Kişisel Verileri Koruma Kurumu

BÜLTEN

Aralık 2024 - Şubat 2025 Sayı:7

108 SAYILI SÖZLEŞME VE VERİ KORUMA GÜNÜ

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Kişisel Verileri Koruma Kurumu
KVKK Bülten
www.kvkk.gov.tr
Sayı:7
Kişisel Verileri Koruma Kurumu
Adına İmtiyaz Sahibi
Prof. Dr. Faruk BİLİR

Yönetim Yeri
Nasuh Akar Mahallesi 1407. Sokak
No:4 Balgat Çankaya/ANKARA
Tel: (312) 216 50 00

VERİ KORUMA HUKUKUNUN TEMELİ: 108 SAYILI SÖZLEŞME

Hukukun, bireyler arasındaki ilişkileri olduğu kadar toplumlar arası düzeni sağlamak için de vazgeçilmez bir unsur olduğu, birçok düşünür tarafından vurgulanmıştır. Bu bağlamda, hukukun toplumla iç içe olduğu şu sözle ifade edilmiştir:

"Nerede toplum varsa, orada hukuk vardır."

Toplumlar arası hukuk düzeninin temel taşlarından biri uluslararası sözleşmelerdir. Bu sözleşmelerden biri de kişisel verilerin korunmasında uluslararası açıdan milat olarak kabul edilen *"Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"*dir. Kısa adıyla *"108 Sayılı Sözleşme"* olarak anılan bu Sözleşme, 28 Ocak 1981 tarihinde Strazburg'ta imzaya açılmıştır.

Türkiye, 108 Sayılı Sözleşme'yi ilk imzalayan ülkelerden biri olmuştur. Dolayısıyla, ülkemizin kişisel verilerin korunması konusundaki serüveninin, bu Sözleşme'nin imzalanmasıyla başladığını söyleyebiliriz. Ancak, Sözleşme ile ilgili asıl somut adım, 2016 yılında kişisel verilerin korunmasına yönelik gerçekleştirilen hukuki düzenlemeler kapsamında, Sözleşme'nin onaylanması hakkında Karar'ın 17 Mart 2016 tarihinde Resmî Gazete'de yayımlanmasıyla atılmıştır. Sözleşme'nin iç hukukumuza dahil edilmesi, ülkemizin Avrupa Konseyi çerçevesinde oluşturulan ortak hukuk sistemine kişisel verilerin korunması alanında da dahil olmasını sağlamıştır.

108 Sayılı Sözleşme'nin en önemli özelliği, kişisel verilerin işlenmesi konusunda bağlayıcı nitelikteki ilk uluslararası sözleşme olmasıdır. 108 Sayılı Sözleşme, günümüz veri koruma hukukunun temelini teşkil etmektedir. Sözleşme, kişisel verilerin korunması açısından önemli güvenceler getirmiş ve bu alanda uygulanacak temel ilkeler ile asgari veri koruma standartlarını belirlemiştir. Söz konusu Sözleşme, ilkelere dayalı yapısı sayesinde 44 yıldır geçerliliğini devam ettirmektedir. Bununla birlikte, teknolojide meydana gelen güncel gelişmeler ışığında Sözleşme zaman içerisinde modernize edilmiş ve 108+ olarak güncellenmiştir.

Sözleşme'nin imzaya açıldığı 28 Ocak günü, 2006 yılında Avrupa Konseyi tarafından *"Veri Koruma Günü"* olarak ilan edilmiştir. Veri Koruma Günü, ülkemizde Kurumumuz öncülüğünde kutlanmaktadır.

KVKK Bülten'in yedinci sayısını *"108 Sayılı Sözleşme ve Veri Koruma Günü"* konusuna ayırarak, hem 108 Sayılı Sözleşme'nin kişisel verilerin korunması alanındaki yol gösterici rolünü hem de Veri Koruma Günü'nün simgelediği bilinç ve farkındalığın önemini vurgulamayı amaçlıyoruz.

Bülten'in tüm okuyuculara faydalı olmasını diliyorum.

Prof. Dr. Faruk BİLİR

Kişisel Verileri Koruma Kurumu Başkanı

Dr. Öğr. Üyesi Alper IŞIK*
İstanbul Medeniyet Üniversitesi Hukuk Fakültesi
Genel Kamu Hukuku Anabilim Dalı Öğretim Üyesi

KİŞİSEL VERİLERİN KORUNMASINDA ÖNCÜ BİR DÜZENLEME: AVRUPA KONSEYİ'NİN 108 SAYILI SÖZLEŞMESİ

108 Sayılı Sözleşme'nin Ortaya Çıkışı

Kişisel verilerin korunması bugün dünyada birçok ülkede kanuni bir güvenceye sahiptir. Ancak geçmişe gittiğimizde konunun bağlayıcı olarak bir hukuki düzleme kavuşmasının ilk olarak bir uluslararası sözleşmeyle olduğunu görürüz. Sonrasında başta Avrupa kıtası olmak üzere birçok ülke kendi müstakil veri koruma kanunlarını yapmıştır. Bütün bu ulusal kanunların arkasında ise Avrupa Konseyi'nin 28 Ocak 1981 tarihinde ortaya çıkarmış olduğu "Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına Dair Sözleşme" (kısaca 108 sayılı Sözleşme) vardır. Bu sözleşme, kişisel verilerin korunmasına yönelik uluslararası düzeyde bağlayıcı ilk metin olup taraf devletlere belirli hukuki yükümlülükler getirmektedir.

Türkiye de 108 sayılı Sözleşme'yi 28 Ocak 1981 tarihinde imzalamış, 2 Mayıs 2016 tarihinde uygun bulmuş ve 1 Eylül 2016 tarihinde Resmî Gazete'de yayınlayarak yürürlüğe koymuştur[1]. Sözleşme her ne kadar bir Avrupa Konseyi sözleşmesi olsa da Konsey ülkelerinin dışında da uygulama alanı bulmaktadır. 108 sayılı Sözleşme hazırlanırken Avrupa Konseyi dışından ülkelerin de katılma ihtimaline binaen, herhangi bir coğrafi sınır içermeyen bir isim tercih edilmiştir. Bu öngörünün haklılığı 2013 yılında kendini göstermiş ve Uruguay bu tarihte 108 Sayılı Sözleşme'ye taraf olmuştur. Devamında ise Arjantin, Yeşil Burun, Mauritius, Meksika, Fas, Senegal ve Tunus, Sözleşme'yi imzalamış ve yürürlüğe koymuştur. Güncel olarak Sözleşme'ye 55 ülke taraftır.

Sözleşmenin temel amacı, kişisel verilerin işlenmesi sürecinde bireylerin temel hak ve özgürlüklerini, özellikle de mahremiyet hakkını korumaktır. Sözleşme, kamu ve özel sektörde gerçekleştirilen kişisel veri işleme faaliyetlerini kapsamakta olup veri sahiplerine belirli haklar tanımaktadır. Kapsam konusunda özellikle belirtmek gerekir ki Sözleşme, kişisel verilerin otomatik işlenmesi hallerinde bireylerin korunmasını düzenlemektedir. Dolayısıyla otomatik olmayan yollarla veri işlenmesi halinde 108 sayılı Sözleşme uygulama alanı bulmayacaktır.

Temel Prensipler ve Güvenceler

108 sayılı Sözleşme, kişisel verilerin korunmasına dair birtakım temel prensipleri getirmektedir. Bunlardan ilki verilerin hukuka uygun ve adil bir şekilde elde edilmesidir. Sonrasında verilerin işlenmesine ilişkin belirli kriterler getirilmiştir. Buna göre veriler, belirli, meşru ve açık amaçlar doğrultusunda toplanmalı ve bu amaçlara uygun olarak işlenmelidir. Aynı zamanda veri minimizasyonu ilkesi de 108 sayılı Sözleşme'de yer alan bir ilkedir. Buna göre gereksiz veri işlenmesinin önüne geçilerek yalnızca gerekli olan verilerin işlenmesi sağlanmalıdır. 108 sayılı Sözleşme'nin getirdiği bir diğer ilke ise verilerin doğruluğuna ilişkindir. Verilerin doğru ve güncel olmasına önem veren 108 sayılı Sözleşme, yanlış veya eksik verilerin düzeltilmesi veya silinmesinin sağlanmasını da hüküm altına almaktadır. Son olarak verilerin amaca uygunluk için gerekli olan süreyi aşmayacak şekilde saklanması bir ilke olarak 108 sayılı Sözleşme'de yer almaktadır.

108 sayılı Sözleşme özel nitelikli kişisel verileri de tanımlar ve bunların otomatik işleme tabi tutulmasını yasaklar. 108 sayılı Sözleşme'ye göre bu veriler; ırk kökeni, siyasi düşünce, dini ve diğer inançlar, sağlık veya cinsel hayata ilişkin veriler ve ceza mahkumiyetine ilişkin bilgilerdir. Uygun güvenceler sağlanmadıkça bu veriler işlenememektedir.

108 sayılı Sözleşme'nin getirmiş olduğu bir diğer güvence ise ilgili kişinin haklarına yöneliktir. Buna göre herkes; kişiler verilerine ilişkin temel bilgileri öğrenme, bilgileri anlaşılır bir formatta alma, verileri düzeltme ve sildirme, bu talepleri karşılanmazsa da bir başvuru yolundan yararlanma hakkına sahiptir.

108 sayılı Sözleşme otomatik dosyalarda tutulan kişisel verilerin kaza sonucu veya izinsiz olarak imhasına, kaybolmasına ya da başkasının eline geçmesine, değiştirilmesine karşı uygun önlemlerin alınacağını düzenlemektedir. Ancak 108 sayılı Sözleşme bu noktaya kadar belirttiği yükümlülükleri yaptırıma bağlama konusunda zayıf kalmaktadır. Bu yüzden 108 sayılı Sözleşme'nin 10. maddesi yaptırımlar konusunu ele almaktadır. Maddeye göre taraf devletler 108 sayılı Sözleşme'de yer verilen temel ilkelere geçerlilik sağlayan iç hukuk kurallarına aykırı davranılması halinde uygun yaptırımlar ve başvuru yolları getirmelidir.

108 sayılı Sözleşme'nin üçüncü bölümü sınır ötesi veri akışı konusunu düzenlemektedir. Bu madde, verilerin ulusal sınırların ötesine aktarımına ilişkin esasları belirlemektedir. Taraf devletler arasındaki kişisel veri aktarımlarında yalnızca özel hayatın korunması amacıyla bir kısıtlamaya gidilmesi mümkün değildir. Dolayısıyla taraf devlet bu tür bir gerekçeyle verilerin diğer taraf devletlere aktarılmasını yasaklayamaz ya da özel bir izne tabi kılamaz. Veri akışının yasaklanması ya da özel izne tabi olabilmesi, 108 sayılı Sözleşme'ye göre iki durumda mümkündür. İlk durum ülkenin mevzuatının belli kişisel veri kategorileri için özel düzenlemeler içermesi halinde diğer tarafın eşdeğer bir koruma sağlamıyor olmasıdır. İkinci durum ise transferin yapıldığı taraf devletin mevzuat boşluklarından faydalanmak amacıyla bu devlet üzerinden taraf olmayan bir devlete aktarım yapılması halidir. Dolayısıyla bu tür transferleri engellemek amacıyla taraf devletler arasında veri aktarımı yasaklanabilir ya da özel bir izne tabi kılınabilir. Bunun dışındaki durumlarda yasaklama ya da özel bir izne tabi kılmak 108 sayılı Sözleşme'ye aykırı olacaktır.

