinin kullanılmasında, mevcut pil seviyesinin yüksek hassasiyetli (çift hassasiyetli veya 15-17 anlamlı basamak) okumalarına izin verilmesi farklı web siteleri arasında (kökenler arasında) ilişkilendirilen kısa dönemli bir tanımlayıcı sağlayacaktır. Bu değerin yuvarlanması ise işlevsellik üzerinde olumsuz etki oluşturmazken entropi miktarını azaltarak parmak izi çıkarılmasında önleyici bir tedbir olarak yer alacaktır.

Pasif olarak dijital parmak izi çıkarımı için kullanılan kullanıcı aracısı dizesi başlığını tamamen kaldırmak yakın vadede pek mümkün görünmese de işlenen bilginin amacının tespitine yarayan yöntemler benimsenebilmektedir. Eğer web siteleri, HTTP başlıklarında bilgi göndermeden önce bilgiye erişim için bir istekte bulunursa, pasif parmak izi çıkarmada kullanılan HTTP başlıkları ile gönderilen bilginin kapsamının ne olduğu anlaşılabileceğinden, pasif dijital parmak izi çıkarımının tespiti de kolaylaşacaktır. Kullanıcı aracı dizesinde tüm bilgilerin toplu bir şekilde gönderilmesi yerine proaktif talep ile aşamalı bilgi gönderimi pasif olarak dijital parmak izi çıkarmada işlenen veri noktalarının ne olduğu hususunda bir şeffaflık oluşturacaktır.

Tarayıcıların, dijital parmak izine katkı sağlayan nitelikleri standart bir değer oluşturarak sunuculara göndermesi dijital parmak izi çıkarımına katkı sağlayan ayırt edici niteliklerin ortadan kaldırılmasına yardımcı olabilecektir ("Mitiga-

ting Browser Fingerprinting in Web Specifications", 2019). TOR tarayıcısı, dijital parmak izine yüksek katkı sağlayan API'lerden olan WebGL API ve Canvas API kullanımını tamamen ortadan kaldırıp yazı tipi listesini standartlaştırmaktadır. Bunun yanı sıra HTTP başlık bilgisini değiştirerek kullanılan işletim sistemini standart Windows olarak ayarlamaktadır. Ancak hala TOR kullanıcılarını ayırt edebilecek nitelikler mevcuttur. Kullanıcı, ekran boyutunu TOR'un varsayılan olarak ayarladığı boyuttan farklı bir boyutta kullandığında, bu tanımlamaya katkı sağlayan bir nitelik olarak karşımıza çıkacaktır. Eğer TOR'un varsayılan ayarlarına bağlı kalınırsa, söz konusu tarayıcı dijital parmak izi çıkarımına güçlü bir koruma sağlarken bu özelliklerden ayrılan kullanıcılar diğer tarayıcıları kullananlardan daha fazla takip edilebilir hale gelebilmektedir (Laperdrix ve diğerleri, 2020).

Dijital parmak izi çıkarma yöntemlerinde bahsettiğimiz çerez benzeri dijital parmak izi çıkarımında, çerez ve dijital parmak izinin farklı avantajlarından yararlanılarak iki teknik birleştirilmektedir. Bu tarz bir parmak izi çıkarmaya yönelik olarak kullanıcının terminal cihazında kalıcı olarak tanımlayıcı depolayan dizayn şeklinden kaçınılması önerilmektedir ("Mitigating Browser Fingerprinting in Web Specifications", 2019). Ayrıca kullanıcıya terminal cihazında depolama alanı olarak kullanılabilecek tüm alanları çok fazla uğraş gerektirmeden silebilme imkânı sağlanmalıdır. Kendini yenileyen çerez uygulamasının kullanıcıyı yanıltan ve şeffaf bir uygulama örneği olmaması nedeniyle kullanılmaması gerektiği değerlendirilmektedir.

Do Not Track (DNT), kullanıcıların opt out olarak ziyaret etmediğiniz tüm internet siteleri (analitik hizmetler, reklam ağları, sosyal platformlar dahil) tarafından takipten çıkılmasına imkân veren W3C tarafından önerilen bir mekanizmadır. Bu seçenek varsayılan olarak seçili gelmediği için kullanıcının bunu aktif bir şekilde tarayıcıdan etkinleştirmesi gerekmektedir. DNT başlığın uygun bir şekilde takip konusunda iş birliği yapan web siteleri olabilecektir. Ancak bazı web siteleri kullanıcının bu talebine uygun davranmayabilir. Hatta kullanıcının DNT talebini benzersiz tanımlama amacıyla kullanılabilecektir. İspanyol Veri Koruma Otoritesi (AEPD) web sitelerinin kullanıcıların DNT talebine uygun davranıp davranmadığına ilişkin yaptığı araştırmada; DNT seçeneği etkin olmasına rağmen araştırma grubunda yer alan üçüncü taraf web sitelerinin %96,12'sinin *Canvas API* aracılığıyla, %72,18'sının *WebRTC API*, %64,29'u ise *AudioContext API* aracılığıyla fonksiyon çağrısı yaparak dijital parmak izi çıkarma işlemine devam ettiği tespit edilmiştir (AEPD, 2019).

Tarayıcı ayarlarından *JavaScript* kullanımı kısıtlanabilmekte, böylelikle dijital parmak izi çıkarımına katkı sağlayan bilgi miktarı azaltılmaktadır. Sık kullanılan tarayıcılarda sitelere göre *JavaScript* kullanımı için seçim yapabilme imkânı tanınmaktadır. *Javascript* işlevsellik için hemen her sitede kullanılmaktadır. Javascript kullanımının bir web sitesi için tamamen engellenmesi işlevsellikte bozulmalara neden olabilecekken dijital parmak izi çıkarımında kullanıcı için önleyici bir tedbir olarak yer almaktadır.

Dijital parmak izi durumsuz bir takip teknolojisi olarak karşımıza çıkmaktadır. Yani, kullanıcının terminal cihazında bir tanımlayıcı depolayan durum denetlemeli takip teknolojilerine göre kullanıcı için daha görünmez olması nedeniyle çevrim içi mahremiyete zarar verici nitelikte kullanabilmektedir. Herhangi bir kullanıcının herhangi bir aydınlatma metninde bu konuda bilgi verilmeksizin dijital parmak izi kullanımını tespit etmesi için kod analizi yapması gerekecektir. Sıradan bir kullanıcının kod analizi yapamayacağı hususu açıktır. Kod analizi yaparak dijital parmak izi kullanımını tespit etmek özel bir uzmanlık gerektirmektedir. Kod geliştiricileri için manuel olarak tespit yapmak, kullanılan kodlarda gizleme ve minimizasyon yapılmasının vermiş olduğu karmaşıklığı da göz önünde bulundurduğumuzda zaman bakımından oldukça maliyetli olacaktır. Bu yüzden dijital parmak izi kullanımının tespiti için makine öğrenmesi yöntemleri kullanan çözümler geliştirilmiştir.

Fp-Block, her yeni etki alanı için yeni bir dijital parmak izi oluşturmaktadır (Torres ve diğerleri, t.y.). Farklı etki alanları için farklı parmak izlerinin sağlanması ile çapraz izlemenin önüne geçilmesi amaçlanmaktadır. FP-Block'un yaklaşımı, üçüncü tarafların gömülü oldukları her sitede farklı parmak izleri görmesi ve böylece izlemenin engellenmesidir.

Pouneh Nikkhah Bahrami, Umar Iqbal ve Zubair Shafiq'in bir çalışmasında FP-Radar çözümü ile son 10 yıldaki en sık kullanılan 100 bin web sitesinde üzerinden bir ölçüm gerçekleştirilmiştir. FP-Radar ile API kullanım desenlerine göre dijital parmak izi kullanımının tespiti yapılmıştır (Bahrami, Iqbal ve Shafiq, 2021).

Umar Iqbal, Steven Englehardt ve Zubair Shafig tarafından dijital parmak izi kullanımının tespiti üzerine yapılan çalışmada; kullanılan API, erişilen özellik ad ve erişilen yöntem adı, parametreler, bir özelliğin değeri veya döndürülen değeri, API çağırma zamanı *OpenWPM* adı verilen bir araç ile kayıt altına alınmıştır. (Iqbal, Englehardt ve Shafiq, 2021). *FP-Inspector* olarak adlandırılan çözüm ile makine öğrenmesine dayalı olarak dijital parmak izi kullanan scriptleri tespit etmişlerdir. Bu çözüm ile dijital parmak izi kullanımını engelleme seçeneği de sunulmaktadır.

İspanya Veri Koruma Otoritesinin yapmış olduğu araştırma raporunda; açık kaynak kodlu uBlock Origin ve Ghostery eklentilerinin, belirli şartlar altında (üçüncü taraf çerezlerin kabul edilmediği, Flash eklentisinin aktif olmadığı ve DNT başlığının gönderildiği durumda) dijital parmak izi çıkarımının önemli ölçüde azalttığı tespit edilmiştir (AEPD, 2019.). Kullanıcıları şu iki konuda uyarmak gereklidir: (i) Tarayıcıların özel mod ile kullanılması veya (ii) VPN kullanılması dijital parmak izi çıkarımını engellememektedir.

Her ne kadar cihaz parmak izi gözlenmesi zor olsa da çeşitli analiz araçları sayesinde günümüzde tespiti yapılabilmektedir. Örneğin, web sitesi yayımcıları tarafından reklamcılık amacıyla web sitesine konulan gömülü içerik nedeniyle dijital parmak izinin çıkarımı yapılıp yapılmadığının teyit edilmesi gerektiği değerlendirilmektir. Web sitesi yayımcılarının reklam dağıtım yolları hakkında bilgi sahibi olması ve mahremiyet odaklı kuruluşlarla iş birliği yapması önerilmektedir. Özellikle küçük işletmeler hem web sitesi yayımcısı olarak hem de reklam verenler olarak reklamcılık ekosisteminden ekonomik olarak fayda görmektedirler. Bu işletmeler için reklam ekosisteminde yer alan aracı kurumlarla müzakere etmesi kimi zaman zor olabilse de dijital ekonomide güvenin oluşturulmasının işletmeye olumlu etkisi olacağından, mahremiyet odaklı kuruluşlar ile iş birliği yapılması tavsiye edilmektedir.

Reklam ağlarının veya web sitesi yayımcılarının dijital parmak izi kullanması halinde, açık rızanın unsurlarını karşılamasa da bir önlem olarak tarayıcılarda veya işletim sistemlerinde yer alan “beni takip etme” seçeneğine uygun olarak hareket etmesi gerektiği değerlendirilmektedir. Diğer işleme şartlarına gidilemediği durumlarda uygun açık rıza alınması ve Kanun’un 10’uncu maddesi uyarınca aydınlatma yükümlülüğünü yerine getirmesi gerekmektedir. Ortak veri sorumluluğu gündeme geldiğinde, dijital parmak izi kullanımına katkı sağlayan taraflar aydınlatma ve açık rıza alınması bakımından sorumluluk sınırlarını belirleyebilecektir.

Genel ilkelerin gözetilerek amaçla bağlantılı, sınırlı ve ölçülü olarak kişisel veri işlenmesi, açık rıza alınan amaçtan farklı olarak amaç değiştiğinde tekrar açık rıza alınması gereklidir. Mevzuatta öngörülen veya işlendikleri amaç için gerekli süre bakımından değerlendirildiğinde özellikle işlendiği amaç için gerekli süre kadar benzersiz dijital parmak izi ve bununla bağlantılı kişisel veriler muhafaza edilmelidir. İşlenmesini gerektiren sebeplerin ortadan kalkması durumunda Kanun 7’inci maddesi ve ilgili yönetmeliğe uygun olarak silinmeli, yok edilmeli veya anonim hale getirilmelidir. Kanun’un 11’nci maddesinden sayılan hakların kullanılabilmesinin sağlanması gereklidir. Envanter ve Sicile kayıt ve bildirim yükümlülüğü olması halinde dijital parmak izi kullanımına dayalı kişisel veri

işlenen süreçlerin de göz önünde bulundurulması gereklidir. Dijital parmak izi çıkarılması amacıyla yurt dışına veri aktarılması gerekebilir, genellikle toplanan verilerden sunucu tarafında benzersiz dijital parmak izleri oluşturulsa da kullanıcıdan toplanan verilerin de kişisel veri olarak ele alınması ve yurt dışına aktarım hükümlerinin göz önünde bulundurulması gerektiği değerlendirilmektedir.

Öte yandan, sahte reklam verenler tarafından kötücül reklamcılık için dijital parmak izi çıkarımına katkı sağlayan niteliklerin sorgulanmasının meşru bir zemini bulunmamaktadır. Bu tür kötücül kullanımlar için yayımcıların reklam ağları hakkında bilgi edinerek reklam dağıtımı yolları ve güvenlik önlemleri hakkında bilgi sahibi olması gerekmektedir. Reklam öğeleri davranışlarını keşfetmek kötücül kullanımları engellemek için Web Application Firewall kullanımı ve mümkünse reklam gösterimi için reklam alanı içinde herhangi bir JavaScript veya benzeri kodun çalıştırılmasına izin verilmemesi tercih edilebilecektir (Malvertising, t.y.).

SONUÇ

Kullanıcının çevrim içi takibini kılan birçok takip teknolojisi bulunmakta olup bu teknolojiler kullanıcılar açısından her zaman aynı veri koruma risklerine neden olmamaktadır. Bazı teknolojiler yalnızca oturum boyunca kullanılabilmekteyken diğerleri daha uzun süreler için kullanıcının çevrim içi takibini mümkün kılmaktadır. Dijital parmak izi çıkarımı mahremiyet açısından yüksek riskli bir takip teknolojisidir. Özellikle pasif yöntemle dijital parmak izi çıkarımında şeffaflık eksikliği, kontrolünün ve tespit edilebilirliğin zor olması, farklı tarayıcılar arası izlemenin mümkün olması bireyler açısından mahremiyet riski oluşturmaktadır.

Davranışsal reklamcılık, satış veya pazarlama veya analitik amacıyla izleme, güvenlik, kimlik doğrulama vb. amaçlarıyla dijital parmak izi çıkarımında kullanıcının belirli bir kesinlik derecesiyle benzersiz olarak tanımlanması gereklidir. Kişinin dijital parmak izi aracılığıyla tekilleştirilerek kişi hakkında çıkarım yapılmasına ya da kişiye belirli bir şekilde davranılmasına neden olacaktır. Dijital parmak izi aracılığıyla toplanan bilgiler, kişi bakımından sonuç doğurabilecek veya içerik bakımından bu kişi hakkında olabilecektir. Hatta dijital parmak izi aracılığıyla takip edilen kişi hakkında elde edilen bilgiler kişinin kimliğini belirlenmesine yol açabilecektir. Benzersiz dijital parmak izleri ile kişinin tekilleştirilmesi, kişi hakkında bilgi toplanması ve hakkında çıkarım yapılmasının, kişisel veri işlenmesini de gerektireceği değerlendirilmektedir.

Tarayıcıların cihaz bağımsız olarak çalışabilmesi, kullanıcı deneyiminin iyileştirilmesi, zengin içerik görüntüleme fırsatlarını sunabilmesi kullanım açısından olumlu olsa da eklenen özellikler kullanıcı mahremiyetini olumsuz etkilemiş ve kullanıcının web üzerinde anonim kalabilmesini zor bir hale getirmiştir. İşlevsellik ve mahremiyet arasındaki dengenin kurulabilmesi kullanıcının mahremiyetinin korunması açısından önem arz etmektedir. Dijital parmak izi kullanımının ilgili kişi için görünmez ve anlaşılması zor bir teknik olduğu açıktır. Bu yüzden dijital parmak izi kullanımdan etkilenen kişiler açısından farkındalığın oluşturulması ve alabileceği önlemler konusunda kişilerin bilgilendirilmesi gereklidir.

Mahremiyet riskleri arasında dijital parmak izi aracılığıyla takip edilen bireyin zaman içinde kimliğinin belirlenmesi riski bulunmakta olup dijital parmak izi aracılığıyla toplanan verilerin başka verilerle birleştirilmesinin birçok yolu bulunmaktadır. Çevrim içi dünyada bireyin dijital parmak izi aracılığıyla izlenmesi yoluyla elde edilen bilgiler, çevrim içi veya çevrim dışı olarak başka verilerle birleştirilebilmektedir. Veri komisyoncuları kişisel verileri toplayarak verilerin ticaretini yaparak veri setlerinin birleştirilmesinde rol oynamaktadır. Takip edilen kişinin çevrim içi oluşturulan dijital kimliğinin; adı soy adı, sosyal güvenlik numarası gibi bilgilerle eşleştirilerek kimliğinin belirlenmesinin ise daha riskli bir durumdur. Toplanan veriler birçok yolla başka verilerle birleştirilerek satış ve pazarlama dahil olmak üzere çeşitli amaçlarla kullanılabilmektedir. Kişiye ilişkin toplanan bilgilerin birleştirilmesi üçüncü taraf servisler, üçüncü taraf sitelere bilgi sızıntısı, veri ihlalleri, şirket birleşmeleri nedeniyle kişinin kimliğinin belirlenmesinin nedenleri arasında sayılabilir.

Dijital parmak izinin ortaya çıkardığı diğer bir risk ise kişinin dijital parmak izi aracılığıyla stabil şekilde benzersiz olarak tanımlanmasının sağlanması halinde, farklı tarayıcılar kullanılsa bile takibin engellenememesi ve farklı tarayıcılar arası internet tarama kullanım bilgilerini ilişkilendirilebilmesidir. Bununla birlikte hem araştırmacılar hem de kullanıcılar dijital parmak izi çıkarımının şeffaf olmayan bir şekilde yapılması sebebiyle kullanımını tespit etmekte güçlük çekmektedir. Araştırmacılar aktif olarak dijital parmak izi çıkarılıp çıkarılmadığının tespiti için bir web sayfasının kaynak kodunda yer alan *"script"*leri (kod parçacıkları) sınıflandırma yoluna gitmişlerdir. Kod parçacıkları benzer içerikte olsa dahi iki kod parçacığının kullanım amacı değişebildiğinden bir kod parçacığının dijital parmak izi çıkarma amacıyla mı yoksa başka bir amaç için mi kullanıldığının ayrımının yapılmasında güçlük çekilmektedir.

Dijital parmak izinin mahremiyet odaklı olarak meşru kullanılabilmesi için teknoloji üreticileri ve geliştiricilerine de bazı sorumluluklar düşmektedir. Teknoloji üreticileri tarafından dijital parmak izi çıkarılan yüzeyin dengelenmesi, tespit edilebilirliğin sağlanması, standardizasyon sağlanarak homojen parmak izlerinin oluşturulması, bütüncül silme imkânının sağlanması gibi önlemler çerçevesinde web teknolojilerinin mahremiyet odaklı şekilde tasarlanması ve üretilmesi önerilmektedir. Öncelikle ilgili kişiler açısından farkındalığın oluşturulması ile kişilerin bu konuda önlem alması sağlanabilecektir. İlgili kişilere bu konudaki önlem önerileri olarak tarayıcı ayarlarından "takip etme" seçeneğinin seçilmesi, JavaScriptin devre dışı bırakılması, mahremiyet artırıcı teknolojilerin kullanılması önerilmektedir.

Her ne kadar cihaz parmak izi gözlenmesi zor olsa da çeşitli analiz araçları sayesinde günümüzde tespiti yapılabilmektedir. Örneğin reklamcılık amacıyla web sitesine konulan gömülü içerik nedeniyle dijital parmak izi çıkarımı yapılıp yapılmadığının teyit edilmesi gerekmektedir. Özellikle küçük işletmeler hem web sitesi yayımcısı olarak hem de reklam verenler olarak reklamcılık ekosisteminden ekonomik olarak fayda görmektedirler. Bu işletmeler için reklam ekosisteminde yer alan aracı kurumlarla müzakere etmesi kimi zaman zor olabilse de dijital

ekonomide güvenin oluşturulmasının işletmeye olumlu etkisi olacağından, mahremiyet odaklı kuruluşlarla iş birliği yapılması tavsiye edilmektedir.

Diğer işleme şartlarına gidilemediği durumlarda veri sorumlusu tarafından uygun açık rıza alınması ve Kanun'un 10'uncu maddesi uyarınca aydınlatma yükümlülüğünü yerine getirilmesi gerekmektedir. Ortak veri sorumluluğu söz konusu olduğunda dijital parmak izi kullanımına katkı sağlayan taraflar aydınlatma ve açık rıza alınması bakımından sorumluluk sınırlarını belirleyebilecektir. Genel ilkelerin gözetilerek amaçla bağlantılı, sınırlı ve ölçülü olarak kişisel veri işlenmesi, açık rıza alınan işleme amacı değiştiğinde tekrar açık rıza alınması gerekmektedir. Benzersiz dijital parmak izi ve bununla bağlantılı kişisel veriler mevzuatta öngörülen veya işlendikleri amaç için gerekli süre bakımından muhafaza edilmelidir. İşlenmesini gerektiren sebeplerin ortadan kalkması durumunda Kanun'un 7'nci maddesi ve ilgili yönetmeliğe uygun olarak silinmeli, yok edilmeli veya anonim hale getirilmelidir. Veri sorumluları tarafından, Kanun'un 11'nci maddesinde sayılan hakların etkin olarak kullanılabilmesi sağlanmalıdır. Envanter ve Sicile kayıt ve bildirim yükümlülüğü olması halinde dijital parmak izi kullanımına dayalı kişisel veri işlenen süreçlerin de göz önünde bulundurulması gereklidir. Dijital parmak izi çıkarılması amacıyla yurt dışına veri aktarılması gerekebilir, genellikle toplanan verilerden sunucu tarafında benzersiz dijital parmak izleri oluşturulsa da toplanan verilerin de bu durumda kişisel veri olarak ele alınmasının ve yurt dışına aktarım hükümlerinin göz önünde bulundurulmasının uygun olacağı değerlendirilmektedir

Ayrıca sahte reklam verenler tarafından kötücül reklamcılık için dijital parmak izi çıkarımına katkı sağlayan niteliklerin sorgulanmasının meşru bir zemini bulunmamaktadır. Bu tür kötücül kullanımlar için web sitesi operatörlerinin reklam ağları hakkında bilgi edinerek reklam dağıtımı yolları hakkında sahibi olması ve bu konuda teknik tedbirlerin alınması gereklidir.

Araştırmacıların literatürde geniş çaplı ölçüm çalışmaları bulunmakta olsa da henüz Türkiye özelinde bir ölçüm çalışması yapılmamıştır. Dijital parmak izinin çıkarımının çevrim içi gözetim aracı olarak kullanılabilecek bir yöntem olması ve tespit edilebilirliğin zor olması, tarayıcılar arası çapraz izlenebilirlik ve kişinin kimliğinin belirlenmesi riskleri göz önünde bulundurulduğunda, Türkiye'de en sık kullanılan web siteleri için geniş bir ölçüm çalışması yürütülerek yıllar periyodundaki yaygınlığı gözlemlenebilecektir. Böyle bir araştırmanın ayrıca bu çalışmanın amaçlarından da olan dijital parmak izi çıkarımına yönelik olarak farkındalığa katkı sağlayacağı değerlendirilmektedir. ◆

KAYNAKÇA

- Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 674–689. doi: 10.1145/2660267.2660347

- Agencia Española Protecciòn Datos (2019, Şubat). Survey on Device Fingerprinting. Erişim adresi (01.09.2023): https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa

- Araç kiralama programları yazılımcısı ve satıcısı firmalar tarafından, ilgili kişilerin verilerinin işlenmesi ve bu verilerin araç kiralama firmaları arasında paylaşılmasını sağlayan bir kara liste programı oluşturulması hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 tarihli ve 2021/1303 sayılı Karar Özeti (2021, Aralık 23). Erişim adresi (01.09.2023): https://www.kvkk.gov.tr/Icerik/7288/2021-1303

- Avrupa Birliği Adalet Divanı (ABAD). (Aralık, 2018). Judgment in Fashion ID, C-40/17, ECLI:EU:2018:1039. Erişim adresi (01.09.2023): https://curia.europa.eu/juris/recherche.jsf?language=en

- Bahrami, P.N., Iqbal, U., & Shafiq, Z. (2021). FP-Radar: Longitudinal Measurement and Early Detection of Browser Fingerprinting. *Proceedings on Privacy Enhancing Technologies, 2022,* 557- 577. DOI:10.2478/popets-2022-0056. Corpus ID: 244896504.

- Bekavac, I., & Pranicevic, D.G. (2015). Web analytics tools and web metrics tools: An overview and comparative analysis. *Croatian Operational Research Review, 6,* 373-386. DOI:10.17535/crorr.2015.0029

- Bujlow, T., Carela-Español, V., Solé-Pareta, J. & Barlet-Ro, P. (2017). A Survey on Web Tracking: Mechanisms, Implications, and Defenses. Proceedings of the IEEE, 105, 1476-1510. DOI: 10.1109/JPROC.2016.2637878.

- Cao, Y., Li, S., & Wijmans, E. (2017). (Cross-)Browser Fingerprinting via OS and Hardware Level Features. *Network and Distributed System Security Symposium.* doi: 10.14722/ndss.2017.23152

◊ Cooper, A., Tschofenig, H., Aboba, B., Morris, J. P., Hansen, M., & Smith, R. (Temmuz, 2013). Privacy Considerations for Internet Protocols, Erişim adresi: https://datatracker.ietf.org/doc/

◊ Çekin, M. S. (2019). *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku.* İstanbul: On İki Levha Yayıncılık

◊ Eckersley, P. (2010). How Unique is Your Web Browser? *Privacy Enhancing Technologies, 10th International Symposium,* URL: https://api.semanticscholar.org/CorpusID:15233734)

◊ Englehardt, S., & Narayanan, A. (2016). Online Tracking: A 1-million-site Measurement and Analysis. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: Association for Computing Machinery. DOI: 10.1145/2976749.2978313

◊ European Data Protection Board. (2019a). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. Erişim adresi (01.09.2023): https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

◊ European Data Protection Board. (2019b). Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). Monitoring of data subjects' behaviour. Erişim adresi (01.09.2023):https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

◊ European Network and Information Security Agency. (2012). Privacy considerations of online behavioural tracking. Erişim Adresi (08.09.2022): https://www.enisa.europe.eu

◊ Falola, O. O. (2020). Internet Of Things (IOT) *Device Fingerprinting For Anomaly Detection* (Yüksek lisans rezi, Regina Üniversitesi, Kanada). Erişim adresi (01.09.2023): https://ourspace.uregina.ca/items/7286b101-ab0e-4dbb-930b-f700a57a1176

◊ Farid, Z., Nordin, R., & Ismail, M. (2013). Recent Advances in Wireless Indoor Localization Techniques and System. *Journal of Computer Networks and Communications,* 185138:1-185138:12. DOI: 10.1155/2013/185138

◊ Federal Trade Commission. (2016). Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers. Erişim adresi (01.09.2023): https://www.ftc.gov/news-events/news/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive-personal-information-scammers

◊ Felten, E. (2009, Haziran 7). If You're Going to Track Me, Please Use Cookies. Erişim adresi (01.09.2023): https://freedom-to-tinker.com/2009/07/07/if-youre-going-track-me-please-use-cookies/ adresinden alındı.

◊ Fielding R., Reschke E., J., (2014). Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. Erişim adresi (01.09.2023): https://tools.ietf.org/html/rfc7231

◊ Fouad, I., Santos, C., Legout, A., & Bielova, N. (2021, Mayıs 7). Did I delete my cookies? Cookies respawning with browser fingerprinting. Erişim adresi (01.09.2023) https://arxiv.org/pdf/2105.04381.pdf

◊ Gómez-Boix, A., Laperdrix, P., & Baudry, B. (2018). Hiding in the Crowd: an Analysis of the. *WWW2018 - TheWebConf 2018 : 27th International World Wide Web Conference,* 1-10. Erişim adresi (01.09.2023): https://hal.inria.fr/hal-01718234v2

◊ Grajek, G. F., Liu, C., Quach, A. Y., & Lo, J. C. (Mayıs, 2018). Amerika Birleşik Devletler Patent No. US20150237039A1. Erişim adresi (01.09.2023): https://patents.google.com/patent/US20180124039A1/en?inventor=grajek&oq=grajek

◊ HTTP referer explanation (t.y), Erişim Adresi (23.09.2022): https://privacyinternational.org/guide-step/4150/http-referer-explanation

◊ Information Commissioner's Office (2019, Haziran 20). Update report into adtech and real time bidding, Erişim adresi (01.09.2023): https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

◊ Information Commissioner's Office. (t.y.a). What does the UK GDPR say about cookies? Erişim adresi (01.09.2023): https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-the-cookie-rules-relate-to-the-gdpr/

◊ Information Commissioner's Office. (t.y.b). What are cookies and similar technologies?. Erişim adresi (01.09.2023): https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-cookies-and-similar-technologies/

◊ Iqbal, U., Englehardt, S., & Shafiq, Z. (2021). Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors. *2021 IEEE Symposium on Security and Privacy (SP),* 1143-1161. DOI: https://doi.org/10.48550/arXiv.2008.04480

◊ Johnston, A. (2020). Reforming privacy laws to protect against digital harms. Erişim adresi (01.09.2023): http://classic.austlii.edu.au/au/journals/ANZCompuLawJl/2021/11.pdf

◊ Kim, S., Yoo, S. G., & Kim, J. (2017). Privacy Protection Mechanism for Indoor Positioning Systems. International Journal of Applied Engineering Research, 12(9), 1982-1986. Erişim adresi (01.09.2023): https://www.ripublication.com/journals.htm

◊ Laperdrix, P., Bielova, N., Baudry, B., & Avoine, G. (2020). Browser Fingerprinting: Survey. *ACM Transactions on the Web. 14(2).* 1-33. DOI: https://doi.org/10.1145/3386040

◊ Madde 29 Veri Koruma Çalışma Grubu. (2007). Opinion 4/2007 on the concept of personal data, Erişim Adresi (01.09.2023): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4

◊ Madde 29 Veri Koruma Çalışma Grubu. (2010a). Opinion 1/2010 on the concepts of "controller" and "processor". Erişim Adresi (01.09.2023): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4

◊ Madde 29 Veri Koruma Çalışma Grubu. (2010b). Opinion 02/2010 on online behavioural advertising. Erişim Adresi (01.09.2023): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4

◊ Madde 29 Veri Koruma Çalışma Grubu. (2011). Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising. Brüksel: Avrupa Komisyonu. Erişim Adresi (01.09.2023): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4

◊ Madde 29 Veri Koruma Çalışma Grubu. (2014a). Opinion 05/2014 on Anonymisation Techniques. Erişim Adresi (01.09.2023): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4

◊ Madde 29 Veri Koruma Çalışma Grubu. (2014b). Opinion 8/2014 on the on Recent Developments on the Internet of Things. Erişim Adresi (01.09.2023): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4

◊ Madde 29 Veri Koruma Çalışma Grubu. (2014c). Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting. Erişim adresi(01.09.2023): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

◊ Madde 29 Veri Koruma Çalışma Grubu. (2017a). Guidelines on Data Protection Officers ('DPOs') (wp243rev.01), Erişim adresi (01.09.2023): https://ec.europa.eu/newsroom/article29/items/itemType/1360

◊ Madde 29 Veri Koruma Çalışma Grubu. (2017b). *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)* Erişim Adresi (01.09.2023): https://ec.europa.eu/newsroom/article29/items/610140/en

◊ Malvertising. (t.y.). Erişim adresi (01.09.2023): https://www.imperva.com/learn/application-security/malvertising/

◊ Mitigating Browser Fingerprinting in Web Specifications (2019, Mart 28). Erişim adresi (01.09.2023): https://www.w3.org/TR/fingerprinting-guidance/

◊ Molitorisz, S., Meese, J., & Hagedorn, J. (2021). From Shadow Profiles to Contact Tracing: Qualitative Research into Consent and Privacy. Law, Technology and Humans, 3(2), 46-60. DOI:10.5204/lthj.1874

◊ Nalpas, M. (2021, Ekim 14). Referer and Referrer-Policy Best Practices [Blog Yazısı]. Erişim Adresi (01.09.2023): https://web.dev/referrer-best-practices/

◊ Network Advertising Initiative. (2021, Temmuz 23). Retargeting. Erişim adresi (01.09.2023): https://thenai.org/glossary/retargeting/

◊ Nottingham, M. (2020, Aralık 16). Not Similar to Cookies: Device and Browser Fingerprinting as Sensitive Personal Data. DOI: http://dx.doi.org/10.2139/ssrn.3890545

◊ Olejnik, Ł., Acar, G., Castelluccia, C., & Diaz, C. (2016). The Leaking Battery. J. N.-A. Garcia-Alfaro içinde, *Data Privacy Management, and Security Assurance.* Cilt vol 9481. 254-263. DOI:10.1007/978-3-319-29883-2_18

◊ Laperdrix P., Rudametkin W. ve Baudry B. (2016), Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints, 2016 IEEE Symposium on Security and Privacy (SP), 878-894, doi: 10.1109/SP.2016.57.

◊ Plausible. (t.y.). Plausible: GDPR, CCPA and cookie law compliant site analytics. Erişim adresi (01.09.2023): https://plausible.io/data-policy

◊ Rich, J. (2015). Beyond Cookies: Privacy lessons for Online Advertising (Speech, AdExchanger Industry Preview, 21 January 2015), Erişim adresi (01.09.2023): https://www.ftc.gov/system/files/documents/public_statements/620061/150121beyondcookies.pdf

◊ Johnstone, A & Culcane, C. (2020). Cookies and Other Online Identifiers-Research Paper for the Office of the Australian. Erişim Adresi (01.09.2023): https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/research-publications-on-the-privacy-act.

◊ Segers, W. (2021). *A survey and evaluation of browser* (Yüksek lisans tezi, Maastricht University). Erişim adresi (01.09.2023): https://documentserver.uhasselt.be/bitstream/1942/35316/1/fae24997-cffe-46e1-a2b6-2d8a542c18be.pdf

◊ Segura, J. (Malwarebytes), Aseev E. (GeoEdge). (t.y.). Operation Fingerprint: A look into several Angler Exploit Kit malvertising campaigns. Erişim adresi (01.09.2023): https://site.geoedge.com/downloads/documents/Malware_Operation_Fingerprint.pdf?ge_campaign=malware_fingerprint

◊ Top 12+ web analytics tools to improve your site and grow your business. (2023, Haziran 14) Erişim adresi (01.09.2023): https://www.hotjar.com/web-analytics/tools/

◊ Torres, C., Jonker, H., & Mauw, S. (t.y.). FP-Block: usable web privacy by controlling browser fingerprinting. Erişim adresi (01.09.2023): https://core.ac.uk/download/pdf/31206626.pdf

◊ Web Analytics Association. (2010). Social Media Standards . Erişim adresi (01.09.2023): https://www.digitalanalyticsassociation.org/Files/PDF_standards/WAAStandardsSocialMediaDefin.pdf

◊ Web Analytics Association. (2011). Outlook 2011: Survey Report. Erişim Adresi (01.09.2023): https://www.digitalanalyticsassociation.org/Files/PDF_research/outlook_survey_2011.pdf

ELEKTRONİK SÖZLEŞMELER KAPSAMINDA KİŞİSEL VERİ İŞLEME FAALİYETİ VE VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

Neslihan KOÇAK

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "Elektronik Ticaret Hukukunda Kişisel Verilerin Korunması" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Günümüz teknolojisi çok hızlı ve çok çeşitli yönlerden gelişmektedir. Özellikle yapay zekanın son yıllardaki gelişimi, robot teknolojilerinin hayatın hemen her alanında kullanılmaya başlanması, otonom araçların ve cihazların yaygınlaşması, elektronik ticaretin gittikçe genişleyen ticaret hacmi artık dijital çağda belirli bir eşiğin geçildiğini ve bu gelişim hızının zamanla daha da artacağını göstermektedir.

Diğer taraftan, dijital çağın ve internetin gelişimiyle beraber elektronik ortamda gerçekleştirilen ticari ilişkiler ve sözleşmeler de yaygınlaşmaktadır. Elektronik sözleşmelerin yaygınlaşmasıyla beraber insanların kişisel verileri üzerindeki hassasiyeti artmaya ve insan haklarının gereği olarak kişisel verilerin korunması daha çok önem arz etmeye başlamıştır. Zira söz konusu elektronik sözleşmeler vasıtasıyla sözleşmenin güçlü tarafi olan "veri sorumlusu", sözleşmenin diğer tarafi olan "ilgili kişi"lere ait pek çok kişisel veriyi elde etmektedir. Bu kişisel verilerin veri sorumlusu tarafından hukuka uygun işlenmesi, amacına uygun kullanılması ve güvenliğinin sağlanması bir gereklilik ve aynı zamanda veri sorumlusu için bir yükümlülüktür.

Öte yandan, elektronik sözleşme vasıtasıyla işlenen kişisel verilerin analiz edilerek ilgili kişilerin tüketici alışkanlıklarının tespit edilmesi ve ilgili kişilere bu alışkanlıkları doğrultusunda ürün sunularak söz konusu kişisel verilerin veri sorumlusunun ticari kazancını artırmak üzere kullanılması da mevzu bahis olmaktadır. Bu durumda ise, bireyin kişisel verilerinin korunması hakkı ile veri sorumlusunun sözleşmesel hakları arasında bireyin aleyhine bir dengesizlik oluşabilmektedir.

Bu kapsamda, çalışmada öncelikle elektronik sözleşme ve türlerine dair bilgi verilmiş, daha sonra elektronik sözleşmeler kapsamında genellikle işlenmekte olan kişisel verilere, kişisel veri işleme şartlarına, veri sorumlusunun tespitine ve veri sorumlusunun yükümlülüklerine ilişkin 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve sair mevzuat çerçevesinde bilgilendirmede bulunulmuştur.

ELEKTRONİK SÖZLEŞMELER

Genel Olarak

Günlük hayatta *"elektronik ticaret"* ile *"elektronik sözleşme"* kavramları aynı anlamdaymış gibi birbirlerinin yerine kullanılsa da *"elektronik ticaret"* kavramı, *"elektronik sözleşme"* kavramını da kapsayan ve elektronik ortamda yapılan hukuki işlemleri ile ticari faaliyetleri de içine alan daha geniş niteliğe sahip bir üst kavramdır (Kuntoğlu, 2021, s.202; Hamamcıoğlu, 2018, s.49).

"Elektronik sözleşme", "Uluslararası Ticaret Odası" (ICC) tarafından *"tarafların bilgisayarları aracılığıyla ister ağa bağlı olarak ister elektronik mesajlaşma yoluyla sözleşme yapmalarının otomatikleştirilmiş süreci"* olarak tanımlanmaktadır (Wang, 2014, s.33). Buna göre elektronik sözleşme aslında bir sözleşme türü olmayıp, sözleşmenin kuruluş şekliyle alakalı bir terimdir. Elektronik sözleşmenin yazılı sözleşmeden temel farkı da elektronik sözleşmenin elektronik ortamda kuruluyor olmasıdır (Kocasakal Özdemir, 2003 s.37; Önder Balaman, 2016, s.29; Sağlam Atabarut, 2003, s.51; Bayram, 2015, s.334). Bu bakımdan, sözleşmelerin kuruluşuna, geçerliliğine ve ifasına ilişkin Türk Borçlar Hukuku'ndaki düzenlemeler mahiyetine uygun bulunduğu ölçüde e-sözleşmelere de uygulanmaktadır (Kocasakal Özdemir, 2003, s.37; Turan, 2008, s.92). Dolayısıyla, karşılıklı ve birbirine uygun olarak kurucu irade beyanlarının elektronik ortamda icrası elektronik sözleşmeden söz edebilmek için şarttır (Bayram, 2015, s.334; Önder Balaman, 2017, s.289).

Aynı şekilde, UNCITRAL internet üzerinde kurulan sözleşmelerle ilgili özel bir tanımlama tapma ihtiyacı duymamıştır. Zira UNCITRAL tarafından da Türk Hukukuyla paralel olarak, internet vasıtasıyla kurulan sözleşmeler farklı bir sözleşme tipi şeklinde değerlendirilmemekte ve fakat sözleşmenin kurulmasındaki bir yöntem olarak görülmektedir (Turan, 2008, s.92).

Günümüz ticari hayatında, neredeyse sınırsız mal ve hizmet üretilmekte, topluma arz edilmekte ve bu yolla binlerce sözleşme akdedilmektedir. Bu nedenle sözleşmeyi hazırlayan taraflar, her defasında aynı sözleşme konusu üzerinde yeniden içerik hazırlamak yerine "standart sözleşmeler" vasıtasıyla iş yapmayı tercih etmişlerdir (Önder Balaman, 2017, s.291). Bu sözleşmelere tarafi olacak kişilerin ise iradelerini kullanabileceği tek yöntem kabul veya red beyanı yöneltmek şeklindedir. Elektronik sözleşmeler bakımından da aynı husus söz konusu olup, sözleşmenin tarafları irade beyanlarını dijital ortamda icra ettiklerinden genellikle sözleşme maddelerini karşı tarafla müzakere etme imkânına sahip olamamaktadır. Bu tür sözleşmeler, çoğunlukla satıcının önceden hazırladığı sözleşme şartlarını internet sitesi aracılığıyla sunması, müşterinin ise bu şartları olduğu gibi kabul etmesiyle kurulmaktadır (Önder Balaman, 2017, s.292). Bu bakımdan, elektronik sözleşmeler kuruluş şekli açısından genellikle *"iltihakî (katılmalı) sözleşme"* özelliği göstermektedir (Turan, 2008, s.95).

6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunu'nun (ETDHK) 2/1 maddesinin (c) bendindeki *"ticari elektronik ileti" tanımında yer verilen araçlara göre; "Elektronik posta, çağrı merkezi, telefon, faks, akıllı ses kaydedici sistem, otomatik arama makinesi ve kısa mesaj gibi vasıtalar aracılığıyla"* yapılan sözleşmelerin, elektronik sözleşme olacağı yorumu yapılabilmektedir (Önder Balaman, 2017, s.290). Bununla birlikte, internet aracılığıyla yapılan tüm sözleşmelerin elektronik sözleşme olacağını söylemek mümkün değildir. Zira, *"Web sayfası kurulması, bir servis sağlayıcı ile internete bağlanmak üzere aralarında sözleşme yapılması bir server üzerine reklam yapılması, vb. işlemler"* elektronik sözleşme kapsamında değerlendirilmemektedir. Örneğin, konusu kişinin internet üzerinden satış yapacağı web sayfasının hazırlanması olan bir sözleşmenin, bir "eser sözleşmesi" olarak kabul edilmesi gerekmektedir (Önder Balaman, 2017, s.290).

Elektronik Sözleşme Türleri

Ürünlerin Niteliği Açısından Elektronik Sözleşmeler

Mal Satımına İlişkin Elektronik Sözleşmeler

Mal satımını konu alan elektronik sözleşmelerde, sözleşme internet üzerinden kuruluyor olsa da sözleşmenin ifası ise kurye, posta vb. fiziksel yöntemler aracılı-

ğıyla yapılmaktadır (Arslan ve Öz, 2020, s.17; Turan, 2008, s.93). Sözleşmenin konusunu kitap, oyuncak, kıyafet gibi her çeşit mal oluşturabilmektedir. Sözleşmeye konu ürünün fiziksel olarak teslim edilmesi nedeniyle bahis olunan sözleşmelere *"dolaylı (offline) elektronik sözleşme"* denmektedir.

Dijital Ürün Satımına Yönelik Elektronik Sözleşmeler

Elektronik ortamda bulunan yazılım, bilgisayar programı gibi ürünlerin online olarak alıcının sistemine yüklenmesini konu alan sözleşmelerdir. Burada sözleşme ve teslimatın her ikisinin de elektronik araçlarla gerçekleştirilmesi nedeniyle *"doğrudan (online) elektronik sözleşme"* söz konusu olmaktadır (Turan, 2008, s.93).

Hizmet Sunumuna Yönelik Elektronik Sözleşmeler

Konusu *"tren/konser/tiyatro bileti temin etme, bankacılık hizmetleri, otel rezervasyonu vb."* hizmetin yerine getirilmesi olmaktadır. Söz konusu hizmet edimi internet ortamında ifa edilmektedir (Turan, 2008, s.93).

İrade Beyanlarının Açıklanma Anı Açısından Elektronik Sözleşmeler

Hazırlar arası sözleşmeler, sözleşmenin taraflarının sözleşmenin kuruluş beyanlarını aynı anda birbirlerine açıklama fırsatı buldukları sözleşmeler olma özelliğini göstermektedir. Diğer taraftan ***hazır olmayanlar arası sözleşmeler,*** sözleşmenin kuruluş beyanları ile bu beyanların muhatabına ulaşması arasında bir zamanın geçtiği sözleşmelerdir (Kılıçoğlu, 2012, s.64).

Sözleşmelerin hazırlar arası olup olmadığı ortaya koyan unsur, tarafların birbirlerinin beyanlarını karşılıklı şekilde anında öğrenme ve karşılık olarak cevap verme imkânlarının bulunması olup, tarafların fiziksel olarak bir arada olup olmaları önem arz etmemektedir. Bu açıdan, irade beyanlarının iletilmesinde kullanılan vasıtalar ya da yöntemler, sözleşmenin kuruluş beyanlarının anlık olarak karşı tarafa erişmesine elverişli ise "hazırlar arası elektronik sözleşme" gündeme gelmektedir (Arslan ve Öz, 2020, s.18-19; Turan, 2008, s.94-95; Önder Balaman, 2017, s.291). Örnek verilecek olursa; irade beyanları anlık olarak karşı tarafa iletildiğinden video/görüntülü görüşmeler aracılığıyla kurulmuş sözleşmeler *"hazırlar arasında"*, anlık olarak irade beyanları karşıdaki muhataba iletilmediğinden e-posta vasıtasıyla kurulan sözleşmeler *"hazır olmayanlar arasında"*dır (Arslan ve Öz, 2020, s.18-19; Turan, 2008, s.94-95).

Teknolojinin gelişmesiyle birlikte, telgraf, telefon, teleks, faks ve son olarak internet vasıtasıyla da sözleşmenin kuruluş beyanlarının icra edilmesi mümkün olmuştur (Turan, 2008, s.93-94).

İrade Beyanını Açıklamada Kullanılan Araçlar Açısından Elektronik Sözleşmeler

Elektronik sözleşmeler Borçlar Hukuku anlamında kurulduğu elektronik ortamdan başka bir farklılık arz etmediğinden, genel kurallarla paralel şekilde e-sözleşmeler bakımından da irade beyanları özel bir şekil şartına bağlı bulunmamaktadır. Burada önem arz eden nokta, tarafların anlaşmaya varmalarıdır. Böylelikle taraflar irade beyanlarını online bir görüşmede, e-posta aracılığıyla veyahut bir internet sayfasındaki sipariş formunu doldurup satıcıya iletmek suretiyle elektronik yöntemlerle açıklayabilir.

İnternet ortamında akdedilen sözleşmeler bakımından internet sayfasında duyurulan genel nitelikteki şartlardan sonra yer verilen *"kabul ediyorum"* sekmesinin seçilmesi yoluyla kabul beyanı açıklanabileceği gibi, e-posta aracılığıyla iletilen öneriyi karşıdaki muhatabın da aynı şekilde e-posta vasıtasıyla açıkça kabul ettiğini belirtmesiyle irade açıklamasında bulunabilir (Önder Balaman, 2017, s.296).

İnternet aracılığıyla kurulan e-sözleşmelerin, temel olarak ***web sitesi, e-posta, EDI, spamming ve chat (internet relay chat – IRC)*** vasıtasıyla kurulan sözleşmeler olarak sınıflandırılması mümkündür.

ELEKTRONİK SÖZLEŞMELER VE KİŞİSEL VERİLERİN KORUNMASI

Bilindiği gibi, günümüzde sayısız mal ve hizmet alışverişi elektronik ortamda yapılmaktadır. Bu bağlamda işletmeler ve alıcıların ikisi için de önem arz eden dezavantajlı durum ise "güvenlik" olarak görülmektedir (Hamamcıoğlu, 2018, s.44). Zira elektronik ortamda gerçekleştirilen işlemler neticesinde pek çok kişisel verinin elde edilmesi ve işlenmesi söz konusu olmaktadır.

Aslında kişisel verilerin elde edilmesi ve işlenmesi devlet kurumunun oluşmasını takiben söz konusu olmuştur. Devlet, kamu hizmeti ve güvenlik gibi çeşitli unsurları gerekçe göstererek kişisel veri işleme faaliyetine başlamıştır. Daha sonra tüketim ekonomisine geçilmesi sonucu işletmeler de müşteri çevresi kapsamında kişisel veri toplamaya başlamışlardır (Oğuz, 2018, s.122). Bu bakımdan, özellikle e-ticaret faaliyetleri kapsamında şirketlerin kişisel veri işlemeleri kaçınılmaz olmuştur.

Nitekim, elektronik platform üzerinden yapılan ticarî faaliyetler bakımından

başta gelen bir vasıta olarak elektronik sözleşmeler de bu açıdan pek çok kişisel verinin işlenmesine konu olmaktadır. Bu kapsamda çalışmamızın aşağıdaki bölümünde, e-sözleşmeler çerçevesinde kişisel verilerin işlenmesi *"6563 sayılı ETDHK", "6698 sayılı KVKK"* ve sair ikincil mevzuat hükümleri çerçevesinde ele alınacak ve değerlendirmelerde bulunulacaktır.

ELEKTRONİK SÖZLEŞMELERDE İŞLENEBİLEN KİŞİSEL VERİLER

"Kişisel veri" tanımına 6698 sayılı KVKK'nin 3/1 maddesinin (d) bendinde; "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak yer verilmiştir. KVKK hazırlanmasına temel teşkil eden "AB Veri Koruma Direktifi" m.2 kapsamında yer verilen tanım da mevzuatımızdaki tanım ile paralel bulunmaktadır. KVKK gerekçesinde de "özgeçmiş, pasaport numarası, sosyal güvenlik numarası gibi verilerin dolaylı da olsa kişiyi belirlenebilir kılmaya elverişli olmaları nedeniyle kişisel veri olarak değerlendirilmesinin gerekli olduğu"na işaret edilmiştir. Bu kapsamda kişisel verinin;

> *"Kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğiyle ilişkili somut bir nitelik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayacak nitelikte olması" gerekmekte olup; "ad, soyad, telefon numarası, doğum tarihi, doğum yeri, T.C. kimlik numarası, kişinin fiziksel, ekonomik ve sair özelliklerine ilişkin bilgiler ile ailesine ilişkin bilgiler, kişiye ait motorlu taşıt plakası bilgisi gibi veriler"*

olduğu kabul edilmektedir (Kişisel Verileri Koruma Kurumu, 2019a, s.1).

Öte yandan, ABAD *"Patrick Breyer v. Federal Republic of Germany"* davasında vermiş olduğu kararına göre;

> *"Kendilerine ait siteleri ziyaret edenlerin 'IP adreslerini', siber saldırılara karşı korunma gerekçesiyle depolamakta olan Alman kurumlarının işlemlerini değerlendirmiştir. Divan kararında, dinamik IP adreslerinin her ne kadar kime ait olduğu bilinmese de erişim sağlayıcılardan elde edilecek ek bilgi ile kime ait oldukları anlaşılacağından söz konusu IP adres verilerinin kimliği belirlenebilir kişiye ait kişisel veriler olduğu neticesine varılmıştır"* (CJEU, 2016).
>
> *Divana göre, ek verinin veri sorumlusunun elinde olması şart olmayıp mühim olan ek veriye ulaşılabilmesidir. Ancak ek veriye ulaşmak yasaksa ya da masraf, emek ve zaman bakımından güçlük söz konusu ise veriler belirlenebilir kabul edilmeyecektir (Keser, 2019). Ayrıca Divan; "İnternet sitesinin elinde bulunan IP adresinin mutlak olarak kişisel veri olarak değerlendirilemeyeceğini, her somut durumun kendi içerisinde değerlendirilmesi gerektiğini ve dinamik IP adresi ile ilgili kişinin belirlenebilmesi hususunda internet servis sağlayıcısı nezdindeki ek bilgilerin birleştirilebilmesi imkânına önem atfetmiştir."*

Bilindiği üzere, elektronik sözleşmeler kapsamında da sözleşmenin taraflarına ilişkin olarak çeşitli veriler işlenmektedir. Söz konusu verilerin "kişisel veri" olmasındaki belirleyici kriter, *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin"* olmasıdır. Bu çerçevede, elektronik sözleşmeler önceki bölümlerde bilgi verilen elektronik ticaret türlerinden herhangi biri (B2B, B2C, C2C, C2B, B2G, G2C) kapsamında kurulabilecekse de kişisel verilerden bahsedebilmek için elektronik sözleşmenin taraflarından birinin mutlaka gerçek kişi olması gerekmemekle birlikte, sözleşmede gerçek kişiye ait kişisel verilerin işlenmiş olması gerektiğinin önemle altı çizilmelidir.

Diğer taraftan, işletmeler arasında (B2B) ya da işletme ile idare arasında (B2G) kurulan bir elektronik sözleşmede pek tabii gerçek kişilere ait kişisel verilerin işlenmiş olması mümkündür. En basit örnekle, elektronik sözleşme tüzel kişiliği haiz işletmeler arasında kurulmuş olsa da sözleşmede işletmenin yetkilisi olan gerçek kişilerin e-imzası bulunacaktır. Burada gerçek kişiler elektronik sözleşmenin tarafı değildir fakat, şirket yetkilisi olmalarından ötürü ad, soyad, e-imza vb. kişisel verilerinin sözleşme kapsamında işlenmesi söz konusudur. Bu nedenle bu kişiler de KVKK kapsamında "ilgili kişi" sıfatını haiz olabilecek ve yasal korumadan yararlanabilecektir. Dolayısıyla, her somut olay özelliklerine göre değerlendirilmeli ve öncelikle elektronik sözleşme kapsamında kişisel veri işlenip işlenmediği gözden geçirilmelidir.

Veri sorumlusu konumundaki aracı hizmet sağlayıcılar ile hizmet sağlayıcıların, alıcı konumundaki kişilerden e-ticaret çerçevesinde ne tür verileri talep edebilecekleri ise 6563 sayılı Kanun'da belirtilmemiş olup, özel bir düzenleme bulunmaması nedeniyle 6698 sayılı KVKK'de düzenlenen kişisel veri işleme şartları ile genel ilkeler kapsamında kişisel veriler işlenebilecektir (Kuntoğlu, 2021, s.208). Bu çerçevede, elektronik sözleşmeler kapsamında işlenen başlıca kişisel veriler konusunu ilerleyen başlıklar altında ele alacağız.

Sözleşmeye İlişkin Veriler

Elektronik sözleşmelerde öncelikle ***"sözleşmenin kurulması için gerekli"*** birtakım kişisel verilerin işlendiği görülmektedir. Sözleşmenin kurulmasına yönelik ola-

rak işlenen kişisel veriler temel nitelikte olup, faturalandırma işlemi için *"kimlik bilgileri"* (ad, soyad, TCKN); faturalandırma ve sözleşme konusu ürün teslimatı işlemleri için "iletişim bilgileri" (telefon numarası, e-posta adresi, adres bilgileri) bu nitelikteki kişisel verilere örnek oluşturacaktır.

Doğal olarak, her elektronik sözleşmenin konusuna göre, işlenmesi gerekli temel veriler de farklılık arz edebilecektir. Örneğin elektronik ortamda akdedilen bir özel sağlık sigortası sözleşmesi için başkaca kişisel veriler ve özel nitelikli kişisel veriler üzerinde işleme faaliyeti yürütülmesi gündeme gelebilecektir. Burada dikkat edilmesi gereken husus, veri minimizasyonu ilkesine riayet edilmesi gerektiğidir. Mesela, alıcı konumundaki ilgili kişilerden talep edilen kimlik bilgileri, tüm kimlik bilgilerini değil, sözleşmenin kurulması kapsamında alıcı tarafın kimliğini belirlemeye yarayacak ölçüde bilgiyi kapsamalıdır (Demirbaş, 2015, s.66).

Yine, ABAD'ın *"Patrick Breyer v. Federal Republic of Germany"* kararı doğrultusunda, ilgili kişilerin IP adreslerinin işlenmesi hâlinde, her somut durumda veri sorumlusunun bu bilgiyle ilgili kişinin kimliğini belirleyip belirleyemediğine göre kişisel veri değerlendirmesi yapılmalıdır.

Diğer taraftan, elektronik sözleşmeler kapsamında, sözleşmenin konusunu oluşturan hizmetin niteliklerini veya ürünün özelliklerini belirten ***"sözleşme içeriği verileri"*** arasında da sözleşmenin taraflarına ilişkin kişisel verilerin bulunması mümkündür.

Kullanıcı Profili Verileri

İlgili kişilerin e-ticaret siteleri üzerinden kurdukları elektronik satış sözleşmeleri neticesinde, "müşteri işlem bilgileri" olarak adlandırabileceğimiz, *"Sipariş ve fatura bilgileri, teslimat bilgileri, alışverişle ilgili gerçekleşen işlem geçmişi bilgisi, talep ve şikâyet bilgisi, platformda yer alan ürünlere ilişkin yapılan yorumlar, müşteri hizmetleriyle yapılan konuşma içeriklerine yönelik bilgiler vb."* şeklindeki kişisel veri niteliğini haiz olabilecek bilgileri de işlenebilmektedir. Söz konusu kişisel veriler, ilgili kişinin söz konusu e-ticaret sitesinde kayıtlı bir "kullanıcı profili" oluşturması durumunda yine bu profil kapsamında kaydedilebilmektedir.
İlgili kişilerin internet sayfalarındaki hareketleri ve yaptıkları alışverişler baz alınarak psikolojik ve istatistiksel analizler neticesinde ilgileri, alışkanlıkları ve diğer özellikleri kapsamında kişilikleri hakkında ayrıntılı ve gerçeğe yakın bir sonuç çıkarılması ile elde edilen verilerin oluşturduğu bütüne "kullanıcı profili" adı verilmektedir (Demirbaş, 2015, s.70). İlgili kişilere ait bu kullanıcı profili verilerinin analiz edilmesi suretiyle, ilgili kişilerin internet üzerinde yaptıkları işlemler

detaylı şekilde tespit edilmekte; daha sonra tüketim alışkanlıklarına uygun şekilde ilgili kişilere satış önerilerinde bulunulmaktadır (Kuntoğlu, 2021, s.209-210). Bu açıdan, ETDHK'nin 10. maddesi ve KVKK'nin veri sorumlusunun yükümlülüklerine yönelik ilgili maddeleri çerçevesinde, hizmet sağlayıcılar ve aracı hizmet sağlayıcıların akdettikleri e-sözleşmeler vasıtasıyla elde ettikleri kişisel verilerin hukuka uygun işlenmesini ve güvenliğini sağlama yükümlülükleri ilgili kişilerin kullanıcı profillerini de kapsamalıdır (Demirbaş, 2015, s.72).

Bağlantı Verileri

"Log kaydı, şifre vb." kullanıcılar tarafından internet üzerindeki gezintilerine ilişkin ögelerden meydana gelen verilere ***"bağlantı verileri"*** denilmektedir. Bağlantı verileri de elektronik ortamda sunulan hizmetler bakımından koruma kapsamında dahil olan kişisel veri türlerindendir. Bu veriler, ilgili kişilerin kullanıcı adı, şifresi, ziyaret ettiği web sayfaları ve eriştiği bilgiler ile internet ortamında yüklediği verilerin log kaydı hâlindeki versiyonlarıdır (Demirbaş, 2015, s.67-68; Kuntoğlu, 2021, s.208).

Ödeme Verileri

Ödeme verileri, internet ortamında sunulan hizmetlerin ya da satılan ürünlerin karşılığı olarak kullanıcıların yüklendikleri borcun ifasına yönelik olarak paylaşılan banka hesap bilgileri, banka kartı ya da kredi kartı bilgileridir (Demirbaş, 2015, s.68).

Farklı ödeme araçları e-sözleşmelerin ifasında kullanılmaktadır. Bu bakımdan ödeme işlemleri için; *"Kredi kartı, elektronik fon transferi (bir paranın bir bankadaki hesaptan bir başka bankadaki hesaba elektronik ortamda nakli), akıllı kart veya elektronik para (dijital ortamda bulunan ve mali değer içeren elektronik veri), elektronik çek gibi diğer ödeme araçları"* tercih edilebilmektedir (Önder Balaman, 2016, s.75).

Bununla beraber, e-ticaret faaliyetlerinde ödeme aracı olarak büyük bir çoğunlukla banka kartları ve özellikle kredi kartları tercih edilmektedir. İlgili kişi e-sözleşme konusu mal veya hizmetin bedelini ödemek üzere e-ticaret platformundaki ilgili bölüme kartının türü (banka kartı ya da kredi kartı), kart sahibinin adı ve soyadı, kart numarası, son kullanma tarihi ve güvenlik kodundan oluşan verilerin girişini yapmaktadır. Bunu takiben hizmet sağlayıcı ya kendisi ya da bir "ödeme hizmeti sağlayıcısı" (6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun"un

13. maddesi uyarınca ödeme kuruluşları, elektronik para kuruluşları, 5411 sayılı Bankacılık Kanunu kapsamındaki bankalar ve PTT ödeme hizmeti sunabilir ve bu kuruluşlar "Ödeme Hizmeti Sağlayıcısı" olarak adlandırılır.) vasıtasıyla, sunduğu mal veya hizmetin bedeli olarak alacağını tahsil etmektedir.

Kart bilgilerinin sisteme girilmesinde itibaren ilgili kişiye ait bu kişisel verilerin üçüncü kişilerin eline geçmesi ve ilgili kişinin bu bilgiler kullanılmak suretiyle zarara uğratılması tehlikesi ortaya çıkmaktadır. Hizmet sağlayıcılar ya da sundukları aracılık hizmetinden yararlanılan aracı hizmet sağlayıcılar tarafından ilgili kişinin kart bilgilerinin korunması için gerekli idarî ve teknik tedbirler alınmış olmalıdır (Demirbaş, 2015, s.68-69).

Bu çerçevede, ödeme bilgileri de KVKK kapsamında koruma altındaki verilerdendir. Ödeme verilerine ilişkin olarak KVKK'nin sağladığı korumanın yanı sıra ***"5464 sayılı Banka Kartları ve Kredi Kartları Kanunu"*** ihtivasında da özel düzenleme bulunmaktadır. Bu bağlamda, 5464 sayılı Kanun'un "Bilgilerin saklanması" başlıklı 23. maddesinde;

> *"'Üye işyerleri', kartın kullanımı sonucunda kart ve 'kart hamili' ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına açıklayamaz, saklayamaz ve kopyalayamaz. Üye işyerleri, kart bilgilerini üye işyeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamaz, satamaz, satın alamaz ve takas edemez. Üye işyeri anlaşması yapan kuruluşlar, bu fıkranın uygulanmasını gözetmekle yükümlüdür.*
> *Kart çıkaran kuruluşlar, edindikleri kişisel bilgileri gizli tutmak, kendi hizmetlerinin pazarlanması dışında başka amaçlarla kullanmamak ve kanunla yetkili kılınan kişi, kurum ve kuruluşlar dışında kalanların bu bilgilere ulaşmasını engellemek amacıyla gereken önlemleri almakla yükümlüdür."*
> hükmü düzenlenmiştir.

Ödeme banka kartı ya da kredi kartı ile gerçekleştirdiğinde, kart üzerinde bulunan çipteki veriler POS (Point of Sale) cihazları ile sayısal veriye dönüştürülerek elektronik ortamda saklanabilir, kopyalanabilir ya da aktarılabilir duruma gelmektedir. Bu noktada, bankalar alışveriş esnasında kullanılan banka kartı veya kredi kartı gibi ödeme araçlarıyla transfer edilen kişisel verilerin üye işyeri tarafından saklanması ya da bunların üçüncü kişilere aktarılmasını engelleyecek teknik imkânlar hazırlamakla yükümlü bulunmaktadır (Demirbaş, 2015, s.70).

Elektronik İmza

Sözleşmelerin yapılması herhangi bir şekle bağlı olmamakla birlikte, yazılı şeklin öngörüldüğü sözleşmeler bakımından borç altına girenlerin imza yükümlülüğü bulunmaktadır. TBK 14/2 maddesi uyarınca; *"Kanunda aksi öngörülmedikçe, imzalı bir mektup, asılları borç altına girenlerce imzalanmış telgraf, teyit edilmiş olmaları kaydıyla faks veya buna benzer iletişim araçları ya da güvenli elektronik imza ile gönderilip saklanabilen metinler de yazılı şekil yerine geçer."*

Yine, TBK "İmza" başlıklı 15/1 maddesine göre, güvenli e-imza el yazısıyla atılmış imzanın tüm hukuksal neticelerini doğurmaktadır. Gelişen teknolojinin bir getirisi olan e-ticaret sayesinde tarafların birbirlerini görmeden ve tanımadan e-sözleşmeler kurmaları mümkün hâle gelmiştir. Bu noktada e-imzaların sağladığı imkânla yazılı şekle başvurmadan geçerli sözleşmeler kurabilmektedir (Önder Balaman, 2016, s.65-66).

5070 sayılı EİK'nin 3/1 maddesinin (a) fıkrasında ***"elektronik veri",*** *"elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar"* olarak tanımlanmakta olup, Kanun'un 3/1 maddesinin (b) fıkrasında ***"elektronik imza",*** *"başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"* şeklinde açıklanmıştır. Kanun'da yapılan tanımdan yola çıkarak elektronik imzanın, "Elektronik ortamda oluşturulmuş bir mesajın bütünlüğünü ve değişmemiş olduğunu belirten veya imzalayan kişinin kimliğinin tanınmasına imkân veren ve veri mesajı içeriğini onayladığını gösteren elektronik formattaki her türlü işaret." olarak tanımlanması mümkündür (Önder Balaman, 2016, s.66). Elektronik sertifika hizmet sağlayıcıları e-imza hizmeti verdikleri ilgili kişilerin ad, soyad, iletişim bilgileri (e-posta adresi, adres, telefon numarası), iş bilgileri (unvan, iş yeriyle ilgili bilgiler), ıslak imza, IP adresi, diğer benzersiz cihaz tanımlayıcıları ve coğrafi konum bilgileri gibi kişisel verilerini işlediğinden, yeterli gizlilik koruması sağlamaları ve ilgili kişilere kişisel verilerine erişim hakkı vermeleri önemlidir.

Elektronik imza, *"güvenli elektronik imza"* ile *"basit elektronik imza"* olarak iki ayrı çeşide ayrılmakta olup, güvenli elektronik imza ve basit elektronik imzanın ayırımı, ispat hukuku açısından önem arz etmektedir (Önder Balaman, 2016, s.71-72). Buna göre, ***"Basit elektronik imza",*** *"Bilgisayar ekranına, belirli bir sayısal şifre ile kodlama yapılmaksızın kalemle atılan imzalar, biyometrik imzalar, elle atılan imzanın sonradan tarayıcıdan geçirilerek taranarak elektronik ortama atılıp saklanması şeklinde olan imzalar."* olarak sayılabilir.

"Güvenli elektronik imza" ise, *"Elektronik verinin bütünlüğünün korunmasına ek olarak, imzalayan kişinin kimliğini de koruyan bir yapıya sahiptir."* Güvenli elektronik imza, EİK'nin 4. maddesinde şu şekilde tanımlanmıştır:

> *"Güvenli elektronik imza; a) Münhasıran imza sahibine bağlı olan, b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan, elektronik imzadır."*

Bu düzenlemeye göre,

> *"Güvenli elektronik imzanın kimlik doğrulama fonksiyonunun sağlıklı şekilde gerçekleşmesi için münhasıran imza sahibine bağlı olması mecburîdir. Bu şekilde, elektronik imza kişiselleştirilerek, münhasıran imza sahibine bağlı olduğu garanti edilmekte ve elle atılan imzanın niteliklerini haiz olmaktadır. Ayrıca, sadece imza sahibinin tasarrufu altındaki güvenli e-imza, nitelikli elektronik sertifika sağlayıcılar tarafından oluşturulurken; e-imza verilerinin bir benzeri bulunmamalı ve gizliliğini korunmalıdır. Bahis olunan verilerin üçüncü kişilerce elde edilememesi, kullanılamaması, değiştirilememesi ve e-imzanın sahteciliğine karşı korunması gerekmektedir."* (Önder Balaman, 2016, s.72).

Diğer taraftan ilgili Kanun maddesinde, güvenli e-imza oluşturma aracının yalnızca imza sahibinin tasarrufunda bulunması gerektiği belirtilmiştir. Buradaki sorumluluk ise esasen imza sahibinin olmaktadır. Elektronik sertifika hizmet sağlayıcıları bu açıdan hukuki sorumluluk altında bulunmaktadır. EİK'nin 10/1 maddesinin (f) bendinde, *"Elektronik sertifika hizmet sağlayıcısının sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirme yükümlü olduğu belirtilmiştir."* (Önder Balaman, 2016, s.72-73).

E-sözleşmelerde güvenli elektronik imzanın kullanılmasıyla tarafların ehliyetlerine ilişkin tereddütler de ortadan kalmaktadır. Zira, kimlik bilgilerinin bilinmesi sebebiyle güvenli e-imza vasıtasıyla sözleşme yapmakta olan şahısların ehliyetle ilgili sorun yaşaması gündeme gelmeyecektir (Önder Balaman, 2016, s.73).

Çerezler

E-ticaret kapsamında kişisel verilerin elde edilmesine ilişkin diğer bir yöntemise çerezler (*cookies*) dir. Çerez;

> *"İnternet sitesi operatörleri tarafından kullanıcı cihazına yerleştirilen bir tür metin dosyası olup HTTP(S) (Hiper Metin Transferi Protokolü) talebinin bir parçası olarak aktarılır. Diğer bir tanıma göre ise çerezler, bir internet sayfası ziyaret edildiğinde kullanıcılara ilişkin birtakım bilgilerin kullanıcıların terminal cihazlarında depolanmasına izin veren düşük boyutlu zengin metin biçimli text formatlarıdır."* (Kişisel Verileri Koruma Kurumu, 2022a, s.8).

Çerezlerin kısaca, web sunucuları tarafından tarayıcı vasıtasıyla kullanıcıların bilgisayarlarına sonraki kullanımlar için yerleştirilen bilgi parçacıkları olarak tanımlanması da mümkündür. Bu yöntemle kullanıcıların internet ortamındaki eğilimleri analiz edilmektedir. Mesela çerezler, kişiye en hitap eden tanıtımın gönderilmesi maksadıyla kullanılabilmektedir. Çerezlerin teknik olarak virüs taşımaları ya da herhangi bir kod çalıştırmaları mümkün olmayıp, silinmeleri ve engellenmeleri mümkündür (Oğuz, 2013, s.4-6).

> *"Yalnızca kişisel verileri elde edilecek kişinin açık rızası ile çerezlerin kullanılabilmesi gerekirken; kişinin çerez kullanımını kabul etmediği takdirde ilgili sayfayı kullanamaması ya da çerez kullanımını kabul ettiği takdirde ne tür kişisel verilerinin elde edileceği konusunda yeterince aydınlatılamaması ilgili kişinin iradesine bir müdahale olup bir insan hakları sorunu olduğu değerlendirilmektedir."* (Kuntoğlu, 2021, s.209-210).

> *"Günümüzde 'kişisel veri', 21. yüzyılın petrolü; çerezler ise bu petrolün çıkarıldığı sondaj cihazları konumundadır. ABD'nin çerez diliminin %50'si Google'ın elinde; geri kalan önemli bir kısmı ise Amazon, Facebook ve Twitter gibi kuruluşların elinde bulunmaktadır. Çerez üreticileri elde ettikleri veriler ile ilgili kişiyi belirleyemediklerini iddia etmekte iseler de teknolojinin geldiği aşamada ilgili kişilerin çerezlerin yanında ek bilgilerle belirlenebilir olacakları aşikârdır. Nitekim ABAD da çerezlerin kişisel veri mahiyetinde olduğunu düşünmektedir. Bu itibarla, ETDHK m. 10 ve KVKK kapsamında hizmet sağlayıcılar ve aracı hizmet sağlayıcıların kişisel verilerin korunması çerçevesindeki sorumlulukları şüphesiz çerezleri de kapsamaktadır."* (Kuntoğlu, 2021, s.209-210).

KİŞİSEL VERİ İŞLEME ŞARTLARI

"Kişisel verilerin işlenmesi" KVKK'nın 3. maddesinin birinci fıkrasının (e) bendinde;

"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem" olarak belirtilmiştir.

KVKK'nin 5. maddesi şu şekilde kaleme alınmıştır:

"(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

Özel nitelikli kişisel verilerin işlenme şartları ise Kanun'un 6. maddesinde düzenlenmiş olup, kural olarak özel nitelikli kişisel verilerin, ilgili kişinin açık rızası olmaksızın işlenmesi yasaktır. Bununla birlikte, "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri"arasından sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir.

Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak; *"Kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın"* işlenebilir.

Bu çerçevede "açık rıza", kişisel verilerin işlenmesi için en temel şarttır. KVKK'nin 5. maddesinin ikinci fıkrasının (c) bendinde, açık rıza işleme şartının istisnaları

arasında düzenlenen *"Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması"* durumu da elektronik sözleşmeler için bakımından önem arz eden bir kişisel veri işleme gerekçesi oluşturmaktadır (Kuntoğlu, 2021, s.208). Nitekim, e-sözleşme akdeden veri sorumlusunun sözleşmenin karşı tarafi olan gerçek kişiye ait "ad, soyad, iletişim bilgisi, adres bilgisi gibi" kişisel veri niteliğini haiz bilgileri işlemesi bu veri işleme şartına dayalı olarak gerçekleştirilecektir.

Kişisel verilerin işlenmesi 5. madde kapsamında açık rıza dışındaki bir işleme şartına dayalı olarak gerçekleştirilmesine karşın, ilgili kişilerden açık rıza alınmış ise bu durum Kişisel Verileri Koruma Kurulu tarafından kötü niyetli olarak değerlendirilmektedir. Nitekim, *"Kişisel Verileri Koruma Kurulunun 20/04/2021 tarihli ve 2021/389 sayılı Kararı"*nda, yerinde bir değerlendirmede bulunularak;

"...Ayrıca söz konusu kişisel veri işleme faaliyeti, Kanunda yer alan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmadığı ve veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılmasının, aldatıcı ve hakkın kötüye kullanımı niteliğinde olacağı ve bu durumun ise Kanunun 4 üncü maddesinin ikinci fıkrasının (a) bendinde düzenlenen "hukuka ve dürüstlük kurallarına uygun olma" ilkesine aykırılık teşkil ettiği, değerlendirmelerinden hareketle; Kanunun 5 inci maddesinde yer alan diğer işleme şartları mevcut iken ilgili kişilerin açık rızasının alınmasının Kanunun 4 üncü maddesinde yer alan "hukuka ve dürüstlük kurallarına uygun olma" ilkesine aykırı olduğu dikkate alındığında Kanunun 12 nci maddesinin (1) numaralı fıkrasında yer alan yükümlülüklerini yerine getirmeyen veri sorumlusu hakkında, Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca söz konusu uygulamanın ihbar eden dışında pek çok kişi üzerinde olumsuz etki doğurabileceği, veri sorumlusunun sunduğu hizmet bakımından geniş bir müşteri kitlesi bulunduğu, Şirketin kusuru, ekonomik durumu ve haksızlık içeriği gibi hususlar da göz önünde bulundurularak 250.000 TL idari para cezası uygulanmasına..." karar verilmiştir (Kişisel Verileri Koruma Kurumu, 2022b, s.489).

Aynı şekilde, KVKK'nin 5. maddesinin ikinci fıkrasının (ç) bendinde düzenlenen, *"Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması"* hâli elektronik sözleşmeler için önemli bir kişisel veri işleme gerekçesi oluşturmaktadır. Zira, elektronik sözleşmeden kaynaklanan bir davada hâkim kararıyla e-ticaret hizmet sağlayıcısından kişisel veri içeren elektronik sözleşme örneğinin talep edilmesi ve bunun mahkemeye ibraz edilmesi durumunda, veri sorumlusu

konumundaki e-ticaret hizmet sağlayıcısının bu veri işleme şartı kapsamında kişisel verileri aktardığı söylenebilecektir.

Yine, elektronik sözleşmeler kapsamında KVKK'nin 5. maddesinin ikinci fıkrasının (e) bendinde düzenlenen, *"Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması"* şartının da gündeme gelmesi söz konusu olabilecektir. Örneğin, internet üzerinden akdedilmiş bir satış sözleşmesine ilişkin faturanın saklanması ve gerekli olduğu anda kullanılması bu kişisel veri işleme şartına dayandırılabilecektir. Aynı doğrultuda, e-sözleşmenin sona ermesini takiben, muhtemel kanunî takip veya davalar nedeniyle zamanaşımı süresinin bitimine kadar fatura, sözleşme, kefaletname gibi belgelerin bu amaçlar için muhafaza edilmesi söz konusu kişisel veri işleme şartı kapsamında değerlendirilmektedir.

Öte yandan, ABAD'ın 2019 tarihli *"Planet49 Kararı"* açık rızanın alınma şekline ilişkin olarak önemli tespitler içermektedir (Kuntoğlu, 2021, s.190):

> *"İlgili kişi internet sitesinde aydınlatma metnini açtığı zaman kişisel verilerin işlenmesine dair seçenek kutucukları hazır işaretlenmiş geliyorsa burada açık rızadan bahsedilemeyecektir. Açıklanan rıza "her türlü veri işleme faaliyetine" ya da "her türlü ticari işleme ilişkin" veya bu ifadelere benzer şekilde konu sınırlandırması yapılmadan verilmiş ise, "battaniye rıza" söz konusu olacaktır. Battaniye rıza açık rıza olarak kabul edilmeyecektir. Avrupa Birliği'nde bu tür rıza metinleri geçerli görülmemektedir."*

VERİ SORUMLUSUNUN TESPİTİ

Bilindiği gibi, KVKK'nın 3'üncü maddesinde *"veri sorumlusu",* kişisel verilerin işleme vasıtalarını ve amaçlarını belirlemekle yetkili; veri kayıt sisteminin yönetiminden ve kurulumundan sorumlu tüzel veya gerçek kişiler olarak tanımlanmaktadır. Bu çerçevede, e-ticaret sektörünün öznesi olan *"hizmet sağlayıcılar"* ve *"aracı hizmet sağlayıcılar"* somut olaya göre veri sorumlusu sıfatına sahip olabileceklerdir.

Öte yandan kişisel veri işleme faaliyetlerinde veri sorumlusu her zaman kolayca tespit edilemeyebilir. Özellikle elektronik ortamda toplanan kişisel veriler bakımından bu zorluklar gündeme gelebilmektedir. Örneğin, bir e-ticaret platformunda veri sorumlusunun tespiti kolay görünmektedir. Burada platformun işleticisi veri sorumlusu olarak kabul edilmektedir. ETDHK'de *"aracı hizmet sağlayıcı",* elektronik ticaret faaliyeti gerçekleştiren tüzel veya gerçek kişiler, 3. kişilere ait ticari ve iktisadi faaliyetlerin gerçekleşmesinde uygun elektronik ortamı sağlayan tüzel veya gerçek kişiler olarak tanımlanmıştır. E-ticaret platformu ilgili kişiye doğrudan mal veya hizmet sunuyor ve bu kapsamda aralarında elektronik sözleşme kuruluyorsa, "hizmet sağlayıcı" olarak veri sorumlusu olacaktır. Fakat, e-ticaret platformu ilgili kişiye doğrudan mal veya hizmet sunmuyor, bunun yerine elektronik ortamda başka işletmelere mal veya hizmet sunma imkânı veriyorsa "aracı hizmet sağlayıcı" olarak veri sorumlusu olacaktır. Bu son durumda, ilgili kişiye mal veya hizmeti sunan "hizmet sağlayıcı" da aynı zamanda veri sorumlusu olacaktır. Dolayısıyla her somut olayda veri sorumlusunun tespiti gerekmekte olup ilişkili veri işleme faaliyetinde bir veya daha fazla veri sorumlusu ya da ortak veri sorumlusu bulunması ihtimali de vardır. Elektronik sözleşmeler bakımından ise veri sorumlusunun tespiti nispeten daha kolaydır. Zira e-sözleşmelerde sözleşmenin tarafları belirli olduğundan, kanuni tanıma göre kimin veri sorumlusu olduğu daha kolay tespit edilebilecektir.

Burada 95/46/AT sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GVKT) ile KVKK arasındaki bir farka da dikkate çekmek gerekmektedir. KVKK'da "veri sorumlusu" bir kişi olarak tanımlanmakta iken, AB Veri Koruma Direktifi ve GVKT'de ise birlikte veri sorumlusuna dikkat çekilmiştir (Memiş, 2017, s.12-13).

Uygulamada veri sorumlusuna birkaç örnek verilecek olursa;

> *"Yer, konum, fotoğraf vb. çok sayıda kişisel veriye erişim hakkı uygulama geliştiricileri tarafından toplanmaktadır. Bu durumda, söz konusu uygulama sunucularının veri sorumlusu olduğundan şüphe edilmemelidir. Bulut sunucuları için geliştirilen uygulamalar için aynı değerlendirme yapılmalıdır."* (Memiş, 2017, s.12-13).

> *"Bir işletmenin şubelerinin veri sorumlusu olması mümkün değildir. Zira şubelerin bağımsızlığı ve tüzel kişiliği bulunmamaktadır. Buna karşın bir holding yapılanması içinde yavru şirketlerin bağımsızlığı söz konusudur. Bu nedenle bir holding yapılanması içinde elde edilen veriler bakımından diğer bağlı-yavru şirketler üçüncü kişi olarak kabul edilir ve holding yapılanmasından ayrı birer veri sorumlusu olurlar."* (Memiş, 2017, s.12).

> *"İnternet üzerinden satış gerçekleştiren bir e-ticaret platformunun bir ödeme hizmeti şirketi ile anlaşması ve müşterilerinin verilerinin bu şekilde işlenmesi durumunda; ödeme hizmeti şirketi, e-ticaret platformunun veri işleyeni olmamaktadır. Ödeme hizmeti şirketi, bu verilerin işlenmesi bakımından veri sorumlusu statüsündedir. Zira ödeme hizmeti şirketi; toplanan verilerin hangi*

amaçla kullanılacağı konusunda kontrol sahibi olup, ödemelerin doğru yapılabilmesi için müşterilerden hangi verilerin toplanması gerektiğine karar vermekte; e-ticaret platformundan bağımsız olarak doğrudan kişisel verileri işlenen müşterilere uyguladığı kendi hüküm ve şartları bulunmakta; e-ticaret platformundan bağımsız olarak kendi tabi olduğu hukuki yükümlülükleri bulunmaktadır. Örneğin; kredi kartı bilgilerinin silinmesi gibi." (Kişisel Verileri Koruma Kurumu, 2019b, s.59)

VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

Aydınlatma Yükümlülüğü

Kişisel veri işleme faaliyetlerinde aydınlatma yükümlülüğü esas olarak, 6698 sayılı KVKK kapsamında düzenlenmiş bulunmaktadır. Öte yandan, 6563 sayılı ETDHK'de da aracı hizmet sağlayıcıların ve hizmet sağlayıcıların alıcılara karşı bilgi verme yükümlülüğü kapsamında detaylı bir düzenleme yer almaktadır.

Bu düzenlemeler arasında benzer hükümler yer alsa da KVKK ile ETDHK arasında farklı hukuk alanlarını düzenlemeleri sebebiyle genel kanun-özel kanun ilişkisi bulunmadığından, her iki düzenlemeye de ayrı ayrı uyulması gerekmekte olup, ETDHK kapsamında bilgi verme yükümlülüğünün yerine getirilmesi doğrudan KVKK kapsamında aydınlatma yükümlülüğünün yerine getirildiği anlamını taşımamaktadır. Dolayısıyla, birbirleriyle iç içe geçen yönleri bulunsa da her iki düzenleme müstakil özel alanlarında kendi sistematikleriyle uygulanmaya devam edilmeli ve kendi alanlarına ilişkin beraber uygulanmalıdır (Kaya, 2020, s.159).

