Kişisel Verileri Koruma Kurumu

BÜLTEN

Nisan - Temmuz 2024 Sayı:5

DİJİTAL ÇAĞDA MAHREMİYET: ÇOCUKLARIN KİŞİSEL VERİLERİNİN KORUNMASI

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Kişisel Verileri Koruma Kurumu
KVKK Bülten
www.kvkk.gov.tr
Sayı:5
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

Giriş 5

Makale 6

Kişisel Verileri Koruma Günü'nün Anlam ve Önemi 10

Çocukların Kişisel Verilerinin Korunması Hakkında Broşür Çalışması 12

Çocukların Kişisel Verilerinin Korunmasına İlişkin Tavsiyeler 14

Çocuklarınız İçin 5 Adımda Daha Güvenli Oyun 20

KVKK Okulda Projesi 22

Yapay Zekânın Düzenlenmesinde Yeni Bir Dönem: AB Yapay Zekâ Yasası 24

Öne Çıkan Gelişmeler 30

Bizden Haberler 38

Bundan 15-20 yıl önce, çocuklar sokaklarda oynayıp arkadaşları ile yüz yüze iletişim kurabilme konusunda daha etkindi. Şimdilerde ise tek bir tıkla oyun parkları, arkadaşlıklar, fotoğraf albümleri ve hatta neredeyse tüm dünya evimize sığıyor.

Günümüz çocukları sosyalleşme, eğlence ve iletişim ihtiyaçlarını büyük oranda internet ve sosyal medya üzerinden karşılıyor. Peki tüm bunlar olurken yanı başımızda neler gerçekleşiyor? Çocuğumuz internette neler yapıyor? Kimlerle sohbet ediyor, kendisi hakkında ne anlatıyor, hangi sitelere giriyor, hangi uygulamaları kullanıyor, buralarda hangi bilgilerini paylaşıyor? Kullandığı cihazı ya da sosyal ağ hesabını herkesin erişimine açık hale mi getiriyor? Yaşına uygun olmayan içeriklere maruz kalıyor mu?

Bunun gibi sorulabilecek pek çok soru var...

Bülten'in bu sayısında; çocukların kişisel verilerinin korunması için daha güvenli bir ortam oluşturmak adına neler yapılabileceği hususuna değinmeye çalıştık.

Tüm ilgililere faydalı olması temennisiyle, iyi okumalar dileriz.

DOÇ. DR. EMEL BADUR*
Çankaya Üniversitesi Hukuk Fakültesi
Medeni Hukuk Anabilim Dalı

SOSYAL MEDYADA ÇOCUĞA DAİR EBEVEYN PAYLAŞIMLARI (SHARENTING) VE ÇOCUĞUN ÖZEL HAYATI

İçinden geçtiğimiz günlerde teknolojik gelişmelerin baş döndürücü bir hızla yaşandığı, dijital ortamın hayatın merkezine konumlandığı ve bunların sonucunda sosyal medyada çocuk görünürlüğünün de giderek arttığı yadsınamaz bir gerçektir. Açıklanan yaşam şartlarında çocuğun pek çok kişisel verisi, pek çok veri sorumlusu tarafından işlenmektedir. Çocuğun kişisel verilerinin büyük bir kısmı, ona eğitim, sağlık, güvenlik ve diğer hizmetlerin sunulması ya da başkaca faydaların sağlanması için işlenmektedir. Çocuğun kişisel verilerinin ister rızaya ister diğer hukuka uygunluk sebeplerinden birine dayalı olarak işlendiği her durumda göz önünde bulundurulması gereken, bu işleme faaliyetinin çocuğun üstün yararı ilkesine hizmet etmesi gerekliliğidir. Ancak çocuğun kişisel verilerinin sosyal medyada paylaşılmasının, bu ilkeye hizmet ettiğinin söylenmesi mümkün görülmemektedir.

Çocukluğun insan yaşamının en korunmaya muhtaç dönemi olduğu ve hukuk sistemlerinin bu korumayı -kural olarak- çocuğun ebeveynlerine bıraktığı göz önünde bulundurulduğunda, çocuğun kişisel verilerinin korunmasını da sağlayacak kişilerin öncelikle onun ebeveynleri olduğu düşünülür. Ancak çocuğun barınması, beslenmesi ve sağlığının korunması açısından genellikle yerinde olan bu tercih, çocuğun kişisel verilerinin korunması söz konusu olduğunda her zaman doğru çıkmayabilir. Zira ebeveyn açısından sadece çocukla geçirilen mutlu anların, anıların -sınırlı sayıda ve tanınan- kişilerle paylaşılması anlamını taşıyan sosyal medya içeriklerinin, çocuğun kişisel verilerinin korunmasını tehlikeye düşürmesi mümkündür. Hukuk sistemlerinde rıza ehliyetine sahip olmayan çocukların kişisel verilerin işlenmesi konusundaki rıza açıklama yetkisi yasal temsilcisine bırakılırken, ebeveynleri tarafından çocuğun zararına olabilecek işlemeler yapılması ihtimali üzerinde durulmamıştır.

Özellikle sosyal medyanın giderek yaygınlaşması ve yetişkinlerin hayatındaki önemini arttırması, yetişkinler arasındaki mahremiyet ve özel hayat sınırlarının kendi iradeleri ile yeniden çizilmesine neden olmuştur. Ancak yetişkinler, mahremiyet anlayışlarını değiştirirken, sosyal medya paylaşımlarının içeriğini sadece kendileriyle sınırlı tutmak yerine, bu paylaşımlara çocuklarını da dahil etmeyi tercih etmişlerdir. Zira çocukların bizatihi kendileri ve görüntüleri başta olmak üzere; sergiledikleri sevimli ve eğlenceli hareketler etkileşim, takipçi ve beğeni kazanmak açısından fayda sağlamaktadır.

Mahremiyetin sınırlarının rıza ehliyetine sahip kişilerce ve kendi özel hayatlarıyla sınırlı olmak üzere yeniden belirlenmesinin önünde özel hukuktan kaynaklanan bir engel bulunmamakla birlikte; hukuken sorunlu alan, yetişkinlerin bu sınırların kapsamına çocuklarını dahil ettikleri yerde başlamaktadır. Muhtemeldir ki ebeveynler çocuklarının özel hayatını da kendi özel hayatlarının bir parçası olarak değerlendirmek eğilimindedirler. Ebeveynlerin özellikle yeni çocuk sahibi oldukları dönemde, sosyal hayattan uzaklaşmaları ve yalnızlaştıklarını hissetmeleri, sosyal medya etkileşim ve ilişkilerinin psikolojik gereksinimlerinin karşılanması açısından önemli bir işlev görmesine; hatta ebeveynlik deneyimlerini en iyi şekilde gerçekleştirdikleri konusunda toplumsal bir onay almalarına bile katkı sağlamaktadır.

Ancak gerek ebeveynlerin psikolojik sağlık refahlarına gerek takipçi ve beğeni sayılarına sağlanan katkı, çocukların kişisel verilerinin onların rızası aranmaksızın ana-babaları tarafından sosyal medyada paylaşılmasını hukuka uygun kılmaya yeterli değildir. Başka bir ifadeyle ebeveynlerin özel hayatıyla çocuğun özel hayatının kesişim kümesinin geniş olduğu bir gerçek olmakla birlikte; velayet sahibinin çocuğuyla ilgili yaptığı çeşitli sosyal medya paylaşımlarının (fotoğraf, video vb.), çocuğun özel hayatına ve kişilik değerlerine yönelik olduğu tartışmasızdır.

Türkçede henüz yerleşik bir karşılığı bulunmamakla birlikte, ana/babaların sosyal medyada çocuklarının özel hayatlarıyla ilgili düzenli (ve ayrıntılı) paylaşım yapmaları İngilizcede *"Sharenting" (paylaşanebeveynlik)* adı verilen özel bir terimle ifade olunmaya başlanmıştır. Kelimenin oluşturulma sebebi, sıklıkla görülen bir fiilin isimlendirilmesi ihtiyacıdır.[1] Sharenting İngilizce *"to share (paylaşmak)" ve "parenting (ebeveynlik etmek)"* kelimelerinin birleştirilmesiyle oluşturulan yeni bir sözcüktür.

Hatta sharenting kavramının yaratılmasından kısa bir süre sonra ebeveynlerin çocuklarına ilişkin ses ve görüntüleri aşırı (sıklıkla) paylaşmaları halini ifade eden *"Over sharenting"* kavramı da türetilmiştir. Ebeveynlerin çocuklarının kişisel verilerini sıklıkla paylaştığı durumlar blog yazarlığı (bloggerlık), sosyal medya fenomenliği (içerik üreticiliği, influencerlık), youtuberlık, insta-mom sayfaları paylaşımcılığı olarak öne çıkmakta ve sayılan adlarla isimlendirilerek yürütülmektedir. Ayrıca ana babaların çocuklarının sosyal medya içerik üreticisi olmaları konusundaki çabalarının da bu kapsamda değerlendirilmesi mümkündür.