* alper.isik@medeniyet.edu.tr, Orcid Id: 0000-0002-3784-8297.

1 Güncel durum için bknz. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 Erişim Tarihi: 07.03.2025.

Türkiye ve 108 Sayılı Sözleşme

Türkiye, Avrupa Konseyi üyesi olarak 108 sayılı Sözleşme'ye taraf ülkeler arasındadır. 108 sayılı Sözleşme'nin yürürlüğe girmesi 6698 sayılı Kişisel Verilerin Korunması Kanunu'yla (KVKK) aynı döneme denk gelmektedir. Hatta Türkiye 108 sayılı Sözleşme'de tanınan hakları daha da genişletmek adına, tanıma kanununun beyanlar kısmında otomatik olmayan yollarla işlenen veriler açısından da 108 sayılı Sözleşme'nin uygulanacağını ifade etmiştir[2]. Türk anayasal sistemi açısından bakıldığında 108 sayılı Sözleşme bir uluslararası sözleşmedir. Anayasamızın 90. maddesine göre usulüne göre yürürlüğe konulmuş uluslararası andlaşmalar kanun hükmündedir. Dolayısıyla 108 sayılı Sözleşme, Türk hukuku açısından kanun hükmünde bir düzenlemedir. Üstelik konusunun temel hak ve özgürlüklere ilişkin olmasından dolayı Anayasa'nın 90/5 maddesi uyarınca kanunlarla çatışma halinde esas alınacak bir uluslararası andlaşma vasfına sahiptir. Dolayısıyla ilgili Sözleşme Türk hukuku açısından da büyük bir önem taşımaktadır.

Reform Çalışmaları

Sözleşme'nin uzun zaman önce hazırlanması ve teknolojik gelişmeler neticesinde kat edilen mesafe bir reform ihtiyacı doğurmuştur. Ayrıca Sözleşme hazırlandığı dönemde Avrupa'da birçok ülkede veri koruma hukukuna ilişkin düzenleme mevcut değildir. Ancak günümüzde özellikle AB ülkeleri açısından GDPR'ın yürürlüğe girmesi ve ülke mevzuatlarında düzenleme yapılması Sözleşme'nin önemini azaltmıştır. Bu yüzden 2018 yılında Sözleşme'nin modernize edilmiş versiyonu olan 108+ Sözleşmesi imzaya açılmıştır. 108+ Sözleşmesi, teknolojik gelişmeler ışığında sözleşmenin güncellenmesini sağlamış ve kişisel verilerin işlenmesine yönelik ek güvenceler getirmiştir. Ancak bu düzenleme yeterli sayıda ülke tarafından onaylanmadığı için henüz yürürlüğe girmemiştir.

Sonuç

Avrupa Konseyi'nin 108 sayılı Sözleşmesi, kişisel verilerin korunması alanında temel bir uluslararası hukuki çerçeve sunmaktadır. Hazırlandığı dönemde öncü bir düzenleme olarak nitelendirilen 108 sayılı Sözleşme, taraf ülkelerin veri koruma kanunlarını yürürlüğe koyma sürecinde bir rehber işlevi görmüştür. Türkiye ise 108 sayılı Sözleşme'ye taraf olarak kişisel verilerin korunması konusundaki çabasını ortaya koymaktadır. Sözleşme ile 6698 sayılı KVKK'nın yakın zamanlarda yürürlüğe girmesi iki düzenleme arasındaki etkilenmeyi göstermesi açısından da önemlidir. 108 Sayılı Sözleşme'nin Avrupa Birliği ülkelerinde GDPR'ın yürürlüğe girmesiyle önemi azalsa da 108+ Sözleşmesi ile başlanan reform çalışmaları sürmektedir.

2 https://www.resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf Erişim Tarihi: 08.03.2025.

KİŞİSEL VERİLERİN OTOMATİK İŞLEME TABİ TUTULMASI KARŞISINDA BİREYLERİN KORUNMASI SÖZLEŞMESİ DANIŞMA KOMİTESİ

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi Danışma Komitesi (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [T-PD]) Avrupa Konseyi bünyesinde 1981 tarihli 108 No'lu Sözleşme (Convention 108) uyarınca oluşturulmuş bir danışma komitesidir. Komite yalnızca Avrupa Konseyi değil uluslararası alanda kişisel verilerin korunmasına yönelik uzmanlaşmış organların en önemlileri arasında sayılmaktadır. Bu bakımdan Komite, kişisel verilerin korunmasına yönelik standartları belirleme ve geliştirme konusunda aktif rol oynamakta ve uluslararası veri koruma politikalarının şekillendirilmesine katkıda bulunmaktadır.

Komitenin görevleri arasında Avrupa Konseyi himayesinde kabul edilen 108 Sayılı Sözleşme'nin uygulanmasını izleme ve yorumlanmasının yanı sıra kişisel verilerin korunmasına yönelik yeni politikalar ve rehber ilkeler geliştirme, Sözleşme tarafı ülkeler arasında iş birliğini teşvik etme ve veri koruma standartlarını uyumlu hale getirme, uluslararası iş birliğini güçlendirme, küresel düzeyde veri koruma düzenlemelerinin uyumlaştırılmasına katkıda bulunma ve ayrıca Avrupa Konseyi'nin ilgili organlarına danışmanlık sağlama gibi hususlar da bulunmaktadır.

Komite bu görevleri yerine getirirken üye devletlere yönelik veri koruma uygulamaları hakkında rehberler yayınlamakta, kişisel verilerin korunması konusunda farkındalığı artırmak için çeşitli etkinlikler düzenlemekte ve Avrupa Birliği, Birleşmiş Milletler ve diğer uluslararası kuruluşlarla ortak projeler yürütmekte olup bunların yanında her yıl iki kez olmak üzere üye devletlerin temsilcilerinin katılımlarıyla Fransa'nın Strazburg şehrinde yer alan Avrupa Konseyi ev sahipliğinde Komite toplantıları düzenlenmektedir.

Söz konusu toplantılara ülkemizi temsilen Kurumumuz tarafından da katılım sağlanmaktadır. Bu kapsamda sınır ötesi kişisel veri aktarımı konusu başta olmak üzere üye devletlerin 108 Sayılı Sözleşmeye uyumu, yapay zekâ ve büyük veri kullanımının mahremiyete etkileri gibi çeşitli alanlarda yapılan çalışma ve toplantılara Kurumumuz tarafından katkı sunulmaktadır.

KİŞİSEL VERİLERİN OTOMATİK İŞLEME TÂBİ TUTULMASI KARŞISINDA BİREYLERİN KORUNMASINA DAİR SÖZLEŞMEYİ DEĞİŞTİREN 223 SAYILI PROTOKOL

108 Sayılı Sözleşme, yeni bilgi iletişim teknolojilerinin getirdiği mahremiyet sorunlarını ele almak ve sözleşmenin etkili bir biçimde uygulanabilmesi amacıyla 18 Mayıs 2018 tarihinde Avrupa Konseyi Bakanlar Komitesinin 128. oturumunda kabul edilen Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına Dair Sözleşmeyi Değiştiren 223 Sayılı Protokol (108 +) ile güncellenmiştir[1].

Hâlihazırda 33 ülke tarafından onaylanan[2] 108+, yeni güvence yollarının 108 Sayılı sözleşmeye entegre edilmesi ile modern bir yapıya kavuşmuştur. Yapılan güncellemeler ile sınırlar arası veri akışı kolaylaşırken sözleşmenin Avrupa Birliği mevzuatı da dahil olmak üzere dünya genelindeki normatif çerçevelerle uyumlu olması hedeflenmektedir.

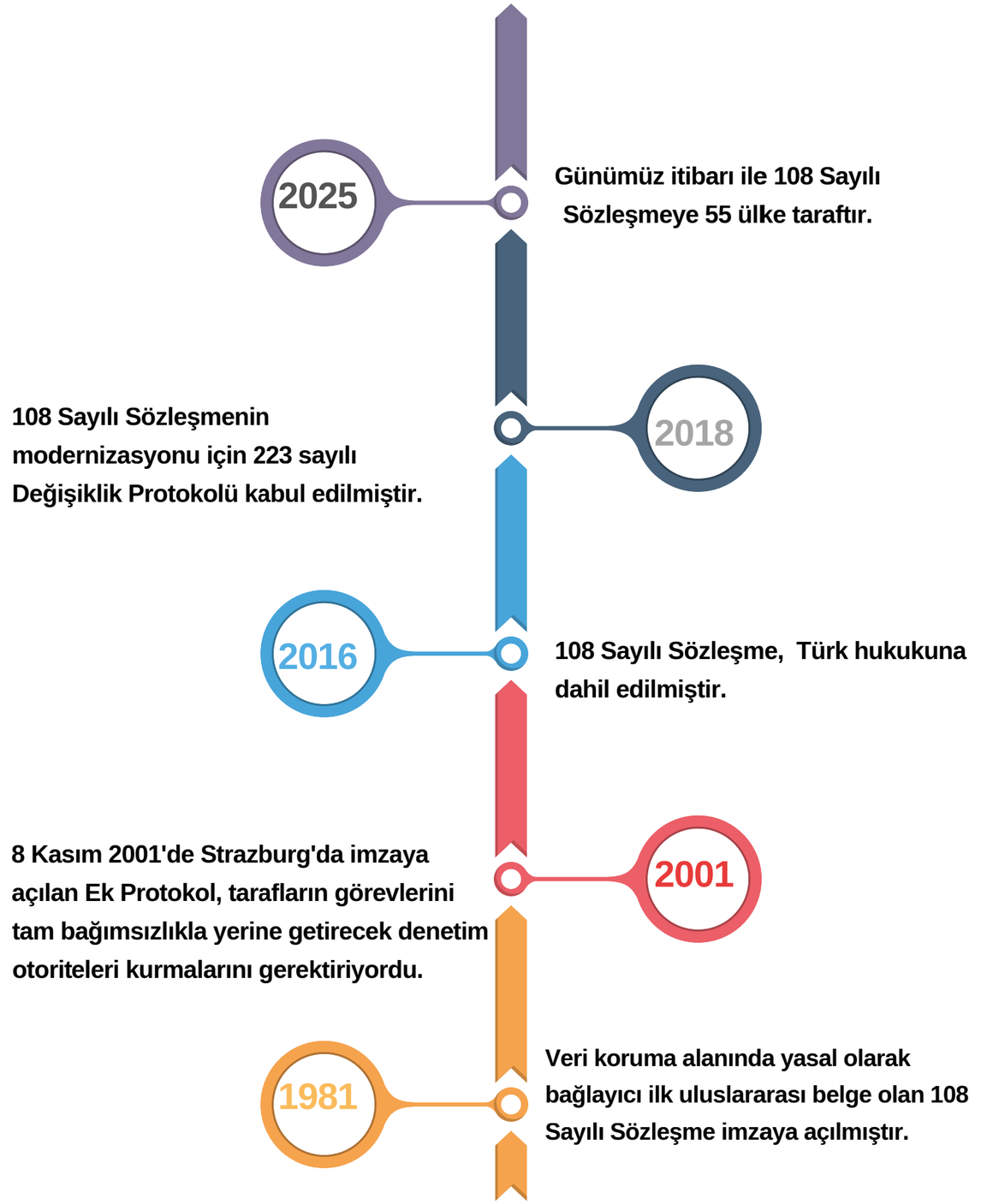
Yapılan güncellemeler ile kısaca[3];