KVKK Kapsamında Aydınlatma Yükümlülüğü

Şüphesiz, ilgili kişinin işleme faaliyetlerine dair denetimini ve kişisel verilerinin üzerindeki kontrolünü artırmanın en önemli aşaması işleme faaliyeti ile olarak ilgili kişiyi bilgilendirmektir. Bu kapsamda kanun koyucu, veri sorumlusunu verileri topladığı sırada ilgili kişileri bilgilendirmek ile yükümlü tutmuştur (Kaya ve Tolun, 2020, s.110).

KVKK'nın 10'uncu maddesinde düzenlenen aydınlatma yükümlülüğü kapsamında veri sorumlusunun, kişisel verilerin elde edilmesi sırasında yetkilendirdiği kişi veya bizzat aracılığıyla kişisel verilerin hangi amaçla işleneceğine, veri sorumlusunun ve varsa temsilcisinin kimliğine, kişisel veri toplamanın yöntemi ve hukuki sebeplerine, kişisel verilerin kimlere ve hangi amaçla aktarılabileceğine, ilgili kişinin Madde 11 kapsamındaki haklarına yönelik verisi işlenen kişilere bilgi

vermesi gerekmektedir (Kişisel Verileri Koruma Kurumu, 2019a, s.10).
Aydınlatma ilgili kişinin talebi üzerine yerine getirilen bir yükümlülük değildir. *"Açık rıza"* veya diğer veri işleme şartlarından farklı bir şekilde en geç verinin işlendiği sırada yerine getirilmesi gereken bir yükümlülüktür. Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı da veri sorumlusuna aittir. Ayrıca aydınlatma yükümlülüğü 6698 sayılı Kanun'un 4'üncü maddesindeki genel ilkeler göz önünde bulundurularak yerine getirilmelidir (Kişisel Verileri Koruma Kurumu, 2019c, s.9).

Diğer taraftan, veri sorumlusunun aydınlatma yükümlülüğünü yerine getirirken Resmî Gazete'nin 30356 sayılı 10.03.2018 tarihli nüshası ile yürürlüğe giren *"Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"* ile belirlenen usul ve esaslara uyması gerekmektedir. Tebliğ'e göre aydınlatma yükümlülüğü yazılı ya da sözlü olarak yerine getirilebilmektedir. Bununla beraber, aydınlatma yükümlülüğünün yerine getirildiğine dair ispatın veri sorumlusunca yapılması gerektiği düşünüldüğünde, sözlü olarak yerine getirilen aydınlatmanın ispat edilebilir olması da veri sorumlusunun göz önünde bulundurması gereken bir husustur.

Veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmemesi hâlinde, KVKK'nın "Kabahatler" başlıklı 18'inci maddesi çerçevesinde Kurul tarafından verilecek idari para cezasına muhatap olması ihtimali gündeme gelecektir.

ETDHK Kapsamında Bilgi Verme Yükümlülüğü

ETDHK'nin 3'üncü maddesinde sözleşmenin kurulma aşamasından önce alıcı gruba yapılması gereken bilgilendirmeye ilişkin hizmet sağlayıcılara yönelik düzenleme getirilmiş; ayrıca *"Elektronik Ticarette Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcıları Hakkında Yönetmelik"*in 5'inci maddesinde de bu yükümlülükler ayrıntılı şekilde düzenlenmiştir. İlgili kişilerin sözleşme konusu hizmet veya mal hakkındaki güncel bilgileri, sözleşmenin kurulması için paylaşılan kişisel verilerinin nasıl korunacağı ve gerekli olan teknik adımlar vb. hususlarda alıcının sözleşme yapma konusunda daha bilinçli hareket etmesini ve sözleşme yapılmadan önce bilgilendirilmesini sağlamaktadır (Hamamcıoğlu, 2018, s.56).

ETDHK kapsamındaki bilgi verme yükümlülüğünün gerçekleştirilebilmiş sayılabilmesi Kanunda ve Yönetmelikte sayılan verilerin alıcılara ulaştırılması gereklidir. Bahis olunan yükümlülükler, öncelikle hizmet sağlayıcılar için öngörülmüş olmakla birlikte; eğer hizmet sağlayıcı aracı hizmet sağlayıcısının sunduğu imkânla e-ticaret faaliyetini sürdürüyorsa, aracı hizmet sağlayıcılar için de geçerli

olacaktır (Hamamcıoğlu, 2018, s.57). Buna göre; hizmet sağlayıcı, elektronik iletişim araçlarıyla bir sözleşmenin kurulmasından önce aşağıda sayılan yükümlülükleri yerine getirmelidir (Hamamcıoğlu, 2018, s.57-58):

> *"İlgili kişilerin kolayca ulaşabileceği şekilde ve güncel olarak tanıtıcı bilgilerini sunmalıdır. Kanunda açıkça e-posta veya diğer iletişim imkânlarına yer verilmesinden bahsedilmemektedir. Bu konudaki eksiklik Yönetmelik ile tamamlanmıştır. Yönetmelik'in 5. maddesinin birinci fıkrasında, tebligata elverişli KEP adresi, e-posta adresi ve telefon numarası ile varsa işletme adı veya tescilli marka adına ilişkin bilgilerin e-ticaret faaliyetine başlanmadan önce eksiksiz olarak hazır bulundurulması gereği düzenlenmiştir.*
>
> *Sözleşmenin kurulabilmesi için izlenecek teknik adımlara ilişkin bilgileri sunmalıdır. Sözleşme metninin sözleşmenin kurulmasından sonra hizmet sağlayıcı tarafından saklanıp saklanmayacağı ile bu sözleşmeye alıcının daha sonra erişiminin mümkün olup olmayacağı ve bu erişimin ne kadar süreyle sağlanacağına ilişkin bilgileri sunmalıdır.*
>
> *Veri girişindeki hataların açık ve anlaşılır bir şekilde belirlenmesine ve düzeltilmesine ilişkin teknik araçlara ilişkin bilgileri sunmalıdır. Uygulanan gizlilik kuralları ve varsa alternatif uyuşmazlık çözüm mekanizmalarına ilişkin bilgileri sunmakla yükümlüdür.*
>
> *Hizmet sağlayıcı, varsa mensubu olduğu meslek odası ile meslekle ilgili davranış kurallarını ve bunlara elektronik olarak ne şekilde ulaşılabileceğini belirtmekle yükümlüdür. Yönetmelik'in 5. maddesinin birinci fıkrasında, hizmet sağlayıcının üyesi olduğu sektörel kuruluşlar hakkında da bilgi vermesi gerektiği düzenlenerek maddenin daha geniş yorumlandığı görülmektedir.*
>
> *Hizmet sağlayıcı ayrıca sözleşme hükümlerinin ve genel işlem şartlarının alıcı konumdaki ilgili kişi tarafından saklanmasına da imkân sağlamakla yükümlüdür. E-ticarette elektronik ortamda kurulan sözleşme metnine alıcıların erişebilmesi, sözleşmeden kaynaklı hak ve yükümlülüklerin belirlenmesi ve çıkacak herhangi bir uyuşmazlık durumunda metnin yetkili mercilere sunulabilmesi noktasında önem arz etmektedir."*

ETDHK'nin 3'üncü maddesinin üçüncü fıkrasında ise aracı hizmet sağlayıcıların ve hizmet sağlayıcıların bilgi verme yükümlülüğünün istisnaları düzenlenmiştir. Bu bağlamda, tarafların tüketici olmadığı durumlarda söz konusu yükümlülüklerin aksinin kararlaştırılabilmesi mümkün bulunmaktadır. Fakat, taraflar bu

hususta anlaşsalar dahi, veri girişindeki hataların tespit edilmesine ve tashih edilmesine dair teknik araçlara ilişkin bilgi verilmesi hususunda ETDHK'nin 3'üncü maddesinin 1'inci fıkrasının (ç) bendi dürüstlük kuralından kaynaklanan bir gereklilik olarak varlığını sürdürür (Demirbaş, 2015, s.42). Dolayısıyla hizmet sağlayıcının genel işlem şartlarının ve sözleşme metninin ilgili kişi tarafından saklanmasına olanak sağlamasına yönelik yükümlülüğü burada da devam etmektedir (Hamamcıoğlu, 2018, s.57-58).

ETDHK'nin 3'üncü maddesinin beşinci fıkrasında ise münhasıran e-posta vb. iletişim araçları vasıtasıyla kurulan sözleşmelerde aynı hükümlerin uygulanma alanı bulmayacağı düzenlenmiştir. Bu iletişim araçları kullanılarak yapılmış olan sözleşmelerde taraflar arasında müzakere etme ve doğrudan haberleşme olanağının yaratılması için böyle bir istisna oluşturulduğu düşünülmektedir (Demirbaş, 2015, s.43-44).

Veri Güvenliğini Sağlama Yükümlülüğü

KVKK'nın 12/1 maddesine göre; *"(1) Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır."* Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, bu tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

Veri sorumlusunun anılan maddede sayılan yükümlülüklere uymaması halinde, Kanun'un "Kabahatler" başlıklı 18'inci maddesi çerçevesinde Kurul tarafından verilecek idari para cezasına muhatap olması ihtimali gündeme gelecektir.

Bu kapsamda veri sorumlusu çalışanlarının iyi niyet gözetmeyen davranışlar sergileme olasılığı dikkate alınmalı, çalışanlar seçilirken azami özen gösterilmeli, çalışanların gerekli eğitimleri almaları sağlamalı ve iç işleyişle rutin denetimlerin yapılmalıdır. Bütün veri sorumluları elde edilen verilerin hukuka aykırı işlenmesinden sorumludur öyle ki söz konusu verilere hukuka aykırı erişimin önlenmesi ve bu verilerin güvenli bir şekilde depolanmasını sağlamakla mükelleftir. Bunun yanı sıra verilerin depolanmasında hem idari hem teknik yönden her türlü tedbir veri sorumluları tarafından alınmalıdır. Kişisel veri işleme faaliyeti veri sorumlusu tarafından 3. bir kişiye devredilmişse yasal düzenlemeye göre veri sorumlusu, veriyi işleyen 3. kişi ile ortak sorumluluk üstlenecektir (Kuntoğlu, 2021, s.194).

ETDHK'nin 10'nuncu maddesi bakımından ise hizmet sağlayıcılar ve aracı hizmet sağlayıcılara *"6563 sayılı Kanun çerçevesinde yapmış oldukları işlemler vasıtasıyla elde ettikleri kişisel verileri güvenle saklamak yükümlülüğü"* getirilmiştir. Kişisel verileri ilgili kişinin onayı olmadan üçüncü kişilere iletmeleri ve başka amaçla kullanmaları ise yasaklanmıştır (Hamamcıoğlu, 2018, s.68). Öğretide,

> *"Hizmet sağlayıcı ve aracı hizmet sağlayıcıların kişisel verilerini koruma ve saklama yükümü altında olduğu kişilerin yalnızca alıcılarla sınırlı olarak anlaşılmaması gerektiği belirtilmiş ve hükmün lafiz ve amacından da hareketle e-ticaret faaliyeti nedeniyle internet sitelerine girişi yapılan tüm kişisel verilerin de bu kapsamda koruma altında olması gerektiği; bu bakımdan kişisel verilerinin korunması gereken kişi ile hizmet sağlayıcı arasında mutlaka bir sözleşmenin varlığının da aranmayacağı (...)"* ifade edilmiştir (Demirbaş, 2015, s.64).

Veri sorumlusunun genel itibariyle şu tedbirleri aldığını ispat etmesi gerektiği değerlendirilmektedir (Memiş, 2017, s.19-20):

> *"Yetkisiz kişilerin bilişim/veri sistem odasına girişinin engellenmesi, yetkisiz kişilerin sisteme erişiminin engellenmesi,*
> *Yetkili kimselerin sisteme erişiminde dahi bunların yetkisiz olarak kop-yalanması, değiştirilmesi, çoğaltılması ve silinmesinin engellenmesi,*
> *Kişisel verilerin naklinde yetkisiz kimselerin erişiminin engellenmesi, hangi yerlerden kişisel verilere erişimin yapıldığının kontrolü ve tespiti,*
> *Sonradan veri girişlerinin kontrol edilmesi,*
> *Veri sahibinin talepleri doğrultusunda söz konusu verilerin talebe uygun işlenip işlenmediğinin kontrolü,*
> *Kişisel verilerin ani kaybı ve zarar görmelerine karşı önlemlerin alınması,*
> *Farklı amaçlarla elde edilmiş verilerin ayrılarak işlenmesi."*

Veri sorumlusunun çevrimiçi bir hizmetle verilen topladığı hallerde ise bu tedbirlere ilave olarak, ilgili kişiye veri işlemeyi derhâl durdurabilme yetkisi, sürekli saldırılara karşı korunma hakkı sağlanması gibi birçok tedbirin alınması gerekecektir (Memiş, 2017, s.19-20).

SONUÇ

Bilişim teknolojileri ve özellikle internetin gelişimi, toplumun iletişimsel, etik ve ahlaki değer yargılarında olduğu kadar ticarete bakış açılarında da belirleyici bir rol üstlenmiş, bu anlamda toplumsal gelişim ve dönüşümde son derece etkili olmuştur. Söz konusu gelişim ve dönüşümün getirisi olarak, geleneksel ticaretten daha farklı bir yapıya sahip olan "e-ticaret" insan hayatına girmiştir. 1970'lerde ortaya çıkan e-ticaret, önceleri teknik altyapının maliyet yüksekliğinden ötürü büyük işletmeler bünyesinde sınırlı kalmıştır. Bugünlerde ise internete kolaylıkla erişebilme imkânı neticesinde herkesin bir e-ticaret ilişkisinin tarafı olması mümkündür.

E-ticaret, firmalara internet üzerinden az miktardaki bütçeyle uluslararası boyutta iş yapma imkânı sağlamaktadır. Bu durum da küçük ve orta ölçekli işletmelere rekabet edebilme olanağı sunmaktadır. Benzer şekilde, alıcılar da e-sözleşmeler sayesinde minimum düzeyde para ve çaba harcamak suretiyle satış görevlisi etkisi olmaksızın bulunduğu yerden ayrılmadan alışveriş yapabilmekte ve gerektiğinde coğrafi sınırları aşarak ihtiyaçlarını karşılayabilmektedir.

Kurulmasında kullanılan iletişim aracının özelliklerine göre e-sözleşmeler hazırlar arası veyahut hazır olmayanlar arası şeklinde sınıflandırılabilmektedir. Diğer yandan, çok sayıda sözleşmenin hızlı şekilde kurulabilmesi ve ifa edilebilmesini teminen önceden hazırlanan sözleşme şartlarının sadece kabulü ile kurulmasından ötürü e-sözleşmeler iltihakî sözleşme niteliğinde olabilmektedir. Bunların yanında, e-sözleşmeler *"mesafeli sözleşme"* olarak da kurulabilmektedir. Dolayısıyla, tarafların aynı anda fiziksel olarak bir araya gelmeksizin ürün veya hizmetlerin mesafeli satış sistemi vasıtasıyla uzaktan iletişim araçlarıyla sözleşme kurması durumunda mesafeli sözleşme gündeme gelecektir.

Son dönemlerde hızla gelişen elektronik ticaret sektörünün, Covid-19 salgınıyla da beraber kişilerin ihtiyaçlarını online platformlardan sağlama eğilimlerinin artmasıyla daha kişiselleştirilmiş ürünler sunabilmek adına kişilerin tüketim alışkanlıklarını analiz ederek "profilleme" yaptığı ve sadece bu yönden bile kişisel verilerin korunması hakkının daha da önemli hale geldiği de tartışmasızdır. E-ticaret işlemleri neticesinde büyük ölçekte kişisel veri kaydı yapılmaktadır. E-ticaret sektöründe veri işleme faaliyetinde bulunan şirketler, işlemiş oldukları kişisel veriler üzerinde kullanıcı profilleri dâhil istatistikî değerlendirmelerde bulunarak ve bu verilerin aktarıldığı ve depolandığı büyük veri havuzundaki (kullanıcı eğilimleri, alışkanlıkları vb.) verileri analiz ederek iktisadi politikalar yürütülmektedir.

Kamu hizmetlerinin efektif sunumu, sosyal ve ekonomik hayatın devamlılığı, mal ya da hizmetlerin iktisadî ihtiyaçlara göre geliştirilmesi, dağıtılması ve pazarlanması için kişisel verilerin toplanmasının kaçınılmaz olduğu düşünülmekle birlikte, kişisel verilerin gelişigüzel ve sınırsız şekilde toplanmasının, yetkisiz kişilerin erişimine açılmasının, ifşası, amaç dışı ya da kötüye kullanımı sonucu kişisel hakların ihlal edilmesinin engellenmesi elzemdir. Bu bakımdan, ülkemizdeki mevzuat çalışmalarının geç başlamış olmasına rağmen kişisel verilerin korunması alanında son yıllarda hızlı bir ilerleme kaydedildiğini söylemek mümkündür.

Bununla birlikte, sözleşmenin zayıf tarafı olan ve KVKK kapsamında "ilgili kişi" sıfatını taşıyan gerçek kişi tüketicilerin elektronik sözleşmeler ile işlenen kişisel verileri bakımından bilinç ve farkındalık düzeyinin yükseltilmesi bir ihtiyaçtır. Daha önce de bahsedildiği üzere, elektronik sözleşmelerin çoğu iltihakî nitelikte olup genel işlem şartları içermektedir.

Bu nedenle ilgili kişiler çoğu zaman sözleşme şartlarını müzakere etme şansına sahip olamamakta ve sırf sözleşmeyi kurabilmek adına sözleşmenin kurulması için gerekli olmadığı halde kendisinden talep edilen kişisel veri niteliğindeki bilgileri elektronik sözleşmenin diğer tarafi ve KVKK kapsamında "veri sorumlusu" sıfatını haiz kişilere vermektedirler. Bu noktada, veri sorumlularının KVKK hükümlerine uyum sağlamalarının büyük önem arz ettiğinin ve KVKK düzenlemelerine aykırılık teşkil eden durumlar bakımından Kanun'un 18. maddesi ile düzenlenen idari yaptırımlara muhatap olduklarının altının bir kez daha çizilmesi yerinde olacaktır.

Kişisel verilerin hukuka uygun işlendiğinden bahsetmek için ise *"işlemenin veri işleme şartlarına dayanması, aydınlatmanın gerçekleşmiş olması, genel ilkelere uygun olması"* şartlarının tamamının birlikte sağlanması gerekmektedir. Veri sorumlusunun aydınlatma yükümlülüğü esas olarak, KVKK kapsamında düzenlenmiş bulunmaktadır. Öte yandan, ETDHK kapsamında da hizmet sağlayıcı ve aracı hizmet sağlayıcıların alıcılara karşı bilgi verme yükümlülüğü kapsamında detaylı bir düzenleme yer almaktadır. Bu düzenlemeler arasında benzer hükümler yer alsa da KVKK ile ETDHK arasında farklı hukuk alanlarını düzenlemeleri sebebiyle genel kanun-özel kanun ilişkisi bulunmadığından, birbirleriyle iç içe geçen yönleri bulunsa da her iki düzenleme müstakil özel alanlarında kendi sistematikleriyle uygulanmaya devam edilmeli ve kendi alanlarına ilişkin beraber uygulanmalıdır.

E-ticaretin en önemli olumsuz yanı ise, güvenlik zafiyetinin bulunması riskidir. Tüketicilerin genellikle ödemelerini internet üzerinden kredi kartıyla yapması, kişisel bilgilere hukuka aykırı şekilde erişilerek dolandırıcılık riskini doğurmaktadır. Bu nedenle veri sorumlusunun veri güvenliğine ilişkin yükümlülüklerini yerine getirmesi yüksek önem arz etmektedir.

Netice olarak, e-ticaret ve elektronik ortamda akdedilen sözleşmeler bakımından ilgili kişilerin kişisel verilerinin korunması hususundaki farkındalıklarının artırılması gerektiği değerlendirilmektedir. Ayrıca veri sorumlusu sıfatını haiz hizmet sağlayıcı ve aracı hizmet sağlayıcıların bu hususdaki yükümlülüklerinin daha somut şekilde tespit edilmesi, bahis olunan yükümlülüklerin yerine getirilip getirilmediğini denetleyecek mekanizmaların meydana getirilerek bu mekanizmaların daha işlevsel hale getirilmesi kişisel verilerin korunması konusunda göz önünde bulundurulması şart olan bir gerekliliktir. ◆

KAYNAKÇA

- Kılıçoğlu A. M. (2012). *Borçlar Hukuku- Genel Hükümler,* Ankara: Turhan Kitabevi (16. bs.), Ankara.
- Bayram, A. E. (2015). Güncel Gelişmeler Işığında Elektronik Sözleşmelerin Kurulması, Türkiye Barolar Birliği Dergisi. 28(119), 331- 366
- Hamamcıoğlu, E. (2018). Elektronik Ticaretin Hukuksal Boyutu, *Kocaeli Üniversitesi Sosyal Bilimler Dergisi.* 35, 43-72
- Wang, F. F. (2014) *Law of Electronic Commercial Transactions Contemporary Issues in the EU,* US and China, Second Edition, Routledge, London.
- Turan G. (2008). *Elektronik Sözleşmeler* ve Elektronik Sözleşmelere Uygulanacak Hukukun Tespiti, TBB Dergisi, 21(77), 87-119.
- Demirbaş, H. (2015). 6563 *Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Kapsamında Hizmet Sağlayıcıları ve Aracı Hizmet Sağlayıcılarının Yükümlülükleri.* Ankara: Seçkin Yayıncılık.
- Kocasakal Özdemir, H. (2003). *Elektronik Sözleşmeden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti,* İstanbul: Vedat Kitapçılık.
- Sağlam Atabarut, İ. (2003). Elektronik Sözleşmeler (Doktora Tezi). Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Kaya, İ. S ve Tolun, Y. (2020). *Uygulayıcılar İçin Türkiye'de ve Avrupa'da Kişisel Verilerin İşlenmesi KVKK-GDPR Karşılaştırması,* Ankara: Adalet Yayınevi (1. bs.).
- Arslan İ. K. ve Öz N. (2020). Elektronik Ticaret Sözleşmelerine Uygulanacak Hukuk, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 19(38), 13-31.
- Kaya, M. B. (2020). Elektronik Ticaret Hukuku – Ticari Elektronik İletiler, İstanbul: On İki Levha Yayıncılık (2 bs.).
- Kişisel Verileri Koruma Kurumu. (2019a). 6698 Sayılı Kanunda Yer Alan Terimler. https://www.kvkk.gov.tr/Icerik/5383/Diger-Dokumanlar, e.t: 18.09.2023.

- Kişisel Verileri Koruma Kurumu. (2019b). Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf, e.t. 14.11.2021.
- Kişisel Verileri Koruma Kurumu. (2019c). Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, https://www.kvkk.gov.tr/Icerik/2030/Rehberler, e.t. 18.09.2023
- Kişisel Verileri Koruma Kurumu. (2022a), Çerez Uygulamaları Hakkında Rehber, https://www.kvkk.gov.tr/Icerik/2030/Rehberler, e.t. 18.09.2023
- Kişisel Verileri Koruma Kurumu. (2022b) Yayımlanmış Kişisel Verileri Koruma Kurul Kararları 2018-2021, https://www.kvkk.gov.tr/Icerik/5383/Diger-Dokumanlar, e.t. 18.09.2023
- Keser L. (2016, Kasım 22). *Kişisel Veriler Kanunu'nun Getirdikleri* [Video]. https://www.youtube.com/watch?v=yyMUPZSXtoY, e.t. 09.06.2022.
- Tekin M. (2017). Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", *Beykent Üniversitesi Hukuk Fakültesi Dergisi,* 3(6), 9-23.
- Oğuz, H. (2013). Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum. *Uyuşmazlık Mahkemesi Dergisi,* 1(3), 1-38.
- Kuntoğlu Ö. F. (2021). Elektronik Ticarette Kişisel Verilerin Korunması. *Ankara Sosyal Bilimler Üniversitesi Bilişim Hukuku Dergisi.* 3(1). 176-229
- Oğuz S. (2018). Kişisel Verilerin Korunması Hukukunun Genel İlkeleri. *Bilgi Ekonomisi ve Yönetimi Dergisi.* 13(2), 121-138.
- Önder Balaman, S. (2017). Yabancı Unsurlu Elektronik Tüketici Sözleşmelerinin MÖHUK Kapsamında İncelenmesi. *Kesit Akademi Dergisi.* Sayı 9, 285-312. DOI: 10.18020/kesit.1196
- Önder Balaman, S. (2016). Milletlerarası Özel Hukukta Elektronik Sözleşmeler (Yüksek Lisans Tezi). Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta.

◊ The Court of Justice of The European Union. (2016). "Judgment of 19 October 2016, Breyer, C-582/14, EU: C: 2016: 779", http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2725971), e.t. 09.06.2022.

ÇEREZLER VE 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA UYGULANMASI

Yeliz YILMAZ

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "Çerezler Vasıtasıyla Kişisel Verilerin İşlenmesi (Hukuki Bakış)" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Çerezler, rakam ve harflerden oluşan, kullanıcının terminal ekipmanına bırakılan bir tür metin dosyasıdır. Kullanıcının internet sitesine bir daha girip girmediğini kontrol etmek olan ilk kullanım amacı dışına çıkılarak kullanıcıların daha fazla bilgisinin alınması yönünde kullanılmaya başlanmıştır. Özelikle çevrimiçi davranışsal reklamcılık faaliyetleri kapsamında, kişiye özel reklam içeriği sunulması hususunda çerezlerden oldukça faydalanıldığı aşikârdır. Bu durumda çerezin her ne kadar rakam ve harften oluştuğu belirtilse de belirli koşullar altında kişisel veri niteliği olduğunun kabulü kaçınılmaz hale gelmektedir (La Agencia Española de Protección de Datos (AEPD), 2021, s.13).

Türk Hukukunda çerezler aracılığıyla kişisel verilerin işlenmesi faaliyetlerinin tümüne yönelik doğrudan uygulanacak bir düzenleme bulunmamakta olup, çerezler aracılığıyla kişisel verilerin işlenmesi hususuna ilişkin bir hüküm 6698 sayılı Kişisel Verilerin Korunması Kanununda da yer almamaktadır. Bu durum çerezler aracılığıyla kişisel verilerin işlenmesi durumunda hangi kuralların uygulanacağı sorusunu gündeme getirmekte ve belirsizlik yaratmaktadır (Aksoy ve Halıcıoğlu, 2021, s.62).

Bu çalışmada Türk Hukukunda çerezler yoluyla kişisel verilerin işlenebileceği haller ve bu hususta hukuki düzenleme yapılmasının gerekli olup olmadığı üzerinde durulacaktır. Ayrıca çerezlere ilişkin Avrupa Birliği mevzuatında mevcut olan düzenlemelere de değinilecektir.

ÇEREZLER HAKKINDA GENEL BİLGİLER

Çerez Nedir?

Çerez, bir ağ sağlayıcısı tarafından kullanıcı bilgisayarında depolanan kısa bir alfasayısal metindir (Carey, 2018, s.198; Herberger, 2013, s.3; Article 29 Data Protection Working Party, 2/2010, s.6; Doğan ve Bozkurt, 2010; IAB Türkiye, 2019) ve HTTP (Hiber Metin Transferi Protokolü) talebinin bir parçası olarak aktarılır (Keser Berber, 2014, s.XVIII). Http, internet sitelerine bağlanmayı sağlayan bir anahtardır (Mediaclick Http Nedir?, (t.y.), Ayvaz (Ed.)). Diğer bir deyişle, çerezler, normalde yalnızca harflerden ve rakamlardan oluşan ve kullanıcılar tarafından ziyaret edildiğinde çevrimiçi hizmetlerin sağladığı küçük bilgi parçalarıdır. Kullanıcının cihazındaki yazılım (örneğin bir web tarayıcısı) çerezleri saklayabilir ve bir sonraki ziyaretlerinde bunları internet sitesine geri gönderebilir (Information Commissioner's Office (ICO), 2019, s.5).

Bu metin dosyasına "çerez" isminin verilmesinin nedeni bilişim dünyasında bilinen "magic cookie"den (sihirli çerezler) esinlenilmesidir (Turan, 2020, Keser Berber ve Bilgili (Yay. haz.), s.130).

ÇEREZ ÇEŞİTLERİ

Çerezlere ilişkin birçok ayrım yapılsa da uygulamada daha çok sürelerine göre, amaçlarına göre ve taraflarına göre olmak üzere üç ana başlıkta (Cookies, the GDPR, and the ePrivacy Directive, (t.y.); Doğan ve Bozkurt, 2010) sınıflandırmaya tabi tutulmaktadır.

Sürelerine Göre Çerezler

Oturum Çerezleri

Oturum çerezleri, kullanıcı seçimleri ve dolaşma durumlarını saklayan ve oturum süresince tutulan çerezlerdendir. Kullanıcının bir hizmete giriş yapmasıyla yüklenip sistemden çıkış yapmasıyla da (veya tarayıcı kapatılması halinde) silinen çerez çeşididir (Carey, 2018, s.199; Article 29 Data Protection Working Party, 04/2012, s.4; Keser Berber, 2014, s..XVIII).

Oturum çerezleri, internet sitelerinin bir tarama oturumu boyunca bir kullanıcının eylemlerini tanımasına ve bağlantı kurmasına izin vermektedir. Oturum süresi sona erdikten sonra saklanmadığı için, oturum çerezleri bazen kalıcı çerezlere kıyasla mahremiyete daha az müdahaleci olarak kabul edilebilmektedir (ICO, 2019, s.5).

Kalıcı Çerezler

Özellikle silinmediği ya da tanımlanan süreleri dolmadığı sürece tarayıcıda mevcut olarak bulunmaya devam eden çerez türüdür (Keser Berber, 2014, s.XVIII; Zorer, 2019). Kalıcı çerezler, kullanıcının bir sitedeki (veya farklı internet sitelerindeki) tercihlerinin veya eylemlerinin hatırlanmasını sağlayabilmekte olup, kullanıcıların bir siteyi kullanırken tercihlerini ve seçimlerini hatırlamak veya hedefli reklamcılık gibi çeşitli amaçlar için kullanılabilmektedir. Ayrıca, kullanıcılar önceden yerleştirilmiş kalıcı çerezleri manuel olarak silebilecek veya tarayıcı ayarlarını çerezleri belirli bir aralıkta silmek için ayarlayabilecektir (ICO, 2019, s.6).

Taraflarına Göre Çerezler

Bir çerezin birinci veya üçüncü taraf olup olmadığı, çerezi yerleştiren internet sitesi veya domain (alan)'e göre farklılık arz etmektedir (ICO, 2019, s.6).

Birinci Taraf Çerezler

Birinci taraf çerezler doğrudan ziyaret edilen internet sitesi tarafından yani tarayıcının adres çubuğunda görüntülenen URL tarafından yerleştirilmektedir.

Üçüncü Taraf Çerezler

Üçüncü taraf çerezler, kullanıcının ziyaret ettiği internet sitesinden (veya domain) farklı bir üçüncü kişi tarafından yerleştirilmektedir. Bu durum genellikle, internet sitesi diğer sitelerden resim, sosyal medya eklentileri veya reklamlar gibi öğeler içerdiğinde meydana gelmektedir. Tarayıcı veya diğer yazılımlar bu öğeleri diğer sitelerden aldığında, çerezleri de yerleştirebilmektedirler (ICO, 2019, s.6).

Amaçlarına Göre Çerezler

Kesinlikle Gerekli Çerezler

Kullanıcının bir internet sitesine, platforma veya uygulamaya göz atması ve internet sitesinin veri trafiğini ve iletişimini kontrol etme, oturumu tanımlama, sepete eklenen öğeleri hatırlama, ödeme sürecini tamamlama gibi hizmetlerin yerine getirilmesi için gereklidir (AEPD, 2021, s.10-11).

İşlevsel Çerezler (Tercih Çerezleri)

Bu çerezler, kullanıcıların dil, görüntülenmiş arama sonuçlarının sayısı gibi kendi deneyimlerini diğer kullanıcıların deneyimlerinden ayıran belirli koşullar altında hizmete erişebilmeleri için internet sitesinin bilgileri hatırlamasını sağlamaktadır. Örneğin, kullanıcılar internet sitesinin dilinin hatırlanması amacıyla bir bayrak ikonuna tıkladığında, münhasıran bu amaç için kullanılması şartıyla kullanıcının dil hizmetini açıkça talep ettiği anlaşıldığından kullanıcıdan açık rıza alınması gerekmeyecektir (AEPD, 2021, s.11).

Performans-Analitik Çerezleri

İnternet sitelerinde kullanıcı davranışlarının analiz ve takip edilmesini sağlayan çerezlerdir. Bu tür çerezler aracılığıyla toplanan bilgiler, hizmet kullanımına ilişkin verilerin analizinin işlevinde iyileştirmeler sağlamak amacıyla kullanılır, bu duruma bir reklamın kullanıcılar üzerindeki etkisinin ölçümü de dahildir (AEPD, 2021, s.11-12). Bir internet sitesinin kullanılmasına dair ziyaret edilen sayfaların neler olduğu, nelere tıklanıldığını izlemek için kullanılmaktadırlar. Genellikle üçüncü taraflarca yerleştirilmektedir (Zorer, 2019).

Reklam/Pazarlama Çerezleri

Bu çerezler, çevrimiçi alışkanlıkların izlenmesi yoluyla elde edilen kullanıcı davranışları hakkında bilgi depolamak, belirli bir profil geliştirmek ve bu profile uygun reklam yayınlanmasına yardımcı olmak için kullanılmaktadır (AEPD, 2021, s.12). Bunlar kalıcı çerezlerdir ve genellikle üçüncü taraf çerezlerdendir.

ÇEREZLER YOLUYLA KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN AVRUPA BİRLİĞİNDE YER ALAN DÜZENLEMELER

2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması Direktifi

95/46/EC sayılı Direktifin parçası olan, Avrupa Birliğinde elektronik haberleşme sektörüne yönelik düzenlemeler içeren ve 97/66/EC Sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Özel Hayatın Korunmasına İlişkin Direktifi yürürlükten kaldıran 2002/58/EC sayılı Direktif'in iletişimin gizliliği başlıklı 5 inci maddesinin üçüncü fikrası çevrimiçi davranışsal reklamcılık kapsamında olup çerezler vasıtasıyla kişisel verilerin işlenmesi noktasında önem teşkil etmektedir. Söz konusu maddenin değişiklik içermeyen ilk halinde; üye devletlerin, bir abonenin veya kullanıcının terminal ekipmanında (bir çerezin yerleştirildiği genellikle bilgisayar ya da mobil cihaz) saklanan bilgilere erişim sağlamak veya bilgiyi depolamak için elektronik iletişim ağlarının kullanımına, yalnızca ilgili abone veya kullanıcıya 95/46/EC sayılı Direktif uyarınca açık ve kapsamlı bilgi sağlanması ve söz konusu işlemeyi reddetme hakkı sunulması şartıyla izin verilmesini sağlaması gerektiği düzenlenmiştir (Eur-Lex, 2022a).

2002/58/EC sayılı Direktif, 2009/136/EC sayılı Direktif ile belli hususlarda değişikliğe uğramıştır. 2009/136/EC sayılı Direktif ile değişikliğe uğrayan 2002/58/EC sayılı Direktifin 5 inci maddesinin üçüncü fikrasında, kullanıcının terminal ekipmanlarında verinin depolanması veya saklanan verilere erişmeye yalnızca kullanıcıya açık ve kapsamlı bilgi verilmesi ve kullanıcı rızasının alınması halinde izin verildiği belirtilerek anılan maddenin ilk halinde yer alan şartlara ek olarak kullanıcı veya abonenin rızasının alınması gerektiği de düzenlenmiştir (Alternatif Bilişim Derneği, 2013; Eur-Lex, 2022b; European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law 2018 Edition, 2018, s.327-329).

Ayrıca bu konuda en ayrıntılı değerlendirme 29 Veri Koruması Çalışma Grubunun (29 Veri Koruması Çalışma Grubu: Genel Veri Koruma Tüzüğünün (GVKT) yürürlüğe girdiği 25 Mayıs 2018 tarihine kadar mahremiyetin ve kişisel verilerin korunmasına ilişkin konularla ilgilenen bağımsız Avrupa çalışma grubudur. Bu çalışma grubunun yerini daha sonra, Avrupa Veri Koruma Kurulu (EDPB) almıştır. (bkz. https://www.dataprotection.ie/en/dpc-guidance/guidance-from-the-european-data-protection-board)) 22 Haziran 2010 tarih ve 2/2010 sayılı "Çevrimiçi Davranışsal Reklam Hakkında Görüş"ünde yapılmıştır (Karaarslan, Eren ve Koç, 2014, s.190; Keser Berber, 2014, s.36; Alternatif Bilişim Derneği, 2013).

29 Veri Koruması Çalışma Grubunun 22 Haziran 2010 Tarih ve 2/2010 sayılı Çevrimiçi Davranışsal Reklam Hakkında Görüşü

29 Veri Koruması Çalışma Grubunun 22 Haziran 2010 tarih ve 2/2010 sayılı "Çevrimiçi Davranışsal Reklam Hakkında Görüş"ünde, 2002/58/EC sayılı Direktifin 2009/136/EC sayılı Direktif ile değişikliğe uğrayan 5 inci maddesinin üçüncü fikrası ve 95/46/EC sayılı Direktifin çevrimiçi davranışsal reklamcılık bünyesinde nasıl uygulanacağı hususlarında değerlendirmelerde bulunulmuştur (Keser Berber, 2014, s.37). 2/2010 sayılı "Çevrimiçi Davranışsal Reklam Hakkında Görüş"te konu ile ilgili ilkeler belirlenmiş, bilgilendirme yükümlülüğü ve rıza kavramı ayrıntılarıyla açıklanmış (Popoli, 2012, s.16), rızanın geri alınması, verilerin anonimleştirilmesi, anonimleştirilen verilerin daha sonra kullanıcıyla ilişkilendirilmesinin önlenmesi, verilerin toplanma amacıyla sınırlandırılması, mahremiyet tabanlı tasarım, hassas içerikli veriler, çocukların korunması hususlarına değinilmiştir (Karaarslan, Eren ve Koç, 2014, s.190).

29 Veri Koruması Çalışma Grubunun 22 Haziran 2010 tarih ve 2/2010 sayılı "Çevrimiçi Davranışsal Reklam Hakkında Görüşü"ü (Article 29 Data Protection Working Party, 2/2010) incelendiğinde aydınlatma yükümlülüğü ve rıza alınması hususunun aşağıdaki şekilde detaylandırıldığı görülmektedir;

- Çerezler vasıtasıyla kişilerin internet ortamında takip edilmesi faaliyetine 2002/58/EC sayılı Direktifin 5 inci maddesinin üçüncü fikrasının uygulanması yargısına iki hususa dikkat çekilerek ulaşılmıştır. Bunlar, takip çerezlerinin ilgili kişilerin terminal cihazında saklanan bilgiler olduğu ve bu bilgilere çevrimiçi davranışsal reklamcılık amacıyla erişildiğidir (Keser Berber, 2014, s.37; Article 29 Data Protection Working Party, 2/2010, s.8).

- Çevrimiçi davranışsal reklamcılık uygulamaları yönünden aydınlatma yükümlülüğünün nasıl olacağı ayrıntılı şekilde açıklanmıştır. İnternet kullanıcılarının ulaşabileceği şekilde bilgilendirme yapılmasının önemi vurgulanmıştır. Bilgilendirmenin açık ve kapsamlı olması gerektiği ve genel açıklamaların yeterli olmayacağı hususu, 2002/58/EC sayılı Direktifin Giriş Bölümünün 25 inci hükmünde açıklanmıştır. Yine 2002/58/EC sayılı Direktifin Giriş Bölümünün 25 inci hükmünde bilgilendirmenin mümkün olduğunca kullanıcı dostu şeklinde yapılması gerektiği belirtilmiştir. Kullanıcı dostu şeklinde bilgilendirme; bilgilendirmenin doğrudan ekran üzerinde ve interaktif şekilde yapılması, kolaylıkla ulaşılabilir ve anlaşılabilir olması ilkeleri kapsamında düşünülmektedir. Bu kapsam dışında alternatif yöntemlerin de uygulanabileceği belirtilmiştir. Ayrıca bilgilendirmenin düzenli aralıklarla tekrarlanması gerektiği ve düzenli tekrarlama yapılmadıkça ilgili kişilerin izin verdiği veri işleme faaliyetini unutabilecekleri üzerinde durularak izin verilen veri işleme faaliyetini hatırlatıcı sembollere yer verilebileceği ifade edilmiştir. Bilgilendirmenin 2002/58/EC sayılı Direktifin 5 inci maddesinin üçüncü fikrası gereği çerez gönderen ya da çerezdeki bilgiyi okuyan taraf tarafından yapılacağı; çoğunlukla bunun reklam ağı sağlayıcıları tarafından yapıldığı, ancak internet sitesi ile reklam ağı sağlayıcının bazı durumlarda (örneğin; interneti sitesinin doğrudan tanımlanabilir bilgileri reklam ağı sağlayıcılarına aktardığı durum) ortak veri sorumlusu olacağı ve bilgilendirme yükümlülüğünün yerine getirilmesinde sorumlu oldukları ve internet sitelerinin bilgilendirme yükümlülüğünü yerine getirmesindeki öneminin üzerinde durulmuştur (Article 29 Data Protection Working Party, 2/2010, s.17-19; Keser Berber, 2014, s.39-41).

Çerez ve benzeri araçlarla veriye erişilmesi ve bilgi toplanması için kullanıcının önceden alınmış ve bilgilendirilmiş rızasının gerekli olduğu belirtilmiştir (Alternatif Bilişim Derneği, 2013). Rıza alma yükümlülüğü kullanıcı terminal cihazına çerezi yerleştiren ya da çerezdeki bilgiye erişen taraftadır. Bu rızanın özellikleri de bu görüşte ayrıntılı olarak düzenlenmiştir (Article 29 Data Protection Working Party, 2/2010, s.13);

- Rıza, kullanıcı terminal cihazına çerezin yerleştirilmesi ve/veya bilginin toplanması anından önce alınmalıdır,

- Bilgilendirme yükümlülüğü (çerezin gönderilme ve amacı hakkında bilgi) yerine getirildikten sonra rıza alınmalıdır,

- Rıza özgürce verilmeli, belirli olmalı ve bilgilendirilmiş kullanıcının taleplerinin işareti olmalıdır,

- Rıza geri alınabilir olmalıdır.

Çeşitli rıza alma yöntemleri de bu görüşte belirtilmiştir. Bunlar; tarayıcı ayarları yoluyla, opt-out (reddetme hakkı) ve opt-in (önceden izin alınması) yöntemidir.

Tarayıcı ayarları yoluyla kullanıcıların terminal cihazlarına çerez yerleştirilmesinin önlenebileceği, internet siteleri ya da reklam ağı sağlayıcılarının gizlilik politikalarında bu duruma yer verdikleri ve bilgilendirme yaptıkları; ancak bu durumun 2002/58/EC sayılı Direktifin 5 inci maddesinin üçüncü fikrası kapsamındaki rıza alma yükümlülüğünü karşılamadığı belirtilmiştir. Bu durumu

kullanıcıların çoğunluğunun çerezler aracılığıyla izlendiği ve tarayıcı ayarları yoluyla bu çerezlerin engellenebileceği hususlarında bilgi sahibi olmamalarına, dolayısıyla kullanıcıların hareketsiz kalmasının çerezlere izin vermesi anlamına gelmeyeceğine; tarayıcı ayarları ile bilgilendirilmiş rızanın verildiğinin kabulü için kullanıcının seçimleri dışında hareket etme imkânının olmamasının gerektiği; tarayıcı ayarlarının değiştirilmemesinin ileride meydana gelecek her türlü işleme faaliyetine rıza verildiği anlamına gelmesinin geçerli rızayla ilgili genel kurallara aykırılık teşkil edeceği belirtilmiştir. Ayrıca tarayıcı ayarlarıyla çerezler engellense bile flash çerezlerin bu ayarlar vasıtasıyla temizlenmediği hususuna da değinilmiştir (Keser Berber, 2014, s.43-44).

Reddetme hakkı (opt-out) verilmesi yönteminde, kullanıcının ilgili reklam ağlarının bulunduğu internet sitelerine girerek davranışsal reklamcılık amacıyla takip edilmeyi reddettiğini seçmesi gerektiği belirtilmiştir. Bu yöntemin rıza alınması yükümlülüğünü tam olarak karşılamadığı; ancak çok sınırlı hallerde yeterli olabileceği buna örnek olarak da kullanıcının davranışsal reklamcılık amacıyla takip edildiğinin bilincinde olarak reddetme hakkının varlığını bilmesi ve bundan yararlanmak istememesi verilmiştir. Opt-out yönteminin rıza alma yükümlülüğüne ilişkin genel kurallara aykırılık teşkil ettiği belirtilmiştir (Keser Berber, 2014, s.45-46).

Önceden izin alınmasının (opt-in) en uygun yöntem olduğu, kullanıcıların çerezin ne zaman alınacağı, saklanacağı ya da gönderileceği hususlarında anlaşılabilir dille; hangi bilginin bu çerezde saklanacağı ve çerez yoluyla toplanan bilginin ne amaçla toplanacağı ve bu çerezin geçerlilik süresinin de açıklanarak bilgilendirilmesi sonrasında bu yöntemin uygulanmasının gerektiği belirtilmiştir. Ayrıca kullanıcıların rıza vermesinin çerez gönderilmesi, bu çerez vasıtasıyla veri toplanması ve işlenmesi hususlarını da kapsaması gerektiği yargısına ulaşılmıştır. Verilen rızanın süre bakımından sınırlandırılması gerektiği, bu sürenin örneğin bir sene olabileceği ve belirlenen süre sonunda yeniden rıza alınması gerektiği ifade edilmiştir (Keser Berber, 2014, s.46).

Öte yandan, bilgilendirilmiş rızanın genel kurallara uyulması kaydıyla alternatif yollarla da alınabileceği belirtilmiştir (Article 29 Data Protection Working Party, 2/2010, s.17).

29 Veri Koruması Çalışma Grubunun 2 Ekim 2013 Tarih ve 02/2013 Sayılı Çerez Kullanımına İlişkin Rıza Alımına İlişkin Rehberi

Çerezlere ilişkin ilgili kişilerin rızasının alınması bakımından 29 Veri Koruması

Çalışma Grubu'nun 2 Ekim 2013 tarih ve 02/2013 sayılı "Çerez Kullanımına İlişkin Rıza Alımına İlişkin Rehber"inde (Article 29 Data Protection Working Party, 02/2013) görüş ve tavsiyeleri bulunmaktadır. Bu kapsamda, çerez kullanımına ilişkin rıza alımına yönelik bu rehberde hangi düzenlemelere yer verildiği üzerinde durulacaktır.

Tüm Avrupa Birliği üye ülkelerinde uygulanan 2002/58/EC sayılı Direktifte yapılan 2009 yılı değişiklikleri ile birlikte internet sitesi operatörleri ya da üçüncü gruplar tarafından hedeflenmiş reklamcılık, ürün optimizasyonu, analiz yapmak ve fonksiyonelliği geliştirmek gibi çeşitli amaçlarla çerezlerin kullanılması için rıza alınmasına yönelik bir dizi düzenlemeler geliştirildiği ve internet sitesi operatörleri tarafından geliştirilmiş bir dizi rıza mekanizmasının hedef kitle türlerini ve organizasyonların çeşitliliğini yansıttığı ifade edilmiştir.

Söz konusu Görüşte belirtildiği üzere, 2002/58/EC sayılı Direktif çerezlere ulaşmak ya da çerezleri depolamak için rıza almaya yönelik şartlar koymasına rağmen Avrupa Birliği üye ülkelerinin internet sitesi operatörleri arasında pratikte (uygulamada) farklılıklar bulunmaktadır ve gözlemlenen uygulamalar;

- Kullanıcının, kullanılan çerez türleri hakkında link veya linkler sağlayarak katmanlı bir yaklaşımla daha fazla bilgi edinebileceği çerez türlerinin kullanıldığına dair anlık bildiri,
- Kullanıcının internet sitesinde bulunan çerezleri kabul etmesine yönelik anlık uyarı,
- Kullanıcının çerezleri tercih etmesini ve sonrasında bu tercihini geri çekmesini sağlayan bilgi,
- Çerezlerin tamamını ya da bazılarını seçip kabul etmesini ya da reddetmesini sağlayan mekanizma,
- Kullanıcıların çerezlere ilişkin öncelikli tercihi değiştirebileceği seçenek

yöntemlerinden bir ya da birkaç tanesine dayanmaktadır. Şunu da belirtmek gerekir ki; bu yöntemlerden her biri rıza mekanizmasının önemli birer parçası olmalarına karşın, her bir yöntemin diğerlerinden bağımsız olarak uygulanması geçerli rızanın sağlanması için yeterli olmayabilecektir. Çünkü geçerli rızanın sağlanabilmesi için tüm unsurların bir arada olması gerekmektedir (örneğin seçim mekanizmaları aynı zamanda bildirim ve bilgilendirmeyi de içermektedir).

2002/58/EC sayılı Direktifin farklı yorumları ve ilgili pratik uygulamalar dikkate alındığında; tüm Avrupa Birliği üye devletlerinde faaliyet gösteren bir internet sitesi için hangi uygulamanın yasal olarak uyumlu olacağı sorusunun gündeme geldiği belirtilerek, bu soru 2002/58/EC sayılı Direktifin 2 nci maddesinin (f) bendi ve 17 nci Resitalinin, 95/46/EC sayılı Direktife atıfta bulunarak rıza kavramını tanımladığı, 95/46/EC sayılı Direktifin 2 nci maddesinin (h) bendinin bireylerin kişisel verilerinin işlenmesine yönelik rızasının bireyin bu veri işlemeyi kabul ettiğini belirttiği, isteklerinin özgürce verilen, spesifik ve bilinçli bir göstergesi olması ve 95/46/EC sayılı Direktifin 7 nci maddesine göre rızanın ayrıca açık olması gerektiği şeklinde yanıtlanmıştır.

Bu Görüşe göre geçerli bir rıza için gerekli ana unsurlar (Article 29 Data Protection Working Party, 02/2013, s.3-5) şunlardır;

- **Belirli Bilgi (Specific Information):** Geçerli olması için, rıza belirli olmalı ve uygun bilgiye dayanmalıdır. Başka bir deyişle işlemin kesin amacını belirtmeyen battaniye rıza kabul edilemez. Rıza arandığı anda (ve aynı yerde) çerez kullanımı hakkında açık, kapsamlı ve görünür uyarı sağlanmalıdır. Örneğin kullanıcı bir internet sitesinin giriş sayfasına göz atmaya başladığında bu uyarı sunulabilir. Kullanıcı internet sitesine eriştiğinde, internet sitesi tarafından kullanılan farklı tip ve amaçlardaki çerezler hakkında gerekli olan tüm bilgiye ulaşabilmelidir. İnternet sitesi, kullandığı tüm çerez tiplerini belirlenmiş bir lokasyonda görünür bir şekilde bir link yardımıyla sergilemelidir. Çerezlerin amaçları hakkında bilgi verilmesi gereklidir ve eğer ilgili ise üçüncü taraflardan (third-party) kaynaklı olası çerezler gösterilmeli veya çerezler tarafından internet sitesinde toplanmış verilere üçüncü tarafların erişimi hakkında bilgi verilmelidir. Muhafaza süresi, üçüncü taraf çerezler hakkında ayrıntılı bilgi ve diğer teknik bilgiler, kullanıcıyı tam anlamıyla bilgilendirmek için dahil edilmelidir. Kullanıcılar çerezlere ilişkin isteklerini ifade edebilecekleri tüm yollar hakkında da bilgilendirilmelidir. Örneğin, çerezlerin tamamını, birkaçını veya hiçbirini kabul edip edemeyeceği ve ilerleyen zamanda tercihlerini nasıl değiştirebileceği konusunda bilgilendirilmelidir.

- **Zamanlama (Timing):** Genel kural, rızanın kişisel veri işlenmesi faaliyeti başlamadan önce verilmesidir. 29 Veri Koruması Çalışma Grubunun 15/2011 Sayılı (Working Party Opinion 15/2011 on the definition of consent) görüşünde karara bağlandığı üzere, kişisel veri işleme faaliyeti başlamadan önce rıza verilmelidir. Söz konusu Görüş 2002/58/EC sayılı Direktifin 5 inci maddesinin üçüncü fikrasının kapsamına da uygunluk sağlamaktadır. İnternet sitesi, kullanıcı çerezlere ilişkin isteklerini bildirmeden önce (kullanıcı rızasını gerektirmeyen çerezler haricinde) kullanıcının cihazına hiçbir çerezin yerleştirilmediği bir rıza alma mekanizması sunmalıdır.

- **Aktif Seçim (Active Choice/ Active Behaviour): R**ıza, açık olmalı ve belirsizliğe mahal vermemelidir. Bu nedenle, rıza verme prosedürü ilgili kişide hiçbir şüphe bırakmamalıdır. Kural olarak rızanın alınmasında şekli açıdan bir sınır yoktur. Ama rızanın geçerli olması için kullanıcının isteklerinin aktif göstergesi olmalıdır. Bu minimum gösterge ifadeleri, ilgili kişinin isteklerini kapsayacak ve veri sorumlusu tarafından anlaşılabilecek yeterli açıklıktaki uyarılardır.

  Çerezlerin tipleri ve amaçları hakkındaki bilgiye ek olarak; internet sitesi, kullanıcının göz atmaya başladığı sayfada açık ve kapsamlı bilgi sunmalıdır. Rıza almak için kullanılan araçlar, açılış ekranları, banner, örnek model iletişim kutuları, tarayıcı ayarları vs. içerebilir.

  İnternet sitesi operatörünün kullanıcının tam olarak bilgilendirildiğinden ve tarayıcılarını veya diğer uygulamaları aktif olarak yapılandırdığından emin olduğu durumlarda, doğru koşullarda böyle bir yapılandırma “aktif seçim” olarak adlandırılır. Geçerli ve etkili rıza alınması için gerekli olan tarayıcı ayarları şartları 29 Veri Koruması Çalışma Grubunun 2/2010 sayılı görüşünde tanımlanmıştır. Kullanıcıların olumlu bir eylem veya aktif seçim vasıtasıyla çerezler için rıza belirttikleri süreç, o eylem hakkında tam olarak bilgilendirildiklerini göstermektedir. Böylece butona, linke veya kutuya tıklayarak ya da internet sitesi operatörü tarafından net ve kesin bir şekilde açıklanmış rıza anlamına gelen diğer aktif seçimler ile kullanıcı rızasını belirtebilir.

  Aktif eylemle ifade edilen seçimin bu eylemle çerezlerin ayarlanacağına dair açık bilgilendirmeye dayandığından emin olunmalıdır. Bu nedenle aktif seçimi gösteren buton, link, kutunun içinde ya da yakınında bilgilendirmenin sunulması kullanıcının eylemi gerçekleştirirken bilgilendirmeden faydalandığını kanıtlamak açısından gereklidir. Bilgilendirme internet sitesi üzerinde hazır bulunmalıdır ve kullanıcı rızasını vermeden kaybolmamalıdır. İnternet sitesi operatörü de belirsizliğe mahal vermeksizin kesin rızanın verildiğinden emin olmalıdır. Kullanıcının bir internet sitesine girmesi halinde çerezler hakkında bilgilendirme gösterilmiş fakat kullanıcı olumlu eylemde bulunmamışsa yani yalnızca başlangıç sayfasında aktif seçim yapmadan kalmışsa rızanın belirsizliğe mahal vermeden verildiği söylenemeyecektir.

- **Özgürce Verilmiş Rıza (Freely Given Consent/Real Choice):** Rıza, sadece ilgili kişi gerçek tercihini uygularsa ve tehdit, baskı, hile ya da ilgili kişi rıza vermediğinde bu tip önemli olumsuz sonuçlarla karşılaşma riski olmazsa geçerli olabilmektedir.

  Rıza mekanizması, giriş sayfasında çerezlere ilişkin gerçek ve anlamlı bir seçenekle kullanıcıya sunulmalıdır. Kullanıcı birkaç çerezi ya da tüm çerezleri kabul etmek veya reddetmek hususunda özgürce seçim yapma ve gelecekte çerez ayarlarını değiştirme imkanına sahip olmalıdır.

29 Veri Koruması Çalışma Grubunun 7 Haziran 2012 Tarih ve 04/2012 Sayılı Çerez Rızası İstisnası Görüşü

29 Veri Koruması Çalışma Grubunun 7 Haziran 2012 Tarih ve 04/2012 Sayılı Çerez Rızası İstisnası Görüşünde çerezler vasıtasıyla kişisel verilerin işlenmesi faaliyetinde rıza muafiyetinin hangi hallerde uygulanacağına dair görüşlere yer verilmektedir.

2002/58/EC sayılı Direktifin 5 inci maddesinin üçüncü fikrası aşağıda belirtilecek iki kriterden birinin sağlandığı hallerde çerezleri bilgilendirilmiş rıza şartından muaf tutmaktadır. Bunlar (Carey, 2018, s.199);

Kriter A: Çerez "tek amaç (sole purpose) olarak bir iletişimin elektronik iletişim ağı üzerindeki iletimini gerçekleştirmek" için kullanılır.

Kriter B: "Abonenin veya kullanıcının hizmet almak için açıkça talep ettiği, bilgi toplum hizmetleri için kesinlikle gerekli (strictly necessary) olan çerezlerdir.

Söz konusu Görüşte belirtilen tavsiyelere dair hususlara bu bölümde yer verilecektir.

Kriterlerin Analizi

Kriter A

Kriter A'da (Article 29 Data Protection Working Party, 04/2012, s.2-3) "tek amaç" terimi, açıkça bu kriterin kullanımını sınırlandırmak ve farklı yorumlar katılmasını engellemek için kullanılmıştır. Çerezin Kriter A muafiyeti kapsamında değerlendirilmesi için çerez kullanılmadığı takdirde iletişimin elektronik iletişim ağı üzerinden aktarımının imkânsız olması gerekmektedir.

İki taraf arasında bir ağ üzerinde iletişimin olabilmesi için kesinlikle gerekli olan üç unsur vardır:

1. Özellikle iletişim uç noktalarını tanımlayarak, bilgiyi ağ üzerinden yönlendirebilmek,

2. Özellikle veri paketlerini numaralandırarak, veri öğelerini istenen sırayla değiştirmek,

3. İletişim hatalarını veya bilgi kaybını saptayabilmek.

Kriter A'da yer alan "bir elektronik iletişim ağı üzerinden bir iletişimin aktarımı" terimleri ve özellikle "üzerinden" kelimesinin, elektronik iletişim ağının kurulmasında gerekli teknik veri alışverişleriyle sınırlı olmaksızın, potansiyel olarak yukarıda tanımlanan özelliklerden en az birini karşılayan "uygulama seviyesi" verilerini içeren 2002/21/EC sayılı Direktifte tanımlandığı gibi elektronik iletişim ağının kullanımıyla gerçekleşen her türlü veri alışverişini ifade ettiği anlaşılmaktadır. İnternet iletişiminde, yukarıdaki üç özelliğin en az birini sağlayan çerezler Kriter A kapsamındadır.

Kriter B

Bir çerezin Kriter B (Article 29 Data Protection Working Party, 04/2012, s.3-4) muafiyeti kapsamında değerlendirilmesi için iki şart bulunmaktadır;

1. Bilgi toplum hizmetleri, kullanıcı veya abone tarafından açıkça talep edilmelidir.

2. Çerez, bilgi toplum hizmetini etkin kılmak için kesinlikle gerekli olmalıdır. Aksi halde hizmet çalışamaz hale gelmelidir.

Başka bir ifadeyle istisna durumunun oluşması için, çerezin kesinlikle gerekli olması ile kullanıcı tarafından talep edilen hizmet sunumu arasında çok açık bir bağlantı olması gerekmektedir.

Kullanıcı ya da abonenin açıkça talep ettiği bilgi toplum hizmetini bir örnekle açıklamak gerekirse; çevrimiçi bir gazeteye herkes özgürce erişebilir, fakat üyeleri için ek fonksiyonları olabilir (yorum yazabilmek gibi). İşte bu ek fonksiyonlar kendi çerezleri ile çalıştırılmalıdır. Bu özel bağlamda, 29 Veri Koruması Çalışma Grubu bir bilgi toplumu hizmetinin çeşitli işlevlerin toplamı olarak görülmesi

gerektiğini ve bu tür bir hizmetin kesin kapsamının kullanıcı (veya abone) tarafından talep edilen işlevlere göre değişebileceğini düşünmektedir. Sonuç olarak, Kriter B bilgi toplum hizmeti tarafından sunulan "fonksiyonellikler" olarak düşünülebilmektedir. Bu bağlamda Kriter B muafiyetine dahil olan bir çerezin aşağıdaki testleri geçmesi gerekmektedir;

1. Çerez kullanıcı ya da aboneye belirli bir işlev sağlamak için gerekli olmalıdır; eğer çerez etkisiz ise fonksiyonellik söz konusu olmayacaktır.

2. Bu fonksiyonellik, kullanıcı veya abone tarafından açıkça talep edilmiş olmalıdır.

Çerezlerin Ayırt Edici Özellikleri

Bu bölümde yukarıda belirtilen kriterlere göre çerez kategorilerinin ayırt edici özellikleri (Article 29 Data Protection Working Party, 04/2012, s.4-5) değerlendirilecektir. Bir çerezin hizmet için "kesinlikle gerekli", "kullanıcı tarafından açıkça talep edilmiş" veya "tek amaç" ile sınırlandırılmış olması Kriter A veya Kriter B muafiyeti kapsamında değerlendirilmesi için dikkate alınması gereken özelliklerdir.

Çerezin rıza şartından muaf olması için bir geçerlilik süresi olması gerekmektedir. Bu geçerlilik süresinin de çerezin ne için kullanıldığı ile doğrudan ilgisi olmalıdır. Ortalama bir kullanıcı ya da abonenin beklentileri göz önüne alınarak geçerlilik süre sınırı konulmalıdır. Bu da gösteriyor ki; Kriter A ve Kriter B ile eşleşen çerezlerde tarayıcı oturumunun bitmesi veya daha önceden belirlenmiş bir süre bitiminin bulunması muhtemeldir. Ancak durum her zaman böyle olmamaktadır. Örneğin, daha sonra değinilecek olan alışveriş sepeti senaryosunda, satıcı çerezi tarayıcı oturumunun bitmesi sonrasında da devam etmek için veya kullanıcının tarayıcıyı yanlışlıkla kapatmış olabileceğini ve alışveriş içeriğinin kurtarılması beklentisini hesaba katarak gelecek birkaç saat için kurabilmektedir. Diğer durumlarda kullanıcı bazı bilgilerinin bir oturumdan diğer oturuma hatırlanması için açıkça istekte bulunmalıdır ki bu durum kalıcı çerezleri kullanmayı gerektirmektedir.

Bu açıklananlara ek olarak, bir internet sitesini ziyaret eden kullanıcı için "üçüncü taraf" çerezler genellikle "kesinlikle gerekli" değildir, çünkü bu çerezler genellikle kullanıcı tarafından "açıkça talep edilenden" farklı bir hizmetle ilgilidir. Sonuç olarak, birinci taraf oturum çerezlerinin üçüncü taraf kalıcı çerezlere kıyasla rızadan muaf olmaları çok daha muhtemeldir. Ancak, üçüncü taraf çerezler

genellikle "kesinlikle gerekli" olma koşulunu sağlamamaktadırlar; ayrıca kullanıcı tarafından açıkça talep edilen çerezlerden farklılıkları bulunmaktadır. Bununla birlikte, birinci ya da üçüncü taraf olması bir çerezin Kriter A veya B muafiyeti kapsamında olduğunu değerlendirmek için tek başına yeterli değildir. Kullanıcının hesabına girmesini sağlamak için oluşturulmuş bir çerez ya da benzer şekilde kullanıcıyı tanımlamak ve etki alanı çerçevesinde takip etmek ve isteğe uyarlanmış içerikler ve reklamlar göndermek için kullanılan çerezler dikkate alındığında bu iki çerez türü de benzer çerez türleridir (oturum çerezi ya da sürekli çerez). Bu çerezlerin benzer süre bitimleri olabilmekte veya üçüncü taraflar tarafından kontrol edilebilmektedirler. Veri korumanın riski çerezin taşıdığı bilgiden değil, devam eden işleme amacından gelmektedir. Nihayetinde bir çerezin Kriter A ya da Kriter B'ye göre rızadan muaf olmasına karar vermek için amacı, kendine özgü uygulaması ve gerçekleştirilen işlem göz önüne alınmalıdır.

Çok Amaçlı Çerezler

Bir çerez birçok amaç için kullanılıyor ise, bu tip çerezin rızadan muaf olabilmesi için her bir amacın ayrı ayrı rızadan muaf olması gerekmektedir. Örneğin, kullanıcı tercihlerini hatırlamak ve izlemek gibi iki farklı amacı olan çerezin, kullanıcının tercihlerini hatırlama özelliği istisna kapsamında değerlendirilirken izleme özelliği Kriter A veya Kriter B ile bağdaşmamaktadır. Bu durumda internet sitesi, izleme amacı için kullanıcı rızasına ihtiyaç duymaktadır. Uygulamada bu durum, internet sitesi sahipleri tarafından farklı amaçlar için farklı çerezlerin kullanılmasını desteklemektedir (Article 29 Data Protection Working Party, 04/2012, s.6).

Çerez Kullanım Senaryoları

Bu bölümde, 29 Veri Koruması Çalışma Grubu 7 Haziran 2012 Tarih ve 04/2012 Sayılı Çerez Rızası İstisnası Görüşünde açıklanan rızadan muaf olan çerezlerin kullanım senaryoları (Article 29 Data Protection Working Party, 04/2012, s.6-9) üzerinde durulacaktır. Bu senaryolara göre; *Kullanıcı Girdili Çerezler;* kullanıcının girdilerini izleyip bunları seri mesaj değişimi servis sağlayıcıya aktaran oturum çerezleridir. Bu çerezlerin, genellikle bir Oturum Kimliğine (rastgele geçici benzersiz bir sayı) dayanan birinci taraf çerezler olması ve en geç oturum sona erdiğinde sona ermesi beklenmektedir. Birinci taraf kullanıcı girdili oturum çerezleri, tipik olarak çevrimiçi formları doldururken veya bir alışveriş sepetine seçtiği öğeleri eklerken kullanıcıyı izleyen, kullanıcının butonu tıklayarak seçtiği parçaların kaydını tutan çerezlerdir. Bu çerez türü Kriter B kapsamında rızadan muaf tutulabilmektedir.

Kimlik Doğrulama Çerezleri; kullanıcıyı giriş yaptığında tanımlamak için kullanılmaktadırlar (Örneğin, çevrimiçi bankacılık sitesinde). Bu çerezler, internet sitesinin ziyaret edilmesi veya içeriğe ulaşılması için (örneğin, banka hesaplarına bakmak, havale yapmak gibi) gereklidir. Bu tip çerezler Kriter B kapsamında rızadan muaf tutulabilmektedir.

Kullanıcı Merkezli Güvenlik Çerezleri; Kriter B kapsamında kimlik doğrulama çerezlerinde açıklanan muafiyet, kullanıcı tarafından açıkça talep edilen hizmet güvenliğini artırmaya yönelik belirli bir amacı olan çerezlere uygulanabilmektedir. Bu durum, bir internet sitesinde tekrarlanan başarısız oturum açma girişimlerini tespit etmek için kullanılan çerezler veya oturum açma sistemini kötüye kullanımlardan korumak için tasarlanmış diğer benzer mekanizmalar için geçerli olmaktadır. Ancak bu muafiyet, internet sitelerinin güvenliği için kullanılan çerezler veya kullanıcı tarafından açıkça talep edilmeyen üçüncü taraf hizmetlerin kullanımını kapsamamaktadır.

Multimedya Oynatıcısı Oturum Çerezleri; görüntü kalitesi, ağ bağlantı hızı ve ara bellek parametreleri gibi video veya ses içeriğini oynatmak için gereken teknik verileri depolamak için kullanılmaktadır. Bu multimedya oynatıcısı oturum çerezleri, günümüzde kullanılan en yaygın internet video teknolojisinin Adobe Flash olması nedeniyle yaygın olarak "flash çerezler" olarak bilinmektedir. Bu bilgilere ihtiyaç olmadığında, oturum sona erdikten sonra çerezlerin süresinin de sona ermesi gerekmektedir. Kullanıcı video veya yazı içeriğine ulaşmak istediğinde açıkça talep ettiği için bu video gösterim işlevi Kriter B muafiyeti kapsamında değerlendirilmektedir.

Yük Dengelemesi Oturum Çerezleri; Yük dengeleme birden çok makinenin internet sunucusu taleplerinin dağıtılması işlemlerine izin veren bir tekniktir. Kullanıcılardan gelen web istekleri, istek havuzundaki mevcut dahili sunuculardan birine iletilen bir yük dengeleme ağ geçidine yönlendirilmektedir. Bu yeniden yönlendirme bir oturum boyunca kalıcı olmaya ihtiyaç duyar, işlemenin tutarlılığını korumak için belirli bir kullanıcıdan kaynaklanan tüm istekler her zaman havuzdaki aynı sunucuya iletilmelidir. Yük dengeleyicinin isteklerinin uygun şekilde yeniden yönlendirilmesi amacıyla havuzdaki sunucunun tespiti için bu çerez kullanılabilmektedir. Bunlar oturum çerezleridir. Çerezin tek amacı iletişim uç noktalarını (havuzlardaki sunuculardan biri) tanımlamaktır. Çerez, ağ üzerindeki iletişimin gerçekleştirilmesi için gereklidir. Bu tür çerezler Kriter A kapsamında rızadan muaf tutulabilmektedir.

Kullanıcı Arayüzü Kişiselleştirme Çerezleri; kullanıcının internet sayfalarındaki

hizmete ilişkin tercihlerini depolamak için kullanılmaktadır ve kullanıcı adı gibi diğer kalıcı tanımlayıcılarla bağlantılı değildir. Yalnızca kullanıcı açıkça belirli bir bilgiyi hatırlamak için hizmet talep etmişse kurulabilmektedirler. Örneğin, bir butonu tıklamak veya kutuyu işaretlemek gibi. Bunlar, oturum çerezleri olabilmektedirler veya amaçlarına göre geçerlilik süreleri haftalar veya ayları kapsayabilmektedir. Kişiselleştirme çerezine tipik olarak; çok dilli bir internet sitesinde bir kullanıcı tarafından seçilen dili hatırlamak için kullanılan dil tercihi çerezleri (bayrağa tıklayarak) veya kullanıcının çevrimiçi arama sorgularıyla ilgili tercihini hatırlamak için kullanılan sonuç gösterme tercihi çerezleri (sayfa başına sonuç sayısını seçerek) örnek gösterilebilmektedir.

Sosyal Eklenti İçerik Paylaşımı Çerezleri; Birçok sosyal ağ, internet sitesi operatörlerinin özellikle belirli bir sosyal ağ hesabında tarayıcıları aracılığıyla "oturum açmış" ve üye olan kullanıcıların beğendikleri içerikleri veya yaptığı yorumları "arkadaşlarıyla" paylaşmasına izin vermek için internet sitesi operatörleri tarafından kendi platformlarına entegre edebilecekleri "sosyal eklenti modülleri" önermektedir. Bu eklentiler sayesinde, sosyal ağın üyeleri bu eklentilerle etkileşime geçtiklerinde üyelerin tespit edilmesini sağlamak için kullanıcının terminal ekipmanında çerezler depolanmakta ve bu çerezlere ulaşılmaktadır. Bu tür çerezler Kriter B kapsamında rızadan muaf tutulabilmektedir.

Rızadan Muaf Tutulmayan Çerezler

Bu bölümde, Kriter A veya B muafiyeti kapsamına girmeyen çerez kullanım senaryolarına (Article 29 Data Protection Working Party, 04/2012, s.9-11) yer verilmektedir.

Sosyal Eklenti Takip Çerezleri; daha önce de bahsedildiği üzere, birçok sosyal ağ, üyeleri tarafından "açıkça talep edilmiş" olarak kabul edilebilecek bazı hizmetleri sağlamak için internet sitesi sahiplerinin platformlarına entegre edebilecekleri "sosyal eklenti modülleri" sunmaktadır. Ancak bu modüller, örneğin davranışsal reklamcılık, analitik veya pazar araştırması gibi ek amaçlar için üçüncü taraf çerezlerle hem üye olan hem de üye olmayan bireyleri izlemek için de kullanılabilmektedir. Bu durumda söz konusu çerezler, kullanıcı tarafından açıkça talep edilen bir işlevselliği sağlamak için "kesinlikle gerekli" olarak kabul edilemeyecektir. Bu nedenle, izleme çerezleri Kriter B kapsamında muaf tutulamaz.

Üçüncü Taraf Reklamcılık Çerezleri; davranışsal reklamcılık için kullanılan üçüncü taraf çerezler, rızadan muaf değildir. Bu rıza gerekliliği, doğal olarak gösterim sıklığı, finansal günlük kayıt tutma, reklam ortaklığı, tıklama sahtekarlığı tespiti,

araştırma ve pazar analizi, ürün geliştirme ve hata ayıklama amacıyla kullanılan çerezler dahil olmak üzere reklamcılıktaki tüm ilgili üçüncü taraf operasyonel çerezleri kapsamaktadır ve bu amaçlardan hiçbirinin Kriter B uyarınca, kullanıcı tarafından açıkça talep edilen bir bilgi toplumu hizmetinin işlevselliği ile ilgili olduğu düşünülemeyecektir. Bu bağlamda, Avrupa vatandaşlarına çerez sunan şirketlerin Do Not Track standardına uyum sağlaması için Do Not Track istisnasız olarak etkin bir şekilde "Toplama Yapma" anlamına gelmelidir. Bu nedenle, bir kullanıcının izlenmeme tercihini belirttiği durumlarda, izleme amacıyla hiçbir tanımlayıcı kurulmamalı veya başka bir şekilde işlenmemelidir.

Birinci Taraf Analitik Çerezler; analitikler, genellikle çerezlere dayanan, internet siteleri için istatistiksel kitle ölçüm araçlarıdır. Bu araçlar özellikle internet sitesi sahipleri tarafından tekil ziyaretçi sayısını tahmin etmek, bir internet sayfasına yönlendiren önemli arama motoru anahtar kelimelerini tespit etmek veya internet sitesinde gezinme durumunu izlemek için kullanılmaktadır. Bugün mevcut olan analitik araçlar, her biri farklı veri koruma riskleri sunan bir dizi farklı veri toplama ve analiz modeli kullanmaktadır. "Birinci taraf" çerezlere dayalı birinci taraf analitik sistemler, "üçüncü taraf" çerezlere dayalı üçüncü taraf analitik sistemlere kıyasla farklı riskler barındırmaktadır. Bu diğer taraf, verileri kendi amaçları için kullanıp kullanmadığına veya teknik veya sözleşmeye dayalı düzenlemelerle yasaklanıp yasaklanmadığına bağlı olarak ortak veri sorumlusu veya veri işleyen olarak kabul edilecektir. Genellikle internet sitesi operatörleri için "kesinlikle gerekli" bir araç olarak kabul edilmekle birlikte, kullanıcı (veya abone) tarafından açıkça talep edilen bir işlevselliği sağlamak için kesinlikle gerekli değildirler. Kullanıcı, bu tür çerezler devre dışı bırakıldığında internet sitesi tarafından sağlanan tüm işlevlere erişebilmektedir. Sonuç olarak, bu çerezler Kriter A veya B'de tanımlanan muafiyet kapsamına girmemektedir.

Bununla birlikte, 29 Veri Koruması Çalışma Grubu tarafından birinci taraf analitik çerezlerin birinci taraf toplulaştırılmış istatistiksel amaçlar için kesin sınırlı olduklarında ve gizlilik politikalarında ek olarak yeterli mahremiyet önlemleri hakkında açık bilgi sağlayan internet siteleri tarafından kullanıldığında mahremiyet riski oluşturma olasılığı bulunmadığı değerlendirilmektedir. Bu tür önlemlerin, IP adresleri gibi tanımlanabilir diğer toplanan bilgilere uygulanan kapsamlı anonimleştirme mekanizmaları ve kullanıcı dostu opt-out mekanizması *(Kullanıcı dostu opt-out mekanizması; kullanıcıların kolayca erişebileceği ve önüne seçili gelen kutucukları reddedebileceği mekanizma anlamına gelmektedir. 29 Veri Koruması Çalışma Grubu, mahremiyet önlemleri içerisinde bu mekanizmanın olabileceğini belirtmektedir)* içermesi beklenmektedir.

Bu bağlamda, 29 Veri Koruması Çalışma Grubu tarafından 2002/58/EC sayılı Direktifin 5 inci maddesinin üçüncü fıkrasının gözden geçirilmesi halinde, birinci taraf anonimleştirilmiş ve istatistiksel amaçlarla toplulaştırılmış veri ile kesinlikle sınırlı olan çerezler için rıza alınması kriterine üçüncü bir muafiyet kriteri olarak eklenebileceğini belirtilmiştir ve E- Gizlilik Tüzük taslağına da bu yönde istisna hükmü getirildiği görülmektedir.

Taslak Halinde Olan E-Gizlilik Tüzüğünde Çerezlere Dair Yer Alan Hususlar

E-Gizlilik Tüzük taslağı ile 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması Direktifinin, teknolojik ilerlemeler ve çağın ihtiyaçlarını karşılamadığı dikkate alınarak bir dizi değişiklikler yapılmıştır.

Rıza alınması gerekliliğine dair etkili değişiklik yapılmamış olup, 2002/58/EC sayılı Direktifte yer alan istisnalar haricinde yeni istisnalar düzenlenmiş ve istisnalar daha net bir şekilde belirtilmiştir (Keser Berber, Atabey ve Mert, 2019, s.71). 2002/58/EC sayılı Direktifte Kriter A kapsamında "elektronik iletişimin sağlanması" ifadesi yer alırken söz konusu Taslakta *"elektronik haberleşme hizmetinin sağlanması"* düzenlenmiştir. Birinci taraf analitik çerezler açısından, çerez kullanımında (yalnızca kullanıcı davranışlarının istatistiki amaçla ölçümlenmesi) kullanıcının rızasının alınmasının gerekli olmayacağı ve bu istatistiki ölçümlemenin üçüncü kişiler tarafından müşterek sorumlu sıfatıyla gerçekleştirilmesi durumunda GVKT'nin 26 ve 28 inci maddeleri kapsamındaki koşullara uygun hareket etmek şartıyla bu istisnadan yararlanabilecekleri; *bilgi toplumu hizmetlerinin veya terminal ekipmanın güvenliğinin sağlanması, dolandırıcılığı önlemek veya teknik hataları önlemek veya tespit etmek* amacıyla çerezlerin bu amaç için gerekli olan süre boyunca kullanıcı rızası alınmadan kullanılabileceği ifade edilmiştir. Diğer taraftan, *yazılım güncellemesi* kapsamında belirli koşulların sağlanması şartıyla kullanıcı rızasına gerek olmadan çerezlerin kullanılabileceği; acil durumlarda, terminal cihazın bulunduğu yerin tespiti için kullanılacak *konum tespit çerezleri*nin istisna kapsamında olduğu düzenlenmiştir. Ayrıca, Taslak metinde verilerin, *elde edilme amacından farklı bir amaçla işlenmesi* bakımından kullanıcının rızası veya Birlik veya üye devlet hukukunda yasal düzenleme olmayan hallerde; elektronik iletişim verilerinin başka bir amaç için işlemenin başlangıçta toplama amacıyla uyumlu olup olmadığının tespitinin gerektiği ve bu tespitte kullanıcı ve çerezi kullanan işletme arasındaki ilişki, veri işleme faaliyetinin niteliği, farklı amaçla veri işlemenin olası sonuçları ve gerekli güvenlik önlemlerinin alınıp alınmadığının dikkate alınacağı, verilerin başka bir amaç için işlenmesi faaliyetinin başlangıçtaki veri işleme amacıyla uyumlu olduğu tespit edilirse; bu tür veri işleme faaliyetinde, bilginin amacı yerine getirmek için artık

gerekli olmadığı anda silinmesi veya anonim hale getirilmesi, işlemenin takma adlı bilgilerle (pseudonymised) sınırlı olması ve bilginin kullanıcı profili oluşturmak için kullanılmaması koşullarının sağlanması halinde kullanıcının rızasının gerekmeyeceği belirtilmiştir (Aksoy ve Halıcıoğlu, 2021, s.71-72).

KİŞİSEL VERİLERİN İŞLENMESİ BOYUTUYLA TÜRK HUKUKUNDA ÇEREZLER

5809 Sayılı Elektronik Haberleşme Kanunu

Türk Hukukunda çerezlere dair özel hüküm niteliğinde tek düzenleme 5809 sayılı Elektronik Haberleşme Kanununda (5809 sayılı EHK) bulunmaktadır. 5809 sayılı Kanunun 3 üncü maddesinin birinci fıkrasının (e) bendinde elektronik haberleşme: elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması, (j) bendinde elektronik haberleşme hizmeti: elektronik haberleşme tanımına giren faaliyetlerin bir kısmının veya tamamının hizmet olarak sunulması, (z) bendinde işletmeci: yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirket olarak tanımlanmıştır.

5809 sayılı EHK'de elektronik haberleşme sektöründe kişisel verilerin korunmasıyla ilgili hükümler yer almakta olup "İşletmecilerin hak ve yükümlülükleri" başlıklı 12 nci maddesinin ikinci fıkrasının (d) bendinde kişisel veri ve gizliliğin korunması yükümlülüğü düzenlenmiştir (Ayözger, 2016, s.107). Ayrıca, 5809 sayılı EHK'nin 6 ncı maddesinin birinci fıkrasının (c) bendinde abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak Bilgi Teknolojileri ve İletişim Kurumunun görevleri arasında sayılmaktadır. Aynı Kanunun "Kişisel verilerin işlenmesi ve gizliliğin korunması" başlıklı 51 inci maddesinin üçüncü fıkrasında *"elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabildiği"* ifade edilmiştir (Küzeci, 2019, s.439-442).

5809 sayılı EHK'nin 51 inci maddesinin üçüncü fıkrasının 2002/58/EC sayılı Direktifin 5 inci maddesinin üçüncü fıkrası ile benzer şekilde düzenlendiği yorumu yapılabilecektir (Aksoy ve Halıcıoğlu, 2021, s.76; Çekin, 2020, s.249).

Öte yandan, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik (Mevzuat Bilgi Sistemi, 2020) 04.12.2020 tarih ve 31324 sayılı Resmi Gazetede yayınlanmış olup bu Yönetmeliğin amacı, özel hayatın gizliliği ile kişi temel hak ve özgürlüklerinin korunmasını teminen elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğin korunmasına yönelik usul ve esasları belirlemektir. Yönetmeliğin 2 nci maddesinde elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin tüzel kişi abonelikleri dâhil elektronik haberleşme hizmeti sunulması kapsamında elde ettikleri veriler bakımından uyacakları usul ve esasları kapsadığı hüküm altına alınmıştır. Ayrıca, söz konusu yönetmelik ile ilkeler, açık rıza alma şartları ve aydınlatma yükümlülüğü hususları da düzenlenmiştir.

6698 Sayılı Kişisel Verilerin Korunması Kanunu

Çerezlerin teknik olarak rakam ve harf kombinasyonundan oluşması sebebiyle her durumda kişisel veri niteliğini haiz olabileceği söylenemese de belirli şartlar altında kişisel veri niteliğini haiz olduğu kabul edilebilecektir.

Hukukumuzda da kişisel veri, 6698 sayılı Kanunun 3 üncü maddesinin birinci fıkrasının (d) bendinde *"kişisel veri; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* şeklinde tanımlanmıştır. Ayrıca 6698 sayılı Kanunun gerekçesinde kişisel verinin kapsamı "kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Yalnızca ad, soyad, doğum tarihi ve doğum yeri gibi kişinin kesin teşhisini sağlayan bilgiler değil, kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Bu durum, kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar." şeklinde açıklanmıştır.