Sharenting pek çok açıdan ve disiplin (çocuk gelişimi, psikoloji, etik vb.) tarafından eleştirilebilir bir uygulamadır. Zira bir yandan hukuk sistemleri, çocuğun kişisel verilerinin işlenmesine yönelik hukuki koruma mekanizmaları oluşturmaya çalışırken, öte yandan çocukların ebeveynleri, her gün daha fazla kişisel veriyi kendi rızalarıyla paylaşmaktadır. Ebeveynler tarafından paylaşılan bu veriler, ticari gelir elde etmek amacıyla veri toplayan işletmelerce elde edilip, daha sonra reklamcılara, özel okulların ve üniversitelerin kayıt/tanıtım ofislerine satılabilmektedir. Üstelik sharentingin etkileri sadece çocukluk dönemiyle sınırlı kalmamakta, bu dönemde yapılan paylaşımlar, çocuğun yetişkinlik dönemi üzerinde de olumsuz etkilerini sürdürebilmektedir.

Ebeveynlerin çocuklarıyla ilgili yaptıkları paylaşımların, rıza ehliyetine sahip olan ve bu paylaşımlara kendisi rıza gösteren çocuklara ilişkin olanlar istisna tutulmak kaydıyla, çocukların özel hayatlarına müdahale oluşturduğunun söylenmesi yanlış olmayacaktır. Üstelik bütün bu paylaşımların, çocuğun kişisel verilerinin işlenmesi suretiyle gerçekleştirildiği göz önünde bulundurulduğunda, işleme faaliyetini yapanın bizzat yasal temsilci olması nedeniyle, çocuğun kişisel verilerinin hukuka uygun şekilde ve yasal temsilcinin rızasıyla işlendiğinin kabulü de zordur.

Zira velayet sahibi ana ve/veya babanın sosyal medya paylaşımlarındaki, çocuklarını konu alan ifade özgürlüğünün sınırı, çocuğun kişilik hakkı ve üstün yararı ilkesidir. Başka bir ifadeyle çocuğun üstün yararına hizmet etmeyen hiçbir sosyal medya paylaşımının ve bu suretle çocuğun kişisel verisinin işlenmesinin, velayet sahibinin rızasıyla

*badur@cankaya.edu.tr, Orcid Id: 0000-0002-5133-8541.

1 ABD'de çocuklarının %92'sinin iki yaşına kadar ebeveynleri aracılığıyla dijital bir paylaşımda yer aldıkları belirtilmektedir. BESSANT, Claire: "Sharenting: Balancing The Conflicting Rights Of Parents and Children", Communications Law, C. 23, S. 1, 2018, s. 7.

hukuka uygun kılınması mümkün değildir.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GVKT) 2/2/c maddesinde ve Başlangıç kısmının 18. paragrafında; kişisel verilerin gerçek bir kişi tarafından, tamamen kişisel veya ev halkıyla ilgili bir faaliyet sırasında ve mesleki ya da ticari bir faaliyetle bağlantısı olmaksızın işlenmesi hallerinde Tüzüğün uygulanmayacağı belirtilmiştir. Hatta bu tür faaliyetler arasında sosyal ağ paylaşımlarının (ve diğer çevrimiçi faaliyetlerin) sayılabileceği de aynı paragrafta açıklığa kavuşturulmuştur. Bu durum özellikle Başlangıç kısmının 38. paragrafında çocukların kişisel verilerinin korunmasının önemine yapılan vurguyla çelişir nitelikte olmakla ve sharentingi önleyici bir mekanizmanın Tüzüğe dahil edilmemesiyle eleştirilmektedir. Sharenting mağduru çocukların GVKT kapsamında başvurabilecekleri hukuki mekanizmanın -hakkın kullanılma şartlarının varlığı halinde- unutulma hakkı olduğu belirtilmektedir.[2]

Buna karşılık Kişisel Verilerin Korunması Kanunu'nun (KVKK), Kanunun istisnalarına ilişkin 28/1/a maddesinde kullanılan ifadede "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*" hali, kapsam dışında bırakılmış olduğundan; ebeveynlerin sharenting çerçevesinde yaptığı işlemeler Türk Hukuku açısından KVKK'nın kapsamındadır. Bunun anlamı, sosyal medyada çocuğun kişisel verilerinin paylaşılması sonucunu doğuran her türlü paylaşımın KVKK'da düzenlenen hukuka uygunluk sebeplerine dayanmasının zorunlu olduğudur.

KVKK'da sharentinge dair doğrudan bir düzenleme olmaması velayet sahibinin herhangi bir sınırlama olmaksızın çocuğuna ait kişisel verileri istediği gibi paylaşabileceği anlamına gelmez. KVKK'da (ve GVKT'de) bu konuda özel düzenlemeye yer verilmediğinden ebeveynlerin çocuğa ait kişisel verileri işlemesinin sınırını, kişisel verilerin işlenmesine ilişkin genel ilkeler ve çocukların korunmasına dair mevzuat belirleyecektir. Buna göre hukuka uygunluk sebebi olsa dahi kişisel veriler, meşru amaçlara yönelik olarak sınırlı, ölçülü ve yeterli olacak şekilde işlenmelidir. Özellikle çocuğa bir yarar sağlamayan, hatta onu küçük düşüren özel yaşam ihlallerine yasal temsilci tarafından rıza gösterilmemesi gerektiğinin altı çizilmelidir.

Mahremiyet algısı ve rıza ehliyetinde yaşanan eksiklikler, özel hayatının korunması açısından, çocuğun kendisini, bir yetişkine kıyasla daha savunmasız hale getirmektedir. Çocuğun öz korumasında var olan bu eksiklik, hukuk sistemleri tarafından, çocuğun kişilik hakkının (ve bu başlık özelinde özel hayatına ilişkin kişilik değerinin) korunmasının, onun en yakını olan velayet sahibi/sahiplerine bırakılmasıyla giderilmeye çalışılmıştır. Velayet sahibi ana ve/veya babanın, çocuğun özel hayatını en iyi şekilde koruyacaklarına duyulan bu güven, özellikle saldırının bu kişilerden gelmesi halinde, hukuki koruma mekanizmasını yetersiz kılmaktadır. Sharenting aracılığıyla ebeveynler, hem çocuklarının kişisel bilgilerinin koruyucusu (bekçisi) hem de çocuklarının kişisel verilerinin ve hikayelerinin kamuya açık anlatıcıları olarak hareket etmektedirler.

2 Velayet sahiplerinin sharenting kapsamındaki uygulamalarının, ayırt etme gücü edinen çocuğu (veya çocukluktan erginliğe geçen kişiyi) rahatsız etmesi ve çocuğun veya erginin bu dijital içeriklerin kendisiyle bağına son verilmesini talep etmesi mümkündür. Kişinin ergin olduktan sonra kullandığı ve çocukluk dönemine ilişkin içeriklerin kaldırılmasını talep ettiği unutulma hakkı da bu kapsamda değerlendirilebilir. Bu kapsamdaki örnekte İtalya'da yaşayan 16 yaşındaki bir çocuk, annesine karşı rızası olmadan fotoğraflarını paylaştığı ve bunları kaldırmadığı gerekçesiyle açtığı davayı kazanmıştır. İtalyan mahkemeleri, annenin çocuğun fotoğraflarını sosyal medyadan kaldırmaması veya gelecekte de aynı şekilde fotoğraf paylaşması halinde 10.000 Euro ödemesine karar vermişlerdir. https://www.haberturk.com/italyada-cocugun-fotografini-paylasan-anneye-ceza1788741; https://www.bbc.com/turkce/haberler-dunya-42604622, (E. T. 18.03.2024).

KİŞİSEL VERİLERİ KORUMA GÜNÜ'NÜN ANLAM VE ÖNEMİ

Kişisel verilerin korunması bakımından bireyler arasındaki farkındalık ve bilinç düzeyi, en az idari ve teknik tedbirler kadar önem taşımaktadır. Bu önem dolayısıyla, günlük yaşam içerisinde maruz kalınan risk ve tehditlere karşı yeterli farkındalığa ulaşmak gerekmektedir.