- Veri koruma ilkeleri güçlendirilerek orantılılık ve veri minimizasyonu ilkelerinin altı çizilmektedir.
- Özel nitelikli kişisel verilerin kapsamı genişletilerek genetik ve biyometrik veriler, sendika üyeliği ve etnik köken bilgileri de bu sınıfa dahil edilmektedir.
- Veri güvenliğine ilişkin hususlar açısından, herhangi bir güvenlik ihlalinin taraflarca gecikmeksizin bildirilmesi yükümlülüğü getirilmektedir.
- Veri sorumlularının kimlikleri ve işleme faaliyetlerine ilişkin konularda ilgili kişileri bilgilendirmesi hususu taraflarca garanti edilmektedir.
- Özellikle algoritmik karar alma bağlamında ilgili kişilere dijital çağda verileri üzerinde daha fazla kontrole sahip olmaları için yeni haklar tanınmaktadır.
- Hesap verilebilirlik kapsamında veri sorumlularının yükümlülükleri genişletilmektedir.
- Tasarımdan itibaren mahremiyet ilkesinden bahsedilmektedir.
- Veri koruma ilkelerinin, ulusal güvenlik gerekçeleri de dahil olmak üzere, Sözleşme tarafından belirlenen koşullara tabi olarak olası istisnalar ve kısıtlamalarla ve her durumda bağımsız ve etkili inceleme ve denetimle tüm işleme faaliyetlerine uygulanması gerekmektedir.
- Sınır ötesi veri akışlarının rejimi açık bir biçimde belirlenmektedir.
- Veri koruma otoritelerinin yetkileri ve bağımsızlığı güçlendirilerek uluslararası iş birliğinin temeli güçlendirilmektedir.

1 128th Session of the Committee of Ministers, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETSNo.108), 18.05.2018, https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680089ff4e%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}.

2 Anlaşmayı onaylayan imzacı ülkeler için bkz. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223, E.T. 07.03.2025.

3 Modernisation of the Data Protection "Convention 108", https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet, E.T. 07.03.2025.



VERİ KORUMANIN 44 YILI: MAHREMİYET PERSPEKTİFİNDEN YAPAY ZEKÂ ÇAĞI ETKİNLİĞİ

28 Ocak Veri Koruma Günü etkinlikleri kapsamında, Kurumumuz ve Bartın Üniversitesi iş birliğinde, "Veri Korumanın 44 Yılı: Mahremiyet Perspektifinden Yapay Zekâ Çağı" Konferansı gerçekleştirildi. Adalet Bakanımız Sayın Yılmaz TUNÇ'un katılımıyla düzenlenen "Veri Korumanın 44 Yılı: Mahremiyet Perspektifinden Yapay Zekâ Çağı" adlı etkinlik alanında uzman isimleri bir araya getirdi.

Konferansın açılış konuşmasını Adalet Bakanımız Sayın Yılmaz TUNÇ gerçekleştirdi.

Bakan TUNÇ, yapay zekânın hukuki altyapısı üzerine çalıştıklarını açıkladı

Dijital çağda yapay zekâ teknolojilerinin dönüştürücü etkisi olduğunun altını çizen Bakan TUNÇ, "Yeni teknolojiler başta hukuk, sağlık, eğitim, güvenlik olmak üzere her sektörde farklı uygulamalar ve yazılımlarla hayatımızı kolaylaştırmaktadır. Yapay zekâ teknolojileri, sunduğu bu imkânlar yanında bazı riskleri de beraberinde getirirken kişisel verilerin güvenliğini sağlama konusundaki sorumluluğumuzu da artırmaktadır. Bu anlayışla 28 Ocak Veri Koruma Günü kapsamında Kişisel Verileri Koruma Kurumu iş birliğiyle dijital izler olan verilerimizin korunması konusunun Bartın Üniversitesi ev sahipliğinde ele alınmasını oldukça önemli buluyorum. Programdan elde edilecek çıktıların yapay zekâ teknolojisi üzerine geliştirilecek mevzuata ışık tutacağına yürekten inanıyorum" ifadelerini kullandı.

"Yapay Zekâ Bilim Komisyonu kuruyoruz"

Adalet Bakanlığı bünyesinde 'Yapay Zekâ Bilim Komisyonu' kuracaklarını da açıklayan Bakan TUNÇ, "TBMM'de 2 Ekim 2024 tarihinde alınan kararla bir araştırma komisyonu kuruldu. Bu komisyon yapay zekânın kazanımlarına yönelik atılacak adımların belirlenmesi, bu alanda hukuki altyapının oluşturulması ve yapay zekâ kullanımının barındırdığı risklerin önlenmesine ilişkin tedbirlerin belirlenmesi yönünde çalışmalar yapıyor. Biz de yapılacak bu çalışmalara teknik destek vereceğiz. Bu amaçla Adalet Bakanlığımız bünyesinde 'Yapay Zekâ Bilim Komisyonu' kuruyoruz. Bu komisyon, hem hukuki altyapıyı destekleyecek çalışmalar yapacak hem de akademik araştırmalara katkıda bulunacak" diye konuştu.

"Yapay zekâ çağında kişisel verilerin işlenmesi hukuka uygun olmalıdır"

Veri korumanın temelinin bireyin mahremiyetine dayandığına işaret eden Kurum Başkanımız Faruk BİLİR, "Mahremiyet yalnızca bir hak ve özgürlük değil, insanın varlığını anlamlandırma sürecinin ayrılmaz bir parçasıdır. Mahremiyet ve buna bağlı olarak kişisel verilerin korunması insanlığın ortak konusudur. Ülkemiz ise bu bağlamda 28 Ocak 1981 tarihinde imzaya açılan veri korunması sözleşmesini imzalayan ilk ülkelerden biri olmuştur.

Günümüzde kişisel verilerin işlenmesi hayatın bir gerçeğidir. Ancak verilerin işlenmesi hukuka uygun olarak olmalı, yapay zekânın bu süreçlerdeki etkisi de bu gibi etkinliklerle topluma anlatılmalıdır" şeklinde konuştu.

"Kişisel verilerin korunmasında akademik çalışmalar önemli rol oynamaktadır"

Yapay zekânın yeni olanaklarla birlikte mahremiyet ve veri güvenliği konularında köklü değişiklikleri beraberinde getirdiğini vurgulayan Bartın Üniversitesi Rektörü Orhan Uzun ise "Yapay zekâ teknolojilerinin hayatımıza daha fazla dâhil olduğu günümüzde, kişisel verilerin korunması, büyük bir toplumsal sorumluluk haline gelmiştir. Bu alanda akademik çalışmaların ve kurumlar arası iş birliklerinin yapılması önemli rol oynamaktadır. Bugün Kişisel Verileri Koruma Kurumu ile birlikte düzenlediğimiz bu panel, hem veri koruma konusunda hem de yapay zekânın mahremiyet üzerindeki etkileri noktasında değerli bir çalışma olacaktır" dedi.

İlk oturumda yapay zekânın hukuki ve etik temelleri konuşuldu

Açılış konuşmalarının ardından geçilen oturumun moderatörlüğünü yapan Türkiye Adalet Akademisi Başkanı Bekir Altun "Kişisel verilerin mahremiyetini koruma gerekliliği hukuk, teknoloji ve etik arasındaki dengede yeni sorumluluklar getirmektedir. Bu dengeyi program boyunca derinlemesine tartışarak geleceğe ışık tutacak fikirler ve çözüm önerilerini ele alacağız. Yapay zekâ gibi çığır açıcı bir teknolojinin hukuki ve etik temellerini konuşmak geleceğimizi şekillendirmek açısından kritik bir öneme sahiptir" ifadelerini kullandı.

Yapay zekâ sistemlerinde veri güvenliğinin hukuki boyutunun konuşulduğu oturumda ilk olarak Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Birim Müdürü Dr. Atilla Aydın "Ulusal Yapay Zekâ Stratejimiz ve Yapay Zekâda Türkiye'nin Gelecek Vizyonu" hakkında var olan çalışmalar ile gelecekte yapılması planlanan uygulamalar hakkında bilgilendirmelerde bulundu. KVKK Hukuk İşleri Dairesi Başkanı Ezgi Ergüneş Duran "Yapay Zekânın Hukuki Sorumluluğu", KVKK Uzmanı Ezgi Turgut Bilgiç ise "Yapay Zekâ Teknolojilerinde Kişisel Verilerin Otomatik İşleme Tabi Tutulması ve 108 Sayılı Sözleşme"ye dair detayları aktardı.

İkinci oturumda dijital çağdaki güncel yaklaşımlar ele alındı

Bartın Üniversitesi Rektör Yardımcısı Prof. Dr. Mehmet Zahmakıran'ın moderatörlüğünde gerçekleştirilen ikinci oturumda, yapay zekâ teknolojisinde güncel yaklaşımlar farklı açılardan değerlendirildi. Bartın Üniversitesi Fen Fakültesinden Prof. Dr. Ramazan Yılmaz "Üretken Yapay Zekâ ve Mahremiyet: Güçlükler ve Fırsatlar" başlıklı sunumunda dünyadaki son gelişmeler üzerinden bir değerlendirme yaparak Türkiye'deki yapay zekâ çalışmalarını anlattı.

Bartın Üniversitesi Mühendislik, Mimarlık ve Tasarım Fakültesinden Dr. Öğr. Üyesi Onur Çakırgöz "Yapay Zekâ Sistemlerinde Algoritmik Şeffaflık ve Hesap Verebilirlik" konusuna dikkat çekti. Aynı fakülteden Doç. Dr. Eyüp Burak Ceyhan "Yapay Zekâ Kullanımının İnsan Hakları ile İlişkisi ve Hukuki Boyutu", Dr. Öğr. Üyesi Ümit Demirbaga ise "Üretken Yapay Zekânın Temelleri: Teknolojiler ve Modeller" konularını kapsamlı bir şekilde ele aldı.

* Avrupa Veri Koruma Kurulu (EDPB), yapay zekâ modellerinin geliştirilmesi ve yerleştirilmesinde (deployment) kişisel verilerin kullanımına ilişkin 28/2024 sayılı Görüşünü yayımladı[1]. İrlanda Veri Koruma Otoritesi'nin talebi üzerine hazırlanan bahse konu Görüş kapsamında;

  - Yapay zekâ modellerinin ne zaman ve nasıl anonim olarak kabul edilebileceği,
  - Meşru menfaatin, yapay zekâ modellerinin geliştirilmesi ve kullanılmasında hukuki dayanak olarak kullanılıp kullanılamayacağı ve ne şekilde kullanılabileceği,
  - Hukuka aykırı şekilde işlenen kişisel veriler kullanılarak geliştirilen yapay zekâ modellerine ne olacağı konuları ele alınmaktadır.