6698 sayılı Kanunun ilgili maddesine bakıldığında çerezlerin kişisel veri olduğuna yönelik doğrudan bir düzenleme yer almasa da çerezlerin tek başına ya da diğer bilgilerle ilişkilendirilmesi noktasında Kanun kapsamında çerezlerin kişisel veri olduğunun kabul edilmesi gerektiği değerlendirilmektedir. Bu çerçevede, çerezlerin kişisel veri olarak değerlendirildiği her durumda çerezler vasıtasıyla kişisel verilerin işlenmesi faaliyetinin 6698 sayılı Kanun kapsamında olduğu düşünülebilecektir (Aksoy ve Halıcıoğlu, 2021, s.76).

5809 Sayılı Elektronik Haberleşme Kanunu ile 6698 Sayılı Kişisel Verilerin Korunması Kanunu Arasındaki İlişki

Söz konusu her iki kanunun da çerezlere dair hüküm barındırdığı dikkate alındığında çerezlerin kullanıldığı hallerde hangi kanunun uygulama alanı bulacağı sorusu gündeme gelmektedir.

5809 sayılı EHK'nin 51 inci maddesinin üçüncü fıkrası yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketler tarafından çerezler yoluyla kişisel verilerin işlenmesini kapsamaktadır. Dolayısıyla anılan maddede geçen "işletmeci" tanımından hareketle, 5809 sayılı EHK'nin 51 inci maddesinin üçüncü fıkrası, internet sitesi operatörleri ve OTT (Over The Top) (Netflix, PuhuTV gibi platformlar) hizmetlerine uygulanamamaktadır. İşletmeci kavramı dışında kalan veri sorumluları, 6698 sayılı Kanun kapsamında kişisel veri işleme faaliyetinde bulunacaktır. Ayrıca 5809 sayılı EHK'nin 51 inci maddesinin üçüncü fıkrasında işletmeci olan veri sorumlarının, kişisel verilerin işlenmesi faaliyetinde haberleşmenin sağlanması amacıyla çerezlerin kullanıldığı hallerde aydınlatma yükümlülüğü ve açık rıza alınmasına gerek olmadığı belirtilerek 2002/58/EC sayılı Direktifin 5 inci maddesinin üçüncü fıkrasında düzenlenen Kriter A'ya yer verildiği görülmektedir. Bu kapsamda, çerezler konusunda 5809 sayılı EHK'nin uygulama alanının dar olduğu düşünülmektedir (Çekin, 2020, s.249-250; Aksoy ve Halıcıoğlu, 2021, s.76-77).

6698 sayılı Kanun ve 5809 sayılı EHK arasındaki ilişkinin nasıl olduğu hususunun ortaya konulması bakımından özel kanun genel kanun yorum ilkesine değinmekte fayda görülmektedir. Zira doktrinde de kabul edilen görüşe göre 6698 sayılı Kanun tüm kişisel veri işleme faaliyetlerinin düzenlendiği "genel kanun", 5809 sayılı EHK'nin 51 inci maddesinin üçüncü fıkrası ise elektronik haberleşme kapsamında işletmeciler tarafından çerezlerin kullanılmasını hüküm altına alan "özel kanun" niteliğindedir (Article 29 Data Protection Working Party, 2/2010, s.10; Aksoy ve Halıcıoğlu, 2021, s.77).

Bilindiği üzere, önceki tarihli özel kanun yürürlükteyken sonrasında genel nitelikli yeni kanunun yürürlüğe girdiği durumlarda doktrine göre kanun koyucunun yeni kanunu çıkarma amacına bakılması gerekmektedir. Bu kapsamda, her iki kanunun sistem ve dayandığı ilkelerin birbirine uyumunun olduğu noktada yeni tarihli genel kanunun, eski tarihli özel kanunun kapsamına giren konulara genel şekilde değinerek söz konusu konuların ayrıntılı halinin düzenlenmesini eski tarihli özel kanuna bıraktığı hallerde yeni tarihli genel kanunun eski tarihli özel kanunu yürürlükten kaldırmadığı (Doktrindeki baskın görüşün; önceki tarihli özel kanunun, sonraki tarihli genel kanun ile yürürlükten kaldırılamayacağı yönünde olduğuna dair bkz. Gözler, 2013, Ergül (Haz.), s.103-104); öte yandan yeni tarihli genel kanunun, eski tarihli özel kanunla düzenlenmiş konuları farklı bir şekilde ya da ayrıntılı düzenlediği durumlarda eski tarihli özel kanunu yürürlükten kaldırdığı sonucuna varılmaktadır (Akipek, Akıntürk ve Ateş, 2015, s.102-103). Bu kapsamda, 6698 sayılı Kanunun "genel kanun" ve 5809 sayılı EHK'nin "özel kanun" olduğu, 6698 sayılı Kanunun 5809 sayılı EHK'yi yürürlükten kaldırmadığı da dikkate alındığında ilk olarak özel kanun olan 5809 sayılı EHK'nin uygulama alanı bulması gerekmektedir. Dolayısıyla işletmeciler tarafından kullanıcıların terminal ekipmanına çerez yerleştirildiği hallerde 5809 sayılı EHK'nin 51 inci maddesinin üçüncü fıkrasında yer alan istisnai halin 6698 sayılı Kanun ile genişletilmesi söz konusu olmayacaktır (Aksoy ve Halıcıoğlu, 2021, s.77). Her ne kadar özel kanun uygulama alanı bulsa da, genel kanun niteliğinde olan 6698 sayılı Kanun'da özel düzenleme alanı bulan veya daha üstün şekilde kişi hak ve hürriyetlerinin korunması amaçlanan hallerde 6698 sayılı Kanunun da uygulama alanı bulacağı düşünülmektedir (Çekin, 2019, s.187-188).

6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Çerezler Aracılığıyla Kişisel Verilerin İşlenmesi Şartları

Yukarıda da bahsedildiği üzere, 5809 sayılı EHK kapsamı dışında kalan çerezler yoluyla kişisel verilerin işlenmesi faaliyetlerinde 6698 sayılı Kanun uygulama alanı bulacaktır. Bu kısımda 6698 sayılı Kanun çerçevesinde hangi veri işleme şartlarına dayanılabileceği hususu anlatılacaktır.

6698 sayılı Kanunun 5 inci maddesinde kişisel verilerin işlenme şartları, 6 ncı maddesinde ise özel nitelikli kişisel verilerin işlenme şartları düzenlenmiş olup, söz konusu iki maddede veri işleme şartları farklı esaslara bağlanmıştır.

Bu kapsamda, özel nitelikli olmayan kişisel verilerin hangi hallerde hukuka uygun olarak işlenebileceği şu şekilde hüküm altına alınmıştır;

"(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:
a) Kanunlarda açıkça öngörülmesi.
b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir baş-

kasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

Söz konusu kişisel verilerin işlenme şartları 6698 sayılı Kanunda sınırlı sayıda sayılmış olup bu şartlar dışında başka bir şart getirilerek genişletilemeyecektir (Kişisel Verileri Koruma Kurumu, 2019 b, s.40).

Özel nitelikli kişisel veriler, öğrenilmesi halinde kişilerin ayrımcılığa maruz kalmasına sebep olabilecek (Özel nitelikli kişisel veri tanımı için bkz: Kaya, 2011, s.318-320) bu nedenle daha fazla korunması gereken kişisel verilerdendir. 6698 sayılı Kanunun 6 ncı maddesi uyarınca;

"(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

(2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

(3) Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

(4) Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."

Bu çerçevede, özel nitelikli kişisel verilerin işlenmesi faaliyetinde açık rıza gerekmeyen haller yukarıda yer alan iki halde gerçekleşebilecektir (Aksoy ve Halıcıoğlu, 2021, s.78). Dolayısıyla özel nitelikli kişisel verilerin çerezler yoluyla işlenmesi sıkı şartlara tabidir (Data Protection Commission, 2020, s.15).

Genel nitelikli kişisel veriler açısından ise, ilgili kişinin açık rızasının alınması veya veri sorumlusunun çerezler aracılığıyla kişisel veri işleme faaliyetine ilişkin yapacağı değerlendirme sonucunda Kanunun 5 inci maddesinin ikinci fıkrasında yer alan kişisel veri işleme şartlarını göz önünde bulundurması gerektiği, uygulamada en çok bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması ya da ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hallerinde çerezler vasıtasıyla kişisel verilerin işlenebileceği değerlendirilmektedir.

Bir Sözleşmenin Kurulması veya İfasıyla Doğrudan Doğruya İlgili Olması Kaydıyla, Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesinin Gerekli Olması

Çerezler yoluyla kişisel verilerin işlenmesi faaliyetinde uygulamada en çok karşılaşılabilecek hukuka uygunluk sebeplerinden bir tanesi sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması halidir.

Bu işleme şartına örnek çerez kullanım faaliyeti olarak; kullanıcının bir alışveriş sepetine seçtiği öğeleri eklemesi suretiyle çerezler yoluyla kişisel verilerinin işlenmesi gösterilebilecektir. Zira burada, kullanıcının e-ticaret sitesine girerek alışveriş sepetine belli öğeleri eklemesi ve satın alması ile bir satış sözleşmesinin kurulması ve bu satış sözleşmesi kapsamında kullanıcının kişisel verilerinin işlenmesi söz konusu olmaktadır. Ayrıca, doktrindeki bir görüşe göre; GVKT'nin 6 ncı maddesinin birinci fıkrasının (b) bendinde belirtilen bir sözleşme yapılmadan önce işleme faaliyetinin gerçekleşmesi için ilgili kişinin talepte bulunması şartının 6698 sayılı Kanunda yer almasa da sözleşmenin kurulması veya ifası şartında aranması gerektiği, yoksa ilgili kişilerin rızası olmaksızın verilerinin işlenmesinin söz konusu olacağı üzerinde durulmuştur (Aksoy ve Halıcıoğlu, 2021, s.78-79).

İlgili Kişinin Temel Hak ve Özgürlüklerine Zarar Vermemek Kaydıyla, Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması

Çerezler aracılığıyla kişisel verilerin işlenmesinde 6698 sayılı Kanunun 5 inci maddesi kapsamında uygulamada en çok karşılaşılabilecek bir diğer hukuki sebebin, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri

sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması olduğu düşünülmektedir.

Bu şarta dayanılarak kişisel veri işleme faaliyetinde bulunulması için yarışan menfaatler (ilgili kişilerin temel hak ve özgürlükleri ile veri sorumlusunun menfaati) arasında yapılacak olan değerlendirme sonucunda kişisel verilerin bu hüküm kapsamında işlenip işlenemeyeceğine karar verilmesi gerektiğinden bahisle, söz konusu veri işleme şartı veri işlenmesine ilişkin sınırsız bir yetki olarak değerlendirilemeyecektir. Tam tersine, veri sorumlusunun menfaati ile ilgili kişinin temel hak ve özgürlükleri arasında makul bir denge sağlanması gerekmektedir (Kişisel Verileri Koruma Kurumu, 2019 c, s.78-79). Öte yandan, Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Kararında, yarışan haklar arasında denge testi yapılırken veri sorumluları tarafından şu hususların değerlendirilmesi gerektiği belirtilmiştir;

"...

- *Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması,*

- *Söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi,*

- *Meşru menfaatin halihazırda mevcut, belirli ve açık olması,*

- *İlgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması,*

- *Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması,*

- *Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması,*

- *Kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması,*

- *Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması,*

- *Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması"*

Ayrıca, çerezler vasıtasıyla kişisel verilerin işlenmesinin temel hak ve özgürlükler açısından ağır bir müdahale niteliği taşıması nedeniyle bu müdahalenin salt ekonomik menfaatlerle meşru kabul edilmesi ancak istisnai hallerde söz konusu olmalıdır (Çekin, 2019, s.188-189).

Bu veri işleme şartına örnek olarak, bir internet sitesinin ilgili kişilerin taleplerini internet sunucuları arasında dengeli şekilde dağıtmak suretiyle haberleşmenin sağlanması amacıyla kullanılan yük dengeleme oturum çerezi gösterilebilmektedir.

Aydınlatma Yükümlülüğü ve Açık Rıza Alınması

Çerezlere dair 6698 sayılı Kanun kapsamında işleme şartlarını ele aldıktan sonra değinilmesi gereken bir diğer konu aydınlatma yükümlülüğü ve ilgili kişilerden açık rıza alınmasıdır.

Veri sorumlularının aydınlatma yükümlülüğü, 6698 sayılı Kanunun 10 uncu maddesinde hüküm altına alınmış olup ayrıca, aydınlatma yükümlülüğü kapsamında uyulacak usul ve esasları belirleyen 10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete'de yayınlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ de bulunmaktadır.

Aydınlatma yükümlülüğü, ilgili kişinin talebine bağlı bir yükümlülük değildir. Bu kapsamda, 6698 sayılı Kanunda yer alan işleme şartlarından hangisine dayanılırsa dayanılsın bunlardan bağımsız olarak veri sorumluları tarafından aydınlatma yükümlülüğü yerine getirilmelidir. Aydınlatma yükümlülüğünün yerine getirilmesi ispatı veri sorumlularındadır. Kişisel veri işleme amacı değiştiğinde, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmelidir. Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir (Kişisel Verileri Koruma Kurumu, 2019a, s.13). Diğer taraftan, 6698 sayılı Kanunun 10 uncu maddesinde,

aydınlatma yükümlülüğü yerine getirilirken; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ve 11 inci maddede sayılan diğer hakları hakkında bilgi verilmesi gerektiği belirtilmiştir.

Ayrıca, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5 inci maddesinde ayrıntılı ele alındığı üzere; aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekmektedir. Genel nitelikte ve muğlak ifadeler kullanılmamalıdır. Söz konusu yükümlülük kapsamında gerçekleştirilen bildirimin açık, anlaşılır ve sade bir dille yapılması gerekmektedir. Eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir.

Söz konusu Tebliğ'de aydınlatma yükümlülüğü kapsamında kişisel verilerin, tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerden hangisiyle elde edildiğinin açık bir şekilde belirtilmesi gerektiğinin hükme bağlandığının ifade edilmesinde fayda görülmektedir. Zira, özellikle reklam/pazarlama çerezleri yoluyla kişisel verilerin işlenmesi suretiyle ilgili kişiler aleyhine bir sonucun ortaya çıkması mümkün olup (Aksoy ve Halıcıoğlu, 2021, s.81), bu noktada itiraz etme hakkı, 6698 sayılı Kanunun 11 inci maddesinin birinci fıkrasının (g) bendi "ilgili kişi işlenen verilerinin yalnızca otomatik sistemler vasıtası ile analiz edilmesi yoluyla kişinin kendisi aleyhine bir sonucun çıkmasına itiraz etme hakkına sahiptir." hükmünde düzenlenmiştir. GVKT'den farklı olarak 6698 sayılı Kanun "aleyhine bir sonuç ortaya çıkmasına" vurgu yapmaktadır (Çekin, 2019, s.99).

6698 sayılı Kanun kapsamında uygun açık rızanın alınması hususunda ise esaslı noktalar şunlardır (Kişisel Verileri Koruma Kurumu, (t.y.), s.3; Açık rızanın şartlarına ayrıntılı olarak bkz: Polater, 2019, s.9-15);

- Açık rıza, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile ya da karşı taraftan gelen istek üzerine, onay vermesi anlamını taşır,

- Açık rıza açıklaması, veri işleyene gerçekleştireceği fiil konusunda yol göstermesi hususunda önemlidir, kişi açık rıza açıklaması ile aslında veri sorumlusuna kendi hukuksal değerine ilişkin verdiği kararı bildirmektedir,

- Açık rıza, rıza veren kişinin "olumlu irade beyanı"nı içermelidir,

- 6698 sayılı Kanunun 3 üncü maddesinde yer verilen açık rıza tanımına göre, açık rızanın 3 unsuru bulunmaktadır;

» belirli bir konuya ilişkin olması,
» bilgilendirmeye dayanması,
» özgür iradeyle açıklanması.

29 Veri Koruması Çalışma Grubunun 2 Ekim 2013 Tarih ve 02/2013 Sayılı Çerez Kullanımına İlişkin Rıza Alımına İlişkin Rehberi'nde yer alan çerezlere ilişkin aydınlatma yükümlülüğü ve açık rıza alınmasına dair unsur ve yöntemlerin 6698 sayılı Kanun kapsamında da uygulanabileceği değerlendirilmektedir. Bu kapsamda, açık rıza belirli olmalı ve uygun bilgiye dayanmalıdır. Rıza arandığı anda (ve aynı yerde) çerez kullanımı hakkında açık, kapsamlı ve görünür uyarı sağlanmalıdır. İyi uygulama örneği olarak, ilgili kişi bir internet sitesine göz atmaya başladığında bu uyarının sunulması verilebilir. İnternet sitesine erişildiğinde, internet sitesi tarafından kullanılan farklı tip ve amaçlardaki çerezler hakkında gerekli olan tüm bilgiye ulaşabilmesi gereklidir, bu anlamda internet sitesi belirli bir alanda görünür bir şekilde yer alacak olan bir linkten yararlanabilir. Ayrıca, çerezlerin amaçları, saklama süresi, üçüncü taraf çerez kullanılıyorsa bunlar hakkında bilgi verilmesi gereklidir. Açık rızanın geçerli olması için kullanıcının isteklerinin aktif göstergesi olmalıdır; yine açık rıza ilgili kişinin özgür iradesiyle verilmeli, ilgili kişiler çerezleri kabul etme, reddetme veya ilerleyen süreçte çerez ayarlarını değiştirme imkânına sahip olmalıdır.

Öte yandan, Planet 49 Kararında da (Planet 49 GmbH Kararı, 2019) belirtildiği üzere açık rızanın önceden işaretlenmiş kutucuk yoluyla geçerli bir şekilde oluşturulmadığı, bu anlamda açık rıza alınması gereken çerezler açısından ilgili kişilere sunulacak kutucukların işaretlenmemiş olması ya da çerez panelinde bu çerezlerin pasif olarak sunulması önem arz etmektedir.

Rıza Yorgunluğu

Çerezler hususunda tartışmalı konulardan biri rıza yorgunluğudur. Çerezler yoluyla kişisel verilerin işlenmesinde ilgili kişilerden sık sık açık rıza alınmasının ilgili kişilerde rıza yorgunluğuna sebebiyet verebileceğinden bahisle, açık rıza verilmesinin belli süreyle sınırlanması gerektiği, zira ilgili kişilerde rıza yorgunluğuna yol açabileceği değerlendirilmekte olup, 29 Veri Koruması Çalışma Grubunun 22 Haziran 2010 tarih ve 2/2010 sayılı "Çevrimiçi Davranışsal Reklam Hakkında Görüşü"nde belirtildiği gibi, periyodik hatırlatma süresinin belirlenebileceği düşünülmektedir.

Diğer yandan, EDPB de, e-Gizlilik Tüzük taslağında kullanıcılara kontrolün geri verilerek ve rıza yorgunluğu düzenlenerek mevcut durumun iyileştirilmesine yönelik düzenleme yapılması gerektiğinin altını çizmiştir (European Data Protection Board, 2021, s.3; Aksoy ve Halıcıoğlu, 2021, s.74). Keser Berber, Atabey ve Mert'in de ifade ettiği üzere; rıza yorgunluğuna ilişkin olarak Avrupa Birliğinde, e-Gizlilik Tüzük Taslağı 20a numaralı açıklamasında rıza yorgunluğu ifadesi çıkarılmış olsa da ilgili hükmün lafzından hala zımni olarak rıza yorgunluğuna atıfta bulunduğu şeklinde yorumlanabilecektir (Keser Berber, Atabey ve Mert, 2019, s.70).

Çerez Duvarları (Cookie Walls)

Avrupa Birliği uygulamalarında tartışmalı olan konulardan bir diğeri "çerez duvarları"dır.

Çerez duvarı; bir hizmete erişimin, internet kullanıcısının bilgisayarına çerezlerin yüklenmesini kabul etmesine bağlı hale getirilmesini ifade etmektedir. Başka bir deyişle, internet kullanıcısı siteye erişmek isterse, para veya "veri olarak" bir bedel sağlamakla yükümlüdür, bu da aslında hizmeti ücrete tabi kılmaktadır (Commission Nationale De L'informatique Et Des Libertés (CNIL), (t.y.)). Avrupa Birliği uygulamalarına bakıldığında eskiye nazaran yakın dönemde çerez duvarlarının belli şartlar altında kullanılmasına ılımlı bir yaklaşım olduğu söylenebilecektir.

CNIL, 2019 tarihli Kararıyla çerez duvarları konusunda mutlak şekilde yasaklayan yönlendirmede bulunmuş iken Fransız Danıştayı 19 Haziran 2020 tarihli Kararıyla CNIL'in söz konusu kararını iptal etmiştir ve özellikle çerezlerin reddedilmesi durumunda kullanıcılara sunulan gerçek ve tatmin edici alternatifler dikkate alınarak rızanın özgürce verildiğinin somut olaya göre değerlendirilmesi gerektiğine hükmedilmiştir. CNIL, bunun üzerine çerez duvarlarına dair 31.05.2021 tarihli bir duyuru yayınlamıştır. Söz konusu duyuruda, en yaygın örneğin, internet sitesi yayıncısı tarafından içeriğe erişimin reklam çerezlerinin kabul edilmesi veya makul bir tutarın ödenmesi suretiyle olduğu belirtilmiştir. Ayrıca verileri karşılık olarak kullanmanın iki riski olduğuna dikkat çekilmiştir (CNIL, (t.y.));

- En savunmasız kişiler, hizmetlere ücretsiz olarak erişmek veya ek ücret almak için verilerini verirken, daha varlıklı olan diğerlerinin kişisel veri sağlamadan veya kişisel verilerine para özelliği kazandırmadan bir hizmete erişmelerine izin veren bir abone bedelini ödeyebilmesi,

- Belirli üçüncü taraflar karşısında anonimliği koruma olasılığının birkaç kişi dışında diğerleri için hariç tutulması.

Bu örnek modelin zaten yaygın olmasına rağmen, insanların verileri üzerindeki kontrolünü güçlendirmek veya internet sitelerinin veri toplama dışında finanse edilmesine izin vermek için alternatiflerin mevcut olduğu ifade edilmiş, bunlardan birinin verinin toplu yönetimi, diğerinin ise dijital cüzdanlar olabileceği de belirtilmiştir.

Yine, İtalyan Veri Koruma Otoritesi de rehberinde (Garante Per La Protezione Dei Dati Personali (GDPD), 2021 s.24) kullanıcının çerezlerin veya diğer izleme araçlarının kullanılmasına izin vermek zorunda olduğu bir 'al ya da bırak' mekanizması anlamına gelen çerez duvarının özgür rızaya ilişkin gerekliliklerle uyumlu olarak değerlendirilemeyeceği, buna göre, ilgili kişinin çerezlerin veya diğer izleme araçlarının saklanmasına ve kullanılmasına rıza vermeden eşdeğer içeriğe veya hizmetlere erişme seçeneği sunduğu durumlar dışında (olay bazında doğrulanması halinde) mevzuata uygun olarak kabul edilmeyeceği, her halükarda yerine getirilmesi gereken önemli bir koşulun önerilen alternatif ile kişisel verilerin hukuka uygun, adil bir şekilde işlenmesi olduğu; yani hukuka uygunluk, hakkaniyet ve şeffaflık ilkesine uyumun esas olduğu belirtilmiştir.

Öte yandan, e-Gizlilik Tüzük Taslağının 20aaaa (E-Gizlilik Tüzük Taslağı, 2021) numaralı açıklamasında da kullanıcıların çerezler ve benzer tekniklerin amaçları hakkında açık, öz ve kullanıcı dostu şekilde bilgilendirilmesi ve kullanıcılara adil alternatif sunulması suretiyle çerez duvarının kullanılabileceği düzenlenmiştir (Aksoy ve Halıcıoğlu, 2021, s.73).

Bu kapsamda, internet sitesine erişim için çerez duvarının kullanılması ve rıza verilmediğinde içeriğe erişilememesi hizmetin açık rıza şartına bağlanması olarak değerlendirilebilecektir; ancak son dönemdeki Avrupa Birliği uygulamaları da dikkate alındığında, ilgili kişilere çerezlerin amaçları hakkında açık, sade, kullanıcı dostu bir bilgilendirme yapılarak çerez duvarının reddedilmesi halinde adil alternatiflerin sunulmasının mümkün olduğu düşünülmektedir.

Veri Sorumlusu

Üçüncü taraf çerez kullanılan internet sitelerinde taraflar arasında sorumluluğun nasıl olacağı hususu tartışmalı konulardandır. Bu kapsamda, üçüncü taraf çerezlerin kullanılması halinde hem internet sitesi sahibi hem de üçüncü tarafın, kullanıcıların çerezler hakkında net bir şekilde bilgilendirilmesini sağlamak ve

rıza almasını sağlamakla yükümlü olduğunu söylemek mümkündür. Uygulamada kullanıcı ile arayüz üzerinde daha az doğrudan kontrolü olan üçüncü bir tarafın bunu başarmasının ise çok daha zor olduğunu belirtmekte fayda vardır. Bundan dolayı ICO, internet sitesi sahibi ve üçüncü taraf arasında sözleşme yapılması gerektiği ve bunun da üçüncü taraf çerezler hakkında bilgi sağlamak ve rıza almak için uygun adımların atılacağına dair güvence sağlayabileceğini ifade etmektedir (ICO, 2019, s.33-34; Aksoy ve Halıcıoğlu, 2021, s. 74).

Bilindiği üzere, GVKT'nin "Müşterek veri sorumluları" başlıklı 26 ncı maddesinde iki veya daha fazla veri sorumlusunun işleme amaç ve vasıtalarını birlikte belirledikleri hallerde ortak veri sorumlusu olacağı düzenlenmiştir. Bu maddeye göre ilgili kişiler GVKT'den kaynaklanan haklarını müşterek veri sorumlularından herhangi birine karşı ileri sürebilecektir (Develioğlu, 2017, s.206-207). Dolayısıyla GVKT'nin açık şekilde ortak veri sorumluluğu kurumunu düzenlediği görülmektedir. Bu çerçevede, müşterek veri sorumluluğu hakkında ABAD'ın Fashion ID kararına da değinmekte fayda görülmektedir. Fashion ID çevrimiçi satış yapan internet sitesi olup, bu internet sitesine "Facebook Beğen" butonunu yerleştirmiştir. Böylece ziyaretçilerin internet sitesini kullanmaları sonucu kişisel verileri Facebook İrlanda'ya aktarılmıştır. Söz konusu bu aktarımın ise kullanıcıların söz konusu beğen butonuna tıklayıp tıklamadıklarına bakılmaksızın gerçekleştirildiği anlaşılmıştır.

Daha sonra bu olay ABAD önüne gelmiştir ve ABAD, Fashion ID'nin hangi verilerin Facebook İrlanda'ya aktarılacağı ve sonraki işleme faaliyetleri açısından veri sorumlusu olmadığı; söz konusu eklentiye internet sitesinde yer verilerek verilerin elde edilmesi ve aktarılması hususunda Fashion ID ve Facebook İrlanda'nın ortak veri sorumlusu olduğuna karar vermiştir (Avrupa Adalet Divanı: Fashion ID Kararı, (t.y.); Fashion ID Kararı, 2019; Dülger, 2021, s.9-11).

Türk Hukukunda ise 6698 sayılı Kanunda ortak veri sorumluluğu kavramına dair herhangi bir düzenleme yer almamakla birlikte, Kişisel Verileri Koruma Kurulunun Araç Kiralama Sektöründeki Kara Liste Uygulamaları Hakkında 23.12.2021 tarih ve 2021/1304 sayılı İlke Kararı ile araç kiralama şirketleri ve yazılım şirketlerinin ortak veri sorumlusu olarak değerlendirileceğine karar verilmiştir. Bu da göstermektedir ki; 6698 sayılı Kanunda ortak veri sorumlusu kurumuna yer verilmese de İlke Kararıyla söz konusu kavramın uygulanabilir olduğu kabul edilmiştir. Dolayısıyla, çerezler aracılığıyla kişisel verilerin işlenmesi ve üçüncü taraf çerez yerleştirilmesi söz konusu olduğunda, yukarıda yer alan açıklamalar ışığında tarafların sorumluluğunun her somut olay özelinde değerlendirilebileceği düşünülmektedir.

Yurtdışına Veri Aktarımı

Kişisel verilerin yurtdışına aktarımı 6698 sayılı Kanunun 9 uncu maddesinde hükme bağlanmış olup, söz konusu maddenin birinci fıkrasına göre ilk aktarım şartı ilgili kişinin açık rızasının alınmasıdır. Açık rıza alınması şartı dışında, 6698 sayılı Kanunun 5 inci maddesinin ikinci fıkrası veya 6 ncı maddesinin üçüncü fıkrasında belirtilen kişisel veri işleme şartlarının olması kaydıyla yeterli korumanın bulunması veya yeterli korumanın bulunmaması halinde Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ile Kişisel Verileri Koruma Kurulunun izninin bulunması durumlarında ilgili kişinin kişisel verileri yurt dışına aktarılabilecektir (Aşıkoğlu ve Uzun, 2020, s.926-928 ; Akçalı Gür, 2019, s.868-870). Belirtmek gerekir ki; Kişisel Verileri Koruma Kurulu şu ana kadar herhangi bir ülkeyi güvenli ülke olarak ilan etmiş değildir. Öte yandan, yurtdışına veri aktarımında veri sorumlularınca hazırlanacak taahhütnamede yer alacak asgari unsurlar (Kişisel Verileri Koruma Kurumu, 2018) ve taahhütnamelerde dikkat edilmesi gereken hususlara (Kişisel Verileri Koruma Kurumu, 2020) ilişkin duyuru Kurumun resmi internet sayfasında duyurulmuştur. Şimdiye kadar Kişisel Verileri Koruma Kurulu tarafından yurt dışına kişisel veri aktarımı yapılması hususundaki 7 tane Taahhütname başvurusu 6698 sayılı Kanunun 9 uncu maddesinin ikinci fıkrasının (b) bendi kapsamında değerlendirilmiş ve veri aktarımlarına izin verilmiştir.

Bu çerçevede, Türkiye'de faaliyet gösteren internet sitelerinin büyük çoğunluğunun yurtdışında yerleşik olan şirketler vasıtasıyla çerez kullandığı dikkate alındığında, çerezler aracılığıyla yurtdışına veri aktarımı faaliyeti gerçekleştiği ve bu işleme faaliyetinin 6698 sayılı Kanunun 9 uncu maddesindeki şartlara uygun şekilde yapılması gerektiği söylenebilecektir. Özellikle, açık rızayla kişisel verilerin yurtdışına aktarıldığı hallerde, kişisel verilerin kimlere ve hangi amaçla aktarılabileceği hususunda açık, anlaşılır ve sade bir dille ilgili kişilerin bilgilendirilmesi gerekmektedir.

Öte yandan, Kişisel Verileri Koruma Kurulunun 10.03.2022 tarih ve 2022/229 sayılı Kararı ile; *"...Kanunun 9 uncu maddesinde yer alan aktarım usullerinden herhangi birine dayanılmaksızın çerezler vasıtasıyla yurt dışına veri aktarıldığı..."*ndan bahisle idari para cezası uygulanmasına karar verilmiştir.

6698 sayılı Kanunun 9 uncu maddesinin, GVKT'de hüküm altına alınan yurtdışına veri aktarımı düzenlemesine kıyasla uygulama alanının çok dar olduğundan bahisle, şu aşamada çerez yerleştiren veri sorumluları nezdinde yurt dışına aktarım faaliyeti gerçekleştirilirken açık rıza alınması ya da taahhütname fonksiyo-

nunun işletilmesinden başka bir mekanizma bulunmamaktadır. Bu kapsamda, 6698 sayılı Kanunda yer alan yurtdışına veri aktarılmasına yönelik düzenlemenin GVKT'dekine benzer şekilde değiştirilerek uygulamada yaşanılan aksamaların önüne geçilebileceği değerlendirilmektedir (Aşıkoğlu ve Uzun, 2020, s.966-967).

SONUÇ

Çerezlerin teknik olarak rakam ve harf kombinasyonundan oluşması sebebiyle her durumda kişisel veri niteliğini haiz olabileceği söylenemese de belirli şartlar altında kişisel veri niteliğini haiz olduğu kabul edilebilecektir. Özellikle çevrimiçi davranışsal reklamcılık uygulamalarında çevrimiçi izleme tekniklerinde kullanılan çerezler, kullanıcıların kişisel bilgileri (adı, e-posta adresi, telefon numarası vb.) de dahil olmak üzere birçok farklı bilgiyi içine alabilmektedir. Kısacası kişisel verilerin elde edilme yöntemlerinden biri çerezlerdir.

Avrupa Birliğine bakıldığında, 2002/58/EC sayılı Direktifin iletişimin gizliliği başlıklı 5 inci maddesinin üçüncü fıkrası çerezler vasıtasıyla kişisel verilerin işlenmesi açısından önem teşkil etmektedir. Bu çerçevede, çerez yerleştirilmesi suretiyle kişisel verilerin işlenmesi bakımından bilgilendirme yükümlülüğünün yerine getirilerek kullanıcı rızasının alınması gerekmekte olup, geçerli bir rıza için gerekli ana unsurlar şunlardır; rızanın belirli olması ve uygun bilgiye dayanması, kişisel veri işlenmesi faaliyeti başlamadan önce verilmesi, kullanıcının isteklerinin aktif göstergesi olması ve özgürce verilmesi.

Avrupa Birliği uygulamasında, çerezler aracılığıyla kişisel verilerin işlenmesi noktasında genel kural bilgilendirme yükümlülüğünün yerine getirilerek kullanıcı rızasının alınması olmakla birlikte, 2002/58/EC sayılı Direktifin 5 inci maddesinin üçüncü fıkrasında yer alan Kriter A "tek amacı (sole purpose) bir iletişimin elektronik iletişim ağı üzerindeki iletimini gerçekleştirmek" veya Kriter B "abonenin veya kullanıcının hizmet sağlamak için açıkça talep ettiği, bilgi toplum hizmetleri için kesinlikle gerekli (strictly necessary)" kapsamına giren çerezler bakımından rıza muafiyeti bulunmaktadır.

Türk hukukunda çerezlerin yer aldığı hukuki düzenleme 5809 sayılı EHK'nin 51 inci maddesinin üçüncü fıkrasıdır, söz konusu fıkra ise sadece elektronik haberleşme işletmecileri açısından uygulanabilir niteliktedir. Dolayısıyla, işletmeci kavramı dışında kalan veri sorumluları, 6698 sayılı Kanun kapsamında kişisel veri işleme faaliyetinde bulunabilecektir.

5809 sayılı EHK'nin 51 inci maddesinin üçüncü fıkrasının 2002/58/EC sayılı Direktif ile kısmi uyum sağladığı, Avrupa Birliğindeki güncel gelişmelerden ve tartışmalardan uzak kaldığı, yalnızca işletmeciler açısından uygulanabilirliği dikkate alındığında, kişisel verilerin korunması ilke ve yöntemlerini düzenleyen 6698 sayılı Kanuna çerezler ve benzer teknolojileri de kapsayan bu yönde hüküm konulmasının uygun olabileceği değerlendirilmektedir.

Yukarıda ayrıntılı olarak bahsettiğimiz çerezler vasıtasıyla kişisel verilerin işlenmesine hukuki geçerlilik sağlayacak "açık rıza" kavramının unsurları doğrultusunda ilgili kişiden alınan açık rızanın hukuka uygun olup olmadığı en önemli hususlardan biridir. Açık ve anlaşılır biçimde çerezlerin tipi, kullanım amaçları, kullanım periyodu, üçüncü taraf çerez kullanılıyorsa bununla ilgili detaylar hususunda ilgili kişiler/kullanıcılar bilgilendirilmeli, açık rızanın geçerli olması için kullanıcının isteklerinin aktif göstergesi olmalıdır; yine açık rıza ilgili kişinin özgür iradesiyle verilmeli, ilgili kişiler çerezleri kabul etme, reddetme veya ilerleyen süreçte çerez ayarlarını değiştirme imkânına sahip olmalıdır.

Açık rıza dışında veri sorumlusunun çerezler aracılığıyla kişisel veri işleme faaliyetine ilişkin yapacağı değerlendirme sonucunda Kanunun 5 inci maddesinin ikinci fıkrasında yer alan kişisel veri işleme şartlarını göz önünde bulundurması gerektiği, uygulamada en çok bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması veya ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hallerinde çerezler vasıtasıyla kişisel verilerin işlenebileceği değerlendirilmektedir.

Türkiye'de faaliyet gösteren internet sitelerinin büyük çoğunluğunun yurtdışında yerleşik olan şirketler vasıtasıyla çerez kullandığı dikkate alındığında, çerezler aracılığıyla yurtdışına veri aktarımı faaliyeti gerçekleşmekte ve bu işleme faaliyetinin 6698 sayılı Kanunun 9 uncu maddesindeki şartlara uygun şekilde yapılması gerekmektedir. 6698 sayılı Kanunun uygulama alanının şu aşamada GVKT'deki düzenlemeye kıyasen dar olduğu, güvenli ülkeler ilan edilene kadar açık rıza alınması ya da taahhütname yoluna gidilmesinden başka bir mekanizma bulunmadığı söylenebilecektir. Bu kapsamda, 6698 sayılı Kanunun ilgili maddesinin GVKT'dekine benzer şekilde değiştirilerek uygulamada yaşanılan aksamaların önüne geçilebilecektir. ◆

KAYNAKÇA

◊ Akçalı Gür B. (2019). Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi. Cilt 25, Sayı 2. https://dergipark.org.tr/tr/download/article-file/902576 adresinden 21.04.2022 tarihinde alınmıştır.

◊ Akipek J., Akıntürk T., ve Ateş D. (2015). Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku. İstanbul: Beta

◊ Aksoy H. C., ve Halıcıoğlu M. (2021). AB ve Türk Hukuklarında Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme. Kişisel Verileri Koruma Kurumu Dergisi. Cilt 3, Sayı 1. https://dergipark.org.tr/tr/download/article-file/1788317 adresinden 02.04.2022 tarihinde alınmıştır.

◊ Alternatif Bilişim Derneği. (2013). Çevrimiçi Davranışsal Reklamcılık (ÇDR) Kapsamında 'Kişisel Verilerin Korunması Kanunu Tasarısı' Hakkında Alternatif Bilişim Derneği'nin Görüşleri. Docplayer. https://docplayer.biz.tr/748024-Kisisel-veriler-ilgili-kisinin-acik-rizasi-olmadan-islenemez.html adresinden 15.03.2022 tarihinde alınmıştır.

◊ Aşıkoğlu Ş. İ., ve Uzun F. B. (2020). Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3683903 adresinden 21.04.2022 tarihinde alınmıştır.

◊ Avrupa Adalet Divanı: Fashion ID Kararı. (t.y.). zumbul.av.tr. https://www.zumbul.av.tr/en/data-privacy/like-button adresinden 22.04.2022 tarihinde alınmıştır.

◊ Ayözger A. Ç. (2016). Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması. (Doktora Tezi). İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul

◊ Article 29 Data Protection Working Party. (2010). Opinion 2/2010 on online behavioural advertising, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf adresinden 19.02.2022 tarihinde alınmıştır.

◊ Article 29 Data Protection Working Party. (2012). Opinion 04/2012 on Cookie Consent Exemption. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf adresinden 11.03.2022 tarihinde alınmıştır.

◊ Article 29 Data Protection Working Party. (2013). Working Document 02/2013 providing guidance on obtaining consent for Cookies. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf adresinden 21.03.2022 tarihinde alınmıştır.

◊ Carey P. (2018). Data Protection (A Practical Guide to UK and EU law) (Fifth edition). United Kingdom: Oxford University Pres

◊ Commission Nationale De L'informatique Et Des Libertés (CNIL). (t.y.). Cookie walls et monétisation des données personnelles: les enjeux juridiques et éthiques. https://www.cnil.fr/fr/cookie-walls-et-monetisation-des-donnees-personnelles-les-enjeux-juridiques-et-ethiques adresinden 20.04.2022 tarihinde alınmıştır.

◊ Cookies, the GDPR, and the ePrivacy Directive. (t.y.). GDPR.EU. https://gdpr.eu/cookies/ adresinden 13.04.2022 tarihinde alınmıştır.

◊ Çekin M. S. (2019). Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu. İstanbul: On İki Levha Yayıncılık

◊ Çekin M. S. (2020). Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku. İstanbul: On İki Levha Yayıncılık

◊ Data Protection Commission. (2020). Guidance on Cookies and Other Tracking Technologies. https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf adresinden 07.04.2022 tarihinde alınmıştır.

◊ Develioğlu H. M. (2017). 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul: On İki Levha Yayıncılık

◊ Doğan B., ve Bozkurt T. (2010). Kişisel Verilerin Korunması Çerçevesinde Çerezler; Türleri, Kullanımları ve Uygulama Örnekleriyle. Lexpera Blog. https://blog.lexpera.com.tr/kisisel-verilerin-korunmasi-cercevesinde-cerezler-turleri-kullanimlari-ve-uygulama-ornekleriyle/ adresinden 18.02.2022 tarihinde alınmıştır.

◊ Dülger M. V. (2021). GDPR'da Bulunan Ancak KVKK'da Yer Verilmeyen Bir Kavram: Ortak Veri Sorumlusu Kavramı ve Güncel Kararlar Işığında Değerlendirilmesi. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792323 adresinden 22.04.2022 tarihinde alınmıştır.

◊ E-Gizlilik Tüzük Taslağı. (2021). https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf adresinden 28.03.2022 tarihinde alınmıştır.

◊ Eur-Lex. (2022 a). Directive 2002/58/EC of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 adresinden 16.03.2022 tarihinde alınmıştır.

◊ Eur-Lex. (2022b). Directive 2009/136/EC Of The European Parliament And Of The Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136 adresinden 15.03.2022 tarihinde alınmıştır.

◊ European Data Protection Board. (2021). Statement 03/2021 on the ePrivacy Regulation Adopted on 9 March 2021. https://edpb.europa.eu/system/files/2021-03/edpb_statement_032021_eprivacy_regulation_en_0.pdf adresinden 24.03.2022 tarihinde alınmıştır.

◊ European Union Agency for Fundamental Rights and Council of Europe. (2018). Handbook on European data protection law 2018 Edition. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf adresinden 15.03.2022 tarihinde alınmıştır.

◊ Fashion ID Kararı. (2019). EurLex. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0040 adresinden 29.04.2022 tarihinde alınmıştır.

◊ Garante Per La Protezione Dei Dati Personali (GDPD). (2021). Guidelines on the use of cookies and other tracking tools", 2021, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876#english adresinden 20.02.2022 tarihinde alınmıştır.

◊ Gözler K. (2013). Yorum İlkeleri. Kamu Hukukçuları Platformu Anayasa Hukukunda Yorum ve Norm Somutlaşması, Ergül O. (Haz.), (s.15-119). Ankara: Türkiye Barolar Birliği Yayınları

◊ Herberger N. (2013). Freedom of Expression and The Dutch Cookie-Wall. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2197251 adresinden 19.02.2022 tarihinde alınmıştır.

◊ HTTP Nedir? (t.y.). Mediaclick. https://www.mediaclick.com.tr/blog/http-nedir adresinden 19.02.2022 tarihinde alınmıştır.

◊ IAB Türkiye. (2019). Çerez (Cookie). https://iabtr.org/UploadFiles/Reports/iab_Cookie8102019172025.pdf adresinden 18.02.2022 tarihinde alınmıştır.

◊ Information Commissioner's Office (ICO). (2019). Guidance on the use of cookies and similar Technologies. https://ico.org.uk/media/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf adresinden 12.07.2023 tarihinde alınmıştır.

◊ Karaarslan E., Eren M. B., ve Koç S. (2014). Çevrimiçi Mahremiyet: Teknik ve Hukuksal Durum İncelemesi. inet-tr'14 - XIX. Türkiye'de İnternet Konferansı Bildirileri, (s.187-195). İzmir: İnternet Teknolojileri Derneği

◊ Kaya C. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi. İÜHFM. Cilt LXIX, Sayı l-2. https://dergipark.org.tr/tr/download/article-file/97634 adresinden 15.04.2022 tarihinde alınmıştır.

◊ Keser Berber L. (2014). Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulama Özelinde Kişisel Verilerin Korunması, İstanbul: On İki Levha Yayıncılık

◊ Keser Berber L., Atabey A., ve Mert M. (2019). E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler. Kişisel Verileri Koruma Kurumu Dergisi. Cilt 1, Sayı 2. https://dergipark.org.tr/tr/download/article-file/904846 adresinden 12.04.2022 tarihinde alınmıştır.

◊ Kişisel Verileri Koruma Kurumu. (2018). Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar. https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar adresinden 21.04.2022 tarihinde alınmıştır.

◊ Kişisel Verileri Koruma Kurumu. 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/5434/2019-78 adresinden 17.04.2022 tarihinde alınmıştır.

◊ Kişisel Verileri Koruma Kurumu. (2019 a). Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf adresinden 19.04.2022 tarihinde alınmıştır.

◊ Kişisel Verileri Koruma Kurumu. (2019 b). 100 Soruda Kişisel Verilerin Korunması Kanunu. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf adresinden 15.04.2022 tarihinde alınmıştır.

◊ Kişisel Verileri Koruma Kurumu. (2019 c). Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF adresinden 14.04.2022 tarihinde alınmıştır.

◊ Kişisel Verileri Koruma Kurumu. (2020). Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru. https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU adresinden 21.04.2022 tarihinde alınmıştır.

◊ Kişisel Verileri Koruma Kurumu. Araç Kiralama Sektöründeki Kara Liste Uygulamaları Hakkında 23.12.2021 tarih ve 2021/1304 sayılı İlke Kararı. https://www.resmigazete.gov.tr/eskiler/2022/01/20220120-10.pdf adresinden 22.04.2022 tarihinde alınmıştır.

◊ Kişisel Verileri Koruma Kurumu. 10/03/2022 tarih ve 2022/229 sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/7275/2022-229 adresinden 23.05.2022 tarihinde alınmıştır.

◊ Kişisel Verileri Koruma Kurumu. (t.y.). Açık Rıza. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf adresinden 19.04.2022 tarihinde alınmıştır.

◊ Küzeci E. (2019). Kişisel Verilerin Korunması. Ankara: Turhan Kitabevi

◊ La Agencia Española de Protección de Datos (AEPD). (2021). Guide on use of cookies. https://www.aepd.es/es/documento/guia-cookies-en.pdf adresinden 12.07.2023 tarihinde alınmıştır.

◊ Mevzuat Bilgi Sistemi. (2020). Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=38663&MevzuatTur=7&MevzuatTertip=5 adresinden 13.04.2022 tarihinde alınmıştır.

◊ Planet 49 GmbH. Curia.Europa.EU. https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125en.pdf adresinden 10.04.2022 tarihinde alınmıştır.

◊ Polater S. (2019). Kişisel Verilerin Reklam Amaçlı İşlenmesinde Hukuka Uygunluk Sebepleri. Kişisel Verileri Koruma Kurumu Dergisi. Cilt 1, Sayı 1. https://dergipark.org.tr/tr/download/article-file/741785 adresinden 02.03.2022 tarihinde alınmıştır.

◊ Popoli A. R. (2012). Cookies and Electronic Commerce: a Survey About Actual Knowledge of the Issues Concerning Privacy. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2187496 adresinden 05.05.2022 tarihinde alınmıştır.

◊ Turan S. (2020). Çevrimiçi Mahkumiyet: Çerezler Karşısında Özgür İrade Ütopyası. Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku Marmara Hukuk Bilimsel Toplantılar Serisi-I, Keser Berber L., ve Bilgili A. C. (Yay. haz.), (s.121-135). İstanbul: On İki Levha Yayıncılık

◊ Zorer U. (2019). Çerezler Hakkında Hukuki Değerlendirme. Medium.com. https://medium.com/@umutzorer/%C3%A7erezler-hakk%C4%B1nda-hukuki-de%C4%9Ferlendirme-44c58d3eba32 adresinden 11.03.2022 tarihinde alınmıştır.

HEDEFLİ REKLAMCILIK UYGULAMALARININ KİŞİSEL VERİLERİN KORUNMASI HUKUKU AÇISINDAN DEĞERLENDİRİLMESİ

Meryem Betül MURATOĞLU

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "E-Ticaret Sektöründe Profilleme ve Otomatik Karar Alma Uygulamaları Bakımından Kişisel Verilerin Korunması" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Çevrim içi ortamlarda izleme teknolojilerinin gelişmesi ve çeşitlenmesiyle birlikte bireylerin her bir adımı takip edilip kaydedilmekte ve bu adımlar dijital ayak izlerini oluşturmaktadır. Dijital ayak izleri, bilinçli bir şekilde ve isteyerek yapılan beğeni, paylaşım, yorum gibi verileri içerebileceği gibi kullanıcının farkında olmayacağı şekilde toplanan arama geçmişi, çevrim içi davranışları, IP adresi, konum verilerini de içerebilmektedir. Ancak dijital ayak izlerini oluşturan ve sınırsız bir boyutta toplanabilecek bu veriler, tek başına bir anlam ifade etmeyecektir. Dolayısıyla veriyi kullanma becerisinin gelişmesiyle bu büyük miktardaki anlamsız verinin anlamlı bir hale getirilerek stratejik bilgilere dönüştürülebilmesi amacıyla veri madenciliği metotları ile aralarındaki kalıp ve ilişkiler ortaya çıkarılmakta, buna bağlı olarak kullanıcı hakkında yapılan çıkarım veya türetilen yeni veriler ile kullanıcıların profili oluşturulmaktadır. İlk aşamada herhangi bir anlam ifade etmeyen büyük verinin profilleme ile anlamlı ve stratejik bilgilere dönüştürülmesinden sonra, daha akıllıca seçimler yapılması ve yargılara varılması amacıyla bu bilgiler tamamen otomatik işleyen karar alma mekanizmalarına dayanak olmaktadır.

Dijital dünyadaki profilleme ve otomatik karar alma uygulamalarının bir yansıması olarak karşımıza çıkan hedefli reklamlar, geleneksel reklamcılık yöntemlerindeki kitlesel reklamlara göre genellikle doğru kişiye doğru zamanda ve doğru bağlamda ulaşılabilmesini amaçlamaktadır. Bu sayede, ilgi ve alaka düzeyine göre reklam faaliyetleri yürütülerek ekonomik açıdan bir fayda sağlamak istenmektedir. Reklamların hedeflenmesi sürecinde verinin temel bileşen olması, büyük miktarda ve çeşitlilikte veri elde edilmesi gerektiği anlayışını yerleştirmiştir. Özellikle yapılan hedeflemenin kişi hakkında oluşturulan varsayımlara dayandığı göz önünde bulundurulduğunda doğruluk ve tutarlılığı sağlamak için amaçlanan kullanıma uygun boyut ve çeşitlilikte verilerin elde edilmesi daha önemli hale gelmektedir.

Diğer taraftan, söz konusu reklamların büyük miktarda veriden beslenmesi, bireyler özelinde karar alınmasını sağlayan ve onları belirlenebilir kılan kişisel veriler açısından birtakım riskleri barındırması mümkündür. Zira bu otomatik kararlarda, profilleme sonucunda oluşturulan çıkarımsal veya türetilmiş verilere dayanılmakla birlikte doğruluğu kesin olmayan bu bilgilere dayanılarak kişi hakkında hukuki sonuçlar doğuran veya kendisini kayda değer ölçüde etkileyen bir kararın alınması da muhtemeldir. Çevrim içi ortamdaki bir reklamın, bireyler üzerinde hukuki veya benzer ölçüdeki sonuçlara yol açmayacağı düşünülse de dijital ayak izlerinin sınırsızca izlenebilmesi ve bu yolla satın alma davranışlarının manipüle edilmek istenmesi, bireyler üzerinde ekonomik sonuçlar doğurabilecek fiyat ayrımcılığı veya fiyat yönlendirmesi gibi olumsuz sonuçlara yol açabilecektir. Dolayısıyla kişisel verilerin kapalı kutu olarak tabir edilebilecek yollarla işlendiği hedefli reklamcılık uygulamalarında kişisel verilerin korunması ve bu uygulamaların veri koruma düzenlemeleri ışığında hukuka uygunluğunun değerlendirilmesi önem arz etmektedir. Bu çalışma kapsamında hedefli reklamcılık uygulamaları, kişisel verilerin korunması yönüyle 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Avrupa Birliğindeki düzenleme ve kararlar özelinde incelenecektir.

HEDEFLİ REKLAMCILIK

Hedefli reklamcılık, kullanıcı hakkında çeşitli veri kaynaklarından elde edilen veriye dayalı olarak kullanıcıların ilgi alanlarına göre hedeflenmesini ifade eder. Algoritmik sistemler olan çevrim içi hedefleme sistemleri, belirli bir kişi veya grubun ilgisini çekebilecek içeriğin tahmin edilmesi ve davranışların yönlendirilmesi amacıyla bir döngüde çalışmaya devam eder. Diğer bir deyişle, çevrim içi izleme yöntemleri ile veriler toplanır ve analiz edilerek kullanıcının profili oluşturulur, kullanıcının ilgisini çekebilecek içerikler tahmin edilir ve kullanıcının hedefleneceği içeriğe karar verilir, sonrasında kullanıcının bu içeriğe verdiği yanıtlara ilişkin veriler toplanarak yinelemeli bir döngü ile sistem geri beslenir (Centre for Data Ethics and Innovation, 2020). Öte yandan çevrim içi izleme yöntemleriyle elde edilen verilerin analiz edilmesi sonucunda bireyler hakkında çıkarımsal ve türetilmiş veriler elde edilir. Çıkarımsal ve türetilmiş veriler doğrudan kişi tarafından sağlanan veya kullanıcının gözlemlenmesiyle elde edilen veriler olmayıp diğer verilerden oluşturulan yeni verilerdir. Türetilmiş veri, eldeki verilerden yeni bir veri oluşturulması iken çıkarımsal veriler davranış tahminleri oluşturmak için veriler arasındaki bağlantıların tespitinin bir sonucudur (Organisation for Economic Co-operation and Development, 2014). Profilleme sonucunda elde edilen bu veriler ile demografik, davranışsal, ilgi alanları, konum gibi bilgiler üzerinden kişi veya kişi gruplarına yönelik hedefleme yapılması mümkündür. Örneğin, yeni bir ürün için tüketicilere ulaşmak isteyen bir reklam veren yakın zamanda reklama konu ürün kategorisi ile ilgili arama yapılması ve benzer internet sayfalarının ziyaret edilmesi, reklam verenin internet sitesinin daha önce ziyaret edilmiş olması, reklam verenin mevcut müşterileriyle benzer demografik profile sahip olunması, yaşam tarzı çıkarımlarına göre yüksek olasılıkla ürüne ilgi gösterilebilecek olması gibi yaklaşımlarla kişi veya kişi gruplarını hedefleyebilir (Adshead, Forsyth, Wood, & Wilkinson, 2019).

Hedefli reklamlar, özellikle çevrim içi izleme teknolojilerinin sürekli olarak gelişmesi ve verinin elde edilebileceği kaynakların genişlemesi sebebiyle çevrim içi hedeflemenin daha tutarlı bir şekilde yapılabilmesi sayesinde reklamın başarısına katkıda bulunmaktadır. Bir diğer katkısı ise reklam yoluyla hizmet veya içeriğe erişen ziyaretçilere ilişkin verilerin analiz edilmesiyle reklamların başarısının ölçülebilmesini sağlamasıdır (Fourberg, ve diğerleri, 2021). Bu reklam türleri, çevrim içi reklamcılık yöntemleri arasında yer alan arama motoru reklamları ve görüntülü reklamlar yoluyla uygulanabilir. Arama motoru reklamları, kullanıcının arama yaptığı kelime veya kelime grubuna bağlı olarak arama sonuçlarında reklam verenlerin internet sitesinin organik arama sonuçlarıyla birlikte gösterilmesini sağlar. Genellikle bu reklam yönteminde görüntülenecek reklam içeriği, arama sorgusu ile belirlendiğinden kullanıcı verisinden ziyade arama yapılan anahtar kelimelere dayalı olarak bağlamsal hedefleme ile belirlenir. Ancak bazı durumlarda reklamın belirlenmesi sürecini desteklemek için kullanıcı segmenti gibi kullanıcı hakkındaki veriler de kullanılabilir. Görüntülü reklamlar ise internet siteleri, sosyal medya platformları veya diğer uygulamalara yerleştirilen çeşitli formlardaki reklamları ifade eder. Kullanıcıların bulundukları çevrim içi ortamdaki etkileşimleri, gezinme davranışları gibi verileri kullanıcının ilgisini çekebilecek içeriklerin tahmin edilerek kullanıcıyı hedeflemek için kullanılabilir (Fourberg, ve diğerleri, 2021).

Hedefli Reklamcılıkta Taraflar

Hedefli reklamcılık da dâhil olmak üzere çevrim içi reklamcılık sektörünün geniş kapsamlı olması sebebiyle bir kişinin çevrim içi ortamlarda izlenmesi ve hedeflenmesi süreçlerindeki aktörler değişkenlik göstermektedir. Ancak temel olarak ana aktörler bakımından bir internet uygulaması veya hizmetin geliştiricisi olan taraf, yayıncı; ürün veya hizmetlerini tanıtmak çevrim içi reklamcılığı kullanan işletme sahibi, reklam veren; reklamı yapılan ürün veya hizmete yönelik hedeflemenin yapıldığı kişi ise tüketici olarak adlandırılmaktadır (Cai, Yee, Gu, & Lung, 2020). Kullanıcıların hedeflenmesinde reklam ekosistemine göre aktörler arasındaki veri akışı değişebilmekte ve hedefleme yapılması ile reklamların dağıtımında rol üstelenen çeşitli aracılar da bu sürece dâhil olabilmektedir.

Arama motorları, internet siteleri, sosyal medya platformları, video barındırma platformları, mobil uygulamalar gibi çeşitli içeriklerin barındırıldığı ve belirli bir okuyucu/kullanıcı kitlesine sahip yayıncılar, çevrim içi ortamda reklamların yayımlanması için reklam verenlere alan sağlar. Facebook, Google gibi büyük şirketler sahip oldukları reklam alanlarını doğrudan satabilecek bir altyapıya sahipken haber siteleri gibi daha küçük boyutlu taraflar ise reklam alanlarını, çeşitli aracılar vasıtasıyla reklam verenlere satmaktadır (Competition and Markets Authority, 2020). Bu noktada, arz tarafi platformları (supply side platform-SSP), yayıncıların reklam alanlarının yönetilmesi, satılması amacıyla hareket ederken talep tarafi platformları (demand side platform-DSP), reklam verenler adına reklamların gösterilmesi için farklı dijital mecralardaki reklam alanlarının veriye dayalı olarak satın alınmasını ve çevrim içi reklam kampanyalarının yönetilmesini sağlar (Adshead ve diğerleri, 2019).

Programatik Satın Alma Yönteminin Hedefli Reklamcılıktaki Rolü

Doğrudan satış dışında reklam alanlarının satılmasının bir diğer yöntemi olan programatik satın alma, Birleşik Krallık İnteraktif Reklamcılık Bürosu tarafından "reklam alanlarının insan eylemleri yerine otomatik yöntemlerle alınıp satılması" şeklinde tanımlanmıştır. Bu noktada reklam borsası (ad exchange) olarak adlandırılan platform, programatik satın almanın gerçekleşmesi için reklamcılık teknolojisindeki tüm tarafları birbirine bağlayarak reklam alanlarının alınıp satılmasını sağlamaktadır. Bu sayede programatik satın alma yöntemi ile reklam alanlarının alım-satım sürecinin anlık olacak şekilde ve algoritmalar vasıtasıyla otomatikleştirilmiş olması, belirli müşterilere erişebilmek için hedefleme yapılması ve birden çok alıcı ve satıcı tarafının birbirine bağlanması gibi temel özellikler programatik satın almayı etkili kılmaktadır (Adshead ve diğerleri, 2019).

Genel anlamda programatik kavramı, satın alma sürecinin otomatik bir şekilde gerçekleştiğini ifade etmekle birlikte programatik satın alma yaklaşımı gerçek zamanlı teklif verme (real time bidding), özel teklif verme (private marketplace) ve programatik garantili satış (programmatic direct) gibi farklı satın alma modellerini barındırmaktadır. Gerçek zamanlı teklif verme, reklam verenlerin açık artırmalar ile reklam alanlarının satın alınmasını sağlarken özel teklif verme modeli açık artırmaya davet edilen belirli sayıdaki reklam verenin açık artırmaya katılmasına olanak tanır. Doğrudan satışa benzerlik gösteren programatik garantili satış modelinde ise yayıncı ve reklam veren tarafından envanter ve fiyatın belirlenmesi sonrasında reklamlar, programatik teknoloji yoluyla gerçek zamanlı sunulur (Simpson, 2021). Bu modeller reklam envanterinin fiyatının açık artırma usulü veya sabit olması, açık artırmaya katılan alıcılar gibi hususlar bakımından değişiklik gösterse de programatik satın almanın temel özelliği alım-satım sürecinin çok az insan müdahalesi ile gerçekleşmesi ve hedefleme sürecinin otomatik bir şekilde yürütülmesidir. Özellikle reklam verenler açısından programatik; profilleme, otomatik karar alma, reklamların dağıtımı, dinamik reklam içeriği sunulması gibi tüm reklam sürecinin anlık olarak gerçekleşmesini sağlamakla birlikte bu süreçler hedef kitle olan tüketiciler açısından şeffaf olmayan bir şekilde yürütülmektedir (McStay, 2017).

Reklam alanlarının satışının açık artırma yoluyla gerçekleştiği ve herhangi bir kısıtlama olmaksızın bütün reklam verenlerin açık artırmaya katılabildiği gerçek zamanlı teklif verme, kullanıcı hakkında edinilen bilgilere dayanılarak hedef kitlelere daha tutarlı bir şekilde ulaşabilmek için reklam alanlarına teklif verilmesine olanak tanır. Gerçek zamanlı teklif vermeyi oluşturan bu açık artırmaların arka planında birçok aracı, alıcı ve satıcının bağlantı kurması sağlanarak ve hedefli reklamlar oluşturmak için tüketici verileri kullanılarak algoritmalar vasıtasıyla reklamlara değer katılması amaçlanır. İnteraktif Reklamcılık Bürosuna göre gerçek zamanlı teklif vermenin iş akışı ise Şekil 1'de[2] gösterildiği üzere aşağıdaki şekilde ilerlemektedir (Interactive Advertising Bureau, 2014):

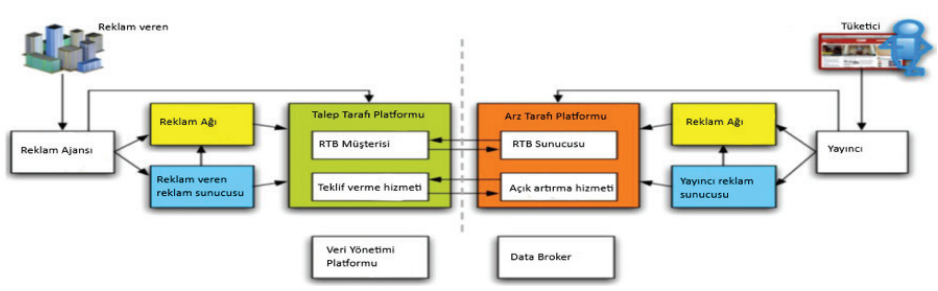
» "Tüketici konumundaki kullanıcı bir yayıncının internet sitesini ziyaret ettiğinde burada yer alan reklam alanı için tarayıcı, yayıncının reklam sunucusuna bağlanır. Reklam sunucusu ilgili reklam alanının özel teklifler için ayrılmış olup olmadığı veya kullanıcı hakkında herhangi bir veriye sahip olunup olunmadığı gibi hususları kontrol ederek reklam alanı için gerçek zamanlı teklif alınmasına karar verebilir.

» Gerçek zamanlı teklif açık artırmasında reklam gösteriminin sunulması için reklam sunucusu, arz tarafi platformuna bağlanır.

» Arz tarafi platformu, reklam isteğini ve kullanıcı hakkında edinilmiş verileri potansiyel alıcıların (örneğin talep tarafi platformları, reklam ağları) bulunduğu reklam borsasına iletir.

» Reklam borsası, kullanıcı bilgileri[3] ile birlikte bir teklif isteği aracılığıyla potansiyel alıcılara mevcut reklam gösterimini duyurur. Anlık ve otomatik olarak yapılan teklifler arasından en yüksek teklife göre kazanan alıcı belirlenir. Daha sonra talep tarafi platformu, reklam isteğini reklam borsası aracılığıyla arz tarafi platformuna iletir.

» Arz tarafi platformu, bu isteği yayıncının reklam sunucusuna gönderir. Yayıncının reklam sunucusu ise tarayıcıyı, reklam verenin reklam sunucusuna yönlendirerek reklam sunucusu tarafından reklam öğesi tarayıcıya gönderilir ve kullanıcıya en uygun şekilde eşleşmiş olan reklam kullanıcıya gösterilir.”



Şekil 1. Reklam teknolojisinde yer alan taraflar arasındaki gerçek zamanlı teklif verme sürecine ilişkin iş ve veri akışı

Gerçek zamanlı teklif verme sürecinde, kullanıcıyla eşleşen reklamın belirlenmesi noktasında teklif isteği ve yanıtları aracılığıyla alıcı ve satıcı tarafları arasında veri akışı gerçekleşmektedir. Özellikle alıcı tarafının teklifte bulunma aşamasında karar vermesine yardımcı olması ve bu sayede isabetli bir hedefleme yapılarak reklam yatırımından en üst düzeyde geri dönüş sağlanması amacıyla kullanıcı hakkında bilinen veriler de bu veri akışına dahil edilmektedir. Bu kapsamda alıcılar ve satıcılar arasında ortak iletişim ve birlikte çalışabilirliğin sağlanmasına yönelik bir standart oluşturulması amacıyla İnteraktif Reklamcılık Bürosu tarafından OpenRTB ve Google tarafından “Authorized Buyers” protokolleri geliştirilmiştir. Bu protokoller, gerçek zamanlı teklif verme açık artırması için gerçekleştiğinde teklif isteği ve yanıtları ile hangi verilerin paylaşıldığını ve bu paylaşımın nasıl

gerçekleştiğini belirlemektedir. Reklam borsasının potansiyel alıcılar için duyurduğu teklif istekleri her iki protokol için genel olarak reklamın yayımlanacağı internet sitesi veya uygulama, kullanıcı, reklam alanı, yayıncı, kullanılan cihaza ilişkin verileri; teklif isteklerine yanıt olarak alıcılar tarafından iletilen teklif yanıtları ise ilgili reklam alanı için teklif edilen miktar ile birlikte görüntülenmek istenen reklama ilişkin bilgileri içermektedir.[4] Bununla birlikte teklif istekleri ile kullanıcının kişisel verileri birçok potansiyel alıcıya aktarılmakta olup bu kişisel veriler arasında; IP adresi, konum, ilgi alanları, demografik veriler (yaş, cinsiyet, gelir düzeyi vb.), davranışsal veriler (ziyaret edilen site üzerindeki etkileşimler, bağlantılar yoluyla diğer sayfalara yapılan ziyaretler vb.), kullanıcının dahil olduğu segment bilgisi, kullanıcının benzersiz tanımlayıcısı, kullanılan cihaz türü, cihazın işletim sistemi, tarayıcı bilgileri, ziyaret edilen internet sayfasının adresi ve sayfa içeriğinin kategorisi/konusu bulunabilir (Information Commissioner’s Office, 2019).

Bir reklam alanı için teklif verilirken son kullanıcı hakkında sahip olunan bilgi miktarıyla doğru orantılı olarak teklif edilen ücret değişmektedir. Ancak gerçek zamanlı teklif verme sürecinde reklam veren adına teklifte bulunan talep tarafi platformu, teklif verip açık artırmayı kazanmadan kullanıcı ile iletişim kuramayacağından kullanıcı hakkında sahip olunan bilgiler, teklif isteğinde yer alan bilgiler ile sınırlı kalacaktır. Bu durumda talep tarafi platformlarınca teklif istekleri veri yönetimi platformu (data management platform-DMP) olarak adlandırılan taraflara gönderilerek bu platformlar aracılığıyla kullanıcının tanımlanması ve farklı kaynaklardan elde edilen verilerle birleştirilmesi yoluyla sahip olunan verilerin zenginleştirilmesi amaçlanır (Veale & Borgesius, 2022). Öte yandan açık artırmanın kazanılması halinde veri yönetimi platformunun kullanıcıya atadığı çerez, reklam borsasının çerezi ile eşleştirilerek gelecekte aynı reklam borsası tarafından düzenlenen bir açık artırmaya dahil olunması halinde kullanıcının tanımlanması da sağlanabilir (Bashir, 2019).

HEDEFLİ REKLAMCILIK UYGULAMALARINDA KİŞİSEL VERİLERİN KORUNMASI

Hedefli reklamcılık gibi kişiselleştirme sağlayan uygulamalarda, profilleme yapılarak kişiler hakkında otomatik bir karar alındığı göz önünde bulundurulduğunda hedef kitle ne kadar iyi tanınırsa alınan kararlar da o kadar tutarlı olacaktır. Bunu sağlamak için ise dijital ortamlardaki her bir veri, kişiler hakkında anlamlı bir bilgi elde edilebilmesi amacıyla izlenerek kaydedilmekte ve analiz edilmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanunu’nda (KVKK) kişisel veri, “Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak ta-

nımlanmış olup elde edilen bu verilerin niteliğine bakıldığında ise kişiselleştirilmiş hizmet sunulmasının amaçlandığı, kişileri benzersiz kılan tanımlayıcılar ile eşleştirildiği dikkate alındığında söz konusu uygulamalar kapsamında elde edilen veriler, kişisel veri niteliğinde olacağı açıktır. Keza, kişisel verinin tanımlandığı KVKK'nın 3'üncü maddesinin gerekçesinde "...Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir..." ifade edilerek tek başına bir anlam ifade etmeyen ancak başka verilerle birleştirildiğinde kişiyi belirlenebilir kılan verilerin de kişisel veri olduğu vurgulanmıştır.

Kişisel verinin benzer bir şekilde tanımlandığı Avrupa Birliği Genel Veri Koruma Tüzüğü'nde (GVKT) özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı gibi bir tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak bu kişisel verilerin bir kişiyi belirlenebilir kılabileceği belirtilmiştir. Buna ilişkin GVKT'nin 30 numaralı gerekçesinde; gerçek kişilerin internet protokol adresleri, çerez tanımlayıcıları veya radyo frekansı tanımlama etiketleri gibi cihazlar, uygulamalar, araçlar ya da protokoller tarafından sağlanan çevrim içi tanımlayıcılarda ilişkilendirilebileceği; özellikle benzersiz tanımlayıcıların diğer bilgilerle eşleştirilmesi halinde gerçek kişilerin tanımlanarak profillerinin oluşturulabileceğine yer verilmiştir. Bu benzersiz tanımlayıcılar kişiye özgü olarak tanımlanabileceği gibi tarayıcı parmak izi[5], reklam kimliği[6], MAC adresi[7] gibi kişinin kullandığı cihaza yönelik de olabilmektedir. Söz konusu tanımlayıcılar ile her ne kadar kişinin kimliğine doğrudan ulaşılmıyor olsa da bu tanımlayıcılar aracılığıyla gerçek kişiler hakkında kişisel verileri olan çeşitli bilgiler elde edilebilmektedir. Örneğin çevrim içi izleme yöntemleriyle bir kişinin profilinin oluşturulması amacıyla ziyaret ettiği internet sitelerinin bir tanımlayıcıyla bağlı olarak izlenmesi kişisel verilerinin işlendiği anlamına gelecektir.

Bununla birlikte Avrupa Birliği Adalet Divanı'nın (ABAD), dinamik IP adresinin[8] kişiyi belirlenebilir kılıp kılmadığına ilişkin bir kararında; hizmet sağlayıcı tarafından kaydedilen dinamik IP adresinin bir gerçek kişinin kimliğini doğrudan belirlenebilir kılmadığı ancak internet servis sağlayıcı nezdinde tutulan ek verilerle birleştirildiğinde ve hizmet sağlayıcının bu ek verilerle gerçek kişinin kimliğinin tanımlanmasını sağlayan yasal araçlara sahip olduğu durumlarda dinamik IP adresinin kişisel veri niteliğini taşıdığına kanaat getirmiştir. Bahse konu ABAD kararında, bir gerçek kişinin kimliğinin tespit edilmesini sağlayan tüm bilgilerin bir tarafın elinde bulunmasının şart olmadığına yer verilmiştir. Yalnızca tanımlanma riskinin düşük olduğu, gerçek kişinin kimliğinin belirlenmesinin kanunlarda yasaklanmış olması ya da zaman, maliyet ve insan gücü açısından orantısız bir çaba gerektirmesi nedeniyle pratikte imkânsız olması hallerinde gerçek kişinin tanımlanması için makul olarak kullanılabilecek bir araç bulunmadığı belirtilmiştir (Patrick Breyer v. Bundesrepublik Deutschland, 2016, para. 46). Bu hususta, GVKT'nin 26 numaralı gerekçesinde de "...Ek bilgilerin kullanılmasıyla bir gerçek kişiye atfedilebilecek olan, takma adlandırmaya tabi tutulmuş kişisel veriler, kimliği belirlenebilir bir gerçek kişiye ilişkin bilgi olarak kabul edilmelidir. Bir gerçek kişinin tanımlanabilir olup olmadığını belirlemek için, gerçek kişinin doğrudan veya dolaylı olarak tanımlanmasını sağlayan, kimliğin tespit edilmesi gibi veri sorumlusu veya başka bir kişi tarafından makul olarak kullanılması muhtemel tüm araçlar dikkate alınmalıdır..." ifadeleri yer almakta olup veri sorumlusu dışında başka bir tarafın da ek bilgilerle gerçek kişinin kimliğini tespit edebilme durumunun dikkate alınması gerektiği vurgulanmıştır.

Benzer yöndeki İngiltere ve Galler Temyiz Mahkemesinin bir kararında ise Google tarafından çerezler vasıtasıyla Apple Safari tarayıcıları üzerinden oluşturulan bilgilerin elde edilmesi ve DoubleClick reklam hizmeti aracılığıyla hedefli reklamların sunulmasına ilişkin mahkeme tarafından tarayıcının oluşturulan bilgilerin kişisel veri olup olmadığı konusunda da tespitlerde bulunmuştur. Bu çerçevede mahkeme, kişinin belirlenebilir olmasının kimliğinin tespit edilmesi ve diğerlerinden ayırt edilmesi anlamında kişiyi "özgünleştiren" verilerle ilgili olduğunu ve tarayıcı tarafından oluşturulan verilerin kişiyi ayırt ettiği göz önünde bulundurulduğunda bu verilerin kullanıcıyı adlandırmıyor olmasının önemsiz olduğu ifade edilerek aşağıdaki hususlar çerçevesinde tarayıcı tarafından oluşturulan verilerin, 1998 Veri Koruma Kanunu'nun 1(1)(a) bölümünün amaçları doğrultusunda kişiyi doğrudan tanımlaması sebebiyle söz konusu verilerin kişisel veri olduğu kanaatine varmıştır (Vidal-Hall v. Google Inc, 2015):

i. "Tarayıcı tarafından oluşturulan veriler iki ilgili unsurdan oluşur: (a) ziyaret edilen web sitesi ve web sitelerinin ziyaret edildiği tarihler ve saatler gibi bir dizi unsuru içeren ayrıntılı tarama geçmişleri; (b) tarama geçmişlerinin bireysel bir cihaza/kullanıcıya bağlanmasını sağlayan benzersiz bir tanımlayıcıya denk gelen 'DoubleClick' çerezinin kullanımından elde edilen bilgiler

ve davalının kullanıcının ne zaman ve nerede çevrim içi olduğunu bilmesi, böylece tarama geçmişlerinin analizine dayalı olarak reklamların onlara hedeflenmesi.

ii. Bu iki unsuru bir araya getiren tarayıcı tarafından oluşturulan veriler, davalıya (i) kullanıcının kullandığı cihazın benzersiz ISP adresi, yani sanal bir posta adresi; (ii) kullanıcının hangi internet sitelerini ziyaret ettiği; (iii) kullanıcının onları ne zaman ziyaret ettiği; (iv) ve mümkünse kullanıcının internet sitesini ziyaret ederken ki konumu; (v) tarayıcının bütün tarama geçmişi; (vi) kullanıcının çevrim içi iken ne zaman tarayıcı etkinliklerinin gerçekleştirdiği bilgilerini açıklayarak kullanıcıların ayırt edilmesini sağlar. Davalı bu nedenle yalnızca kullanıcının (sanal) adresini bilmekle kalmaz; kullanıcının (sanal) evinde olduğunu bilir."

Temelinde profilleme ve otomatik karar almayı barındıran hedefli reklamcılık uygulamaları, gerçek kişilerin çevrim içi izleme yöntemleri aracılığıyla izlenmesi sonucunda elde edilen verileri kişiyi benzersiz kılan tanımlayıcı veriler ile eşleştirerek kişiyi ayırt etmeyi amaçlamakta ve daha sonrasında profilleme yapılması amacıyla bu verileri analiz etmektedir. Hatta hedefli reklamcılık özelinde çerez senkronizasyonu ve birden çok tarafın kişiye atadığı benzersiz tanımlayıcıların eşleştirilmesi ile reklam platformları, elde ettikleri verileri birbirlerine aktarabilmektedir. Dolayısıyla kişiyi belirlenebilir kılan bu veriler, kişisel veri niteliğine sahip olmakla birlikte bu uygulamaların kişisel verilerden beslenmesi sebebiyle büyük sayıda verinin elde edilmesi ve birden çok tarafa aktarılması sonucunda bireylerin kişisel verileri üzerindeki kontrolünün azaldığı durumlarda söz konusu uygulamalar, mahremiyet açısından soru işaretleri doğurmaktadır.

Kişisel Verilerin Korunması Açısından Riskler

Kişiselleştirme sağlayan bu reklamlar bireylerin ne istediği, kim olduğu, çevrim içi ortamdaki davranışlarının belirli kalıplar gösterip göstermediğini ayrıntılı olarak öğrenilmesini sağladığı için kişisel verilerin gizliliği açısından bir risk teşkil edebilecektir. Profilleme sonucunda yeni verilerin türetilmesi veya kişi hakkında çıkarım yapılması ile şirketlerin kişiler hakkında detaylı bilgilere sahip olması, kişilerin kararlarını yönlendirmek amacıyla kişinin kendi kişisel verileri üzerinde kontrolünün sınırlı olduğu bir şekilde kullanılmasına sebebiyet vermektedir (Hof & Prins, 2008). Hatta, söz konusu kişisel verilerin çoğunlukla kişinin haberinin olmadığı bir şekilde çevrim içi ortamdaki davranışlarının gözlemlenmesi ile elde edilmesi sebebiyle şirketler tarafından bu bilgilere göre kişi hakkında bir sonuca varılarak hareket edildiğinin farkında olunmamasına yol açmaktadır.

Algoritmanın otomatik bir şekilde türettiği ve çıkarım yaptığı verilere dayanan profillerin yanlış veya sistematik olarak önyargılı olabileceği göz önünde bulundurulduğunda aynı zamanda profilleme, kişilerin hatalı tanımlanmasına veya sınıflandırılmasına sebebiyet vererek kişi hakkında yanlış bir karar alınmasına yol açabilmektedir (Kaltheuner & Bietti, 2018). Birleşmiş Milletler İnsan Hakları Konseyi, profillemenin bireyleri etkileyen bir karar alınması amacıyla kullanıldığı durumlarda bu uygulamaların insan hakları hukuku temelinde daha fazla tartışılması ve analiz edilmesi gerektiğini kabul ederek "Bireylerin profilinin oluşturulması için kişisel verilerin otomatik olarak işlenmesi, ayrımcılığa veya ekonomik, sosyal ve kültürel haklar dahil olmak üzere insan haklarından yararlanmayı etkileme potansiyeline sahip kararlara yol açabilir." açıklaması ile endişelerini dile getirmiştir (United Nations General Assembly, 2017).

Bireylerin çevrim içi ortamdaki sanal hayatlarını kişiselleştirmeyi amaçlayan hedefli reklamların sunulması için algoritmalar vasıtasıyla bireylerin oluşturulan profillerine dayanılarak otomatik bir şekilde karar alınmaktadır. Bu tür otomatik kararlar kişinin ilgi alanları, davranışları, demografik bilgilerine göre alınabilmekle beraber bir kişinin ikna edilmeye karşı tahmin edilen savunmasızlığı veya satın alma gücüne dair yapılan çıkarıma bile dayanabilmektedir. Hatta söz konusu kişiselleştirme uygulamaları, gerçek hayatta dahi karşımıza çıkabilmektedir. 2017 yılında Tokyo'da test edilen "DeepAd Projesi" kapsamında Japonya'nın en yoğun otoyolundaki reklam panolarına, araba modellerine göre reklam yansıtılmıştır. Bu amaçla, reklam panosu normal şartlarda mevcut hava durumunu yansıtırken lüks araç kategorisindeki bir araba algılandığında reklam içeriği, golf oynama imkânı sunan tesisleri; aile aracı kategorisinde olan bir araba algılandığında ise popüler eğlence parklarını teşvik edecek şekilde sürücüleri hedeflemektedir (Deep Learning, 2017).

Kişinin aradığı, ulaşmak istediği ürün veya hizmet kapsamında çevrim içi reklamların gösterilmesinin bir avantaj sağlayacağı düşünülse de bu kişiselleştirme, kişilerin aleyhine de kullanılabilmektedir. GVKT'ye göre profilleme ve otomatik karar alma sonucunda kişinin kendisiyle ilgili hukuki sonuçlar doğuran veya benzer şekilde kendisini kayda değer ölçüde etkileyen kararların alınması, bireyler için ciddi sonuçlar doğurabilmektedir. Hedefli reklamcılık özelinde kişi hakkında hukuki sonuçlar doğuran kararların alınması riski nispeten daha düşük olsa da tamamen otomatik bir şekilde gerçekleşen profilleme ve otomatik karar alma aşamalarında rol alan algoritmaların kişiyi kayda değer ölçüde etkileyen sonuçlar doğurabilecek bir şekilde geliştirilmesi mümkündür. Madde 29 Çalışma Grubu, kararın kişiyi kayda değer ölçüde etkilemesi için ilgili bireylerin durum, davranış ve seçimlerini önemli ölçüde etkilemesi; birey üzerinde uzun süreli veya kalıcı

bir etkiye sebep olması ya da en uç noktada bireylerin dışlanmasına veya ayrımcılığa yol açması potansiyellerine sahip olması gerektiğini belirtmiştir. Özellikle hedefli reklamcılık bakımından alınan kararın kişiyi kayda değer ölçüde etkileyip etkilemediğine yönelik bir değerlendirmenin, bireylerin farklı web siteleri, cihazlar ve hizmetler arasında izlenmesi dahil olmak üzere profilleme sürecinin müdahaleciliği; ilgili kişilerin beklenti ve istekleri, reklamın iletilme şekli; hedeflenen kişilerin savunmasız olduğu hususlara ilişkin bilgilerin kullanılması faktörlerine bağlı olarak yapılabileceği ifade edilmiştir. Buna ilişkin örneğin, mali açıdan kötü durumda olan veya olması muhtemel bir kişinin yüksek faizli kredi reklamları ile düzenli olarak hedeflenen kişiler bu krediden faydalanması üzerine daha fazla borca maruz kalabilir. Benzer şekilde fiyat ayrımcılığı yapılarak belirli kişi veya kişi gruplarına yönelik farklı fiyatlandırma politikasının uygulanması sonucunda aşırı derecede yüksek fiyatların bir kişiyi belirli mal veya hizmetlerden faydalanmasını alıkoyması durumunda da otomatik karar verme önemli bir etkiye sahip olabilir (Article 29 Data Protection Working Party, 2018). Diğer bir yönüyle, bireylerin ayrımcılığa uğrayacağı şekilde Facebook tarafından reklam verenlere, "yaş ve cinsiyet gibi bilgilere dayalı olarak kullanıcıları reklam almaktan hariç tutma" seçeneği sağlanmakla birlikte özellikle herhangi bir ürüne yönelik reklamlardan ziyade iş ilanı reklamlarında bu ayrımcılık, olumsuz sonuçlara yol açacaktır (BBC, 2018).