Ülkemizin geleceğinin teminatı olan çocuklar da bir birey olarak kişisel verilerinin korunmasını isteme hakkına sahiptir. Bununla birlikte veri koruma bilincinin küçük yaşlardan itibaren zihinlere yerleştirilmesi, toplumda veri koruma kültürünün oluşmasına ve bu kültürün gelişmesine katkı sağlayacaktır.

Bu doğrultuda Kurumumuz ile Milli Eğitim Bakanlığı iş birliği içerisinde yürütülen çalışmalar neticesinde 1 Eylül 2018 tarihli Resmi Gazete'de yayımlanan "Milli Eğitim Bakanlığı Eğitim Kurumları Sosyal Etkinlikler Yönetmeliği"nde yapılan düzenleme ile Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girdiği gün olan 7 Nisan'ın ***"Kişisel Verileri Koruma Günü"*** olarak kutlanması ve okullarda "Kişisel Verileri Koruma Kulüpleri"nin kurulması kararlaştırılmıştır.

Bu tarihten itibaren her yıl 7 Nisan Kişisel Verileri Koruma Günü, Kurumumuzca düzenlenen çeşitli etkinlikler vasıtasıyla kutlanmaktadır. Ayrıca her yıl bu gün dolayısıyla ortaöğretim öğrencilerine yönelik olarak slogan ve karikatür, yüksek lisans ve doktora öğrencilerine yönelik olarak ise makale yarışmaları düzenlenmektedir.

Bu etkinlik ve yarışmalarla, öğrencilerin kişisel verilerin korunması konusundaki farkındalığını artırmak, veri koruma kültürünün çocuklar ve gençler arasında yaygınlaşmasını sağlamak amaçlanmaktadır.

7 Nisan Kişisel Verileri Koruma Günü;

- 2019 yılında düzenlenen program ile
- 2021 yılında çevrim içi gerçekleştirilen program ile
- 2022 yılında "Dijital Çağda Mahremiyet: Çocukların Kişisel Verilerinin Korunması" paneli ile
- Geçtiğimiz yıl "Dijital Çağda Çocukların Kişisel Verilerinin Korunması" etkinliği ile
- Bu yıl ise "Teknoloji ve Çocukların Kişisel Verilerinin Korunması" etkinliği ile

Kurumumuz tarafından kutlanmıştır.

ÇOCUKLARIN KİŞİSEL VERİLERİNİN KORUNMASI HAKKINDA BROŞÜR ÇALIŞMASI

Çocuklar arasında yeni teknolojilerin kullanımının yaygınlığı, çocuğun algı düzeyi ve yaşı itibarıyla kişisel verilerini paylaşmasının sonuçlarını öngörememesi, risklerin farkında olmaması, yasal haklarını ve bu hakların nasıl kullanılacağını bilmemesi ve ebeveyn kontrolünün dijital alanlarda zayıf olması gibi hususlar, çocukları çevrim içi ortamdaki risklere karşı savunmasız kılmaktadır.

Eğitim, sosyalleşme, eğlence, iletişim gibi amaçlarla internet ve sosyal medyanın çocuklar tarafından yoğun olarak kullanıldığı dikkate alındığında, çocukların kişisel verilerinin korunmasına özen göstermek ve onları muhtemel risklerden korumak önem arz etmektedir. Gelinen noktada, çocukların kişisel verilerinin korunmasına ilişkin ebeveynlere her zamankinden daha fazla sorumluluk düşmektedir.

Bu kapsamda, öncelikle ailelerin çocukların kişisel verilerinin korunması hususunda bilgi düzeyi ve farkındalıklarını artırması, akabinde çocuklarını bu konuda yönlendirerek kişisel veri mahremiyetinin gündelik sohbetlerinin bir parçası haline getirmeleri, yine çocuklara yönelik ürün ve hizmet geliştirenler tarafından Kişisel Verilerin Korunması Kanunu'na uyum konusunda azami özenin gösterilmesi gerekmektedir.

Buradan hareketle, geleceğimizin teminatı olan çocuklarımızın kişisel verilerinin etkin şekilde korunması amacıyla, Kurumumuz tarafından pratik önerilerin yer aldığı broşürler yayımlanmıştır[1].

1 Ayrıntılı bilgi için bkz. https://www.kvkk.gov.tr/Icerik/6737/Cocuklarin-Kisisel-Verilerinin-Korunmasi-Bakimindan-Dikkat-Edilmesi-Gerekenler

ÜRÜN VE HİZMET GELİŞTİRENLER TARAFINDAN DİKKAT EDİLMESİ GEREKENLER

ÇOCUKLARIN KİŞİSEL VERİLERİNİN KORUNMASI HAKKINA SAYGILI OLUNMASI

Çocukların haklarını bilmelerini ve kullanabilmelerini sağlayacak uygun politika ve mekanizmalar geliştirilmelidir.

KİŞİSEL VERİLERİN KORUNMASI KANUNU İLE BELİRLENEN USUL VE ESASLARA UYGUN HAREKET EDİLMESİ

Ürün ve hizmetlerde çocukların kişisel verilerinin işlenmesi söz konusu ise 6698 sayılı Kişisel Verilerin Korunması Kanunu'na uyum konusunda azami özen gösterilmelidir.

ÇOCUKLARIN KİŞİSEL VERİLERİNİN EN AZ SEVİYEDE İŞLENMESİ

Ürün ve hizmetlerde çocukların kişisel verilerinin işlenmesi gerekli ise veri minimizasyonu ilkesine uygun olarak veri işleme faaliyeti en az seviyede tutulmalıdır.

ÇOCUKLARA ÖZEL AYDINLATMA YAPILMASI

Ürün ve hizmetin hitap edeceği kitle çocuklar ise aydınlatma yükümlülüğü kapsamında çocukların algı düzeyine uygun bilgilendirici metinler hazırlanmalıdır. Gerekirse resim ve görsel efektlerle desteklenen daha anlaşılır, sade ve açık bir dil kullanılmalıdır.

ÇOCUKLARIN YAŞINI DOĞRULAYACAK SİSTEMLERİN KULLANILMASI

Mevcut teknoloji göz önünde bulundurularak çocuğun yaşını doğrulayacak sistemler kullanılmalıdır.

(Örneğin verilen açık rızayı kontrol etmek ve yaş doğrulaması yapmak için ancak o yaşlardaki bir çocuğun cevaplayabileceği sorular sorulabilir. Gerekli durumlarda velayet/vesayet hakkı sahiplerinin doğrulanmış iletişim bilgilerine bilgilendirme ve açık rıza onay metinleri gönderilebilir.)

ÇOCUKLARIN KİŞİSEL VERİLERİNİ İŞLERKEN VERİ GÜVENLİĞİNİ SAĞLAMAYA YÖNELİK TEKNİK VE İDARİ TEDBİRLERİN DAHA HASSAS BİR ŞEKİLDE ELE ALINMASI

Çocukların verilerinin işlendiği durumlarda, teknik ve idari tedbirlerin en üst seviyede alınmasına yönelik bir yaklaşım benimsenmelidir.

YETİŞKİNLER TARAFINDAN DİKKAT EDİLMESİ GEREKENLER

Çocuğumun Kişisel Verisini ve Mahremiyetini Nasıl Korurum?

Dijitalleşen hayatlarımız, çocuklarımızın çok erken yaşlarda cep telefonu, bilgisayar, tablet gibi cihazlarla, internet ve sosyal medya ile tanışmasına ve aktif birer kullanıcı olmasına yol açmıştır. Günümüzde çocuklar doğdukları andan itibaren ebeveynleri, küçük yaşlardan itibaren de bizzat teknolojinin kullanıcısı olarak kendileri tarafından paylaşılan kişisel verileri ile çevrim içi kimliklere sahip olmakta ve alışılagelmiş mahremiyet algısının dışına çıkmaktadır.

Bazen aile albümümüzdeki bir fotoğrafın misafirlere gösterilmesi bile belirli bir bilinç düzeyine gelen çocuklarımızı rahatsız ederken, çevrim içi dünyada bıraktıkları ayak izlerinin onları ne denli belirlenebilir ve savunmasız kılacağı konusunda önce kendimizi sonra çocuklarımızı bilgilendirmek ve basit birtakım önlemler almak son derece faydalı olacaktır.

- Dijital yaşamın bir gereği olarak çocuklarınızı kişisel veri, mahremiyet, istenmeyen (spam) ve önemsiz (junk) elektronik postalar gibi konular hakkında bilgilendirin ve bunun gündelik sohbetinizin bir parçası olmasını sağlayın.
- Mahremiyetlerine saygılı olacak şekilde, çocuklarınızın çevrim içi aktivitelerine dâhil olmak için vakit ayırın ve onları çevrim içi güvenlik hakkında bilgilendirin.
- Çevrim içi ortamlarda yer alan tehlikelerin gerçek dünyadaki tehlikelerden farklı olmadığının bilincinde olun. Öyle ki; çevrim içi ortamlar bazen daha ciddi tehlikeler arz edebilir.
- Çocuğunuza yönelik kişisel veri işleyen ürün ve hizmetlerin bilgilendirici metinlerini okuyun.