Anonimlik konusunda; bir yapay zekâ modelinin anonim olup olmadığının veri koruma otoriteleri tarafından her bir vaka özelinde değerlendirilmesi gerektiği ifade edilmektedir. Diğer yandan bir modelin "anonim" kabul edilebilmesi için; (1) modelin geliştirilmesinde kullanılan verilerle ilişkili bireylerin doğrudan veya dolaylı olarak belirlenmesinin ve (2) sorgular yoluyla modelden bu kişisel verilerin çıkarılabilmesinin oldukça düşük bir ihtimal olmasının arandığı belirtilmektedir. Bu çerçevede Görüş metninde, anonimliği ortaya koymak için kullanılabilecek yöntemlere dair bağlayıcı olmayan ve sınırlı sayma şeklinde gösterilmeyen bir liste de sunulmaktadır.

1 https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en, 18.12.2024.

Meşru menfaat konusunda ise yapay zekâ modellerinin geliştirilmesi ve yerleştirilmesi için kişisel verilerin işlenmesinde meşru menfaatin uygun bir yasal dayanak olup olmadığını değerlendirmek için veri koruma otoriteleri tarafından dikkate alınması gereken genel hususlar açıklanmaktadır. Meşru menfaatin uygun bir yasal dayanak olarak kullanılmasının değerlendirmesine yardımcı olmak üzere bir denge testi önerilmekte ve bu kapsamda meşru bir menfaatin varlığı, bu menfaatin sağlanması için işlemenin kesinlikle gerekli olması ile bu menfaatin bireylerin hak ve özgürlükleriyle dengelenmesinin arandığı belirtilmektedir.

Diğer yandan Görüş kapsamında bireylerin, kişisel verilerinin belirli amaçlarla kullanılmasını makul bir şekilde bekleyip bekleyemeyeceğini değerlendirmek üzere bir dizi kriter sunulmakta olup bu kriterler arasında;

- Kişisel verilerin kamuya açık olup olmadığı,
- Birey ile veri sorumlusu arasındaki ilişkinin niteliği,
- Hizmetin niteliği,
- Kişisel verilerin toplandığı bağlam,
- Verilerin toplandığı kaynak,
- Modelin olası diğer kullanımları,
- Bireylerin, kişisel verilerinin çevrim içi olduğunun farkında olup olmadığı

gibi unsurlar sayılmaktadır.

Ayrıca denge testinin, bireyler üzerindeki olumsuz etki nedeniyle işlemenin gerçekleştirilmemesi gerektiğini göstermesi durumunda ise bu olumsuz etkiyi sınırlandırmak için hafifletici tedbirler alınabileceği belirtilmekte olup bu tedbirlerin teknik önlemler, şeffaflık artırıcı adımlar veya bireylerin haklarını kullanmasını kolaylaştırıcı yöntemler gibi unsurları içerebileceği ifade edilmektedir.

Son olarak ise hukuka aykırı bir şekilde işlenmiş kişisel verilerle geliştirilen bir yapay zekâ modeli, uygun şekilde anonimleştirildiği takdirde, bu durumun hukuka aykırılık kaynaklı sorunları giderebileceği ve fakat uygun/etkili bir anonimleştirme yapılmadığı takdirde ise modelin yerleştirilmesinin hukuka uygunluğu üzerinde etkili olabileceği belirtilmektedir.

* Birleşik Krallık Veri Koruma Otoritesi (ICO), üretici yapay zekâya ilişkin olarak geçtiğimiz yılın ocak ayında kamuoyu görüşüne açılan metinlere son hâlinin verildiğini duyurdu ve bu çerçevede sonuç raporunu yayımladı[2]. Söz konusu Rapor'da; (1) üretici yapay zekâ modellerini eğitmede kullanılan web kazıma işleminin yasal dayanağı, (2) üretici yapay zekâ yaşam döngüsünde amacın sınırlandırılması, (3) eğitim verilerinin ve model çıktılarının doğruluğu, (4) üretici yapay zekâ modellerinde bireylerin haklarını kullanmalarının sağlanması ve (5) üretici yapay zekâ tedarik zincirinde sorumluluğun belirlenmesi olmak üzere beş temel konu başlığı ele alınmaktadır.

2 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/12/generative-ai-developers-it-s-time-to-tell-people-how-you-re-using-their-information/, 12.12.2024.

* Bağımsız uzmanlar tarafından hazırlanan genel amaçlı yapay zekâ uygulama kurallarının 14.11.2024 tarihinde yayımlanan ilk taslağına yönelik iletilen geri bildirimler doğrultusunda hazırlanan ikinci taslak metin yayımlandı[3].

* Avrupa Parlamentosu Araştırma Servisi (EPRS), AB Siber Dayanıklılık Tüzüğü'ne ilişkin bilgilendirici bir doküman yayımladı[4]. Bu çerçevede bahse konu dokümanda; düzenlemenin kabulüne ilişkin süreç, düzenlemenin amaç ve kapsamı, temel hükümleri ve düzenlemeye yönelik ileri sürülen çeşitli görüşler gibi başlıklara yer verilmektedir.

  Genel olarak bakıldığında 2024/2847 sayılı AB Siber Dayanıklılık Tüzüğü, cihazlara veya ağlara doğrudan ya da dolaylı veri bağlantısı içeren dijital unsurlara sahip tüm ürünler için siber güvenlik yükümlülükleri getirmekte, tasarımda ve varsayılan olarak siber güvenlik ilkelerini tanıtmakta ve ürünlerin yaşam döngüsü boyunca özen yükümlülüğü öngörmektedir.

  20.11.2024 tarihli AB Resmî Gazetesi'nde yayımlanan düzenleme, 11.12.2027 tarihi itibarıyla tüm hükümleriyle uygulanacaktır.

* Fransa Veri Koruma Otoritesi (CNIL), iletilen şikâyetler doğrultusunda yanıltıcı olduğu değerlendirilen çerez banner'larını bir ay içerisinde değiştirmeleri yönünde web sitesi yayıncılarına talimat verildiğini duyurdu[5]. Konuya ilişkin yapılan açıklamada, çerezlerin kullanımının reddedilmesinin bu çerezlerin kabul edilmesi kadar kolay bir şekilde yapılamadığı ve belirsiz ya da yanıltıcı tasarımlarla ilgili kişilerin çerez kullanımına rıza vermeye teşvik edildiği belirtildi.

  Bunun yanı sıra, tespit edilen yanıltıcı uygulamalar şu hususları içermektedir:

  - Tıklanabilir bir bağlantı olarak sunulan reddetme seçeneğinin renk, yazı tipi boyutu ve stili ile kabul etme seçeneğine kıyasla orantısız bir şekilde daha az belirgin hâle getirilmesi,
  - Çerezleri reddetme seçeneğinin kolaylıkla fark edilemeyecek şekilde konumlandırılması, diğer paragraflarla arasında yeterli boşluk bırakılmaksızın sunulması ve görsel olarak diğer bilgilerden ayırt edilmesinin zorlaştırılması,
  - Çerezleri kabul etme seçeneğinin banner içerisinde birden fazla kez sunulmasına karşın reddetme seçeneğinin yalnızca bir kez ve dolaylı ifadelerle sunulması ("Gerekli olmayan amaçları reddediyorum" gibi).

3 https://digital-strategy.ec.europa.eu/en/library/second-draft-general-purpose-ai-code-practice-published-written-independent-experts, 19.12.2024.

4 https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739259, 20.12.2024.

5 https://www.cnil.fr/en/dark-patterns-cookie-banners-cnil-issues-formal-notice-website-publishers, 12.12.2024.

* Güney Kore, Avrupa Birliği'nin ardından yapay zekâya yönelik kapsamlı bir düzenleme oluşturan ikinci ülke oldu[6]. "Yapay Zekânın Geliştirilmesi ve Güvenin Tesisi Hakkında Temel Yasa" ismini taşıyan ve AB Yapay Zekâ Tüzüğü ile büyük ölçüde benzerlik taşıdığı şeklindeki yorumlarla karşı karşıya kalan düzenleme Meclis'te kabul edildi.

  Bu çerçevede genel olarak bakıldığında; düzenlemede risk temelli bir yaklaşım benimsendiği, yüksek etkili yapay zekâ sistemlerini belirlemek için bir sınıflandırma çerçevesi oluşturulduğu ve bu sistemlere yönelik daha katı yükümlülüklerin öngörüldüğü, yapay zekânın kullanımı ve geliştirilmesinde etik yönergeler oluşturulması ile şeffaflığın sağlanması gibi gereklilikler benimsendiği ve düzenlemeyi ihlal eden işletmeler hakkında 30 milyon KRW'ye (yaklaşık 20.500$) kadar para cezası uygulanabileceği belirtilmektedir.

* AB genelinde siber güvenlik olaylarına hazırlık yapılması, bu olayların tespit edilmesi ve uygun müdahalelerin gerçekleştirilmesi süreçlerinin iyileştirilmesi gibi amaçlar taşıyan 2025/38 sayılı AB Siber Dayanışma Tüzüğü *(Cyber Solidarity Act)* 15.01.2025 tarihli AB Resmî Gazetesinde yayımlandı[7].

* Avrupa Parlamentosu Araştırma Servisi (EPRS), karanlık tasarımlara *(dark patterns)* yönelik olarak çerçeve niteliğinde bir doküman yayımladı[8]. Bu kapsamda bahse konu dokümanda;

  - Karanlık tasarımların, genellikle kullanıcıların bilgileri veya rızaları bulunmaksızın, kullanıcı davranışlarını manipüle etmek amacıyla çevrim içi platformlar tarafından başvurulan aldatıcı teknikler olduğu,
  - Zararlı çevrim içi seçim mimarisine dayanan karanlık tasarımların, geniş bir yelpazede bilinçli seçimler yapma yeteneğini engelleyerek bireylerin kararlarını kasıtlı olarak etkilediği,
  - Karanlık tasarımlar konusunda AB'nin düzenleyici çerçevesinin parçalanmış bir yapıda olduğu,
  - Bu kavrama yönelik yeknesak bir tanım bulunmamasının, hukuki açıdan belirsizliğe ve farklı uygulamalara yol açabildiği,
  - Paydaşların ve akademisyenlerin, bu kavrama yönelik daha net tanımlar getirilmesi, daha güçlü güvenlik önlemleri alınması ve mevcut düzenlemelerin daha etkili bir şekilde uygulanması yönünde taleplerinin bulunduğu gibi hususlara değinilmektedir.

* Fransa Veri Koruma Otoritesi (CNIL), kullanıcıların mahremiyetine saygı duyulmasını sağlamak üzere mobil uygulamalarda talep edilen izinlerin nasıl olması gerektiğine yönelik bir içerik yayımladı[9].

6 https://www.ccn.com/news/technology/south-korea-ai-basic-act-joins-eu/, 26.12.2024.

7 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500038, 15.01.2025.

8 https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2025)767191, 13.01.2025.

9 https://www.cnil.fr/fr/permissions-applications-mobiles-recommandations-de-la-cnil-pour-respecter-la-vie-privee, 14.01.2025.

* Avrupa Veri Koruma Kurulu (EDPB), veri koruma hukuku ile rekabet hukuku arasındaki etkileşimin ve bu hususta düzenleyiciler arasındaki iş birliğinin nasıl iyileştirilebileceğinin ele alındığı bir görüş dokümanı yayımladı[10]. Bu çerçevede bahse konu dokümanda; veri koruma ile rekabet hukukunun etkileşim içerisinde bulunduğu noktalar ile ortak amaçlardan bahsedilmekte, veri koruma uygulamalarına rekabete ilişkin faktörlerin dahil edilmesi ve rekabet hukuku kapsamındaki değerlendirmelerde veri koruma kurallarının da dikkate alınmasına yönelik adımlar önerilmekte ve düzenleyiciler arasındaki iş birliğinin geliştirilmesine ilişkin önerilerde bulunulmaktadır.