Hedefli reklamlara maruz kalan kişiler açısından hedefli reklamcılığın bir türü olan çevrim içi davranışsal reklamlara yönelik tutum ve endişelerin incelendiği Ur ve diğerleri tarafından yapılan çalışmada, katılımcıların bu reklamları yararlı bulmakla beraber mahremiyetlerinin ihlal edilmesinden endişe duyduğu, ancak bu tutumun gerçekte olduğundan daha fazla veri toplandığı düşüncesinden kaynaklandığı sonucuna ulaşılmıştır (Ur, Leon, Cranor, Shay, & Wang, 2012). Gökdemir ve Akıncı'nın bu konuda yaptığı bir diğer çalışmada ise çevrim içi davranışsal reklamcılık hakkında kullanıcılara yeterli bir bilgi sağlanmaması ve seçim hakkı tanınmaması ya da bu mekanizmaların yetersiz olmasının da katılımcıların olumsuz düşüncelere sahip olmasına sebebiyet verdiği belirtilmiştir. Bunun aksine, kişisel verilerin işlenmesi bakımından bir seçim hakkının bulunması, söz konusu reklam uygulamalarının çalışma mantığı ve işlenen kişisel veriler hakkında net ve anlaşılır bilgilerin sağlanmasının katılımcıların çevrim içi davranışsal reklamcılığa karşı olumsuz tutumlarının değişmesinde etkili olduğu sonucuna varılmıştır (Gökdemir & Akıncı, 2019). Yapılan çalışmalarda da ortaya koyulduğu üzere özellikle profilleme ve otomatik karar alma gibi kişisel verilerin şeffaf olmayan bir şekilde birçok teknik işlemden geçirildiği uygulamalarda kullanıcılar açısından farkındalığın düşük olması ve özellikle şirketlerin kullanıcıların kişisel verileri üzerindeki kontrolünü sağlamak adına yeterli mekanizmaları sunmuyor olmasının söz konusu uygulamaları daha belirsiz bir hale getirdiği söylenebilecektir.

Veri Sorumluluğunun Tespiti

Hedefli reklamcılık uygulamalarında kişisel verilerin korunması açısından yükümlülüklerin belirlenmesi için öncelikle bu uygulamalarda aktif faaliyet gösteren aktörlerin sorumluluk rollerinin tespit edilmesi gerekmektedir. Kişisel veri koruma hukuku çerçevesinde belirli yükümlülüklere tabi olan aktörler veri sorumlusu ve veri işleyen olarak belirlenmiş olup KVKK'da veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; veri işleyen ise veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlanmıştır. Ayrıca Kişisel Verileri Koruma Kurulunun 2020/71 sayılı kararı ile veri sorumlusu ve veri işleyenin tespitinde göz önünde bulundurulması gereken hususlara yer verilmiştir. Buna göre veri sorumlusu, veri işleme faaliyetinin temel unsurları, neden ve nasıl olacağı gibi hususlara kimseden emir ve talimat almaksızın veri işleme süreçlerinin her anında serbestçe karar verme yetkisine sahip olan taraf iken veri işleyen, veri sorumlusunun çıkarlarını gözeterek veri sorumlusundan alınan yetki ve talimatlar çerçevesinde veri işleme faaliyetini gerçekleştiren taraf olacaktır. Buna ek olarak GVKT'de veri sorumlusunun kişisel verilerin işleme amaç ve vasıtalarını tek başına veya başkalarıyla birlikte belirleyebileceğine yer verilmiş olup bu durumda birden fazla tarafin "ortak veri sorumluları" olarak nitelendirilmesi mümkündür. Bu sorumluluğun taraflar arasında eşit derecede olması şart olmamakla beraber bu taraflar veri işleme faaliyetinin farklı aşamalarında farklı sorumluluk dereceleriyle rol alabilir. Bu hususta önemli olan birden fazla tarafin işleme faaliyetinin amaç ve vasıtaları üzerinde ortak bir karar ya da birbirini tamamlayan kararların birleştirilmesi ile belirleyici bir etkiye sahip olmasıdır (European Data Protection Board, 2021, para. 57-58).

Ortak veri sorumluluğuna ilişkin değerlendirmelerin yer aldığı internet sitesine, sosyal medya platformu Facebook'un sosyal eklentisi olan "beğen" butonunu yerleştiren çevrim içi giyim mağazasının operatörü olan Fashion ID hakkındaki ABAD kararında, bu eklentinin eklenmesiyle ilgili internet sitesinin ziyaretçilerinin kişisel verilerinin Facebook'a iletilmesinin sağlandığı, dolayısıyla söz konusu kişisel verilerin Facebook'a iletilmesi yoluyla toplanması ve açıklanmasını içeren faaliyetler bakımından amaç ve araçların ortaklaşa belirlenmesi sebebiyle Fashion ID ve Facebook'un ortak veri sorumluları olarak kabul edilebileceği; ancak bu kişisel verilerin iletilmesinden sonra Facebook tarafından gerçekleştirilen işleme faaliyetleri bakımından Fashion ID'nin veri sorumlusu olarak kabul edilemeyece-

ği kanaatine varılmıştır. Bu hususta Fashion ID'nin internet sitesine beğen butonu eklentisini yerleştirmesinin, Facebook'ta daha görünür hale getirerek ürünlerinin tanıtımına olanak sağladığı ve böylece ticari bir avantaj elde ettiği; benzer şekilde bu verileri kendi ticari amaçları için kullanabilen Facebook'un da ekonomik çıkarları doğrultusunda olduğu belirtilmiştir. Buna ek olarak Fashion ID, sosyal eklenti vasıtasıyla ziyaretçilerinin kişisel verilerinin sosyal eklentinin sağlayıcısı olan Facebook'a iletilmesi üzerinde bu eklenti olmadan gerçekleşmeyecek olan belirleyici bir etki uygulamaktadır. Ayrıca Facebook'a iletilen ve işleme amaç ve araçları ortak bir şekilde belirlenen söz konusu kişisel verilere Fashion ID'nin erişiminin olmaması veri sorumlusu sıfatını haiz olmasını engellemeyecektir. Özellikle Facebook hesabı olmayan ziyaretçilerin Fashion ID'nin internet sitesi erişim sağlaması ile kişisel verilerinin Facebook tarafından işlenmesini tetiklemesi sebebiyle Fashion ID'nin bu ziyaretçilerin kişisel verilerinin işlenmesine ilişkin sorumluluğu daha fazla olacaktır (Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, 2019).

Hedefli reklamcılık özelinde hem kendi platformlarında reklam alanları bulunan hem de bünyesindeki altyapı ile hedefli reklamların sunulmasını sağlayan kapalı ekosisteme sahip büyük ölçekli şirketler, yayıncı ve reklam ağı olarak hizmet verebilmektedir. Bununla beraber, programatik satın alma yoluyla yürütülen hedefli reklamcılık faaliyetleri, açık bir ekosistemde birçok tarafın bu sürece dahil olmasını gerektirmektedir. Kapalı ekosisteme sahip olan bir reklam ağının sağladığı hedefli reklamcılık faaliyetlerinde, reklam verenin internet sitesine entegre edilen reklam ağına ait çerez, takip pikseli gibi bir çevrim içi izleme aracı ile kullanıcıların hareketleri izlenerek elde edilen veriler ile reklam ağına ait olan reklam alanlarında kullanıcıya hedefli reklamlar gösterilmektedir. Bu durumda reklam ağı tarafından geliştirilen izleme aracının reklam verenin internet sitesine yerleştirilmesi ile kullanıcıların kişisel verilerini otomatik olarak toplanmasını sağlamakta olup reklam verenin, işleme araçları üzerinde belirleyici bir etkiye sahip olduğu söylenebilecektir. Ayrıca hedef kitleyi oluşturan kullanıcılara reklamların hedeflenmesinde, reklam ağının sunduğu teknik imkanlar kapsamında hedefleme kriterlerinin (demografik bilgiler, ilgi alanları, konum vb.) belirlenmesi ile reklam veren ve reklam ağı işleme amacına birlikte karar vermektedir (European Data Protection Board, 2021).

Öte yandan, tüm reklam satış ekosisteminde var olan reklam alanları ve geniş taleplere açık erişim sağlayan açık ekosistemde ise belirli kullanıcı ve kitlelerin hedeflenerek reklamların sunulmasında her bir aşamada ilgili reklam teknolojisinde rol oynayan farklı taraflar yer almaktadır. Belçika Veri Koruma Otoritesinin IAB Europe tarafından geliştirilen ve OpenRTB protokolü bağlamında gerçekleşen

gerçek zamanlı teklif verme süreçlerindeki veri işleme faaliyetlerinin GVKT ile uyumlu olmasını sağlamak için operasyonel bir çerçeve sağlayan Şeffaflık ve Rıza Çerçevesi hakkındaki kararında, Şeffaflık ve Rıza Çerçevesinin uygulanmasında yer alan ana aktörlerin sorumluluğuna ilişkin değerlendirmelerde de bulunulmuştur. Bu kapsamda, ortak veri sorumluluğundan söz edebilmek için özdeş bir kararın var olmasının gerekmediği, belirlenen amaçların birbirini tamamlayıcı nitelikte olmasının yeterli olduğu; bu hususta sorulması gereken sorunun kişisel verilerin amaçlanan şekilde işlenmesinin tüm tarafların katılımı olmaksızın imkânsız olup olmayacağı yani her bir tarafça gerçekleştirilen işleme faaliyetlerinin ayrılmaz ve bölünmez olup olmadığının değerlendirilmesi gerektiği belirtilmiştir. Sonuç olarak, IAB Europe'un kullanıcıların rızaları, itirazları ve tercihlerini kendi amaçları için değil, üçüncü taraflarca (yani yayıncılar ve reklam teknolojisi tarafları) daha fazla işlenmesini kolaylaştırmak için toplandığı ve değiş tokuş edildiği bir ekosistem sağladığı; bu ekosistemde hem IAB Europe hem de diğer tarafların kişisel verilerin işlenmesine ilişkin kararlarının birbirini tamamlayıcı, yakınsak kararlar olduğuna dayanılarak tüm tarafların ortak veri sorumlusu olarak kabul edilmesi gerektiğine karar verilmiştir (Belgian Data Protection Authority, 2022).

Reklamların kullanıcılara gösterilmesi için alanları sağlayan yayıncılar açısından, sahip oldukları internet siteleri kullanıcılar tarafından ziyaret edildiğinde kullanıcının tarayıcısı otomatik olarak kullanıcıyı reklam ağına yönlendirerek kullanıcının benzersiz bir şekilde tanımlanması, çerezler gibi izleme araçları vasıtayla takip edilmesi ve kişiye özel hedefli reklamların sunulmasına katkıda bulunulmaktadır. Her ne kadar yayıncılar tarafından doğrudan kullanıcıların kişisel verileri reklam ağına aktarılmıyor olsa da söz konusu çevrim içi izleme, yayıncının internet sitesini otomatik olarak kullanıcıyı reklam ağına yönlendirecek şekilde ayarlaması sebebiyle gerçekleşir. Diğer bir ifadeyle, kullanıcının yalnızca yayıncının internet sitesini ziyaret etmeyi amaçlamakla birlikte yayıncı, çevrim içi izlemeye izin verecek olan ilk adımı tetiklemektedir (Article 29 Data Protection Working Party, 2010). Gerçek zamanlı teklif vermenin sonraki aşamalarında ise teklif talepleri, yayıncıların temsilcileri sıfatıyla arz tarafı platformları tarafından reklam vereni temsil eden talep tarafı platformlarına gönderilir. Kullanıcıya ilişkin kişisel verilerin de yer aldığı teklif talepleri esas olarak yayıncılar ve çeşitli reklam teknolojisi taraflarınca işlenmektedir (Belgian Data Protection Authority, 2022). İlgili reklam alanında gösterilecek reklamın belirlenmesinden sonra kullanıcı reklama tıkladığında ve reklam verenin internet sitesini ziyaret ettiğinde reklam veren, reklam kampanyasına ilişkin veriler ile birlikte kullanıcıyı çevrim içi ortamda izleyebilmekte ve ilgili veri işleme faaliyetleri bakımından ayrı bir veri sorumlusu olarak kabul edilmektedir (Article 29 Data Protection Working Party, 2010). Genel olarak reklamların gerçek zamanlı teklif verme yoluyla belirlen-

mesinde kişisel verilerin işlenme süreçlerinin her bir aşamasında farklı taraflar dahil olmakta ve farklı rollerde katkı sağlamaktadır. Bu sebeple ilgili tarafların katkı sağlayarak gerçekleştirdiği işleme faaliyetleri kapsamında kişisel verilerin işleme amaç ve araçları üzerinde etki ve kontrole sahip oldukları süreç özelinde sorumluluğun bulunacağı söylenebilecektir.

Hukuki Gerekçe

Hedefli reklamcılık kapsamında gerçekleşecek veri işleme faaliyetlerinin veri koruma hukukuna uyum sağlaması için hukuki bir dayanağının bulunması gerekmektedir. Bu kapsamda, verinin toplanması aşamasında başvurulan çevrim içi izleme yöntemlerine ilişkin özel bir düzenlemenin yer aldığı Elektronik Haberleşme Kanunu'nun 51'inci maddesinin 3'üncü fikrası ile işletmeciler tarafından çerezler veya benzer teknolojiler vasıtasıyla abonelerin/kullanıcıların terminal cihazlarında bilgilerin işlenmesi, haberleşmenin sağlanması amacı dışında ancak açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması şartıyla gerçekleşebilmektedir. Ancak ilgili hüküm, işletmecilerin tanımlandığı şekilde yalnızca yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketleri kapsamaktadır. Örneğin, işletmeci konumunda olan internet servis sağlayıcıları tarafından haberleşmenin sağlanması dışındaki faaliyetler kapsamında abonelerinin/kullanıcılarının terminal cihazlarına yerleştirilen çevrim içi izleme araçları vasıtasıyla bilginin saklanması ve bilgiye erişilmesi ilgili kişinin açık rızası ile mümkün olacaktır.

Avrupa Birliği'nde uygulanmakta olan 2002/58/EC sayılı E-Gizlilik Direktifi'nin 5'inci maddesinin 3'üncü fikrasında da benzer şekilde, kullanıcının veya abonenin terminal cihazında bilgi saklanması ve bu bilgiye erişilmesi, ilgili abone veya kullanıcının rızası doğrultusunda açık ve kapsamlı bilgilendirmenin yapılması ile mümkün olacaktır. Ancak bu şart, bir elektronik haberleşme ağı üzerinden yalnızca haberleşmenin iletimini gerçekleştirme amacının taşındığı veya abone ya da kullanıcı tarafından açıkça talep edilen bir bilgi toplumu hizmetinin sağlayıcısı tarafından sunulabilmesi için kesinlikle gerekli olduğu hallerde uygulanmayacaktır. Madde 29 Çalışma Grubu, terminal cihaza bilgi saklanmasını sağlayan araçlar kullanılmaksızın haberleşmenin gerçekleştirilemediği hallerde haberleşmenin iletiminin gerçekleştirilmesi kriterine dayanılabileceğini, tek amacın haberleşmenin iletimini gerçekleştirme olması gerektiği, dolayısıyla bu kriterin geniş bir şekilde yorumlanamayacağını ifade etmiştir. Bilgi toplumu hizmetinin sunulması kriterinin kapsamı ise ilgili hizmet açısından belirli bir işlevsellik sağlanması için kullanıcı veya abonenin terminal cihazına bilgi saklanmasının kesinlikle gerekli olması ve bilgi toplumu hizmetinin kullanıcı tarafından açıkça talep edilmesi ile belirlenecektir (Article 29 Data Protection Working Party, 2012). Örneğin kullanıcı ara yüzünün kişiselleştirilmesinin sağlanması, kullanıcının alışveriş sepetine eklediği ögelerin takip edilmesi, giriş yaptıktan sonra kullanıcı kimliğinin tanımlanması gibi amaçlarla terminal cihazlarda bilgi saklanmasını sağlayan çerez ve benzer teknolojilerin kullanılması bir bilgi toplumu hizmetinin sunulması için gereklidir.

Her iki düzenlemede de işleme amacı bakımından açık rıza şartına tabi olmayan istisna kriterleri getirilmiş olup genel olarak ana faaliyet olan haberleşmenin sağlanması ya da hizmetin sağlanması için kesinlikle gerekli olması hallerinde açık rıza aranmamaktadır. Ayrıca Madde 29 Çalışma Grubu buradaki "kesinlikle gerekli olma" ifadesinin değerlendirilmesinde hizmet sağlayıcının değil kullanıcının bakış açısından bir değerlendirme yapılmasının önemli olduğunu ifade etmiştir. Kullanıcı, söz konusu çevrim içi izleme faaliyeti olmaksızın internet sitesi tarafından sağlanan hizmetlere hatasız ve işlevsel bir şekilde erişebiliyorsa ilgili izleme faaliyeti "kesinlikle gerekli" olarak değerlendirilemeyecektir (Article 29 Data Protection Working Party, 2012). Bu çerçevede, reklamlar olmaksızın kullanıcının internet sitesinin sağladığı temel hizmetleri kullanabilme olanağı bulunduğundan kullanıcıların hedefli reklamların gösterilmesi amacıyla çevrim içi izlenmesi, yalnızca haberleşmenin sağlanması veya kullanıcı tarafından açıkça talep edilen bir işlevselliği sağlamak için "kesinlikle gerekli" olarak tanımlanamayacaktır.

Hedefli reklamcılık uygulamalarında kişisel verilerin işlenmesi ise genel kanun niteliğindeki KVKK ile düzenlenmiş olup çevrim içi izleme ve hedefleme amacıyla gerçekleştirilen her türlü kişisel veri işleme faaliyeti KVKK kapsamında olacaktır (Aksoy & Halıcıoğlu, 2021). KVKK'nın 5'inci maddesinde ise hukuka uygunluk sebepleri olan kişisel verilerin işleme şartlarına yer verilmiş olup buna göre kişisel verilerin işlenebilmesi için ilgili kişinin açık rızası gerekmekle birlikte anılan maddenin 2'nci fikrasında sıralanan yedi şarttan birinin mevcut olması halinde açık rıza aranmayacağı düzenlenmiştir. Benzer şekilde GVKT'nin 6'ncı maddesinin 1'inci fikrasında ilgili kişinin rızası ve veri sorumlusunun meşru menfaati şartları ile birlikte diğer hukuka uygunluk şartlarına yer verilmiştir. Bu kapsamda, hedefli reklamcılık uygulamalarındaki kişisel veri işleme faaliyetlerinde ilgili kişinin açık rızasına dayanılmasının geçerli bir hukuki gerekçe olması dışında "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" şartının hedefli reklamcılık için yasal dayanak olup olamayacağı tartışılabilir.

Hedefli reklamcılık uygulamaları, şirketlerin reklam faaliyetlerinin kişiselleştirilmesini sağlayarak doğru yer ve zamanda hedefleme yapılması ile hedef kitleyi daha belirgin bir şekilde etkilemekte ve satın almaya yöneltebilmektedir. Bu durum, gelir artışına katkıda bulunmakta olup şirketlerin ekonomik anlamda bir meşru menfaat sağladığı söylenebilir. Ancak meşru menfaat koşulunun sağlanması işleme faaliyetinin meşru menfaat için KVKK açısından "zorunlu"; GVKT açısından "gerekli" olduğu ve ilgili kişinin temel hak ve özgürlüklerini ihlal etmediği sürece geçerli olacaktır. Yani, meşru menfaati karşılamanın insanların mahremiyetine daha az müdahale eden başka bir yolunun mevcut olması halinde ilgili işleme faaliyetinin meşru menfaat için zorunlu olduğu söylenemeyecektir (Information Commissioner's Office, 2017, para. 67). GVKT'nin 47 numaralı gerekçesinde ilgili kişilerin menfaatleri veya temel hak ve özgürlüklerinin ağır basmaması koşuluyla veri sorumlusunun meşru menfaatinin varlığının belirlenmesinde ilgili kişilerin işleme faaliyetine dair makul beklentileri de dahil olmak üzere bir değerlendirme yapılması gerektiği belirtilmiştir. Birleşik Krallık Bilgi Komiserliği Ofisi ise meşru menfaatin yasal dayanak olarak belirlenmesine yönelik amaç, gereklilik ve denge testi yapılması gerektiğini vurgulamaktadır (Information Commissioner's Office, 2019). Kişisel Verileri Koruma Kurulunun 25.03.2019 tarihli ve 2019/78 sayılı kararında ise geçerli bir meşru menfaatin varlığının tespitinde aşağıdaki kriterlerin değerlendirilmesi gerektiği belirtilmiştir;

- Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması,
- Söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi,
- Meşru menfaatin halihazırda mevcut, belirli ve açık olması,
- İlgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması,
- Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması,
- Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması,
- Kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması,
- Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması,
- Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması.

Hedefli reklamlar açısından meşru menfaatin varlığı belirlendikten sonra elde edilecek menfaat için kişisel verilerin işlenmesinin gerekli olup olmadığı değerlendirilmelidir. Bu hususta, kişisel verilerin işlenmesini gerektirmeyen veya büyük miktarda kişisel verinin toplanmasına ve farklı taraflara aktarılmasına ihtiyaç duyulmayan yollar mevcut ise söz konusu menfaatin yerine getirilmesi için kişisel verilerin işlenmesi gereklilik arz etmeyecektir. Örneğin, bireylerin ayrıntılı profillenmesini içeren davranışsal hedefleme yerine yalnızca internet sitesi veya site içeriğini esas alan içeriğe dayalı hedefleme yönteminin kullanılması mümkünse söz konu menfaate ulaşmak için alternatif yolların mevcut olduğu söylenebilir.

Son olarak ilgili kişilerin temel hak ve özgürlükleri ile veri sorumlularının menfaatleri açısından bir denge testi uygulandığında profilleme ve otomatik karar alma süreçlerini içeren hedefli reklamcılık uygulamalarının varsayım, tahmin veya çıkarıma dayandığı, genellikle şeffaf olmayan yollarla gerçekleştiği ve kişisel verilerin bireylerin makul beklentisinin ötesinde orantısız bir şekilde işlenme riskinin bulunduğu dikkate alındığında söz konusu uygulamaların veri sorumlusu veya veri sorumlularına sağladığı ekonomik menfaatin ilgili kişilerin temel hak ve özgürlükleri ile yarışabilir düzeyde olmayacağı sonucuna varılmaktadır (Information Commissioner's Office, tarih yok). Diğer taraftan GVKT'nin 47 numaralı gerekçesinde kişisel verilerin doğrudan pazarlama amacıyla işlenmesinin meşru bir menfaat için gerçekleştirilmiş olarak kabul edilebileceğine yer verilmişse de profilleme ve otomatik karar almayı barındıran hedefli reklamcılık uygulamalarının yoğun miktarda kişisel veriden beslendiği ve bireylerin kişilik haklarına müdahale edebilecek nitelikte olduğu göz önünde bulundurularak bir değerlendirme yapılmalıdır (Çekin, 2020).

Nitekim, kişisel verilerin işlenmesi bakımından veri sorumlusunun meşru menfaatini öne sürebilmesi için bu menfaatin, ilgili kişinin temel hak ve özgürlükleri ile yarışabilir düzeyde olması gerekmektedir. Dolayısıyla bireyler üzerinde bir

olumsuz bir sonuç doğurma riskini barındıran hedefli reklamcılık uygulamalarına karşı bireylerin seçim hakkına sahip olması ve kontrol yetkisini elinde bulundurması amacıyla kişisel verilerinin işlenebilmesi için açık rızalarına başvurulması gerektiği değerlendirilmektedir. Bu konuda ABAD tarafından da iş modeli temel olarak kullanıcı profillerine göre kişiselleştirilmiş reklamcılığa dayanan Facebook'un bu kapsamdaki faaliyetlerinde, kişisel verileri toplaması ve kullanmasının GVKT m. 6/1(f)'de yer alan meşru menfaat şartına dayanılmasının uygun olup olmadığı bakımından değerlendirmelerde bulunulmuştur. Karara göre; söz konusu işleme faaliyetinin veri sorumlusunun menfaatini elde edebilmesi için gerekli olması gerektiği, ayrıca veri sorumlusu ve ilgili kişinin karşıt haklarının dengelenmesi bağlamında, özellikle ilgili kişinin makul beklentilerinin yanı sıra söz konusu işleme faaliyetinin ölçeği ve bu kişi üzerindeki etkisinin de dikkate alınması gerektiği, dolayısıyla Facebook gibi bir sosyal ağın hizmetlerinin ücretsiz olmasına rağmen kullanıcıların rızası olmaksızın kişiselleştirilmiş reklam sunmak amacıyla kişisel verilerinin işlenmesini, makul bir şekilde beklemeyeceği, bu koşullarda kullanıcıların menfaati ve temel haklarının veri sorumlusunun menfaatlerinin önüne geçtiği ve sonuç olarak bu amaçla yapılan işlemenin meşru menfaat kapsamında girmeyeceğine karar verilmiştir (Meta Platforms and Others, 2023).

Kişisel Verilerin İşlenmesine İlişkin İlkelere Uyulması

Bütün kişisel veri işleme faaliyetlerinin özünde bulunması gereken ilkelere KVKK ve GVKT kapsamında yer verilmiş olup bu ilkelere uyum sağlanması ile özellikle profilleme ve otomatik karar almanın sebep olabileceği olumsuz etkilerin yanı sıra, taraflar arasında bilgi gücünün dengesiz olabilmesi, çok sayıda kişiyi etkileyebilmesi gibi riskler en aza indirgenebilir. Dolayısıyla kişisel verilerin işlendiği bir faaliyetin veri koruma düzenlemelerine uygun olabilmesi için ilk olarak yasal bir hukuki gerekçeye dayanması yanında birlikte genel ilkeleri de ihlal etmemesi gerekmektedir.

KVKK'nın 4'üncü maddesinin 2'nci fıkrasında genel ilkeler; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayılmıştır. Diğer taraftan GVKT'nin 5'inci maddesinde ise kişisel verilerin işlenmesine ilişkin ilkeler; hukuka uygunluk, dürüstlük ve şeffaflık, amaçla sınırlı olma, veri minimizasyonu, doğruluk, sınırlı saklama, bütünlük ve gizlilik ile veri sorumlularının bu ilkelerden sorumlu olup uygunluğunu gösterebilecek şekilde hesap verebilir olma şeklinde belirtilmektedir.

Kişisel verilerin işlenmesinde hukuka uygunluk ilkesi, bütün ilkelere uygun hareket edilmesinin gerekliliğini içermekte olup kapsayıcı bir niteliktedir. Diğer ilkeler açısından, ilgili kişilere karşı şeffaf ve dürüst olunması gerekmekle birlikte dürüstlük ilkesi, hem ilgili kişilere şeffaflık yönünden dürüst olunması hem de profilleme ve otomatik karar alma gibi tekniklerin sonucundaki çıkarım veya kararın kabul edilebilir, uygun ve güvenilir olması bakımından ele alınabilecektir (Küzeci, 2020). Buna ilişkin GVKT'nin 71 numaralı gerekçesinde, dürüst ve şeffaf işleme faaliyetlerinin sağlanması amacıyla profilleme için uygun matematiksel veya istatistiksel prosedürlerin kullanılması, özellikle kişisel verilerde yanlışlıklara neden olan faktörlerin düzeltilmesini ve hata riskinin en aza indirilmesini sağlamak için uygun teknik ve organizasyonel tedbirlerin uygulanması, işleme faaliyetinin içerdiği potansiyel riskler ile ilgili kişinin menfaat ve hakları göz önünde bulundurularak kişisel verilerin güvenliğinin sağlanması gerektiği vurgulanmıştır. Bu hususta, profilleme ve otomatik karar alma gibi özellikle yeni teknolojilerin kullanıldığı, işleme faaliyetinin ilgili kişilerin hak ve özgürlükleri açısından yüksek bir riske yol açmasının muhtemel olduğu hallerde oluşabilecek risklerin ve bu riskleri önlemek için öngörülen önlemlerin yer aldığı bir veri koruma etki değerlendirmesinin hazırlanması GVKT ile zorunlu tutulmuştur. Bunların yanı sıra ırk veya etnik köken, siyasi görüş, din veya inançlar, sendika üyeliği, genetik veya sağlık durumu veya cinsel yönelim temelinde gerçek kişiler üzerinde ayrımcı etkileri olan ya da bu tür bir etkiyle sonuçlanan işleme faaliyetlerinin önlenmesi, özel nitelikli kişisel verilere dayalı profil oluşturma ve otomatik karar vermeye yalnızca belirli koşullar altında izin verilmesi de dürüstlük ilkesi kapsamında değerlendirilebilir.

Hedefli reklamcılık uygulamaları bakımından özellikle bağlamlar arası geniş bir çevrim içi izleme yapılabilmesi sebebiyle aşırı düzeyde kişisel veri toplanması ve bu kişisel verilerin toplanma sürecinin şeffaf olmayan bir şekilde yürütülmesinin mümkün olduğu dikkate alındığında ilkelerin ihlal edilmesi riski daha yüksek olabilecektir. Örneğin farklı bir amaçla elde edilen veriler hedefli reklamcılık kapsamında davranışsal reklamlar gösterebilmek amacıyla işlenebilir, hatta davranışsal reklamların gösterilmesi için geçerli bir açık rızanın mevcut olduğu bir durumda amaçla bağlantısız ve ölçüsüz bir şekilde kişisel veriler işlenebilir veya mevcut veriler üçüncü taraflardan elde edilen verilerle zenginleştirilebilir. Bu hususta, kişisel verilerin ilk elde edilme amacına uygun bir işleme faaliyetinin yürütülmemesi bireylerin kişisel verileri üzerindeki kontrolü kaybetmesine yol açacağından kişisel verilerin ilk elde edilme amacı ile sonraki ikincil amaçların uyumlu olup olmadığına dikkat edilerek uyumsuz olan farklı amaçlar için mevcut kişisel veriler işlenmemeli ve kişisel veriler elde edilme amacı ile orantılı ve ölçülü bir şekilde veri minimizasyonu ilkesine uygun işlenmelidir (Küzeci, 2020, s. 236).

Buna ek olarak, ilgili kişiler hakkındaki varsayım veya çıkarıma dayanılarak otomatik bir karar alındığı göz önünde bulundurulduğunda girdi olarak kullanılan kişisel verilerin doğruluğu ve güncelliği hususundaki eksikliklerin ilgili kişiler ile birlikte veri sorumlusunun da çıkarlarını olumsuz yönde etkileyebileceği söylenebilir (Küzeci, 2020, s. 243). Dolayısıyla, hedefli reklamlar özelinde kişisel verilerin doğru ve güncel olmasını sağlayacak geri bildirim mekanizmalarının bulunması ve bireylerin denetim yetkisini artıran erişim hakkının etkili bir şekilde kullanılabilmesini sağlayan araçların bulunmasının elzem olduğu düşünülmektedir. Bu husus, hem kişisel verilerin doğruluğu ve güncelliğinin saptanmasını hem de işleme faaliyeti için geçerli bir amaç ve hukuki dayanak bulunmadığında veya saklama süresi sona erdiğinde kişisel verilerin imha edilmesi yükümlülüğü üzerinde de bireylerin kontrolünü sağlayacak olup böylece veri minimizasyonu ilkesine de hizmet edecektir. Bununla birlikte, Amerika Birleşik Devletleri Federal Ticaret Komisyonu tarafından çevrim içi reklamcılıkta rol oynayan aktörlerin kullanıcıların bilgilerini toplarken gizliliklerini en iyi şekilde nasıl koruyabileceklerine ilişkin çevrim içi davranışsal reklamcılık alanında sektörün kendi kendini düzenlemesini teşvik etmek amacıyla ilkeler yayımlamıştır. Bu ilkeler üçüncü taraflarla hiçbir verinin paylaşılmadığı birinci taraf reklamcılığı veya içeriğe dayalı reklamcılıktan ziyade arama sorguları, internet sitesi ziyaretleri, görüntülenen içerikler gibi kullanıcıların çevrim içi faaliyetlerinin zaman içinde izlenerek kullanıcının ilgi alanlarına yönelik yapılan reklam türlerini hedeflemektedir. Buna göre şeffaflık ve kullanıcıların verileri üzerindeki kontrolün artırılması için kullanıcıların çevrim içi faaliyetleri hakkındaki verilerin hedefli reklamlar sağlamak için kullanılmak üzere toplandığı ve kullanıcıların verilerini bu amaçla toplanıp toplanmayacağını seçebileceklerine dair kullanıcılara açık, öz ve kolayca ulaşılabilir bir şekilde açıklama sağlanması ve karşılaşılabilecek risklere göre yeterli düzeyde veri güvenliğinin sağlanması ve sınırlı veri saklanması gerekmektedir. Ayrıca, kullanıcı verilerinin nasıl işleneceği veya korunacağı hususunda verilen taahhütlerin yerine getirilmesi ve mevcut gizlilik taahhütlerindeki önemli değişiklikler ile davranışsal reklamcılık için hassas verilerin kullanılabilmesine yönelik kullanıcıların açık rızasının alınması tavsiye edilmektedir (Federal Trade Commission, 2009).

Şeffaflığın Sağlanması

Hedefli reklamcılık uygulamalarının hukuka uygunluğunun sağlanabilmesi için bir diğer koşul, hedef kitleye anlamlı bir bilgi sağlanması gerekliliğidir. Zira ilgili kişiler, bu uygulamaları anlayabildiği sürece faydaları ve riskleri hakkında fikir sahibi ve kişisel verileri üzerinde kontrole sahip olabilecektir. İlgili uygulamalarda anlaşılabilirlik ve şeffaflığın sağlanabilmesi için asgari olarak KVKK'nın 10'uncu maddesinde yer aldığı üzere veri sorumlusunun ve varsa temsilcisinin kimliği,

kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ile 11'inci maddede sayılan ilgili kişilerin diğer haklarına ilişkin açık, sade ve anlaşılabilir bir dilde bilgi verilmesi gerekmektedir. Ayrıca, çerezlerle gerçekleştirilen işleme faaliyetlerinde Kişisel Verileri Koruma Kurumunca aydınlatma metninde çerezin adı, kullanım amacı ve süresi, çerezin birinci taraf veya üçüncü taraf olup olmadığı hakkında bilgi verilmesi de tavsiye edilmektedir (Kişisel Verileri Koruma Kurumu, 2022).

GVKT'nin 13 ve 14'üncü maddeleri, profilleme ve otomatik karar almanın mevcut olması halinde ilgili kişilere bu uygulamaların varlığı ve mantığı hakkında anlamlı bilgilerin sağlanmasının yanı sıra söz konusu kişisel veri işleme faaliyetinin ilgili kişi için önemi ve öngörülen sonuçlarının da açıklanmasını gerektirmektedir. Veri sorumluları, profilleme ve otomatik karar almanın mantığı hakkında anlamlı bir bilgi sağlarken otomatik bir şekilde verilen kararın arkasındaki algoritmanın karmaşık bir açıklamasını ya da tamamının ifşa edilmesini değil bu kararın gerekçesini veya karara ulaşılırken dayanılan kriterleri basit ve açık bir dille anlatmalıdır (Article 29 Data Protection Working Party, 2018). Bununla birlikte, GVKT'nin 58 numaralı gerekçesinde, çevrim içi reklamcılıkta birden çok aktörün dahil olması ve teknolojik açıdan karmaşıklığın bulunması sebebiyle ilgili kişilerin kendisiyle ilgili kişisel verilerin toplanıp toplanmadığını, kim tarafından ve hangi amaçla toplandığını bilmesini ve anlamasını zorlaştırdığı durumlarda her türlü bilginin kısa, kolay erişilebilir ve anlaşılır olması, açık ve sade bir dil kullanılması ve ayrıca mümkünse görselleştirilmesinin özellikle önemli olduğu vurgulanmıştır. Özellikle kişisel verilerin üçüncü taraflarca işlenmesi, birinci tarafın alacağı açık rızaya dayandığı hallerde üçüncü taraf alıcı gruplarının açık bir şekilde belirtilmesi gerekmektedir. Ancak çevrim içi reklamcılıkta kullanılan gerçek zamanlı teklif verme gibi yöntemlerin ekosisteminin karmaşık yapısı ve alıcı gruplarının belirsizliği dikkate alındığında gerekli olan bilgiler her durumda ilgili kişiye tam ve doğru bir şekilde sağlanamayabilir. Diğer taraftan, hedefli reklamcılık için oluşturulan kullanıcı profilleri, kullanıcıların birden fazla internet sitesi veya cihazlarındaki kullanım hareketleri ya da diğer veri eşleştirme hizmetleri aracılığıyla elde edilen verilerle zenginleştirilmiş olabilir. Bu şekilde çok detaylı profillerin oluşturulması orantısız bir işleme faaliyetine yol açmakla birlikte hangi kişisel verilerin işlendiği hakkındaki bilginin ilgili kişiye sağlanması noktasında yetersiz olmasına da sebebiyet verebilecektir (Information Commissioner's Office, 2019). Buna yönelik, aydınlatma yapılırken sağlanan bilgilere ek olarak kişisel verilerinin doğrudan ilgili kişiden elde edilmediği durumlarda toplanan kişisel verilerin kaynağı, aktarımın yasal dayanağı ve ilgili kişinin bu aktarıma itiraz etme hakkının bulunduğuna dair bir bilginin de ilgili kişiye sağ-

lanması halinde şeffaf bir bilgilendirmenin varlığından söz edilebilecektir.

Diğer taraftan Avrupa Konseyi, kişisel verilerin profilleme kapsamında işlendiği hallerde profilleme yapılırken adil bir şekilde kişisel verilerin işlendiğinin garanti altına alınması için diğer kişisel verilerin toplandığı veya toplanacağı taraflar, kişisel verilerin saklanma süreleri, mümkünse profillemenin ilgili kişi üzerindeki potansiyel etkisi, profilleme ve kullanılan modelin altında yatan gerekçeler hakkında anlamlı bilgiler gibi açıklamaların yapılabileceğini tavsiye etmektedir (Council of Europe, 2011). Genel olarak hedefli reklamcılık uygulamaları özelinde adil bir işleme faaliyetinin gerçekleştiğinin ispatı için ilgili kişilere temelde sağlanacak bilgilerin yanında profilleme ve otomatik karar almaya ilişkin ilave bilgilerin de sağlanması gerekmektedir.

İlgili Kişilerin Haklarının Yerine Getirilmesi

Veri koruma düzenlemeleri, kişisel verilerin etkin bir şekilde korunmasını sağlamak için veri sorumlularına yükümlülükler getirirken ilgili kişilerin de kişisel verileri üzerinde kontrole sahip olabilmesi için ilgili kişilere birtakım haklar getirmektedir. KVKK'nın 11'inci maddesinde ilgili kişilerin hakları sıralanmış olup genel olarak kişisel verilerin işlenip işlenmediği, işleniyorsa buna ilişkin bilgi talep etme, işlenme amacını öğrenme ve aktarıldığı üçüncü kişileri bilme hakkı; kişisel verilerin eksik veya yanlış olması halinde bunların düzeltilmesini isteme hakkı, kişisel verilerin silinmesini veya yok edilmesini ve bu hususların üçüncü kişilere de bildirilmesini isteme hakkı; işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkı ile kişisel verilerin kanuna aykırı işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme hakkı ilgili kişilere tanınmıştır. GVKT'de ise KVKK ile ilgili kişilere tanınan haklara ek olarak işlemeyi kısıtlama, veri taşınabilirliği ve işlemeye itiraz hakkı açıkça ilgili kişilerin hakları arasında sayılmıştır. İlgili kişilere tanınan bu hakların, profilleme ve otomatik karar alma süreçlerini barındıran hedefli reklamcılık uygulamalarında da etkili bir şekilde kullanılabilmesi için veri sorumlularının uygun mekanizmaları sağlaması gerekmektedir. Bu bakımdan, hedefli reklamcılık kapsamında önemli noktaların yer aldığı düşünülen bilgi talep etme, açık rızanın geri alınması, itiraz ve karara tabi olmama hakları özel olarak ele alınmıştır.

KVKK'nın 11'inci maddesinin 1'inci fıkrasının (b) bendi ile ilgili kişilere kişisel verilerine ilişkin bilgi talep etme hakkı tanınmıştır. Bu husus GVKT'de profilleme ve otomatik karar alma özelinde düzenlenmiş olup 15'inci maddenin 1'inci fıkrasının (h) bendinde profilleme dahil otomatik karar almanın varlığı ve en azından

bu durumlarda, ilgili mantık hakkında anlamlı bilgilerin yanı sıra bu tür işlemenin önemi ve öngörülen sonuçları hakkında ilgili kişilerin bilgi talep edebileceği düzenlenmiştir. Bu çerçevede veri sorumlusu, profilin oluşturulmasına esas olan kişisel verilerin yanı sıra profile ilişkin bilgilere ve profilleme sonucunda ilgili kişinin hangi segmentlere yerleştirildiğine ilişkin detaylara erişim sağlamakla yükümlü olduğu söylenebilecektir (Article 29 Data Protection Working Party, 2018). Zira bu madde ile ilgili kişilere sağlanacak olan anlamlı bilgiler sayesinde kişi karara karşı itiraz hakkını kullanıp kullanmayacağını da değerlendirebilecektir.

Bilgi talep etme hakkına ilişkin Avusturya Veri Koruma Otoritesinin (Datenschutzbehörde - DSB) bir kararında, veri sorumlusunun müşterilerinin ait olabileceği belirli demografik grupların yüzdelik olasılıklarını hesaplayarak pazarlamaya ilişkin müşteri skorlarının elde edildiği belirtilerek bu skorların nasıl hesaplandığına ilişkin bilgi talep edilmiş ancak veri sorumlusu, talep edilen bilgilerin ticari sır niteliğinde olduğunu iddia ederek söz konusu talebi reddetmesi hakkında değerlendirmelerde bulunulmuştur. DSB tarafından GVKT madde 15(1)(h) uyarınca "Madde 22(1) ve (4)'te atıfta bulunulan profil oluşturma da dahil olmak üzere otomatik karar alma sürecinin varlığı ve en azından bu durumlarda, ilgili mantık hakkında anlamlı bilgilerin yanı sıra söz konusu işlemenin veri sahibi için önemi ve öngörülen sonuçları" hakkında bilgi edinme hakkı kapsamının yalnızca profilleme dahil otomatik karar almayla sınırlı olmadığı, "en azından bu durumlarda" ifadesinin geniş bir uygulama alanına işaret ettiği, dolayısıyla ilgili hakkın profillemeyi de kapsadığı sonucuna varılmıştır. Ancak bu skorların oluşturulmasında kullanılan mantığın ticari sır niteliğinde olduğu, bu amaçla kullanılan algoritma veya kaynak kodun ilgili kişiye açıklanmasının gerekmediği, bunun yerine ilgili kişinin skorunun hesaplanmasıyla bağlantılı olarak parametreler ve girdi değişkenleri ile bunların nasıl elde edildiği; parametreler ve girdi değişkenlerinin skor üzerindeki etkisi; ilgili kişinin profilleme sonucunda neden belirli bir gruba atandığına ilişkin açıklama; olası profil kategorilerinin listesi ve ilgili kişinin düzeltme ve silme haklarını kullanmasını ve işlemenin yasallığını gözden geçirmesini sağlayan benzer eşdeğer bilgilerin açıklanması gerektiği belirtilmiştir.[10] Buradan hareketle, bilgi talep etme hakkının ilgili kişilerin kişisel verileri üzerinde sahip olduğu kontrolü artırırken diğer hakların etkin bir şekilde kullanılmasına da katkı sağladığı anlaşılmaktadır.

Hedefli reklamcılık uygulamalarının açık rızaya dayanması gerektiği göz önünde bulundurulduğunda ilgili kişinin açık rızasını geri alma hakkı da bulunmaktadır. Kişisel verilerinin işlenmesinde özgür iradesiyle rıza gösteren kişinin rızasını geri almak istemesi halinde, bu talep ileriye yönelik sonuç doğuracak olup veri sorumlusunun kişisel verilerin işlenmesine son vermesi gerekmekle birlikte ki-

şisel verilerin imha edilmesini tetikleyecektir. GVKT'nin 17'nci maddesinde de ilgili kişi rızasını geri aldığında işleme için başka bir yasal dayanak mevcut değilse veri sorumlusu gecikmeksizin kişisel verileri silmekle yükümlüdür. Bu durumda, hedefli reklamların gösterilmesini durdurmak yeterli olmayacak olup ilgili kişiyi belirlenebilir kılan benzersiz tanımlayıcı ile kişi arasındaki bağın koparılması veya bu tanımlayıcıya bağlı kişi hakkında toplanan verilerin silinmesi önem arz etmektedir (Commission Nationale Informatique & Libertés [CNIL], 2023). Özellikle kişisel verilerin birçok tarafa aktarılabildiği hedefli reklamcılık uygulamalarında, geri alınan rızaya dayanarak kişisel veri işleme faaliyeti yürüten diğer taraflara da bu hususun bildirilmesi gerekmektedir.

KVKK'nın 11'inci maddesinin 1'inci fikrasının (g) bendi ile münhasıran otomatik sistemler vasıtasıyla kişisel verilerin analiz edilmesi suretiyle işlenmesinde, kişinin aleyhine bir sonucun ortaya çıkması halinde bu sonuca itiraz etme hakkı mevcuttur. İtiraz hakkı ile kişisel verilerin tamamen otomatik sistemler vasıtasıyla işlendiği, herhangi bir insan müdahalesinin bulunmadığı işleme faaliyetleri bakımından ilgili kişilere aktif bir şekilde itirazda bulunma hakkı tanınmış olup itiraza karşı veri sorumlusunun otomatik alınmış olan kararı gözden geçirmesi gerekecektir. Bu kapsamda, profilleme sonucunda otomatik bir kararın alındığı durumlarda da bu kararın kişinin aleyhinde olması halinde bu hak öne sürülebilecektir. GVKT'de ise 22'nci maddenin 1'inci fikrası ile bireyler, kendisiyle ilgili hukuki sonuçlar doğuran veya benzer şekilde kendisini kayda değer ölçüde etkileyen bir karara tabi olmama hakkına sahiptir. GVKT ile düzenlenen karara tabi olmama hakkının, ilgili kişilere getirilen bir itiraz hakkından ziyade veri sorumlularına getirilmiş bir yasak olduğu görüşü ağır basmaktadır. Zira, bireylerin her durumda profilleme ve otomatik karar almanın varlığından haberdar olamayacağı dikkate alındığında bu hususta bir yasağın bulunması, kişisel verilerin daha etkin bir şekilde korunmasını sağlayabilecektir (Aksoy, 2022). Hedefli reklamların sonucunda bireylerin ikna edilebilirlik düzeylerine göre sınıflandırılabilmesi bariz bir şekilde haksız bir ayrımcılık içermesine veya kişi üzerinde önemsiz olmayan ekonomik sonuçlara yol açabilir (Sartor, Lagioia, & Galli, 2021). Örneğin reklam verenlerin etnik köken, din, cinsiyet gibi bilgilere göre bireyleri hedefleyebilmesi, hatta belirli grupları bu reklamlardan hariç tutabilmesi ayrımcılığa yol açabilmektedir (Angwin & Jr., 2016). Reklam amaçlı profilleme yapılırken bireylerin farklı web siteleri, cihazlar ve hizmetler arasında izlenmesi de dahil olmak üzere profil oluşturma sürecinin müdahaleciliği; bireylerin beklenti ve istekleri, reklamın sunulma şekli veya hedeflenen kişinin zayıf noktalarına ilişkin bilginin kullanılmasına bağlı olarak bireyler üzerinde önemli bir etkiye sahip olabilecektir (Article 29 Data Protection Working Party, 2018).

SONUÇ

Reklam faaliyetlerinin dijital ortamda gerçekleşmesi ile ilgi ve alaka düzeylerine göre hedef kitlenin belirlenerek reklamların kime veya kimlere yönelik olacağını seçebilme imkânı mümkün kılınmıştır. Böylece hem doğru zamanda doğru yerde ürün veya hizmetle ilgili olan müşteri veya potansiyel müşterilere erişilebilmekte ve daha yüksek geri dönüş oranı elde edilebilmekte hem de reklam için harcanan bütçe daha etkili ve ekonomik bir şekilde kullanılmış olmaktadır. Bu noktada ise bireylerin çevrim içi ortamda izlenmesiyle elde edilen veriler analiz edilerek bir profili oluşturulmakta ve bu profile dayanılarak ilgi alanları, davranışlar, demografik yapıları gibi belirleyici özelliklere göre söz konusu dijital tüketiciler otomatik bir şekilde kişiselleştirilmiş reklamlar ile çevrim içi ortamda hedeflenmektedir.

Reklam ve pazarlama amacıyla dijital tüketicilerin profilinin oluşturulması ve buna dayanarak hedeflenmesi, birçok avantaj sağlamakla birlikte ayrıca tüketiciler açısından da bu uygulamaların tüketicilerin çevrim içi ortamlarını kişiselleştirerek istek ve ihtiyaçlarına yönelik reklamların alaka düzeyini artırdığı öne sürülebilmektedir. Ancak söz konusu kişiselleştirmenin sağlanması için dijital tüketiciler açık olmayan tekniklerle, tamamen otomatik işleyen bir çevrim içi izleme ve hedeflemeye maruz kalmakta ve bu durum, tüketiciye özgü hedefli reklamların sunulması amacıyla tüketicilerin dijital ortamda belirlenebilir kılınarak yoğun bir şekilde kişisel verilerinin toplanması, analiz edilmesi, üçüncü taraflara aktarılması gibi sonuçlara sebebiyet vermektedir. Hatta daha ileri bir seviyede tüketicilerin ırk, etnik köken, sağlık gibi özel nitelikli kişisel verileri hakkında çıkarım veya tahmin yapılması ile özel nitelikli verilerin reklam amacıyla kullanılarak tüketicinin hedeflenebilmesi; tüketicilerin belirli özelliklerine göre ayrıştırılarak tüketiciye fayda sağlayabilecek nitelikteki reklam faaliyetlerine dahil edilmemesi ya da daha yüksek fiyatlı ürünlere yönlendirme yapılması ile ayrımcılığa müsait bir ortam bulunması; tüketicilere yeterli düzeyde bilgi sağlamayarak kişisel verilerin şeffaf olmayan yöntemlerle elde edilebilmesi ve tüketicilerin zayıf ve güçlü yönleri gibi kişisel özellikleri hakkında bir varsayıma ulaşılarak satın alma alışkanlıklarının manipüle edilebilmesi ekonomik bir zarara uğrama riskine yol açabilecektir. Bu bakımdan profilleme ve otomatik karar alma gibi yoğun bir şekilde kişisel verilerin işlenmesini gerektiren teknikleri birlikte barındıran hedefli reklamcılık uygulamalarının, tüketicilerin kişisel verilerinin korunması hakkını ihlal etme riskini yüksek düzeyde barındırdığı söylenebilecektir.

Sonuç olarak, kişisel verilerin korunması hakkının etkin bir şekilde yerine getirilebilmesi için yürürlükteki mevzuat ile bireylerin dijital dünyada kaçınılmaz

olan bir gözetime maruz kalmadan özgürce hareket edebilmesi ve profilleme yapılarak elde edilecek yeni verilerle maruz kalınabilecek olan manipülasyon, ayrımcılık gibi sonuçlardan da korunmalarının sağlanması amaçlanmaktadır. Bunun yanında, algoritmalar vasıtasıyla kişisel verilerin işlendiği dikkate alındığında bireylerin çıkarları, hak ve özgürlüklerine odaklanarak hem yasal hem de etik kurallar açısından veri koruma ilkelerinin temel alınması gerekmektedir. ◆

KAYNAKÇA

- Adshead, S., Forsyth, G., Wood, S., & Wilkinson, L. (2019). Online advertising in the UK, Plum Consulting.
- Aksoy, H. C. (2022). Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme. Kişisel Verileri Koruma Dergisi, 4 (2), 69-87.
- Aksoy, H. C., & Halıcıoğlu, M. (2021). AB ve Türk Hukuklarında Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme. Kişisel Verileri Koruma Dergisi, 3(1), 61-88.
- Angwin, J., & Jr., T. P. (2016). Facebook Lets Advertisers Exclude Users by Race. https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race adresinden alındı.
- Article 29 Data Protection Working Party. (2010). Opinion 2/2010 on online behavioural advertising.
- Article 29 Data Protection Working Party. (2012). Opinion 04/2012 on Cookie Consent Exemption. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf adresinden alındı.
- Article 29 Data Protection Working Party. (2014). Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting. https://www.dataprotection.ro/servlet/ViewDocument?id=1089 adresinden alındı.
- Article 29 Data Protection Working Party. (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.
- Bashir, M. A. (2019). On the Privacy Implications of Real Time Bidding. Northeastern University.
- BBC. (2018). Facebook accused of job ad gender discrimination. https://www.bbc.com/news/technology-45569227 adresinden alındı.
- Belgian Data Protection Authority. (2022). 2 Şubat 2022 tarih ve 21/2022 esas sayılı Belçika Veri Koruma Otoritesi kararı. https://edpb.europa.eu/system/files/2022-03/be_2022-02_decisionpublic_0.pdf adresinden alındı.

◊ Cai, Y., Yee, G. O., Gu, Y. X., & Lung, C.-H. (2020). Threats to Online Advertising and Countermeasures: A Technical Survey. Digital Threats: Research and Practice, Vol. 1(No. 2), 11:2.

◊ Centre for Data Ethics and Innovation. (2020). Online targeting: Final report and recommendations. https://www.gov.uk/government/publications/cdei-review-of-online-targeting/online-targeting-final-report-and-recommendations adresinden alındı.

◊ Commission Nationale Informatique & Libertés (CNIL). (2023). Personalised advertising: CRITEO fined EUR 40 million. https://www.cnil.fr/en/personalised-advertising-criteo-fined-eur-40-million adresinden alındı.

◊ Competition and Markets Authority. (2020). Online platforms and digital advertising market study. https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf adresinden alındı.

◊ Council of Europe. (2011). The protection of individuals with regard to automatic processing of personal data in the context of profiling - Recommendation CM/Rec(2010)13 and explanatory memorandum (2011). Council of Europe Publishing. https://rm.coe.int/16807096c3 adresinden alındı.

◊ Çekin, M. S. (2020). Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku. On İki Levha Yayıncılık.

◊ Deep Learning Enables Intelligent Billboard or Dynamic, Targeted Advertising on Tokyo Expressway (Case Study). (2017). https://builders.intel.com/docs/storagebuilders/deep_learning_enables_intelligent_billboard_for_dynamic_targeted_advertising_on_tokyo_expressway.pdf adresinden alındı.

◊ European Data Protection Board. (2021). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf adresinden alındı.

◊ European Data Protection Board. (2021). Guidelines 8/2020 on the targeting of social media users. (Version 2.0). https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf adresinden alındı.

◊ Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, C-40/17 (Court of Justice of the European Union). https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=163572 adresinden alındı.

◊ Federal Trade Commission. (2009). FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf adresinden alındı.

◊ Fourberg, N., Taş, S., Wiewiorra, L., Godlovitch, I., Streel, A. D., Jacquemin, H., Hill, J., Nunu, M., Bourguigon, C., Jacques, F., Ledger, M., Lognoul, M. (2021). Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice.

◊ Gökdemir, Ş. Ş., & Akıncı, S. (2019). Çevrimiçi Davranışsal Reklamcılığa Yönelik Tüketici Tutumları ve Mahremiyet Endişeleri. Erciyes İletişim Dergisi Uluslararası Dijital Çağda İletişim Sempozyumu Özel Sayısı, 21-38. doi:10.17680/erciyesiletisim.483907

◊ Hof, S. v., & Prins, C. (2008). Personalisation and Its Influence on Identities, Behaviour and Social Values. M. Hildebrandt, & S. G. (Yay. Haz.). Profiling the European Citizen: Cross-Disciplinary Perspectives içinde (s. 111-127).

◊ Information Commissioner's Office. (2017). Big data, artificial intelligence, machine learning and data protection. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf adresinden alındı.

◊ Information Commissioner's Office. (2019). Update report into adtech and real time bidding. https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf adresinden alındı.

◊ Information Commissioner's Office. (tarih yok). What is automated individual decision-making and profiling?. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/#id3 adresinden alındı.

◊ Interactive Advertising Bureau. (2014). How an Ad is Served with Real Time Bidding (RTB) - IAB Digital Simplified. https://www.youtube.com/watch?v=-Glgi9RRuJs adresinden alındı.

◊ Kaltheuner, F., & Bietti, E. (2018). Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR. Journal of Information Rights, Policy and Practice.

◊ Kişisel Verileri Koruma Kurumu. (2022). Çerez Uygulamaları Hakkında Rehber. https://www.kvkk.gov.tr/Icerik/7353/Cerez-Uygulamalari-Hakkinda-Rehber adresinden alındı.

◊ Küzeci, E. (2020). Kişisel Verilerin Korunması. On İki Levha Yayıncılık.

◊ Meta Platforms and Others. (2023). C-252/21. The Court of Justice of the European Union. https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3729767 adresinden alındı.

◊ McStay, A. (2017). Micro-Moments, Liquidity, Intimacy and Automation: Developments in Programmatic Ad-tech. Gabriele Siegert, M. B. Rimscha, & S. G. (Yay. Haz.). Commercial Communication in the Digital Age - Information or Disinformation? içinde (s. 143-159). doi:https://doi.org/10.1515/9783110416794

◊ Organisation for Economic Co-operation and Development. (2014). SUMMARY OF THE OECD PRIVACY EXPERT ROUNDTABLE Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking.

◊ Patrick Breyer v. Bundesrepublik Deutschland, C-582/14, The Court of Justice of the European Union (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582 adresinden alındı

◊ Sartor, P. G., Lagioia, D. F., & Galli, D. F. (2021). Regulating targeted and behavioural advertising in digital services: How to ensure users' informed consent. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694680/IPOL_STU(2021)694680_EN.pdf adresinden alındı.

◊ Simpson, I. (2021). Real-Time Bidding (RTB) & Programmatic: One and the Same? https://clearcode.cc/blog/difference-between-rtb-programmatic/ adresinden alındı

◊ The International Chamber of Commerce United Kingdom. (2012, Kasım). ICC UK Cookie guide.

◊ United Nations General Assembly. (2017). The right to privacy in the digital age, A/HRC/RES/34/7. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/34/7 adresinden alındı.

◊ Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: perceptions of online behavioral advertising. SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security (s. 1-15). doi:10.1145/2335356.2335362

◊ Veale, M., & Borgesius, F. Z. (2022). Adtech and Real-Time Bidding under European Data Protection Law. German Law Journal 23 (2), 226-256. doi:10.1017/glj.2022.18

◊ Vidal-Hall v. Google Inc, [2015] EWCA Civ 311, The Court of Appeal (2015). https://www.judiciary.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf adresinden alındı

EK NOTLAR

[2] Şekil, https://edpb.europa.eu/system/files/2022-03/be_2022-02_decisionpublic_0.pdf adresinden alınmıştır.

[3] Bu bilgiler, kullanıcının dahil olduğu segment bilgisi de olabilir. Örneğin kullanıcının "Türkiye'de yaşayan ve 25-40 yaş arasındaki kadınlar" segmentinde yer aldığı bilgisi iletilebilir.

[4] IAB Tech. Lab. tarafından versiyon bazında yayımlanan OpenRTB protokolü ile sağlanan iletişimde yer alan alanlar hakkında daha fazla bilgi için https://iabtechlab.com/standards/openrtb/; Authorized Buyers gerçek zamanlı teklif verme protokolünde yer alan alanlar hakkında daha fazla bilgi için https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide bakılabilir.

[5] Tarayıcı parmak izi, bir web sayfası yüklendiğinde web sitesinin bilgisayar ve tarayıcı hakkında elde edebileceği verilerin bir derlemesidir.

[6] Reklam hizmetlerinin kişiselleştirilebilmesini sağlamak için bir mobil cihaza atanan benzersiz bir değerdir. Apple reklam kimliklerini "Identifier for Advertisers" (IDFA); Google "Android Advertising ID" (AAID) olarak adlandırmaktadır.

[7] Ortam erişim kontrolü (Media Access Control) adresi, bir cihazın ağ donanımlarına tanımlanan benzersiz bir tanımlayıcıdır. IP adresinden farklı olarak değişmez ve tektir.

[8] Dinamik IP adresi, değişmeyen ve ağa bağlı cihazın sürekli tanımlanmasına izin veren statik IP adreslerinin aksine, her internet bağlantısında cihaza tanımlanan ve sonraki bağlantılarda değişen geçici adreslerdir.

[9] Benzer şekilde Article 29 WP, cihaz parmak izi ile ilgili görüşünde cihaz parmak izinin çevrim içi davranışsal reklamcılık amacıyla kullanılmasının kesinlikle gerekli olmadığını değerlendirerek kullanıcının rızasını gerektirdiğini ifade etmiştir. Daha fazla bilgi için bkz. (Article 29 Data Protection Working Party, 2014, s. 9)

[10] Avusturya Veri Koruma Otoritesinin 08.09.2020 tarihli ve 2020-0.436.002 numaralı kararının resmi olmayan İngilizce çevirisi için bkz. https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2020-0.436.002

İŞ YÖNETİMİ VE PLANLAMASI ÇERÇEVESİNDE KİŞİSEL VERİLERİN İŞLENMESİ

Tuğçe ARICI ŞİRİN

Kişisel Verileri Koruma Uzmanı

"Bu çalışma 14.02.2023 tarihinde kabul edilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 4857 sayılı İş Kanunu Kapsamında Kişisel Verilerin Korunması başlıklı uzmanlık tezinden alınmıştır."

GİRİŞ

Modern teknolojiler çalışanların akıllı telefonlar, masaüstü bilgisayarlar, tabletler, araçlar, giyilebilir cihazlar gibi birçok farklı cihaz aracılığıyla iş yerlerinde ve çalıştıkları herhangi bir ortamda takip edilmesine imkân sağlamaktadır (Article 29 Data Protection Working Party, 2017, s.9.). Kişisel verilerin iş yönetimi ve planlaması çerçevesinde işlenmesinde genel ilkeler gözetilmez ve işverenin bu kapsamdaki kontrol ve denetimini sınırsız bir biçimde kullanımı söz konusu olursa çalışanlar bakımından haksız ve müdahaleci bir izleme ortaya çıkabilir. Sürekli izlenen ve gözetim altında bulunan şeffaflaşan birey kişiliğini serbestçe geliştiremeyebilir ve kendisinden beklendiği davranış kalıbının dışına çıkamayabilir (Küzeci, 2018, s.77).

İşverenlerin iş sözleşmesi akdedildikten sonraki süreçte iş yönetimi ve planlaması çerçevesinde kişisel verilerin işlenmesini gerektiren durumlar ortaya çıkmaktadır. İşverenin iş güvenliğinin sağlanması, sözleşmenin gereği gibi ve doğru şekilde ifa edilmesinin sağlanması, işverenin menfaatine aykırı düşen bir durumun yaşanmaması adına gerekli tedbirleri alması gerekmektedir. Bu tedbirlerin, iş-

verenin yönetim hakkının kapsamında değerlendirilebilmesi mümkün olmakla birlikte aynı zamanda, iş yerinde işin yürütülmesi, iş yerinin düzeninin ve güvenliğinin sağlanması ile sınırlı olduğunu (Anayasa Mahkemesi, 2016/13010 Başvuru Numaralı ve 17/09/2020 Tarihli Karar), bu amaçların dışında ve temel hak ve hürriyetleri zedeleyici bir boyuta ulaşan faaliyetlerin yönetim yetkisinin kapsamına dahil edilemeyeceğini söylemek mümkündür. Bu anlamda, işverenin yönetim yetkisi kapsamında belirlediği kurallar ile iş yerinde sağlamayı amaçladığı huzur ve disiplin ile işçinin özel hayatına saygı hakkı arasında bir çatışma söz konusu olabilecektir (Anayasa Mahkemesi, 2013/4825 Başvuru Numaralı ve 24/03/2016 Tarihli Karar).

Bu kapsamda, işçinin iş yerine giriş çıkışının kontrolü, işçinin elektronik ortamda gerçekleştirmiş olduğu işlemlerin kontrolü ve iş yerinde görüntü/ses kayıt cihazları vasıtasıyla gerçekleştirilen kontroller kişisel verilerin işlenmesini mümkün kılan durumlar olup işverenlerin bu anlamda sınırsız yetkisi bulunmamaktadır. Çalışmamızda işverenlerin bu kontrolleri hangi hukuki dayanak çerçevesinde ve hangi sınırlarda gerçekleştirebileceğine değinilmeye çalışılacaktır.

İŞ YERİNE GİRİŞ, ÇIKIŞ VE GEÇİŞ KONTROLLERİ

İşçilerin işe giriş çıkış saatleri, iş yerinde geçirilen süre, işe giriş çıkış sıklığı, iş yerinde birimler/bölümler arası geçişleri işveren tarafından farklı amaçlar ve farklı şekillerde kontrol edilmektedir. İşveren, yönetim hakkı çerçevesinde işçi ile aralarında çıkabilecek bir ihtilaf ya da durum tespiti (eksik çalışma, devamsızlık, çalışma saatlerinde iş yerinde bulunmama) dolayısıyla bu kontrolleri sağlayabileceği gibi aynı zamanda güvenlik amacı ile de bu yöntemlere başvurmaktadır. İşverenin söz konusu amaçlar çerçevesinde kullandığı yöntemler önemli bir araç olmakla birlikte aynı zamanda işçinin iş yerindeki faaliyetlerine ilişkin müdahaleci düzeyde bilgi ve kontrol sağlama riskini de beraberinde getirmektedir (Article 29 Data Protection Working Party, 2017, s.18). İşçiler üzerindeki bu yöndeki kontrol mekanizması farklı yöntemler vasıtasıyla gerçekleştirilebilmektedir. Biyometrik veriler (parmak, damar, avuç izleri, yüz, retina) işlenmek suretiyle, manyetik kimlik kartları, güvenlik kameraları ve imza defterleri vasıtasıyla giriş çıkış ve geçişler ile sağlanabilmektedir.

Biyometrik Yöntemler

Biyometrik veriler, kişilerin diğer kişilerden ayırt edilmesini sağlayan, kişilere has olan her türlü biyolojik ve davranışsal özelliklerin bütünü olarak tanımlanabilecek olup kişilerin biyometrik verilerini ömür boyu taşımaları ve bu verilerin neredeyse hiç değişmemesi dolayısıyla en önemli kişisel verilerdendir (Erdinç, 2020, s.2). Biyometrik veriler benzersiz ve kimlik doğrulama niteliğine sahip olduğundan işverenler tarafından güvenlik ve takip amacıyla başvurulan bir yöntemdir. Biyometrik doğrulama/kimlik doğrulama, bir kişinin biyometrik sistem tarafından doğrulama sırasında elde edilen biyometrik verilerinin cihazda depolanan tek bir biyometrik şablonla eşleştirilmesi sürecidir (Article 29 Data Protection Working Party, 2012, s.6).

Kişisel Verilerin Korunması Kanunu'nun 6'ncı maddesinde biyometrik veriler özel nitelikli kişisel veri olarak addedilmiştir. Biyometrik verinin tanımına Kanun'da yer verilmezken Genel Veri Koruma Tüzüğü'nde biyometrik veri yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veriler olarak tanımlanmaktadır. Bu tanımlar çerçevesinde parmak, damar, avuç izi, yüz ve retina taramak suretiyle işlenen kişisel veriler biyometrik veri kategorisinde kişiye özel olan fiziksel özellikleridir. Bu kapsamda, öncelikli olarak genel ilkeler ve özel nitelikli kişisel verilerin işlenmesi şartlarına riayet edilmesi gerekmekle birlikte aynı zamanda özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı Kararı ile belirlenen önlemlerin de alınması gerekmektedir. Özel nitelikli kişisel verilerin işlenme şartları dikkate alındığında biyometrik veriler yalnızca ilgili kişinin açık rızası ve kanunlarda öngörülen hallerde işlenebilecektir. Kanunlarda öngörülme şartı ile kastedilen husus özel nitelikli kişisel verilerin işlenmesine ilişkin olarak ilgili faaliyet alanına veya sektöre ilişkin kanunlarda ayrıca ve açıkça düzenleme olmasıdır (Anayasa Mahkemesi, 2018/11988 Başvuru Numaralı ve 10.03.2022 tarihli Karar). Mesai takibi ve güvenlik amacıyla işverene birtakım denetim yetkileri İş Kanunu ve İş Sağlığı ve Güvenliği Kanunu ile tanınabilmekle birlikte çalışanın mesai takibi ve bu amaçla özel nitelikli kişisel verilerin işlenmesine ilişkin açıkça bir düzenleme olmadığından yalnızca çalışanların açık rızası bulunması durumunda biyometrik veriler işlenecek olup işçi işveren arasındaki dengesizlik dikkate alındığında açık rızanın da kural olarak özgür iradeyle verilebileceğini söylemek mümkün değildir. Kanun'un 3'üncü maddesinin birinci fıkrasının (a) bendinde açık rızanın belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade ettiği belirtilmiştir. Rızanın özgür iradeyle verilmiş olması kişilerin verileri üzerinde kontrol hakkına sahip olması ve bireylere gerçek bir seçim hakkının tanınmış olması ile sağlanmaktadır. Özgür irade, dışarıdan gelen hiçbir sosyal, ekonomik, psikolojik veya bunlar dışındaki herhangi bir baskıya maruz kalmaksızın kararların ayırt etme gücüne sahip iken ve serbest irade ile vere-

bilmesi anlamına gelmektedir (Braun, 2018, s.22). Birey rıza vermemenin sonucunda hizmetten yararlanamıyor ise, yani reddin bir yaptırımı var ise bu bireyin karar verme mekanizmasını etkileyecek bir duruma sebebiyet verebilir (Küzeci, 2018, s.268). Bu durum özellikle güç dengesizliğinin var olduğu, tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda kendisini gösterebilmektedir (Kişisel Verileri Koruma Kurumu, Açık Rıza, s.6). Madde 29 Çalışma Grubu, bunu istihdam ve veri sorumlusu veya denetim makamının kamu otoritesi olduğu durumlar bağlamında açıklamaktadır. İstihdam bağlamında güç dengesizliği, işçi işveren arasındaki dengesizlikten kaynaklı olmaktadır. Örneğin, bir çalışanın mesai saatlerinin takibine ilişkin parmak izi sistemleri kullanılmasına herhangi bir baskı hissetmeden rıza göstermesi muhtemel görünmemektedir. Çalışana rıza göstermeme imkânının etkin bir biçimde sunulmadığı, rıza vermediği durumlarda işiyle ilgili olumsuz bir durumun ortaya çıktığı, işe alınma durumunun zarar gördüğü veya işveren tarafından kendisine karşı olumsuz bir muamele ile yaklaşılma ihtimalinin bulunduğu durumlarda çalışanın gerçek bir seçeneğe sahip olduğunu, dolayısıyla rızanın özgür iradeye dayandığını söylemek mümkün olmamaktadır (Kişisel Verileri Koruma Kurumu, Açık Rıza, s.6.). Dolayısıyla, işçi ile işveren ilişkisinin kendi dinamikleri işçinin rızasına başvurulmasını yanıltıcı hale getirebilmektedir (Küzeci, 2018, s.267). Öte yandan, çalışanlar biyometrik verilerinin işlenmesine dair açık rıza vermiş olsa dahi her halükârda veri işlemenin Kanun'da yer verilen genel ilkelere uygun olması gerekmektedir. Bu çerçevede, veri işleme faaliyetinin hukuki dayanağı açık rıza olsa bile işlenen kişisel verilerin mahiyeti de dikkate alındığında amaçla bağlantılı ve ölçülü bir yöntem olup olmadığının sorgulanması gerekecektir.

Biyometrik veri işleme suretiyle elde edilen fayda bir kişinin kesin ve doğru bir şekilde tanımlanması iken zarar ise kişinin biyometrik verilerine erişilmesi suretiyle kişinin ayrımcılığa, çalıştırılmamasına maruz kalmasıdır (Akgül, 2015, s.205). Bu çerçevede, işçinin biyometrik verilerinin işlenmesi sonucu ortaya çıkabilecek zararlar ile işverenin kişiyi kesin ve net olarak belirleyebilmesi sonucu ortaya çıkan fayda arasında bir denge testi yapılması gerekmektedir. Bu denge testi, başvurulan yöntemin işleme amacına ulaşılabilmesi bakımından elverişli olması, ulaşılmak istenen amaç bakımından gerekli olması, ulaşılmak istenilen amaç ve aracın arasında orantı bulunması hususları göz önünde bulundurularak yapılmalıdır (Kişisel Verileri Koruma Kurumu, Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber, s.9-10).

Zira, Danıştay'ın 2014/2242 Esas ve 2015/499 sayılı Kararına göre de ilgili kişilerin mesai takibi amacıyla parmak izinin alınması suretiyle kişisel verilerin işlenmesinin özel hayatın gizliliği ilkesi kapsamında bulunması karşısında uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağının bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmaması, işlemi hukuka aykırı hale getirmektedir. İşverenler tarafından sıklıkla tercih edilen biyometrik veri işleme suretiyle mesai takibi yöntemi parmak izi olup bu hususta mahkemeler ve Kişisel Verileri Koruma Kurulunun da kararları bulunmaktadır. Parmak izinin her bireyde farklı olduğu ve kişinin biyolojik olarak teşhisine imkan verecek nitelikte kişiye özgü bilgi içerdiği gözetildiğinde biyometik veri niteliğine haiz olduğu, bu durumda parmak izinin belirli bir gerçek kişi hakkındaki bilgi kapsamında olduğu dikkate alındığında bu bilgilerin işlenmesinin özel hayata saygı hakkı kapsamında kişisel verilerin korunmasını isteme yönü bulunmaktadır (Anayasa Mahkemesi, 2018/11988 Başvuru numaralı ve 10.03.2022 tarihli Karar). Kişisel Verileri Koruma Kurulunun 20/05/2020 tarihli ve 2020/404 sayılı Kararında ilgili kişinin çalışmış olduğu Şirket tarafından parmak izinin alındığı ve işçilere bunun zorunlu kılındığı, parmak izi alındığı sırada ilgili kişilerin açık rızalarının alınmadığı ve aydınlatma yükümlülüğünün de yerine getirilmediği iddialarına yönelik veri sorumlusu tarafından acil durum yönetimi sürecinin yürütülmesi, fiziksel mekan güvenliği ve yetkili kurum ve kuruluşlara bilgi verilmesi amaçlarıyla bu yöntemin kullanıldığı, parmak izlerinin kriptografik yöntemlerle muhafaza edildiği, bu sebeple bu verilerin biyometrik veri niteliği taşımadığı şeklinde savunma yapılmış olmakla birlikte Kurul tarafından yapılan inceleme neticesinde;

> *"...biyometrik verilerin hash yöntemi ile saklandıklarında biyometrik veri olma niteliklerini kaybetmedikleri, bu bakımdan açık rızanın bulunmadığı hallerde biyometrik verilerin ancak Kanunun 6 ncı maddesinde öngörülen kanunlarda öngörülme şartı doğrultusunda işlenebileceği, bununla birlikte söz konusu verinin işlenme amacının da Kanunun genel ilkeleri arasında yer alan "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine de aykırı olduğu, örneğin fiziksel mekan güvenliğinin sağlanabilmesi için giriş esnasında manyetik kart sistemi, RFID etiketi, cep telefonuna gönderilecek bir SMS'in sisteme girilmesi gibi alternatif yollar ile sağlanması mümkünken çalışanların biyometrik veri niteliğindeki parmak izi verisinin alınmasının Kanunun 4 üncü maddesinin (2) numaralı fıkrasında yer alan "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesi ile bağdaşmadığı, bu çerçevede "acil durum yönetimi sürecinin yürütülmesi, fiziksel mekan güvenliği ve yetkili kurum ve kuruluşlara bilgi verilmesi amaçları"nın farklı yollarla da hasıl olması mümkünken söz konusu veri işleme faaliyeti ile orantısız bir veri işleme yapıldığı"*

değerlendirmesinden hareketle ilgili veri sorumlusuna idari yaptırım uygulanmıştır. Söz konusu Kararda açık rıza olmaksızın biyometrik veri işlenmesi ve genel

ilkelere aykırı bir işlemenin varlığından bahsedilse de Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/81 sayılı Karar ve 31/05/2019 tarihli ve 2019/165 sayılı spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kararda;

> *"...Spor kulübünde giriş çıkış kontrolünün yapılabilmesi ve kulüp hizmetlerinden faydalanmak isteyen kişilere ilişkin giriş kontrolünün alternatif yollar ile sağlanması mümkün iken kişilerin biyometrik veri niteliğindeki avuç içi izi verisinin alınmasının 6698 sayılı Kişisel Verilerin Korunması Kanununun 4 üncü maddesinin (2) numaralı fıkrasında yer alan "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesi ile bağdaşmadığı, öte yandan özel nitelikli kişisel verilerin Kanun kapsamında ancak ilgili kişilerin açık rızasına ya da Kanunun 6 ncı maddesinin (3) numaralı fıkrasında sayılan şartlar çerçevesinde işlenebileceği, bu kapsamda adı geçen veri sorumlusu tarafından avuç içi izi verisinin işlenmesi için kişilerden açık rızalarının alınması yoluna gidildiği ancak açık rıza verilmemesi durumunda kulüp hizmetlerinden yararlanamadıkları dikkate alındığında üyelerden alınan açık rızanın Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırılık teşkil etmesi nedeniyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında idari para cezası uygulanmasına..."*

değerlendirmelerine yer verilmiştir. Bu çerçevede, her ne kadar işverenler ilgili kişilerin biyometrik verilerini işleyebilmek adına açık rızalarına başvursa da bu geçerli bir veri işleme şartı olmayacak, açık rızanın özgür iradeyle verilmemiş olması ve işleme faaliyetinin genel ilkelere uygun olmaması biyometrik verilerin işlenmesini hukuka aykırı hale getirecektir.

Zira, Danıştay'ın 2013/5342 Esas ve 2013/9525 numaralı bir kamu kurumunda çalışanların mesai takibinde parmak izi uygulamasının kullanılmasına ilişkin vermiş olduğu Kararda mesai kontrol sisteminin şekli ve içeriği dikkate alındığında, sözü edilen uygulama ile kurumca amaçlanan kamu yararı arasında orantılılık bulunmadığından bu uygulamanın, anayasal ilke olan ölçülülük ilkesine aykırılık teşkil ettiğine karar verilmiştir. Bu çerçevede, amaca ulaşmak için daha az müdahaleci yöntemler mevcut iken biyometrik veriler işlenmek suretiyle giriş, çıkış ve geçiş takibi yapılması amaçla bağlantılı ve ölçülü olma ilkesine aykırılık teşkil edecektir.

Buna karşın, imza defteri ve manyetik kimlik kartı uygulamaları ile takibin yapılmasının amaca hizmet edemeyeceği yetkisiz girişlerin engellenmesi zaruri olan tehlikeli işler, fiziki ve işlem güvenliği bakımından önem arz eden iş yerleri

bakımından biyometrik yöntemlerin kullanılması gerekecektir. İş yerinin güvenliğinin sağlanması ve korunmasına ilişkin üstün yarar/meşru bir amacın varlığı bulunması durumunda, hak ve özgürlüklere daha az müdahale ile bu amacı gerçekleştirmeye elverişli başka bir yolun olmaması halinde amaçla sınırlı olmak üzere (Anayasa Mahkemesi, 2018/11988 Başvuru Numaralı ve 10/03/2022 Tarihli Karar) işçinin biyometrik verilerinin işlenmesinin dayanağı Kanunun 6'ncı maddesi uyarınca kanunlarda öngörülme ve açık rıza olabilecek olup işverenler tarafından kanunlarda biyometrik verilerin bu amaçlarla işlenmesine ilişkin herhangi bir hüküm mevcut değil ise açık rızanın tüm unsurları göz önünde bulundurularak işçilerden açık rıza alınması gerekecektir. Bu hususta, açık rızanın özgür iradeye dayalı olarak verilemeyeceği ve açık rıza verilmemesi gibi bir seçeneğin bulunmaması dolayısıyla unsurların tam olarak karşılanamayacağı ve açık rızanın geçersiz kabul edilebileceği yönünde değerlendirilme yapılabilecek olsa da veri sorumlusunun işin niteliği gereği bu yola başvurması zaruri, başka bir seçeneği de yok ve bu hususlar kanıtlanabiliyor ise açık rızanın unsurlarının yerine getirilmediği yönünde değerlendirme yapılmamasının da mümkün olabileceği düşünülmektedir. Ancak, bu durumda da işverenin amacı dışında söz konusu verileri kullanmaması ve amacına yönelik kullanım sonrasında biyometrik verileri imha etmesi gerekecektir.

Manyetik Kimlik Kartı, İmza Defteri

Çalışanların işe giriş çıkış ve birimler arası geçişlerinin kontrolü için kullanılan yöntemlerden en az müdahaleci nitelikte olanları manyetik kimlik kartı ve imza defterleridir. Bunlar, biyometrik verileri işlemek yerine alternatif olarak tercih edilebilecek yöntemler olup kartlar temaslı ya da temassız olma özelliğine sahip olabilmekte, genellikle de temassız okuma özelliğine sahip olan RFID (Radio Frequency Identification) okuyucular tercih edilmektedir. RFID, radyo frekansı ile haberleşen ve içinde belirli bir miktarda bilgi tutabilen (benzersiz bir numara) bir teknolojidir (Gaukler ve Seifert, 2007, s.30). Kullanılacak kart ile okuyucu birbirine entegre olup eşleşme sağlandığı durumlarda geçişe izin verilmektedir (Kartlı Geçiş Sistemi Nedir? Çalışma Prensibi Nasıldır?, 2022). Bu açıklamalardan anlaşıldığı üzere kart ile geçiş sistemlerinde kişiye özel benzersiz bir numaranın kartla eşleşmesi sonucu doğrulama yapılmakta ve geçiş sağlanmaktadır. İşverenler tarafından amaçlandığı üzere giriş, çıkış saatleri ile numara arasında eşleşme yapıldığından bu yöntemlerin amaçla bağlantılı olduğunu söylemek mümkündür.

Öte yandan, işçilerin başkası yerine imza atma ve kart okutma gibi yöntemlere başvurması işverenlerin biyometrik yöntemlere yönelmesine yol açsa da (Uncular, 2014, s.95) işçilerin bu yöntemlere başvurmaması adına uyarılması ve tespit

edildiğinde uygulanacak yaptırımların belirlenerek işçilere bu hususta bilgilendirme yapılması ile kötü niyetli kullanımların önüne geçilmesi sağlanabilecektir. Bununla birlikte, imza defterine çalışanların isimlerinin bulunduğu kısma imza atması ve saat yazması gibi yöntemler ile de işveren tarafından amaca ulaşılabilmekle birlikte ıslak imza davranışsal statik bir (imzanın nasıl göründüğü veya geometrik özelliklerine göre analiz edilmesi) biyometrik veri olarak kabul edilmekle (Article 29 Data Protection Working Party, 2012, s.27) beraber işverenin mesai takibi amacıyla elde ettiği imza ile biyometrik bir analiz yapılmadığı dikkate alındığında amaçsal bir yorum yaparak işverenin biyometrik veri işlemediği değerlendirmesi yapılabilecektir. Elbette ki böyle bir yoruma varılması ancak imzanın sadece kimlik doğrulama amacıyla kullanılması ve biyometrik herhangi bir işleme tabi tutulup sonucunda başka bir veri seti elde edilmemesi ile mümkün olabilecektir.