- Çocuklarınızın kişisel verilerini ve özellikle fotoğraflarını çevrim içi ortamlarda herkese açık bir şekilde paylaşmayın.
- Güçlü parolalar kullanın ve çocuklarınıza güçlü parola oluşturma konusunda bilgiler verin.
- Çocuklarınızın kişisel verilerine internet bağlantılı oyuncaklar, oyun konsolları, akıllı televizyonlar, saatler vb. üzerinden de erişilebileceğini, ayrıca ortak cihaz kullanımında tehlikenin yetişkinlere de yöneldiğini unutmayın.
- Çocuklarınızın sahip olduğu veya kullandığı bilgisayar, cep telefonu veya oyun konsolları için internet filtreleme özelliği kullanabileceğinizi unutmayın.

Çocuğum Sosyal Medya Kullanıyor, Kişisel Verilerini Nasıl Koruyabilirim?

- Çocuğunuzun sosyal medya hesabının gizli/onaya tâbi olması, kişisel verilerine sınırlı ve tanıdığı bir çevre tarafından ulaşılmasını sağlar.
- Sosyal medya kullanımı sırasında gerekli olmadıkça kamera kapağının ve mikrofonun kapalı olması olası ihlallerden çocuğunuzu ve sizi korur.
- Çocuğunuzu başkası adına hesap açma/profil oluşturma ve başkalarının verilerini izinleri olmadan paylaşma gibi hususların uygun olmadığı konusunda bilgilendirmek faydalı olur.

ÇOCUKLAR TARAFINDAN DİKKAT EDİLMESİ GEREKENLER

1. Adın, soyadın, adresin, yaşın ya da fotoğrafın gibi kişisel verilerin senden isteniyorsa ya da kullanılıyor ise bu konuda bilgilendirilme hakkın var.

2. Kişisel verilerinin özellikle sosyal medyada haberin olmadan kullanıldığını ya da paylaşıldığını fark edersen (örneğin birisi senin adına bir profil açmış olabilir) annene, babana ya da güvendiğin bir büyüğüne haber vermelisin.

   Çünkü sana ait bilgilerin bu şekilde kullanımı uygun değil ve bunu engellemek için kullanabileceğin hakların var.

3. Başkalarıyla paylaşmak istediğin ve istemediğin bilgileri dikkatli bir şekilde seçmelisin.

4. Sosyal medya veya uygulamalar aracılığı ile tanıştığın kişiler çoğu zaman dost canlısı olmayabilir. Bu kişiler senden fotoğraf, video, adres, okul adı gibi bilgilerini istediğinde, güvendiğin bir büyüğe danışmalısın.

5. Sen sildiğini düşünsen de, internette paylaştığın hiçbir şeyin kaybolmayacağını bilmelisin. Paylaştığın şeyler, karşına farklı şekilde çıkabilir. Bu yüzden sonradan pişman olabileceğin görüntü ve bilgileri paylaşmamalısın.

6. Eğer paylaşacağın bir fotoğrafta başka kişiler bulunuyorsa, fotoğrafları paylaşmadan önce o kişilerden izin almalısın. Bu kişiler kendi fotoğraflarının paylaşılmasını istemiyor olabilirler.

7. İnternet sitelerinin, internet bağlantılı oyuncakların, oyun konsollarının ya da uygulamaların; konum bilgin, fotoğraf arşivin, rehberin gibi sana özel birçok bilgiye kolayca erişebildiğini unutma.

   Gizlilik ayarları konusunda biraz araştırma yapman, güçlü parolalar kullanman ve çok gerekli olmadıkça kişisel verilerini paylaşmaman seni birçok tehlikeden koruyacaktır.

8. Bilgisayar, telefon ve tablet gibi kullandığın cihazlarda parolalarını seçerken başkalarının tahmin edemeyeceği parolalar bulmalı ve bunları kimseyle paylaşmamalısın.

9. Her zaman aynı arama motorunu ya da cihazda yüklü olanı kullanmak zorunda değilsin. İnternette arama yaparken yaşına uygun olarak tasarlanmış arama motoru özelliklerini tercih edebilirsin.

10. İnternette bazı siteler/uygulamalar yalnızca yetişkinler içindir. Bunları kullanmamalısın.

    Eğer kullandığın internet sitesi ya da uygulamaların sana uygun olup olmadığı konusunda şüphen varsa bir büyüğüne danışmalısın.

11. İnterneti keyifli ve güvenli bir şekilde kullanmak için internet tarayıcısı ayarlarını düzenlemelisin. Bunun için büyüklerinden yardım isteyebilirsin. Bu sayede maruz kalmaman gereken içeriklerden kendini koruyabilirsin.

12. İnternette vakit geçirirken şüphe uyandıran, olağan dışı bir durumla karşılaştığında, güvendiğin bir büyüğüne mutlaka haber vermelisin.

ÇOCUKLARINIZ İÇİN 5 ADIMDA DAHA GÜVENLİ OYUN

1 YAŞ SINIRINI KONTROL EDİNİZ

Yaş derecelendirmelerine bakarak hangi oyunun hangi yaş grubuna uygun olduğunu öğrenebilirsiniz.

2 OYUNUN EBEVEYN DENETİMİ OLUP OLMADIĞINA BAKINIZ

Bazı oyunlar, çocuğunuzun çevrim içi olduğu süreler, oynadığı oyunlar ve kullanıcı geçmişi gibi bilgileri sizinle otomatik olarak paylaşır.

Oyunun ebeveynler için bir denetim mekanizması sunup sunmadığını öğreniniz.

3 ÇOCUĞUNUZUN YABANCI KİŞİLERLE OYUN İÇİ YÖNTEMLER ÜZERİNDEN İLETİŞİME GEÇİP GEÇMEDİĞİNİ KONTROL EDİNİZ

Pek çok oyun, kullanıcılara çevrim içi sohbet, görüntülü veya sesli konuşma imkânı sağlamaktadır. Bazı oyunlarda çocuğunuz sadece kendi arkadaş listesinde olan kişilerle iletişime geçebilirken bazı oyunlarda ise herkese açık sohbet odalarında tanımadığı kişilerle iletişime geçebilir.

Bu nedenle oyunların kamera, ses, sohbet odası, çevrim içi iletişim gibi özelliklerinin olup olmadığına ve varsa hangi yaş grubunun kullanımına açık olduğuna dikkat edilmelidir.

4 OYUNUN GİZLİLİK AYARLARINI KONTROL EDİNİZ

Birçok oyun; konum bilgisi, telefon numarası, kişi listesi gibi bilgilere erişim izni isteyebilir.

Oyun indirilmeden önce hangi verilere erişim izni istendiği kontrol edilmelidir ve oyun ile herhangi bir ilişkisi bulunmayan kişisel veri taleplerine karşı dikkatli olunmalıdır.

5 OYUNUN AYDINLATMA METNİNİ GÖZDEN GEÇİRİNİZ

Çoğu oyun, oyuna giriş ana ekranında aydınlatma metnini sunduğu gibi bu metne internet sitesinde de yer vermektedir.

Çocuğunuz bir oyunu oynamadan önce oyunun, çocuğunuzun hangi verilerini ne amaçla topladığı gibi hususları kontrol etmenizi tavsiye ederiz.

KVKK OKULDA PROJESİ

Çocukların ve gençlerin kişisel verilerle tanışması, veri koruma bilinciyle yetişmesi ve buna yönelik farkındalık oluşması amacıyla birçok çalışma ve projeyi hayata geçiren Kurumumuz, bu kapsamda Milli Eğitim Bakanlığı ile iş birliği içerisinde 25 Nisan-24 Mayıs 2024 tarihleri arasında "KVKK Okulda Projesi"ni gerçekleştirdi.

Proje çerçevesinde Adana, Osmaniye, Sivas, Yozgat, Aydın, Manisa, Trabzon, Rize, Kırklareli, Edirne olmak üzere 10 ilimizde belirlenen ilköğretim okullarında 8. sınıf öğrencilerine yönelik Kurum personelimiz tarafından bilgilendirme etkinlikleri düzenlendi.