* 08.01.2025 tarih ve 32776 sayılı Resmî Gazete'de yayımlanan 177 sayılı Cumhurbaşkanlığı Kararnamesi ile "Siber Güvenlik Başkanlığı" kuruldu[11].

  Bu çerçevede Başkanlığın görev ve yetkileri şu şekilde belirlendi:

  - Siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, eylem planları hazırlamak, mevzuat çalışmalarını yürütmek, ilgili faaliyetlerin koordinasyonunu sağlamak, bunların etkin şekilde uygulanmasını takip etmek,
  - Siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek,
  - Siber güvenlik ve bilgi güvenliğini destekleyici projeler yürütmek,
  - Siber güvenlik alanında kamu, özel sektör ve üniversiteler arasındaki iş birliğinin artırılmasına yönelik çalışmalar yapmak,
  - Siber güvenlik ekosistemi ile yerli ve milli ürün ve teknolojilerin geliştirilmesine ve yerli girişimcilerin dünya pazarında rekabetçi konuma gelmesine yönelik çalışmalar yapmak,
  - Siber güvenliğe ilişkin ihtiyaç duyulan alanlarda Ar-Ge ve teknoloji transferi yapmak,
  - Siber güvenlik ile ilgili yurt içinde veya yurt dışında düzenlenen tatbikat, etkinlik ve fuarlara katılımın özendirilmesine yönelik çalışmalar yürütmek,
  - Siber güvenlik zafiyetlerinin tespit edilmesi amacıyla çalışmalar yürütmek,
  - Siber güvenlik alanındaki kapasitenin kritik alanlara yönlendirilmesi ve mükerrer yatırımların önlenmesi için öncelikli siber güvenlik alanlarını belirlemek,
  - Siber güvenlik acil durum ve kriz yönetim planları oluşturmak, bu planlar çerçevesinde ortak operasyon merkezleri kurmak,
  - Siber güvenlik alanında kamu kurum ve kuruluşları tarafından verilecek teşviklere ilişkin görüş bildirmek,
  - Mevzuatla verilen diğer görevleri yapmak.

* Google Cloud, işletmelerin geleceğini şekillendirme potansiyeli taşıyan, 2025 yılının yapay zekâ trendlerine ilişkin bir rapor yayımladı[12]. Bu çerçevede raporda;

  - Metin, görüntü ve ses gibi birden fazla türde girdiyi aynı anda işleyebilme yeteneğiyle öne çıkan çok modlu yapay zekâ modellerinin daha kapsamlı bir perspektif sağlayarak çeşitli sektörlerde farklı avantajlar sunacağı,
  - Yapay zekâ ajanlarının karmaşık görevleri basitleştireceği, karmaşık iş akışlarını yönetebileceği, iş süreçlerini otomatikleştirebileceği ve çalışanları destekleyebileceği,
  - Şirket bünyesinde kullanılan dahili arama motorları gibi kurumsal arama sistemlerinin bilgiye erişimi kolaylaştıracağı,
  - Yapay zekâ destekli çözümler ile müşteri deneyimlerinin daha iyi bir hâle geleceği,
  - Yapay zekânın güvenlik sistemlerini geliştireceği, tehditleri belirleme ve bunlarla mücadele etme, güvenlik görevlerini otomatikleştirme ve yanıt sürelerini hızlandırma vb. görevlerde yardımcı olacağı gibi hususlara değinilmektedir.

* Florida'da görülmekte olan bir ceza davasında sanık avukatı, yargıcın olayı sanığın gözünden görmesini sağlamak üzere, sanığın düğün salonunda meydana gelen bir kavga sırasında yaşadığı tehlikeyi ve kendisini koruma amacıyla silah çektiği durumu yansıtan bir simülasyon hazırlattı[13]. İddia konusu suçun sanal gerçeklik ile oluşturulmuş simülasyonunun delil olarak sunulmasını kabul eden yargıç, olay anını sanal gerçeklik gözlüğü aracılığıyla sanığın bakış açısından deneyimleme fırsatı buldu.

* Avrupa Birliği Adalet Divanı'nın [ABAD] C-203/22 sayılı Kararında, otomatik yollarla gerçekleştirilen kredi değerlendirmesi kapsamında, ilgili kişinin kendisi hakkında alınan kararın nasıl verildiğine dair açıklama talep etme hakkına sahip olduğu ve bu açıklamanın, ilgili kişinin kararı anlamasına ve itiraz etmesine imkân tanıyacak nitelikte olması gerektiğine hükmedilmiştir[14].

  Karara konu olayda; Avusturya'daki bir mobil telefon operatörü, bir müşterinin kredi notunun yetersiz olduğu gerekçesiyle sözleşme yapmasına izin vermeyi reddetmiş ve bu kararı, *Dun&Bradstreet Austria* tarafından otomatik yollarla gerçekleştirilen bir kredi değerlendirmesine dayandırmıştır. ABAD, otomatik karar alma sürecinde hangi kişisel verilerin kullanıldığını ve bu verilerin nasıl değerlendirildiğini ilgili kişinin anlayabilmesi için uygulanan prosedürü ve ilkeleri veri sorumlusunun açıklaması gerektiğini belirtmiş; ancak yalnızca algoritmanın kendisinin paylaşılmasının yeterince açık ve anlaşılır bir açıklama oluşturmayacağını vurgulamıştır. Bunun yanı sıra, sağlanacak bilginin üçüncü kişilere ait verileri veya ticari sırları içermesi durumunda, veri sorumlusunun bu bilgiyi yetkili denetim otoritesine

10 https://www.edpb.europa.eu/news/news/2025/edpb-adopts-pseudonymisation-guidelines-and-paves-way-improve-cooperation_en, 17.01.2025.

11 https://www.resmigazete.gov.tr/eskiler/2025/01/20250108-1.pdf, 08.01.2025.

12 https://blog.google/products/google-cloud/ai-trends-business-2025/, 17.12.2024.

13 https://gizmodo.com/florida-judge-allows-vr-simulation-of-alleged-crime-to-be-submitted-as-evidence-2000544922, 02.01.2025.

14 https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-02/cp250022en.pdf, 27.02.2025

veya mahkemeye sağlaması gerektiği belirtilmiştir.

* Avrupa Sağlık Veri Alanı'na ilişkin 2025/327 sayılı Tüzük, 05.03.2025 tarihli AB Resmî Gazetesi'nde yayımlandı[15]. Genel olarak bakıldığında; AB genelinde elektronik sağlık verilerinin kullanımı ve değişimi konusunda ortak bir çerçeve oluşturmayı amaçlayan bu düzenleme, bireylerin kişisel elektronik sağlık verilerine erişimini ve bu veriler üzerinde sahip oldukları kontrolü artırırken, aynı zamanda belirli verilerin birtakım amaçlar (örneğin; kamu yararı, bilimsel araştırma) doğrultusunda yeniden kullanılmasına olanak tanımaktadır.

  Bu çerçevede bahse konu Tüzük ile;

  - Bireyler, sınır ötesi sağlık hizmetlerinde kullanılmak üzere elektronik sağlık verilerine erişebilecek, bunları kontrol edebilecek ve paylaşabilecek (birincil kullanım),
  - Sağlık verilerinin araştırma, inovasyon, politika oluşturma ve düzenleyici faaliyetler için güvenli ve güvenilir bir şekilde yeniden kullanılması sağlanacak (ikincil kullanım),
  - Elektronik sağlık kaydı (EHR) sistemleri için tek bir pazar oluşturularak hem birincil hem de ikincil kullanım desteklenecektir.

  Tüzük, 26.03.2025 tarihinde yürürlüğe girecek ve ardından kademeli olarak uygulanmaya başlanacaktır.

* Avrupa Komisyonu, temel hakları ihlal etmeleri nedeniyle AB değerlerine aykırı kabul edilen ve AB Yapay Zekâ Tüzüğü'nün *(AI Act)* 5. maddesi kapsamında yasaklanan yapay zekâ uygulamalarına ilişkin olarak yol gösterici mahiyette bir rehber yayımladı[16].

* Avrupa Komisyonu, AB Yapay Zekâ Tüzüğü'nün *(AI Act)* uygulanmasını kolaylaştırmak amacıyla "yapay zekâ sistemi" tanımına ilişkin yol gösterici mahiyette bir rehber yayımladı[17]. Sağlayıcıların ve diğer ilgililerin, bir yazılım sisteminin "yapay zekâ sistemi" olarak nitelendirilmesinin mümkün olup olmadığını belirlemelerine yardımcı olması amaçlanan Rehber'in, zaman içerisinde ortaya çıkan deneyimler, yeni sorular ve kullanım durumları ışığında gerektiği şekilde güncelleneceği ifade edilmektedir.

15 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500327, 05.03.2025.

16 https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act, 04.02.2025.

17 https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application, 06.02.2025.

* Avrupa Parlamentosu Araştırma Servisi (EPRS), AB Yapay Zekâ Tüzüğü *(AI Act)* ile AB Genel Veri Koruma Tüzüğü (GDPR) arasındaki etkileşimin ve algoritmik ayrımcılığın bu düzenlemeler çerçevesinde nasıl ele alındığının incelendiği bir çalışma yayımladı[18]. Genel olarak bakıldığında AB Yapay Zekâ Tüzüğü, bireylerin kişisel verilerinin korunması hakkı da dâhil olmak üzere temel hak ve özgürlüklere saygılı bir yaklaşım benimserken; aynı zamanda insan merkezli, güvenilir ve sürdürülebilir yapay zekânın teşvik edilmesini amaçlamaktadır.

  Bu kapsamda söz konusu çalışmada; AB Yapay Zekâ Tüzüğü'nün özellikle yüksek riskli yapay zekâ sistemlerinde ayrımcılığın ve ön yargının azaltılmasını hedeflediği, bu doğrultuda belirli koşullar altında özel nitelikli kişisel verilerin işlenmesine izin verildiği, diğer yandan AB Genel Veri Koruma Tüzüğü'nün bu tür verilerin işlenmesi konusunda daha kısıtlayıcı bir yaklaşım benimsediği ve bu durumun AB Yapay Zekâ Tüzüğü'nün uygulanmasında birtakım belirsizlikler ortaya çıkardığı ifade edilmektedir. Bu çerçevede, iki düzenleme arasında uyum sağlanmasının ek rehberlik sunulmasını veya mevzuatta değişiklik yapılmasını gerektirebileceği belirtilmektedir.

* Avrupa Veri Koruma Kurulu (EDPB), çocuklara yönelik yaş güvencesi hakkında bir bildiri yayımladı[19]. Veri koruma ilkelerine uygun bir şekilde hareket ederken küçükleri korumak için tutarlı bir Avrupa yaş güvencesi yaklaşımı sağlanmasının amaçlandığı bildiride, bir bireyin yaşı veya yaş aralığı belirlenirken kişisel verilerin uyumlu bir şekilde işlenmesi için on ilke sıralanmaktadır.

* Avrupa Veri Koruma Kurulu (EDPB), ChatGPT görev gücünün kapsamının yapay zekâ denetimlerini de kapsayacak şekilde genişletilmesine karar verildiğini duyurdu[20].