Bu çerçevede, manyetik kimlik kartları ve imza defteri ile güvenlik ve mesai takibinin genel nitelikte kişisel verilerin işlenmesi kapsamında değerlendirilebileceği dikkate alındığında; bu veri işleme faaliyetinin İş Kanunu'nda yer alan çalışma saatlerine riayet edilip edilmediğinin tespiti amacıyla gerçekleştirilmesi durumunda işverenin meşru menfaati kapsamında (Kişisel Verilerin Korunması Kanunu 5'inci maddenin ikinci fıkrasının (f) bendi) değerlendirilmesi mümkün olmaktadır. Ayrıca, işverenin fazla çalışma saatlerini tespit ederek bu kapsamda işçiye ek ödeme yapması durumunda ise bir hakkın tesisi (Kişisel Verilerin Korunması Kanunu 5'inci maddenin ikinci fıkrasının (e) bendi) kapsamında söz konusu verinin işlendiğini söylemek mümkündür.

Öte yandan, işverenin güvenlik amacıyla bu verileri işlemesi durumunda ise İş Sağlığı ve Güvenliği mevzuatı söz konusu olabilecek olup bu kapsamda bir güvenlik önlemi mevcut ise kanunlarda öngörülme şartı (Kişisel Verilerin Korunması Kanunu 5'inci maddenin ikinci fıkrasının (a) bendi) gündeme gelebilecek olmakla birlikte bu mevzuatta yer edinmemiş ancak işverenin denge testi yapılması suretiyle meşru menfaati söz konusuysa meşru menfaat kapsamında da veriler işlenebilecektir. Bu çerçevede, amaca göre veri işleme şartının değişebileceğini söylemek mümkündür.

Güvenlik Kameraları

İşverenin iş yeri giriş çıkışına ve birimler arası geçişlere yerleştirmek suretiyle ve mesai takibi ve yetkisiz girişlerin engellenmesi amacıyla çalışanların kişisel verilerini işlemesi de mümkündür. Güvenlik kameraları, birçok amaca aynı anda hizmet edebileceğinden iş yeri güvenliğinin sağlanmasına yönelik konumlandırılmış kameraların da bu amaçla kullanılabilmesi mümkündür. Manyetik kartlar ve imza defterlerindeki çalışanların suiistimallerinin tespiti için onlar ile birlikte ek olarak güvenlik kamerası konulması da gündeme gelebilmektedir. Bu tespitin yapılabilmesi imza defterinde imzaların karşılaştırılması ile kısmen mümkün olabilirken kartlı geçişlerde pek de mümkün görünmemektedir.

Bu çerçevede, işverenin olası bir suiistimalin tespiti için güvenlik kamerası vasıtasıyla takipte bulunmasında menfaat bulunduğu iddia edilebilecekken işverenin bu yönteme yalnızca şüphe duyulduğu takdirde başvurması da işverenin amacına hizmet edebilecektir. Zira, Danıştay'ın 2015/5190 Esas numaralı Kararında bir hastanede mesai takibi amacıyla elektronik sisteme entegre edilen kamera vasıtasıyla rıza aranmaksızın her işlem esnasında personelin fotoğrafının çekildiğine ilişkin uygulama hizmetin gerektirdiği güvenlik düzeyi ile orantılı olmadığı ve personelin örgütsel bağlılık düzeyini olumsuz yönde etkileyecek nitelikte bulunduğundan uygulamanın kaldırılmasına ilişkin talebin reddine ilişkin ilk derece mahkemesinin vermiş olduğu karar hukuka aykırı bulunarak yürütmenin durdurulmasına karar verilmiştir. Öte yandan, kameralar vasıtasıyla da imzada olduğu gibi biyometrik yöntemlerle analiz edilmesi sonucu biyometrik veriler elde edilebilecektir. Burada dikkat edilmesi gereken hususun işverenin amacının net bir biçimde ortaya konulması ve amacın dışında herhangi bir veri işleme faaliyeti gerçekleştirilmemesidir.

İŞÇİNİN ELEKTRONİK ORTAMDA GÖZETLENMESİ

İş yöntemlerinin teknolojik gelişmelerle birlikte değişmesi ile birlikte işveren, kaynakların verimli kullanılmasını sağlamak, ticari gizliliği ve yönetim risklerini korumak, kanuni yükümlülükleri yerine getirmek, çalışanlar tarafından suç işlenmesini önlemek (European Commission, 2021, s. 10; Beytar, 2018, s. 188.), cezai ve hukuki sorumluluğa karşı korunmak, bilgi akışının kontrolünü sağlamak (Anayasa Mahkemesi, 2016/13010 Başvuru Numaralı ve 17/09/2020 Tarihli Karar) amaçlarıyla işçiyi elektronik yöntemlerle gözetim altında tutmaktadır. Mevcut teknolojik gelişmeler ve yeni çalışma stilleri ile organizasyonları çalışanların daha çok gözetlenmesini tetikleyen unsurlar olarak karşımıza çıkmakta ve işçilerin temel hak ve özgürlüklerine kolaylıkla müdahale edilebilecek şekilde kullanım imkânları sunmaktadır. İş yerinde işveren tarafından işçilerin kullanması amacıyla tahsis edilen iletişim araçlarının işverene ait olması nedeniyle işverenin sınırsız ve mutlak gözetleme denetleme yetkisinin bulunduğunun kabul edilmesi, işçinin temel hak ve özgürlüklerine iş yerinde de saygı gösterilmesi yönündeki makul beklentisine aykırılık teşkil edecektir (Anayasa Mahkemesi, 2016/13010 Başvuru Numaralı ve 17/09/2020 Tarihli Karar).

Her ne kadar dijital sistemler ve yeni iletişim teknolojileri denetim ve gözetim fark edilebilirliğini en alt düzeye çekse de aşırı ve orantısız izleme hukuka aykırılık barındırabileceği gibi aynı zamanda işçinin üzerinde psikolojik olumsuzlukları da beraberinde getirmekte ve stres, baskı, güvensizlik ve iş verimliliğinde düşüşe sebebiyet vermektedir. İşçilerin iş yerinde belirli bir derecede mahremiyet hakkına sahip olmalarına karşın bu hakkın işverenin işleyişi kontrol etme ve savunma hakkı ile dengelenmesi gerekmektedir (Article 29 Data Protection Working Party, 2002, s.6). Bu anlamda, işverenin gözetiminin iş ilişkisi çerçevesinde kalması gerekirken bazı durumlarda bu gözetim çalışanların mahremiyetlerine de zarar verebilmektedir. Mahremiyet "kişilerin yalnız başlarına kalabildikleri, başkalarıyla hangi koşullarda ilişki içerisine gireceklerine kendilerinin karar verebildikleri bir alan" olarak tanımlanabilmekte olup (Çelikoğlu, 2007, s.11; Yüksel, 2003, s.182) bireylerin başkalarından sakındıkları ve bilinmesini istemedikleri bir alana sahip olma hakları vardır. Mahremiyet soyut bir kavram olmakla birlikte çalışma alanında sınırlarının çizilebilmesi de bazı zorluklar barındırmaktadır. Bu çerçevede, işverenlerin elektronik ortamda gerçekleştireceği gözetim mekanizmaları bakımından çalışma alanı ve kişinin mahrem alanı ayrımını net bir şekilde belirlemesi gerekmektedir. Zira, iş yerinde izleme ve gözetleme uygulamaları neticesinde işçinin maddi ve manevi varlığını koruma ve geliştirme hakkı, haberleşme özgürlüğü, ifade özgürlüğü, özel hayatın gizliliği ve kişisel verilerin korunması hakkı gibi temel hak ve özgürlükleri zarar görebilecektir (Uncular, 2018, s.237).

Elektronik iletişimin denetlenmesi haberleşme hürriyeti ile bizzat ilişkilidir. Anayasa'nın 22'nci maddesinde güvence altına alınan haberleşme hürriyeti, haberleşmenin içeriğinin gizliliğini de güvence altına almakta olup haberleşme bağlamında bireylerin karşılıklı ve toplu olarak sözlü, yazılı ve görsel iletişimlerine konu olan ifadelerin gizliliğinin sağlanması ve haberleşmeye yönelik haksız müdahalede bulunulmaması gerekmektedir (Anayasa Mahkemesi, 2013/7054 Başvuru Numaralı ve 06/01/2015 Tarihli Karar). Bu anlamda, işveren tarafından iletişimin denetlenmesine yönelik gerçekleştirilecek denetimler kişinin birçok hakkına aynı anda müdahale niteliği taşıyabilecek olup müdahalenin haksız olmaması ancak hukuka uygunluğunun sağlanması ile mümkün olabilecektir.

Öte yandan, bireyler dijital alanlarda gerçek hayata oranla gözetim altında olduklarının ve izlendiklerinin daha az bilincinde olduğundan (Çaycı ve Çaycı, 2016, s.160; Article 29 Data Protection Working Party, 2017, s.10) işverenler tarafından bu gözetimlerin amacının belirli açık ve meşru bir şekilde belirlenmesi ve bu kapsamda bilgilendirmenin yapılması büyük önem arz etmektedir. Uluslararası Çalışma Örgütü'nün işçinin kişisel verilerinin korunmasına ilişkin kılavuzunda da işçiler izleniyorsa izleme nedenleri, zaman çizelgesi, kullanılan yöntem ve

teknikler ve toplanacak veriler hakkında önceden bilgilendirilmesi gerektiği ve işverenin işçilerin özel hayatına müdahaleyi en aza indirmesi gerektiği genel ilke olarak belirlenmiştir (International Labour Organisation, 1997, s.18). İşverenler tarafından bazı durumlarda izlenen personelin bilgisi olmaksızın gizli izleme yöntemlerine başvurulabilmekle birlikte kılavuzda gizli izlemeye yalnızca ulusal mevzuat uygun ise, makul gerekçelerle suç faaliyeti veya yanlış yapıldığına ilişkin ciddi bir şüphe varsa başvurulabileceği belirtilmektedir (International Labour Organisation, 1997, s.4).

Kişisel Verilerin Korunması Kanunu kapsamında aydınlatma yükümlülüğü yerine getirilmeksizin kişisel verilerin işlenmesi faaliyeti hukuka uygun olmayacaktır. Ancak, Kanun'un istisnalarının belirlendiği 28'inci maddedeki durumlardan birinin ortaya çıkması halinde kısmi veya tam istisna olması fark etmeksizin aydınlatma yükümlülüğü yerine getirilmeyecek olup uygulamada işçi işveren ilişkisi bağlamında Kanun'dan istisna sayılabilecek bir veri işleme faaliyetinin bulunmadığı değerlendirilmektedir. Bu çerçevede, istisnalardan yalnızca 28'inci maddenin ikinci fıkrasının (a) bendinde yer alan *"Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması."* şartı uygun olarak düşünülebilecek olsa da söz konusu suçun işlenmesinin önlenmesinden anlaşılması gereken; yalnızca suçun işlenmesini önlemekle görevli kişi ve kurumlar tarafından bu faaliyetin gerçekleştirilmesi durumudur. Bu anlamda, suçun işlenmesi ve suç soruşturmasının yürütülmesi hususunda kolluk ve yargı makamları yetkili olup işverenin bu şekilde bir görevi ve yetkisi bulunmamakla birlikte suçun işlenmesini önlemeye yönelik araçlara da sahip değildir.

Sonuç olarak, işverenin bu anlamda bir faaliyet gerçekleştirmesi mümkün olmayıp işverenlerin gizli izleme yapmak suretiyle kişisel verileri işlemesi hukuka aykırı olacak ve işverenlerin işçiyi önceden bilgilendirmek suretiyle amaçlarını da net bir şekilde ortaya koyarak İş Kanunu'nun 25'inci maddesinde yer alan ahlak ve iyi niyet kurallarına uymayan haller ve benzerlerinin bulunması, işverenin meşru menfaatinin aksine bir durumdan şüphe duyulması durumlarında izleme gerçekleştirilebilecektir. Ancak, aydınlatma yükümlülüğü yerine getirilirken hangi durumlarda izleme yapılabileceğinin net bir şekilde belirtilmesi gerekmektedir. Bu durumda da izleme suretiyle gerçekleştirilecek kişisel verileri işleme faaliyetlerinin yalnızca ilgili personelle sınırlı tutularak, amaca yönelik kişisel veri ile sınırlı olarak ve yalnızca amaçlanan çerçevede sürdürülmesi gerekmektedir.

Bu çerçevede, örneğin işveren bir çalışanının ticari sırlarını ifşa ettiği ihtimali üzerinde durmakta ve bu kapsamda işçinin e-postasını izlemesi gerekmektedir. İşverenin işçiye baştan itibaren e-posta verilerinin izleneceği yönünde bildirim

yapmadığı bir senaryoda işverenin bu aşamadan sonra kuvvetli ve somut bir şüphesi bulunsa da aydınlatma yapılmaksızın e-posta aracılığıyla kişisel verileri elde etmesi hukuka aykırı olacaktır. İşverenin bu tarz durumlarla karşılaşmaması adına işçileri bu yöndeki izlemelere karşı önceden bilgilendirmesi, bilgilendirmede bulunan koşulların varlığı halinde de kişisel verileri işlemesi uygun olacaktır. İşçinin iş yerinde izlenmesi ve gözetlenmesi, altyapı ve uygulama açısından gelişen bilgi ve iletişim teknolojileri ile birlikte işçinin temel haklarına ve özgürlüğüne yönelik müdahaleci, riskli ve kuşatıcı yöntemlere dayanmaktadır. Bu nedenle, gözetleme sırasında elde edilen verinin bu kapsamda elde edilecek amaç için yeterli ve ilgili olması gerekmekte olup mümkün olan en az müdahaleci yöntemlerin tercih edilmesi gerekmektedir (Article 29 Data Protection Working Party, 2001, 2001, s.4).

Ek olarak, işveren tarafından gerçekleştirilecek kişisel veri işleme faaliyetinin hukuki bir dayanağı olması gerekmekte olup işverenin elektronik ortamda gerçekleştireceği izleme faaliyetleri bakımından açık rızaya başvurulması yanıltıcı olabilecektir. Zira, açık rızaya ancak işçinin özgür seçime sahip olduğu durumlarda başvurulması gerekmekte olup somut durumda işçinin rıza vermemesi veya rızasını geri çekmesi durumunda işveren tarafından izleme yapılması veya izlemeye devam edilmesi bu bağlamda açık rızanın uygun bir kişisel veri işleme dayanağı olmadığını kanıtlamaktadır. Öte yandan, işveren tarafından açık rızası olmayan işçiler bakımından izleme yapılmaması gibi bir seçenek mevcut ise açık rızası bulunan işçiler bakımından izleme yapılması genel ilkelere uygun bir işleme olmadığını göstermektedir.

Türk Borçlar Kanunu'nun "Özen ve Sadakat" borcu başlıklı 396'ncı maddesinde;

> *"İşçi, yüklendiği işi özenle yapmak ve işverenin haklı menfaatinin korunmasında sadakatle davranmak zorundadır. İşçi, işverene ait makineleri, araç ve gereçleri, teknik sistemleri, tesisleri ve taşıtları usulüne uygun olarak kullanmak ve bunlarla birlikte işin görülmesi için kendisine teslim edilmiş olan malzemeye özen göstermekle yükümlüdür. İşçi, hizmet ilişkisi devam ettiği sürece, sadakat borcuna aykırı olarak bir ücret karşılığında üçüncü kişiye hizmette bulunamaz ve özellikle kendi işvereni ile rekabete girişemez. İşçi, iş gördüğü sırada öğrendiği, özellikle üretim ve iş sırları gibi bilgileri, hizmet ilişkisinin devamı süresince kendi yararına kullanamaz veya başkalarına açıklayamaz. İşverenin haklı menfaatinin korunması için gerekli olduğu ölçüde işçi, hizmet ilişkisinin sona ermesinden sonra da sır saklamakla yükümlüdür."* hükmü bulunmaktadır.

Bu çerçevede, işverenin söz konusu veri işleme faaliyeti bakımından bu maddede öngörülen denetimi gerçekleştirmek için kişisel veri işlemesi gerekli olsa da ilgili Kanun maddesinde kişisel verilerin işleneceğine ilişkin açıkça bir hüküm bulunmaması nedeniyle işverenin "kanunlarda açıkça öngörülmesi" işleme şartına dayanması, Anayasa'da da yer alan temel hak ve özgürlüklerin kanunlarla sınırlandırılabileceği ilkesine de ters düşmektedir.

Öte yandan, kanunlarda açıkça öngörülmeden anlaşılması gerekenin bir Kanun'un gerektirdiği bir işin dolaylı olarak kişisel veri işlenmesini zorunlu kılması, ayrıca kişisel verilerin işlenebileceğine ilişkin herhangi bir ifade yer almaması veri işleme faaliyetinin kanunda açıkça öngörüldüğü anlamına gelmeyecektir. Zira, bu şekilde yorumlanmaması durumunda kişisel verilerin müdahaleye açık hale geleceği aşikardır. İşverenin veri işleme faaliyetinin dayanağı bakımından meşru menfaat kapsamında veri işlemesi söz konusu olabilecek olup ilgili kişinin temel hak ve özgürlüklerine zarar verilmemesi ve işlemenin zorunlu olması hususlarına riayet edilmesi, bunun sağlanabilmesi için de meşru menfaat denge testinin yapılması önem arz etmektedir.

Ayrıca, işveren tarafından, bir ihtilaf bulunması durumunda tespit etme amacıyla örneğin bir mahkemede delil olarak kullanılması suretiyle işverenin savunma hakkını kullanabilmesi için elektronik iletişimin denetlenmesi söz konusu olabilecektir. Bu çerçevede, işverenin bu kapsamda gerçekleştirdiği kişisel verilerin işlenmesi faaliyetinin dayanağı Kanun'un 5'inci maddesinin ikinci fıkrasının (e) bendinde yer alan "bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" şartı olabilecektir.

İşin niteliğine bağlı olarak değişebilecek olan sözleşmenin ifasının gerektirdiği hususlar elektronik iletişimin sürekli olarak denetlenmesini de mümkün kılabilecektir. Örneğin, bir çağrı merkezinde çalışan işçiler bakımından telefon, e-posta ya da bir uygulama aracılığıyla gerçekleştirilen görüşmelerin kayıt altına alınması veri sorumlusunun sözleşmenin yükümlülüğünün gereği gibi yerine getirilip getirilmemesi, ayrıca işlem güvenliği bakımından söz konusu kayıtların saklanması bakımından denetimin gerçekleştirilmesi için zorunluluk arz edebilecektir. Bu yönde işin niteliğinin söz konusu araçların sürekli olarak izlenmesini gerektirdiği durumlarda işverenin Kanun'un 5'inci maddesinin ikinci fıkrasının (c) bendinde yer alan bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması şartına dayalı olarak kişisel verileri işlemesi mümkün olabilecektir.

İşverenler tarafından farklı amaçlara hizmet edebilecek şekilde birçok elektronik

izleme yöntemi bulunmakla birlikte başlıca izleme yöntemleri bilgisayar ve internet kullanımı, e-posta kullanımı, telefon kullanımı gibi iletişimin denetlenmesine yönelik yöntemler ve araç GPS takibi ve giyilebilir cihaz takibi ile konumun denetlenmesine yönelik yöntemlerdir. Bu anlamda, söz konusu yöntemlere ilişkin detaylı bir değerlendirme yapılmasında fayda görülmektedir.

Bilgisayar, İnternet ve E-Posta Kullanımı

İşverenlerin farklı kurumsal yapıları farklı amaçlarla bilgisayar ve internet kullanımına ilişkin izleme yapmasına olanak vermektedir. İşçinin bilgisayar, internet, e-posta ve telefon kullanımı sonucunda bu araçlarda bulunan ve belirli bir gerçek kişi hakkında bilgiye ulaştırabilecek bilgiler kişisel veri niteliğinde olup işveren tarafından bu bilgilere erişilmesi suretiyle gerçekleştirilen kişisel veri işleme faaliyeti de kişisel verilerin korunmasını isteme hakkı kapsamında bulunacaktır (Anayasa Mahkemesi, 2016/13010 Başvuru Numaralı ve 17/09/2020 Tarihli Karar). Genel olarak, işverenin bu yönde bir izleme yapması; işverenin iletişim araç ve gereçlerini işçinin kullanımına sunması sonucunda oluşan uyuşmazlıkların çözümü (Anayasa Mahkemesi) bilgi güvenliği süreçlerinin yürütülmesi ve iş faaliyetlerinin yürütülmesi ile denetimi kapsamında değerlendirilebilecektir.

Elektronik araçlarla gerçekleştirilecek izleme öncesinde işverenler tarafından bir değerlendirme yapılması suretiyle izlemenin gerekliliğine karar verilmesi gerektiğine ilişkin Madde 29 Çalışma Grubunun iş yerinde elektronik iletişimin gözetimi hakkında çalışma belgesinde bazı ilkeler belirlenmiştir. Buna göre; izlemenin işçiler için şeffaf olup olmadığı, işveren açısından bu izlemenin gerekli bulunup bulunmadığı ve daha geleneksel yöntemlerle aynı sonuca ulaşılıp ulaşılamayacağı, işlenecek olan kişisel verilerin çalışanlar açısından yasal olup olmadığı ve kişisel verilerin ulaşılması istenen amaçla orantılı olup olmadığı hususunda bir değerlendirme yapılması gerektiği belirtilmektedir (Article 29 Data Protection Working Party, 2002, s. 4). Bu ilkeler esasen Kişisel Verilerin Korunması Kanunu kapsamında yer alan genel ilkeler ve aydınlatma yükümlülüğünün yerine getirilmesi ile bağlantılı olup her veri işleme faaliyetinde öncelikli olarak dikkate alınması gereken hususlardır. Öncelikli olarak şeffaflığın sağlanabilmesi adına elektronik araçlar vasıtasıyla kişisel verilerin işlenmesinin öncesinde işçinin "Aydınlatma Yükümlülüğü" ve buna ilişkin tebliğ kapsamında bilgilendirilmesi gerekecektir. Burada önem arz eden bir husus da elektronik izlemenin gizli yapılabilmesinin diğer izlemelere oranla daha olası olduğu dikkate alınarak gizli izlemenin hukuka uygun olmayacağı ve işçinin her halükârda önceden bilgilendirilmesinin gerektiğidir.

Türk Borçlar Kanunu'nun 396'ncı maddesi uyarınca işçinin özen ve sadakat borcu bulunduğundan bahsedilmişti. Bu çerçevede, işverenin iş yerindeki internet, bilgisayar ve e-posta ile telefon kullanımını tamamen iş amaçlı kullanım için özgülemesi mümkün olup iş amaçlı kullanım yalnızca bu araçların iş sözleşmesi kapsamında işin ifasının yerine getirilmesi için kullanılmasıdır (Gürsel, 2016, s. 380). İşverenin, elektronik iletişimin özel amaçlı kullanımı sonucunda bu araçlara gelebilecek muhtemel zararları önlemek (Uncular, 2018, s. 249), mesai saatleri içerisinde özel amaçlı kullanımın yol açacağı vakit kaybını önlemek, işçinin işveren nezdinde bulunan elektronik iletişim araçları ile gerçekleştirmiş olduğu eylemlerden işverenin de hukuki ve cezai olarak sorumlu tutulabileceği durumların oluşması ihtimalini ortadan kaldırmak gibi amaçlarla bu yöndeki kullanımları engellemeye yönelik birtakım tedbirler alması mümkündür. Ancak bu tedbirlerin işçinin özel kullanım gerçekleştirip gerçekleştirmediğini tespit etmek yerine teknik yollarla cihazların bu amaçlarla kullanımının engellenmesi şeklinde gerçekleştirilmesi daha iyi bir yöntem olacaktır (Article 29 Data Protection Working Party, Opinion 2/2017, s.15). Örneğin, işverenin çıkarlarına aykırı ya da kötüye bir kullanım olarak değerlendirilebilecek bir bahis oyun sitesinin kullanılıp kullanılmadığının denetlenmesi yerine işverenin kendi cihazlarından ya da kendi internet ağından söz konusu siteye girişin engellenmesi şeklinde bir uygulamada bulunması kişisel verilerin korunması hakkı bağlamında daha az müdahaleci olacaktır.

Öte yandan, işverenin bu kontrollerdeki amacı yalnızca bunlarla sınırlı olmayıp Borçlar Kanunu'nun 396'ncı maddesinin devamında sadakat borcu ve sır saklama yükümlülüğü düzenlenmiştir. Bu kapsamda, işverenin elektronik iletişim araçları ile işçinin sadakat yükümlülüğüne aykırı şekilde davranıp davranmadığını tespit edebilmesi için bu araçların kontrol ve denetimini yapması gerekecektir. Ancak, günümüz çalışma sistemleri düşünüldüğünde özel hayat ve profesyonel hayatın kolaylıkla ayırt edilmesi pek de mümkün görünmemektedir. Çalışma koşulları, çalışma saatleri (evden, uzaktan çalışma), işçinin kendi elektronik araçlarını iş için de kullanıyor olması, işverenin elektronik araçların kullanımında özel kullanıma da izin vermesi gibi fiziksel çalışma ortamının dışındaki faaliyetlerin izlenmesi özel hayat ile iş hayatı arasındaki çizgilerin silikleşmesine neden olmaktadır (Article 29 Data Protection Working Party, 2017, s.4; International Labour Organization, s.9).

Bu anlamda, işverenin elektronik araçlar vasıtasıyla izleme yapacağı durumlarda bu ayrımın farkında olması ve sınırlarını baştan çizmesi, sonrasında yaşanabilecek olası özel hayat ihlallerinin de önüne geçebilecektir. İşçinin işveren nezdinde ve işveren tarafından tahsis edilmiş araç ve gereçleri özel amaçla kullanması duru-

munda bu kullanımların denetlenmeyeceği yönünde bir makul beklentisi olabilir. Ancak, işverenin de yukarıda bahsedilen güvenlik ve sadakat yükümlülüğünün yerine getirilip getirilmediğini denetlemesi, özel ve iş alanı arasındaki ayrımın silikleşmesi nedeniyle iş alanı ile sınırlı kalamayacaktır. Bu anlamda, her ne kadar işçinin iş yeri nezdindeki elektronik cihazların gözetlemeye tabi olduğuna ilişkin bilgisinin bulunması gerekse de işverenlerin özel amaçlı kullanımlara karşı ve bu yönde bir kullanımın da denetime hangi amaçlarla tabi olacağı konusunda işçiyi bilgilendirmesi gerekmektedir. Zira, işçinin iletişimin denetlenebileceği ve kullanım koşullarına ilişkin net bir bilgilendirme yapılmayan durumlarda temel hak ve özgürlüklerinin korunacağına ilişkin makul bir mahremiyet beklentisi olabilecektir (Anayasa Mahkemesi, 2016/13010 Başvuru Numaralı ve 17/09/2020 Tarihli Karar).

Aydınlatma yükümlülüğü kapsamı dışında bu bilgilendirmenin asgari olarak; şirketin sahip olduğu iletişim olanaklarının çalışanlar tarafından kişisel/özel iletişim için ne ölçüde kullanılabileceği (kullanım süresi/süre sınırlaması), varsa gözetimin gerçekleştirilme nedenleri ve amaçları, gözetim önlemlerinin kim tarafından nasıl ve ne zaman alınabileceği ve ihlalin tespit edilmesi durumunda izlenecek prosedürlerin ayrıntıları hususlarını içermesi sürecin şeffaflığını sağlayacaktır (Article 29 Data Protection Working Party, 2002, s.15; Anayasa Mahkemesi, 2016/13010 Başvuru Numaralı ve 17/09/2020 Tarihli Karar). Bilgilendirme belli bir şekil şartına bağlı olmamakla birlikte şeffaflığın (Anayasa Mahkemesi, 2016/13010 Başvuru Numaralı ve 17/09/2020 Tarihli Karar) ve işçiler üzerindeki farkındalığın sürdürülebilirliği adına bu bilgilendirmelerin işçilerin her zaman kolaylıkla ulaşabilecekleri yerlerde ve belli aralıklarla hatırlatmada bulunmak suretiyle yapılması önem arz etmektedir.

Yargıtay 22. Hukuk Dairesinin 2017/21857 Esas ve 2019/9884 numaralı Kararında işverenin işçinin bilgisayarına bir izleme programı yerleştirildiği ve bu konuda işçinin bilgilendirilmediği, işçinin rızası ve bilgisi olmaksızın özel veya işe ilişkin bilgi ayırt edilmeksizin günlük olarak elde edilmesi sonucunda elde edilen bilgilerin fesih sebebi olarak sayılamayacağı sonucuna varılmıştır. Ayrıca, işverenin yönetim hakkı çerçevesinde işçiyi elektronik ortamda takip etmesinin mümkün olduğu ancak bu izleme hakkında işçinin bilgilendirilmiş olması gerektiği belirtilmektedir. İşçinin hangi yöntemlerle izlendiğine dair bilgilendirilmemiş olması ve gizlice izlenmesi neticesinde elde edilen verilerin iş sözleşmesinin işçi tarafından ihlal edildiğini açıkça ortaya koysa da hukuka aykırı kabul edileceği ve bunun haklı fesih sebebi olarak ileri sürülemeyeceğine karar verilmiştir.

Ayrıca, Kişisel Verileri Koruma Kurulunun 25/11/2021 tarihli ve 2021/1187 sayılı

Kararında; işveren tarafından tahsis edilen kurumsal e-posta hesabının yalnızca işin ifası kapsamında kullanılabileceği veya işveren tarafından kurumsal e-posta hesabının denetlenebileceğine ilişkin mevzuat kapsamında herhangi bir aydınlatma yapılmadığı gerekçesiyle veri sorumlusu hakkında idari para cezası uygulanmıştır.

Öte yandan, elektronik araçlarla gözetim suretiyle gerçekleştirilen kişisel veri işleme faaliyetinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması gerekmektedir. İşveren tarafından işçinin kişisel verilerinin korunması hakkı ve haberleşme hürriyetine yapılan müdahale, işverenin ulaşmak istediği amacı ile ilgili ve elverişli olmalı, öte yandan bu doğrultuda işlenen kişisel verilerin yalnızca işverenin kişisel veri işleme faaliyetine konu amacı ile bağlantılı olarak kullanılması gerekmektedir (Anayasa Mahkemesi, 2016/13010 Başvuru Numaralı ve 17/09/2020 Tarihli Karar). Bu anlamda, her işverenin elektronik ortamda her türlü kişisel veriyi yukarıda bahsedilen amaçlarla işlemesi zorunlu olmayıp işverenler işin niteliği gereği risklerini belirlemeli ve riskin türüne ve derecesine göre özel olarak bir veri işleme politikası oluşturmalıdır (Article 29 Data Protection Working Party, 2002, s.17). Sürekli ve otomatik olarak işçilerin elektronik araçlarında izleme yapılması orantılı olmayıp ayrıca gereği kadar kişisel veri ile de sınırlandırılması gerekmektedir. Zira, söz konusu izlemenin gerekliliği ancak müdahale ile ulaşılmak istenen amacın zorunlu olması, aynı amaca daha hafif bir müdahale ile ulaşılmasının mümkün olmaması ile söz konusu olabilecektir (Anayasa Mahkemesi, 2016/13010 Başvuru Numaralı ve 17/09/2020 Tarihli Karar). Örneğin, bir çalışanın tuş vuruşları, fare hareketlerini kaydetme, ekran görüntüsü alma, kameranın etkinleştirilmesi gibi uygulamalar vasıtasıyla gerçekleştirilen kişisel veri işleme faaliyetlerinin yasal bir dayanağı bulunduğunu savunmak pek de olanaklı görünmemektedir (Article 29 Data Protection Working Party, 2017, s.16).

İletişimin denetlenmesi hususunda iletişim akışı ve iletişim içeriklerinin denetlenmesi arasında bir ayrım yapılması gerekmekte olup iletişim içeriklerinin denetlenmesi daha katı gerekçelere bağlıdır (Anayasa Mahkemesi, 2016/13010 Başvuru Numaralı ve 17/09/2020 Tarihli Karar). Zira, iletişim trafiğine ilişkin bilgiler de iletişimin içeriği kadar önem arz etmekte olup bu yönde yapılan ihlaller de kişisel verilerin korunması hakkına güvence sağlayan özel hayatın gizliliği ile haberleşmenin gizliliği hakkının ihlali niteliğinde sayılabilecektir (Küzeci, 2018, s.109). E-posta kullanımının denetlenmesinde işverenin amacı elverdiği kadarıyla iletişimin içeriğinden ziyade öncelikli olarak işverenin menfaatine ters düşecek şekilde bir güvenlik ve sadakat ihlali olabilecek durumların tespiti sonrasında iletişimin içeriğine ilişkin bir denetim yapılmalıdır. İletişimin içeriğinin hiçbir şekilde denetlenemeyeceği yönünde görüşler mevcut olsa da işveren ihlalin var

olup olmadığını ancak içerik denetimi ile tespit edebilecekse bu anlamda içeriğin denetlenememesi işverenin menfaatine aykırı bir durum ortaya çıkaracaktır. Bu hususa ilişkin olarak "Veri sorumlusunun çalışanlarına tahsis ettiği kurumsal e-posta adresindeki içerikleri izleme, erişme ve depolama suretiyle kişisel verileri işlemesi" hakkında alınan Kurulun 19/01/2023 tarihli ve 2023/86 sayılı Kararında özetle; ilgili kişinin veri sorumlusu şirkette iş akdinin feshedildiği, fesih sebebinin şirket içi verilerin şirketin tahsis etmiş olduğu e-posta adresi üzerinden kişisel e-posta adresine gönderilmesi ve şirketin bir başka çalışanı ile gerçekleştirilen telefon görüşmesinin gizlice kayıt altına alınarak yine kişisel e-posta adresi ile avukatının e-posta adresine gönderilmesi olduğu, aydınlatma ve açık rızanın usulüne uygun olmadığı iddiaları ile gereğinin yapılmasının talep edildiği şikayete ilişkin yapılan inceleme neticesinde;

- Veri sorumlusunun giyim sektöründe ticari faaliyette bulunan bir şirket olduğu, iş ile ilgili ticari sır veya herhangi bir bilginin üçüncü taraflarla paylaşılmamasını isteme noktasında ve kurumsal iletişim araçlarının kişisel amaçlarla kullanılmamasının sağlanması hususunda haklı menfaati bulunduğu, ayrıca ilgili kişinin yönetici pozisyonunda görev yaptığı ve bu anlamda şirketin gizli kalmasında menfaati bulunan bilgileri haiz olabileceği dikkate alındığında, İş Kanunu'nun 25'inci maddesinde yer alan "işverenin meslek sırlarını ortaya atmak gibi doğruluk ve bağlılığa uymayan davranışlar"ın tespiti ve Türk Borçlar Kanunu'nun 396'ncı maddesinde yer alan "işverene ait teknik sistemlerin usulüne uygun kullanılması ve iş sırları gibi bilgileri hizmet ilişkisinin devamı süresince kendi yararına kullanamayacağı ve başkalarına açıklayamayacağı" hususlarının tespiti amacıyla veri sorumlusunun e-posta denetimi suretiyle kişisel verileri işlemesinde haklı menfaati bulunduğu,

- Veri sorumlusu tarafından Kuruma intikal ettirilen Bilgi Güvenliği Yönetim Sistemi Kurumsal Mail Aktivite Denetim Raporu ve elde edilen bulgulara ilişkin ekran görüntüsü incelendiğinde veri sorumlusunun şüpheli konuya sahip ve kurumsal e-posta adresinden üçüncü şahıslar ve çalışanın şahsi e-posta adresine iletilen e-postaların tespit edildiği ve sonrasında iletişimin içeriğine ilişkin bir denetim gerçekleştirildiğinin anlaşıldığı, somut olayda veri sorumlusunun herhangi bir ihlalin gerçekleşip gerçekleşmediğini ancak içerik denetimi ile ortaya koyabileceği dikkate alındığında veri sorumlusu tarafından yalnızca ilgili personelle ve amaca yönelik kişisel veri ile sınırlı tutularak ve yine yalnızca amaçlanan çerçevede bir kişisel veri işleme faaliyeti gerçekleştirildiği, dolayısıyla söz konusu işlemenin "işlendikleri, amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesine de aykırılık teşkil etmediği, kişisel veri işleme faaliyetinin Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendinde yer alan "bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" hükmü ile (f) bendinde yer alan "İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması." işleme şartları kapsamında gerçekleştirildiği,

hususları dikkate alındığında veri sorumlusu hakkında Kanun kapsamında yapılacak bir işlem bulunmadığına karar verilmiştir. Dolayısıyla, veri sorumlusunun mutlak suretle içeriği denetleyemeyeceği yönündeki katı bir görüş pratik ve uygulanabilir olmayacak, veri sorumlusunun savunma hakkı ve meşru menfaati kapsamında yapacağı bir denetim belirli koşullar gözetilmek suretiyle hukuka aykırılık teşkil etmeyebilecektir.

Ayrıca e-postanın içeriğine erişimin kesinlikle gerekli olduğu durumlarda denetime konu çalışan haricinde bulunan üçüncü kişilerin verilerinin işlenmesi de gündeme gelebilecektir. Bu kişiler bakımından açık rıza alınması gibi bir durum söz konusu olamayacağından üçüncü kişilerin bu faaliyetlerden etkilenebileceği ölçüde izleme faaliyetlerinin varlığından haberdar edilmesi adına işverenin makul bir çaba göstermesi beklenmektedir (Article 29 Working Party, 2002, s.17).

Avrupa İnsan Hakları Mahkemesi'nin 12 Ocak 2016 tarihli "Bărbulescu v. Romanya" Kararında bir çalışanın iş amacıyla tahsis edilen Yahoo Messenger hesabının işveren tarafından kontrol edilmesinin Avrupa İnsan Hakları Sözleşmesinin 8'inci maddesinde yer alan özel ve aile hayatına saygı hakkını ihlal edip etmeyeceğine ilişkin bir değerlendirmede bulunulmuştur. AİHM bu kararda işverenin hangi ilkeleri göz önünde bulundurarak denetim yapabileceğine ilişkin değerlendirmelere yer vermiştir. Bu bağlamda, işçinin kişisel verilerinin korunması hakkı ile işverenin denetim hakkı arasında denge kurulurken; işverenin iletişimi denetlemek için önlem alma olasılığı ve bu önlemlerin uygulanması konusunda çalışanı bilgilendirip bilgilendirmediği, bu bilgilendirmenin açık ve net olarak izleme öncesinde yapılıp yapılmadığı, işveren tarafından yapılan izlemenin kapsamı ve işçinin mahremiyetine yapılan müdahalenin derecesi, iletişim akışı ve içeriklerin izlenmesi arasında bir ayrım yapılıp yapılmadığı, iletişimin bir kısmı veya tamamının mı izlendiği, izlemenin zaman açısından sınırlı olup olmadığı, sonuçlara erişimi olan kişilerin sayısı, işverenin iletişimi denetlemek ve içeriğe erişmeyi haklı çıkarmak için meşru gerekçeler sunup sunmadığı, çalışanın iletişimlerinin içeriğine doğrudan erişmekten daha az müdahaleci yöntem ve önlemlere dayalı bir denetim mekanizmasının mümkün olup olmadığı, işçi için izlemenin sonuçları ve sonuçların bilgilendirmede bulunan amaca ulaşmak için kullanılıp kullanılmadığı, işverenin izleme faaliyetlerinin müdahaleci nitelikte

olması durumunda işçiye yeterli güvence sağlanıp sağlanmadığı hususlarının dikkate alınması gerektiği, her bir olay özelinde bu hususların tek tek irdelenmesi gerektiği yönünde değerlendirme yapılmıştır.

Ayrıca, işçinin bir kuruluştan ayrılması durumunda, işverenin, çalışanın elektronik araçlarını otomatik olarak devre dışı bırakmak için gerekli organizasyonel ve teknik önlemleri alması gerekmekte olup işverenin hesapların içeriğine ulaşmasının gerekli olduğu durumlarda da bunu çalışanın ayrılmasından önce ve mümkün olduğunca çalışanın huzurunda yapması gerekmektedir (Council of Europe, 2015, s.8). İşten çıkarma sürecinde işveren tarafından şirket bilgisayarı ve e-postasına ilişkin yapılan işlemlerin hukuka aykırılığına ilişkin iddiaya ilişkin olarak verilen Kişisel Verileri Koruma Kurulu'nun 09/03/2021 tarihli ve 2021/205 sayılı Kararında;

> *"iş sözleşmesi feshedildikten sonra ilgili kişinin kullanımına tahsis edilen şirket bilgisayarının formatlanması ve şirket e-postasının kapatılmasının Kanuna aykırılık teşkil etmediği, iş sözleşmesinin sonlanmasından sonra veri sorumlusu şirket tarafından, işçinin e-posta adresinin kapatılmasının ve işçinin kullanımına tahsis edilmiş bilgisayarın geri alınmasının hayatın olağan akışı gereği olduğu, ilgili kişi e-posta adresinin kapatılması suretiyle hesabına erişiminin engellendiğini belirtmişse de bu durumun Kanuna aykırılık teşkil etmeyeceği"*

değerlendirmelerine yer verilmiştir. Bu çerçevede, her olay özelinde ayrıca bir değerlendirme yapılması gerekmekte olup denetimin hukuka uygunluğu somut olayın koşullarına göre şekillenecektir.

Telefon

İşveren tarafından işçilerin telefon ve telefonlarında yer alan uygulamaların kullanımı ve içerikleri hakkında denetleme faaliyetinde bulunulduğu durumlar söz konusu olabilmektedir. İşçinin telefonunda yapılacak bir denetleme faaliyeti direkt olarak haberleşmenin gizliliğini ihlal niteliğinde sayılabilecektir. Ancak, işin niteliği gereği; örneğin çağrı merkezi faaliyeti yürütülen bir işte telefon görüşmelerinin işçi bilgilendirilmek suretiyle kayıt altına alınması mümkündür.

Öte yandan, işveren tarafından işçiye bir telefon tahsis edilmiş olması işverenin ölçüsüz bir şekilde telefon vasıtasıyla denetim yapabileceği anlamına gelmemektedir. Öncelikli olarak, işveren tarafından söz konusu telefonun özel amaçlı kullanılıp kullanılmayacağı hususunda bir karar verilmesi gerekmekte olup bu

hususun işçiye bildirilmesi gerekmektedir. Bu anlamda işverenin; işçinin Borçlar Kanunu'ndan kaynaklı özen ve sadakat yükümlülüğü ya da çalışma performansına ilişkin değerlendirme yapılması amaçları ile işveren tarafından yalnızca iş amaçlı kullanım için tahsis edilen bir telefona ilişkin kayıtların denetlenmesinde menfaati bulunabileceği iddia edilebilecektir. Ancak bu durumda dahi kayıtların denetlenmesi haberleşmenin gizliliğini ihlal suçunun konusunu oluşturabileceğinden bir şüphe mevcut ise yargı mercilerine başvurulmasının uygun olacağını söylemek mümkündür (Gürsel, 2016, s.402).

Öte yandan, telefonda yer alan uygulamaların denetimine ilişkin olarak Yargıtay 9. Hukuk Dairesinin 2016/14203 Esas ve 2017/9524 numaralı Kararında bazı değerlendirmelerde bulunulmuştur. İşçinin Whatsapp üzerinden iş yeri ve yöneticiler hakkında olumsuz beyanlarda bulunması gerekçe gösterilerek iş akdi feshedilmiştir. Yargıtay'ın Whatsapp konuşmalarına ilişkin olarak görüşü işçilerin iş akışını bozmadığı ve çalışmalarını etkilemediği sürece bir grup kurması ve bu grupta iletişim içerisinde olmasının yasak olmadığı ve işçilerin bu kapsamdaki iletişimlerinin kişisel veri olarak korunmasının esas olduğudur. Somut olayda, grup içerisinde başka bir işçi tarafından yazışmalar işverene iletilmiş olup işverenin gizli kalması gereken verileri yasak bir şekilde elde ettiği şeklinde değerlendirme yapılmıştır. İşverenin veri sorumlusu sıfatı ile Whatsapp yazışmalarını işçinin aleyhinde kullanmak üzere denetlemesi orantılı bir veri işleme faaliyeti olmamakla birlikte üçüncü bir kişi tarafından kendisine iletilen yazışmalar bakımından hukuka aykırı elde etme durumu söz konusu olacaktır. Bu durumda, işverenin yazışmaları iş sözleşmesi çerçevesinde işveren sıfatıyla kullanması Kişisel Verilerin Korunması Kanunu kapsamında hukuka aykırı veri işleme faaliyeti olarak değerlendirilebilecekken yazışmaları işveren ile paylaşan diğer işçi bakımından Türk Ceza Kanunu 136'ncı madde ve devamı geçerli olabilecektir.

Ancak, işin niteliği gereği iş sözleşmesi kapsamında edim Whatsapp ya da başka herhangi bir sosyal medya, iletişim platformundan yürütülüyor ise işverenin bu yazışmaları denetlemesi aydınlatma yükümlülüğü yerine getirilmek şartı ile mümkün olabilecektir. Bu şekilde yürütülen işler bakımından işverenlerin özel kullanım ve iş kullanımını ayırması zorlaşabilecek olup işverenlerin işçilerin şahsi kullanımında bulunulan araçlarla işleri yürütmesi durumunda ayrımı net bir şekilde yapabilmesi ve özel alana müdahale etmemesi adına gerekli tedbirleri alması ya da işçinin yalnızca iş amacıyla kullanabileceği araçları temin etmesi gerekmektedir.

Lokasyon Takibi

Kişisel konum verileri bir kişiyle doğrudan veya dolaylı olarak bağlantılı olan veya bir kişiyi tanımlamak için doğrudan veya dolaylı olarak kullanılabilen herhangi bir konum verisidir (European Commission, 2016, s.9). Örneğin, bir otomobile yerleştirilen GPS koordinat bilgileri konum verisi sayılabilecekken otomobili kullanan çalışanın o konumda yer aldığı bilgisi kişisel konum verisi olarak sayılabilecek olup iki veri kaynağının birleştirilmesi ile kişisel veriden söz etmek mümkün olacaktır. İş yeri kavramının fiziki olarak belirli bir yer olmaması veya işin niteliğinin tek bir yerde bulunmayı gerektirmediği durumlarda işveren tarafından işçinin işinin başında bulunup bulunmadığı ve iş için tahsis edilen araçların amacına uygun olarak kullanılıp kullanılmadığının anlık veya sonradan tespiti amacıyla birtakım yer belirleme sistemleri kullanılabilmektedir. Faaliyet konusuna göre bu kullanım amacı değişebilmekle birlikte özellikle kuryelik, nakliye hizmeti, ulaşım hizmetleri gibi lokasyonun önem arz ettiği iş kollarında sıklıkla takip sistemleri tercih edilmektedir. İşveren lokasyon takibini iş sağlığı ve güvenliği yükümlülüklerinin yerine getirilebilmesini teminen hukuki yükümlülük çerçevesinde gerçekleştirebileceği gibi işverenin işçinin kullanmış olduğu araçların o anki konumunu bilmekte meşru menfaatinden bahsetmek mümkün olabilecektir. Ancak, bu durumda meşru menfaat mevcut ise denge testi yapılması, amaca yönelik olarak işlemenin gerekli, orantılı olup olmadığına ilişkin değerlendirmede bulunulması gerekecektir (Article 29 Data Protection Working Party, 2017, s. 19-20). Zira, konum verileri yalnızca bir kişinin nerede olduğu hakkında değil, kim olduğu, ilgi ve tercihlerinin neler olduğu hakkında da bilgi vermektedir (European Commission, s.5).

Öte yandan, işveren tarafından araçların özel olarak kullanımına izin verildiği durumlarda işçinin çalışma saatleri dışında veya özel olarak kullanım sağlayacağı durumlarda konum takibini kapatma seçeneği bulunması gerekmekte olup ayrıca çalışma saatleri dışında konum verisinin işlenmesinin ancak aracın hırsızlık, gasp gibi risklere karşı korunmasını sağlamak amacıyla etkinleştirilmesi, amaçla bağlantılı olarak bu verinin işlenmesini sağlaması bakımından önem arz etmektedir (Artıcle 29 Data Protection Working Party, 2017, s. 20). Çalışanların izlemenin ne zaman yapılacağını kontrol edebildiği durumlarda işveren tarafından gerçekleştirilen izlemenin daha adil ve daha az müdahaleci olduğu değerlendirilmektedir (European Commission, 2021, s.19).

Konum verilerini elde etmek için işçilerin kullanmış olduğu telefon, bilgisayar, otomobil gibi araçlara teknik cihazlar takılmak suretiyle ya da cihazın internet bağlantısı ile veri işleme faaliyetleri de gerçekleştirilebilmektedir. Bu veri işleme

faaliyetleri işçinin örneğin araç kullanımı esnasında ani fren, yön değişikliği veya kaza durumunda video, ses kaydı alabilme gibi teknik özelliklere sahip cihazlar ile gerçekleştirilmektedir. Konum verilerinden farklı olarak bu şekilde bir veri işleme faaliyeti ancak işçi hakkında sonradan ortaya çıkan bir durumun tespitinde meşru bir amaç için işlenmesi gerekliliği varsa gerçekleştirilebilecektir (Artıcle 29 Data Protection Working Party, 2017, s. 21).

Öte yandan, işçinin konum verilerinin yalnızca veri işleme dayanağının bulunduğu durumlarda ve genel ilkelere uygun olarak kullanılması önem arz etmekte olup ayrıca işçinin bu hususta amaçları net bir şekilde belirtilmek suretiyle bilgilendirilmiş olması kişisel veri işlemeyi hukuka uygun hale getirecektir. İşverenlerin tasarım gereği varsayılan olarak mahremiyet odaklı bir yaklaşım benimseyerek konum verilerini yalnızca iş akışı için gerekli olduğu, işçiden bağımsız olarak gerekli olduğu durumlarda anonimleştirilmiş, kişiden bağımsız bir şekilde işlemesi veri minimizasyonunu ve amaçla bağlantılı ve sınırlı olarak kişisel verilerin işlenmesini sağlayacaktır. Ayrıca, verilerin saklanacağı sürenin sınırlanması, verinin saklanmasına ilişkin tedbirlerin alınması ve amacın hasıl olması ile birlikte verilerin imha edilmesi gerekmektedir. Saklama süresine ilişkin hukuki yükümlülük ve kanunda açıkça öngörülme durumu olmadığı sürece net bir süre belirlemek her olay özelinde farklı olmakla birlikte kişinin mahremiyeti ile kişisel verilerin toplanma amacı arasında bir denge gözetilmek suretiyle belirlenmelidir.

Giyilebilir Cihaz Takibi

Teknolojinin iş yaşamına yansımalarının önemli sonuçlarından biri de giyilebilir teknolojilerdir. İş gücünde giyilebilir teknolojilerin işçilerin eğitimi ve üretkenliğini değiştireceği, işe başlama aşamasında gerçek zamanlı eğitim ve geri bildirimlerin alınabileceği, ayrıca işçilerin zamanlarını nasıl harcadıklarının tespiti, süreçleri düzene koyma ve verimlilikleri üst düzeye çıkarma hususlarında işverene yardımcı olacağı düşünülmektedir (Bilgi Teknolojileri ve İletişim Kurumu, 2020). Giyilebilir teknolojiler bireylerin aksesuar olarak takabileceği, giysilere gömülebilen veya vücuda yerleştirilebilen cihazlardır (Hayes, 2021). Giyilebilir teknolojiler eş zamanlı olarak bir ağ ve cihaz arasında veri akışını sağlayabilen internete bağlı cihazlar olup bireylere ilişkin birçok kişisel veriyi barındırmaktadır. Giyilebilir cihazlar ile birlikte dijital izleme uygulamaları, vücudu bir veri deposu olarak konumlandırma eğiliminde olup belirli dijital sensörler ile vücudun çeşitli bölümlerinden topladığı bilgileri yararlı bir bilgi haline dönüştürme amacı ile kullanılırlar (Amoore ve Hall, 2009). Cihazların topladığı kişisel verilerin saklanma yöntemi ve veri güvenliğine ilişkin belirsizlikler mevcut olmakla birlikte kişisel verilerin yanlış işlenmesi veya farklı amaçlarla kullanılmaması adına

alınan önlemler net görünmemektedir. Giyilebilir teknoloji uygulamaları genel olarak akıllı giysiler, akıllı gözlükler, aktivite izleyiciler, 3D hareket sensörleri ve akıllı telefon ile uyumlu saatler olarak kullanılmaktadır (European Commission, 2015, s.3).

Bu cihazlar sağlık, gıda, eğlence, medya, spor gibi birçok alanda farklı amaçlarla kullanılmakla (European Commission, 2015, s.2) birlikte işverenler tarafından işçinin faaliyetlerinin ve konumunun iş yeri içerisinde ve dışarısında takip edilmesi amacıyla kullanılmaktadır (Artıcle 29 Data Protection Working Party, 2017, s.17). Bu takip özünde işçinin konumu, hareket halinde olup olmadığı hakkında bilgileri işverene sağlamaktadır. Çalışan sayısının çok ve kontrol edilmesinin zor olduğu, ayrıca iş yeri haricinde bir çalışma ortamının bulunduğu durumlarda işçinin sürekli olarak konumundan haberdar olunmasında menfaat bulunduğunun ileri sürülebileceği durumlarda işveren açısından kolay bir takip yöntemi olabilecektir. Bu durumda her ne kadar işveren bakımından bir meşru menfaat olduğu düşünülebilecek olsa da meşru menfaat kriterleri kapsamında değerlendirme yapıldığında kişinin temel hak ve hürriyetlerinin veri sorumlusunun meşru menfaatine ağır geldiği kuşkusuzdur. Öte yandan, söz konusu verilerin sağlığa ilişkin bilgileri de içerebileceği dikkate alındığında Kanun'un 6'ncı maddesi uyarınca bir veri işleme dayanağının bulunması pek de olası görünmemekte olup işçinin bu yönde vereceği rızanın işçinin bağımlılığı nedeniyle özgür iradeye dayandığı söylenemeyecektir (Article 29 Data Protection Working Party, 2017, s.18).

Bununla birlikte, söz konusu veri işleme faaliyetinin genel ilkelere uygun olması gerekmekte olup işçinin her an takip ediliyor olması amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırılık teşkil etmektedir. Zira, çalışanların iş sözleşmesinin gereğini yerine getirip getirmediğinin kontrolünün sürekli olarak konum ve hareket takibi dışında daha az müdahaleci yöntemlerle de yapılması mümkündür.

Öte yandan, işçilerin bu yönde bir takipten haberi olmaksızın kıyafetlerine veya kullandıkları herhangi bir araca çip takılması ve sonrasında bu veri işleme faaliyeti sonucunda ilgililer hakkında işlem tesis edilmesi hukuka aykırı olabilecektir. Örneğin; Türk Tabipleri Birliği tarafından 2017 yılında yapılan haberde sağlık çalışanlarının formalarına çip yerleştirildiği ve bir sağlık çalışanının çiple yapılan takip sonucunda işten çıkarıldığı iddia edilmekle birlikte (Türk Tabipleri Birliği, 2017) hastane tarafından çiplerin formalara yalnızca çamaşır hizmetlerinin yerine getirilmesi amacıyla sabitlendiğinin (T24, 2017) iddia edildiği belirtilmektedir. Somut olayda, işçilerin kişisel verisi işlenmeksizin yalnızca çamaşır takibi amacıyla çip takıldığı iddia edilmekle birlikte söz konusu çipin nasıl bir teknolojiye sahip olduğu bilinmemekte olup veri sorumlusu tarafından sonrasında çipin farklı amaçlarla kullanılmayacağı hususu belirsizlikler içermektedir. Bu çerçevede, her ne kadar kişisel veri işleme faaliyeti amacı gütmeyen giyilebilir cihazlar kullanılsa da gerçek kişiyle ilişkilendirilebilecek ve hakkında kişisel veri işlenmesine sebebiyet verebilecek nitelikteki cihazların tercih edilmemesi, farklı yöntemlerle istenilen amaca ulaşıldığı durumlarda o yöntemlere başvurulması önem arz etmektedir.

GÖRÜNTÜ VE/VEYA SES KAYIT CİHAZLARI

Güvenlik kameraları ile işçilerin görüntü ve seslerinin kaydedilmesi vasıtasıyla işverenler tarafından işçilerin genel ve özel nitelikli kişisel verileri işlenebilmektedir. İşverenin kamera ile gerçekleştirmiş olduğu kişisel veri işleme faaliyeti iş sağlığı ve güvenliği kapsamındaki yükümlülüklerin yerine getirilebilmesi, üretim süreçlerinin kontrolü, iş yerinin ve müşterinin korunması, işçinin performansının değerlendirilmesi ve suç şüphesinin aydınlatılması gibi birçok amaca hizmet edebilmektedir (Gürsel, 2016, s. 363).

Bu amaçlar çerçevesinde görüntü ve ses kayıtlarının özel nitelikli veya genel nitelikte kişisel veri olup olmadığı hususunda bir değerlendirme yapılması uygun olacaktır. Zira, söz konusu verinin niteliği Kanun'un 5'inci ve 6'ncı maddesinde yer alan kişisel veri işleme şartlarından birinin bulunması ve faaliyetin hukuka uygunluğunu belirleyecektir. İşverenin kullanım amacına göre tercih edeceği kameranın teknik özellikleri de işlenecek olan kişisel verilerde farklılıklar yaratmaktadır. Kameraların yüz tanıma özelliği bulunması halinde ve bu özellik ile bireylerin yüzünde yer alan göz yuvaları, elmacık kemikleri, ağız kenarı gibi özelliklerinden dijital görüntülerin bir referans şablonla karşılaştırılarak kullanılması sonucu elde edilen veri biyometrik veri niteliğini haiz olacak (Erdinç, 2020, s. 77) olup ayrıca, kameraların ses kayıt özelliği bulunması veya ses kayıt cihazları vasıtasıyla işçilerin seslerinin kaydedilmesi durumunda her bireyin sesindeki ton, perde, ahenk farklılığı olması ve sesin eşsiz ve kişiye özgü olması nedeniyle bu veriler de biyometrik veri kategorisinde yer alacak ve yüz tanıma ile ses tanıma özellikli araçlar vasıtasıyla gerçekleştirilen kişisel veri işleme faaliyetleri bakımından özel nitelikli kişisel verilerin işlenmesi söz konusu olacaktır.

Bu çerçevede, söz konusu verilerin işlenme şartı işçinin açık rızası veya kanunlarda öngörülen haller olabilecektir. İşçinin açık rızasının işçi işveren ilişkisi içerisinde her zaman geçerli olmayabileceği dikkate alındığında söz konusu verilerin ancak kanunlarda öngörülen hallerde işlenebileceğini söylemek mümkündür. Bir işveren tarafından işçilerin yüzlerinin tanınmasına imkân sağlayacak sistemlerin kullanılması, söz konusu sistemler profil çıkarma ve otomatik karar alma me-

kanizmalarını da içereceğinden orantısız ve hukuka aykırı bir uygulama olarak değerlendirilebilecektir (Article 29 Data Protection Working Party, 2017, s.19). Bu durumun istisnası ancak yüksek güvenlik önlemi gerektiren işler bakımından bu verilerin işlenmesinin zorunluluğu olabilecek olup bu kapsamda kanunlarda öngörülen bir veri işleme faaliyeti mevcut değil ise işçiler bilgilendirilmek suretiyle açık rızalarına başvurulması gerekebilecektir. Açık rıza dışında bir veri işleme şartı bulunmuyor ve veri sorumlusunun da kişisel verileri işlemesi işin niteliği için zorunluluk arz ediyorsa somut olay değerlendirilmek suretiyle açık rızanın geçersizliğinden bahsetmek işverenin aleyhine bir durum oluşturabilecektir.

Bununla birlikte, söz konusu kameraların biyometrik veri işleme özelliğine sahip olmaması durumunda işverenin amacına göre Kanun'un 5'inci maddesine istinaden veri işleme faaliyeti de farklılık gösterecektir. Örneğin, müşteri ile işlemlerin telefon aracılığıyla yürütüldüğü faaliyetler bakımından görüşmelerin kayıt altına alınması gerekliliği bulunması durumunda veri sorumlusunun bir ihtilaf durumunda kendisini ispatlaması amacıyla gerçekleştirilen kişisel veri işleme faaliyetinin bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması şartına dayanılarak gerçekleştiği değerlendirilebilecektir. Kişisel Verileri Koruma Kurulu'nun 25/06/2020 tarihli ve 2020/494 sayılı Kararında, bir işçinin işverene karşı açmış olduğu işe iade davasında işverenin ilgili kişiye ait kamera görüntülerini mahkemeye sunarak kişisel verileri hukuka aykırı bir biçimde işlediği iddiasına ilişkin olarak yapılan değerlendirme neticesinde;

> *"...veri sorumlusunun savunmaya yönelik dayandığı vakıaları beyan dilekçesiyle mahkemeye sunduğunun anlaşıldığı, Kanunun 8 inci maddesine uygun olarak Kanunun 5 inci maddesinin (2) numaralı fıkrasının (e) bendindeki; "Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" hukuki sebebi uyarınca söz konusu kamera kaydının mahkemeye sunulmasının hukuka uygun bir veri işleme faaliyeti olduğu"*

yönünde karar verilmiştir. Söz konusu kararda ayrıca, işçi ile işveren arasındaki dava ile kamera kayıtlarının ilgisinin bulunup bulunmadığı yönünde bir değerlendirmeye yer verilmiş ve iş akdinin haklı nedenle fesih gerekçesinin işçinin çalışma arkadaşına fiziksel şiddet uygulaması olduğu, işçinin aynı zamanda söz konusu kamera kaydının alındığına ilişkin bilgilendirildiği, bu kapsamda görüntülerin mahkemeye sunulduğu belirtilmiştir. Bu anlamda, işveren tarafından bir hakkın tesisi kapsamında gerçekleştirilen kişisel veri işleme faaliyetinin de bir sınırı bulunmakta olup bu sınırı genel ilkeler belirlemektedir. Zira, dava ile ilgisi bulunmayan ve bilgilendirme yapılmaksızın işlenen verilerin hukuka uygun olarak işlendiği kabul edilemeyebilecektir.

İşçinin bilgisi olmaksızın gizli olarak görüntülerin ve seslerin kaydedilmesi öncelikle aydınlatma yükümlülüğü yerine getirilmeksizin veri işleme faaliyeti gerçekleştirildiğinden hukuka uygun sayılmayacaktır. Açık izleme, işçinin herkes tarafından görülebilecek bir kamera yardımıyla izlenmesi iken gizli kamera ve ses kayıt sistemleri işverenin işçileri izleyen araçları işçilerin göremeyeceği biçimde yerleştirmesi ile gizli şekilde ses ve görüntülerinin kaydedilmesini ifade etmektedir (Beytar, 2018, s.190-191). Kayıt yapıyormuş görünümünde bulunan kameralar ve ses kayıt cihazlarının kullanıldığı ve işçinin gözetlendiğini bildiği ancak araçların yerini bilmediği durumlarda işçinin yanılgı ve sürekli izlenme endişesi ile baskı altında bırakıldığı göz önünde bulundurulduğunda her ne kadar kişisel veri işleme faaliyetinde bulunulmasa da Borçlar Kanunu'nun 417'nci maddesinde de yer aldığı üzere işverenin, hizmet ilişkisinde işçinin kişiliğini korumak ve saygı göstermek ve iş yerinde dürüstlük ilkelerine uygun bir düzeni sağlamakla, özellikle işçilerin psikolojik tacize uğramamaları için gerekli önlemleri almakla yükümlü olduğu dikkate alınmalıdır.

Uluslararası Çalışma Örgütü'nün kılavuzunda gizli izlemeye yalnızca ulusal mevzuat uygun ise, makul gerekçelerle suç faaliyeti veya yanlış yapıldığına ilişkin ciddi bir şüphe varsa başvurulabileceğine değinilmiş ve Kişisel Verilerin Korunması Kanunu kapsamında bunun mümkün olmayacağı hususu "İşçinin Elektronik Ortamda Gözetlenmesi" başlığında açıklanmıştır. Yine de, gizli izlemenin istisnası olarak iş yerinde suç işleneceğine dair bir şüphenin bulunması halinde gizli kamera ile gözetleme yapılabileceği ve işverenin şüphesindeki haklılığını gözetlemeden sonra ispat edebileceği yönünde görüşler (Beytar, 2018, s. 192) bulunmakla birlikte önceden işçiyi bilgilendirmek kaydıyla somut ve kuvvetli bir suç şüphesinin var olduğu haller dışında gizli gözetleme yapılamaması gerekmekte olup ayrıca ileride işlenebileceği varsayılan suçlar için de gizli kamera ile gözetleme yapılmaması gerektiği değerlendirilmektedir (Uncular, 2018, s.295).

Bu kapsamda, işverenin aydınlatma yükümlülüğünü yerine getirirken suç şüphesinin varlığı halinde gizli izleme yapılabileceğini belirtmesi mümkün bulunmakla birlikte Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 5'inci maddesinin (g) bendinde gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadelerin kullanılmaması gerektiği ifade edilmektedir. İşverenin meşru menfaati ve hakkın tesisini gerçekleştirebilmek için başka bir seçeneğinin bulunmadığı dikkate alındığında her ne kadar somut bir şüphenin varlığı gündeme gelmesi muhtemel bir amaç gibi görünse de işverenin suç şüphesinin varlığı halinde bu şekilde bir yönteme başvurabileceğini işçiye belirtmesi ve bu şüpheyi somut olarak ortaya koyması durumunda söz konusu veri işleme faaliyetinin aydınlatma

yükümlülüğü bakımından hukuka aykırı sayılması işverenin aleyhine bir durum ortaya çıkarabilecektir. Ancak yine de işveren gizli izleme dışında açık bir şekilde de ispat yükümlülüğünü yerine getirebilecekse gizli izlemeye başvurmaması işçinin kişilik haklarına müdahaleyi de en aza indirecek, ayrıca kişisel veri işleme faaliyetinin hukuka uygunluğuna da halel getirmeyecektir. Zira, suçun işlenmesi ve suç soruşturmasının yürütülmesi hususunda kolluk ve yargı makamları yetkili olup işverenin bu şekilde bir görevi ve yetkisi bulunmamakla birlikte kolluk güçleri tarafından yapılacak faaliyetler için dahi yargı kararının gerekli olduğu dikkate alındığında işverene bu hakkın, istisnai şekilde de olsa tanınması işverenin kamu makamlarına bile tanınmayan bir yetkiyle donatılması anlamına gelecektir (Sevimli, 2006, s.243). İşverenin bazı haklı nedenlerin varlığı halinde işçileri gözetleyebileceği, hangi durumların haklı neden teşkil edip etmediğinin somut olayın özelliklerine göre belirlenebileceği ve belirlemedeki önemli hususlardan birinin işçinin 'haklı mahremiyet beklentisi' olduğu değerlendirilmektedir (Erdoğan, 2017, s.117).

İşçinin önceden bilgilendirilmeksizin görüntü ile birlikte sesinin de kaydedilmesi hususunda Yargıtay 22. Hukuk Dairesi'nin 2015/28830 E. ve 2018/15646 numaralı Kararında işverenin çalışanının kamera sistemi üzerinden kendisi hakkındaki kötü sözlerini duyduğu ve bunun üzerine iş sözleşmesinin feshedilmesine ilişkin olayda Yargıtay, kıdem tazminatının belirlenmesine kamera kayıtları ve olay esnasında sarf edilen sözlerin içeriği belirlenerek karar verilmesi gerektiği şeklinde hüküm tesis etmiştir. Ancak, Kararda yer alan karşı oyda iş yerinin niteliği kapsamında kamera ile gözetlenmenin haklı bir neden oluşturabileceği ancak işçilerin konuşmalarının dinlenmesi için haklı bir nedenden söz edilemeyeceği, dosya kapsamında işçinin konuşmalarının dinlendiğinden önceden haberdar olmadığı dikkate alındığında konuşmaların dinlenmediği konusunda işçide haklı bir mahremiyet beklentisinin doğduğu, bu kapsamda da kişilik haklarının ihlal edildiği, delillerin hukuka aykırı elde edildiği belirtilmektedir.

İşçinin kameralar ve ses kayıt cihazları ile kişisel verilerinin işlenmesinin genel ilkelere uygunluğu, kişilik haklarına müdahalenin sınırlarının çizilmesinde önem arz eden bir husustur. İş yerine konumlandırılan kamera sayısı, kameraların görüş açısı, mesafeleri ve yerleştirildikleri alanlar, kaydedilen görüntülerin ve seslerin toplanma ve işlenme amaçları ile saklama süreleri (Uncular, 2018, s.293), ses kayıt cihazlarının kullanım yerleri, cihazların teknik özellikleri, verilerin depolanması ve verilere kimler tarafından erişilebileceği, veri işleme faaliyetinin kimleri hedeflediği ve verisi işlenen farklı gruplar için farklı sonuçların olup olmadığı (European Commission, 2021, s. 29) hususları gözetleme uygulamalarının hukuka uygunluğunun değerlendirilmesinde dikkate alınmaktadır. Bu çerçevede,

işveren tarafından gerçekleştirilecek işlemenin belirli, açık ve meşru amaçlarının bulunması, ayrıca işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması gerekmektedir. İşverenin amacının belirsiz olması veya sonradan ortaya çıkan farklı bir amaç için kişisel verileri işlemesi durumunda çalışanlar bu hususta bilgilendirilmediğinden veri işleme faaliyeti farklı amaç bakımından hukuka uygun olmayacaktır. Ayrıca, işçilerin aleyhlerine bir durum söz konusu olduğunda bu kayıtların amaç dışı kullanımı işçilerin kişisel verileri üzerindeki kontrolünün de kaybedilmesine sebebiyet verecektir. Bu kapsamda, işverenin amaçlarını net bir şekilde belirlemesi ve işlendikleri amacın dışına çıkacak bir biçimde ölçüsüz bir gözetleme faaliyeti gerçekleştirmemesi gerekmektedir. Amaca ulaşılabilecek ve kişilik haklarına daha az müdahale edebilecek nitelikte bir yol mevcut ise bu yolun tercih edilmesi önem arz edecektir.

Görüntü ve ses kaydı vasıtasıyla gerçekleştirilen gözetleme faaliyetinin işçinin kendisini baskı altında hissetmesi ve baskının sonucu ortaya çıkan stres nedeniyle psikolojisinin olumsuz etkilenerek davranışlarında değişimin meydana gelmesine sebebiyet vermesi olasıdır (Article 29 Data Protection Working Party, 2017, s.10; Manav, 2015, s.124). İşçinin akvaryum içerisindeki bir balık gibi sürekli olarak ve her hareketinin izlendiğine ilişkin bir düşüncede olması olumsuz bir etkiye sebebiyet vermektedir (Küzeci, 2018, s.469, Gürsel, 2016, s.1). İşçinin izlenmesi durumunda baskının aksine işçilerin kendilerini daha güvende hissettikleri, üretimin daha verimli ve kaliteli olduğu, bu izlemenin iş yerindeki üretim kapasitesi ve kalitesine de faydalı olduğu yönünde görüşler mevcut olsa da sürekli olarak gözetleme baskısı altında çalışma tersine verimliliği, üretkenliği ve kaliteyi olumsuz yönde etkilemekte (Uncular, 2018, s. 293) ve işverenin verimliliğin artması adına almış olduğu önlemin iş yeri bakımından uzun vadede yararından çok zararı bulunmaktadır. Bu anlamda, kişisel veri işleme faaliyeti sınırsız ve şeffaf değil ise işverenin verimliliğinin artırılması ve varlıklarının korunmasına yönelik haksız ve müdahaleci bir izleme ortaya çıkacaktır (Article 29 Data Protection Working Party, 2017, s.9).

Öte yandan, iş yerinde çalışanların makul bir mahremiyet beklentisine sahip oldukları soyunma odaları, tuvaletler, duşlar, mescit, dinlenme odaları ve emzirme odalarının gözetlenmesi ölçülü ve amaçla bağlantılı bir gözetleme faaliyeti olmayacaktır (European Commission, 2021, s.29). Buna ek olarak, kameraların ve ses kayıt cihazlarının işverenin amacının gerçekleştirileceği ölçüde minimum kişisel veri işlemek üzere konumlandırılmış olması gerekmekte olup örneğin üretim sürecinin kontrol edilmesine ilişkin gerçekleştirilecek bir gözetleme faaliyetinin işçiye özel alan bırakacak şekilde yalnızca makineyi görebilecek şekilde (Uncular, 2018, s. 293), satış yapılan iş yerlerinde çalışan ve müşterinin gerçekleştire-

bileceği olası hırsızlık vakalarının tespiti amacıyla gözetimde yalnızca kasanın görülebileceği noktaların kayda alınması ölçülülük kriteri açısından önem arz etmektedir. Bu kapsamda, "Veri sorumlusu tarafından iş yerinde güvenlik kamerası vasıtasıyla ve işe giriş-çıkışlarda yüz tanıma sistemi kullanılması suretiyle kişisel verilerin hukuka aykırı işlenmesi" hakkında Kişisel Verileri Koruma Kurulunun 04/08/2022 tarih ve 2022/797 sayılı Kararında özetle; ilgili kişilerin çalıştıkları fabrikada işe giriş-çıkışlarda yüz tanıma sistemi uygulandığı ve bununla ilgili olarak ilgili kişilere açık rızalarının olduğuna ilişkin genel bir aydınlatma metni imzalatıldığı, bu metnin açık rızanın unsurlarını taşımadığı, aydınlatma yapılması ve açık rıza alınması işlemlerinin ayrı ayrı yerine getirilmesi şartına uyulmadığı, işe giriş-çıkışlarda alternatif seçenekler varken kullanılan yüz tanıma sisteminin orantısız bir uygulama olduğu, öte yandan, çalışanların tuvalette geçirdiği zamanı ölçmek için güvenlik kameralarının ilgili kişileri fiziksel olarak etkileyebilecek şekilde lavabolara da konulduğu iddialarına ilişkin olarak yapılan inceleme neticesinde; veri sorumlusunun iş yerinde yer alan kameraları işçilerin makul mahremiyet beklentisini zedeleyecek bir şekilde konumlandırmaması, bu çerçevede iş yerlerindeki tüm kameraların gözden geçirilerek konumlarının düzenlenmesi yönünde veri sorumlusunun talimatlandırılmasına, ayrıca veri sorumlusu tarafından ilgili kişilerin giriş-çıkış esnasında yüz tanıma sistemi vasıtasıyla biyometrik verilerini işlenmesinin Kanun'un 6'ncı maddesi kapsamında herhangi bir veri işleme şartına dayanılmaksızın gerçekleştirildiği dikkate alınarak idari para cezası uygulanmasına ve açık rıza, aydınlatma metinlerinin Kanun ve Tebliğ hükümlerine uygun hale getirilerek hukuka aykırı işlenen kişisel verilerin imha edilmesi yönünde veri sorumlusunun talimatlandırılmasına karar verilmiştir.

Diğer taraftan, ses kayıt özelliği bulunan güvenlik kamerası kullanılması ile ilgili Kişisel Verileri Koruma Kurulunun 12/03/2020 tarihli ve 2020/212 sayılı Kararında sesli kamera kaydının hukuka uygunluğu Anayasanın 13'üncü maddesinde yer alan temel hak ve özgürlüğün sınırlandırılmasının kriterleri kapsamında değerlendirilmiş olup ses kaydı ile amaçlananın ses kaydı olmaksızın görüntü kaydı ile de elde edileceği hallerde ses kaydının da yapılmasının, gerçekleştirilecek kişisel veri işleme faaliyeti ile ulaşılmak istenen amaç arasındaki dengenin bozulmasına yol açacağından ölçülülük ilkesine aykırılık teşkil edeceği, gözetim sistemlerinde görüntü kaydı ile birlikte ses kayıt sisteminin de kullanılmasının sadece görüntü kaydına göre çok daha müdahaleci olacağı değerlendirilmiştir.

SONUÇ

Kişisel veri, kimliği belirli ya da belirlenebilir kişiye ilişkin her türlü bilgi olarak tanımlanmakta olup kişisel veri günümüz teknolojisi ile birlikte hayatın her alanında işlenerek bireylerin kişisel verileri üzerindeki kontrol mekanizmasının yitirilmesine yol açmaktadır. Nitekim, kişisel verilerin işçi işveren ilişkilerinde işlenmesi noktasındaki kontrolün güç dengesizliği sebebiyle işverende bulunması dolayısıyla işçilerin kişisel verilerinin işlenmesi hususundaki hak ihlalleri yoğun bir şekilde yaşanmaktadır. Bu çerçevede, kişisel verilerin işlenmesine ilişkin hukuki düzenlemeler herkes için geçerlilik arz ederken işçi işveren ilişkisinde kişisel verilerin farklı görünümlerde işlenmesi ayrıca bir korumayı gerektirmektedir.

İş Kanunu ve Kişisel Verilerin Korunması Kanunu bağlamında işçinin kişisel verilerinin işlenmesinin sınırları somut olay kapsamında değerlendirilebilecek olmakla birlikte her veri işleme faaliyetinde hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerinin öncelikli olarak dikkate alınması önem arz etmektedir. Zira, söz konusu ilkeler bir kişisel veri işleme faaliyetinin hukuka uygunluğunun sağlanmasının temel taşını oluşturmaktadır. Ayrıca, kişisel verilerin işlenmesinde veri işleme şartlarını düzenleyen Kişisel Verilerin Korunması Kanunu'nun 5'inci, 6'ncı, 8'inci ve 9'uncu maddelerinin doğru bir şekilde ayrıştırılması ve veri sorumluları tarafından kişisel veri işleme amacına en uygun dayanak seçilerek hareket edilmesi gerekmektedir. Bir veri işleme faaliyetinin hukuka uygunluğu yalnızca genel ilkelere uyum ve veri işleme şartının bulunması olmayıp aynı zamanda veri sorumlusu sıfatı ile işverenlerin aydınlatma yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, ilgili kişiler tarafından Kanun kapsamında iletilen taleplerin karşılanması gibi farklı yükümlülükleri de bulunmaktadır. Bu anlamda, işverenlerin kişisel verilerin işlenmesi süreçlerini bir bütün olarak değerlendirmesi ve özümsemesi, fazla verinin işlenmesinin daha fayda sağlayacağı düşüncesine kapılmaktan ziyade minimum veri ile amacına ulaşabilmek adına gerekli düzenlemeleri yapması gerekmektedir.

Kişisel verilerin korunması hukukunun ülkemizde yeni gelişmekte olan bir alan olması vehukuki düzenlemelerin yeterli seviyede detaylandırılmamış olması nedeniyle işçilerin haklarının etkin bir şekilde korunması noktasında açıkta kalabilecek bazı noktalar bulunmakta olup bu anlamda baştan itibaren mahremiyet odaklı bir bakış açısı ile işverenlerin bilinçlendirilerek gözetim uygulamalarının buna göre geliştirilmesi ve uygulanması, iş yeri politikalarının işçilerin makul

mahremiyet beklentileri dikkate alınarak gizlilik esaslı oluşturulması, hukuki düzenlemelerin teknolojik gelişmeler ve uygulamada yaşanan problemler dikkate alınmak suretiyle açıkta bir alan kalmayacak ve işçi ile işverenin aynı anda menfaatlerini koruyacak şekilde düzenlenmesi gerekmektedir. ◆

KAYNAKÇA

- AKGÜL, A. (2015). Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı. TBB Dergisi, 118, 200-222
- AMOORE L. ve HALL A. (2009). Taking People Apart: Digitised Dissection and the Body at the Border. Society and Space, 27(3),.444-464. Erişim adresi: https://journals.sagepub.com/doi/abs/10.1068/d1208
- Anayasa Mahkemesi. (2013). 2013/4825 Başvuru Numaralı ve 24/03/2016 Tarihli Karar. Erişim adresi: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/4825
- Anayasa Mahkemesi. (2013). 2013/7054 Başvuru Numaralı ve 06/01/2015 Tarihli Karar. Erişim adresi: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/7054?KelimeAra%5B0%5D=ya&page=759
- Anayasa Mahkemesi. (2013). 2016/13010 Başvuru Numaralı ve 17/09/2020 Tarihli Karar. Erişim adresi: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2016/13010
- Anayasa Mahkemesi. (2013). 2018/11988 Başvuru Numaralı ve 10.03.2022 tarihli Karar. Erişim adresi:https://www.resmigazete.gov.tr/eskiler/2022/04/20220419-7.pdf
- Article 29 Data Protection Working Party. (2001). Opinion 8/2001 on The Proccessing Of Personal Data In The Employment Context. Erişim adresi: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf
- Article 29 Data Protection Working Party. (2002). Working Document on The Surveillance of Electronic Communications in The Workplace. Erişim adresi: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf
- Article 29 Data Protection Working Party. (2012). Opinion 3/2012 -on Developments I-in Biometric Technologies
- Article 29 Data Protection Working Party. (2017). Opinion 2/2017 on Data Processing at Work

◊ Avrupa İnsan Hakları Mahkemesi. (2016). Bărbulescu v. Romanya Kararı, Erişim adresi:https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Barbulescu%22],%22itemid%22:[%22001-177082%22]}

◊ BEYTAR, E. (2018). İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması, On İki Levha Yayıncılık, İstanbul

◊ Bilgi Teknolojileri ve İletişim Kurumu. (2020). Giyilebilir Teknolojiler, Erişim adresi: https://www.btk.gov.tr/uploads/pages/arastirma-raporlari/giyilebilir-teknolojiler-arastirma-raporu.pdf

◊ BRAUN, C. A. (2018). "Kişisel Verilerin İşlenmesinde Rıza. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 15(1),13-33.* Erişim adresi: https://law.yeditepe.edu.tr/sites/default/files/yuhf_dergisi_v.14.pdf

◊ Council of Europe. (2015). Recommendation CM/Rec(2015)5 Of The Committee Of Ministers To Member States on The Processing of Personal Data in the Context of Employment. Erişim adresi:https://rm.coe.int/cmrec-2015-5-on-the-processing-of-personal-data-in-the-context-of-empl/1680a43b68

◊ ÇAYCI, A.E ve ÇAYCI, B. İletişimin Dijitalleşmesi:Dijital Gözetim ve Mahremiyet. İnönü Üniversitesi İletişim Fakültesi Elektronik Dergisi, 1(2), 157-169

◊ ÇELİKOĞLU, N. (2007) .Türkiye'de Üniversite Gençliğinde Mahremiyetin Dönüşümü, Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü

◊ Danıştay. (2013). 2013/5342 Esas ve 2013/9525 sayılı Karar.

◊ Danıştay. (2015). 2014/2242 Esas ve 2015/499 sayılı Karar.

◊ Danıştay. (2015). 2015/5190 Esas numaralı Karar

◊ ERDİNÇ, G. H. (2020). Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi. Kişisel Verileri Koruma Dergisi, 2(1), 1-19.

◊ ERDOĞAN, C. (2017). Kişilik Hakkı Kapsamında İşçilerin İzlemesi ve Gözetlenmesi, Yetkin Yayıncılık, Ankara.

◊ European Commission. (2021). Electronic Monitoring and Surveillance in the Workplace, Publications Office of the European Union.

◊ European Commission. (2016). Guidelines -for Public Administration on Location Privacy.

◊ GAUKLER, G. M. SEİFERT, R. W. (2007). Trends in Supply Chain Design and Management. Springer Series in Advanced Manufacturing, 29-48

◊ GÜRSEL, İ. (2016). İşçinin Kişisel Verilerinin Korunması Hakkı, Adalet Yayınevi, Ankara.

◊ HAYES, A. (2021). Wearable Technology. Erişim adresi:https://www.investopedia.com/terms/w/wearable-technology.asp

◊ International Labour Organization. (1997). Protection of Workers' Personal Data. Erişim adresi: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf.