KVKK Okulda Projesinin amaçlarını; okul çağındaki gençler arasında kişisel veri farkındalığı oluşturmak, çevrim içi mahremiyet konusunda bilinç meydana getirmek ve kişisel verilerin korunmasına yönelik pratik bilgiler paylaşmak olarak sıralayan Kurum Başkanımız Prof. Dr. Faruk BİLİR, proje kapsamında gerçekleştirilen etkinliklerle kişisel verilerin korunması, kişisel veri farkındalığı ve kişisel veri güvenliği konularında öğrencilerin yaş gruplarına uygun olarak sunumlar yapıldığını, ayrıca kişisel verilerin korunmasıyla ilgili hazırlanan farkındalık ve bilgilendirme videolarının izletildiğini belirtti.

BİLİR, proje sayesinde öğrencilere güçlü parola oluşturma teknikleri, güvenli çevrim içi alışveriş, internet ortamında paylaşılan bilgiler konusunda nelere dikkat edilmesi gerektiği ve sosyal medyada kişisel verilerin korunması gibi konularda önemli hatırlatmalarda bulunduklarını ifade etti.

YAPAY ZEKÂNIN DÜZENLENMESİNDE YENİ BİR DÖNEM: AB YAPAY ZEKÂ YASASI

AB Yapay Zekâ Yasası (2024/1689), 12.07.2024 tarihli AB Resmî Gazetesi'nde yayımlandı[1]. Yapay zekânın potansiyel risklerini ve bu teknolojinin toplum üzerindeki etkilerini ele almak amacıyla oluşturulan ve dünya genelinde yapay zekâya ilişkin kapsamlı ilk yasal çerçeve olan bu düzenlemenin getirdiği temel kurallar ile yapay zekâ sistemlerinin temel haklara, güvenliğe ve etik ilkelere saygı göstermesini sağlamak ve güçlü/etkili yapay zekâ modellerinin risklerini ele alarak Avrupa'da ve ötesinde güvenilir yapay zekânın teşvik edilmesi amaçlanmaktadır.

Düzenleme kapsamında, farklı gereklilikler ve yükümlülüklere tabi yapay zekâ sistemleri için "risk temelli yaklaşıma" uygun bir sınıflandırma sunulmaktadır. Bu çerçevede örneğin; "kabul edilemez" riskler ortaya çıkaran birtakım yapay zekâ sistemleri yasaklanırken; bireylerin sağlığı, güvenliği veya temel hakları üzerinde zararlı etkiler doğurabilecek "yüksek riskli" yapay zekâ sistemlerine, belirli yükümlülüklerin yerine getirilmesi koşuluyla, izin verilmektedir.

Bu çerçevede yazının devamında; mevcut düzenlemenin amacı ve kapsamı, getirdiği yenilikler ve ortaya çıkardığı temel zorluklar, risk kategorilerine göre yapay zekâ sistemlerinin sınıflandırılması ve ihlal durumunda öngörülen yaptırımlar gibi hususlar, *IAPP AI Governance Center* tarafından hazırlanan *"EU AI ACT:101"* başlıklı çalışma[2] üzerinden özetlenmiştir.

1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

2 https://iapp.org/resources/article/eu-ai-act-101/

YAPAY ZEKÂ YASASI'NIN AMACI

» AB değerleri ile uyumlu bir şekilde, AB'de yapay zekâ geliştirilmesi, pazarlanması ve kullanımı için kapsamlı bir yasal çerçeve oluşturmak.

» Sağlık, güvenlik ve temel hakların -demokrasi, hukukun üstünlüğü ve çevrenin korunması da dahil olmak üzere- yüksek düzeyde korunmasını sağlarken, insan merkezli ve güvenilir yapay zekânın benimsenmesini teşvik etmek.

» AB'de yapay zekâ sistemlerinin zararlı etkilerini azaltırken yeniliği desteklemek.

YAPAY ZEKÂ YASASI'NIN GETİRECEĞİ TEMEL DEĞİŞİKLİKLER

» Yapay zekâ sistemlerini risk düzeyine göre sınıflandırır ve risk sınıflandırmasına bağlı olarak geliştirme, dağıtım *(deployment)* ve kullanım gerekliliklerini zorunlu kılar.

» Genel amaçlı yapay zekâ modellerini denetlemek, standartlar ve test uygulamaları geliştirilmesine katkıda bulunmak ve üye devletler arasında kuralları uygulamak üzere Yapay Zekâ Ofisi'ni *(AI Office)*; Avrupa Komisyonu ve üye devletlerin yetkili otoritelerine tavsiye vermek ve yardımcı olmak üzere Yapay Zekâ Kurulunu *(AI Board)*; Kurula ve Komisyona tavsiyede bulunmak ve teknik uzmanlık sağlamak üzere Danışma Forumunu *(Advisory Forum)*; Yasa'nın uygulanmasını ve icrasını desteklemek üzere bağımsız uzmanlardan oluşan Bilimsel Paneli *(Scientific Panel)* kurar.

» Kabul edilemez risk taşıyan yapay zekâyı yasaklar.

» Temel haklar etki değerlendirmeleri ve uygunluk değerlendirmeleri de dahil olmak üzere, yüksek riskli yapay zekâ sistemleri için artırılmış teknik ve belgeleme gereklilikleri getirir.

» İnsan gözetimi ve veri yönetişimi gerektirir.

YAPAY ZEKÂ YASASI'NIN ORTAYA ÇIKARDIĞI TEMEL ZORLUKLAR

» Yapay zekâ sistemlerinin geliştirilmesi ve kullanımında sürdürülebilir ve sorumlu veri işleme yoluyla kişisel verilerin, özel hayatın ve iletişimin gizliliğinin korunmasına ilişkin temel hakları korumak.

» Yapay zekâ ekosisteminde yeniliği ve rekabetçiliği teşvik etmek ve gelişimini kolaylaştırmak.

» Yapay Zekâ Yasası ile veri koruma, fikri mülkiyet ve veri yönetişimi de dahil olmak üzere yapay zekâ için geçerli olan mevcut kurallar arasındaki etkileşimi anlamak.

» Oluşmakta olan karmaşık denetim ve uygulama paydaş haritasında yolunu bulmak.

» Kuruluşlar içerisinde uygun çok disiplinli yönetişim yapıları tasarlamak ve bunları uygulamak.

YAKLAŞMAKTA OLAN ÖNEMLİ TARİHLER

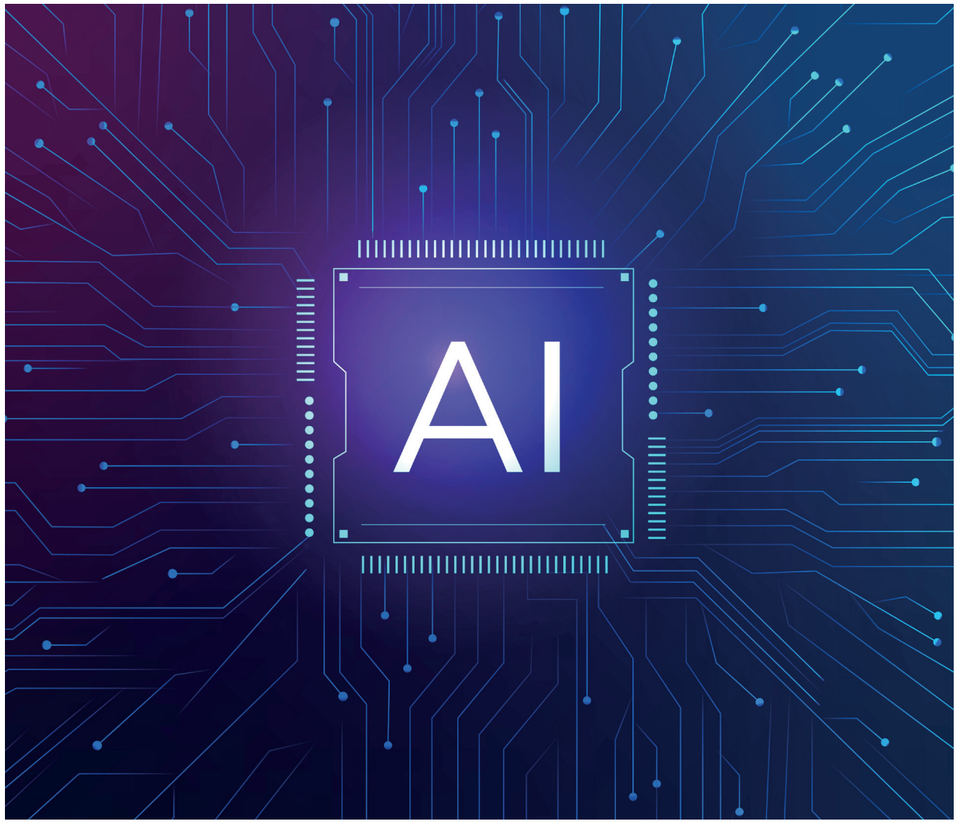
» Yapay Zekâ Yasası, AB Resmî Gazetesi'nde 12.07.2024 tarihinde yayımlanmış olup 01.08.2024 tarihinde yürürlüğe girmiştir. Yürürlüğe girmesinden 24 ay sonra, aşağıdaki kademeli yaklaşımla, tamamen uygulanabilir olacaktır.