* Avrupa Parlamentosu Araştırma Servisi (EPRS), çocukların üretken yapay zekâ araçlarını kullanımından elde edilebilecek fırsatlar ile karşılaşılabilecek zorlukların ele alındığı bir çalışma yayımladı[21]. Çalışmada öne çıkan bulgulardan biri, 2024 yılında Birleşik Krallık'ta yapılan bir ankete göre, 13-18 yaş arasındaki çocukların %77.1'inin üretken yapay zekâ araçlarını kullandığı, bu oranın yetişkinlere kıyasla iki kat daha yüksek olduğu ve bu araçların en yaygın kullanım alanlarının ödevlere yardımcı olmak ve eğlence amaçlı içerik aramak olduğu yönündedir.

  Bahse konu çalışmada, üretken yapay zekâ araçlarının eğitim süreçlerine entegre edilmesinden sağlanabilecek faydalar arasında; uygun bir şekilde kullanıldığında çocukların yaratıcılığını ve problem çözme becerilerini geliştirebileceği ve farklı öğrenme ihtiyaçlarını destekleyerek engelli bireyler için eğitimi daha erişilebilir hâle getirebileceği sayılmaktadır.

  Bu araçların eğitimde kullanılmasının beraberinde getirdiği temel zorluklar kapsamında ise;

  - Üretken yapay zekâ ile oluşturulan içeriklerin artışının dezenformasyon tehlikesini yükseltebileceği, özellikle deepfake gibi manipülatif içeriklere karşı çocukların savunmasız olduğu dikkate alındığında siber zorbalık veya çevrim içi istismar gibi tehditlere daha açık hâle gelebilecekleri,

18 https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2025)769509, 26.02.2025.

19 https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-12025-age-assurance_en, 12.02.2025.

20 https://www.edpb.europa.eu/news/news/2025/edpb-adopts-statement-age-assurance-creates-task-force-ai-enforcement-and-gives_en, 12.02.2025.

21 https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2025)769494, 18.02.2025.

- Üretken yapay zekânın veri analizi ve otomasyon yeteneklerinin çocukların araştırma, yazma ve akıl yürütme becerilerini zayıflatabileceği,

- Yapay zekâ araçlarını günlük hayatta etkili bir şekilde kullanmak için gerekli beceri ve bilgiler ile bunlarla ilişkili riskler ve fırsatlar konusunda farkındalığa sahip olunmasını ifade eden yapay zekâ okuryazarlığına ilişkin eğitimin, ilkokullardan ziyade daha yaygın olarak ortaokullarda ve üniversitelerde sunulduğu, diğer yandan bu araçların cinsiyet eşitsizliğini derinleştirebileceği ve dil verisi sınırlı dillerde eğitilen modellerin güvenlik açısından riskler barındırabileceği belirtilmektedir.

* Birleşik Krallık Veri Koruma Otoritesi (ICO), "rıza veya ödeme" modelini uygulayan ya da uygulamayı düşünen kuruluşlara rehberlik sağlamak amacıyla bir rehber yayımladı[22]. Genel olarak bakıldığında bu model kapsamında bireylere üç seçenek sunulmaktadır: (1) çevrim içi bir ürün veya hizmete erişmek için kişisel verilerinin kişiselleştirilmiş reklamcılık amacıyla kullanılmasına rıza göstermek, (2) kişisel verileri kullanılmadan belirli bir ücret ödeyerek ilgili ürün veya hizmete erişmek ve (3) ilgili ürün veya hizmeti kullanmamayı tercih etmek.

  Bahse konu Rehber'de, bu modelin geçerli bir rızanın şartlarını karşılayıp karşılamadığını değerlendirmek için dikkate alınması gereken temel faktörleri içeren bir çerçeve sunulmaktadır. Ayrıca, bu modeli uygulayan kuruluşların bireylerin kişiselleştirilmiş reklamcılığa özgür iradeyle rıza verdiklerini gösterebilmeleri gerektiği vurgulanmakta ve veri koruma etki değerlendirmesi kapsamında modelin incelenmesi gerektiği belirtilmektedir. Bu süreçte, yürürlükteki veri koruma ilkeleri ile Otorite'nin ilgili diğer rehberlerinin de dikkate alınması gerektiği ifade edilmektedir.

* Fransa Veri Koruma Otoritesi (CNIL), çok uluslu şirketlerin Bağlayıcı Şirket Kuralları (BCR) uygulama süreçlerini değerlendirmelerine yardımcı olmak amacıyla bir öz değerlendirme aracı yayımladı[23]. Söz konusu aracın, BCR sürecinin olgunluk seviyesini test ederek uyumluluk skoru ve bir eylem planı sunduğu, böylece şirketlerin başvuru öncesinde eksikliklerini gidermelerine olanak tanıdığı belirtilmektedir.

* Avrupa Veri Koruma Kurulu (EDPB), 2025 yılı Koordineli Uygulama Çerçevesi *(Coordinated Enforcement Framework)* eylemini başlattı[24]. 2024 yılında ilgili kişilerin erişim hakkına odaklanan EDPB, 2025 yılında AB Genel Veri Koruma Tüzüğü'nün (GDPR) 17'nci maddesi kapsamında "silme hakkı (unutulma hakkı)"nın uygulanmasının inceleneceğini duyurdu. Bu çerçevede, yıl içerisinde otuz iki veri koruma otoritesinin çeşitli sektörlerdeki veri sorumlularını inceleyeceği, verilerin silinmesi yönündeki taleplerin veri sorumlularınca nasıl ele alındığının ve bu hakkın kullanılmasına ilişkin koşullar ile istisnaların nasıl uygulandığının değerlendirileceği, süreç boyunca veri koruma otoritelerinin bulgularını paylaşacakları ve gerekli analizleri gerçekleştirecekleri belirtildi.

22 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/online-tracking/consent-or-pay/about-this-guidance/, 23.01.2025.

23 https://www.cnil.fr/en/binding-corporate-rules-bcr-cnil-publishes-self-assessment-tool, 14.02.2025.

24 https://www.edpb.europa.eu/news/news/2025/cef-2025-launch-coordinated-enforcement-right-erasure_en, 05.03.2025.

* ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), diferansiyel mahremiyet kavramına ilişkin olarak uygulayıcılara yönelik bir çalışma yayımladı[25]. Söz konusu çalışmada, diferansiyel mahremiyet piramidinde dikkate alınması gereken faktörler tanımlanmakta ve mahremiyet riskleri ile diferansiyel mahremiyetin uygulanmasında karşılaşılan yaygın tuzaklara dikkat çekilmektedir.

* Güneydoğu Asya Ülkeleri Birliği (ASEAN), verilerin anonimleştirilmesine ilişkin bir rehber yayımladı[26]. Bahse konu Rehber'de; anonimleştirmeye ilişkin terminoloji, temel kavramlar, anonimleştirme süreci, temel anonimleştirme teknikleri, anonimleştirmeye ilişkin yaygın olarak yanlış anlaşılan hususlar ve anonimleştirme araçları gibi başlıklar ele alınmaktadır.

25 https://www.nist.gov/publications/guidelines-evaluating-differential-privacy-guarantees, 06.03.2025.

26 https://asean.org/book/asean-guide-on-data-anonymisation/, Ocak 2025.

İNSAN HAKLARI KURUMLARI DEĞERLENDİRME TOPLANTISI

Kurum Başkanımız Faruk BİLİR, 11 Aralık 2024 tarihinde Adalet Bakanımız Sayın Yılmaz TUNÇ'un başkanlığında gerçekleştirilen "İnsan Hakları Kurumları Değerlendirme Toplantısı"na katılım sağladı.

"MAHREMİYET VE ETİK İLKELER IŞIĞINDA YAPAY ZEKÂ" PANELİ

Kurumumuz ile Kamu Görevlileri Etik Kurulu'nun iş birliğinde "Mahremiyet ve Etik İlkeler Işığında Yapay Zekâ" paneli, 17 Aralık 2024 tarihinde KVKK Konferans Salonunda düzenlendi. Kamu Başdenetçisi Mehmet AKARCA'nın, Kurul Üyelerinin, kamu kurum ve kuruluşları ile çeşitli meslek gruplarının temsilcilerinin katılım sağladığı panelin açılış konuşmaları, Kurum Başkanımız Prof. Dr. Faruk BİLİR ile Kamu Görevlileri Etik Kurulu Başkanı Zerrin GÜNGÖR tarafından gerçekleştirildi.

BİLİR, günümüzde insanlığın keskin bir yapay zekâ virajında olduğunu, bu virajın nasıl alınacağının insanlığın geleceği adına belirleyici olacağını söyleyerek, yapay zekâ ile ilgili felaket senaryolarının oluşturduğu algılara teslim olmamak gerektiğini, esas konunun teknolojik gelişmeleri ülkemiz ve insanlık adına fırsat olarak düşünmek ve buna yönelik adımlar atmak olduğunu dile getirdi. Yapay zekâ tartışmalarının genel olarak aşırı iyimser veya aşırı kötümser görüşler arasında gündeme geldiğini belirten BİLİR, yapay zekâ konusunun gerçekçi bir zeminde ele alınarak çağın gereklerine uygun bir anlayışla değerlendirilmesi gerektiğini ifade etti. Yapay zekâ üzerindeki kontrolün kaybedilmemesi için etik kurallara ihtiyaç bulunduğunu söyleyen BİLİR, söz konusu etik kurallardan birinin mahremiyet olduğunu vurguladı.

"Mahremiyetin temelinde bireyin kendi geleceği hakkında karar verebilme gücü vardır." diyen BİLİR, "Teknoloji ile mahremiyet arasında bir dengenin kurulması, yalnızca bireylerin hak ve özgürlüklerinin korunmasını sağlamakla kalmayacak, aynı zamanda toplumun yapay zekâ gibi güncel teknolojilere güven duymasını sağlayacaktır." dedi.

Hukuka uygun veri işlemenin önemine işaret eden BİLİR şöyle devam etti: "Kişisel veri işleme temelli yapay zekâ çalışmaları; verilerin doğru ve güncel olması, veri kullanım amacının belirli ve sınırlı olması ilkeleri ile veri güvenliği yaklaşımına dayalı olmalıdır. Ayrıca veri işlemede bireyin mahremiyeti öncelikli konulardan biri olmalı, veri üzerindeki esas kontrolün bireylerde olduğu dikkate alınmalıdır."
BİLİR ayrıca, dijital çağda insan kalabilme idealinin önemini de vurgulayarak, "Dijital çağda insan kalmak, mahremiyet gibi bizi biz yapan değerlerimize sahip çıkmak ve yapay zekâ uygulamalarını insani bir çerçevede, insan odaklı bir anlayışla hayata geçirmek mümkündür." dedi.

Kişisel Verileri Koruma Kurumu Başkan Yardımcısı Dr. Cihan KANLIGÖZ'ün moderatörlüğünde düzenlenen panelde ise; Kamu Görevlileri Etik Kurulu Üyesi M. Fatih UŞAN "Kamu Görevlileri Etik Kurulu Yapısı ve Faaliyetleri", Kişisel Verileri Koruma Kurulu Üyesi Cennet ALAS ŞEKERBAY "Kişisel Verileri Koruma Kurumu Yapısı ve Faaliyetleri", Kişisel Verileri Koruma Kurumu Hukuk İşleri Dairesi Başkanı Ezgi ERGÜNEŞ DURAN "Yapay Zekânın Hukuki Sorumluluğu", Ankara Üniversitesi'nden Doç. Dr. Tuba Nur UMUT ise "Yapay Zekânın Kullanımında Kamu Görevlilerinin Uyması Gereken Etik Davranış İlkeleri" konularını anlattılar.