◊ "Kartlı Geçiş Sistemi Nedir? Çalışma Prensibi Nasıldır?". (2022). Erişim adresi: https://www.netser.com.tr/tr/blog/kartli-gecis-sistemi-nedir-calisma-prensibi-nasil-netser-blog

◊ Kişisel Verileri Koruma Kurulu. (2019). 25/03/2019 tarihli ve 2019/81 Sayılı Karar, 31/05/2019 Tarihli ve 2019/165 sayılı Karar. Erişim adresi: https://www.kvkk.gov.tr/Icerik/5496/2019-81-165

◊ Kişisel Verileri Koruma Kurulu. (2020). 12/03/2020 tarihli ve 2020/212 sayılı Karar. Erişim adresi: https://www.kvkk.gov.tr/Icerik/6892/2020-212

◊ Kişisel Verileri Koruma Kurulu. (2020). 20/05/2020 tarihli ve 2020/404 sayılı Karar. Erişim adresi: https://www.kvkk.gov.tr/Icerik/6913/2020-404

◊ Kişisel Verileri Koruma Kurulu. (2020). 25/06/2020 tarihli ve 2020/494 sayılı Karar. Erişim adresi: https://www.kvkk.gov.tr/Icerik/6925/2020-494

◊ Kişisel Verileri Koruma Kurulu. (2021). 09/03/2021 Tarihli ve 2021/205 Sayılı Karar. Erişim adresi: https://www.kvkk.gov.tr/Icerik/7113/2021-205

◊ Kişisel Verileri Koruma Kurulu. (2021). 25/11/2021 Tarihli ve 2021/1187 sayılı Karar. Erişim adresi: https://www.kvkk.gov.tr/Icerik/7269/2021-1187

◊ Kişisel Verileri Koruma Kurulu. (2022). 04/08/2022 tarih ve 2022/797 sayılı Karar. Erişim adresi: https://www.kvkk.gov.tr/Icerik/7434/2022-797

◊ Kişisel Verileri Koruma Kurulu. (2023). 19/01/2023 tarihli ve 2023/86 sayılı Karar. Erişim adresi: https://www.kvkk.gov.tr/Icerik/7593/2023-86

◊ Kişisel Verileri Koruma Kurumu. Açık Rıza. Erişim adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf

◊ Kişisel Verileri Koruma Kurumu. Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber. Erişim adresi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abe1-d32dc18e-2d7e.pdf

◊ KÜZECİ, E. (2018). Kişisel Verilerin Korunması, Turhan Kitabevi, Ankara.

◊ MANAV, E. (2015). İş İlişkisinde İşçinin Kişisel Verilerinin Korunması. *Gazi Üniversitesi Hukuk Fakültesi Dergisi, 19(2),* 95-136

◊ SEVİMLİ, A. (2006). İşçinin Özel Yaşamına Müdahalenin Sınırları. Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

◊ T24. (2017). Şehir Hastanesinde Eşyalar Bile Takip Ediliyor, Çalışanlar Çipli Köle Mi?. Erişim adresi: https://t24.com.tr/haber/sehir-hastanesinde-esyalar-bile-takip-ediliyor-calisanlar-cipli-kole-mi,516532

◊ Türk Tabipleri Birliği. (2017). Şehir hastanelerindeki çipli takibe son verilmelidir. Erişim adresi: https://ttb.org.tr/haber_goster.php?Guid=84cc8a3a-ea-ed-11e7-ad3f-8fdeacc2c79e

◊ UNCULAR, S. (2014). İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Seçkin Yayıncılık, Ankara

◊ UNCULAR, S. (2018). İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Seçkin Yayıncılık, Ankara

◊ Yargıtay 22. Hukuk Dairesi. (2015). 2015/28830 Esas ve 2018/15646 sayılı Karar.

◊ Yargıtay 22. Hukuk Dairesi. (2017). 2017/21857 Esas ve 2019/9884 sayılı Karar. Erişim adresi: https://www.lexpera.com.tr/ictihat/yargitay/22-hukuk-daire-si-e-2017-21857-k-2019-9884-t-7-5-2019.

◊ Yargıtay 9. Hukuk Dairesi. (2016). 2016/14203 Esas ve 2017/9524 sayılı Karar.

◊ YÜKSEL, M. (2003). Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi. *Ankara Üniversitesi SBF Dergisi, 58(1),* 181-213.

KÜÇÜK VE ORTA BÜYÜKLÜKTEKİ İŞLETMELERİN VERİ KORUMA HUKUKUNA UYUMU SÜRECİNDE DAVRANIŞ KURALLARI MEKANİZMASI

Gökalp YAVUZ

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "Küçük ve Orta Büyüklükteki İşletmelerin Kişisel Verilerin Korunması Mevzuatına Uyumu Sürecinde Davranış Kuralları Mekanizmasının Önemi ve Türkiye'de Uygulanabilirliği" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Toplum hayatında meydana gelen her değişiklikte olduğu gibi kişisel verilerin korunması da dijitalleşmeye koşut olarak 1970'li yıllardan itibaren hukuki düzenlemelerin gerçekleştirilmesini gündeme getirmiştir (Aktaran: Vincent, 2017, s. 202). Söz konusu düzenlemelerden bir tanesi olan 1981 yılında kabul edilen 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin (108 sayılı Sözleşme) girişinde yer alan temel değerler olan özel yaşama saygı ile bilgilerin serbest dolaşımı arasındaki uyumun sağlanması vurgusu, hem dijitalleşmenin getirdiği umutlar ve korkular arasında bir denge kurulması hem de kişisel verilerin korunması ile diğer temel hak ve özgürlükler arasındaki ilişkinin sınırlarının değerlendirilmesindeki yaklaşımı yansıtmaktadır (Aktaran: Vincent, 2017, s. 205).

Avrupa Birliği (AB) hukukunda kişisel verilerin korunması alanında yıllardır süregelen düzenlemelerin geldiği son noktaya işaret eden Avrupa Genel Veri Koruma

Tüzüğü (GVKT) kabul edildiği dönemin gereklerine göre mahremiyetin korunması amacını güderken bu hedefini diğer temel hak ve özgürlüklerle dengeli bir biçimde gerçekleştirmeyi gözetmektedir (Wachter, 2017). Bu kapsamda, kişisel verilerin etkin bir biçimde korunmasını sağlarken diğer temel hak ve özgürlüklere zarar verilmemesini teminen getirilen en önemli mekanizmalardan bir tanesi Avrupa Parlamentosu ve Avrupa Konseyinin Kişisel Verileri İşlenen Bireylerin Korunması ve Bu Verilerin Serbest Dolaşımı Hakkında 24 Ekim 1995 tarihli ve 95/46/EC sayılı Direktifi'nde (Direktif) de yer almasına rağmen GVKT'de çok daha kapsamlı bir şekilde düzenlenen davranış kurallarıdır. Davranış kuralları, özellikle belirli sektörlerin ve mikro, küçük ve orta ölçekli işletmelerin veri koruma hukukuna uyum sorununa getirilen bir çözüm olmakla birlikte dünya ekonomisinin ana omurgasını teşkil eden bu işletmelerin bir aktarım mekanizması olarak kullanabilmeleri sebebiyle ilgili kişilere ve veri sorumlusu veya veri işleyen olarak hareket eden bu işletmelere önemli faydalar sağlamaktadır.

Türkiye ekonomisinin de temelini teşkil eden küçük ve orta büyüklükteki işletmelerin (KOBİ) ekonomik ve kültürel sermaye kaynaklarının yetersizliği sorunlarının bulunduğu Türkiye'de veri koruma hukukuna ilişkin farkındalık her geçen gün artmakla birlikte alanın görece yeni olması ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (6698 sayılı Kanun) kapsamının davranış kuralları gibi mekanizmaları içine alacak şekilde hazırlanmaması gibi sebeplerle özellikle sınırlı kaynaklara sahip olan KOBİ'lerin 6698 sayılı Kanun ve ikincil düzenlemelere uyum sağlama hususunda sorunlar yaşadığı gözlemlenmektedir. Bu kapsamda, söz konusu sorunlar nedeniyle 6698 sayılı Kanun ve ikincil düzenlemelerine uyum sürecinde başarısızlıklar yaşanması veya uyum sürecinin gecikmesi sonucunda KOBİ'lerin Kanun uyarınca veri sorumlusu sıfatıyla idari yaptırımlara maruz kalması hususu gündeme gelebilecektir.

Bu çalışmada, veri koruma hukuka uyum sorunlarının temel nedenlerini de içinde barındıran KOBİ'lerin AB ve Türkiye'de veri koruma hukukuna uyum hususundaki sorunları ile AB hukukunda bu sorunların giderilmesinde kullanılabilen davranış kurallarına ilişkin düzenlemeler incelenecek olup bu mekanizmanın Türkiye'de uygulanabilirliğine ilişkin değerlendirmelere yer verilecektir.

KÜÇÜK VE ORTA BÜYÜKLÜKTEKİ İŞLETMELER (KOBİ)

KOBİ kavramı gündelik hayatta sıkça duyduğumuz bir tamlama olmakla ve dünya ekonomilerinin temel dinamiğini teşkil etmekle birlikte kavrama ilişkin genel geçer bir tanım bulunmamaktadır (Aktaran: Mecek, 2020). Bununla birlikte, Avrupa Birliği ve Türk hukukunda KOBİ'lere yönelik tanımlar ve sınıflandırmalar

yapılmıştır. Avrupa Komisyonu tarafından yayımlanan rehberde, Avrupa Birliği (AB) ölçeğinde ilk KOBİ tanımının 3 Nisan 1996 tarihli ve 96/280/EC sayılı Komisyon Tavsiyesiyle yapıldığı belirtilmekte olup bu tanımın bugün geçerliliğini sürdüren 6 Mayıs 2003 tarihli ve 2003/361/EC sayılı Komisyon Tavsiyesiyle revize edildiği ifade edilmektedir (European Commission, 2015). 1 Ocak 2005 tarihinde yürürlüğe giren bu Komisyon Tavsiyesinde KOBİ'ler 250 kişiden az çalışanı olan ve yıllık cirosu 50 milyon Euro'yu, yıllık bilançosu ise 43 milyon Euro'yu geçmeyen işletmeler olarak tanımlanmaktadır. Bu tanım altında yapılan sınıflandırmada, mikro ölçekli işletmeler, 10 kişiden az çalışanı olan ve yıllık cirosu ve/veya yıllık bilançosu 2 milyon Euro'yu geçmeyen, küçük ölçekli işletmeler ise 50'den az çalışanı bulunan ve yıllık cirosu ve/veya yıllık bilançosu 10 milyon Euro'yu geçmeyen işletmeler olarak belirlenmiştir (EUR-LEX, 2003).

Türk hukukunda ise, 16 Nisan 2005 tarihli Resmî Gazetede yayımlanarak yürürlüğe giren 5331 sayılı Sanayi ve Ticaret Bakanlığının Teşkilât ve Görevleri Hakkında Kanuna Bir Ek Madde Eklenmesine İlişkin Kanun ile kurum ve kuruluşların uygulamada kullanacakları bir tanımlama yapılmıştır (Çatal, 2007). Buna göre; KOBİ'lerin tanımlanmasına, niteliklerine, sınıflandırılmasına ve uygulamalarına ilişkin esasların; net satış hasılatları, mali bilanço tutarları ve çalışan sayıları dikkate alınarak Bakanlıkça hazırlanan ve Bakanlar Kurulunca yürürlüğe konulan yönetmelikle belirleneceği hüküm altına alınmıştır (Sanayi ve Ticaret Bakanlığının Teşkilât ve Görevleri, 2005). 1 Ocak 2005 tarihinde AB'de yapılan ortak tanımın aday devletlere de tavsiye edilmesi üzerine 18 Kasım 2005 tarihli Resmî Gazete'de yayımlanan Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri ve Sınıflandırılması Hakkında Yönetmelik 18 Mayıs 2006 tarihinde yürürlüğe girmiştir. Bu yönetmelikte AB'deki uygulamaya uygun olarak satış büyüklükleri, bilanço ve çalışan sayıları kriterleri dikkate alınmıştır (Aktaran: Mecek, 2020). Söz konusu Yönetmelik'te 250'den az yıllık çalışanı bulunan ve yıllık net satış hasılatı ya da mali bilançosu 25 milyon Yeni Türk Lirasını aşmayan işletmeler KOBİ olarak tanımlanmıştır. Buna göre; mikro işletmeler yıllık çalışan sayısı 10 kişiden az ve yıllık net satış hasılatı ya da mali bilançosu 1 milyon Yeni Türk Lirasını aşmayan, küçük işletmeler 50 kişiden az yıllık çalışan sayısı bulunan ve yıllık net satış hasılatı ya da mali bilançosu 5 milyon Yeni Türk Lirası'nı aşmayan, orta ölçekli işletmeler ise 250'den az yıllık çalışan sayısı bulunan ve yıllık net satış hasılatı ya da mali bilançosu 25 milyon Yeni Türk Lirası'nı aşmayan işletmeler olarak sınıflandırmaya tabi tutulmuştur (Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri ve Sınıflandırılması, 2005). 25 Mayıs 2023 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe giren ve Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri ve Sınıflandırılması Hakkında Yönetmelik'i yürürlükten kaldıran Küçük ve Orta Büyüklükteki İşletmeler Yönetmelik'inde çalışan sayısı kriterleri

sabit kalmakla birlikte yıllık net satış hasılatı veya yıllık mali bilanço kriterlerinde değişiklik yapılarak üst sınır 500 milyon TL olarak belirlenmiştir. Bu kapsamda, yıllık net satış hasılatı veya yıllık mali bilanço üst sınırında mikro ölçekli işletmeler için 10 milyon TL, küçük ölçekli işletmeler için 100 milyon TL, orta ölçekli işletmeler için ise 500 milyon TL olarak sınıflandırmaya gidilmiştir (Küçük ve Orta Büyüklükteki İşletmeler Yönetmeliği, 2023).

KOBİ'LERİN EKONOMİDEKİ YERİNE SOSYOLOJİK BİR BAKIŞ: PIERRE BOURDIEU'NUN SERMAYE KURAMI, HABİTUS (YATKINLIK) VE ALAN KAVRAMLARI

İktisat biliminde güncel yaklaşımlar daha çok sayısal veriler üzerinden ekonomik göstergeleri analiz etme mantığına yakın olsa da bu yaklaşım makro göstergelere ve teorik açıklamalara odaklanması sebebiyle ülkelerin toplumsal, kültürel ve tarihi özgünlüklerini ve bunların o ülkelerin ekonomik pratiklerine yansımalarını anlamakta zorluklara neden olabilmektedir. Halbuki, her toplumun kendi tarihsel, kültürel ve güncel pratiklerinden gelen özgün nitelikleri bulunmaktadır. Bunları anlamak ve ekonomik hayatı bunlarla birlikte yorumlamak, pratiği anlamak dolayısıyla sorunları tespit etmek ve bu sorunlara yönelik çözüm önerilerini geliştirmek açısından önem arz etmektedir. Ekonomiyi salt sayısal verilere indirgemek yerine toplumsal hayat ve ekonomik pratikler arasındaki dinamik ilişkiyi anlamlandırmaya çalışan bu yaklaşıma literatürde ekonomik sosyoloji adı verilmektedir.

Söz konusu yaklaşımın en önemli temsilcilerinden olan Pierre Bourdieu özellikle Cezayir'de yaptığı etnolojik çalışmalarda bu toplumda şeref ve evlilik kavramları ile akrabalık ilişkileri gibi olguların pratikte ne anlama geldiği sorusuna teorik cevaplar bulmaya çalışmıştır. Bourdieu'nun daha sonra hayatı boyunca yapacağı çalışmaları da şekillendiren bu deneyimi onun bir sosyolojik ekol haline gelmesinde büyük öneme sahip olmuştur (Bourdieu, 2018).

Sermaye Kuramı ve Sermaye Türleri

Bourdieu'da sermaye, yalnızca ekonomik bir değer olarak değerlendirilmeyip bunun yanında iktisadi sermaye, kültürel sermaye, toplumsal sermaye ve simgesel (sembolik) sermaye gibi dallanan ve birbirleriyle ilişkisel bir anlama sahip bir düşünce sisteminin üzerinde şekillendirilmektedir. İktisadi sermaye, bireyin hem maddi varlığı hem de geliri olmak üzere ekonomik kaynaklarının tümü anlamına gelirken kültürel sermaye yetenek, bilgi ve becerilerin yanı sıra sanatsal tablolar ve kitaplar gibi kültürel mallara sahip olmak ile öğretim yoluyla elde edilen unvanların şekillendirdiği bir birikime işaret etmektedir. Yine, toplumsal sermaye bireylerin birbirleriyle tanışmaları ve karşılıklı tanımaya dayalı kurumsallaştırılmış bir ilişkiler ağına bağlı mevcut veya potansiyel bir kaynaklar bütünü olarak kişinin sahip olduğu tanışıklıklar ve ilişkiler ağına (günümüzde sıkça kullanılan tabirle network) işaret ederken simgesel (sembolik) sermaye toplumsal tanınırlık/bilinirlik ve itibar/prestij kavramlarıyla yakından ilişkili bir değer olarak karşımıza çıkmaktadır. Bourdieu'nun kavramlarıyla konuşursak kişinin toplumsal uzamda alacağı pozisyonun ya da diğer ifadeyle konumunun belirlenmesinde en önemli etkenlerden biri hangi sermayeye ne kadar sahip olduğu ve bu sermayeleri birbirine nasıl dönüştürebildiği ile yakından ilişkilidir (Jourdain ve Naulin, 2016, ss. 106-107).

Habitus (Yatkınlık) Kavramı

Swartz'a göre; habitus kavramı Bourdieu'nun birey ile toplumu birbirinden ayrı iki varlık olarak değil aynı toplumsal gerçekliğin iki boyutu gibi ilişkisel olarak değerlendirerek Batı entelektüel geleneği içerisindeki klasik birey-toplum ikiliğini aştığını düşündüğü bir formüldür (Swartz, 2015, ss. 138-139). Pierre Bourdieu habitus kavramını "bir amacın ve bu amaca ulaşmak için gerekli işlemlerin bilincinde olunduğunu varsaymadan, nesnel bir şekilde amaçlarına uyumlu olan pratikleri ve tasarımları oluşturan ve düzenleyen ilkeler" olarak tanımlamaktadır (Aktaran: Jourdain ve Naulin, 2016, s. 42).

Ayrıca, "bireylerin toplumsal dünyayı algıladığı zihinsel yapıları" olarak da tanımlanan habitus kavramı Türkçeye, Bourdieu'nun tekrarlı, mekanik ve üretken olmayıp çoğaltkan olan habitude (alışkanlık) kavramı yerine bilinçli bir biçimde etkin bir üretme gücü olduğunu düşünmesi sebebiyle yatkınlık olarak çevrilmektedir (Aktaran: Jourdain ve Naulin, 2016, s. 46). Ökten'e göre; bu tercih yapı kelimesine çok yakın bir anlam sunan örgütleyici bir eylemin sonucunu ifade etmesi ve bir varoluş tarzını, alışıldık bir hali ve bir temayülü tanımlaması sebebiyle uygun bulunmaktadır (Bourdieu, 2018, s. 158).

Bireyin içinde bulunduğu sosyoekonomik koşullar çerçevesinde bilinçdışı bir biçimde geliştirdiği yatkınlıklarına örnek olarak Bourdieu, Cervantes'in kahramanı Don Kişot'un şövalyeliğin ortadan kalkmasına rağmen şövalye gibi davranmaya devam etmesi örneğini verir (aktaran Jourdain ve Naulin, 2016, s. 43). Jourdain ve Naulin'e göre; habitusun koşullarının devamlılığı kişilerin içinde kemikleşmesi ve değişime karşı bir dirence dönüşmesine bağlı olup bireyler sosyoekonomik çevre koşullarında radikal bir dönüşüm olmadığı sürece bu eğilimlerini muhafaza etmeye yatkındır (Jourdain ve Naulin, 2016, s. 43). Swartz'a göre ise; habitusun

karşılaştığı yeni durumlara tepkisi bir uyarlanma sürecine işaret etmekle birlikte bu süreç bilinçdışı olarak yavaş işleyen bir süreç olup belirli yatkınlıklarda kökten değişim yerine bir tür şekillenme/şekillendirme anlamını taşımaktadır (Swartz, 2015, s. 153).

Alan Kavramı

Alan kavramı, Bourdieu'nun iş bölümünün arttığı ve buna bağlı olarak toplumsal dünyada artan farklılaşma süreci sayesinde toplumsal hayatın çevrelerinin özerkleşmesi olarak tanımlanmakta olup söz konusu özerkleşmiş çevreler olan alanların ayırt edici özelliği kendine özgü bir amacının bulunmasıyla ilişkilidir. Her toplumun kendi koşullarına göre siyasi alan, iktisadi alan ve edebi alan gibi çeşitlenen alanların her birinin kendine özgü bir amacı vardır. Örneğin, siyasi alanda eylemde bulunanların amacı iktidarken iktisadi alanın temel amacı zenginlik ve edebi alanın ise tanınırlıktır. Bu hedeflere ulaşmak için ortaya çıkan davranış biçimleri Bourdieu'nun sermaye kuramı ve habitus kavramı ile yakından ilişkilidir. Alanda faaliyette bulunanların bu alanda edindikleri konumunu ellerinde tuttukları çeşitli sermaye türlerinin formülasyonundan oluşan sermaye birikimi belirlemektedir (Jourdain ve Naulin, 2016, s. 122).

Jourdain ve Naulin'e göre Bourdieu'nun alanda eylemde bulunanların konumlarına ilişkin verdikleri mücadelenin iki temel stratejisi muhafaza ve yıkım üzerine kuruludur. Belirli bir alanda hakim durumda bulunanlar muhafaza stratejilerini geliştirirken hakim konuma gelmek isteyenler yıkım stratejilerini kullanmaktadır. Söz konusu alanda konumlanmak için verilen mücadelenin sınırını belirleyen ise hepsinin ortak çıkarı olan alanın varlığını sürdürmesidir. Zira, alanın varlığını kaybetmesi alanda yer alan tüm faillerin alanla birlikte var olan konumlarını kaybetmelerine yol açacaktır (Jourdain ve Naulin, 2016, ss. 126-128). Bir alanda konumunu koruma ve geniş anlamda hayatta kalma mücadelesi veren bir aktörün eylemde bulunurken gösterdiği davranış biçimlerinin en önemli belirleyicisi ise alanın kural ve ödüllerinin tanınırlığını ve bilinirliğini sağlayan alana özgü habitustur. Diğer bir deyişle, habitus bireylerin bilinçli bir hesap yapmaksızın bilinçaltı olarak kendiliğinden alanın gerekliliklerine uygun eylemelerini sağlayan bir araçtır (Jourdain ve Naulin, 2016, s. 124).

Bourdieu Sosyolojisinin Ekonomik Kullanımları

Bourdieu'nun son dönem çalışmalarından biri olan Ekonominin Toplumsal Yapıları isimli eserinde iktisatçıların her sosyal mikro kozmosun kendine özgü tikel yanlarını göz önünde bulundurmama yönünde bir eğilimleri olduğu belirtilirken

iktisat biliminin tarihsel olmayan bu bakış açısına karşın bir taraftan ekonomik faillerin ve özellikle bunların zevkleri, ihtiyaçları, istidatları ve becerilerinin ekonomik yeri ile spesifik bir oyuna benzetilen kendi kurallarını takip eden bir kozmos olarak ekonomik alanın kendisinin oluşumlarının yeniden yapılandırılmasının zorunluluğuna işaret edilmektedir. Bu kapsamda, ihtiyaçlar, tercihler ve istidatlar gibi en temel ekonomik eğilimlerin insan doğasına bağlı bir biçimde dışsal değil özellikle bu eğilimlerin gerekli olduğu ve ödüllendirildiği ekonomik kozmosun tarihine ve genelde tarihe bağlı bir biçimde içsel olduğunu belirtilmektedir (Bourdieu, 2005, ss. 2-8).

Bourdieu alanda faaliyette bulunanlar ile alan arasındaki ilişkinin karşılıklı etkileşime dayalı olduğunu belirtmekte olup kavramı faaliyette bulunanların sahip oldukları alanın mantığına özgü bir habitus ve alanda pozisyon almak için gerekli olan sermaye türleriyle ilişkilendirmektedir. Gündelik hayatta sıkça kullandığımız bir tabir olan sektör kavramını bir alt alan, sektörleri de ekonomik alanın altında alt alanlar olarak değerlendirmektedir. Her alanın ve alt alanın kendi tarihselliği içerisinde belirli özelliklere sahip olmasının yanında alanda bulunan aktörlerin de alandaki etkinlikleri farklı sermaye türleri arasında sahip oldukları formülasyona ve alanın gerektirdiği yatkınlıklara ne denli uyum sağladıklarına bağlı olarak değişmektedir (Bourdieu, 2005, ss. 193-215).

Türkiye'de ticaret hayatı özelinde düşünüldüğünde KOBİ'ler arasında toplumsal sermaye ve sembolik sermayeye dayanan sermaye birikimi stratejilerinin geleneksel olarak pek çok alt alanda görüldüğünü söylemek mümkün iken ekonomide ve teknolojide yaşanan dönüşümler sebebiyle toplumsal sermaye ve sembolik sermayenin ekonomik sermayeye dönüştürülmesinde karşılıklı güvene dayanan ilişkilerin bankacılık sektörü üzerinden yürütülen iş ve işlemler üzerinden ekonomik sermaye birikimine yönelen bir dönüşüm geçirdiğini söylemek yanlış olmayacaktır.

Ayrıca, KOBİ'lerin teknolojik gelişmelere ve yeniliklere uyum sağlaması; rekabet halinde oldukları ulusal ve uluslararası alanlarda oyunun kurallarını değiştirme şansını kendilerine vermesi açısından önemli bir faktör olmakla birlikte yerleşik oldukları ülkelerin mevzuatlarının söz konusu gelişme ve yeniliklere engel olmaması kadar KOBİ'lerin yürürlükte olan ulusal ve ulus ötesi mevzuatlara uyumu da büyük önem arz etmektedir. Mevzuatların, Bourdieu'nun ortaya koyduğu ulusal sermaye kavramıyla birlikte düşünülmesi halinde firmaların küresel ölçekte birbirleriyle rekabetlerinde pozitif veya negatif anlamda çarpan etkisi yaratabileceğini göz önünde bulundurmak gerekmektedir (Bourdieu, 2005, s. 229).

Bu kapsamda, Türkiye'de yerleşik küçük ve orta büyüklükteki işletmelerin hem ulusal pazarda hem uluslararası pazarda büyük ölçekli firmalarla rekabet edebilmesi dezavantajlı durumda bulundukları noktalarda desteklenmeleriyle mümkün olacaktır. Halihazırda, devlet tarafından KOBİ'lere sağlanan çok sayıda destek bulunmakla birlikte 6698 sayılı Kanun'a ve ilgili mevzuata uyum ve bununla da ilişkili olarak AB vatandaşlarına yönelik ürün ve hizmet sunumunda bulunmaları sebebiyle GVKT'ye uyum hususlarında ekonomik ve kültürel sermaye yetersizliği sebebiyle gerekli teknik ve hukuki gerekliliklere büyük işletmeler kadar kolay ulaşamamaları bir sorun olarak karşımıza çıkmaktadır.

AB hukukunda söz konusu soruna ilişkin belirli mekanizmalar geliştirilmiş olmakla birlikte Türk hukukunda kişisel verilerin korunması konusunun yeni olması sebebiyle sektörlere özel mekanizmaların gelişmemiş olduğu değerlendirilmektedir. Sonraki bölümlerde, KOBİ'lerin Avrupa ve Türkiye'de veri koruma mevzuatına uyum konusunda yaşadıkları sorunlara detaylı bir biçimde değinilecek olup Avrupa'da buna ilişkin geliştirilen ve Türkiye'de geliştirilmesi mümkün olduğu düşünülen mekanizmalara değinilecektir.

KOBİ'LERİN VERİ KORUMA HUKUKUNA UYUM SORUNLARI

Küçük ve orta büyüklükteki işletmeler, büyük işletmelere nazaran daha az ekonomik sermayeye sahip olmaları, daha az kurumsallaşmış yapıları ve alanda iş yapma biçimlerinden doğan yatkınlıkları sebepleriyle ilişkili olarak yaşadıkları hukuki düzenlemelere uyum sorununu 1970'li yıllardan itibaren teknolojideki gelişmelere koşut olarak Avrupa'da ortaya çıkıp gelişmeye başlayan kişisel verilerin korunması alanında da alanın hem hukuki hem teknik bilgi gerektirmesi ve çok hızlı değişime açık olması sebebiyle daha şiddetli hissetmektedirler.

Avrupa Birliği ülkelerinde 1970'lerden itibaren başlayıp bugünlere kadar gerçekleştirilen çok sayıda hukuki düzenlemeye ve tecrübeye rağmen KOBİ'ler bugün tüm Avrupa Birliği üye ülkelerinde yürürlükte bulunan GVKT'ye uyum hususunda halen sorunlar yaşayabilmektedirler. Birleşik Krallık Veri ve Pazarlama Kuruluşunun (DMA) KOBİ'lerde çalışan 293 pazarlama uzmanıyla yaptığı çalışmaya katılan KOBİ'lerin %74'ünün şirketlerinin GVKT hakkında bilgisinin yüksek olduğunu ifade etmesine rağmen rapordan sadece %10'unun tam anlamıyla uyumlu olduğu, %25'inin uyum hususunda erken aşamalarda bulunduğu ve %65'inin ise uyum konusunda yolun yarısı veya 3/4'ü kadar mesafe kat ettiği anlaşılmaktadır. Rapora göre, KOBİ'lerin %38'i GVKT'nin elde ettikleri ve işledikleri müşteri verilerine uygulanmadığına inanır görünürken sektörün çok büyük bölümünün GVKT'den haberdar olmakla birlikte bilgi eksikliği ve orta ölçekli işletmelerde

sunulan eğitimlerle ilgili bir sorunun olduğu tespitinde bulunulmaktadır (DMA Survey Highlights Gaps, 2020).

Türkiye'de ise ilk olarak 2004 yılında 5237 sayılı Türk Ceza Kanunu'nda ve 2010 yılındaki Türkiye Cumhuriyeti Anayasası'ndaki değişikliklerle kişisel verilerin korunması hakkında hukuki düzenlemelere gidilmiş olup son olarak 2016 yılında yürürlüğe giren 6698 sayılı Kanun ile alana ilişkin hukuki düzenlemelere yer verilmiştir. Bu kapsamda, kişisel verilerin korunması Türk hukukunda yeni bir alan olma özelliğini korumaktadır. KOBİ'lerin söz konusu içkin dezavantajlarının yanı sıra, alanın Türk hukukundaki ve kamuoyundaki yeni olma özelliği küçük ve orta ölçekli işletmelerin uyum sorununu AB üyesi ülkelerdeki işletmelere nazaran daha büyük bir sorun haline getirmektedir.

Kişisel verilerin korunması alanının Türkiye'de görece yeni bir alan olmasının yanı sıra KOBİ'lerin uzun tecrübelerin bir bakiyesi olarak kazandıkları yatkınlıklarının mevzuata uyum konusunda da sorun yaşamalarına sebep olduğu değerlendirilmektedir. Büyük şirketler, AB ülkelerine mal ve hizmet sunmaları, hukuk müşavirliği ve bilgi teknolojileri gibi departmanlara sahip olmaları sebebiyle mevcut ekonomik ve kültürel sermaye kaynaklarını mevzuata uyum için kullanabilirken KOBİ'ler söz konusu sermaye kıtlıkları sebebiyle uyum problemleri yaşamaktadırlar.

Avrupa Birliği Hukukunda KOBİ'lerin Uyum Sorunları

Direktif Kapsamında KOBİ'lerin Uyum Sorunları

Komisyon tarafından kendisine özellikle yeni teknolojiler ve küreselleşme ışığında kişisel verilerin korunmasında yeni sorunlara ilişkin görüşünün sorulması üzerine WP29, 1 Aralık 2009 tarihli Mahremiyetin Geleceği isimli görüşünde Direktif'in uygulamadaki yansımalarına ilişkin bazı tespitlerde bulunmakta olup yeni bir yasal çerçeve ihtiyacının bulunduğunu ifade etmektedir (Article 29 Working Party, 2009). Söz konusu tespitlerden bir veri sorumlusu veya veri işleyen olarak hareket eden KOBİ'lerin karşılaştığı uyum sorunlarına ilişkin çıkarımlarda bulunmak mümkündür.

Görüşte, Direktif'in AB genelinde bir düzenleme olarak iki amacının AB içerisinde bir üye devletten diğerine kişisel verilerin serbestçe aktarılmasına izin veren bir iç pazarın tesis edilmesi ve işlerlik kazanması ve aynı zamanda bireylerin temel haklarının yüksek bir seviyede korunmasının güvence altına alınması olduğu belirtilmektedir. Bununla birlikte, Direktif döneminde var olan uygulama-

nın, AB yetki alanının tamamını kapsayan daha kapsamlı ve tutarlı veri koruma çerçevesini gerektirdiği ifade edilmektedir. Buradaki amaç uygulamada var olan farklılıkların ve ayrılıkların tüm bireylerin hatasız, tutarlı ve etkili bir biçimde korunmasına engel olması sorununun ortadan kaldırılmasıdır. Söz konusu hatasız, tutarlı ve etkili koruma ile birlikte tüm sektörlerde gerçekleştirilen kişisel veri işleme faaliyetlerinde bütüncül bir yaklaşımı temin etmek üzere temel güvencelerin ve ilkelerin uygulanması gerektiği belirtilmektedir (Article 29 Working Party, 2009, ss. 7-8). Zira Direktif'in, GVKT'den farklı olarak üye devletlerin ulusal hukuklarında doğrudan sonuç doğurmayıp bir yasal çerçeve çizmesi üye devletlerin kişisel veri koruma mevzuatlarında farklılıkların bulunmasına yol açıyordu ve dolayısıyla veri sorumlusu veya veri işleyenlerin her üye devletin mevzuatına ayrı ayrı uyumluluk sağlaması gerekmekteydi.

Görüşte, ihtiyaç duyulan yeni yasal çerçevede rıza ve şeffaflık gibi önemli kavramların netleştirilmesine vurgu yapılmakta olup mevcut kurallarda bazı faydalı yeniliklerin yapılabileceği ifade edilmektedir. Bunlar arasında idari ve teknik tedbirlere ilişkin mevcut hükümlere tasarım aşamasında mahremiyet kavramının dahil edilmesi ve GVKT'nin de temel direğini teşkil eden hesap verebilirlik ilkesine yeni yasal çerçevede yer verilmesi örnekleri verilmektedir (Article 29 Working Party, 2009, s. 6).

WP29'un 13 Temmuz 2010 tarihli Hesap Verebilirlik İlkesi üzerine 3/2010 sayılı görüşünde ise; AB veri koruma ilkelerinin ve yükümlülüklerinin, somut iç tedbirlere ve uygulamalara aktarılmasında yaşanan sorunlara vurgu yapılmakta olup kişisel verilerin korunmasının, bir kuruluşun değerlerinin ve uygulamalarının parçası haline gelmedikçe ve bu kapsamda sorumlulukların çerçevesi çizilmedikçe etkin uyumluluğa ilişkin sorunların çözümünün mümkün olmayacağı ifade edilmektedir (Article 29 Working Party, 2010). Veri korumanın teorik çerçeveden çıkıp pratikte var olan bir olgu haline gelmesinin; diğer bir ifadeyle kişisel verilerin gerçekten korunmasının Mahremiyetin Geleceği isimli görüşte de belirtildiği üzere hesap verebilirliğe dayalı mekanizmaların geliştirilmesiyle mümkün olabileceği ifade edilmektedir. Bu ilkeye yeni yasal çerçevede yer verilmesinin veri sorumlularının rolünün ve sorumluluğunun artırılmasına yardımcı olacağı belirtilmektedir (Article 29 Working Party, 2010, s. 3).

WP29'a göre; yeni yasal çerçevede yeni olan veri sorumlularının uyması gereken ilkeler ve yükümlülükler değil Direktif döneminde zaten var olan bu ilke ve yükümlülüklere etkin bir biçimde uyum sağlanabilmesi imkânı olacaktır. Diğer bir ifadeyle; teorik çerçevede var olan ilke ve yükümlülükler kapsamındaki kişisel verilerin korunmasının pratikte temin edilen bir olguya dönüşmesi hedeflenmektedir (Article 29 Working Party, 2010, s. 10). Bu kapsamda, kişisel verilere yönelik risklerin ve kişisel verilerin değerinin artmasının veri sorumlularının rol ve sorumluluklarının artırılması ihtiyacını doğurduğu belirtilmekte olup bu yeni gerçekliğe hitap edecek düzenleyici çerçevenin veri sorumlularını uygulamada kişisel verilerin korunmasına ilişkin uygun ve etkili tedbirleri almaya teşvik edecek gerekli araçları içermesi gerektiği ifade edilmektedir (Article 29 Working Party, 2010, s. 19).

Direktif'te bu amacı gerçekleştirmeye yönelik yapılacak değişikliğin veri sorumlularının Direktif'te yer alan ilke ve yükümlülüklerini yerine getirmelerini temin etmek adına uygun ve etkili tedbirleri almaya ve otoriteler tarafından talep edildiğinde bunu gösterebilmeye sevk etmesi gerektiği belirtilmektedir. Bu tedbirlerin uyum sorununu çözmeye yardımcı olurken kişisel verilerin korunmasına yönelik ihlallere ilişkin riskleri de asgari düzeye indireceği ifade edilmektedir (Article 29 Working Party, 2010, s. 19). Lambert ise veri koruma reformunun, özellikle KOBİ'ler olmak üzere Avrupa iş dünyası için maliyetlerin ve kırtasiyeciliğin azaltılması sebebiyle ekonomik gelişmeye katkı sağlayacağını ifade etmektedir (Lambert, 2017, ss. 40-41). Bu kapsamda, veri sorumlularının Direktif döneminde kişisel veri koruma hukukuna uyum sorunları ve kişisel verilerin daha etkin bir biçimde korunmasına yönelik çözüm arayışları hesap verebilirlik mantığı üzerine inşa edilen GVKT'de yer verilen yeni yükümlülükler ve uyuma ve uyumluluğun gösterilmesine imkân tanıyan kapsamlı mekanizmalarda somutlaşmıştır.

GVKT Kapsamında KOBİ'lerin Uyum Sorunları

Söz konusu değişiklikler veri sorumlusu veya veri işleyen sıfatını haiz çok sayıda kuruluş için uyum sağlanması gereken yeni bir alan olarak görülmekle birlikte özellikle büyük ölçekli işletmelere göre daha az insani ve finansal kaynağa sahip olan küçük ve orta ölçekli işletmeler açısından aşılması gereken bir zorluk olarak bulunmaktadır. Bu kapsamda, akademik yazında küçük ve orta ölçekli işletmelerin GVKT'ye uyum konusunda karşılaştıkları zorluklara ilişkin olarak yapılan çok sayıda araştırma bulunmaktadır.

Bu araştırmalardan bir tanesinde sektörde yer alan 10 KOBİ ile yüz yüze mülakat yapılmış olup araştırmada ulaşılan temel sonuç işletmelerin kişisel verilerin korunması kapsamındaki yükümlülükleri ve görevleri hususundaki farkındalık eksikliğidir. Diğer bir deyişle, küçük ve orta ölçekli işletmeler bu tezin başında da belirtildiği üzere büyük ölçekli işletmelerle rekabet ettikleri alanlarda ekonomik ve kültürel sermaye yetersizlikleri ve uzun yılların iş yapma deneyimlerine dayanan kemikleşmiş yatkınlıkları sebebiyle yükümlülükleri ve görevleri hakkında

net bir bilgiye sahip değildir (Freitas ve Silva, 2018). İlgili araştırmada, uyum hususunda acil olan şeyin KOBİ'lerin bir uyum metodolojisine sahip olmaları olduğu vurgulanmaktadır. GVKT'de düzenleyici denetleyici otoriteye bildirimde bulunma yükümlülüğü uygulamasının kaldırıldığı belirtilmekte olup kuruluşların topladıkları, depoladıkları ve işledikleri kişisel verilerin güvenliğini, mevcudiyetini, gizliliğini ve bütünlüğünü GVKT'ye uyumlu bir biçimde temin etmek zorunda oldukları ve bunu temin ettiklerini ispat edebilmeleri gerektiğinin altı çizilmektedir (Freitas ve Silva, 2018, ss. 1-2).

İlgili çalışma, Portekiz ekonomisinin önemli bir bölümünü teşkil etmeleri ve ülkedeki istihdamın çok ciddi bir yüzdesini karşıladıkları için KOBİ'ler üzerine gerçekleştirilmiş olup söz konusu işletmelerin %99.9'unu temsil kabiliyetine sahip olduğu ifade edilmektedir. Çalışmada Portekiz rekabet edebilmelerine göre beş ana bölgeye ayrılmış olup Lizbon, Aveiro'nun içinde yer aldığı birinci grubun ve Leiria'nın içinde yer aldığı ikinci grubun rekabet edebilme kapasitesi bağlamında GVKT tarafından getirilen değişikliklere uyum sağlamak hususunda daha iyi kaynaklara sahip bulunduğu ifade edilmektedir. Anketin KOBİ'lerin kuruluş içerisindeki kişisel verilerin toplanması, depolanması ve işlenmesi üzerinde etkide bulunabilecek yetkililerine uygulandığı belirtilmektedir (Freitas ve Silva, 2018, ss. 2-3).

Çalışmanın sonucunda elde edilen istatistikler incelendiğinde işletmelerin %90'ının GVKT hakkında hiçbir bilgisinin bulunmadığı görülmüş olup sadece %10'unun GVKT'den haberdar olduğu anlaşılmıştır. Yine işletmelerin ilgili kişilerden açık rıza alma uygulamaları sorulduğunda ilgili kişilerden açık rıza alındığını kanıtlayan bir belgeye sahip olanların oranı %10 iken, bazı belgelere sahip olanların oranı %10 ve ilgili kişilerden açık rıza alındığını kanıtlayan hiçbir belgesi bulunmayanların oranı ise %80 olarak belirtilmiştir. GVKT'de yer alan işleme faaliyetlerinin ana omurgasını oluşturan ilkelere uyumluğun ölçülmesi için yapılan çalışmada söz konusu ilkelerden biri olan veri minimizasyonu ilkesi hususunda her amaç için veri minimizasyonu ilkesine uyum sağlandığını belirtenler %60 oranındayken veri minimizasyonuna uyum sağlamadığını ifade edenlerin oranı %40 olarak belirtilmiştir. Direktif döneminde var olan düzenleyici ve denetleyici otoriteye bildirimde bulunma yükümlülüğünün kaldırılmasından sonra GVKT'de veri sorumlularına getirilen bir yükümlülük olan işleme faaliyetlerinin kaydının tutulmasına ilişkin olarak video gözetim kameralarının listesinin çalışmaya katılanların yalnızca %20'sı tarafından tutulduğu belirtilmekle birlikte %40'ının video gözetim kameralarına ilişkin herhangi bir liste tutmadığı, geri kalan %40'ının ise video gözetim kamerası kullanmadığı ifade edilmektedir (Freitas ve Silva, 2018, s. 4).

Özetle, söz konusu çalışmanın sonucunda mülakat yapılanların büyük çoğunluğunun GVKT hakkında ve açık rızanın alınması, işlemenin ilkeleri ve işleme faaliyetlerinin kaydının tutulması gibi yükümlülük ve görevleri hakkında bilgi sahibi olmadıkları anlaşılmaktadır. Ayrıca, depoladıkları ve işledikleri kişisel verilerin güvenliğinin temin edilmesi kapsamındaki yükümlülükleri konusunda farkındalık seviyelerinin düşük olduğu görülmüş olup ilgili kişilerin haklarının farkında olmadıkları ve bu hakları kullanmalarının temin edilmesine ilişkin prosedürleri uygulamaya geçirmedikleri ifade edilmektedir. Çalışmaya katılan bütün şirketler çalışan sayılarının 250'den az olduğunu belirtmekte olup hiçbirinin veri koruma görevlisi atamadığı ve söz konusu şirketlerin üçüncü tarafların kendilerine sundukları hizmetin ifası için kişisel verileri elde etmesi, depolaması, erişmesi veya işlemesi zorunlu olduğunda aralarında akdettikleri sözleşmelerin GVKT'ye uyumlu olması gerektiği hususunda bir farkındalıklarının bulunmadığı sonucu ortaya çıkmıştır. Ülkelerden hiçbiri kişisel verileri AB dışındaki üçüncü ülkelere ya da uluslararası kuruluşlara aktarmadığını beyan etmiş olup çalışmanın yapıldığı tarihte hiçbir şirketin kişisel verilere erişimi olan çalışanlarına yönelik görevleri ve yükümlülükleri ile ilgili bilgilendirme yapmamakla birlikte sadece bir şirketin bu hususa ilişkin olarak bir eğitim planının bulunduğu ifade edilmiştir. Son olarak, GVKT'de yer alan temel ilkelerden biri olan veri sorumlusunun hesap verebilirliği hususunun çalışmaya katılan hiçbir şirket farkında olmayıp hiçbir şirketin düzenli bir biçimde veya belirli aralıklarla kişisel verilerin korunması düzenlemelerine ve kanunlarına uyumluluklarını değerlendirmedikleri sonucuna varılmıştır. Yine şirketlerin veri ihlallerini veri koruma otoritesine bildirim yükümlülüğünün farkında olmadıkları anlaşılmıştır (Freitas ve Silva, 2018, ss. 3-5).

Çalışma sonucunda, KOBİ'lerin GVKT ve Portekiz Veri Koruma Kanunu hakkında bilgi eksikliklerinin bulunması kapsamında kişisel verilerin korunmasının yeni gerekliliklerine uyumun temin edilmesi için idari ve teknolojik prosedürlerin uygulanmasına ilişkin bir plana ihtiyaç bulunduğu ifade edilmektedir. Söz konusu planın, sektör, satış veya hizmet birlikleriyle iş birliği içerisinde oluşturulması vurgulanmaktadır. Kuruluşların GVKT'ye uyumunun sadece ağır yaptırımlardan kaçınmak için değil artan bir şekilde küreselleşen dünyada sürdürülebilirliklerini ve hayatta kalmalarını garanti altına alan uyumlu şirketlere hizmetlerini sunabilmeleri için de önemli olduğu ifade edilmekte olup GVKT'de yer alan yükümlülüklere uyumun sağlanması için yeterli düzeyde insan kaynaklarına sahip olmama durumu ile birlikte bazı durumlarda bütçeye ilişkin kısıtlarının da bulunması sebebiyle KOBİ'lerin GVKT'ye uyumu hususunda verimli ve etkili çözümlerin bulunmasının hayati öneme sahip olduğu belirtilmektedir (Freitas ve Silva, 2018, ss. 5-6).

Yine 2018 yılında Birleşik Krallık'ta yayımlanan bir akademik çalışmada, GVKT

ile ilgili çalışmalar yürüten on iki kişiyle kuruluşların düzenlemelerle etkileşimleri sürecindeki deneyimlerini anlamak ve GVKT'ye uyum sürecinde kuruluşlar tarafından kullanılan işlemleri araştırmak amaçlarıyla mülakatlar yapılmıştır. Çalışmanın en önemli sonucu, büyük firmalar GVKT'ye uyumu makul ve gerçekleştirebilir bulurken güvenlik odaklı KOBİ'lerin de büyük firmalarla benzer bir yaklaşıma sahip olduğu, kişisel verilerin korunması alanına daha az odaklanmış KOBİ'lerin ise uyum hususunda zorluklar yaşadığı tespiti olmuştur (Sirur, Nurse ve Webb, 2018).

GVKT'ye uyum hususunda KOBİ'lerin yaşadıkları sorunların üye devletlerin birçoğunda yaşandığı görülmektedir. İrlanda KOBİ Derneği tarafından 2018 yılında yayımlanan bir raporda, KOBİ'lerin GVKT ile gelen değişiklik ihtiyacının farkında olmakla ve değişiklikle ilgilenmekle birlikte sadece %30'unun uyum için gerekli adımları attığı ifade edilmektedir (Brodin, 2019, s. 244). Brodin'e göre GVKT'ye uyum bir kerede yapılıp bitirilebilecek bir süreç olmayıp sürekli güncelleme gerektirmekte olup bu güncellemelerin gerçekleştirilebilmesini temin etmek amacıyla belirli periyotlarla uyumluluk denetimlerinin yapılması önem arz etmektedir (Brodin, 2019, s. 255). Burada dikkat edilmesi gereken bir husus; KOBİ'lere yönelik sınıflandırmanın ekonomik kriterlere dayanılarak yapıldığıdır. Diğer bir ifadeyle, KOBİ sınıflandırmasına dahil olan bir şirket, küçük bir işletme olsa dahi iş süreçleri kapsamında büyük ölçekte ilgili kişilerin düzenli ve sistematik bir biçimde izlenmesini ya da özel nitelikli kişisel verilerin işlenmesini gerektiren işleme faaliyetlerinde bulunabilecektir (Brodin, 2019, s. 246). Bu kapsamda, farklı sektörlerde faaliyette bulunan KOBİ'lerin her birinin kendine özgü uyum sorunları olabileceği hususunun göz önünde bulundurulması önem arz etmektedir.

Türk Hukuku Kapsamında KOBİ'lerin Uyum Sorunları

Türkiye'de kişisel verilerin korunması alanının görece yeni bir alan olması ve 6698 sayılı Kanun'un çerçeve bir düzenleme niteliği taşıması kapsamında uygulamada bazı sorunların ortaya çıkması sebebiyle KOBİ'lerin 6698 sayılı Kanun ve ikincil mevzuatına uyum hususunda zorluklar yaşadıkları bilinmektedir. Bu kapsamda, Türkiye'deki firmaların 6698 sayılı Kanun ve GVKT'ye uyumu hususundaki mevcut durumlarının analizi üzerine gerçekleştirilen bir çalışmada; bilişim, teknoloji, eğitim ve endüstri sektöründe çalışan katılımcılara yönelik bir anket düzenlenmiştir (Savaş, Zaim ve Aydın, 2020). Buna göre, bilgi güvenliğine yönelik eğitim seminer vb. faaliyetler düzenleyenlerin sayısı 24 olup, düzenlemeyenlerin sayısının ise 14 olduğu tespit edilmiştir. Yine ankete katılan 38 firmadan yalnızca 24'ünün Bilgi Güvenliği Yönetim Sistemine sahip olduğu ifade edilmekte olup firmaların 6698 sayılı Kanun ve GVKT kapsamında sorulan sorulara yanlış

cevaplar vermesi sebebiyle kişisel verilerin korunması alanı kavramlarına ilişkin bilgi düzeyinin yetersiz olduğu ifade edilmektedir (Savaş, Zaim ve Aydın, 2020, ss. 221-222).

Çalışmanın sonucunda, özellikle bilişim sektörünün konuya ilişkin farkındalığının daha yüksek olduğu tespit edilmekle birlikte genel olarak farkındalık seviyesinin düşük olduğu ve gerekli tedbirleri alan firmaların sayıca daha az olduklarının tespit edildiği belirtilmektedir. Bu kapsamda, Kişisel Verileri Koruma Kurumu ve ilgili diğer kurumların firmalara yönelik farkındalık çalışmalarını artırmaları, firmalara ait Bilgi Güvenliği Yönetim Sistemlerinin (BGYS) yetkili kurumlar tarafından belirli periyotlarla denetlenmesi ve denetlemenin yöntemine ilişkin çalışmaların gerçekleştirilmesi gerektiği ifade edilmektedir (Savaş, Zaim ve Aydın, 2020, s. 222).

Ayrıca, Sicile kayıt yükümlülüğünün, veri sorumlularının bünyelerinde gerçekleştirdikleri kişisel veri işleme faaliyetlerini analiz etmeleri ve bu işleme faaliyetlerini kişisel verilerin veri koruma mevzuatına uygun hale getirebilmeleri için önemli yükümlülüklerden ve aynı zamanda imkanlardan bir tanesi olduğu değerlendirilmektedir. Bu kapsamda, veri sorumlularının Kanun'a uyum sürecine ilişkin önemli bir gösterge teşkil eden Sicile kayıt yükümlülüğünün yerine getirilmesi hakkında ilk olarak 19.07.2018 tarihli ve 2018/88 sayılı Kurul kararıyla Sicile kayıt yükümlülüğü başlangıç tarihleri ve veri sorumluları için Sicile kayıt yaptırmaları gereken son tarihler belirlenmiş (Kişisel Verileri Koruma Kurumu, 2018) veri sorumlularının Sicile kayıt başvurularında karşılaşılan hatalı ve eksik girişler ve Covid-19 salgını gibi sebeplerle TOBB ve muhtelif sektör temsilcileri ile kamu kurumu ve kamu kurumu niteliğindeki meslek kuruluşlarından gelen talepler kapsamında Kurul tarafından birden fazla olmak üzere süre uzatım kararları verilmiştir (Kişisel Verileri Koruma Kurumu).
Kurum tarafından yayımlanan bilgilendirici rehberler, dokümanlar ve duyurular ile gerçekleştirilen çok sayıda farkındalık faaliyetlerine rağmen Kurumun özellikle süre uzatımı hakkında duyurularında olmak üzere Sicile ilişkin kamuoyu duyurularında ve süre uzatımlarına ilişkin internet sayfasında yayımlanan Kurul kararlarında yapılan tespitlerden veri sorumlularının Kanun ve ikincil mevzuatına uyum sürecinde yaşadığı zorluklara ilişkin çıkarımlar yapmak mümkündür (Kişisel Verileri Koruma Kurumu). Bu kapsamda, Kurulun 17.12.2019 tarihli ve 2019/387 sayılı kayıt süresinin uzatılmasına ilişkin kararında, Sicile kayıt yükümlülüğünün Kanun kapsamında getirilmiş bir yükümlülük olmakla beraber düzenlemeyle asıl hedeflenenin kişisel verilerin işlenmesinde şeffaflığın sağlanması, veri sorumlularının Kanun'a uyumu konusunda özen göstermeleri, kişisel veri işlenmesinin disiplin altına alınması, kişisel verisini işlediği kişilere hesap verebil-

mesi, kişisel verilerin gelişigüzel işlenmesinin önüne geçilmesi ve bu konuda bir kültür ve farkındalık oluşmasının sağlanması olduğu ifade edilmektedir. Kararda, bazı bildirimlerde işlendiği beyan edilen kişisel verilerle işleme amaçlarının, aktarım gerçekleştirildiği beyan edilen alıcı ve alıcı gruplarının, veri konusu kişi gruplarının, alınan teknik ve idari tedbirlerin, özel nitelikli kişisel veriler için alınması gereken yeterli önlemlerin, yurtdışına veri aktarımının ve saklamaya ilişkin beyan edilen sürelerin örtüşmediği ve bu konuda ciddi yanlışlıkların ve Kanun'a ve yönetmeliklere aykırılıkların olduğunun görüldüğü tespitine yer verilmektedir. Buna ilişkin olarak, veri sorumlularının bildirimlerini gelişigüzel değil hazırladıkları envanterlere dayanarak yapmaları gerektiği belirtilmektedir. Kararda ayrıca, sadece kayıt başvuru formunu iletip bildirimlerini tamamlamayan veri sorumlularının bulunduğu ifade edilerek Sicile kayıt yükümlülüğünün kayıt ve bildirimi kapsaması sebebiyle bildirimlerin tamamlanması gerektiği belirtilmektedir (Kişisel Verileri Koruma Kurumu, 2019).

Yine Kurumun 01.10.2020 tarihli kamuoyu duyurusunda kayıt yükümlülüğü bulunmakla birlikte VERBİS'e kayıt başvurusunda bulunmayan veya başvuruda bulunduğu halde bildirimini tamamlamayan veri sorumlularının olduğunun tespit edildiği belirtilmektedir (Sicile Kayıt Yükümlülüğü Hakkında Kamuoyu Duyurusu, 2020). Sicile kayıt yükümlülüğünün yerine getirilmesi için son tarih olan 31.12.2021 tarihinden sonra 04.01.2022 tarihinde yayımlanan kamuoyu duyurusunda ise VERBİS kayıt başvuru formunun sadece sisteme girilmesi veya Kuruma iletilmesinin yükümlülüğün yerine getirilmiş olduğu anlamına gelmediği hatırlatılarak bildirimlerini tamamlamayan veri sorumlularının bildirimlerini tamamlamaları gerektiği uyarısı yapılmıştır (Veri Sorumluları Siciline Kayıt Hakkında Kamuoyu Duyurusu, 2022). Son olarak 21.04.2022 tarihinde yayımlanan duyuruda Sicile kayıt ve bildirim yükümlülüğünü yerine getirmediği tespit edilen veri sorumluları hakkında Kanun'un 18'inci maddesi uyarınca idari yaptırım uygulanmasına başlandığı ifade edilmektedir (Kamuoyu Duyurusu (VERBİS), 2022).

Bu kapsamda, Kurul tarafından alınan süre uzatım kararları ve Kurum tarafından hazırlanan bilgilendirici dokümanlar ve gerçekleştirilen farkındalık faaliyetleri sonucunda veri sorumlularında uyum sürecine ilişkin farkındalık her geçen gün artmakla birlikte halen zorluklar yaşayanların bulunduğu değerlendirilmektedir (Kişisel Verileri Koruma Kurumu). Burada, veri sorumlularının uyum süreci açısından önemli bir yükümlülük ve fırsat olan Sicile kayıt yükümlülüğünün yerine getirilmiş olmasının da tek başına Kanun ve ikincil mevzuatına uyum anlamına gelmediğini belirtmek gerekmektedir. Veri sorumlularının Kanun ve ikincil mevzuat kapsamındaki diğer yükümlülüklerini de yerine getirmeleri uyum sürecinde önem arz eden bir husus olarak karşımıza çıkmaktadır.

BİR UYUM MEKANİZMASI OLARAK DAVRANIŞ KURALLARI

Davranış kuralları bir uyum mekanizması olarak OECD'nin 1980 tarihli Gizlilik İlkeleri'nin ulusal uygulamalara ilişkin dördüncü bölümünde yer alan 19'uncu paragrafta; üye ülkelerin belgede yer alan ilkeleri uygularken oluşturmaları tavsiye edilen yasal, idari veya diğer prosedürler ile kurumların arasında özellikle davranış kuralları veya başka biçimde öz düzenlemeyi teşvik eden mekanizmaları desteklemeleri yönündeki tavsiyesinde yer almaktadır (OECD, 1980). Ayrıca, 1981 yılında kabul edilen ülkemizin de imzacısı olduğu 108 sayılı Sözleşme'nin Açıklayıcı Raporu'nun "Tarafların Görevleri" başlıklı 4'üncü maddesinde tarafların iç hukuklarında düzenleyebilecekleri tedbirler arasında davranış kuralları da sayılmaktadır (Council of Europe, 1981).

Davranış kuralları Direktif'in 27'nci maddesinde ve GVKT'nin 40 ve 41'inci maddelerinde düzenlenmiş olup bir işletmenin veri işleme süreçlerinin ve belirli sektörlerdeki veri işleme faaliyetlerinin hukuka uygun bir biçimde gerçekleşmesi amacıyla oluşturulan kurallar olarak tanımlanmaktadır (Çekin, 2019, s. 178). 2009 yılında ICO'nun sponsorluğunda RAND Europe tarafından Direktif hakkında yayımlanan rapora göre ise davranış kuralları benzer türdeki kuruluşlar için ortak kuralları tanımlayan öz-düzenleyici araçlardır (Robinson, Graux, Botterman ve Valeri, 2009, s. xiii). Kamara'ya göre; hem veri sorumluları ve veri işleyenler hem de veri koruma otoriteleri için olmak üzere çift yönlü faydaya sahiptir. İlk olarak, birbirinden farklı işleme niteliklerine sahip olan sektörlerde faaliyette bulunan veri sorumlusu ve veri işleyenlerin yükümlülüklerini yerine getirmesi ve bunu gösterebilmesi için bir araç olan davranış kuralları söz konusu farklı sektörlere ilişkin risk düzeylerine göre veri sorumlusu veya veri işleyenlerin yükümlülüklerinin tespitini sağlayabilmektedir (Kamara, 2020, s. 718). Buna ek olarak, ICO tarafından da vurgulandığı üzere, küçük ve orta ölçekli işletmelerin özel ihtiyaçlarını da karşılayabileceği ifade edilmektedir (ICO, 2018). Davranış kuralları, veri koruma otoritelerine uyuma ilişkin düzenleyici denetleyici görevlerini yerine getirmelerinde yardımcı olmaktadır (Kamara, 2020, s. 718). Lachaud; Hustinx'in davranış kurallarının gerçekleştirdiği dört amacı tanımladığını belirtmekte olup bunların genel olarak; mevzuattan kaçınmak, mevzuatı öngörmek, uygulamak veya tamamlamak olduğunu ifade etmektedir. Bu kapsamda, davranış kurallarının KOBİ'ler tarafından uyumluluk süreçlerinde ücretsiz bir biçimde erişebilecekleri bir kılavuz olduğu belirtilmektedir (Aktaran: Lachaud, 2019). İrlanda Veri Koruma Otoritesi'nin 2001 yılında yayımladığı 13. yıllık raporunda da davranış kurallarının veri koruma hukukundaki çerçevenin yorumlanması ve uygulanması kapsamında ele alındığı görülmektedir (Data Protection Commission, 2001).

Bununla birlikte, Direktif döneminde; davranış kurallarının kullanımına yönelik eğilim ülkeden ülkeye değişmekle birlikte 2009 yılına gelindiğinde WP29 tarafından Avrupa seviyesinde geçerliliği bulunduğuna karar verilen davranış kuralları sadece iki tane olup bunlar Uluslararası Hava Taşımacılığı Birliği (IATA) ve Avrupa Doğrudan ve Etkileşimli Pazarlama Federasyonu (FEDMA) tarafından hazırlanan kurallardır (Robinson vd., 2009, s. 9). Bu kapsamda; Avrupa Komisyonunun Avrupa Parlamentosu, Avrupa Konseyi, Ekonomik ve Sosyal Komite ve Bölgeler Komitesini muhatap 2010 tarihli Tebliğ'inde ise Direktif döneminde öngörülen davranış kuralları mekanizmasının nadiren başvurulan ve özel sektördeki paydaşlar açısından yetersiz görülen bir araç olduğu tespit edilmektedir. İlgili tebliğde her ne kadar söz konusu tespite yer verilse de veri sorumluları tarafından alınacak öz-düzenleyici inisiyatiflerin veri koruma kurallarının uygulanmasına katkı sağlayacağı da ifade edilmektedir. Bu kapsamda, davranış kurallarının daha etkin bir biçimde kullanılmasını da içeren öz-düzenleyici inisiyatiflerin daha fazla teşvik edilmesinin araçlarının Komisyon tarafından inceleneceği belirtilmektedir (Aktaran: Kamara, 2020, s. 718).

Öte yandan, Direktif döneminde davranış kuralları mekanizmasının beklenen etkiyi yaratamamasının sebeplerinden bir tanesi veri koruma otoritelerinin sektörlerle birlikte iyi veri koruma uygulamalarını şekillendirmekten çok kendi kurallarını tek başına oluşturma eğilimi göstermesi iken diğer bir sebep ise hem veri koruma otoriteleri nezdinde hem genel olarak Avrupa seviyesinde davranış kurallarına ayrılan kaynakların yetersiz olmasıdır (Robinson vd., 2009, s. 37).

GVKT'nin etkin bir biçimde uygulanmasını temin etmek için geliştirilen veri koruma etki değerlendirmesi ve sertifikasyon mekanizmaları gibi davranış kuralları da GVKT'de Direktif'e nazaran daha detaylı bir biçimde düzenlenmektedir. GVKT ile birlikte getirilen yenilik olarak davranış kurallarının GVKT'de daha detaylı yer alması ve uygulamada daha etkin kullanılabilmesinin arkasında yatan asıl sebep kişisel verilerin korunmasında hesap verebilirlik ilkesinin kazandığı önemdir. Teknolojide yaşanan hızlı dönüşümün kişisel verilerin korunması konseptinde yarattığı değişiklik ihtiyacı neticesinde ilgili mevzuata uyum, uyumluluğun ispat edilmesi ve veri koruma otoritelerinin hızlı ve etkin denetim sağlayabilmesi hususlarının çözümünde hesap verebilirlik yaklaşımına ihtiyaç duyulmuştur (Kaya, 2020, ss. 1864-1865) Kaya'ya göre; hesap verebilirlik ilkesi uyum sürecinin ispatlanabilir olmasını da beraberinde getirmektedir. Bu yaklaşım, daha önceki bölümlerde de detaylı bir biçimde ele alınan yükümlülüklerin boyutu göz önünde bulundurulduğunda bazı mekanizmalara olan ihtiyacı ortaya koymuştur (Kaya, 2020, s. 1884).

Söz konusu mekanizmalardan bir tanesi de davranış kuralları mekanizması olup GVKT kapsamında davranış kuralları belirli sektörlerde ya da kendine özgü işleme faaliyetlerinde bulunan veri sorumlusu veya veri işleyenlere veri koruma hukukuna uyum ve hesap verebilirlik hususunda yardımcı olan gönüllülük esasına dayalı kurallar bütünüdür (Data Protection Commission). Çekin'e göre, GVKT'nin en önemli ilkelerinden olan hesap verebilirlik ilkesinin veri sorumlularına getirdiği uyumluluğu ispatlayabilme yükümlülüğü GVKT'nin çeşitli hükümleriyle düzenlenmiş olup davranış kuralları bu yükümlülükleri yerine getirmek bakımından kolaylık sağlayabilecek bir mekanizmadır (Aktaran: Çekin, 2019, s. 178).

Davranış kuralları ile getirilen bir diğer yenilik, Direktif'e göre davranış kuralları mekanizmasının hedeflediği grubun genişlemesidir. Direktif'in davranış kurallarını düzenleyen 27'nci maddesinde sadece veri sorumlularına işaret edilirken GVKT'nin 40 ve 41'inci maddelerinde veri sorumluları ile birlikte veri işleyenler de davranış kurallarına tabi olması muhtemel bir grup olarak öngörülmüştür. Bu yeni yaklaşımın sebepleri, GVKT'nin kurgusunda veri işleyenlere atfedilen rolün ve sorumluluğun artması ve veri işleyenlerin ekonomik öneminin ve rolünün yaşadığı değişimdir (Kamara, 2020, s. 721).

Genel Veri Koruma Tüzüğünde Davranış Kuralları

Davranış kuralları ve onaylanan davranış kurallarının izlenmesi GVKT'nin sırasıyla 40 ve 41'inci maddelerinde düzenlenmiş olup davranış kurallarını düzenleyen 40'ıncı maddede; üye devletlerin, veri koruma otoritelerinin, EDPB'nin ve Komisyonun, işleme faaliyetinde bulunan çeşitli sektörlerin spesifik özelliklerini ve mikro, küçük ve orta ölçekli işletmelerin belirli ihtiyaçlarını göz önünde bulundurarak GVKT'nin doğru bir biçimde uygulanmasına katkı sağlaması amaçlanan davranış kurallarının hazırlanmasını destekleyeceği hüküm altına alınmaktadır. Bunun yanı sıra, veri sorumlularını veya veri işleyenleri temsil eden birliklerin veya diğer kuruluşların adil ve şeffaf veri işleme faaliyeti, kişisel verilerin elde edilmesi, ilgili kişilerin haklarının kullanılması ve kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması gibi hususlara ilişkin olarak GVKT'nin uygulanmasını daha belirgin hale getirmek için davranış kuralları hazırlayabileceği ifade edilmektedir.

Maddede ayrıca, onaylanan ve genel geçerliliği bulunan davranış kurallarına GVKT'ye tabi olmayan üçüncü bir ülkedeki veri sorumluları veya veri işleyenlerin de bağlanabileceği belirtilmekte olup böyle bir senaryoda davranış kurallarının bir yurt dışına aktarım mekanizması olarak kullanılabileceği düzenlenmektedir.

Üçüncü bir ülkedeki veri sorumluları veya veri işleyenlerin davranış kurallarına bağlanırken bağlayıcı ve uygulanabilir taahhütlerini sözleşmesel veya diğer hukuken bağlayıcı araçlarla sunmalarının zorunlu olduğu belirtilmekte olup bunun ilgili kişilerin haklarını da içeren uygun güvencelerin uygulanması için gerekli olduğu hüküm altına alınmaktadır.

Maddede devamla, davranış kurallarının GVKT'nin 41'inci maddesinde düzenlenen kuralların hükümlerine veri sorumlusu veya veri işleyenlerin uyumunun zorunlu olarak bir yapı tarafından izlenmesine ilişkin hükümleri içermesi gerektiği düzenlenmekte ve söz konusu zorunlu izleme faaliyetinin veri koruma otoritesinin görev ve yetkilerine halel getirmeyeceği belirtilmektedir. Ayrıca, veri sorumlularını veya veri işleyenleri temsil eden birliklerin veya diğer kuruluşların hazırladıkları taslak kuralları, var olan kuralları üzerindeki değişiklik veya genişletmelerini yetkili veri koruma otoritesine ibraz edecekleri ve otoritenin ibraz edilen taslağın, değişikliğin veya genişletmenin GVKT'ye uygun olup olmadığı hakkında bir görüş sağlayacağı ve yeterli uygun güvenceleri sağladığını tespit etmesi halinde taslak kuralları, değişikliği veya genişletmeyi onaylayacağı hükmüne yer verilmektedir. Söz konusu kuralların birden çok üye devletteki işleme faaliyetlerine ilişkin olmaması halinde veri koruma otoritesinin bu kuralları tescil edeceği ve yayımlayacağı ifade edilmektedir.

Kuralların birden çok üye devletteki işleme faaliyetlerine ilişkin olması halinde ise; taslak kuralların, değişikliğin veya genişletmenin onaylanmasından önce yetkili veri koruma otoritesi tarafından GVKT'ye uyumluluğa veya yurtdışına aktarım mekanizması olarak kullanılması durumunda uygun güvenceleri sağladığına ilişkin görüşü alınmak üzere taslak kuralların, değişikliğin ya da genişletmenin EDPB'ye sunulacağı hükmüne yer verilmektedir. Bu görüşün; taslak kuralların, değişikliğin veya genişletmenin GVKT'ye uyumluluğunu veya uygun güvenceleri sağladığını kabul etmesi halinde uygulama tasarrufları yoluyla Birlik içerisinde genel geçerliliğe sahip olmasına karar verilmek üzere Komisyona sunulacağı hüküm altına alınmaktadır. Genel geçerliliğe sahip olduğuna karar verilen onaylanmış davranış kurallarının Komisyon tarafından uygun yollarla kamuoyuna açıklanacağı düzenlenmekte olup EDPB'nin ise onaylanan kuralların, değişikliklerin veya genişletmelerin tümünü bir sicilde toplayacağı ve uygun yollarla kamuya açıklayacağı hüküm altına alınmaktadır.

Çekin'e göre, davranış kuralları ve sertifikalar veri koruma otoriteleri ile iş birliği içerisinde öz denetim yöntemlerdir. GVKT, kişisel verilerin korunmasını tekil işlemler olarak değil veri sorumlusunun riskleri tespit ettiği ve buna göre yönetim ve organizasyon altyapısı oluşturduğu ve sürekli gözettiği bir husus olarak

görmektedir. Çekin tarafından, söz konusu proaktif öz düzenleme ve denetleme sürecinin küçük ve orta ölçekli işletme olan veri sorumluları tarafından yürütülmesinin yeterli personel ve maddi imkân kıtlığı sebebiyle gerçekleştirilmesinin her zaman mümkün olmadığı belirtilmektedir (Çekin, 2019, s. 177). Bu noktada, söz konusu veri sorumlularının kültürel ve ekonomik sermaye eksiklikleri ve faaliyette bulundukları alanda elde ettikleri yatkınlıkların yarattığı yeniliklere uyum sağlama hızındaki yavaşlığın yarattığı sorunlar, mevzuata uyum sağlayamamaları nedeniyle idari yaptırımlara maruz kalmaları hem de ortaya çıkabilecek veri ihlalleri sonucunda ürün veya hizmet sundukları ilgili kişiler nezdinde yaşayacakları itibar kaybı sebebiyle ekonomik kayıplara yol açabilecektir. Bu kapsamda, davranış kurallarının KOBİ'lere olumlu yansıması sadece hukuki değil ekonomik de olacaktır. Örneğin, davranış kurallarının varlığı veri sorumlularının maruz kalacağı idari para cezalarının belirlenmesi bağlamında dikkate alınmakta olup GVKT'nin 83'üncü maddesinde 40'ıncı madde uyarınca onaylanmış bir davranış kuralına tabi olmanın idari para cezasına karar verilirken göz önünde bulundurulacağı hususu hükme bağlanmaktadır.

Davranış kuralları veri sorumluları için uygulanması zorunlu bir mekanizma olmayıp gönüllü bir biçimde kullanılabilecek bir uyum aracıdır. Ancak bu durumun bir istisnası bulunmaktadır. Davranış kurallarının bir alandaki ya da meslekteki kayıtlı tüm üyeler için zorunlu hale getirilmesi halinde birliğe üye olanlar için davranış kurallarına tabi olmak zorunlu olabilecektir (Kamara, 2020, ss. 721-722). Bilindiği üzere, bazı meslekler açısından meslek kuruluşlarına üye olmak zorunludur. Bu durumda, meslek kuruluşları tarafından davranış kurallarına uyumun zorunlu kılınabileceği söylenebilecektir. GVKT'ye uyum sorununun çözümü, veri sorumluları veya veri işleyenleri ilgilendiren hususları ve bu hususlara yönelik çözümleri veya tavsiye edilen iyi uygulamaları içeren sektöre özgü ve/veya KOBİ'lere özgü kurallarla mümkün olabilecektir (Kamara, 2020, s. 721).

Küçük ve orta ölçekli işletmelerin, bulundukları sektörler birbirinden farklılık arz etmekte olup bu alanlarda geliştirdikleri kültürel sermayeleri GVKT'nin gerektirdiği bilgi birikimini sağlamayabileceği gibi ekonomik sermayelerinin yetersiz olması söz konusu bilgiye erişebilmek için uzman yardımı almalarını da engelleyebilecektir. Ayrıca, uzman yardımı olarak çeşitli hizmetleri alabilen KOBİ'lerin de uygulamada bazı sorunlarla karşılaştıkları bilinmektedir. KOBİ'lerin GVKT'ye uyumu hususunda Birleşik Krallık'ta yapılan araştırmada, kendilerini GVKT konusunda uzman olarak tanıtan kişilerin işletmelere verdikleri birkaç günlük küçük eğitimlerde yanlış tavsiyelerde bulunduğu belirtilmektedir. Çalışmaya katılan çok sayıda işletme temsilcisinin bu noktaya işaret ettiği ifade edilmekte olup söz konusu hususta en çok etkilenenlerin daha az kaynaklara sahip olan KOBİ'ler

olduğu vurgulanmaktadır (Sirus vd., 2018, s. 6). Davranış kuralları, GVKT'deki soyut hükümlerin, KOBİ'lerin yer aldığı sektörlerde kazandıkları yatkınlıklar sayesinde edindikleri sektöre özgü bilgi birikimine yakınlaşarak somutlaşması ve daha uygulanabilir hale gelmesine imkân tanımaktadır (Çekin, 2019, s. 178).

Davranış kurallarının hazırlanması ve ilgili denetleyici otoritelere sunulması hususunda meslek kuruluşları ve ticaret odaları gibi kuruluşlar yetkili kılınmış olup burada önemli olan ilgili kuruluşların veri sorumlularını ya da veri işleyenleri temsile yetkisinin bulunmasıdır. Bu kapsamda, tüketicilerin korunması ya da veri koruma hukuku alanında faaliyette bulunan dernekler gibi kuruluşların temsil yetkisini haiz olmamaları sebebiyle davranış kuralları hazırlaması mümkün olmamaktadır (Aktaran: Çekin, 2019, s. 179). GVKT'de temsil hususunun dışında, birliklerin üye sayısını dikkate alan niceliksel ya da birliğin faaliyetlerine ilişkin niteliksel bir kriter bulunmamaktadır (Kamara, 2020, s. 721).

Sunulan davranış kurallarının bir üye devletteki işleme faaliyetlerini ilgilendirdiği durumlarda yetkili veri koruma otoritesi, olumlu görüşe sahip olması halinde kuralları onaylayabilecektir. Kuralların birden çok üye devlette gerçekleşen işleme faaliyetlerini ilgilendirmesi halinde ise otorite; söz konusu taslak kuralları, değişiklikleri ya da genişletmeleri onaylamadan önce GVKT'ye uyumluluğu hakkında görüşünü almak üzere EDPB'ye sunar. Komisyon ise, onaylanan davranış kurallarının Birlik içerisinde genel geçerliliğe sahip olduğuna karar verme yetkisini haizdir (Handbook on European Data Protection Law, 2018).

Veri sorumluları ve veri işleyenlerin veri koruma mevzuatına uyumu hususunda davranış kuralları mekanizmasının önemini gösteren bir diğer husus, onaylanmış davranış kurallarına konu olan veri işleme süreçlerinin hukuka uygun sayılmasıdır. Diğer bir ifadeyle, veri sorumlusu veya veri işleyenin onaylanan davranış kuralları çerçevesinde işleme faaliyetinde bulunması halinde veri sorumlusu veya veri işleyene hukuka aykırı işleme faaliyetinde bulunduğu iddiası yöneltilememektedir. Onaylanmış davranış kurallarının, veri koruma otoritelerini bağlaması, detaylı hukuki ve teknik kavramları içeren kapsamlı bir düzenleme olan GVKT'ye uyum hususunda KOBİ'lere kolaylık sağlayabilecek bir unsurdur (Çekin, 2019, s. 180).

Korff'a göre; ulusal hukuklar ve Direktif rejimi altında davranış kurallarının onaylanması titiz bir değerlendirme ve sıklıkla çetrefilli bir sürecin sonunda gerçekleşmekteydi (Aktaran: Kamara, 2020, s. 722). Bu sorunun sebepleri olarak davranış kurallarının onaylanması dışında herhangi bir denetleme mekanizmasının yokluğu ve GVKT'de yer verilen hükümler kadar kapsamlı bir düzenlemenin

bulunmamasının altı çizilmektedir (Kamara, 2020, ss. 722-723). Bu kapsamda, Direktif döneminde onaylanan davranış kurallarının sayısının beklentiyi karşılamaması ve davranış kuralları mekanizmasının uyum için kullanışlı bir araç olmaması anlaşılabilen bir olgudur.

Kuralların onaylanıp işlerlik kazanmasından sonraki süreçte ise; akredite edilmiş kuruluşlar tarafından davranış kurallarına bağlı olan veri sorumluları ve veri işleyenlerin uyumluluğu izlenmektedir. Diğer bir ifadeyle, GVKT veri sorumlularının veya veri işleyenlerin davranış kurallarına uyumunu veri koruma otoriteleri ile birlikte akredite edilmiş kuruluşlar eliyle de denetleme imkânı sağlamaktadır (Çekin, 2019, s. 180). GVKT'de ayrıca, kurallara uyumluluğun kontrolü amacıyla işleme faaliyetinin sadece bir üye devlet ile ilgili olması halinde yetkili otoriteye onaylanan kuralların, değişikliklerin veya genişletmelerin kayıt altına alınması ve yayımlanması, genel geçerlilik kararı alınması halinde Komisyon'a karara konu onaylanan kuralların kamuya açık hale getirilmesi ve son olarak EDPB'ye onaylanan tüm davranış kurallarının, değişikliklerin veya genişletmelerin bir sicilde toplanması ve kamuya açık hale getirilmesi görevleri verilmektedir.

Onaylanan Davranış Kurallarının İzlenmesi

Onaylanan davranış kurallarının izlenmesini düzenleyen 41'inci maddede; yetkili veri koruma otoritesinin görev ve yetkilerine halel getirmeyecek şekilde, davranış kurallarına uyumluluğun izlenmesinin kuralların konusuna ilişkin uygun seviyede uzmanlığa sahip olan bir yapı tarafından gerçekleştirilebileceği hükmüne yer verilmektedir. Söz konusu yapının yetkili veri koruma otoritesi tarafından bu amaca özgü olmak üzere akredite edileceği belirtilmekte olup akreditasyona ilişkin olarak göz önünde bulundurulacak hususlar detaylı bir biçimde düzenlenmektedir.

Yetkili otoritenin, izleyici yapının akreditasyonuna ilişkin taslak gereklilikleri GVKT'nin 63'üncü maddesinde düzenlenen uyumluluk mekanizması uyarınca EDPB'ye sunacağı hüküm altına alınmaktadır. İzleyici yapıya, bir veri sorumlusu veya veri işleyen tarafından kuralların ihlal edilmesi halinde kurallara bağlı olmanın askıya alınması veya kuralların dışına çıkarılma da dahil olmak üzere uygun aksiyonu alma yetkisi verilmekte olup yapının söz konusu aksiyonlar ve bu aksiyonları alma sebepleri hakkında yetkili veri koruma otoritesini bilgilendirme yükümlülüğü bulunmaktadır. Maddede ayrıca, izleyici yapının akreditasyon gerekliliklerini sağlamaması veya yapı tarafından alınan aksiyonların GVKT'yi ihlal etmesi halinde yetkili veri koruma otoritesi tarafından akreditasyonun iptal edileceği hükmü düzenlenmektedir. Onaylanan davranış kurallarının izlenmesini düzenleyen 41'inci madde kamu kurum ve kuruluşları tarafından yürütülen

işleme faaliyetlerine uygulanmamaktadır.

Görüldüğü üzere, GVKT, veri sorumlusu ve veri işleyenlerin davranış kurallarına uyumunun izlenmesine ilişkin olarak veri koruma otoritelerinin yanında akredite kuruluşları da sürece dahil etmektedir. Bu kapsamda, Çekin'e göre ilgili veri sorumluları veya veri işleyenler de bu akredite kuruluşların izleme faaliyetlerine açıkça rıza göstermek zorundadır (Çekin, 2019, s. 180).

GVKT'de ayrı bir madde olarak hüküm altına alınan onaylanan davranış kurallarının izlenmesi hususunda; söz konusu kuralları izleyecek yapıların taşıması gereken özellikler düzenlenmekte olup buna göre kuruluşların tarafsızlıklarını ve bağımsızlıklarını gösterebilmeleri gerekmektedir. Bunun yanı sıra, kişisel verilerin korunmasına ve sektöre ilişkin uzmanlıklarının bulunması önem arz etmekte olup GVKT'de düzenlenen izlemeye ilişkin farklı görevleri yürütebilecek kapasitelerinin bulunduğunu da gösterebilmeleri zorunlu bir unsurdur (Aktaran: Lachaud, 2019, ss. 5-6). Fransa Veri Koruma Otoritesi (CNIL) tarafından 22 Şubat 2022 tarihinde yayımlanan bilgilendirici dokümanda ise, izleyici yapıların akredite edilebilmesi için kural ihlalleri veya kurallara bağlı olanlar tarafından kuralların uygulanma biçimi hakkında şeffaf şikâyet yönetimi prosedürlerine sahip olmaları gerektiği belirtilmektedir. Buna göre izleyici yapının davranış kuralları kapsamında kararları ve yaptırımları almaya yönelik prosedürlerinin de hazır bulunduğunu gösterebilmesinin önemi vurgulanmaktadır (CNIL, 2022).

GVKT'nin 41'inci maddesinin ikinci fıkrasının (c) bendinde; veri sorumluları veya veri işleyenler tarafından kuralların ihlal edilmesi halinde ilgili kişilerin başvurabileceği şikâyet mekanizmasının belirlenmesi ve bunun ilgili kişilere ve kamuoyuna açıklanması hususu düzenlenmektedir. EDPB tarafından verilen örnekte, söz konusu mekanizmanın şikayetleri almak, değerlendirmek, takip etmek, kaydetmek ve çözüme bağlamak üzere oluşturulan bir süreci içerebileceği belirtilmektedir. Bu sürecin, ilgili kişilerin şikâyet sürecini anlayabileceği ve takip edebileceği kamuya açık bir rehberde somutlaştırılabileceği ifade edilmekte olup sürecin bağımsız bir şekilde yürütülmesi için izleyici yapı nezdinde ayrı bir operasyonel ekibin ve yönetim fonksiyonlarının oluşturulabileceği ifade edilmektedir (EDPB, 2019).