» 02.02.2025: Kabul edilemez risk taşıyan yapay zekâya ilişkin yasaklar uygulanabilir hâle gelecektir.

» 02.08.2025: Genel amaçlı yapay zekâ yönetişimine ilişkin yükümlülükler uygulanabilir hâle gelecektir.

» 02.08.2026: Yüksek risk taşıyan sistemlere ilişkin yükümlülükler de dâhil olmak üzere Yapay Zekâ Yasası'nın tüm kuralları uygulanabilir hâle gelecektir.

» 02.08.2027: Diğer tüm yüksek riskli sistemlere ilişkin yükümlülükler uygulanabilir hâle gelecektir.



KAPSAM İÇİNDEKİ KURULUŞLAR: Üçüncü bir ülkede yerleşik olsa dahi, AB pazarına yerleştirilen, AB pazarında hizmete sunulan veya AB'de kullanılan yapay zekâ sistemlerinin veya genel amaçlı yapay zekâ modellerinin sağlayıcıları, ithalatçıları ve dağıtıcıları.

"YAPAY ZEKÂ SİSTEMİ"NİN TANIMI: Değişken düzeylerde özerklikle çalışacak şekilde tasarlanmış, dağıtım sonrası adaptasyon sergileyebilen ve aldığı girdilere dayanarak açık veya örtülü hedefler doğrultusunda tahmin, içerik, tavsiye veya kararlar gibi çıktılar üreten, bu çıktılarla fiziksel veya sanal ortamları etkileyebilen makine tabanlı bir sistem.

RİSK DÜZEYLERİ/KATEGORİLERİ

A. Yasaklanmış Yapay Zekâ Uygulamaları

Temel hakları ihlal etmesi nedeniyle AB değerlerine aykırı olan zararlı yapay zekâ kullanımlarının sınırlı bir kümesi olup şunları içermektedir:

- Sosyal davranış puanlama sistemleri
- İş yerinde ve eğitimde duygu tanıma sistemleri
- Bireylerin yaşları veya engellilik durumları gibi savunmasızlıklarından faydalanmak için kullanılan yapay zekâ
- Davranışsal manipülasyon veya özgür iradenin engellenmesi
- Yüz tanıma için, hedefleme yapılmaksızın yüz görüntülerinin kazınması *(scraping)*
- Belirli hassas özellikler kullanan biyometrik sınıflandırma sistemleri
- Belirli öngörücü kolluk uygulamaları
- Sınırlı ve yetkilendirilmiş durumlar haricinde, kolluk kuvvetlerinin gerçek zamanlı biyometrik tanımlamayı kamuya açık olarak kullanması

B. Yüksek Riskli Yapay Zekâ Sistemleri

Sağlık, güvenlik veya temel haklar açısından önemli risk taşıyan yapay zekâ sistemleri, aşağıdaki kategoriler dahil olmak üzere:

- Profilleme
- Tıbbi cihazlar
- Araçlar
- Duygu tanıma sistemleri
- Kolluk kuvveti
- Kredi puanlama

Bir ürünün güvenlik bileşeni olarak kullanılan veya kendisi bir ürün olan ve ilgili AB sektörel ürün güvenliği yasaları tarafından düzenlenen yapay zekâ sistemleri.

C. Genel Amaçlı Yapay Zekâ Modelleri

Önemli bir genellik sergileyen, piyasada nasıl konumlandırıldıklarından bağımsız olarak çok çeşitli görevleri yetkin bir şekilde yerine getirme kapasitesine sahip olan ve çeşitli alt sistemlere ya da uygulamalara entegre edilebilen yapay zekâ modelleri.

D. Sistemik Riskler Taşıyan Genel Amaçlı Yapay Zekâ Modelleri

İleri düzey genel amaçlı yapay zekâ modellerinde kaydedilen yeteneklere eş değer veya bu yetenekleri aşan "yüksek etki kapasitesi"ne sahip genel amaçlı yapay zekâ modelleri.

Bu modeller aşağıdakilerden biri olmalıdır:

- Uygun teknik araçlar, göstergeler ve kriterler kullanılarak değerlendirilen yüksek etki kapasitelerine sahip olmaları.
- Komisyon veya Bilimsel Panel tarafından sistemik riskler taşıyan genel amaçlı yapay zekâ olarak belirlenmeleri.

E. Şeffaflık Gereklilikleri

Belirli yapay zekâ sistemlerinin sağlayıcıları ve dağıtıcılarına *[deployers]* özel şeffaflık yükümlülükleri getirilmektedir.

Bir yapay zekâ sistemi; hem şeffaflık gerekliliklerine hem de yüksek riskli yapay zekâ sistemleri veya genel amaçlı yapay zekâ modellerine ilişkin gerekliliklere tabi olabilir.

TEMEL GEREKLİLİKLER

A. Yasaklanmış Yapay Zekâ Uygulamaları

Bu tür yapay zekâ sistemleri, Yapay Zekâ Yasası kapsamında yasaklanmıştır.

B. Yüksek Riskli Yapay Zekâ Sistemleri

Bu tür sistemlerde sağlayıcıların, aşağıdakileri temin etmeleri gerekmektedir:

- Risk yönetimi
- Veri kalitesi ve yönetişimi
- Belgeleme ve izlenebilirlik
- Şeffaflık
- İnsan gözetimi
- Doğruluk, siber güvenlik ve sağlamlık
- Uygunluk değerlendirmeleri yoluyla uyumluluğun kanıtlanması
- Kamu otoriteleri tarafından kullanılıyor ise, kolluk kuvvetleri veya göç ile ilgili kullanımlar haricinde, kamuya açık bir AB veri tabanına kayıt yapılması

C. Genel Amaçlı Yapay Zekâ Modelleri

Sağlayıcıların, aşağıdakileri temin etmeleri gerekmektedir:

» Temel haklar etki değerlendirmeleri ve uygunluk değerlendirmeleri gerçekleştirilmelidir.

» Sistemik riskleri sürekli olarak değerlendirmek ve bunları azaltmak için risk yönetimi ve kalite yönetim sistemleri uygulanmalıdır.

» Bireyler, yapay zekâ ile etkileşime girdiklerinde bilgilendirilmelidirler. Yapay zekâ içeriği etiketlenmeli ve tespit edilebilir olmalıdır.

» Doğruluk, sağlamlık ve siber güvenlik açısından test edilmeli ve izlenmelidir.

Sistemik risk taşıyan genel amaçlı yapay zekâ modelleri, daha fazla test ve raporlama gerekliliklerine tabidir.

D. Sistemik Riskler Taşıyan Genel Amaçlı Yapay Zekâ Modelleri

Sistemik riskler taşıyan genel amaçlı yapay zekâ modelleri için belirli yükümlülükler şunları içermektedir:

» Standartlaştırılmış model değerlendirmesi ve saldırı testleri

» Olası sistemik risklerin değerlendirilmesi ve azaltılması

» Ciddi olayların ve düzeltici önlemlerin belgelendirilmesi

» Sistemik riskler taşıyan genel amaçlı yapay zekâ modellerinin yeterli düzeyde siber güvenlik ve fiziksel altyapı seviyesine sahip olması

» Uygulama kurallarına uyum sağlanması

» Ticari sırların yanı sıra, elde edilen her türlü bilgi veya belge için 78. maddede belirtilen gizlilik gerekliliklerine uyum sağlanması

E. Şeffaflık Gereklilikleri

Gerçek kişilerle doğrudan etkileşime giren yapay zekâ sistemlerinin sağlayıcıları, bireysel kullanıcıların bir yapay zekâ sistemi ile etkileşimde olduklarının farkında olmalarını garanti edecek şekilde yapay zekâ sistemleri tasarlamalı ve geliştirmelidir.

Sentetik ses, görüntü, video veya metin içeriği üreten ve genel amaçlı yapay zekâ sistemlerinin sağlayıcıları, çıktıların makine tarafından okunabilir bir formatta işaretlendiğinden ve yapay zekâ tarafından oluşturulduğunda veya manipüle edildiğinde bunun tespit edilebildiğinden emin olmalıdır.

Duygu tanıma veya biyometrik sınıflandırma sistemlerinin dağıtıcıları *[deployers]*, sistemin işleyişi hakkında gerçek kişileri bilgilendirmelidir.