ÖDEME VE ELEKTRONİK PARA SEKTÖRÜNDE KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN İYİ UYGULAMALAR REHBERİ ÇALIŞTAYI

Kurumumuz ile Türkiye Ödeme ve Elektronik Para Kuruluşları Birliği (TÖDEB) iş birliğiyle; ödeme ve elektronik para kuruluşlarının kişisel verilerin korunması mevzuatına uyum sağlaması ve iyi uygulama örnekleri oluşturularak sektör temsilcilerine rehberlik edilmesine yönelik bir rehber hazırlanması amacıyla çalışmalar başlatılarak daha önce kurumlar arası bir dizi toplantı gerçekleştirilmişti. Bu kapsamda TÖDEB üyesi elektronik para kuruluşları, POS hizmeti veren kuruluşlar, mobil ödeme hizmeti sunan kuruluşlar, fatura ödemeye aracılık eden kuruluşlar ve para havalesine aracılık eden kuruluşların kişisel verilerin korunması mevzuatına uyumu bağlamında, her bir faaliyet alanına özel dikkat edilmesi gereken hususlar, uygulanan iş modeli, işlenen kişisel veriler ve bu kişisel verilerin işlenmesindeki amaç, ilgili kişi ve kişisel veri ile temas edilen noktalar gibi başlıkları da ihtiva eden "Ödeme ve Elektronik Para Sektöründe Kişisel Verilerin Korunmasına İlişkin İyi Uygulamalar Rehberi" üzerinde görüş alışverişinde bulunmak amacıyla 21-22 Aralık 2024 tarihlerinde bir çalıştay düzenlendi.

Kurum Başkanımız Prof. Dr. Faruk BİLİR ve TÖDEB Başkanı Ufuk BİLGETEKİN'in açılış konuşmalarıyla başlayan çalıştayda, Ödeme ve Elektronik Para Sektöründe Kişisel Verilerin Korunmasına İlişkin İyi Uygulamalar Rehberi'nin son taslak versiyonu üzerinden görüş alışverişlerinde bulunuldu

KVKK ve TÖDEB Başkanları, Kişisel Verileri Koruma Kurulu üyeleri, KVK uzmanları, TÖDEB temsilcileri ile Türkiye Cumhuriyet Merkez Bankası temsilcilerinin de yer aldığı çalıştayda, sektörün kişisel verilerin korunması mevzuatına uyumunu artıracak ve ilgili kişilerin haklarını korumaya yönelik önlemlerin alınmasını sağlayacak iyi uygulama örneklerinin rehbere yansıması sağlanmaya çalışıldı.

KİŞİSEL VERİLERİ KORUMA GÖNÜLLÜSÜ YETİŞTİRME PROJESİ

"Üniversite Öğrencileri Arasında Kişisel Verileri Koruma Gönüllüsü Yetiştirme Projesi" 13-15 Aralık 2024 tarihlerinde beşinci kez gerçekleştirildi. Proje kapsamında Adalet Teşkilatını Güçlendirme Vakfı (ATGV) Antalya tesislerinde düzenlenen programa çeşitli üniversitelerin hukuk fakültelerinden öğrenciler katılım sağladı.

Program çerçevesinde; "6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda Yer Alan Temel Kavramlar, İlkeler ve Kişisel Verilerin İşlenme Şartları", "İlgili Kişinin Hakları ile Başvuru Usul ve Yöntemleri", "Kişisel Veri Güvenliği ve Farkındalık", "Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması Alanındaki Suçlar", "Kişisel Verileri Koruma Kurulu Kararları ve İlke Kararları" ve "Yapay Zekâ Alanında Kişisel Verilerin Korunması" konuları, Kurumumuz Kişisel Verileri Koruma Uzmanları tarafından anlatıldı. Öte yandan kişisel verilerin korunmasına yönelik farkındalık çalışmaları ve bilgilendirmeler yapılarak buna yönelik yarışmalar, etkinlikler ve atölye çalışmaları düzenlendi.

Programın açılışında konuşan Kurum Başkanımız Prof. Dr. Faruk BİLİR, "Kişisel Verilerin Korunması Kanunu" ile "Üniversite Öğrencileri Arasında Kişisel Verileri Koruma Gönüllüsü Yetiştirme Projesi" hakkında bilgiler paylaştı.

Kişisel verilerin korunmasında yasal düzenlemeler kadar farkındalığın da önem taşıdığını belirten BİLİR, projenin üniversite gençliği arasında kişisel veri farkındalığı oluşturmak ve veri koruma kültürünü üniversite öğrencileri arasında yaygınlaştırmak amacıyla gerçekleştirildiğini ifade etti.

Projenin 2019 yılında başladığını söyleyen BİLİR, daha önce hukuk ve mühendislik fakülteleri olmak üzere farklı öğrenciler ile proje kapsamındaki etkinliklerin dört kez düzenlendiğini, bu yılki etkinliklerle birlikte projenin artık "yaşayan bir proje" haline dönüştüğünü ve Kurum olarak memnuniyet duyduklarını ifade etti.

BİLİR, gerçekleştirilen etkinliklerin devamındaki sürecin, gönüllü öğrencilerin bulundukları fakültelerde, fakülte yönetiminin bilgisi ve onayı dahilinde olmak kaydıyla; kişisel verilerin korunmasıyla ilgili öğrenci kulüplerinin kurulması, eğer mevcutta bir kulüp var ise etkinliğinin artırılması, kişisel verilerin korunmasına yönelik seminer-konferans-panel çalışmaları yapılması yönünde ilerleyeceğini kaydetti.

BİLİR sözlerini şöyle tamamladı:

"Günümüzde teknolojik gelişmelerle uyumlu olmak, dijital dünyanın fırsatlarını ve risklerini değerlendirebilmek önemlidir. Bu durum artık bir tercihten ziyade gereklilik haline gelmiştir. Bununla birlikte hukuki düzenlemelere uyum sağlamak da önemlidir. Bu nedenle hukuk ve teknolojiyi bir arada düşünmek gerekir. Daha önce bu projeyi dört kez gerçekleştirdik ve verimli sonuçlar aldık. Siz değerli öğrencilerle gerçekleştirdiğimiz etkinliklerin de amacına ulaşacağına inanıyorum."

KİŞİSEL VERİLERİN KORUNMASI HUKUKU KİTABI

Uygulayıcıların ve karar vericilerin hukuki bilgilerine katkıda bulunmak ve kişisel verilerin uygulamada daha etkin bir şekilde korunmasını sağlamak amacıyla, Kurumumuz ve Türkiye Adalet Akademisi'nin ortak çalışması sonucunda "Kişisel Verilerin Korunması Hukuku" başlıklı eser hazırlandı.

17 Ocak 2025 tarihinde Bartın Üniversitesi iş birliğinde gerçekleştirilen program ile kutlanan Veri Koruma Günü'nde Adalet Bakanımız Sayın Yılmaz TUNÇ'a takdim edilerek tanıtımı yapılan kitapta;

- Genel Olarak Kişisel Verilerin Korunması
- Kişisel Verilere İlişkin TCK'da Düzenlenen Suçlar
- Kişisel Verilerin Özel Hukukta Korunması
- Kişisel Verilerin İş Hukukunda Korunması

başlıklı bölümler yer almaktadır.

KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASI REHBERİ

Kişisel Verilerin Korunması Kanunu'nun "Kişisel Verilerin Yurt Dışına Aktarılması" başlıklı 9'uncu maddesi kapsamında kişisel veri aktarımlarının uygulanması hakkında veri sorumlularına yol gösterilmesi amacıyla "Kişisel Verilerin Yurt Dışına Aktarılması Rehberi" yayımlandı.

ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN REHBER

Özel nitelikli kişisel verilerin işlendiği durumlarda veri sorumlularının doğru hukuki sebeplere dayalı olarak özel nitelikli kişisel veri işlemeleri ve Kişisel Verilerin Korunması Kanunu'na uygun şekilde yükümlülüklerini yerine getirmeleri için yol gösterici olması amacıyla, "Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Rehber" yayımlandı.

KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN BANKACILIK SEKTÖRÜ İYİ UYGULAMALAR REHBERİ

Kurumumuz ve Türkiye Bankalar Birliği iş birliği ile hazırlanan Kişisel Verilerin Korunmasına İlişkin Bankacılık Sektörü İyi Uygulamalar Rehberi, Kişisel Verilerin Korunması Kanunu'nda yapılan değişiklikler göz önüne alınarak güncellendi.

KABAHATLERİN ZAMAN BAKIMINDAN UYGULANMASI BİLGİ NOTU

Kişisel Verilerin Korunması Kanunu'nda yapılan değişiklikler neticesinde kabahat niteliğindeki fiillerin gerçekleşme zamanı ile Kişisel Verileri Koruma Kurumu'na yapılan şikayet tarihi ve Kurul Kararının verileceği zaman bakımından farklılıklar olması nedeniyle, Kanun'un zaman bakımından uygulanması bağlamında uygulamada oluşan tereddütlerin giderilmesi amacıyla, Kabahatlerin Zaman Bakımından Uygulanması Bilgi Notu yayımlandı.

KAMUOYU DUYURULARI

Arabuluculuk faaliyetleri kapsamında aydınlatma yükümlülüğünün yerine getirilmesine ilişkin kamuoyu duyurusu ile yurt dışına kişisel veri aktarımında kullanılacak standart sözleşmelerde dikkat edilmesi gereken hususlara ilişkin kamuoyu duyurusu yayımlandı.

KİŞİSEL VERİLERİ KORUMA DERGİSİ

Kişisel Verileri Koruma Dergisi'nin on ikinci sayısında;

- Gizlilik Yasalarının Test Edilmesi: Kullanıcıların Bilgi-Rıza Bildirimleri Hakkında Algıları ve Tepkileri
- Bankaların Bilgi Güvenliği Yönetimi Kapsamında Banka Müşterilerinin Kişisel Verilerinin Korunması
- Türkiye'de Biyometrik Veri Güvenliği: Kişisel Verilerin Korunması Kanunu Çerçevesinde Etik Bir Değerlendirme
- Fiyat Dışı Rekabet Parametresi Olarak Veri Gizliliği
- Tüketici – Online Pazar Yerleri - Kargo Şirketleri Üçgeninde Kişisel Veri İşleme Faaliyetleri

başlıklı makaleler, ilgililerin kullanımına sunuldu.