GVKT'ye göre; izleyici yapıların akreditasyonuna ilişkin taslak gereklilikler veri koruma otoritesi tarafından belirlenmekte olup GVKT'nin 63'üncü maddesinde yer alan uyumluluk mekanizması uyarınca EDPB'ye sunulmaktadır. Yetkili veri koruma otoritesi, izleyici yapının gereklilikleri karşılamaması veya GVKT'yi ihlal eden aksiyonlar alması halinde akreditasyonu iptal etmektedir. Maddede, verilen

akreditasyonun geçerlilik süresine ilişkin bir hüküm bulunmamaktadır. Bununla birlikte, CNIL tarafından yayımlanan dokümanda, verilen akreditasyonun geçerlilik süresinin 5 yıl olduğu ifade edilmektedir (CNIL, 2022).

GVKT'nin 43'üncü maddesinde düzenlenen sertifikasyon kuruluşlarının akreditasyon süreçlerinden farklı olarak izleyici yapıların akreditasyonu ulusal akreditasyon kuruluşları dahil olmaksızın yalnızca veri koruma otoriteleri tarafından yapılmaktadır. Kamara'ya göre; 765/2008 sayılı Tüzük'te ulusal akreditasyon kuruluşlarının uyumluluk değerlendirme kuruluşlarını (sertifikasyon kuruluşlarını) akredite edeceğinin hüküm altına alınması sebebiyle davranış kurallarını izleyecek yapının ulusal akreditasyon kuruluşu tarafından akredite edilmesinin sonucunda sadece uyumluluk değerlendirme kuruluşlarının izleyici yapı olabilmesi gündeme gelebileceğinden böyle bir ayrıma gidilmektedir (Kamara, 2020, s. 729).

GVKT'nin davranış kurallarının izlenmesini düzenleyen 41'inci maddesinde; kuralların bir veri sorumlusu veya veri işleyen tarafından ihlal edilmesi durumunda izleyici yapının veri sorumlusu veya veri işleyenlerin kurallardan askıya alınması veya çıkarılması da dahil olmak üzere uygun aksiyonları alabileceği hüküm altına alınmaktadır. İlgili maddede, söz konusu aksiyonların alınması hususunun yetkili veri koruma otoritesinin görev ve yetkileri ile GVKT'nin 8'inci bölümüne halel getirmeyeceği ifadesine yer verilmektedir. Hollanda Veri Koruma Otoritesi tarafından 10 Mart 2021 tarihinde yayımlanan bilgilendirici dokümanda, üyeliğin askıya alınmasının ve üyelikten çıkarmanın sadece ciddi durumlarda uygulanabileceği belirtilmekte olup izleyici yapı tarafından otoriteye sağlanması gereken bilgiler arasında üyeliğin askıya alınması ve üyelikten çıkarma hususu da sayılmaktadır (NL accreditation requirements for GDPR, 2021).

Bu kapsamda, GVKT'nin yürürlüğe girmesinden itibaren uyum hususunda ve bir aktarım mekanizması olarak detaylı bir biçimde düzenleme altına alınan davranış kuralları oluşturulmaya başlanmış olup bazı kurallar onaylanmış ve yürürlük kazanmıştır. Bunlardan ikisi olan Belçika Veri Koruma Otoritesi ve Fransız Veri Koruma Otoritesi (CNIL) tarafından onaylanan davranış kurallarıdır. Söz konusu kurallara ilişkin taslak kararlar GVKT'nin 40'ıncı maddesinin 7'nci fıkrası uyarınca birden çok üye devlette gerçekleştirilen işleme faaliyetini ilgilendirdiği için görüşünün alınmasını teminen EDPB'ye sunulmuş ve EDPB ise bu kurallara ilişkin görüşlerini 19 Mayıs 2021 tarihinde yayımlamıştır (EDPB, 2021). Belçika Veri Koruma Otoritesi tarafından onaylanan davranış kuralları, GVKT'nin yürürlüğe girmesinden itibaren kabul edilen ilk ulusötesi davranış kuralları olma niteliğini taşımaktadır (The BE DPA approves its first European code of conduct,

2021). Yine, yakın dönemde İspanya Veri Koruma Otoritesi tarafından klinik araştırma ve farmakovijilans sektöründe kişisel veri işleme faaliyetinde bulunan veri sorumluları veya veri işleyenlerin GVKT'ye uyumuna yönelik davranış kuralları onaylanmıştır (Spanish Data Protection Authority approves the first industry code of conduct, 2022).

SONUÇ

Dünyada ve Türkiye'de ekonominin ana omurgasını teşkil ettiği kabul edilen küçük ve orta ölçekli işletmelerin veri koruma hukuku kapsamında veri sorumlusu veya veri işleyen olarak belirli yükümlülükleri yerine getirmesi gerekmektedir. Bununla birlikte KOBİ'lerin faaliyette bulundukları alanlar çok çeşitlidir ve bu alanlarda faaliyet göstermek KOBİ'ler için alana özgü farklı sermaye türlerinin kombinasyonunu oluşturmayı gerektirmektedir. Söz konusu alanlarda; sahip oldukları sermayelerle faaliyette bulunan KOBİ'lerin zaman içerisinde bilinçdışı bir biçimde oluşturdukları yatkınlıklar bir yandan süreklilik arz eden işlerinde alana özgü oyunu kurallarına uygun bir biçimde oynayabilmelerini sağlamakla birlikte yeni hukuki düzenlemeler de dahil olmak üzere meydana gelen yeniliklere uyum sağlayabilmelerinde sorunlara yol açmaktadır.

Yeniliklere uyum sağlamalarını zorlaştıran bir diğer husus ise uyum için gerekli olan sermaye türüne sahip olmamalarıdır. Örneğin teknolojide meydana gelen bir değişikliğe uyum sağlayabilmek için ekonomik sermaye gerektiği kadar söz konusu teknolojik gelişmeye ilişkin bilgi anlamına gelen kültürel sermayenin de bulunması gerekmektedir.

Bu kapsamda, veri koruma hukukuna uyumluluk gösterilmesi sadece yükümlülüklerin yerine getirilmesi dolayısıyla olası hukuki sonuçlardan bağışıklık kazanmak anlamına gelmemekte olup aynı zamanda KOBİ'lerin mal veya hizmet sunumunda bulundukları ilgili kişilerin güvenini kazanmaları anlamında rekabet gücünü artırarak ekonomik avantajlar da sağlamaktadır. Ancak, gerek KOBİ'lerin faaliyette bulundukları alanda edindikleri yatkınlıklar sebebiyle gerekse ekonomik ve kültürel sermaye yetersizlikleri sebebiyle veri koruma hukukuna uyum sağlama hususunda sorunlar yaşadığı görülmektedir.

Avrupa'da veri koruma hukukuna ilişkin düzenlemelerin tarihi görece daha eski tarihlere dayanmakla birlikte teknolojide yaşanan hızlı gelişmelere cevap verebilme ihtiyacıyla yeni hukuki düzenlemelere gidildiği bilinmektedir. Uzun yıllardır gündemde olan bir konu olmasına rağmen yapılan çalışmalarda Avrupa'daki KOBİ'lerin devam eden bir uyum sorunu olduğu görülmektedir. Türkiye'de görece yeni bir alan olarak karşımıza çıkan veri koruma hukukuna yönelik farkındalık her geçen gün artmakla birlikte Türkiye'de KOBİ'lerin uyum sağlamaları için alanın kendine özgü nitelikleri kapsamında hukuki ve teknik bilgiye sahip olmamaları, bu bilgiye sahip çalışanlarının bulunmaması ya da dışarıdan uzman desteği alabilmek için yeterli ekonomik sermayelerinin bulunmaması gibi sebeplerle sorunlar yaşadıkları görülmektedir. Ülkemizde KOBİ'lere yönelik gün-

cel tanımlamalar göz önünde bulundurulduğunda birbirinden farklı sektörlerde çok farklılık gösteren ekonomik güçlere sahip olan söz konusu işletmelerin her birinin karşılaştığı uyum sorunlarının niteliğinin kendine özgü olacağı değerlendirilmektedir.

Belirli sektörlerin ve mikro, küçük ve orta ölçekli işletmelerin kendine özgü niteliklerine uygun bir biçimde etkin ve verimli bir biçimde kişisel veri koruma hukukuna uyum sorunlarını çözebilmeleri amacıyla 1980 tarihli OECD Gizlilik İlkelerinde, 108 sayılı Sözleşmenin Açıklayıcı Raporunda, 95/46/EC sayılı Direktif'te ve Genel Veri Koruma Tüzüğü'nde davranış kuralları mekanizması düzenlenmiştir. Direktif döneminde davranış kurallarının uygulamada etkin bir biçimde kullanılamamasının da etkisiyle GVKT'de mekanizmanın etkin bir biçimde kullanılmasını temin etmek amacıyla daha kapsamlı bir düzenlemeye yer verilmiş olup aynı zamanda davranış kuralları bir aktarım mekanizması olarak da düzenleme altına alınmıştır. GVKT'nin temel mantığını yansıtan hesap verebilirlik yaklaşımıyla sorumluluğun veri koruma otoriteleriyle birlikte veri sorumlusu veya veri işleyenlere de yüklendiği bir durumda davranış kuralları sertifikasyon gibi bir öz-düzenleme mekanizması olarak daha da önemli hale gelmektedir.

Türk hukukunda davranış kurallarına ilişkin bir düzenleme bulunmamakla birlikte Türkiye ekonomisinde KOBİ'lerin önemi, Türkiye'de mesleki teşkilatlanmanın Anadolu'daki ahi teşkilatına kadar uzanan tarihsel kökleri (Oğurlu, 2017) ve Cumhuriyet döneminde ticaret ve sanayi odaları ile meslek kuruluşlarının ve sektörel sivil toplum kuruluşlarının yaygın bir biçimde teşkilatlanması ve KOBİ'lerin faaliyette bulundukları alanlara ilişkin meslek kuruluşlarına üye olmalarının ilgili mevzuat gereği zorunlu olması gibi sebeplerle davranış kuralları mekanizmasının Türkiye'de veri koruma hukukunun etkin bir biçimde uygulanmasına önemli derecede katkı sağlayabileceği ve KOBİ'lerin uyum sorununun çözülmesinde faydalı olabileceği değerlendirilmektedir. Diğer bir ifadeyle, söz konusu meslek kuruluşlarının KOBİ'lerin ekonomik, kültürel ve sosyal sermaye yetersizliklerini giderebileceği düşünülmektedir. Bu kapsamda, 11. Kalkınma Planı (Strateji ve Bütçe Başkanlığı, 2019), Yargı Reformu Strateji Belgesi (Adalet Bakanlığı, 2019) ve İnsan Hakları Eylem Planı (Adalet Bakanlığı, 2021) çerçevesinde kişisel veri koruma mevzuatının GVKT ile uyumlulaştırılması çalışmaları kapsamında davranış kuralları mekanizmasının GVKT'deki gibi kapsamlı bir biçimde düzenlenmesinin uygun olacağı düşünülmektedir.

GVKT'ye uygun bir biçimde kapsamlı bir düzenlemenin yapılmasının KOBİ'lerin kişisel veri koruma hukukuna uyum sorununun çözülmesinin yanında 6698 sayılı Kanun'un yurt dışına veri aktarımını düzenleyen 9'uncu maddesinin

uygulanmasına ilişkin birtakım zorlukların giderilmesine de yeni bir aktarım mekanizması olarak katkı sağlayacağı açıktır. Zira mevcut durumda 6698 sayılı Kanun kapsamında kişisel veriler yurt dışına ancak ilgili kişilerin açık rızasının bulunması, Türkiye'deki veri sorumlusu ile yurt dışında yerleşik veri sorumlusu ya da veri işleyen arasında bir taahhütnamenin bulunması veya bağlayıcı şirket kurallarının bulunmasıyla aktarılabilmektedir. Kurul tarafından yeterli düzeyde koruma düzeyini temin eden ülkeler ise henüz ilan edilmemiştir.

Bu kapsamda,davranış kurallarının veri koruma hukukuna uyum sorunlarının çözülmesine etkin bir biçimde katkı sağlaması ihtiyacı ve GVKT'ye uyumlu bir biçimde bir aktarım mekanizması olarak da öngörülmesi gerekliliği göz önünde bulundurulduğunda davranış kurallarına ilişkin düzenlemenin bir Kanun değişikliği gerektirdiği değerlendirilmektedir. Söz konusu düzenleme hazırlanırken dikkat edilmesi gereken bir husus yapılacak Kanun değişikliğinin Türk hukukundaki diğer düzenlemelerle çatışmamasının temin edilmesidir. Burada göz önünde bulundurulması gereken hususlardan bir tanesi; kamu hukukuna tabi, kamu kurumu niteliğindeki odaların veya meslek kuruluşlarının davranış kurallarını hazırlama yetkisi hususunun doktrinde tartışmalı olduğudur (Çekin, 2020, s. 236). Yine, davranış kurallarının Avrupa Birliği hukukundaki uygulamasına göre, kuralların ayrılmaz bir parçası olan izleyici yapıların akredite edilmesinde sertifikasyon kuruluşlarının akredite edilmesinden farklı olarak akreditasyon yetkisi ulusal akreditasyon kuruluşlarına değil veri koruma otoritelerinin söz konusu akreditasyonu tek başlarına gerçekleştirmelerinin beklenmesinin aşırı iyimser bir yaklaşım olduğunu belirten görüşler bulunmakla birlikte yetkili veri koruma otoritelerine verilmiştir (Lachaud, 2019, s. 18). Türk hukukunda ise 4457 sayılı Türk Akreditasyon Kurumu Kuruluş ve Görevleri Hakkında Kanun'un 22'inci maddesi uyarınca Türkiye'de uygunluk değerlendirme faaliyetlerini akredite etmek üzere yetkili tek kurum Türk Akreditasyon Kurumu'dur (Türk Akreditasyon Kurumu Kuruluş ve Görevleri, 1999). Bu kapsamda, GVKT'ye uyum hususunun tek başına 6698 sayılı Kanun ve ikincil düzenlemelerinde yapılacak değişikliklerle sağlanamayacağı değerlendirilmekte olup Türk hukukundaki ilgili diğer düzenlemelerde de ihtiyaç duyulan değişikliklerin yapılması gerektiği düşünülmektedir. ◆

KAYNAKÇA

- Article 29 Working Party. (2010). Opinion 3/2010 on the principle of accountability. Erişim adresi: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf, 09.05.2022.
- Article 29 Working Party (2009). The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Erişim adresi: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf, 09.05.2022.
- Autorité De Protection Des Données (2021). The BE DPA approves its first European code of conduct. Erişim adresi: https://www.dataprotectionauthority.be/citizen/the-be-dpa-approves-its-first-european-code-of-conduct, 09.05.2022.
- Autoriteit Persoonsgegevens (2021). NL accreditation requirements for GDPR code of conduct monitoring bodies, Autoriteit Persoonsgegevens. Erişim adresi: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/nl_accreditation_requirements_for_gdpr_code_of_conduct_monitoring_bodies.pdf, 09.05.2022.
- BOURDIEU, P. (2018). Bir Pratik Teorisi İçin Taslak: Kabiliye Üzerine Üç Etnoloji Çalışması, Çeviren: Nazlı Ökten, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.
- BOURDIEU, P. (2005). The Social Structures of the Economy, Çeviren: Chris Turner, Polity Press, Cambridge: UK.
- BRODIN, M. (2019). A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. *European Journal for Security Research (2019) 4:243–264.* Erişim adresi: https://link.springer.com/content/pdf/10.1007/s41125-019-00042-z.pdf. 04.05.2022.
- CNIL. (2022). The monitoring body designated by the code of conduct. Erişim adresi: https://www.cnil.fr/en/monitoring-body-designated-code-conduct, 09.05.2022.

- Council Of Europe. (1981). Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Erişim adresi: https://rm.coe.int/16800ca434, 09.05.2022.
- Council Of Europe. (2018). Handbook on European Data Protection Law 2018 edition. Erişim adresi: https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf, 09.05.2022.
- ÇATAL, M. F. (2007). Bölgesel Kalkınmada Küçük ve Orta Boy İşletmelerin (KOBİ) Rolü. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi (2007) Cilt 10 Sayı: 2, 333 -352.* Erişim adresi: https://dergipark.org.tr/tr/download/article-file/32070. 09.05.2022.
- ÇEKİN, M. S. (2019). Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku (2.Baskı). On İki Levha Yayıncılık, İstanbul, 2019.
- ÇEKİN, M. S. (2020). Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku (3. Baskı). On İki Levha Yayıncılık, İstanbul.
- Data Protection Commission. Codes of conduct. Erişim adresi: https://www.dataprotection.ie/en/organisations/codes-conduct#:~:text=What%20are%20Codes%20of%20Conduct,relating%20to%20particular%20processing%20operations., 09.05.2022.
- Data Protection Commission. (2001). Thirteenth Annual Report of the Data Protection Commissioner. Erişim adresi: https://www.dataprotection.ie/sites/default/files/uploads/2018-12/annual_report_2001.pdf, 09.05.2022.
- EDPB. (2019). Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679. Erişim adresi: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf, 09.05.2022.
- EDPB. (2021). Our documents. Erişim adresi: https://edpb.europa.eu/our-work-tools/documents/our-documents_en?f%5B0%5D=all_topics%3A125, 09.05.2022.

◊ European Commission. (2015). User Guide to the SME Definition. Erişim adresi: https://ec.europa.eu/regional_policy/sources/conferences/state-aid/sme/smedefinitionguide_en.pdf, 09.05.2022.

◊ Eur-Lex. (2003). Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. Erişim adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32003H0361, 09.05.2022.

◊ FREITAS, M. C., SILVA, M. M. (2018). GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management, 2018, 3(4), 30.* Erişim adresi: https://www.jisem-journal.com/download/gdpr-compliance-in-smes-there-is-much-to-be-done-3941.pdf. 09.05.2022.

◊ Global Compliance News. (2022). Spain: Spanish Data Protection Authority approves the first industry code of conduct to enable compliance of clinical research and pharmacovigilance with the GDPR. Erişim adresi: https://www.globalcompliancenews.com/2022/03/10/spain-spanish-data-protection-authority-approves-the-first-industry-code-of-conduct-to-enable-compliance-of-clinical-research-and-pharmacovigilance-with-the-gdpr/, 09.05.2022..

◊ JOURDAIN, A., NAULIN, S. (2016). Pierre Bourdieu'nun Kuramı ve Sosyolojik Kullanımları, Çeviren: Öykü Elitez, İletişim Yayınları, İstanbul.

◊ KAMARA, I. (2020). Codes of conduct and certification. The EU General Data Protection Regulation (GDPR) A Commentary. Derleyenler: Christopher Kuner, Lee A. Bygrave ve Christopher Docksey, Oxford University Press, Oxford: UK.

◊ KAYA, M. B. (2020). Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi. *İstanbul Hukuk Mecmuası Cilt: 78 Sayı: 4, 1859 – 1897.* Erişim adresi: https://dergipark.org.tr/tr/pub/ihm/issue/60298/879251. 09.05.2022.

◊ Kişisel Verileri Koruma Kurumu https://www.kvkk.gov.tr/, 13.05.2022.

◊ Kişisel Verileri Koruma Kurumu. (2022). Kamuoyu Duyurusu (VERBİS). Erişim adresi: https://www.kvkk.gov.tr/Icerik/7250/Kamuoyu-Duyurusu-VERBIS-, 13.05.2022.

◊ Kişisel Verileri Koruma Kurumu. (2020). SİCİLE KAYIT YÜKÜMLÜLÜĞÜ HAKKINDA KAMUOYU DUYURUSU. Erişim adresi: https://www.kvkk.gov.tr/Icerik/6819/SICILE-KAYIT-YUKUMLULUGU-HAKKINDA-KAMUOYU-DUYURUSU, 13.05.2022.

◊ Kişisel Verileri Koruma Kurumu. (2018). Sicile Kayıt Yükümlülüğünün Başlama Tarihleri ile ilgili Kişisel Verileri Koruma Kurulunun 19/07/2018 Tarihli ve 2018/88 Sayılı Kararı. Erişim adresi: https://www.kvkk.gov.tr/Icerik/5272/2018-88, 13.05.2022.

◊ Kişisel Verileri Koruma Kurumu. (2022). Veri Sorumluları Siciline Kayıt Hakkında Kamuoyu Duyurusu. Erişim adresi: https://www.kvkk.gov.tr/Icerik/7156/Veri-Sorumlulari-Siciline-Kayit-Hakkinda-Kamuoyu-Duyurusu, 13.05.2022.

◊ Kişisel Verileri Koruma Kurumu. (2019). Veri Sorumluları Siciline Kayıt Yükümlülüğüne İlişkin Kurulca Belirlenen Sürelerin Uzatılması ile ilgili Kişisel Verileri Koruma Kurulunun 17/12/2019 Tarihli ve 2019/387 Sayılı Kararı. Erişim adresi: https://www.kvkk.gov.tr/Icerik/6749/2019-387, 13.05.2022.

◊ LAMBERT, P. (2017). Understanding the New European Data Protection Rules, CRC Press, Boca Raton: Florida.

◊ MECEK, G. (2020). Küçük ve Orta Büyüklükteki İşletmelerin (KOBİ) Uluslararası Tanımlama Ölçütleri ve Kavramlaştırılması. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi (JEBPIR) 2020, 6(1), 29-55.* Erişim adresi: https://dergipark.org.tr/tr/download/article-file/1166793, 09.05.2022.

◊ OECD. (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Erişim adresi: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, 09.05.2022.

◊ OĞURLU, Y. (2017). Tarihi 'Ahi Birlikleri'nden Çağdaş 'Kamu Kurumu' Niteliğindeki Meslek Kuruluşları'na İzdüşümler: Mesleki Dayanışma, Disiplin ve İdari Yaptırımlar. Erişim adresi:https://www.researchgate.net/publication/345242941_TARIHI_AHI_BIRLIKLERI_NDEN_CAGDAS_KAMU_KURUMU_NITELIGINDEKI_MESLEK_KURULUSLARI'NA_IZDUSUMLER_MESLEKI_DAYANISMA_DISIPLIN_VE_IDARI_YAPTIRIMLAR_PROJECTIONS_FROM_HISTORICAL_AHI_ASSOCIATIONS_TO_CONTEMPORAR. 09.05.2022

◊ Researchlive. (2020). DMA Survey Highlights Gaps in SME GDPR Knowledge and Compliance. Erişim adresi: https://www.research-live.com/article/news/dma-survey-highlights-gaps-in-sme-gdpr-knowledge-and-compliance/id/5065862, 06.05.2022.

◊ Resmî Gazete. (2005). Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri ve Sınıflandırılması Hakkında Yönetmelik. Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2005/11/20051118-5.htm, 09.05.2022.

◊ Resmî Gazete. (2023). Küçük ve Orta Büyüklükteki İşletmeler Yönetmeliği. Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2023/05/20230525-6.pdf, 07.11.2023.

◊ Resmî Gazete. (2005). Sanayi ve Ticaret Bakanlığının Teşkilât ve Görevleri Hakkında Kanuna Bir Ek Madde Eklenmesine İlişkin Kanun. Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2005/04/20050416-1.htm, 09.05.2022.

◊ ROBINSON, N., GRAUX, H., BOTTERMAN, M., VALERI, L. (2009). Review of the European Data Protection Directive. Rand Corporation, Cambridge: UK.

◊ SIRUR, S., NURSE, J. R.C., WEBB, H. (2018). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). Erişim adresi: https://arxiv.org/pdf/1808.07338.pdf. 09.05.2022.

◊ SAVAŞ, R. N., ZAİM, A. H., AYDIN, M. A. (2020). KVKK ve GDPR Kapsamında Firmaların Mevcut Durum Analizi Üzerine Bir İnceleme. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 19(38), Güz 2020, 208-223.* Erişim adresi: https://dergipark.org.tr/tr/download/article-file/1469528. 09.05.2022.

◊ SWARTZ, D. (2015). Kültür ve İktidar: Pierre Bourdieu'nun Sosyolojisi. Çeviren: Elçin Gen, İletişim Yayınları, İstanbul.

◊ T.C. Adalet Bakanlığı. (2021). İnsan Hakları Eylem Planı ve Uygulama Takvimi. Erişim adresi: https://insanhaklarieylemplani.adalet.gov.tr/resimler/%C4%B0nsan_Haklar%C4%B1_Eylem_Plan%C4%B1_ve_Uygulama_Takvimi.pdf, 11.05.2022.

◊ T.C. Adalet Bakanlığı. (2019). Yargı Reformu Stratejisi. Erişim adresi: https://sgb.adalet.gov.tr/Resimler/SayfaDokuman/23122019162931YRS_TR.pdf, 11.05.2022.

◊ T.C. Cumhurbaşkanlığı Mevzuat Bilgi Sistemi. 6698 sayılı Kişisel Verilerin Korunması Kanunu. Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf, 09.05.2022.

◊ T.C. Cumhurbaşkanlığı Mevzuat Bilgi Sistemi. Türk Akreditasyon Kurumu Kuruluş ve Görevleri Hakkında Kanun. Erişim adresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4457&MevzuatTur=1&MevzuatTertip=5, 11.05.2022.

◊ T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2019). On Birinci Kalkınma Planı (2019-2023. Erişim adresi: https://www.sbb.gov.tr/wp-content/uploads/2019/07/OnbirinciKalkinmaPlani.pdf, 11.05.2022.

◊ VINCENT, D. (2017). Mahremiyet: Kısa Bir Tarih. Çeviren: Deniz Cumhur Başaraner, Epos Yayınları, Ankara.

◊ WACHTER, S. (2017). Privacy: Primus Inter Pares - Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights. Erişim adresi: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514, 09.05.2022.

AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜNDE HESAP VERİLEBİLİRLİK ARAÇLARI

Atakan YALÇIN

Kişisel Verileri Koruma Uzmanı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "Veri Koruma Hukukunda Şeffaflık ve Hesap Verilebilirlik Yükümlülüğü" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Kişisel Verilerin İşlenmesine Dair Bireylerin Korunması Hakkındaki Çalışma Grubu'nun (Madde 29 Çalışma Grubu), 95/46/EC sayılı Direktifin yürürlükte olduğu 2010 tarihinde yayımlanan 3/2010 sayılı görüşünde; somut önlem ve uygulamalar ekseninde Avrupa Birliği veri koruma hukukuna hâkim ilke ve yükümlülüklerin çoğu zaman yetersiz derecede yansıtıldığı ifade edilmektedir. Madde 29 Çalışma Grubu tarafından hazırlanan "Mahremiyetin Geleceği" başlıklı raporda da benzer şekilde mevcut yasal çerçevenin veri koruma alanında öngörülen gerekliliklerin gerçek bir veri korumanın sağlanmasını temin edecek etkin mekanizmalara dönüşme noktasında tam bir başarı gösteremediği ifade edilmiş ve bu hususta gerekli ilerlemenin, merkezine hesap verilebilirliği alan mekanizmalar aracılığıyla gerçekleşebileceği savunulmuştur. Bu çerçevede revize edilmiş veri koruma direktifinde hesap verilebilirlik ilkesine yer verilmesi hususuna yönelik özel bir vurgu yapılarak bu ilkenin veri sorumlusunun oynadığı rolü güçlendireceği ve sorumluluklarını artıracağı ifade edilmiştir. Yasaya dayanan bir hesap verilebilirlik ilkesi, veri sorumlularının Direktifte yer alan ilke ve yükümlüklerin hayata geçirilmesini teminen, uygun ve etkin önlemlerin alınmasını ve talep edilmesi hâlinde bu hususun ispatlanabilir olmasını açık bir biçimde şart koşacaktır

(Madde 29 Çalışma Grubu, 2010). Nitekim günümüzde Avrupa Birliği hukukunda yürürlükte bulunan Avrupa Birliği Genel Veri Koruma Tüzüğünde, 95/46/EC sayılı Direktifin aksine hesap verilebilirlik ilkesine açıkça yer verildiği göz önünde bulundurulduğunda, Madde 29 Çalışma Grubunun yukarıda yer verilen görüş ve raporu ile bu duruma zemin hazırladığını belirtmek mümkündür (Kaya, 2020).

Madde 29 Çalışma Grubu, veri sorumlularının veri korumanın gerçek anlamda sağlanmasını teminen etkin önlemler almalarını gerekli kılan birden çok gerekçenin mevcut olduğunu ifade etmektedir (Madde 29 Çalışma Grubu, 2010). Bu noktada ilk olarak var olan, işlenen ve aktarılan verinin artışıyla ortaya çıkan 'veri tufanı' adlı etkiden bahsedilmektedir. Hem teknolojik gelişmeler (bir başka deyişle bilgi ve iletişim sistemlerindeki büyüme) hem de bireylerin teknoloji ile olan etkileşim kabiliyetindeki artış bu olguyu desteklemektedir. Mevcut veri ile verinin küresel dolaşımı arttıkça, veri ihlallerinin taşıdığı risk de aynı oranda artış gösterecektir. Bu nedenle veri sorumlularının, kişisel verilerin korunması adına gerçek ve etkin mekanizmalar tesis etmelerine duyulan ihtiyaç daha da artmaktadır (Madde 29 Çalışma Grubu, 2010).

İkinci olarak kişisel veri miktarındaki sürekli artışa, sosyal, politik ve ekonomik açıdan verinin taşıdığı değerdeki artış da eşlik etmektedir. Öyle ki bazı sektörlerde (bilhassa çevrimiçi ortamda faaliyet gösterenlerde) kişisel veri, online içeriğe karşılık fiili para birimi hâlini almıştır. Aynı zamanda toplumsal açıdan bakılacak olursa, kişisel veriye atfedilen toplumsal değer de artış göstermektedir. Kısacası, kişisel verilerin veri sorumluları nezdindeki önemi arttıkça, vatandaşlar, tüketiciler ve genel olarak toplum kişisel verilerinin öneminin gittikçe daha da farkında hâle gelecek, bu da hâliyle kişisel verilerin korunması hususunda daha sıkı önlemler alınmasına yönelik ihtiyacı pekiştirecektir (Madde 29 Çalışma Grubu, 2010).

Son olarak, kişisel veri ihlalleri kamu ve özel sektördeki veri sorumlularının itibarları nezdinde ciddi olumsuz etkiler doğuracaktır. Bu nedenle riskleri en aza indirgemek, iyi bir itibar oluşturmak ve bunu sürdürmek, vatandaşların ve müşterilerin güvenlerini kazanmak tüm sektörlerdeki veri sorumluları için gittikçe daha fazla önem arz etmektedir (Madde 29 Çalışma Grubu, 2010).

Özetle yukarıda anlatılanlar, veri sorumlularının yetersiz kişisel veri koruma uygulamalarından doğabilecek yasal, ekonomik ve itibar risklerini en aza indirerek kişisel verilerin korunmasına ilişkin gerçek ve etkin tedbirler alma gereksinimlerini ortaya koymakta olup hesap verilebilirlik merkezli mekanizmalar bu hedefleri yerine getirme amacı taşımaktadırlar (Madde 29 Çalışma Grubu, 2010).

HESAP VERİLEBİLİRLİĞE DAYALI MEKANİZMALARIN HUKUKİ YAPISI

Madde 29 Çalışma Grubuna göre veri sorumlularının uygulamada gerçek anlamda koruma sağlanmasına yönelik önlemler almalarını teşvik edecek yasal çerçevenin izleyeceği yol, diğer bir deyişle hesap verilebilirliğe dayalı mekanizmaların hukuki yapısının nasıl görünmesi gerektiği irdelenmelidir. Belirtmek gerekir ki söz konusu sistemler kişisel verilerin korunmasına ilişkin temel ilkeleri değiştirmemekte veya onları etkilememekte, aksine onların işlerliklerini artırmaktadır (Madde 29 Çalışma Grubu, 2010).

Madde 29 Çalışma Grubu, hesap verilebilirlik ilkesinin revize edilmiş Direktife dâhil edilmesinin, veri sorumlularını bu tür önlemleri uygulamaya sevk edecek yollardan biri olduğunu vurgulamış ve bu tür bir düzenleme ile veri sorumlularını mevcut veri koruma ilkelerini etkin hâle getirecek önlemler almakla ve talep edilmesi hâlinde bunları veri koruma otoritelerine ispat edebilmekle yükümlü kılacak bir etkinin beklenebileceğini ifade etmiştir. Buna ek olarak belirli durumlarda mahremiyet etki analizi yapılması veya veri koruma görevlisi atama yükümlülüğü gibi spesifik gerekliliklerin, genel hesap verilebilirlik ilkesinin tamamlayıcısı olarak öngörülebilmeleri de mümkündür (Madde 29 Çalışma Grubu, 2010).

Belirtmek gerekir ki yasal zorunluluktan kaynaklananlara ek uygulama ve prosedürlerin veri sorumluları tarafından uygulamaya konulmaları mümkündür. Madde 29 Çalışma Grubu bu tip girişimleri takdir ettiğini ifade etmektedir. Bu doğrultuda, bir veri sorumlusunun ilgili kişilerin kişisel verilere erişim taleplerini mevzuatla belirlenenden daha kısa bir süre içerisinde yanıtlandırmayı ya da erişim taleplerini, bilginin hızlı ve etkin bir şekilde alınmasını teminen aynı anda hem çevrimiçi hem de çevrimdışı olarak yanıtlandırmayı tercih etmesi söz konusu olabilecektir. Benzer şekilde veri sorumlusunun tâbi olduğu yasal mevzuatta zorunlu kılınmadığı hâlde bir veri koruma görevlisi ataması ya da veri korumaya ilişkin uygulamalarının ilgili yasal çerçeveye uygunluğunu denetlemesi için üçüncü bir tarafi görevlendirmesi mümkün olacaktır (Madde 29 Çalışma Grubu, 2010).

Yukarıdaki açıklamalar çerçevesinde hesap verilebilirlik mekanizmalarının hukuki yapısının iki kademeden oluştuğu ifade edilebilir. İlk katman tüm veri sorumluları için bağlayıcılığı bulunan temel yasal yükümlülükleri, ikinci katman ise yasada öngörülen asgari seviyenin üzerinde, gönüllülük esasına dayalı hesap verilebilirlik sistemlerini içermektedir. Belirtmek gerekir ki burada ifade edilen yasal zorunluluk; gerekli önlem veya prosedürlerin uygulamaya konulması ile bu hususun ispatlanabilirliği olmak üzere kendi içerisinde iki unsurdan oluşmak-

tadır. İlk katmanının bir bütünleyicisi olarak birtakım spesifik zorunlulukların öngörülmesi de göz önünde bulundurulabilecektir (Madde 29 Çalışma Grubu, 2010).

GENEL VERİ KORUMA TÜZÜĞÜNDE HESAP VERİLEBİLİRLİK

Madde 29 Çalışma Grubunun önerisine uygun olarak Genel Veri Koruma Tüzüğünün (GVKT) 5 inci maddesinin ikinci fıkrasının (a) bendinde hesap verilebilirlik ilkesine açıkça yer verilmiştir. Söz konusu hükümde veri sorumlusunun mezkûr maddenin birinci fıkrasında sayılan kişisel veri işlenmesine ilişkin ilkelere uygun davranmaktan sorumlu olduğu ve buna uygun davrandığını gösterebilir durumda olmakla mükellef olduğu ifade edilmiştir. Söz konusu hükmün Tüzükte yer alması ile kişisel verilerin korunması alanında öngörülen yükümlülüklere uyumun ispatı veri sorumlusuna yüklenerek devlet tarafından denetleme unsuru geri plana atılmış ve sorumluluk veri sorumlusuna verilmiştir (Çekin, 2018).

GVKT kapsamında hesap verilebilirlik, kişisel verilerin korunmasına ilişkin kurallara uyma ve gerektiğinde bunu ispatlayabilme şeklinde iki yükümlülüğü bünyesinde barındırmaktadır. Her ne kadar 95/46/EC sayılı Direktif "hesap verilebilirlik" terimini kullanmamış olsa da veri işleme faaliyeti ile sorumlu tarafın pek tabii Direktife uygun hareket etme yükümlülüğü mevcuttu. Ancak veri sorumlusu veya veri işleyenin herhangi bir şekilde uyumluluğu ispat etme zorunluluğu Direktiftin hiçbir yerinde açıkça öngörülmemekteydi. Bu nedenle Tüzüğün getirdiği asıl yenilik, veri işleme faaliyeti ile sorumlu tarafın uyumluluğu ispat yükümlülüğünün kuvvetli biçimde vurgulanıyor oluşudur. Nitekim İngilizcede "ispat etme" anlamını taşıyan "demonstrate" kelimesine Tüzükte 33 defa yer verilmektedir (Korff ve Georges, 2019).

Bununla birlikte GVKT yalnızca hesap verilebilirlik yükümlülüğünü açıkça düzenlemekle yetinmemiş, hesap verilebilirlik ilkesinin temini adına kimisi uygulanması zorunlu, kimisi gönüllülük esasına dayalı birtakım hesap verilebilirlik araçlarını da düzenleme altına almıştır.

GENEL VERİ KORUMA TÜZÜĞÜNDE HESAP VERİLEBİLİRLİK ARAÇLARI

Tasarımda Mahremiyet ve Varsayılan Mahremiyet

AB Mevzuatı, veri sorumlularının veri koruma ilkelerini etkin bir şekilde uygulaması için düzenlemelerin şartlarını yerine getirmesini ve ilgili kişilerin haklarını korumak için gerekli tedbirleri almasını öngörmüştür. Bu tedbirler hem veri işleme sırasında hem de veri işleme yöntemini belirlerken uygulanmalıdır. Bu tedbirlerin uygulanmasında veri sorumlusunun en son teknolojiyi, uygulama maliyetlerini, kişisel veri işlemenin mahiyetini, kapsamını, amaçlarını ve ilgili kişinin hak ve özgürlükleri üzerinde oluşacak riskleri ve zararları dikkate alması gerekir (Giakoumopoulos, Buttarelli ve O'Flaherty, 2018). Bu kapsamda GVKT'nin 25 inci maddesinde 'tasarımda mahremiyet' ve 'varsayılan mahremiyet' yaklaşımları ortaya konmuştur.

Tasarımda mahremiyet; bir sistemin, hizmetin, ürünün veya faaliyetin, tasarlanma aşamasından itibaren işleme süreci boyunca mahremiyet ve veri koruma gereklilikleri göz önünde bulundurularak ortaya konulmasıdır (ICO, 2023c). Varsayılan mahremiyet ise kullanıcı müdahalesine ihtiyaç duyulmaksızın kişisel verinin yalnızca belirlenen amaç doğrultusunda gerekli olduğu ölçüde işlenmesi anlamına gelmekte olup (Avrupa Veri Koruma Kurulu [EDPB], 2020) temelde veri minimizasyonu ve amaçla sınırlılık ilkeleri ile ilişkili bir yaklaşımdır (ICO, 2023c). Varsayılan mahremiyet, kişisel verilerin herhangi bir iş uygulaması ya da bilgi teknolojisi sisteminde otomatik olarak mümkün olan en üst düzeyde korunmasını sağlamayı amaçlamaktadır (Cavoukian, 2011).

Tasarımda mahremiyet yaklaşımı kişisel verilerin korunmasına ilişkin reaktif değil proaktif önlemler alınması şeklinde nitelendirilebilir. Bu yaklaşım ile mahremiyete yönelik ihlallerin henüz gerçekleşmeden önce öngörülerek engellenmesi mümkün hâle gelmektedir (Cavoukian, 2011). Belirtmek gerekir ki tasarımda mahremiyet, bir donanımın, yazılımın, sistemin veya işlemin kullanım süresi boyunca uygulanacak kişisel verilerin korunmasına yönelik stratejilerin oluşturulması amacıyla risk yönetimi ile hesap verilebilirliği merkezine alacak şekilde tasarlanmaktadır (Agencia Española de Protección de Datos, 2019) Bu çerçevede veri sorumluları ve veri işleyenlerin kişisel veri işlemeye başlamadan önce planlanan veri işleme faaliyetinin ilgili kişilerin hak ve özgürlükleri üzerindeki olası etkilerini değerlendirmeleri, ardından planlanan faaliyeti ilgili kişilerin hak ve özgürlüklerine yönelik müdahaleyi en aza indirgeyecek veya tamamen ortadan kaldıracak şekilde tasarlamaları ve faaliyetin her aşamasında kişisel verilerin korunması temin edecek gerekli teknik ve idari tedbirleri almaları gerekecektir (Giakoumopoulos ve diğerleri, 2018).

Kişisel Veri İşleme Faaliyetlerine İlişkin Kayıtlar

GVKT'nin 30 uncu maddesinin birinci fıkrası uyarınca veri sorumluları ile uygun olduğu hâllerde veri sorumlusu temsilcileri, yükümlü bulundukları kişisel veri işleme faaliyetlerinin kayıtlarını tutmakla mükelleftirler. Söz konusu kayıtlarda;

- Veri sorumlusunun, uygun hallerde ortak veri sorumlusunun, veri sorumlusu temsilcisinin ve veri koruma görevlisinin isim ve iletişim bilgileri,
- Kişisel veri işleme faaliyetinin amaçları,
- İlgili kişi kategorileri ile kişisel veri kategorilerine ilişkin bir açıklama,
- Uluslararası organizasyonlar ve üçüncü ülkelerde yer alan alıcılar da dahil olmak üzere kişisel verilerin aktarıldığı ya da aktarılacağı alıcı grupları,
- Uygun olması hâlinde kişisel verilerin üçüncü ülkelere veya uluslararası organizasyonlara aktarımları, söz konusu üçüncü ülke ve uluslararası organizasyonların belirtilmesi, GVKT'nin 49 uncu maddesinin birinci fıkrasının ikinci alt paragrafında ifade edilen kişisel veri aktarımlarının söz konusu olduğu hallerde uygun güvelik önlemlerinin alındığına ilişkin belgeler,
- Mümkün olması durumunda farklı kategorilerdeki verilerin ne kadar süre sonra silineceğinin öngörüldüğü,
- Mümkün olması durumunda GVKT'nin 32 nci maddesinin birinci fıkrasında yer alan teknik ve idari güvenlik tedbirlerine ilişkin genel bir açıklama

yer almak zorundadır.

Bununla birlikte mezkûr maddenin ikinci fıkrasında ise veri sorumlusu adına gerçekleştirdikleri veri işleme faaliyetleri kapsamında veri işleyenler ile uygun olduğu hâllerde veri işleyen temsilcilerinin tutmakla mükellef oldukları kayıtların içeriğine yer verilmiştir. Bu çerçevede;

- Veri işleyenin, uygun hallerde veri işleyen temsilcisinin, adına hareket edilen veri sorumlusunun/sorumlularının ve veri koruma görevlisinin isim ve iletişim bilgileri,
- Her veri sorumlusu adına gerçekleştirilen işleme kategorileri,
- Uygun olması hâlinde kişisel verilerin üçüncü ülkelere veya uluslararası organizasyonlara aktarımları, söz konusu üçüncü ülke ve uluslararası organizasyonların belirtilmesi, GVKT'nin 49 uncu maddesinin birinci fıkrasının ikinci alt paragrafında ifade edilen kişisel veri aktarımlarının söz konusu olduğu hallerde uygun güvelik önlemlerinin alındığına ilişkin belgeler,
- Mümkün olması durumunda GVKT'nin 32 nci maddesinin birinci fıkrasında yer alan teknik ve idari güvenlik tedbirlerine ilişkin genel bir açıklama,

söz konusu kayıtlarda bulunmalıdır.

Tüzüğün 30 uncu maddesinin dördüncü fıkrası uyarınca; düzenleyici kurum tarafından talep edilmesi hâlinde anılan kayıtların veri sorumlusu veya veri işleyen ve uygun olması hâlinde bunların temsilcileri tarafından hazır bulundurulması gerekmektedir.

Kişisel veri işleme faaliyetlerinin kaydına yönelik yükümlülük doğrudan hesap verilebilirliğin sağlanması için öngörülmüş bir düzenlemedir. Nitekim gerçekleştirilen faaliyetlerin belgelendirilmesi ve kaydedilmesi ile mevzuata uygun hareket edildiği ispatlanabilmekte ve düzenleyici otoritelerin veri işleme faaliyetlerinin hukuka uygunluğunu denetlemesine imkân sağlanmaktadır (Giakoumopoulos ve diğerleri, 2018).

Veri Koruma Etki Değerlendirmesi

Veri işleme faaliyetleri, nitelikleri gereği kişi haklarına karşı risk oluşturmaktadırlar. Kişisel verilerin kaybolmaları, yetkisiz kişilere açıklanabilmeleri veya hukuka aykırı işlenebilmeleri mümkündür. Haliyle veri işlemenin doğası ve kapsamına bağlı olarak bu riskler değişkenlik göstermektedir. Örneğin hassas verilerin işlendiği geniş kapsamlı bir veri işleme faaliyeti, küçük bir şirket tarafından şirket çalışanlarına ait adres ve şahsi telefon numarası verilerinin işlenmesine oranla daha yüksek bir risk taşıyacaktır (Giakoumopoulos ve diğerleri, 2018).

Yeni teknolojilerin ortaya çıkışı ve veri işlemenin gittikçe karmaşık bir hal alıyor oluşu nedeniyle, veri sorumlularının kişisel veri işleme faaliyetine başlamadan önce gerçekleştirilmesi amaçlanan kişisel veri işleme faaliyetinin olası etkilerini irdeleyerek bu tür risklerin üzerine eğilmeleri gerekmektedir. Bu sayede kuruluşlar söz konusu riskleri önceden gereği gibi tespit etme, irdeleme ve hafifletme imkânı bulabileceği gibi, veri işleme faaliyetinin kişiler üzerinde olumsuz bir etki yaratma olasılığı da belirgin ölçüde sınırlandırılmış olacaktır (Giakoumopoulos ve diğerleri, 2018). Buradan hareketle GVKT'nin 35 inci maddesinin birinci fıkrası uyarınca bilhassa yeni teknolojilerin kullanıldığı bir veri işleme faaliyetinin (işlemenin mahiyeti, kapsamı, içeriği ve amacı göz önünde bulundurulmak suretiyle) ilgili kişilerin temel hak ve özgürlükleri üzerinde yüksek risk oluşturma ihtimalinin bulunması hâlinde veri sorumlusu, hayata geçirilmeden önce tasarlanan faaliyetin ilgili kişilerin kişisel verileri üzerinde yaratabileceği etkilere yönelik

bir değerlendirme yapmakla yükümlü kılınmıştır. Veri koruma etki değerlendirmesi, işleme faaliyetinin sistematik ve kapsamlı bir şekilde analiz edilmesine ve veri koruma risklerinin belirlenerek en aza indirilmesine yardımcı olmaktadır (ICO, 2023d).

Veri koruma etki değerlendirmesi, veri sorumlularının GVKT gerekliliklerine uymalarına yardımcı olmakla kalmayıp aynı zamanda Tüzük ile uyumu sağlamak için uygun önlemlerin alındığını ispatlamalarına da yardımcı olduğundan, önemli bir hesap verilebilirlik aracı olarak addedilmektedir (Madde 29 Çalışma Grubu, 2017). Belirtmek gerekir ki veri koruma etki değerlendirmesinin doğru şekilde uygulandığından bahsedebilmesi için sürekli olarak gözden geçirilmesi ve düzenli olarak yeniden değerlendirilmesi gerekmektedir. Nitekim Madde 29 Çalışma Grubunun da vurguladığı üzere mevcut durumda bir veri koruma etki değerlendirmesi yapılmasının gerekli görülmediği hâllerde dahi, veri sorumlusunun gelecekte genel hesap verilebilirlik yükümlülüğü kapsamında veri koruma etki değerlendirmesi yapma zorunluluğu ortaya çıkabilecektir (Madde 29 Çalışma Grubu, 2017).

Tüzüğün 35 inci maddesinin birinci ve onuncu fıkraları ile 90 ve 93 numaralı resitallerinde vurgulandığı üzere veri koruma etki değerlendirmesinin işleme faaliyeti gerçekleştirilmeden önce yapılması gerekmekte olup bu durum tasarımda mahremiyet ve varsayılan mahremiyet ilkeleri ile tutarlılık göstermektedir. Veri koruma etki değerlendirmesinin işleme faaliyetine yönelik karar oluşturma sürecine yardımcı bir araç olarak görülmesi gerekmektedir. Veri koruma etki değerlendirmesini yapmakla yükümlü tarafın kim olduğu hususunda ise Tüzüğün 35 inci maddesinin ikinci fıkrasında veri sorumlusunun veri koruma etki analizinin yapılması noktasında sorumlu olduğu ifade edilmiş, ancak veri sorumlusu bizzat söz konusu değerlendirmeyi kendisi yapmakla yükümlü kılınmamıştır. Nitekim veri sorumlusunun söz konusu değerlendirmeyi organizasyon içinde veya dışında bir başka tarafa yaptırma imkânı mevcuttur. Öte yandan her hâlde veri sorumlusu bu hususta hesap verilebilir olmakla yükümlüdür (Madde 29 Çalışma Grubu, 2017).

Veri koruma etki değerlendirmesinin gerektiği hallerde veri sorumluları, işlemenin gerekliliği ve ölçülülüğü ile bireylerin hakları üzerinde oluşabilecek muhtemel riskleri belirlemelidir. Bununla birlikte veri koruma etki değerlendirmesinin tespit edilen risklerin önüne geçmek için planlanan güvenlik önlemlerini de içermesi gerekmektedir. Değerlendirmeyi takiben veri işlemenin bireylerin hakları üzerinde yüksek risk oluşturacağının ve riski azaltmak için herhangi bir tedbir alınmadığının ortaya çıkması hâlinde, veri sorumlusunun veri işleme faaliyetine

başlamadan önce ilgili düzenleyici otoriteye başvurması gerekecektir (Giakoumopoulos ve diğerleri, 2018).

Bununla birlikte Madde 29 Çalışma Grubu, veri koruma etki değerlendirmesinin veri koruma mevzuatına uyumluluk yönünden yararlı bir araç niteliğini haiz olması sebebiyle, değerlendirmenin gerekli olup olmadığının netleştirilemediği hallerde dahi yapılmasını önermektedir (Madde 29 Çalışma Grubu, 2017).

Veri Koruma Görevlisi

Veri koruma görevlisi, bir şirket veya kuruluşta görev alan ve görev aldığı şirket veya kuruluşun yürürlükteki mevzuata uygun biçimde kişisel verileri korumasını sağlamakla vazifelendirilmiş kişidir (EDPB, TY) GVKT'nin 37 nci maddesinin birinci fıkrası uyarınca;

- Yargı yetkisi dahilinde hareket eden mahkemeler hariç olmak üzere kamu kurum ve kuruluşlarında gerçekleştirilen veri işleme faaliyetleri,

- Veri sorumlusu veya veri işleyenin temel faaliyetlerinin, mahiyeti ve/veya amaçları gereği ilgili kişilerin düzenli ve sistematik bir şekilde geniş ölçüde izlendiği faaliyetlerden oluşması,

- Veri sorumlusu veya veri işleyenin temel faaliyetlerinin geniş ölçüde GVKT'nin 9 uncu maddesinde düzenlenen özel nitelikli kişisel verileri veya Tüzüğün 10 uncu maddesinde düzenlenen cezai hüküm veya suçları içeren veri işleme faaliyetlerinden oluşması,

hâllerinden birinin varlığı hâlinde veri sorumlusu veya veri işleyen, veri koruma görevlisi atamakla yükümlüdür.

Veri koruma görevlisi atama yükümlülüğünün getirilmesi ile organizasyonların faaliyetlerini Tüzüğe uygun biçimde gerçekleştirmeleri, bu faaliyetler kapsamında kişisel verilerin korunmasına ilişkin görüş ve önerilerin oluşturulması, hesap verilebilirliğin sağlanması ve Tüzükte öngörülen veri koruma ilkelerine işlevsellik kazandırılması amaçlanmıştır (Turan, 2021).

Veri koruma görevlileri bağımsız bir konumda görev almaktadırlar. Nitekim GVKT'nin 38 inci maddesinin üçüncü fıkrası uyarınca veri koruma görevlilerine gerçekleştirdikleri faaliyete ilişkin talimat verilemez veya faaliyetlerine ilişkin olarak kendisine işten çıkarma da dahil olmak üzere yaptırım uygulanamaz. Buna

ek olarak veri koruma görevlileri faaliyetlerine ilişkin olarak hazırladıkları raporları doğrudan veri sorumlusu veya veri işleyenin en üst yönetim birimlerine sunmaktadırlar.

Veri sorumluları ile veri işleyenler Tüzükle yükümlü kılınmadıkları hâllerde dahi veri koruma görevlisi atayabilmektedirler. Öte yandan gönüllü olarak veri koruma görevlisi atandığı durumlar ile atamanın zorunlu olduğu haller arasında, bu görevin gereklilikleri ve göreve atanan kişinin vazifeleri yönünden herhangi bir farklılık söz konusu değildir (EDPB, TY).

Bununla birlikte veri koruma görevlisi atama zorunluluğu kapsamına girip girmediği gözetilmeksizin her organizasyon, Tüzükte öngörülen yükümlüklerin yerine getirilebilmesini teminen uygun personel ve kaynağa ihtiyaç duymaktadır. Bu noktada veri koruma görevlisi, mevzuata uyumun sağlanması adına bulunduğu tavsiyeler ve yardımlarıyla görev aldığı organizasyonun yasalar çerçevesinde hareket etmesine destek sağlayabilecektir. Bu yolla veri koruma görevlisinin organizasyonun veri koruma yönetim sürecinde anahtar bir rol üstlendiği ve hesap verilebilirliğin artasına yardımcı olduğu görülebilmektedir (EDPB, TY).

Davranış Kuralları

Genel Veri Koruma Tüzüğünün 40 ıncı maddesinde düzenlenen davranış kuralları; belli bir sektörde faaliyet gösteren veri sorumluları ile veri işleyenleri temsil etmeye yetkili ticaret birliklerince veya diğer temsilci kuruluşlarca sektörün ihtiyaçları gözetilmek suretiyle hazırlanan veri koruma kurallarıdır. Davranış kuralını hazırlayan birliğe üye veri sorumluları ile veri işleyenler, kendi istekleriyle bu kurallara uyacaklarını taahhüt ederek, yetkili veri koruma otoritesi tarafından onaylanmış söz konusu kurallara kendileri bakımından hukuki bağlayıcılık kazandırabilmektedirler (Toparlak, 2021).

Tüzüğün 40 ıncı maddesinde davranış kurallarının; kişisel verilerin adil ve şeffaf biçimde işlenmesi, belirli konularda veri sorumlusunun meşru menfaati, kişisel verinin toplanması, kişisel verilerin takma ad yoluyla maskelenmesi, kamuya ve ilgili kişilere verilen bilgi, sahip olunan hakların ilgili kişilerce kullanımı, çocuklara bilgi sağlanması ve onların korunması, çocuklarına yönelik açık rızanın ebeveynlerden alınma şekli, GVKT'nin 24 ve 25 inci maddelerinde düzenlenen tedbirler ve prosedürler ile GVKT'nin 32 nci maddesinde düzenlenen, veri işleme faaliyetinin güvenliğine ilişkin tedbirler, düzenleyici otoriteye kişisel veri ihlali bildirimi ile bu tür ihlallerde ilgili kişilere yapılacak bildirim, kişisel verilerin üçüncü ülkelere ya da uluslararası organizasyonlara aktarımı, ilgili kişilerin GVKT'nin 77 ve 79

uncu maddelerinde düzenlenen haklarına halel gelmeksizin veri sorumluları ile ilgili kişiler arasında gerçekleşen uyuşmazlıklara ilişkin mahkeme dışı yöntemler veya diğer uyuşmazlık çözüm yöntemleri gibi hususlarda uygulanışını belirlemek amacıyla düzenlenebileceğini ifade ederek davranış kurallarının veri işlemenin şeffaflığını sağlamaya yönelik işlevselliğine doğrudan atıfta bulunulmaktadır.

Davranış kurallarının veri sorumluları ile veri işleyenler açısından en büyük yararı, faaliyet gösterdikleri sektörün ihtiyaçları göz önünde bulundurularak hazırlanmış bu kurallara uygun hareket ettiklerini ispatlamaları hâlinde gerçekleştirdikleri kişisel veri işleme faaliyetlerinin hukuka uygun olduğunun kabul edilebilmesidir (Kaya, 2021).

Belirtmek gerekir ki veri işleme faaliyetini güvenlik ve veri etki analizi kapsamında faaliyetin sahip olduğu etki yönlerinden değerlendirirken ya da idari para cezası tesis edileceği hâllerde veri koruma otoriteleri, onaylanmış davranış kuralına uygun hareket edilişini göz önünde bulundurmaktadır (EDPB, 2019). Aynı doğrultuda İngiliz veri koruma otoritesi ICO 'sektörlerin faaliyet alanlarındaki kişisel verilerin korunmasına ilişkin problemleri tespit edip bunları çözmelerine imkân sağlayan bir gönüllü hesap verilebilirlik aracı' olarak tanımladığı davranış kurallarının şeffaflık ve hesap verilebilirliğin artırılması ile organizasyonun GVKT'ye uygun hareket ettiğine yönelik güvenin artması noktalarında veri sorumluları ile veri işleyenlere yardımcı olabileceğini ifade etmektedir (ICO, 2023b).

Bağlayıcı Şirket Kuralları

İlk defa Genel Veri Koruma Tüzüğünde açıkça düzenlenen bağlayıcı şirket kuralları, Tüzüğün "Tanımlar" başlıklı 4 üncü maddesinin yirminci fikrasında; Avrupa Birliği üyesi devletlerde yerleşik veri sorumluları ile veri işleyenlerin, AB üyesi olmayan devletlerdeki grup şirketlerine ya da ekonomik işbirliği içinde bulunduğu teşebbüslerine yaptıkları kişisel veri aktarımlarında uymayı taahhüt ettikleri kurallar olarak tanımlanmıştır (Toparlak, 2021).

95/46/EC sayılı Direktifin yürürlükte olduğu dönemde çok uluslu şirketlerin grup şirketlerine kişisel veri aktarımı yaparken birden fazla ülkenin kişisel verileri koruma mevzuatına uygun hareket etmeleri gerekmekteydi. Bu durumun söz konusu grup şirketlerinin iş süreçlerini yavaşlatıyor olması nedeniyle şirketler kendi gizlilik politikalarını oluşturarak veri koruma otoritelerine kabul ettirme çabası içine girmişlerdir. Öte yandan söz konusu uygulamanın yurtdışına veri aktarımını grup şirketleri için daha kolay hâle getiriyor olması karşısında veri koruma otoritelerine sunulan gizlilik politikalarının yeterli korumayı sağlama-

dığı görülmekteydi. Bu noktada Madde 29 Çalışma Grubu, söz konusu uygulamanın belirli asgari kişisel veri koruma şartlarını taşıması hâlinde grup şirketleri adına uluslararası kişisel veri aktarımlarında makul bir yöntem olacağını değerlendirerek davranış kurallarından geliştirdiği bağlayıcı şirket kurallarını ortaya çıkarmıştır. Böylece Direktifte açıkça zikredilmemesine karşın bu uygulama Direktifin yürürlükte olduğu dönemde ilk kez kullanılmaya başlanmıştır (Dülger ve Kahraman, 2021).

Madde 29 Çalışma Grubu, uluslararası veri aktarımında kullanılan bağlayıcı şirket kurallarının denetim, eğitim programları, gelen şikayetlerin ele alınmasına yönelik sistemlerin kurulması gibi yollarla veri koruma ilkelerinin etkin hâle getirilmesi amacıyla tasarlanmış, çok uluslu organizasyonlarca düzenlenerek uygulamaya konulan kurallar olduğunu ve hesap verilebilirlik ilkesinin bir yansıması olduğunu ifade etmektedir (Madde 29 Çalışma Grubu, 2010).

Öte yandan bağlayıcı şirket kuralları yalnızca uluslararası veri transferlerinde kullanılan bir araçtan ibaret olmayıp aynı zamanda organizasyon çapında bir mahremiyet yönetim programının omurgası olarak da görülebilmektedirler. Bu nedenle Genel Veri Koruma Tüzüğünde bu araca açıkça yer verilmiş olması, hesap verilebilirlik ilkesine katkıda bulunulması, hukuki kesinliğin sağlanması ve işletmelerin gereksiz yükten kurtarılmasına yardımcı olunması noktasında memnuniyetle karşılanan bir gelişme olarak görülmüştür (Bowman ve Gufflet, 2017).

Uluslararası grup şirketlerince Tüzüğe uygun şekilde hazırlanan ve onaylatılan bağlayıcı şirket kuralları, şirket bünyesinde yer alan kuruluşların tamamı için bağlayıcı niteliği haiz olup söz konusu kuruluşlar arasında Tüzüğe uygun serbest veri akışını sağlamaktadır. Bu sayede grup şirketleri bünyesindeki tüm kuruluşların yeknesak bir veri koruma politikası oluşmakta ve Tüzüğe uyum süreci daha kolay hâle gelmektedir. Buna ek olarak bağlayıcı şirket kurallarının, temelde grup şirketlerinin veri yönetim politikalarını resmileştirerek yayınlaması anlamına gelmesi ve Tüzüğe uyum noktasında bir ispat aracı olarak da kullanılabilmesi yönleri ile hesap verilebilirlik ilkesine uygunluğun sağlanmasına hizmet ettiğini söylemek mümkün olacaktır (Toparlak, 2021).

Sertifikasyon

GVKT kapsamında sertifikasyon, düzenleyici otorite veya düzenleyici otoritenin akredite ettiği bir başka tarafa gönüllü olarak başvuruda bulunan bir organizasyonun değerlendirilerek kişisel verilerin korunması alanında gerekli tedbirleri aldığının belgelendirmesidir. Diğer bir deyişle sertifikasyon, organizasyonların

başka organizasyonlara, bireylere ve düzenleyici otoritelere kişisel verilerin korunmasına yönelik gerekli tedbirleri aldıklarını ispatlamalarına imkân tanıyan bir hesap verilebilirlik aracıdır (An Coimisiún um Chosaint Sonraí, 2020).

Sertifikasyonun kapsamı oldukça genel ve çeşitli ürün, süreç ve servislere ilişkin olabileceği gibi bir dijital kasada bulunan kişisel verilerin güvenli şekilde saklanması ve korunması gibi oldukça spesifik bir hususa ilişkin de olabilecektir. Sertifikasyon, veri sorumlusu veya veri işleyenin bir ürün, işlem veya servis kapsamında gerçekleştirdiği belirli bir veri işleme faaliyetine ilişkindir. Söz konusu faaliyet yetkili sertifikasyon organı tarafından sertifikasyon kriterlerine göre değerlendirilmektedir. Belirtmek gerekir ki sertifikasyon yalnızca veri sorumluları ile veri işleyenlere yönelik bir uygulama olup bu kapsama girmeyen tarafların, örneğin veri koruma görevlilerinin, sertifikalandırılması mümkün değildir (An Coimisiún um Chosaint Sonraí, 2020).

ICO, sertifikasyonun aynı zamanda GVKT'de öngörülen tasarımda mahremiyet ve varsayılan mahremiyet hükümlerine uygun hareket edildiğini ve veri güvenliğinin sağlanması noktasında gerekli teknik ve idari tedbirlerin alındığını ispatlayan ve kişisel verilerin üçüncü ülkelere veya uluslararası organizasyonlara aktarımına destek sağlayan bir araç olduğunu ifade etmektedir (ICO, 2023a). Nitekim GVKT'nin 42 nci maddesinin ikinci fıkrası, Tüzüğe tâbi olmayan veri sorumluları ile veri işleyenlerin, uluslararası kişisel veri aktarımlarında uygun güvenlik önlemlerine sahip olduklarını ispatlama amacıyla sertifikasyondan faydalanabilmelerine imkân tanımaktadır. Buna ek olarak Tüzüğün 100 numaralı resitalinde; şeffaflığı ve Tüzüğe uyumu artırmak için ilgili kişilerin ürün ve hizmetlerin veri koruma düzeylerini rahatça değerlendirmelerine imkân tanıyan sertifikasyon mekanizmaları ile veri koruma mühür ve işaretlerinin kullanımının teşvik edilmesi gerektiği ifade edilerek sertifikasyon mekanizmalarının aynı zamanda şeffaflığın sağlanması amacıyla kullanılabilecek bir araç olduğu da açıkça vurgulanmıştır.

SONUÇ

95/46/EC sayılı Direktifin yürürlükte olduğu dönemde mevcut bulunan somut önlem ve uygulamalar ekseninde Avrupa Birliği veri koruma hukukuna hâkim ilke ve yükümlülüklerin çoğu zaman yetersiz derecede yansıtıldığı düşüncesiyle veri koruma alanında teoriden pratiğe doğru bir yönelime ve hukuki gerekliliklerin gerçek veri koruma önlemlerine dönüştürülmesine ihtiyaç duyulduğu anlaşılmıştır. Bunun sağlanabilmesi için Avrupa Birliğinin veri koruma alanındaki yasal çerçevesinin ek mekanizmalara gereksinim duyduğu sonucuna varılmış, hem Avrupa Birliği nezdinde hem de küresel ölçekte veri korumaya ilişkin yasal çerçevenin geleceğine yönelik tartışmalarda merkezine hesap verilebilirliği alan mekanizmaların veri sorumlularını etkin kişisel veri koruma araçlarını uygulamaya koymaya teşvik edeceği fikri ortaya atılmıştır (Madde 29 Çalışma Grubu, 2010). Böylece Direktifin yerini alan GVKT'de veri sorumlularının hesap verilebilirliğini sağlamaya yönelik muhtelif hesap verilebilirlik araçları ortaya konmuştur.

GVKT'de öngörülen tasarımda mahremiyet ve varsayılan mahremiyet yaklaşımları, veri sorumlusunun kişisel veri işleme faaliyetlerine ilişkin kayıt tutma yükümlülüğü, veri koruma etki değerlendirmesi, veri koruma görevlisi atama yükümlülüğü, davranış kuralları, bağlayıcı şirket kuralları, sertifikasyon düzenlemeleri ile birlikte, sürekli büyüyen kişisel verilerin korunması alanında veri sorumlularına mevzuata uyum noktasında pratik araçlar sunulmuş ve veri koruma otoritelerinin denetim noktasında yükleri azalmış olup (Kaya, 2020) uyumun ispatının veri sorumlusuna yüklenmesiyle devlet tarafından denetleme unsuru geri plana atılarak sorumluluk veri sorumlusuna verilmiştir (Çekin 2018). ◆

KAYNAKÇA

- Agencia Española de Protección de Datos. (2019). A Guide To Privacy By Design, https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf adresinden alınmıştır.
- An Coimisiún um Chosaint Sonraí. (2020). GDPR Certification, https://www.dataprotection.ie/en/organisations/gdpr-certification adresinden alınmıştır.
- Article 29 Working Party. (2017). Guidelines On Data Protection Impact Assessment (DPIA) And Determining Whether Processing Is "Likely To Result In A High Risk" For The Purposes Of Regulation 2016/679, https://ec.europa.eu/newsroom/article29/items/611236 adresinden alınmıştır.
- Article 29 Working Party. (2010). Opinion 3/2010 On The Principle Of Accountability, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf adresinden alınmıştır.
- Bowman, J., Gufflet, M. (2017). Meeting the Challenge of a Global GDPR and BCR Programme, European Data Protection Law Review, 3(2), 257-261.
- Cavoukian, A. (2011). Privacy By Design The 7 Foundational Principles Implementation And Mapping Of Fair Information Practices, https://oarc.duke.edu/sites/default/files/documents/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf adresinden alınmıştır.
- Çekin, M. S. (2018). Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu. İstanbul: On İki Levha Yayıncılık.
- Dülger, M. V., Kahraman, C. C. (2021) KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları, https://www.researchgate.net/publication/349553129_KVKK'dan_Kisisel_Verilerin_Yurt_DiDisi_AktariminAk_Onemli_Bir_Adim_Baglayici_Sirket_Kurallari adresinden alınmıştır.
- EDPB. (2020). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_bb_design_and_by_default_v2.0_en.pdf adresinden alınmıştır.

◊ EDPB. (2019). Guidelines 1/2019 On Codes Of Conduct And Monitoring Bodies Under Regulation 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en adresinden alınmıştır.

◊ EDPB. (TY). "Data Protection Officer (DPO)", https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en adresinden alınmıştır.

◊ Giakoumopoulos, C., Buttarelli, G., O'Fiaherty, M. (2018). Handbook On European Data Protection Law 2018 Edition, https://iapp.org/media/pdf/knowledge_center/Handbook_european_data_protection_02ENG.ppd adresinden alınmıştır.

◊ Kaya, M. B. (2020). Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi, İstanbul Hukuk Mecmuası, 78(4), 1859-1897.

◊ Korff, D., Georges, M. (2019). The DPO Handbook Guidance For Data Protection Officers In The Public And Quasi□Public Sectors On How To Ensure Compliance With The European Union General Data Protection Regulation, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3428957 adresinden alınmıştır.

◊ ICO. (2023a). Certification, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/certification/ adresinden alınmıştır.

◊ ICO. (2023b). Codes Of Conduct, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/ adresinden alınmıştır.

◊ ICO. (2023c). Data Protection By Design And Default, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ adresinden alınmıştır.

◊ ICO. (2023d). Data Protection Impact Assessments", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ adresinden alınmıştır.

◊ Toparlak, R. T. (2021) Genel Veri Koruma Tüzüğünde Bağlayıcı Şirket Kuralları: Avrupa Birliği Hukukunda Uygulama, Yüksek Lisans Tezi, Türk-Alman Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

◊ Turan, M. (2021). Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, Ankara: Seçkin Yayıncılık.

AVRUPA BİRLİĞİ VERİ KORUMA HUKUKUNDA BAĞLANTILI OTOMOBİLLERE İLİŞKİN UYGULAMALAR

İrem ÖZDİL ALTAK

Kişisel Verileri Koruma Uzman Yardımcısı

Bu çalışma, 14.02.2023 tarihinde kabul edilen "Kişisel Veri ve Cihaz Verisi Kavramları: Avrupa Birliği Uygulamaları" başlıklı uzmanlık tezinden alınmıştır.

GİRİŞ

Değişmekte ve dönüşmekte olan toplum sebebiyle dünya da çok hızlı şekilde değişmekte ve bilişim teknolojilerindeki gelişmeler sayesinde bilgiye ulaşmak, bilgi toplamak ve bilgiyi dağıtılmak büyük ölçüde kolaylaşmaktadır (Özkan, 2020). Nesnelerin interneti teknolojisinin gelişmesiyle birlikte; hayatlar kolaylaşmakta, yaşam standartları yükselmekte, verimlilik artmaktadır (Topaloğlu, Tekkanat ve Malakçı, 2019). Nesnelerin interneti teknolojisi ile de tetiklenen dördüncü sanayi devrimi ile üretimden tüketime kadar tüm süreçleri etkilemekte, dolayısıyla temel ilkeler üzerine inşa edilmiş hukuk dallarında bir değişim ve dönüşümü beraberinde getirmektedir (Aşıkoğlu, 2018).

Öte yandan, günümüzde üretilen verinin artış sebebi artık her bir cihazın veri üretebilmesi ve bu cihazların geleneksel yöntemlerden daha nitelikli veriler üretmesi ile açıklanabilir (Aşıkoğlu, 2018). Söz konusu cihazların üretmekte olduğu veriler arasında kişisel verilerin bulunması da muhtemeldir. Cep telefonu, akıllı saatler, bilgisayarlar, akıllı ev eşyaları, akıllı iş yeri sistemleri gibi pek çok alanda nesnelerin interneti teknolojisinden faydalanılarak yeni nesil hizmetler kullanılmaktadır. Günümüzde çoğu otomobil hıza veya sürüşe ilişkin bilgileri kayde-

debilmektedir, küresel yer belirleme sistemi vasıtasıyla yol tarifi hizmeti sunabilmektedir. Söz konusu hizmetler sayesinde yolculara daha rahat ve güvenli bir yolculuk sağlanmasına karşılık yolcuların kişisel verileri kayıt altına alınabilmektedir (Yüzbaşı Topaz, 2021). Teknolojik gelişmenin bir getirisi olarak bağlantılı otomobiller artık geniş kitlelerce ulaşılabilir nitelik kazanmış ve "normal" haline gelmiştir. Bunun bir getirisi olarak bağlantılı otomobillerin kişisel verilerin korunması hukuku bakımından anlamının tespit edilmesi ihtiyacı hasıl olmuştur.

Bağlantılı otomobillere ilişkin olarak ilgili kişilerin kişisel verileri üzerinde tam yetkiye sahip olabilmeleri bakımından gösterge panelinde tüm otomobillerde aynı olacak biçimde standartlaştırılmış simgeler vasıtasıyla kişisel verilerin işlenmesini gerektiren faaliyetin gerçekleştirildiğinin gösterilmesinin, kişisel verilerin işlenmesini gerektiren faaliyetlerin etkinleştirilmesi ya da devre dışı bırakılmasını sağlayan seçenekler sunulmasının ve kişisel veriler kullanılarak özelleştirilen koltuk ayarı, navigasyon tercihleri, iletişim kayıtları gibi hizmetlerin silinebilmesi veya sıfırlanabilmesi imkânı tanınmasının gerektiği yönünde tavsiyeler oluşturulmuştur (Alman Otomotiv Endüstrisi Birliği, 2016). Bu anlamda, kişisel verilerin korunması mevzuatlarının bu yeni teknoloji bakımından uygulanması için çalışmalar yapıldığını söylemek mümkündür. Nihayetinde kişisel verilerin korunması kuralları ile hedeflenen temel amaç kişisel verilerin işlenmesini gerektiren teknolojilerin yasaklanması değil; kişisel verilerin hukuka ve dürüstlük kuralına, diğer bir ifadeyle kişisel verilerin korunması mevzuatı kurallarına uygun işlenmesini sağlamaktır. Kişisel verilerin korunması hukuku ile kişisel verilerin hukuka uygun olarak işlenebilmesini teminen uyulması gereken ilkeler belirlenmektedir (Develioğlu, 2017).

KİŞİSEL VERİ KAVRAMI

Henkoğlu'na (2015) göre, gerçek kişinin adı, medeni hâli, kimlik numarası, nüfusa kayıtlı olduğu yer, doğum yeri ve tarihi gibi kimlik bilgileri gibi, bedenindeki yara izi, ben, dövme gibi ayırt edici işaretler, kişisel görüntüsü, fotoğrafi, telefon numarası, banka hesap numarası veya IBAN numarası, kurum sicil, sosyal sigorta numarası, internet protokolü adresi, elektronik posta adresi, sosyal medya hesap bilgileri, bunlara ilişkin şifre numarası, güvenlik kodları, imzası, sosyal ağlarda yaptığı yazışmalar kişisel veri niteliğini taşımaktadır. Kişisel verinin hukuki niteliğine ilişkin olarak farklı görüşler bulunmaktadır ve kişisel veri kavramı için farklı tanımlar yapılmaktadır.

2010 yılında *"5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun"* ile Anayasanın 20. maddesine yeni bir

fikranın eklenerek *"kişisel verilerin korunmasını isteme hakkı"* Anayasal bir hak olarak tanınmıştır. Anayasal hak terimi, Anayasa tarafından tanınmış ve güvence altına alınmış hakları ifade etmek için kullanılmaktadır.

Kişisel verilerin korunmasını isteme hakkı, özel hayatın gizliliğiyle bağlantılıdır. Özel hayatın gizliliğinin temelinde, tüm insan haklarının temelinde olduğu gibi, insan onuru bulunmaktadır. Özel hayatın gizliliği insanın insan gibi yaşayabileceği şartları yaratmayı, bireyi maddi ve manevi baskılardan korumayı amaçlamaktadır (Korkmaz, 2017). Dülger'e (2019) göre, kişisel verilerin korunması hakkı, uzun bir süre *"özel hayatın gizliliği"* veya *"özel hayata ve aile hayatına saygı"* başlıkları altında değerlendirilmiştir. Ancak, kişisel verilerin korunması hakkı ile özel hayatın gizliliği hakkı arasındaki bağlantı yadsınamaz ise de, özel hayatın gizliliğine ilişkin geleneksel yaklaşım kişisel verilerin korunması bakımından yetersiz kalmaktadır (Küzeci, 2021). Bu noktada önemle belirtmek gerekir ki, kişisel verilerin korunmasını isteme hakkı, özel hayatın gizliliği hakkının bir parçası niteliğini taşımayan bağımsız ve temel bir haktır. Yani kişisel verileri korunmasını isteme hakkı, tamamen özel hayatın gizliliği hakkı altında düzenlenemeyecek kadar geniştir. Nitekim, kişisel verilerin korunması hakkı müstakil bir Anayasal hak olarak düzenlenmiştir ve *"kişisel verilerin işlenmesinin disiplin altına alınması", "temel hak ve özgürlüklerin korunması", "kişinin mahremiyet hakkı ile bilgi güvenliği hakkının korunması" ve "kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlenmesi"* amaçlarıyla 6698 sayılı Kanun yürürlüğe konulmuştur (Kişisel Verileri Koruma Kurumu, 2019).

Kişisel veri, 2016/679 sayılı Kişisel Verilerin İşlenmesine Karşı Gerçek Kişilerin Korunmasına ve Kişisel Verilerin Serbest Dolaşımına İlişkin 95/46/EC sayılı Direktifi Yürürlükten Kaldıran Avrupa Birliği Genel Veri Koruma Tüzüğü'nde (GVKT) *"kişisel veri tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgi"* biçiminde tanımlanmıştır.

95/46/ EC sayılı Kişisel Verilerin İşlenmesine Karşı Gerçek Kişilerin Korunmasına ve Kişisel Verilerin Serbest Dolaşımına İlişkin Direktif (95/46/EC sayılı Direktif) döneminde çalışmalarına başlayan 29. Madde Çalışma Grubu, Kişisel Veri Kavramına İlişkin 4/2007 Sayılı Görüşü'nde kişisel verinin dört adımda ele alınması gerektiğini değerlendirmektedir. Bu adımlar ise tanımı da oluşturmakta olan *"herhangi bir bilgi", "ilişkili olan", "tanımlanmış ya da tanımlanabilir"* ve *"gerçek kişi"* kelime gruplarıdır. Esasen her bir kelime grubu kendi içerisinde kastetmekte olduğu anlamla tanımın bütünsel anlamını oluşturmaktadır. Avrupa Birliği mevzuatındaki ve 6698 sayılı Kanun'daki kişisel veri tanımının paralelliği göz önünde bulundurularak, kişisel veri kavramının açıklanması bakımından bu unsurlara değinilecektir.

Herhangi Bir Bilgi

Tanımın bu unsuruyla, kişisel verinin nesnel ya da öznel olabileceği, verinin içeriğinin veya sunuluş tekniğinin kişisel veri niteliği taşımasına engel olmayacağı kastedilmektedir (29. Madde Çalışma Grubu, 2007). Gerçek kişinin kişisel ve ailevi yaşamına hakkındaki verilerin yanı sıra çalışma ilişkisi, ekonomik ve sosyal davranışlarına ilişkin veriler gibi çok geniş kapsamlı veriler kastedilmektedir. Bu bağlamda, işçi - işveren, satıcı - tüketici, hasta- doktor ilişkisi gibi çok çeşitli ilişkiler kapsamında kişisel verilerin söz konusu olması mümkündür. Kişisel veri tanımının "herhangi bir bilgi" ögesi kişisel verilerin korunması hakkının özel hayatın gizliliği hakkı kapsamında incelenemeyecek kadar kapsamlı bir hak olduğunu vurgulamaktadır. Bu unsurun taşıdığı bir diğer anlam ise, kişisel verinin rakam, resim, fotoğraf, ses, grafik gibi çok çeşitli biçimlerde ortaya çıkabileceğidir. Yani rakam, resim, fotoğraf, ses, grafik gerçek kişiyi belirli ya da belirlenebilir kılması şartıyla kişisel veri olarak nitelendirilebilecektir (29. Madde Çalışma Grubu, 2007).

Diğer taraftan, 6698 sayılı Kanunun 3. maddesinin (d) bendinde yapılan kişisel veri tanımında *"her türlü bilgi"* ifadesine yer verilmektedir. Mezkûr ifade, geniş bir alanın hedeflendiğinin işareti niteliği taşımaktadır (Küzeci, 2021). Diğer taraftan, bilginin, öznel ya da nesnel olmasının kişisel veri tanımı bakımından herhangi bir önemi olmadığı gibi, bilginin sanal ortamda ya da fiziken tutulması; yahut mezkûr bilginin otomatik yollarla ya da otomatik olmayan yollarla işlenmesi, bilginin bilgi olma ve kişisel veri olabilme niteliğini değiştirmemektedir (Yılmaz ve Çavuşoğlu, 2020).

İlişkili Olan

Bu unsur ile kastedilen, verinin kişisel veri olarak nitelendirilebilmesinin ön şartının gerçek kişi ile veri arasında doğrudan ya da dolaylı bir bağlantı kurulması ve kişisel verinin ilgili kişiye yapılacak muamele ile ilgili kişi hakkındaki değerlendirmeyi etkilemesidir (29. Madde Çalışma Grubu, 2007). Diğer bir deyişle, kişisel verinin ilgili kişiye karşı sergilenecek tutumu etkilemesidir. Bu anlamda, bir bilgiyi kişisel veri kılan unsurlardan biri de mezkûr bilginin ilgili kişiye isnat edilebilir nitelik taşımasıdır (Aksoy, 2010). Kişisel verinin ilişkili olma unsurunu meydana getiren üç faktör bulunmaktadır: "içerik", "amaç" ve "sonuç". Önemle belirtmek gerekir ki, söz konusu faktörlerin kümülatif olarak bulunmasına gerek bulunmamakta olup söz konusu faktörler birbirinin alternatifi niteliği taşımaktadır (29. Madde Çalışma Grubu, 2007).

İçerik faktörü, ilgili kişi üzerinde oluşturacağı etkiye bakılmaksızın bir bilginin ilgili kişi hakkında olmasıdır (29. Madde Çalışma Grubu, 2007). Amaç faktörü, kullanılması ihtimal dahilinde olduğunda veya somut olayın koşulları ele alındığında söz konusu bilginin ilgili kişinin durumunu tespit etmek veya davranışını değerlendirmek için kullanılabilmesi demektir (29. Madde Çalışma Grubu, 2007). Sonuç faktörü ise belirli kişinin hakları ya da menfaatleri üzerindeki etkiyi temsil etmektedir (29. Madde Çalışma Grubu, 2007).

Belirli ya da Belirlenebilir

Tanımın bu unsuru, bahse konu bilginin ilgili kişiyi belirlemesini ya da en azından bahse konu veri ile başka veriler birleştiğinde ilgili kişinin belirlenmesinin elverişli kılmasını kastetmektedir. Söz konusu bilgi ilgili kişiyi doğrudan belirli kılabileceği gibi dolaylı olarak belirlenmesini de sağlayabilir (29. Madde Çalışma Grubu, 2007). Öte yandan, bir bilginin ilgili kişiyi belirli ya da belirlenebilir kılmasında veri sorumlusunun kullanılması muhtemel olan makul araçlara sahip olmasıdır (29. Madde Çalışma Grubu, 2007).

Ayrıca bu unsur, kişisel verinin tespitinde somut olayın özelliklerinin önemini vurgular nitelik taşımaktadır. Şöyle ki, isim ve soy isim kişiyi diğerlerinden ayıran diğer bir deyişle belirli kılan kişisel verilerin başında gelir. İsim soy isim aracılığıyla banka hesapları, sosyal güvenlik kayıtları, sağlık raporu gibi çok çeşitli veriye ulaşılması mümkündür. Ancak çok yaygın isimle çok yaygın bir soy isim kombinasyonu geniş bir çevrede içinde düşünüldüğünde kişiyi belirlenebilir kılmayabilir.

Diğer yandan, bazı verilerin kişiyi belirlemesi için başka verilerle birlikte mevcut olması gerekmektedir. Örneğin "siyah saçlı kadın" kişiyi belirli kılmak için yetersiz kalabilir ancak "siyah saçlı, beyaz elbiseli, kırmızı çantalı kadın" kişiyi belirli kılmak bakımından daha etkindir.