Kamuyu ilgilendiren konularda kamuyu bilgilendirmek amacıyla *deepfake* üreten veya metinleri değiştiren yapay zekâ sistemlerinin dağıtıcıları, açıklama gerekliliklerine uymalıdırlar.

ÖNEMLİ HÜKÜMLER

Şeffaflık: Belirli yapay zekâ sistemlerine, örneğin sohbet botlarının kullanımı aracılığıyla manipülasyon riskinin açık olduğu durumlar gibi, gereklilikler getirilmiştir. Kullanıcılar, bir makine ile etkileşimde olduklarının farkında olmalıdırlar.

Temel Haklar Etki Değerlendirmeleri: Kamu hukuku tüzel kişileri, kamu hizmeti sağlayan özel operatörler ve kredibiliteyi, acil durum çağrılarını ya da hayat ve sağlık sigortası risk ve fiyatlandırmasını değerlendirmek için yapay zekâ sistemlerini kullanan özel operatörler, dağıtımdan önce, sistemlerin temel haklar üzerindeki etkisini değerlendirmelidir. Veri koruma etki değerlendirmesi gereken durumlarda, temel haklar etki değerlendirmesi, söz konusu veri koruma etki değerlendirmesi ile birlikte yürütülmelidir.

Uygunluk Değerlendirmeleri: Ürünlerin güvenlik bileşenleri olan veya kendileri de AB ürün güvenliği yasaları kapsamında bulunan yapay zekâ sistemleri için, bu sistemler AB pazarına sürülmeden önce veya yüksek riskli bir yapay zekâ sistemi önemli ölçüde değiştirildiğinde uygunluk değerlendirmeleri gerçekleştirilmelidir. Yapay zekâ sistemlerinin ithalatçıları, yabancı sağlayıcının, öncesinde uygunluk değerlendirmesi prosedürünü uygun bir şekilde yürüttüğünden emin olmalıdır.

Üretici Yapay Zekâ: Sentetik ses, görüntü, video veya metin içeriği üreten sağlayıcılar, içeriğin makine tarafından okunabilir bir formatta işaretlenmesini ve yapay olarak üretilmiş veya manipüle edilmiş olarak tespit edilebilir olmasını sağlamalıdırlar.

UYGULAMA VE CEZALAR

Avrupa Komisyonu bünyesinde yer alan Yapay Zekâ Ofisi, model ve sistemin aynı sağlayıcı tarafından temin edildiği genel amaçlı yapay zekâ modellerine dayalı yapay zekâ sistemlerini denetleyecektir. Bu Ofis, pazarın gözetim otoritesinin yetkilerine sahip olacaktır. Ulusal pazar gözetim otoriteleri, diğer tüm yapay zekâ sistemlerinin denetiminden sorumludur.

Yapay Zekâ Ofisi, üye ülkeler arasındaki yönetişimi koordine etmek ve genel amaçlı yapay zekâ ile ilgili kuralların uygulanmasını denetlemek için çalışacaktır.

Üye devlet otoriteleri, uyarılar ve parasal olmayan tedbirler de dahil olmak üzere, cezalar ve diğer uygulama tedbirlerine ilişkin kuralları belirleyecektir.

Bireyler, pazar gözetimi faaliyetlerini başlatabilecek yetkili ulusal makama, ihlal durumuna yönelik olarak şikâyette bulunabilirler. Yasa'da bireysel zararlar öngörülmemektedir.

Şunlar için cezalar öngörülmektedir:

» Yasaklanmış yapay zekâ ihlallerinde; küresel yıllık cironun %7'sine veya 35 milyon avroya kadar,

» Diğer ihlallerin çoğunda; küresel yıllık cironun %3'üne veya 15 milyon avroya kadar,

» Otoritelere yanlış bilgi verilmesi durumunda; küresel yıllık cironun %1'ine veya 7.5 milyon avroya kadar.

Yapay Zekâ Kurulu; düzenlemenin uygulanması konusunda tavsiyelerde bulunacak, ulusal otoriteler arasında koordinasyon sağlayacak ve öneriler ile görüşler yayımlayacaktır.

DAHA FAZLA DÜZENLEME YAPILMASI

Komisyon, aşağıdaki konularda düzenlemeler çıkarabilir:

» Yapay zekâ sisteminin tanımları

» Yüksek riskli yapay zekâ için kriterler ve kullanım örnekleri

» Sistemik risk taşıyan genel amaçlı yapay zekâ modellerine ilişkin eşikler

» Genel amaçlı yapay zekâ için teknik belgeleme gereklilikleri

» Uygunluk değerlendirmeleri

» AB uygunluk beyanları

Yapay Zekâ Ofisi, genel amaçlı yapay zekâ modelleri sağlayıcılarının yükümlülüklerini kapsayacak, ancak bunlarla sınırlı olmayacak şekilde, uygulama kuralları hazırlayacaktır. Uygulama kuralları, düzenlemenin yürürlüğe girmesinden sonraki en geç dokuz ay içerisinde hazır olmalı ve uygulanmaya başlamadan önce en az üç aylık bir süre tanınmalıdır.

REHBER, ÇALIŞMA VE DÜZENLEYİCİ İŞLEMLER

» AB Yapay Zekâ Yasası (2024/1689), 12.07.2024 tarihli AB Resmî Gazetesi'nde yayımlandı[1]. Bahse konu Yasa, AB Resmî Gazetesi'nde yayımlanmasını takip eden yirminci günde yürürlüğe girmiştir. Yasanın, kademeli bir yaklaşımla 36 ay içerisinde tam olarak uygulanmasına geçilecektir. Yapay zekânın potansiyel risklerini ve bu teknolojinin toplum üzerindeki etkilerini ele almak amacıyla oluşturulan, dünya genelinde yapay zekâya ilişkin kapsamlı ilk yasal çerçeve olan bu düzenlemenin getirdiği temel kurallar ile yapay zekâ sistemlerinin temel haklara, güvenliğe ve etik ilkelere saygı göstermesini sağlamak ve etkili yapay zekâ modellerinin risklerini ele alarak Avrupa'da ve ötesinde güvenilir yapay zekânın teşvik edilmesi amaçlanmaktadır.

» Ülkemizin Ulusal Yapay Zekâ Stratejisi 2024-2025 Eylem Planı yayımlandı[2] .

» Avrupa Komisyonu bünyesindeki bir uzman çalışma grubu tarafından hazırlanan *"AB-ABD Yapay Zekâ Terminolojisi ve Taksonomisi"* başlıklı çalışmanın güncellenmiş versiyonu yayımlandı [3]. Alana yönelik ortak bir terminoloji oluşturulması adına oldukça önem taşıyan bu çalışmada, AB ve ABD'de yayımlanan çeşitli dokümanlara atıfta bulunulmak suretiyle, ilk versiyondan farklı olarak 13 adet yeni terim eklenmiş ve 24 terim üzerinde değişikliğe gidilmiştir.

» Avrupa Parlamentosu Araştırma Servisi (EPRS), yapay zekâ ve siber güvenlik arasındaki ilişkinin üç farklı boyutu ile konu alındığı bir çalışma yayımladı[4]. Bu çerçevede bahse konu çalışmada; yapay zekânın siber güvenliği, siber güvenliğin sağlanmasını desteklemek üzere yapay zekâ kullanılması ve yapay zekânın siber güvenliğe yönelik yeni tehditler yaratma potansiyelini içerecek şekilde yapay zekânın kötü amaçlarla kullanılması hususları ele alınmaktadır.

» Avrupa Komisyonu, Veri Yasası'na *(Data Act)* ilişkin genel bir bakış sunulan rehberini yayımladı[5]. Bahse konu rehberde, verileri (özellikle endüstriyel verileri) daha erişilebilir ve kullanılabilir hâle getirmek, veriye dayalı inovasyonu teşvik etmek ve verilerin kullanılabilirliğini artırmak suretiyle AB'nin veri ekonomisini geliştirme ve rekabetçi bir veri pazarını teşvik etme gibi amaçları gerçekleştirmek üzere tasarlanmış Veri Yasası'nın kapsamı, hedefleri ve pratikte nasıl uygulanacağı gibi hususlara yer verilmektedir.

» Avrupa Veri Koruma Denetçisi (EDPS) Wojciech Wiewiórowski, Kurumun 2023 yılına ilişkin raporunun sunumunu gerçekleştirdi[6]. Bu kapsamda, dijital ve düzenleyici gelişmeler ışığında 2023 yılının uyum sağlama yılı olduğunu vurgulayan Wiewiórowski; AB'de ve ötesinde veri koruma standartlarını yükseltmek için çok taraflı ve sınır ötesi iş birliğinin her zamankinden daha önemli olduğu ve EDPS'nin 20. yıl dönümünün kutlandığı bu yılda, önümüzdeki yirmi yıllık süreçte veri korumaya ilişkin karşılaşılabilecek zorlukları öngörmenin ve bunlara karşı hazırlıklı olmanın önem taşıdığı gibi hususlara işaret etti.