ÇARŞAMBA SEMİNERLERİ

Kurumumuz tarafından düzenlenen Çarşamba Seminerleri kapsamında;

» Türkiye İnsan Hakları ve Eşitlik Kurumu (TİHEK) Başkanı Prof. Dr. Muharrem KILIÇ, "İnsan Haklarının Kurumsallaşması: Ulusal İnsan Hakları Kurumları"

» Bartın Üniversitesi Fen Fakültesi Bilişim Sistemleri ve Teknolojileri Ana Bilim Dalı Bölüm Başkanı Prof. Dr. Ramazan YILMAZ, "Kişisel Verilerin Korunması ve Yapay Zekâ: Riskler ve Çözümler"

» Kurumumuz Kişisel Verileri Koruma Uzmanlarından Büşra DURMUŞOĞLU GÜNEY, "Çocukların Kişisel Verilerinin Korunması: Sosyal Medya Bağlamında Bir Değerlendirme"

» Bartın Üniversitesi Mühendislik, Mimarlık ve Tasarım Fakültesi Bilgisayar Mühendisliği/ Bilgisayar Yazılımı Anabilim Dalı bölümünde görevli Doç. Dr. Eyüp Burak CEYHAN, "Üretken Yapay Zekânın Hukuki Boyutu: Güncel Gelişmeler ve Riskler"

konularında bilgi paylaşımında bulundular.

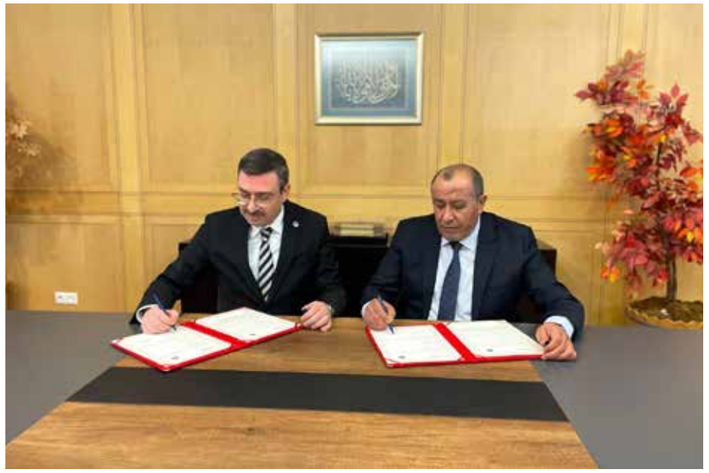
SERMAYE PİYASASI KURULU İLE İŞ BİRLİĞİ

Kurumumuz ve Sermaye Piyasası Kurulu arasında kişisel verilerin işlenmesi ve korunmasına yönelik konularda iş birliği yapmak amacıyla protokol imzalandı.

Protokol ile sermaye piyasalarında kişisel verilerin işlenmesi ve korunması konularında artan ihtiyaçlar doğrultusunda, iki kurum arasında etkin bir koordinasyon ve iş birliğinin sağlanması hedeflenmektedir.

Protokol, her iki kurumun görev alanına giren ortak konularda bilgi ve görüş paylaşımı yapılmasını, bu çerçevede; kişisel verilerin korunması, veri mahremiyeti ve veri güvenliği konularında ortak projeler ve çalışmaların gerçekleştirilmesini, meslek personelinin yetiştirilmesini, ortak yayınlar ve farkındalık artırıcı etkinliklerin düzenlenmesini içermektedir.

Kurumumuz ve Sermaye Piyasası Kurulu birlikteliğinde atılan bu adımın, hem sermaye piyasalarındaki kişisel veri güvenliği süreçlerini güçlendirmesi, hem de kişisel verilerin korunmasına yönelik yapılan çalışmalara örnek teşkil etmesi öngörülmektedir.



TÜRKİYE İNSAN HAKLARI VE EŞİTLİK KURUMU (TİHEK) İLE İŞ BİRLİĞİ

Kurumumuz ile Türkiye İnsan Hakları ve Eşitlik Kurumu (TİHEK) arasında iş birliği protokolü imzalandı.

Protokol ile insan hak ve özgürlüklerinin korunması ve geliştirilmesi, ayrımcılıkla mücadele edilmesi ve buna ilişkin toplumsal farkındalığın geliştirilmesi konusunda çalışmalar yapılması hedeflenmektedir.

Protokol, insan haklarının ve kişisel verilerin korunmasının önemi hususunda kamuoyunda bilincin artırılması adına ortak çalışmalar yapılmasını, belirlenen konulara ilişkin çalıştay, panel, sempozyum gibi ortak programlar düzenlenmesini, kişisel verilerin korunması, ayrımcılığın önlenmesi ve insan hakları ile ilgili konularda farkındalık artırıcı tematik projelerin hayata geçirilmesini ve ortak yayınlar çıkarılmasını içermektedir.

TÜRKİYE BAROLAR BİRLİĞİNE ZİYARET

Kurum Başkanımız Prof. Dr. Faruk BİLİR ile Kurul Üyelerimizden Bayram ARSLAN, Tamer AKSOY ve Muhammed Serdar CAFOĞLU, Türkiye Barolar Birliği'ni (TBB) ziyaret ederek Birlik Başkanı Erinç SAĞKAN ile görüştü.

VERİ KORUMA OTORİTELERİ İSTİŞARE TOPLANTISI

6 Haziran 2024 tarihinde Kurumumuz ev sahipliğinde Azerbaycan, Cezayir, Fas, Malezya, Mali ve Katar temsilcilerinin katılımıyla ilki İstanbul'da düzenlenen Veri Koruma Otoriteleri İstişare Toplantısı'nın devamı niteliğindeki ikinci toplantı, 18-19 Şubat 2025 tarihlerinde Fas'ın Fes şehrinde gerçekleştirildi.

Toplantıya Türkiye ve ev sahibi Fas'ın yanı sıra Benin, Burkina Faso, Gabon, Gambiya, Mali, Moritanya, Nijerya, Senegal ve Somali Veri Koruma Otoriteleri Başkanları ve temsilcileri ile Birleşmiş Milletler Özel Raportörü katılım sağladı. Toplantının açılışında konuşan Kurum Başkanımız Prof. Dr. Faruk BİLİR, kişisel verilerin korunmasına ilişkin ortak konularda bilgi, görüş ve deneyim paylaşımı gerçekleştirmenin, katılımcı ülkeler arasında kişisel verilerin korunması alanını geliştirmeye yönelik çabaları koordine etmenin ve iş birliğinin önemini vurguladı.

Toplantı kapsamında kurulan ortak yapı için İslam Ülkeleri Kişisel Verileri Koruma Otoriteleri Ağı (INPDPA-Islamic Network For Personal Data Protection Authorities) ismi uygun görülerek, kurulan ağın başkanlığını Fas Veri Koruma Otoritesi'nin yürütmesine, daimi sekretarya görevinin ise Kurumumuz tarafından yürütülmesine karar verildi.

Öte yandan Kurumumuz ile Fas Veri Koruma Otoritesi (CNDP) arasında, kişisel verilerin korunması ve mahremiyet konularında bilgi alışverişi ve deneyim paylaşımı amacıyla mutabakat zaptı imzalandı. Mutabakat zaptı çerçevesinde, iyi uygulamaların paylaşımına yönelik iş birliği ve karşılıklı olarak kararlaştırılan diğer iş birliği alanlarına ilişkin ortak çalışmalar yapılması öngörüldü.

KIRGIZ CUMHURİYETİ DEVLET KİŞİSEL VERİLERİ KORUMA AJANSINA ZİYARET

5-6 Aralık 2024 tarihlerinde Kırgız Cumhuriyeti'nin başkenti Bişkek'te "Dijital Çağda Hukukun Sınırları: Kamu, Özel, Dijital" ana temasıyla düzenlenen 2024 Uluslararası Dijital Hukuk Forumuna Kurum Başkanımız Prof. Dr. Faruk BİLİR ile birlikte Kurul Üyelerimizden Recep KESKİN ve Muhammed Serdar CAFOĞLU tarafından katılım sağlandı.

Forum açılışında konuşan BİLİR, dijital çağda veri koruma otoritelerine düşen görevin muadil kurumlarla iş birliği içerisinde çalışmak olduğunu belirtirken, Kırgız Cumhuriyeti Devlet Kişisel Verileri Koruma Ajansı'yla üzerinde mutabık kalınan iş birliği mutabakat zaptının imzalanmasının iki ülke arasındaki kardeşlik bağlarının güçlenmesine katkı sağlayacağını vurguladı. Forumun "Dijital Ortamda Mahremiyetin Temelleri: Düzenlemeye İlişkin İlkeler ve Yaklaşımlar" temalı oturumunda sunumlarını gerçekleştiren Recep KESKİN ise; 6698 sayılı Kanun ve ikincil mevzuatı ile Kurumumuz faaliyetlerine ilişkin bilgi aktarımında bulundu.

Öte yandan Kırgız Cumhuriyeti Başbakan Yardımcısı Edil BAISALOV ile birlikte Ajans Direktörü Adil SDYGALIEV ve heyetiyle iş birliğinin geliştirmesi amacına yönelik bir çalışma toplantısı düzenlendi. Ayrıca Bişkek Büyükelçimiz Ahmet Sadık DOĞAN nezdinde Büyükelçiliğimize ziyaret gerçekleştirildi.

KATAR ULUSAL SİBER GÜVENLİK AJANSINA ZİYARET

Kişisel Verilerin Korunması Kanunu'nda belirtilen ve görev alanına giren konularla ilgili yurt içinde ve yurt dışında yapılan çalışmalar doğrultusunda Kurumumuz tarafından 21-22 Ocak 2025 tarihlerinde Katar Devleti'ne çalışma ziyareti düzenlendi.

Bu çerçevede ilk olarak Kurum Başkanımız Prof. Dr. Faruk BİLİR ile Katar Ulusal Siber Güvenlik Ajansı Başkanı Abdulrahman bin Ali Al Farahid Al Malki ve Ulusal Siber Yönetişim ve Güvence İşleri Direktörü Dana Yousif Al-Abdulla, bir görüşme gerçekleştirdi.

Çalışma ziyareti kapsamında Kurumumuz heyeti 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Kurumumuz çalışmaları hakkında sunum yaptı. Daha sonra Kurumumuz heyetine Katar Ulusal Siber Güvenlik Ajansı ve çalışmaları hakkında bilgi verildi.

Öte yandan Kurum Başkanımız BİLİR, Doha Büyükelçimiz Dr. Mustafa GÖKSU'yu makamında ziyaret etti.

GÜRCİSTAN VERİ KORUMA OTORİTESİNİN KURUMUMUZU ZİYARETİ

Gürcistan Veri Koruma Otoritesi 18 Aralık 2024 tarihinde Kurumumuzu ziyaret etti.

Ziyaret kapsamında iki kurum arasında kişisel verilerin korunması konusunda yapılabilecek iş birliklerinin önemine vurgu yapılarak görüş alışverişinde bulunuldu.

FİLİPİNLER VERİ KORUMA OTORİTESİ İLE İŞ BİRLİĞİ

Kurumumuz ile Filipinler Cumhuriyeti Ulusal Mahremiyet Komisyonu (NPC) arasında veri koruma alanındaki iş birliğini güçlendirmek ve bu kapsamda yapılabilecek çalışmaları geliştirmek amacıyla 11 Şubat 2025 tarihinde mutabakat zaptı imzalandı.

İki kurum arasında iyi uygulamaların paylaşılmasına yönelik iş birliğinin genel çerçevesini çizen anlaşma, aynı zamanda kişisel veri mahremiyeti konusunda ortak çalışmalar yapılmasına da imkan tanımaktadır.

kvkkurumu

Kişisel Verileri Koruma Kurumu

Nasuh Akar Mahallesi 1407. Sokak
No.4 06520 Çankaya | ANKARA
T. 0312 216 50 00
www.kvkk.gov.tr