Bunun dışında verinin kimin tarafından ele edildiği de önem arz edebilir. 079 sicil numaralı personelin giriş yapması iş yeri bakımından, 12789 numaralı anahtar sahibinin siteye girmesi ise site yönetimi açısından anlam ifade edecektir. Diğer taraftan iş yeri sicil numarasının apartman yönetimi açısından, anahtar numarasının ise işyeri bakımından kişisel veri niteliği taşımadığı aşikardır. Bu doğrultuda, bir verinin kişiyi ya da belirlenebilir kılıp kılmadığına ilişkin karar verilirken somut olaya göre yorum yapılması gerekmektedir.

Gerçek Kişi

Tanımın bu unsuruyla, koruma altına alınan verilerin hayatta olan gerçek kişiye ait olması gerektiği vurgulanmaktadır. Bu anlamda, ilgili kişinin belirli bir ülke vatandaşı olması ona ilişkin bilgilerin kişisel veri niteliği taşımasına ilişkin olarak bir önem arz etmemektedir (29. Madde Çalışma Grubu, 2007). Öte yandan, ölmüş kişilerin, doğmamış çocukların ve tüzel kişilerin gerçek kişi olmamaları sebebiyle kişisel verilerinden söz etmek mümkün olmamaktadır (29. Madde Çalışma Grubu, 2007).

Türk Medeni Kanunu'nun *"Kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer. Çocuk hak ehliyetini, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder."* hükmünü amir olan 28. maddesinden yola çıkılarak bireye, sağ ve tam doğmak kaydıyla cenin olarak anne karnın düştüğü an ile ölümü arasındaki süreçte gerçek kişi denir.

Bu doğrultuda ölmüş kişiler açısından kişisel veriden bahsetmek mümkün olmayacaktır; ancak bu noktada önemle belirtmek gerekir ki, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarihli ve 2019/273 sayılı kararında *"... ilgili kişi kavramı "kişisel verileri işlenen gerçek kişi" olarak tanımlanmakta olup; 4721 sayılı Türk Medeni Kanununun 28. maddesinde ise kişiliğin, çocuğun sağ olarak tamamıyla doğduğu anda başladığı ve ölümle sona erdiği hüküm altına alınmıştır. Bu itibarla ölmüş kişilere ait veriler kişisel veri niteliğini haiz olmadığından konuya ilişkin olarak Kanun hükümleri uygulama alanı bulmayacaktır."* denilmektedir (Kişisel Verileri Koruma Kurulu, 2019). Ancak ölmüş kişiye ait bilgilerin ölmüş kişi dışındaki kişilere ait kişisel verileri içermesinin mümkün olabileceği hususunun ayrıca değerlendirilmesi gerekmektedir.

Yine gerçek kişi tanımı dolayısıyla cenin hakkındaki verinin kişisel veri sayılabilmesi için ceninin sağ ve tam doğmuş olması gerekmektedir. Örneğin ceninin sahip olduğu hastalık ancak bebeğin sağ ve tam doğması şartıyla kişisel veri niteliği taşıyacaktır ancak cenin annenin düşük yapması sebebiyle kaybedilmişse artık söz konusu hastalığın kişisel veri niteliği taşıması mümkün değildir. Öte yandan, ceninin genetik bir hastalığa sahip olduğu verisi ceninin üst soyunun sağlık durumu hakkında fikir verebileceğinden söz konusu verinin annenin düşük yapması sebebiyle kaybedilen cenin açısından kişisel veri niteliği taşımasa bile ceninin üst soyu bakımından kişisel veri niteliği taşıyabileceği göz önünde bulundurulmalıdır.

Bu unsur ile vurgulanan bir diğer husus ise tüzel kişilerin kişisel verisinin olmayacağıdır. Ancak, tüzel kişinin bilgilerinden yola çıkılarak gerçek kişiye ait kişisel verilere ulaşılabileceği hususunun ayrıca değerlendirilmesi gerekmektedir.

NESNELERİN İNTERNETİ

Turak'a (2015) göre nesnelerin interneti, nesnelerin ve uygulamaların kendileri arasında iletişim kurmalarını, veri üretmelerini, bu verilerin paylaşımını sağlayan gelişmekte olan bir teknoloji olarak tanımlanmaktadır. Nesnelerin interneti, genel olarak, fiziksel nesnelerin birbirleriyle ya da daha büyük sistemlerle bağlantılı olduğu iletişim ağı biçiminde de tanımlanabilir (Özdemir, Naralan Nursaçan ve Nursaçan, 2018). Veri üreten ve bu verileri internet üzerinden paylaşma yetisine sahip olan cihaz, makine, ve nesneleri birbirine bağlayan teknolojiye "nesnelerin interneti" adı verilir. Birbirlerine yahut başka sistemlere internet aracılığıyla bağlanarak veri aktarabilen cihazlara ise "bağlantılı cihazlar" adı verilir. Nesneler arasındaki bağlantının sağlanması vasıtasıyla insanların hayatlarını kolaylaştıracak uygulamaların geliştirilmesi hedeflenmektedir (Guisto, Iera, Morabito ve Atzori, 2010). Nesnelerin interneti ile amaçlanan bilgisayarların, otomobillerin, fırın, bulaşık makinesi gibi araçların bir ağ üzerindeki birleşmesi, iletişime geçmesi ve birlikte çalışabilir hale gelmesi için altyapı oluşturmaktır.

Nesnelerin interneti dört temel bileşenden meydana gelmektedir. Birbirine ve internete bağlı olan cihazlar nesne bileşenini, nesnelerin internetine etkin olarak bağlantı sağlayan gerçek kişi insan bileşenini, nesneler tarafından elde edilen ve insanlar tarafından üretilen veriler veri bileşenini, nesne insan ve veri elementi arasında bağlantı kurarak doğru verilerin doğru nesne ya da insana aktarılmasını sağlayan bileşen ise süreç bileşenini oluşturmaktadır (Gündüz ve Daş, 2018).

Nesne bileşeni, bilgisayar vasıtasıyla işlenebilmesini teminen fiziksel özellikleri sinyale dönüştüren sensörler; sensörlerden topladığı veriler için internet bağlantısı sağlayan kontrolörler ve kontrolörden aldığı komut doğrultusunda sistemi harekete geçiren aktivatörlerden oluşmaktadır. Veri bileşeni ise bilgisayar tarafından sınıflandırılabilecek ve analiz edilebilecek yapılandırılmış verilerden ve veri tabanının işleyebileceği düzene sokulmamış, ham haldeki yapılandırılmamış verilerden oluşmaktadır. İnsan bileşeninin nesnelerin interneti bakımından en önemli özelliği, istenen sonuç ile elde edilen sonuç arasında bağlantı kurulması ve sisteme geri dönüş sağlamasıdır. Süreç bileşeni ise, nesne insan ve veri bileşenlerinin etkileşiminin düzenlenmesini, doğru verinin doğru zamanda doğru insan ya da nesneye iletilmesini sağlamaktadır (Gündüz ve Daş, 2018).

Nesnelerin interneti vasıtasıyla insan ve sosyal hayatı hakkındaki her nevi bilgi

algılanır, süzülür ve toplanır. Elde edilen veriler, çeşitli hizmetlerin sağlanması amacıyla işlenebilir ve analiz edilebilir (Yan, Zhang ve Vasilakos, 2014). Avustralya Nesnelerin İnterneti İttifakına göre nesnelerin interneti teknolojisine sahip cihazların en çok kullanıldığı alanlar sürü yönetimi de dahil olmak üzere tarımda kullanılan ekipmanlar, otonom operasyonlar ve servis yönetimi dahil olmak üzere otomotiv sektörü, kişisel kullanıma özgülenmiş tıbbi cihazlar ve klinik teşhis ekipmanları, üretim zincirinde yer alan otonom ekipmanlar, altyapı izleme projeleri dahil olmak üzere akıllı şehre ilişkin cihazlar, çevre izleme ve kontrolünü içeren akıllı ev cihazları, kamu hizmetleri, madencilik olarak sıralanmıştır (Avusturalya Nesnelerin İnterneti İttifakı, 2016). Bu kapsamda, nesnelerin interneti teknolojisinin kullanımı söz konusu olduğunda büyük miktarlarda verinin işlenmesi söz konusu olmaktadır. İşlenen ve analize tâbi olan veriler arasında kişisel verilerin de bulunması durumunda kişisel verilerin korunması hukukunun uygulama alanı bulacağına dikkat çekmek gerekmektedir. Bu bağlamda, nesnelerin interneti ile çalışan cihazlar büyük miktarda veri üretir, üretilen veriler arasında kişisel veriler de bulunabilmektedir. Diğer bir deyişle, cihaz tarafından üretilmiş olan verilerin yalnızca cihazdan sadır olmaları sebebi ile kişisel veri niteliği arz etmemeleri mümkün değildir.

Nesnelerin interneti halihazırda geliştiğinden ve ticari bir ürüne dönüştürülerek mali getiri sağlamaya müsait bir alan olduğundan 29. Madde Çalışma Grubu tarafından ilgili kişilere bir ara yüz vasıtasıyla ulaşılabilen ve halihazırda bir cihaz ve / veya hizmet aracılığıyla hayata geçirilmiş olan üç nesnelerin interneti ürününe odaklanılmıştır. Bunlar: Giyilebilir Hesaplayıcılar, Niceliksel Öz ve Ev Otomasyonları olarak belirlenmiştir (29. Madde Çalışma Grubu,2014).

Giyilebilir hesaplayıcılar, gündelik eşyaların üzerine sensörler, mikrofonlar, kameralar ilave edilerek o eşyaların işlevlerinin artırılması biçiminde açıklanabilir. Gündelik eşyaya eklenen teknik cihazlar vasıtasıyla o eşyanın üreticisine gönderilen veriler sayesinde eşya daha işlevsel hale gelmektedir.

Niceliksel öz ise, alışkanlıklarının ya da yaşam şekillerinin özetini tutmak isteyen insanlar için tasarlanmış eşyalardır. Örnek olarak, yağ ve kas oranını hesaplayarak vücut ağırlığını kaydeden tartı; yürüyüş rotasını, hızını, o sırada atılan adım sayısını, kalp atışlarını kaydeden saat verilebilir. Bu cihazlar temel olarak daha sağlıklı ve daha fit bir yaşamı motive etmek amacıyla ortaya çıkmışlar ise de kaydedilen veriler özel nitelikli kişisel verilerden biri olan sağlık verilerini ihtiva edebilir.

Ev otomasyonları ise internete bağlı yangın alarmları, beyaz eşyalar, güvenlik sistemleri ile örneklenebilir. Sensörler ile donatılmış bir evde, o evde yaşayan

kişinin hareket sensörleri aracılığıyla takip edilmesi, odaların ısısını değiştirdiği saatten yola çıkılarak uyku saatinin tespit edilmesi mümkündür. Bu bağlamda kişinin güvende ve özgür hissetmesi ile karakterize olan mekân olan evlerde yer alan ve sürekli internete bağlı olan ev otomasyonlarının çeşitli kişisel verileri üreticilerine iletmesi mümkündür.

29. Madde Çalışma Grubu, nesnelerin interneti ile alakalı olarak meydana gelebilecek veri koruma hukukuna ilişkin zorlukları aşağıdaki biçimde sıralamıştır (29. Madde Çalışma Grubu, 2014):

İlgili kişinin yeterince aydınlatılmaması ve ilgili kişinin cihaz üzerinde tam bir kontrole sahip olamaması ortaya çıkabilecek zorluklardan biridir. Nesnelerin interneti söz konusu olduğunda, cihaz tarafından elde edilen kişisel veri, bir cihazdan diğer cihaza, cihazın üreticisine, arada yer alabilecek bir uygulamanın üreticisine peş peşe ve defaten aktarılabilir. Bu anlamda kişisel verilerin olağan akıştan farklı biçimde işlendiğini söylemek mümkündür. İlgili kişinin, kişisel verisinin işlenmeye başlanmasından önce hangi kişisel verilerinin yaygın biçimde işleneceğini fark etmesi zor olabilir. Diğer bir ifadeyle, cihazlar arasındaki etkileşimin kontrol edilmesi, bu etkileşimin konu veya lokasyon bakımından kısıtlanması olanağının sağlanması zordur.

Açık rızanın unsurlarına uygun olarak alınmamış olması da nesnelerin interneti teknolojisine sahip cihazlar vasıtasıyla kişisel verilerin işlenmesi esnasında ortaya çıkabilecek bir zorluk olarak karşımıza çıkmaktadır. Nesnelerin interneti teknolojisine sahip olan cihazları bu niteliğe sahip olmayan cihazlardan ayırmak ilk bakışta mümkün olmayabilir. Dolayısıyla ilgili kişinin veri işleme faaliyetinden haberdar olmadığı bir senaryo bakımından o işleme faaliyetine ilişkin olarak açık rızasından söz edilemeyecektir. Öte yandan, ilgili kişi kullanmakta olduğu cihazın kişisel verileri elde etmekte olduğunu fark etmeyebilir. İlgili kişi kullanmakta olduğu cihazın nesnelerin interneti teknolojisine sahip olduğunun farkında olsa dahi, kullanılan cihazın yalnızca belirli özelliklerinden yararlanılması belirli özelliklerinin ve bu özelliklerin ihtiyaç duyduğu kişisel verilerin kullanımının engellenmesi çoğu cihaz bakımından mümkün değildir. Bu anlamda, ilgili kişi cihazın sunduğu özelliklerden birini kullanabilmek için cihazın sunduğu diğer özelliğin ihtiyaç duyduğu kişisel verinin elde edilmesine müsamaha göstermektedir. Nitekim böyle bir durumda da ilgili kişinin açık rızasından söz etmek yerinde olmayacaktır.

Bu noktada önemle belirtmek gerekir ki 6698 sayılı Kanuna göre açık rıza, *"belirli bir konuya ilişkin olma", "bilgilendirmeye dayanma"* ve *"özgür iradeyle açıklanma"*

unsurlarının tümünü, kümülatif olarak taşımalıdır. İlgili kişinin bilmediği bir kişisel veri işleme faaliyetine ilişkin olarak açık rızadan bahsetmek mümkün olmayacaktır. Diğer taraftan, nesnelerin interneti teknolojisine sahip bir cihazın bir özelliğinden faydalanabilmek için bu cihazın diğer fonksiyonları için gerekli olan kişisel verilerin işlenmesine rıza gösterilmesi durumunda kişisel verilerin işlenmesi için özgür irade ile verilmiş bir açık rızadan bahsetmek mümkün olmayacaktır. Bu kapsamda, nesnelerin interneti teknolojisine sahip cihazlar vasıtasıyla kişisel veri işleme faaliyeti yürüten veri sorumlularının, açık rıza veri işleme şartına dayanarak kişisel veri işledikleri varsayımında, cihazları ve cihazların sunduğu hizmet ya da özellikleri açık rızanın unsurlarına uygun olarak düzenlemeleri gerektiği hususunun altı çizilmelidir.

Nesnelerin interneti teknolojisine sahip cihazlar vasıtasıyla kişisel verilerin işlenmesi söz konusu olduğunda ortaya çıkabilecek bir diğer zorluk elde edilen kişisel verilerden çıkarımlar yapılması veya bu verilerin farklı amaçlarla kullanılmasıdır. Nesnelerin interneti teknolojisine sahip cihaz tarafından elde edilen kişisel veriler bir araya getirildiklerinde farkı bir anlam ifade edebilir. Hatta, başlangıçta elde edilen veriler kişisel veri niteliğini haiz olmasa bile bu veriler ışığında yapılan çıkarım kişisel veri niteliği taşıyor olabilir. Bu anlamda, ilgili kişinin elde edilen kişisel verilerinin işlenmesinde sakınca görmezken elde edilen kişisel verilerden yapılan çıkarımın teşkil ettiği kişisel verinin işlenmesinde sakınca görüyor olması mümkündür.

Davranış kalıplarının ortaya çıkarılması suretiyle profilleme yapılması da nesnelerin interneti teknolojisine sahip cihazlar vasıtasıyla kişisel verileri işlenmesi söz konusu olduğunda ortaya çıkabilecek zorluklardan biridir. Nesnelerin interneti teknolojisine sahip cihazlar birbirlerinden farklı ve önemsiz görünen verileri elde etmektedir. Ancak birbirleriyle etkileşim haline olan cihazların elde ettikleri verileri analiz ederek ilgili kişiye ilişkin bir profil oluşturmaları mümkündür.

Nesnelerin interneti teknolojisine sahip cihazlarla donatılmış bir ortamda elde edilen verilere dayanılarak ilgili kişiye ait eksiksiz, ayrıntılı yaşam özellikleri ve davranış kalıpları tespit edilebilmesi mümkündür. 29. Madde Çalışma Grubu kapalı devre televizyonların umuma açık ortamda kişilerin sergiledikleri davranışlarda ortaya çıkardığı değişikliklerden yola çıkarak nesnelerin interneti teknolojisine sahip olan cihazların ilgili kişiler üzerinde anormal olarak tanımlanacak davranışları sergilememek adına bir baskı oluşturacağı ve bu baskının özel yaşam üzerindeki etkisinin onulamaz olacağını vurgulamaktadır (29. Madde Çalışma Grubu, 2014).

Nesnelerin interneti teknolojisine sahip cihazların gizliliği zedelemesi ise ortaya çıkabilecek zorluklardan bir diğeridir. Nesnelerin interneti teknolojisine sahip cihazların yaygınlaşmasıyla nesnelerin internetinden faydalanan cihazın sağladığı hizmeti kullanırken anonim kalma veya fark edilmeme ihtimali azalmaktadır. Özellikle taşınması kolay nitelikteki cihazlar ya da giyilebilir cihazlar konum takibi bakımından büyük bir risk oluşturmaktadır. Cihazlar, yalnızca aynı ağa bağlı olan cihazlar tarafından okunabilen ve cihazın kimliğini tanımlayan MAC adresleri (MAC, medya erişim kontrol adresinin kısaltmasıdır. MAC adresleri tektir ve değişmez nitelik taşımaktadır. Bu anlamda, bilgisayar ağı üzerindeki cihazların birbirlerinden ayrılmasını ve cihazların birbirlerini tanıyabilmelerini sağlamaktadır.) sayesinde ilgili kişinin konumu ve bu konumda kimlerle birlikte olduğu hususunda bilgi verebilir. Bu konum verilerinin daha sonra kapalı devre kamera verileriyle birleştirilebileceği de göz önünde bulundurulduğunda nesnelerin interneti teknolojisine sahip cihazlarla donanmış ortamlarda mahremiyetin zedelenmesi endişesi meydana gelecektir (29. Madde Çalışma Grubu, 2014).

Nesnelerin interneti teknolojisine sahip cihazlarla kişisel veri işlenmesi söz konusu olduğunda ortaya çıkabilecek son zorluk ise güvenlik ve verimlilik faktörlerinin yarışmasıdır. Bilgi güvenliğinin unsurları olan gizlilik, bütünlük ve erişilebilirlik nesnelerin interneti teknolojisine sahip cihazlar için de geçerlidir. Bununla birlikte nesnelerin interneti teknolojisine sahip cihazların sağladığı hizmetlerin etkin biçimde sunulabilmesi için cihazların mümkün olduğunca uzun bir kullanım süresi tanımasına ihtiyaç vardır.

Dolayısıyla, cihazın her bir kişisel veri işleme anında gizlilik, bütünlük ve erişilebilirlik unsurlarını sağlayan bir biçimde çalışması ile cihazın enerjiyi efektif kullanması zaman zaman yarışmakta ve cihaz üreticileri tarafından öncelik pil ömrüne verilmektedir Cihaz bilgi güvenliği unsurlarını sağlayacak biçimde tasarlanmış olsa dahi cihaz tarafından işlenen kişisel verilerin güvenliği bilgi güvenliği cihazın bağlı olduğu ağın güvenliği, bu kişisel verilerin gönderildiği cihazların güvenliği, kişisel verilerin depolandığı merkezin güvenliği gibi pek çok unsurla ilişkilidir . 29. Madde Çalışma Grubu bilgi güvenliğinin ölçütünün bir sistemi oluşturan bileşenlerin en zayıf halkası olduğuna dikkat çeker (29. Madde Çalışma Grubu, 2014). Diğer bir ifadeyle, bir sistem en zayıf bileşeni kadar koruma sağlamaya muktedirdir.

BAĞLANTILI OTOMOBİLLER

Bağlantılı otomobiller ile otomobilin kendi içinde yer alan kontrol ünitesi başta olmak üzere otomobilin içinde ve dışında yer alan cihazlarla veri paylaşımı

yapabilen sistemin tümünü içeren geniş bir kavram kastedilmektedir. Akıllı otomobiller, kullanıcısının sürüş deneyimini iyileştirmek ve otomobilin güvenliğini artırmak amacıyla telematik, internet bağlantılı bilgi ve/veya eğlence sistemleri, otomobil içi iletişim ve benzeri katma değer sağlayan sistemleri nesnelerin interneti vasıtasıyla sağlayan otomobiller olarak tanımlanmaktadır (Avrupa Ağ ve Bilgi Güvenliği Ajansı, 2019). Bu anlamda, otomobilin göstergeleri, bilgi veya eğlence panelleri, otomobille bağlantılı olan akıllı telefon veya tablet gibi cihazların veri üretebilmektedir.

Trafik, yol çalışması, sürüş hızı gibi faktörleri birlikte değerlendiren navigasyonlar, otomobilin servise götürülmesi için bildirimde bulunan hatırlatıcılar, uzaktan sürüş modu ya da koltuk konumunu gibi tercihlerin ayarlanabildiği servisler, eller serbest biçimde telefon görüşmesi yapılmasını, sesli komutla radyo frekansı değiştirilmesini sağlayan ara yüzler, kaza ya da sürüş kaydı yapan kameralar, çarpışma ya da sallantı uyarıları, park sensörleri kişisel veri de ihtiva edebilen verilerin işlenmesi vasıtasıyla çalışmaktadır.

Otomobiller, büyük kitlelerce kullanılan cihazlardır. Sürücüyü ve yolcuyu araç dışındaki dünyadan ayırdığı ve otomobile sahip olmaktan kaynaklanan egemenlik duygusundan dolayı seyahat edilen bir aracın ötesindedir. Otomobilin içi, özel bir alan olarak tanımlanabilir. Diğer taraftan, otomobilin sürücüsünün işlenecek kişisel verileri bakımından yeterince aydınlatılıp aydınlatılmadığı hususu dahi muğlakken aracın sahibi olmayan sürücüler yahut yolcular açısından aydınlatma yükümlülüğünün yerine getirilmesi ihtimali daha da düşüktür. Öte yandan otomobil içinde kişisel veri işleme faaliyetleri varsayılan olarak ayarlanmış olabileceğinden otomatik olarak başlayabilir. Gerek yolcular gerek otomobilin yabancısı olan (otomobili kiralayan, ödünç alan vb.) sürücü için anlaşılması ve kontrol edilmesi güç kişisel veri işleme faaliyetleri meydana gelebilir.

Gelişen teknoloji dolayısıyla nesnelerin internetinin ve bağlantılı cihazların yaygınlaşmasından otomobiller de etkilenmiştir. Günümüzde yalnız lüks araçlar değil her kesimden insan tarafından ulaşılabilir olan orta düzey otomobiller de bağlantılı cihaz niteliğini taşımaktadır. Yeni nesil otomobillere sahibini tanıma; sürüş tarzını, motor performansını ve yakıt tüketimini kaydetme; gidilen yerleri kaydetme ve gidilebilecek potansiyel yerleri tespit etme, sürüş esnasındaki kalp atışı, göz hareketleri, manevra biçimlerini belirleme gibi nitelikler sağlayan teknolojiler donanımsal ve yazılımsal olarak entegre edilmiştir.

Otomobilde gerçekleşen veri işleme faaliyeti otomobilin karmaşık yapısından kaynaklanan sebeplerle tek bir veri sorumlusu tarafından gerçekleştirilememektedir. Otomobil içinde yer alan yer alan çevrimiçi müzik uygulamaları, haritalar, oto pilot teknolojisi gibi uygulamaların kullanımı sırasında telekomünikasyon şirketleri, uygulama üreticileri gibi pek çok başka veri sorumlusu da devreye girmektedir. Ancak önemle belirtmek gerekir ki, bağlantılı otomobilden gönderilen verileri elde eden herkes veri sorumlusu olarak değerlendirilemez. Zira bahse konu verilerin kişisel veri olarak kabul edilebilmesi için ilgili kişiyi tanımlanabilir kılması gerekmektedir. Bu durumda veri sorumlusunun tespiti için, veriyi elde edenin bağlantılı otomobilden gönderilen verinin sahibi konumunda olan ilgili kişiyi tespit edebilme kabiliyetinde sahip olup olmadığı değerlendirilmelidir (Uluslararası Otomobil Federasyonu, 2017).

Öte yandan, bağlantılı otomobillerin yaygın olarak kullanılması neticesinde bağlantılı otomobiller tarafından üretilen ve işlenen veri artmaktadır. Bahse konu verilerin içinde kişisel verilerin bulunduğu, otomobil üreticileri, uygulama üreticileri, çeşitli hizmet sağlayıcılar gibi farklı veri sorumlularının bu kişisel veri işleme süreçlerinde devreye girdiği göz önünde bulundurulduğunda bağlantılı otomobiller vasıtasıyla kişisel verilerin işlenmesi hususu dikkat çekici hale gelmektedir.

Teknolojik gelişmeler o kadar hızlıdır ki yasaların bu hızı yakalaması her zaman mümkün olamamaktadır. Ancak gelişme hızındaki bu fark, otomobil üreticilerinin otomobillerinin her zaman güvenli ve güvenilir olmasını sağlama sorumluluğunu ortadan kaldırmaz. Üreticiler hem otomobillerini defalarca test etmekle hem de otomobillere dışarıdan gelebilecek müdahaleleri önlemekle yükümlüdür (IDC Corporate, 2016). Ayrıca veri koruma otoritelerinin ise kişisel verilerin korunmasına ilişkin mevcut mevzuatlarının yeni teknolojiler hakkında uygulanmasına dair yol göstermek eğiliminde olduğunu söylemek mümkündür.

AVRUPA BİRLİĞİ VERİ KORUMA KURULUNUN BAĞLANTILI OTOMOBİLLERE İLİŞKİN GÖRÜŞLERİ

Mezkûr bölümde Avrupa Birliği Veri Koruma Kurulu'nun (ABVKK) bağlantılı otomobillere ilişkin görüşleri, veri işleme faaliyeti esnasında oluşabilecek riskler, belirli veri kategorilerine özgü öneriler, ABVKK'nın tavsiyeleri ve veri işleme faaliyetlerinin amaçları esas alınarak tasnif edilmek suretiyle incelenmektedir.

Bağlantılı Otomobiller Vasıtasıyla Gerçekleştirilen Kişisel Veri İşleme Faaliyetleri Kapsamında Ortaya Çıkabilecek Riskler

Bağlantılı otomobiller vasıtasıyla kişisel veri işleme faaliyeti gerçekleştirilirken

oluşabilecek riskler "ilgili kişinin aydınlatılması", "açık rızanın sıhhati", "işleme amacının değişmesi", "ölçülülük ilkesine uyulmaması" ve "veri güvenliği riskleri" başlıkları altında incelenmektedir.

İlgili Kişinin Aydınlatılması

Risklerden ilki bağlantılı otomobilin sürücüsü ya da yolcularının bağlantılı otomobilde gerçekleştirilebilecek kişisel veri işleme faaliyetlerine ilişkin olarak yeterince aydınlatılmamış olması ihtimalidir. Otomobilin sürücüsü aydınlatılmış olmasına rağmen yolcuların kişisel verileri de kişisel veri işleme faaliyetine konu olabilir. Yahut aydınlatılmış olan araç sahibinin aracın sürücüsü olmaması ihtimaline de kişisel verileri işlenen sürücü aydınlatılmamış olacaktır. Bunun yanında otomobilin satılması, kiralanması, ödünç verilmesi mümkündür. Bu bağlamda otomobilin kullanımı esnasında gerçekleştirilen kişisel veri işleme faaliyetleri hakkında aydınlatılmamış olan ilgili kişilerin kişisel verilerinin işlenmesi ihtimali göz önünde bulundurulmalıdır. İlgili kişiler kişisel veri işleme süreçlerine ilişkin olarak aydınlatılmış olsalar dahi kişisel verilerin işlenmesi varsayılan ayar biçimde ayarlanmışsa ilgili kişinin kişisel verilerinin işlenmesine ilişkin olarak kontrol sağlaması zorlaşacaktır (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Bu noktada belirtmek gerekir ki, 6698 sayılı Kanunun *"Veri Sorumlusunun Aydınlatma Yükümlülüğü"* başlıklı 10 uncu maddesi;

> *"(1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür."*

hükmünü haizdir. Diğer taraftan, veri sorumlusu aydınlatma yükümlülüğünü yerine getirirken "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ" ile getirilmiş usul ve esaslara uymakla yükümlü kılınmıştır.

Açık Rızanın Sıhhati

Diğer risk, gerçekleştirilecek kişisel veri işleme faaliyetlerinin kişisel veri işleme şartlarından açık rızaya dayanılarak işlenmesi durumunda ortaya çıkacaktır. Kişisel verilerin açık rızaya dayanılarak işlenebilmesi için açık rızanın *"belirli bir konuya ilişkin olması", "bilgilendirmeye dayanması"* ve *"özgür iradeyle açıklanması"* gerekmektedir. Bağlantılı otomobilde gerçekleştirilecek kişisel veri işleme bakımından da açık rızanın geçerli olabilmesi ve hukuka uygun bir kişisel veri işleme faaliyeti gerçekleştirilebilmesi için açık rızanın tüm unsurlarının kümülatif olarak bulunması gerekmektedir. Özellikle otomobilin kiralanması, ödünç verilmesi gibi durumlarda sürücünün varsayılan olarak ayarlanmış ve kişisel verilerinin işlenmesine sebep olan ayarları değiştirememesi mümkündür. Öte yandan yolcular da ilgili ayarı yapabilmek açısından yetkilendirilmemiş olabilirler. Dolayısıyla, ilgili kişinin kişisel verilerinin işlendiğinden haberdar olmaması ve açık rızasının geçerliliğinin zedelenmesi ya da ortadan kalkması mümkündür (Avrupa Birliği Veri Koruma Kurulu, 2020a).

İşleme Amacının Değişmesi

Kişisel verilerin birden fazla amaçla işlenmesi ise başkaca bir riski oluşturur. Bu risk ile kastedilen başlangıçta belirli bir kişisel veri işleme faaliyeti bakımından verilen açık rızanın daha sonraki kişisel veri işleme faaliyeti bakımından geçerli olmayacağıdır. Örneğin, otomobilin bakım sıklığının saptanması amacıyla kullanılacak verilerin sürücünün kullanım davranışlarından yola çıkarak oluşturulan sigorta poliçelerinde kullanılmak üzere sigorta şirketine aktarılması halinde bu aktarım faaliyeti bakımından ilgili kişinin açık rızasından bahsetmek mümkün olmayacaktır (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Bu noktada, "belirli, meşru ve açık amaçlarla işleme" ilkesinin göz önünde bulundurulmasında fayda bulunmaktadır. Önemle belirtmek gerekir ki, veri sorumlusunun veri işleme faaliyetinin amacını açık ve kesin olarak belirlemesi gerekmektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a). Veri sorumlularının elde ettikleri kişisel verileri, ilgili kişiye belirttikleri amaçlar dışında başka amaçla kullanmaları durumunda yeni bir işleme faaliyeti söz konusu olmaktadır. Bu bağlamda veri sorumlusu dayanmakta olduğu işleme şartını her bir veri işleme faaliyeti bakımından ayrıca belirlemekle yükümlüdür.

Ölçülülük İlkesine Uyulmaması

Bir diğer risk ise lüzumundan fazla kişisel verinin işlenmesidir. Otomobilde kullanılan sensör, uygulama ve servisler ile doğru orantılı olarak daha fazla kişisel veri işlenmektedir. Fazla kişisel veri işlenmesinin sebebi, yeni teknolojiler geliştirilirken kullanılan makine öğrenmesinde uzun süreli ve büyük miktarlarda veriye ihtiyaç duyulmasıdır. (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Bu noktada belirtmek gerekir ki, kişisel veri işleme faaliyeti gerçekleştirilirken işlenecek kişisel verilerin veri sorumlusu tarafından belirlenen amacı gerçekleştirmeye uygun olarak seçilmesi gerekmektedir. Diğer bir deyişle, kişisel veri işleme faaliyetinin amacı bakımından elverişli olmayan, bu amacın gerçekleştirilmesine hizmet etmeyen, bu amaçla ilgili olmayan veya mezkûr amacın gerçekleştirilmesi bakımından ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılması elzemdir. Ölçülülük ilkesi, veri işleme ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulması anlamını taşımaktadır (Avrupa Birliği Veri Koruma Kurulu, 2020a). Ancak veri işleme faaliyetinin amacının gerektiği ölçüdeki kişisel verilerin işlenmesi hukuken meşrudur.

Veri Güvenliği Riskleri

Tüm kişisel veri işleme faaliyetlerinde olduğu gibi kişisel verilerin güvenliğinin sağlanması da bir risk oluşturmaktadır. ABVKK tarafından, bağlantılı araçlarda gerçekleştirilen kişisel veri işleme faaliyetleri bakımından veri güvenliğinin sağlanmasının olası bir güvenlik ihlalinin sürücü ve çevresindeki insanların hayatını riske atabilmesi ihtimali sebebiyle de önemli olduğu vurgulanmaktadır (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Bu bağlamda, veri sorumluları 6698 sayılı Kanunun 12. maddesi kapsamında yer alan veri güvenliğine ilişkin yükümlülüklerini "Kişisel Veri Güvenliği Rehberi" ışığında yerine getirmelidir. Örneğin, bazı otomobiller, mobil cihaz vasıtasıyla otomobilin wi-fi ağına bağlanılmadığı sürece işlevlerini yerine getirmeyecek biçimde tasarlanmıştır. Ancak otomobiller genellikle insanların evlerinin önüne, evin hemen yanında yer alan garaja park edilmektedir. Diğer taraftan insanların otomobilleri tarafından tanınan mobil cihazları da evin wi-fi ağına bağlı bulunmaktadır. Olası bir sinyal değişimi sebebiyle mobil cihaz, evde bağlı olduğu wi-fi ağından koparak evin önünde park halinde durmakta olan otomobilin wi-fi ağına bağlanabilir. Mobil cihazın otomobilin wi-fi ağına bağlandığı durumlarda otomobilin konumunun tespit edilmesi hatta otomobilin hırsızlıklara karşı alarmının devre dışı bırakılmasının mümkün olduğu görülmektedir (Sızma Testi Ortakları Güvenlik Danışmanlığı ve Test Hizmetleri, t.y.).

Avrupa Birliği Siber Güvenlik Ajansı, otomotiv endüstrisinin deneyimli bir sektör olduğunu ancak otomobillerdeki bağlantılı sistemlerin ve bunların güvenlik üzerindeki etkisine ilişkin çalışmaların zayıf olduğunu vurgulamaktadır. *"Açık bağlantı noktaları bırakılmaması, güvenli bilgi işlem tabanı oluşturulması gibi yöntemlerle sistemin baştan itibaren güvenli olarak tasarlanmamış olması", "tasarımdan itibaren gizliliği sağlanamaması"* (Bu ifade tasarımdan itibaren gizlilik

biçiminde Türkçeye çevrilmiş olup bağlantılı otomobil üreticilerinin ürünlerini ve hizmetlerini ve hizmetlerini kişisel verilerin korunması kurallarına mümkün olabilecek en uygun biçimde tasarlamasını ve üretmesini ifade etmektedir.), *"Dahili ve harici ara yüzlerde güvenlik açıklarının bulunması, zayıf şifre politikaları, VPN'nin yanlış yapılandırılması gibi elektronik kontrol ünitelerine yalnızca yetkili kişilerin ulaşmasının sağlanamaması"* gibi problemlerin önemli güvenlik açıklarına sebebiyet verdiğinin altı çizilmektedir (Avrupa Ağ ve Bilgi Güvenliği Ajansı, 2019).

Avrupa Birliği Siber Güvenlik Ajansı, bağlantılı otomobillerde güvenliğin sağlanması için "otomobillerde siber güvenliğin geliştirilmesi", "otomobil endüstrisinde yer alan üretici ve hizmet sağlayıcıları arasındaki bilgi paylaşımının arttırılması", "sektörde yer alan üretici ve hizmet sağlayıcılar arasındaki sorumluluk dağılımının netleştirilmesi", "iyi uygulama ve teknik standartlar hakkında uzlaşılması", "bağımsız üçüncü kişiler tarafından güvenlik denetimleri yapılması", "bu güvenlik denetimleri için analiz araçları oluşturulması" ve güvenlik denetimi yapan taraflarla iletişim ve bilgi alışverişinin artırılması hususlarını önermektedir (Avrupa Ağ ve Bilgi Güvenliği Ajansı, 2019).

Kişisel Veri İşleme Faaliyetine Konu Olan Veri Kategorilerine Göre Öneriler

ABVKK tarafından coğrafi konum verileri, biyometrik veriler ve suç soruşturmasına veya kovuşturmasına ilişkin veriler veri işleme faaliyetine konu olabilecek diğer kişisel verilerden ayrı tutulmuş ve bu kişisel veri kategorilerine özel tavsiyelerde bulunulmuştur.

Coğrafi Konum Verileri

Coğrafi konum verileri ilgili kişinin özel hayatı hakkında fikir verebilir. Şöyle ki, konum verilerinin işlenmesi söz konusu olduğunda, ilgili kişinin gidiş ve geliş için kullandığı rutin yollar vasıtasıyla işyeri ve ev adresleri tespit edilebilir; düzenli ziyaret edilen ibadethaneler dolayısıyla özel nitelikli kişisel verilerden olan dini belirlenebilir hale gelmektedir. ABVKK konum verilerinin işlenmesi faaliyeti söz konusu olduğunda, elde edilen konum verilerinin ayrıntı düzeyinin ve bağlantılı otomobilin bu verilere erişim sıklığının konum verisi işleme faaliyetinin amacı ile sınırlı olarak belirlenmesi gerektiğini, konum verisinin işlenmesi faaliyetinin amacının detaylı biçimde ilgili kişiye açıklanması gerektiğini, konum verilerinin işlenmesine ilişkin olarak ilgili kişinin açık rızası alınırken açık rızanın unsurlarına dikkat edilmesi gerektiğini, konum verisine yalnızca konum verisi işlenmesini gerektiren fonksiyon çalışırken erişilmesi gerektiğini, ilgili kişinin

bağlantılı otomobilin konum verisine erişimini kesebilmesi gerektiğini, konum verilerinin işlenmesi söz konusu olduğunda ilgili kişinin konum verisinin işlendiği hususunda bir işaret vasıtasıyla uyarılması gerektiğini ve konum verilerinin saklama sürelerinin sınırlı olması gerektiğini vurgulamaktadır (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Biyometrik Veriler

Gelişen teknolojiyle birlikte parmak iziyle kilidi açılan otomobiller, araç bilgisayarının açılması için yüz tanımanın kullanılması gibi sebeplerle bağlantılı araçlarda biyometrik verilerin işlenmesi faaliyeti gerçekleştirilebilmektedir. ABVKK'ya göre, biyometrik verilerin işlenmesi söz konusu hizmetin sağlanması bakımından tek yöntem olarak ilgili kişiye dayatılmamalıdır (Avrupa Birliği Veri Koruma Kurulu, 2020a). Diğer bir ifadeyle, söz konusu hizmetin sunulması bakımından biyometrik verinin işlenmesi yanında ilgili kişinin biyometrik verilerinin işlenmesini gerektirmeyen başka bir metodun sunulması gerekmektedir. Öte yandan, ilgili işinin biyometrik verilerinin üzerinde tam bir hakimiyete sahip olması gerekmektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a). Bu noktada Kişisel Verileri Koruma Kurulunun 25.03.2019 tarihli ve 2019/81 sayılı kararına dikkat çekmek gerekmektedir. Karara göre, spor kulübüne girişin kontrol edilmesi için alternatif yollar mevcutken spor kulübünde giriş çıkış kontrolünün yapılabilmesi amacıyla ilgili kişilerin biyometrik verilerinin kullanılması, *"işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma"* ilkesine aykırı bulunmuştur (Kişisel Verileri Koruma Kurulu, 2019). Bu anlamda, Kurulun biyometrik verilerin işlenmesi hususuna ABVKK'ya nazaran daha temkinli davrandığı ve alternatif yol ile hizmetin sağlanması mümkünken biyometrik verilerin kullanımını ölçülü bulmadığı sonucuna varılabilecektir.

ABVKK, biyometrik verilerin işlenmesi söz konusu olduğunda, biyometrik veri ile yapılacak doğrulamada oluşabilecek hata oranının tespit edilerek biyometrik veri işleme faaliyetinin kullanıldığı hizmetin hassasiyeti için uygun düzeyde güvenlik sağlanmasının önemli olduğuna, biyometrik verilerin elde edilmesini sağlayan sensörün yeterince hassas olmasına, biyometrik veri ile kimlik doğrulaması yapılması denemelerinin sınırlı sayıda tutulmasına, bağlantılı araçta saklanan biyometrik veri şablonunun son teknoloji şifreleme teknikleri ve algoritmalarla korunmasına, biyometrik verilerinin işlenmesi suretiyle gerçekleştirilen kimlik doğrulama faaliyetleri için ham verinin yerel olarak dâhi saklanmaksızın anlık olarak işlenmesi gerektiğine dikkat çekmektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Bir Suçun Soruşturulmasına veya Kovuşturulmasına İlişkin Veriler

Bağlantılı otomobillerde, sürüş ve kaza kameraları ile hız sensörleri vasıtasıyla da kişisel veriler elde edilebilmektedir. Bu yolla elde edilen kişisel verilerin arasında suç soruşturmasına ilişkin verilerin de bulunması mümkündür. Kaza anındaki hız, kazaya sebep olabilecek hareket gibi detayların bu sensörler vasıtasıyla tespit edilmesi olasıdır Bu anlamda ABVKK, suç soruşturmasına ilişkin kişisel verilerin GVKT'nin 10. maddesine uygun olarak işlenmesi gerektiğini vurgulamaktadır (Avrupa Birliği Veri Koruma Kurulu, 2020a). GVKT'nin 10. maddesinde bahse konu kişisel verilerin ancak Avrupa Birliği veya Avrupa Birliğine üye olan ülke hukukuna uygun biçimde işlenebileceği cezai hükümlere dair sicillerin ancak resmi makamları kontrolü dahilinde tutulabileceği belirtilmektedir. Bu anlamda mezkûr kişisel veriler açısından uygulamanın Avrupa Birliğine üye olan ülke hukuku doğrultusunda şekillenmektedir.

ABVKK, otomobil içinde kullanılan servisler bakımından mümkün mertebe bulut hizmetlerinden kaçınılmasını, sürüş güvenliği sağlayan uygulamalar için güvenli ve araç içi bir platform oluşturulması hususuna dikkat çekmektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Avrupa Birliği Veri Koruma Kurulu'nun Bağlantılı Otomobiller Vasıtasıyla Gerçekleştirilen Kişisel Veri İşleme Faaliyetlerine İlişkin Önerileri

ABVKK bağlantılı otomobiller vasıtasıyla kişisel veri işleme faaliyeti gerçekleştirileceğinde aşağıda yer alan hususlara dikkat edilmesini önermektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a):

- İlgili kişiler kişisel verilerinin nasıl elde edildiğini ve ne amaçla kullanıldığını bilmelidir. Bağlantılı araçlar vasıtasıyla işlenen kişisel verileri ancak belirli, meşru ve açık amaçlar ile işlenmelidir.

- Kişisel veri işleme faaliyetine ilişkin aydınlatma ilgili kişinin dilinde yapılmalıdır.

- Kişisel veri işleme faaliyetleri bakımından varsayılan ayar olarak kişisel verilerin işlenmesine izin verilmesi ancak otomobilin işleyişi gerekli olan işlevler bakımında mümkündür.

- İlgili kişiler her bir kişisel veri işleme faaliyeti bakımından kişisel veri işlem faaliyetini etkinleştirme, devre dışı bırakabilme ve kendi kişisel verilerini sil-

me imkânına sahip olmalıdır.

- İlgili kişiler otomobillerini satmaya karar verdiklerinde işlenmiş tüm kişisel verilerini silme imkânına sahip olmalıdır.

- İlgili kişiler, bağlantılı otomobil vasıtasıyla işlenen tüm kişisel verilerine erişim sağlayabilmelidir.

Avrupa Birliği Veri Koruma Kurulu'nun Aydınlatma Yükümlülüğüne İlişkin Önerileri

ABVKK, otomobil üreticisi, ekipman üreticisi, hizmet sağlayıcısı gibi tüm veri sorumlularının ilgili kişiyi aydınlatırken aşağıda yer alan hususları sağlamasını beklemektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

- Kişisel verinin işlenme amaçları ve kişisel veri işleme faaliyetinin hukuki dayanağının belirtilmesi

- Kişisel veri işleme faaliyeti meşru menfaat şartına dayanılarak gerçekleştiriliyorsa meşru menfaatin aydınlatma metnin detaylı olarak açıklanması

- İlgili kişinin kişisel verilerinin aktarımı söz konusu olacaksa kişisel verilerin aktarılacağı taraf ya da tarafların belirtilmesi

- İlgili kişinin kişisel verilerine ilişkin saklama sürelerinin belirtilmesi eğer bu sürenin belirlenmesi mümkün değilse belirlenmesi için kullanılan kriterlerin açıklanması

- Tüm ilgili kişi haklarının hatırlatılmasının yanı sıra veri taşınabilirliğine de dikkat çekilmesi (GVKT'nin 20. maddesi ile getirilen bu ilgili kişi hakkına göre, kişisel veri işleme faaliyetinin açık rızaya ya da bir sözleşmenin kurulması ya da ifa edilmesi işleme şartlarına dayanılarak gerçekleştirilmesi ve kişisel veri işleme faaliyetinin otomatik vasıtalarla gerçekleştirilmesi durumlarında ilgili kişi veri sorumlusuna sağlamış olduğu kişisel verilerinin şekillendirilmiş, kullanılmakta olan ve makine tarafından okunmaya müsait olacak biçimde veri sorumlusundan talep edebilir. Veri sorumlusu, ilgili kişinin talep etmiş olduğu kişisel verilerini başka bir veri sorumlusuna aktarmasına engel olamaz. Öte yandan, ilgili kişi kişisel verilerinin veri sorumlusu tarafından başka bir veri sorumlusuna doğrudan aktarılmasını da talep edebilir. Bunun yanında, veri taşınabilirliği hakkının kullanımı GVKT'nin 17. maddesi ile düzenlenmiş olan unutulma hakkının kullanımına engel teşkil edemez. Mezkûr hakkın kullanımının sınırı diğer kişilerin hak ve özgürlüklerinin olumsuz olarak etkilenmesi olarak belirlenmiştir.)

- Yurt dışına veri aktarılması planlanmaktaysa bu konuda bilgi verilmesi ve yurt dışına kişisel verilerin aktarılmasına ilişkin olarak alınacak güvenlik tedbirlerinin izah edilmesi

- Kişisel veri işleme faaliyetinin sözleşmeden kaynaklanan bir sorumluluk neticesinde mi yoksa sözleşmenin yapılmasını sağlamak amacıyla mı işlendiği hususunun açıklanması ve ilgili kişinin sözleşmeye konu kişisel verileri sağlamak zorunda olup olmadığı ile eğer kişisel verileri sağlamazsa ortaya çıkabilecek sonuçların ortaya koyulması

- Profilleme (Profilleme GVKT'nin 4. maddesinin dördüncü fikrasında ilgili kişinin kişisel verilerinin ilgili kişinin çalışma performansını, ekonomik gücünü, sağlık durumunu, kişisel tercihlerini, ilgi alanlarını,güvenilirliğini ve davranışlarını bulunduğu konum veya yapmakta olduğu hareketlerini analiz etmek ya da tahmin etmek maksadıyla otomatik vasıtalarla işlenmesi biçiminde tanımlanmaktadır.) dahil olmak üzere, ilgili kişi hakkında yasal sonuçlar doğurabilecek ya da ilgili kişiyi önemli şekilde etkileyecek otomatik karar vermek mekanizmalarının var olup olmadığına ilişkin açıklama yapılması,

- Müşterek veri sorumluluğu söz konusuysa her bir veri sorumlusu hakkında açık ve eksiksiz bilgi verilmesi

Avrupa Birliği Veri Koruma Kurulu'nun Veri Güvenliğine İlişkin Önerileri

- ABVKK otomobil üreticisi, ekipman üreticisi, hizmet sağlayıcısı gibi tüm veri sorumlularının veri güvenliğini sağlarken ye aşağıda yer alan hususları sağlamasını beklemektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

- İletişim kanallarının son teknolojiye uygun olarak şifrelenmesi

- Her otomobile kendine özgü şifreleme anahtarı ve yönetim modeli tasarlanması (Uygulamada her markanın aynı model araçlarına aynı şifreleme anahtarını ve yönetim modelini kullandığı görülmektedir.)

- Şifreleme anahtarlarının düzenli olarak yenilenmesini sağlamak

- Kişisel veri aktarılan cihazların kimliğinin doğrulanması
- Veri bütünlüğünün sağlanması

Öte yandan, ABVKK otomobil üreticilerinin veri güvenliğini sağlarken yukarıdakilere ilave olarak;

- Otomobilin hayati işlevlerinin telekomünikasyon hizmetlerinden ayrılması
- Otomobilin kullanım ömrü boyunca güvenlik açıklarının giderilebileceği bir sistem oluşturulması
- Otomobilin hayati işlevleri için ulaşım için ayrılan frekansların kullanılması
- Otomobile bir siber saldırı gerçekleştiğinde otomobilin güvenli modda çalışmasını sağlayacak bir alarm sistemi kurgulanması
- Siber saldırıların ve olası teknik güvenlik problemlerin tespiti ve düzeltilmesi için rutin kontroller yapılması
- Bu temel gerekliliklerin her bir kişisel veri işleme faaliyetinin özellikleri dikkate alınarak geliştirilmesi

hususlarını da sağlanması gerektiğine dikkat çekmektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

ABVKK, otomobil kullanım verilerinin başka bir veri sorumlusuna aktarımı yapılmadan önce bu aktarım faaliyetine ilişkin olarak ilgili kişinin açık rızasının sistemli bir biçimde alınmasını önermektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Kişisel Veri İşleme Faaliyetinin Amacına Göre Bağlantılı Otomobiller Vasıtasıyla Gerçekleştirilen Kişisel Veri İşleme Faaliyetleri

Bu bölümde bağlantılı otomobiller vasıtasıyla gerçekleştirilen kişisel veri işleme faaliyetleri bakımından yaygın olan kişisel veri işleme amaçlarına değinilmektedir.

Üçüncü Taraftan Hizmet Alınması

İlgili kişiler otomobillerine katma değer sağlamak için üçüncü kişilerden hizmet alabilmektedir. Sürdükçe öde tarzı sigorta ile park yeri rezervasyonu ve kiralanması hizmetleri ABVKK tarafından bu hizmetlere örnek olarak verilmiştir.

Sürdükçe Öde Sigortası

Sürdükçe öde sigortasında, otomobile bir cihaz yerleştirilerek ya da cep telefonuna yüklenen bir uygulama vasıtasıyla sürücünün sürüş davranışları ve kat ettiği mesafe kaydedilmektedir. Bu veriler ışığında, güvenli bulunan sürücülerin sigorta primleri daha az belirlenebilmektedir. Söz konusu işlemin gerçekleştirilebilmesini teminen ilgili kişinin kimlik bilgileri, banka kartı bilgileri gibi sigortacılık işlemine yönelik veriler ile birlikte konum verisi, sürüş davranışları, otomobil tarafından üretilen veriler gibi kullanım verileri işlenebilmektedir. İlgili kişinin otomobiline yerleştirilen cihaz ya da cep telefonuna yüklenmiş olan uygulama sayesinde elde edilen veriler bir puanlamaya tâbi tutulmakta ve bu puanlama neticesinde ilgili kişinin güvenilirlik derecesi tayin edilmektedir.

ABVKK, sürdükçe öde tarzı sigortanın işleme, yalnızca bir iletişimin bir elektronik iletişim ağı üzerinden iletilmesini gerçekleştirmek amacıyla veya abone veya kullanıcı tarafından açıkça talep edilen bir bilgi toplumu hizmeti ile ilgili olmaması sebebiyle E-Gizlilik Direktifinin 5. maddesinin üçüncü fıkrasında belirtilen istisna kapsamında bulunmadığının altını çizmektedir. Bu anlamda, veri sorumlusunun işleme şartı olarak GVKT'nin 6. maddesinin birinci fıkrasının (b) bendi uyarınca *"bir sözleşmenin kurulması ya da ifası için gerekli olması"* dayanması gerekmektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

ABVKK otomobile yerleştirilen cihaz ya da ilgili kişinin cep telefonuna yüklenmiş uygulama vasıtasıyla elde edilebilecek kişisel verilerin ilgili kişinin profillenmesi sonucu doğurabileceğine dikkat çekmekte ve söz konusu kişisel veri işleme faaliyetini ilgili kişinin mahremiyeti bakımından bir risk olarak yorumlamaktadır. Bu kapsamda, ilgili kişinin otomobiline yerleştirilen cihazın ya da ilgili kişinin telefonuna yüklenen uygulamanın bir sonuç üretmesi ve sigortacının yalnızca bu sonuca erişebilmesi ABVKK tarafından önerilmektedir. ABVKK'nın konuya ilişkin bir diğer önerisi ise, cihazın ya da ilgili kişinin telefonuna yüklenen uygulamanın elde ettiği sürüş davranışları, kat edilen mesafe, konum gibi kişisel verilerini işleyerek ilgili kişinin güvenilirlik puanını belirleyecek hizmet sağlayıcının ilgili kişinin kimlik bilgileri, plaka, poliçe numarası gibi kişisel verilerle erişememesi; sigortacının ise yalnızca kimlik bilgileri, plaka, poliçe numarası gibi kişisel verile-

re ve hizmet sağlayıcı tarafından belirlenen güvenilirlik puanına erişebilmesidir.

Bir diğer ifadeyle, otomobil tarafından üretilen veriler, konum, kat edilen mesafe gibi kullanım verileri ile ilgili kişinin kimliği, otomobilin plakası, poliçe numarası, ödeme bilgileri gibi sözleşmeye ilişkin ticari nitelikteki kişisel verilerin ayrıştırılması ve tüm bu kişisel verilerin tek bir veri sorumlusu nezdinde topu halde bulunmaması önerilmektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Öte yandan, elde edilen kişisel verilerin sigorta faaliyetleri ile uyumlu olması, diğer bir ifadeyle kişisel veri işleme faaliyetinin ölçülü olması gerekmektedir. Örneğin, sigorta primlerinin belirlenmesi için gerekli olan tek veri otomobilin kaç kilometre kat ettiği ise konum verilerinin elde edilmemesi gerekmektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Sürdükçe öde sigortasının yapılabilmesi için elde edilen kişisel verilerin saklama sürelerine ilişkin olarak ise kişisel veri çeşitleri arasında bir ayrım yapılması gerekmektedir. Örneğin, poliçenin kendisi hukuken belirli bir saklama süresine tâbi olabilecekken sigorta primlerinin tespit edilmesi için kullanılan güvenilirlik puanının hesaplanması için elde edilen kullanım verilerinin ancak güvenlilik puanının doğruluğunun kontrolünün saplanmasının gerektiği süre için saklanmalıdır (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Son olarak, veri sorumlusunun ilgili kişiye tarafından otomobilini kullanım şekli gözetilmeksizin sigorta yaptırma imkânı sunması gerekmektedir. Bir diğer ifade ile sürdükçe öde tarzı sigorta ilgili kişiye yaptırabileceği tek sigorta biçimi olarak sunulamaz (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Park Yeri Kiralanması Veya Rezervasyonu

Park yeri sahibinin park yerini kiralamak maksadıyla bir internet uygulaması vasıtasıyla listeleyebilmekte ve bir sürücü bu park yerlerini aynı uygulama üzerinden belirli kriterlere göre filtreleyebilmekte ve beğendiği park yerini rezerve edebilmektedir. Park yeri sahibinin onayı üzerine ödeme işlemleri sağlanmakta ve sürücü aynı uygulama vasıtasıyla park yerini varış noktası olarak işaretleyerek yol tarifi alabilmektedir.

Söz konusu hizmetin sağlanabilmesi için, ilgili kişinin ismi, e-posta adresi telefon numarası gibi iletişim bilgileri, plaka numarası, park süresi, ödeme için kredi kartı bilgileri ve konum verileri gibi kişisel verilerin işlenmesi söz konusu olabilmektedir. ABVKK, söz konusu uygulamayı bir bilgi toplumu hizmeti olarak

nitelendirmekte ve hizmetin abone tarafından açıkça talep edildiği durumlar bakımından araçta zaten depolanmış olan bilgilere erişim sağlaması bakımından ilgili kişinin için onayını aramamaktadır (Avrupa Birliği Veri Koruma Kurulu, 2020a). Öte yandan, bu hizmetin sağlanmasını teminen işlenmesi gereken kişisel verilerin işlenmesi bakımından, veri sorumlusunun işleme şartı olarak GVKT'nin 6. maddesinin birinci fıkrasının (b) bendi uyarınca *"bir sözleşmenin kurulması ya da ifası için gerekli olması"* işleme şartına dayanması gerekmektedir.

ABVKK, işlenen kişisel verilerin, yalnızca park sözleşmesinin yerine getirilmesi gerektiği sürece saklanmasını ve mezkûr kişisel verilerin bu sürenin sonunda silinmesini ya da anonimleştirilmesini önemekte ise de Avrupa Birliğine mevzuatında veya Avrupa Birliğine üye olan ülke mevzuatında belirlenmiş olan özel bir saklama süreleri mevcutsa bu sürelerin uygulama alanı bulacağına işaret etmektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Ayrıca ABVKK, park yeri kiralama veya rezervasyonu hizmeti bakımından ilgili kişinin GVKT'nin 13. maddesi doğrultusunda adil, şeffaf ve anlaşılır biçimde aydınlatılmasının yanı sıra veri sorumlusunun ilgili kişiyi aydınlatırken ilgili kişinin erişim hakkını kullanabileceği kişisel veriler ile ilgili kişinin veri taşınabilirliği hakkını kullanabileceği kişisel verilerin ayrımını net olarak yapmasını önermektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Elektronik Arama

29 Nisan 2015 tarihinde EU 2015/758 sayılı Acil Arama Sistemine Dayalı Elektronik Aramanın Devreye Sokulmasını Düzenleyen ve 2007/46/EC sayılı Yönergeyi Değiştiren Yönerge yayımlanmıştır. Mezkûr Yönerge doğrultusunda Avrupa Birliği genelinde meydana gelen kaza anında acil durum numarasına elektronik çağrı yapılarak ambulansın kazanın meydana geldiği konuma derhal gönderilmesi sağlanmaktadır. Bahse konu acil durum çağrısı, kaza anında elektronik arama cihazı tarafından başlatılabileceği gibi otomobilin içindeki kişilerin inisiyatifi ile de başlatılabilmektedir.

Elektronik aramanın gerçekleştirilebilmesini teminen elektronik aramanın nasıl başlatıldığı, otomobil kimlik numarası, otomobilin tipi, otomobilin itiş şekli, elektronik aramanın başladığı ilk andaki saat, otomobilin gittiği yönün tayini için elde edilen son üç konum ve otomobilden elde edilebilen son konum verisine göre elde edilen enlem ve boylam bilgileri verilerini içeren minimum veri seti olarak adlandırılan veriler işlenmektedir. Söz konusu verilerin elektronik arama tetiklenmediği sürece işlenmesi söz konusu olmayacaktır. Mezkûr kişisel veri-

lerin işlenmesi bakımından GVKT'nin 6. maddesinin birinci fıkrasının (c) *"veri sorumlusunun tâbi olduğu yükümlülüğe uyulması açısından gerekli olması"* işleme şartına dayanılacaktır. Veri sorumlusunun tâbi olduğu bu yükümlülük 2015/758 sayılı Tüzükte belirlenmiştir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Elektronik aramanın gerçekleştirilebilmesini teminen işlenen kişisel verilerin saklama süreleri 2015/758 sayılı Tüzük ile verilerin acil durumların gereken süre olarak belirlenmiş olup mezkûr veriler, elektronik arama için artık gerekli olmadığında silinmelidir. Ayrıca, elektronik arama sisteminin dahili belleğinde, veriler otomatik ve sürekli olarak silinmelidir. Aracın mevcut konumunu ve etkinlik sırasındaki seyahat yönünü belirtmek kesinlikle gerekli olduğu sürece, yalnızca aracın son üç konumu saklanabilir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

2015/758 sayılı Tüzüğün 6. maddesi doğrultusunda otomobil üreticileri elektronik aramaya için işlenecek kişisel verilere ilişkin olarak ilgili kişiyi açık ve eksiksiz biçimde aydınlatmakla yükümlüdür. Bu aydınlatma kapsamında kişisel verilerin işlenmesine ilişkin yasal dayanağa atıf yapmalı, elektronik aramanın özellikle kapalı olarak ayarlanmadığı müddetçe etkin olacağının altı çizilmeli, elektronik aramanın yalnızca acil durumlar için kullanılacağı belirtilmeli, elektronik arama hizmetinin sağlanmasını teminen işlenecek kişisel veriler ve bu kişisel verilerin aktarılacağı merciler belirtilmeli, otomobilin sürekli olarak takip edilmediği vurgulanmalı son olarak mezkûr faaliyet bakımından işlenen kişisel verilerin farklı amaçlarla işlenmesinin ancak ilgili kişinin açık rızası ile mümkün olacağının ifade edilmelidir. ABVKK, ilgili kişi elektronik aramaya ilişkin olarak aydınlatılırken elektronik aramanın yasal dayanağının açıklanması ve kişisel veri işlenmesini gerektiren hizmetlerden farklı bir nitelik taşıdığı hususlarının vurgulanması gerektiğine dikkat çekmektedir. Kişisel verilerin yasal bir yükümlülük çerçevesinde işlenmesi sebebiyle ilgili kişi haklarından olan itiraz ve veri taşınabilirliği hakları ise uygulama alanı bulmayacaktır (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Elektronik arama için işlenen kişisel veriler elektronik arama başlatılmadan önce otomobilin içindeki elektronik arama sistemi içinde tutulacak olup ancak elektronik aramanın tetiklenmesi halinde kamu güvenliği yanıtlama noktasına (Kamu güvenliği yanıtlama noktası belirli bir bölgeden gelen polis, itfaiye, acil sağlık ekibine yönelik çağrıların yanıtlandığı merkez biçiminde tanımlanmaktadır.) aktarılacaktır. Elektronik aramanın tetiklenmesi ile kastedilen otomobilin içindeki elektronik arama sisteminin şiddetli bir çarpışma tespit etmesi halinde doğrudan devreye girmesi ya da elektronik aramanın otomobildeki kişiler tarafından başlatılmasıdır. Öte yandan, Kamu güvenliği yanıtlama noktası tarafından elde edilen kişisel veriler ilgili kişinin açık rıza alınmaksızın üçüncü kişilere aktarılamaz (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Kazalara İlişkin Çalışmalar

Karayollarında meydana gelen kazaların daha iyi anlaşılması, kazaların nedenlerinin tespit edilmesi ve bilimsel olarak açıklanmasına yönelik çalışmalar yapılmaktadır. Kazaların oluşumunda etkili olan faktörler aynı zamanda kişisel veri niteliği de taşıyabilmektedir. İlgili kişilerin bu minvaldeki çalışmalara gönüllü olarak katılmaları mümkündür.

ABVKK, kazalara ilişkin çalışmalar kapsamında elde edilecek verilerin yalnızca bir iletişimin bir elektronik iletişim ağı üzerinden iletilmesini gerçekleştirmek amacıyla veya abone veya kullanıcı tarafından açıkça talep edilen bir bilgi toplumu hizmeti ile ilgili olmaması sebebiyle E-Gizlilik Direktifinin 5. maddesinin üçüncü fıkrasında belirtilen istisna kapsamında bulunmadığının altını çizmektedir. Bu anlamda, veri sorumlusunun işleme şartı olarak GVKT'nin 6. maddesinin birinci fıkrasının (a) bendi uyarınca *"ilgili kişinin açık rıza göstermesi"* işleme şartına dayanması gerekmektedir. Kazalara ilişkin çalışmaların GVKT'nin 6. maddesinin birinci fıkrasının (e) bendi kapsamında *"veri kamu yararı için gerçekleştirilen bir görevin ifası ya da veri sorumlusunun remi görevi için gerekli olması"* işleme şartı kapsamında işlenmesi de mümkün olsa da ABVKK tarafından kazalara ilişkin çalışmaların ilgili kişinin gönüllü katılımıyla yapılmasının daha uygun olduğu ifade edilmektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Kazalara ilişkin çalışmalar kapsamında, kimlik bilgisi, plaka gibi katılımcı ve otomobile ilişkin verile ile anlık hız gibi otomobilden elde edilen teknik veriler işlenmektedir. ABVKK'ya göre, katılımcı ve otomobile ilişkin veriler çalışma boyunca saklanmasında bir sakınca bulunmamaktadır diğer taraftan, otomobilden elde edilen teknik veriler çalışmanın bitiş tarihinden itibaren en geç beş yıl içinde silinmeli ya da anonim hale getirilmelidir. ABVKK'ya göre kaza çalışmaları kapsamında anlık hıza ilişkin kişisel veri bir suçun soruşturulması ve kovuşturulması kapsamında işlenmemektedir. Dolayısıyla, ABVKK kamu hizmeti yürütmeyen tüzel kişiler tarafından anlık hız verisinin elde edilmesinde herhangi bir sakınca görmemektedir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Ayrıca ABVKK, kaza çalışmaları kapsamında kişisel verileri işlenecek ilgili kişinin GVKT'nin 13. maddesi doğrultusunda adil, şeffaf ve anlaşılır biçimde aydınlatılmasının yanı sıra veri sorumlusunun ilgili kişiyi aydınlatırken ilgili kişinin erişim hakkını kullanabileceği kişisel verileri ile ilgili kişinin veri taşınabilirliği hakkını kullanabileceği kişisel verileri net olarak ayırmasını önermektedir (Avrupa Birliği

Veri Koruma Kurulu, 2020a).

ABVKK, anlık hız verisinin toplandığı durumlarda, takma isim kullanılması, anlık hız ve coğrafi konum verilerinin ayrı bir veri tabanında saklanması, mümkün olan en kısa sürede konum verilerinin silinmesi, doğrudan tanımlayıcı nitelik taşıyan kişisel verilerin daha az kişi tarafından ulaşılabilen ayrı bir veri tabanında saklanması önerilerinde bulunmaktadır (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Otomobil Hırsızlığı İle Mücadele

İlgili kişilerin olası bir hırsızlık durumunda konum verilerinin işlenmesi yoluyla otomobillerinin bulunmasını talep etmeleri mümkündür. Konum verileri, otomobil hırsızlığı ile mücadele amacıyla yetkili makamların sürdürdüğü soruşturma kapsamında ihtiyaç duyulduğu ölçüde kullanılabilir (Avrupa Birliği Veri Koruma Kurulu, 2020a). İlgili kişinin bir hırsızlık beyanında bulunması durumunda ilgili kişinin konum verileri uzaktan gözetim platformu çalışanlarına ve yasal olarak onaylanmış makamlara iletilebilir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

ABVKK, söz konusu uygulamayı bir bilgi toplumu hizmeti olarak nitelendirmekte ve hizmetin abone tarafından açıkça talep edildiği durumlar bakımından otomobilde zaten depolanmış olan bilgilere erişim sağlaması bakımından ilgili kişinin onayını aramamaktadır. Öte yandan, otomobil hırsızlığıyla mücadele amacıyla konum verilerinin işlenmesi bakımından, veri sorumlusunun işleme şartı olarak GVKT'nin 6. maddesinin birinci fikrasının (a) bendi uyarınca *"ilgili kişinin açık rızasının bulunması"* ya da 6. maddesinin birinci fikrasının (b) bendi uyarınca *"bir sözleşmenin kurulması ya da ifası için gerekli olması"* dayanması gerekmektedir. İlgili kişinin bir hırsızlık beyanında bulunması durumunda ilgili kişinin konum verileri uzaktan gözetim platformu çalışanlarına ve yasal olarak onaylanmış makamlara iletilebilir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Konum verileri elektronik iletişim hizmeti ile elde edileceğinden E-Gizlilik Direktifinin beşinci maddesinin üçüncü fikrası uygulama alanı bulacaktır. Otomobilin bulunması bir bilgi toplumu hizmeti olduğu ve abone tarafından hizmet talep edildiği için halihazırda otomobilde kayıtlı olan verilerin elde edilmesi için ayrıca onaya ihtiyaç duyulmayacaktır. Konum verileri soruşturmanın sınırları dahilinde yalnızca yetkili makam tarafından kullanılabilecektir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Otomobil hırsızlığı ile mücadele kapsamında işlenecek konum verisinin işlenmesine ancak ilgili kişinin hırsızlık ile alakalı olarak bildirim yapmasıyla başlanabilir. Konum verileri yalnızca yetkili yasal makamlar tarafından hırsızlıkla ilgili yasal soruşturmanın sürdüğü sürece boyunca saklanabilir (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Ayrıca ABVKK, otomobil hırsızlığıyla mücadele amacıyla kişisel verileri işlenecek ilgili kişinin GVKT'nin 13. maddesi doğrultusunda adil, şeffaf ve anlaşılır biçimde aydınlatılmasının yanı sıra veri sorumlusunun ilgili kişiyi aydınlatırken ilgili kişinin erişim hakkını kullanabileceği kişisel verileri ile ilgili kişinin veri taşınabilirliği hakkını kullanabileceği kişisel verileri net olarak ayırmasını önermektedir. Öte yandan otomobil hırsızlığıyla mücadele amacıyla kişisel veri işleme faaliyeti ilgili kişinin açık rızasına dayanılarak gerçekleştirilmekteyse ilgili kişinin açık rızasını geri alabileceğinin ilgili kişiye açıkça ifade edilmesi gerekmektedir. (Avrupa Birliği Veri Koruma Kurulu, 2020a).

Kiralık Otomobillerin Kontrol Panelinde Saklanan Kişisel Veriler

İlgili kişi kiralamış olduğu otomobilde yol tarifi almak, müzik dinlemek, telefon görüşmesi yapmak gibi amaçlarla kontrol paneliyle bağlantı kurabilir. Bu vasıtayla ilgili kişinin konum geçmişi, internet geçmişi, müzik tercihleri, telefon görüşmeleri geçmişi gibi ilgili kişinin profili hakkında fikir verebilecek kişisel verilere ulaşılması mümkündür.

ABVKK tarafından otomobil kiralama şirketleri kontrol paneli vasıtasıyla yapılacak bu kişisel veri işleme faaliyeti bakımından etkin bir kontrole sahip görülerek veri sorumlusu olarak nitelendirilmektedir. ABVKK, kiralama şirketlerini kontrol panelinde yapılan işlemler kapsamında işlenebilecek kişisel verilerin neler olduğu, bu kişisel veri işleme faaliyetinin amacını, kişisel veri toplama faaliyetinin nasıl devre dışı bırakılacağı, kontrol panelinde kişisel verilerin silinmesini sağlayan sil düğmesine nasıl erişileceği hususlarında ilgili kişinin aydınlatılması ile yükümlü kılmaktadır. Ayrıca, kiralama şirketi, otomobilin gizlilik ayarlarının varsayılan modunu mümkün olan en az kişisel veriyi işleyecek biçimde ayarlamakla ve otomobili yeniden kiralamadan önce işlenmiş kişisel verileri otomobilin kontrol panelinden silmekle de yükümlü kılınmıştır (Avrupa Birliği Veri Koruma Kurulu, 2020b).

SONUÇ

Kişisel verilerin korunması hukukunun ortaya çıkmasının altında yatan üç etken *"çeşitli örgütlerce kişisel verilere duyulan gereksinim", "teknolojideki gelişmeler"* ve *"gözetim ve teknolojideki gelişmeler nedeniyle duyulan kaygı"* biçiminde sıralanabilir. (Küzeci, 2021) Bir diğer ifadeyle, kişisel verilerin korunmasını hukukunu tetikleyen etkenlerden biri teknolojiyken bir diğeri ise bu teknolojinin yarattığı endişedir. Kişisel verilerin korunmasının temini için öncelikle kişisel verilerin tanımının yapılması gerekmektedir. Kişisel verinin tanımı, kişisel verileri, cihazların ürettiği diğer verilerden ayırmaya yaramaktadır. Bu sayede kişisel veriler, kişisel verilerin korunması hukukunun korunaklı alanına dahil edilerek belirli normların koruması altında işleme faaliyetlerine tâbi olmaktadır. Bu anlamda, kişisel veri tanımının *"herhangi bir bilgi", "belirli ya da belirlenebilir", "ilişkili olan"* ve *"gerçek kişi"* unsurlarının her biri ve bunların birbirleri ile olan ilişkisi kişisel verilerin korunması hukukuna hazırlamış olduğu zemin bakımından önem arz etmektedir.

Nesnelerin interneti, nesnelerin hem birbirleriyle hem de içinde bulundukları sistemlerle bağlantılı olduğu ağı ifade etmektedir. Dolayısıyla nesnelerin interneti teknolojisine sahip bağlantılı cihazlar veri üretmekte ve bu verileri internet aracılığıyla birbirleriyle veya bağlantılı oldukları sistemle paylaşmaktadır. Aynı ortamda bulunan bağlantılı cihazların sayısı, bu cihazların birbirleri ile veri paylaşımı yaptığı hususu ve bu veriler arasında bulunabilecek kişisel veriler göz önünde bulundurulduğunda söz konusu teknoloji ilgili kişinin mahremiyetine ilişkin bir tehdit niteliği taşımaktadır. Öte yandan, nesnelerin interneti teknolojisine sahip cihazlar vasıtasıyla üretilen ve işlenen tüm verilerin, kişisel veri niteliği taşımadığının altının çizilmesi gerekmektedir. Bu anlamda, kişisel verilerin korunması hukuku kuralları yalnızca mezkûr cihazlar tarafından işlenmekte olan "kişisel" veriler bakımından geçerli olacaktır.

Gelişen teknolojinin bir getirisi olarak nesnelerin interneti teknolojisi ile bağlantılı cihazlar pek çok sektörde ve hayatımızın pek çok alanında yaygınlaşmıştır. Dolayısıyla bağlantılı otomobiller yalnızca belirli zümrelere değil büyük kitlelere ulaşmakta, hayatın içinde yaygın olarak kullanılmakta ve içinde geçirilen zamanın niceliği ve otomobilin yarattığı özel alan algısından dolayı kişisel verilerin işlenmesi için uygun bir ortam sağlamaktadır. Bağlantılı otomobiller vasıtasıyla hem otomobilin kendi içinde yer alan kontrol ünitesi ile hem otomobilin içinde ve dışında yer alan diğer cihazlarla veri paylaşımı yapılabilmesi mümkündür. Bu noktada ifade etmekte fayda görülmektedir ki, nasıl bağlantılı otomobil vasıtasıyla işlenmekte olan verilerin kişisel veri niteliği taşıması için ilgili kişiyi en azından

tanımlanabilir kılması gerekmekte ise bağlantılı otomobil vasıtasıyla işlenmekte olan kişisel verileri elde eden kişileri veri sorumlusu kılan da kişisel veriyi elde edenin ilgili kişiyi tespit edebilme kabiliyetine sahip olmasıdır.

Nihayetinde, bir veri sorumlusunun bağlantılı otomobil vasıtasıyla kişisel veri işleme faaliyeti gerçekleştirildiği tespiti yapıldığında kişisel verileri koruma hukuku kuralları artık uygulama alanı bulacaktır. Bu anlamda, kişisel verilerin korunması hukuku kurallarının doğrudan bağlantılı otomobillere ilişkin olarak kazuistik biçimde kaleme alınmamış olması, bağlantılı otomobiller vasıtasıyla kişisel verilerin işlenmesi faaliyetleri bakımından uygulama alanı bulmayacağı anlamına gelmemektedir. Bununla birlikte, hem bağlantılı otomobilin teknik yapısının karmaşık olması hem de bağlantılı otomobil aracılığıyla sunulmakta olan hizmetin birden fazla veri sorumlusu veya veri sorumlusu ile birlikte pek çok veri işleyen tarafından icra ediliyor olması kişisel verilerin korunması hukuku bakımından detaylı incelemeler ile karar verilmesini gerektirmektedir.

Bu bağlamda, bağlantılı otomobil üreticilerinin, hizmet sağlayıcılarının, bağlantılı otomobiller için ekipman sağlayan üreticilerin kişisel verilerin korunması hukuku bakımından bilinçlendirilmesi insan hakları bakımından önem arz etmektedir. Öte yandan, kişisel verilerinin işlenmesinin söz konusu olduğu tüm sektörlerde olduğu gibi bağlantılı otomobilin teknik yönüyle meşgul olan ve üretim ya da hizmet sunma işini mali kazanç sağlamak üzere icra eden aktörler de kişisel verilerin korunması hukuku kurallarına uymak ile yükümlüdür.

Bu bağlamda ulusal kişisel veri koruma otoritesi sıfatıyla Kişisel Verileri Koruma Kurumu bağlantılı otomobiller ile ilgili olarak da 6698 sayılı Kanunun 20. maddesinde düzenlenen *"Uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak"* ve *"İhtiyaç duyulması hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle işbirliği yapmak"* ile görevlidir. ◆

KAYNAKÇA

- Aksoy, H.C. (2010) Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara: Çakmak Yayınevi.
- Article 29 Data Protection Working Party (29. Madde Çalışma Grubu), (2007). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf adresinde 03.03.2022 tarihinde alınmıştır.
- Artıcle 29 Data Protection Working Party (29. Madde Çalışma Grubu), (2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendatio n/files/2014/wp223_en.pdf, adresinden 23.05.2022 tarihinde alınmıştır.
- Aşıkoğlu, Ş.İ. (2018) Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul: On İki Levha Yayıncılık.
- Develioğlu, H.M. (2017) 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku. İstanbul: On İki Levha Yayıncılık.
- Dülger, M.V. (2019). Kişisel Verilerin Korunması Hukuku. İstanbul: Hukuk Akademisi
- European Data Protection Board. (2020a). Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf adresinden 10.03.2022 tarihinde alınmıştır.
- European Data Protection Board. (2020b). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en adresinden 10.08.2022 tarihinde alınmıştır.

- European Union Agency for Cybersecurity (Avrupa Ağ ve Bilgi Güvenliği Ajansı, 2019). Enisa Good Practices for Security of Smart Cars (2019). https://www.enisa.europa.eu/publications/smartcars adresinden 11.06.2022 tarihinde alınmıştır.
- Federation Internationale De L'automobile (Uluslararası Otomobil Federasyonu). (2017). What EU legislation says about car data-Legal memorandum on connected vehicles and data. https://mycarmydata.eu/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Data-in-Connected-Vehicles-www.pdf adresinden 02.05.2022 tarihinde alınmıştır.
- Federal and State Governments of Germany and the German Association of the Automotive Industry (Alman Otomotiv Endüstrisi Birliği). (2016). Joint statement of the conference of the independent data protection authorities of the Federal and State Governments of Germany and the German Association of the Automotive Industry (VDA) - Data protection aspects of using connected and non-connected vehicles, https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf adresinden 11.09.2022 tarihinde alınmıştır.
- Giusto, D., Iera, A., Morabito, G., Atzori L. (2010) The Internet of Things 20th Tyrrhenian Workshop on Digital Communications. Springer Publishing: Amerika.
- Gündüz, M.Z., Daş, R. (2018). Nesnelerin İnterneti Gelişimi, Bileşenleri ve Uygulama Alanları. Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 24(2), 327-335.
- Henkoğlu, T. (2015) Bilgi Güvenliği ve Kişisel Verilerin Korunması. Ankara: Yetkin Hukuk Yayınları.
- IDC Corporate USA, (2016). Responsibility for Vehicle Security and Driver Privacy in the Age of the Connected Car. https:// www. veracode. com/sites/default/ files /Resources / Whitepapers /idc-veracode-connected-car-research-whitepaper.pdf adresinden 23.03.2022 tarihinde alınmıştır.
- IoT Allience Australia (Avusturalya Nesnelerin İnterneti İttifakı). (2016). Internet of things security guideline. https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf adresinden 05.04.2022 tarihinde alınmıştır.

◊ Kişisel Verileri Koruma Kurulu. (2019). Ölü kişilerin verilerine yakınlarının erişim talebi hakkında" Kişisel Verileri Koruma Kurulunun 18/09/2019 tarihli ve 2019/273 sayılı karar özeti. https://www.kvkk.gov.tr/Icerik/6710/2019-273 adresinden 14.07.2022 tarihinde alınmıştır.

◊ Kişisel Verileri Koruma Kurumu. (2019). Madde ve gerekçesi ile Kişisel Verilerin Korunması Kanunu (bilgi notu) ve kişisel verilerin korunmasına ilişkin terimler sözlüğü. https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi Kanunu- Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu adresinden 20.08.2022 tarihinde alınmıştır.

◊ Korkmaz, İ. (2017). Kişisel Verilerin Ceza Hukuku Kapsamında Korunması. Ankara: Seçkin Yayıncılık.

◊ Küzeci, E. (2021). Kişisel Verilerin Korunması, İstanbul: On İki Levha Yayıncılık.

◊ Özdemir, A., Naralan Nursaçan, M. N., Nursaçan, İ.C. (2018). 2014 - 2018 Yılları Arasında Nesneleri İnterneti (IoT) Üzerine Bir Literatür Taraması, SOSYAL Bilimler Araştırmaları Dergisi, 1(2), 1-22, https://dergipark.org.tr/tr/pub/banusad/issue/41748/485233 adresinden alınmıştır.

◊ Özkan, O. (2020). Kişisel Verilerin Korunması. Ankara: Yetkin Yayınları.

◊ Pen Test Partners Security Consulting and Testing Services (Sızma Testi Ortakları Güvenlik Danışmanlığı ve Test Hizmetleri). (t.y.). Hacking the Mitsubishi outlander PHEV hybrid. https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/ adresinden 01.03.2022 tarihinde alınmıştır.

◊ Topaloğlu, M., Tekkanat. E., Malakçı, G. (2019). Akıllı Cihaz ve İnsan Etkileşimi: Nesnelerin İnterneti, Ege Eğitim Teknolojileri Dergisi, (3), 11-19. https://dergipark.org.tr/tr/pub/eetd/issue/47459/480158 adresinden erişilmiştir.

◊ Turak Y. (2015). Nesnelerin interneti ve güvenliği. http://www.yigitturak.com/wp-content/uploads/IoTGuvenligi.pdf adresinden 24.06.2022 tarihinde alınmıştır.

◊ Yan, Z., Zhang, P., Vasilakos A. (2014). A survey on trust management for Internet of Things, Journal of Network and Computer Applications, (42), 120-134. https://www.sciencedirect.com/science/article/abs/pii/S1084804514000575 adresinden alınmıştır.

◊ Yılmaz, S., Çavuşoğlu, G.F. (2020). Kişisel Verileri Koruma Hukuku. Ankara: Yetkin Yayınları.

◊ Yüzbaşı Topaz, F. (2021). Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması, (Yayımlanmamış Doktora Tezi), Trabzon Üniversitesi Lisansüstü Eğitim Enstitüsü, Trabzon.

KİŞİSEL VERİLERİN KORUNMASINA

UZMAN BAKIŞ

UZMANLIK TEZLERİ DERLEME ÇALIŞMASI

Adres: Nasuh Akar Mahallesi
1407. Sokak No:4
Balgat Çankaya/ANKARA

Bu çalışmada yer alan fikir ve görüşler
Kurumumuz görüşünü yansıtmamakta olup
yazarların görüşlerini yansıtmaktadır.

KİŞİSEL VERİLERİ KORUMA KURUMU

NASUH AKAR MAH. 1407. SOK.
NO.4 06520 ÇANKAYA / ANKARA
TEL: 0312 216 50 00
WWW.KVKK.GOV.TR

KVKKURUMU