» Fransa Veri Koruma Otoritesi (CNIL), 2023 yılına ilişkin faaliyet raporunu yayımladı[7]. Bahse konu raporun bulguları arasında; Otorite'ye iletilen şikâyetlerde bir önceki yıla kıyasla %35 oranında artış yaşandığı, özel bir çevrim içi hizmet aracılığıyla dolaylı şekilde erişim hakkının kullanılması (belirli bankacılık veya polis dosyalarına erişim kapsamında) hususunda bir önceki yıla kıyasla %217'lik bir artış meydana geldiği, Otorite'nin internet sitesinin yıl içerisinde 11.8 milyon kez ziyaret edildiği ve bu durumun veri korumaya yönelik olarak gitgide artan ilginin bir göstergesi olduğu gibi belirlemeler yer almakta ve Otorite tarafından gerçekleştirilen çeşitli faaliyetlere yönelik bilgilendirmede bulunulmaktadır.

» Yeni Zelanda Mahremiyet Komisyonerliği Ofisi, çocukların çevrim içi mahremiyetlerinin korunmasına ilişkin olarak çeşitli kuruluşlardan ve devlet kurumlarından geri dönüşlerin alındığı bir proje kapsamında ulaşılan anket sonuçlarını yayımladı[8]. Çalışma kapsamında vurgulanan sonuçlar arasında; sosyal medyanın büyük bir endişe kaynağı olduğu ve çocukların

1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689, 12.07.2024.

2 https://cbddo.gov.tr/duyurular/6846/ulusal-yapay-zeka-stratejisi-2024-2025-eylem-plani-yayimlandi, 24.07.2024.

3 https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence-second-edition, 05.04.2024.

4 https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2024)762292, 24.04.2024.

5 https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained, 17.04.2024.

6 https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-annual-report-adaptability-changing-world_en, 09.04.2024. Bahse konu yıllık raporu görüntülemek için bkz. https://www.edps.europa.eu/data-protection/our-work/publications/annual-reports/2024-04-09-annual-report-2023-adaptability-changing-world_en, 09.04.2024.

7 https://www.cnil.fr/en/cnil-publishes-its-annual-report-2023, 23.04.2024.

8 https://privacy.org.nz/publications/statements-media-releases/new-survey-shows-we-all-need-to-sharpen-up-about-privacy-risks-for-kids/, 17.04.2024.

mahremiyetinin korunmasına yönelik riskleri yönetmek için bir dizi düzenleme değişikliğine *(mevcut Yasa'nın unutulma hakkını içerecek şekilde değiştirilmesi, çocuğun yüksek yararının gözetilmesi zorunluluğunun getirilmesi veya bu konuda uygulama kuralları oluşturulması vb. gibi)* ihtiyaç duyulduğu, profesyonelleri/ebeveynlerin/çocukların mahremiyet risklerini daha iyi anlamalarına yardımcı olmak için daha fazla rehberlik sağlanmasının önem taşıdığı, çocukların mahremiyetini ihlal eden kuruluşlara daha yüksek cezalar uygulanmasının fayda sağlayabileceği ve çocukların fotoğraflarını sosyal medyada paylaşmanın riskleri konusunda ebeveynleri bilinçlendirebilecek bir bilgilendirme kampanyası başlatılmasının yararlı olabileceği gibi hususlar yer almaktadır.

» Avrupa Parlamentosu Araştırma Servisi (EPRS), sanal dünyalarda *(metaverse)* çocukların korunmasına yönelik bir çalışma yayımladı[9]. Bahse konu çalışmada; sanal dünyanın sunduğu fırsatlar ile ortaya çıkardığı zorluklar ve bu evrenlerde çocukların korunmasına yönelik olarak AB ile özel sektör kuruluşları tarafından atılan adımlara yönelik bilgiler paylaşılmaktadır.

» OECD tarafından yapay zekâ, veri ve rekabet arasındaki ilişkinin ele alındığı bir çalışma yayımlandı[10]. Bu çerçevede bahse konu çalışmada; üretici yapay zekâya yönelik bilinmesi gerekenler (potansiyel ekonomik etkisi, üretici yapay zekâ yaşam döngüsü, bu modellerin kullanımı vb.), yapay zekâ arzında rekabet (yapısal faktörler, verinin elde edilebilirliği, geçiş maliyetleri, ekosistemden kaynaklanan unsurlar vb.), rekabet otoriteleri tarafından kullanılabilecek araçlar, rekabet politikası ve yapay zekâya ilişkin olarak gelecekte karşılaşılabilecek hususlar gibi konular incelenmektedir.

» 03.05.2024 tarihinde yapılan OECD Bakanlar Konseyi Toplantısında (MCM), "OECD Yapay Zekâ İlkeleri"nde yapılan revizyonların kabul edildiği duyuruldu[11]. Genel amaçlı ve üretici yapay zekânın ortaya çıkışı da dâhil olmak üzere yapay zekâ teknolojilerinde meydana gelen son gelişmelere yanıt olarak güncellendiği belirtilen ilkelerin; mahremiyet, fikri mülkiyet hakları, güvenlik ve bilgi bütünlüğü gibi yapay zekâ ile ilişkili zorlukları daha doğrudan bir şekilde ele aldığı ifade edilmektedir.

» Avrupa Konseyi Yapay Zekâ ve İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi'nin 17.05.2024 tarihinde kabul edildiği duyuruldu[12]. Bu konuda hukuki açıdan bağlayıcılık taşıyan ilk uluslararası sözleşme niteliğini haiz olan metin ile; yapay zekâ sistemlerinin yaşam döngüsü içerisinde gerçekleştirilen faaliyetlerin insan hakları, demokrasi ve hukukun üstünlüğü ile tamamen tutarlı olması ve diğer yandan da teknolojik ilerleme ve yeniliğe destek olunmasının sağlanması amaçlanmaktadır. İnsan hakları, demokrasi ve hukukun üstünlüğüne ilişkin mevcut uluslararası standartları tamamladığı ve teknolojideki hızlı ilerlemelerden kaynaklanabilecek yasal boşlukları doldurmayı hedeflediği belirtilen Sözleşme'nin zamana karşı dayanıklı olabilmek adına teknolojiyi düzenlemediği ve esasen teknoloji açısından tarafsız bir yaklaşım benimsediği ifade edilmektedir. Yapay zekâ sistemlerinin, kamu otoriteleri (kendi adlarına hareket eden özel sektör aktörleri dâhil) ve özel sektör aktörleri tarafından kullanılmasını kapsayan Sözleşme'de, bu sistemlerin kullanımında uyulması gereken ilkeler; (1) İnsan onuru ve bireysel özerklik, (2) Şeffaflık ve gözetim, (3) Hesap verebilirlik ve sorumluluk, (4) Eşitlik ve ayrımcılık yapmama, (5) Mahremiyete ve kişisel verilerin korunmasına saygı, (6) Güvenilirlik ile (7) Güvenli inovasyon şeklinde sayılmıştır.

» Avrupa Veri Koruma Denetçisi (EDPS), üretici yapay zekâ sistemleri kullanılırken kişisel verilerin korunmasına ilişkin düzenlemelere nasıl uyum sağlanabileceği konusunda pratik tavsiyeler sunulan bir metin yayımladı[13]. Bu çerçevede bahse konu metinde; üretici yapay zekâdan ne anlaşılması gerektiği, üretici yapay zekâ sistemleri içeren süreçlere ilişkin olarak veri koruma otoritelerinin rolü, üretici yapay zekâ sistemlerinin kullanımının kişisel verilerin işlenmesini içerip içermediğinin nasıl bilinebileceği, veri koruma etki analizi gerçekleştirilmesi gerekebilecek olan durumlar, bu sistemlerin kullanımı kapsamında kişisel verilerin korunmasına ilişkin ilkelere uygun hareket edilebilmesinin yolları, bireylerin haklarını kullanmalarının sağlanması ile veri güvenliğinin temin edilmesi hususlarına yönelik açıklamalarda bulunulmaktadır.

» Avrupa Parlamentosu Araştırma Servisi (EPRS), iş yerinde yapay zekâ kullanımının ele alındığı bir çalışma yayımladı[14]. Bahse konu çalışmada; iş yerinde yapay zekâ kullanımının ortaya çıkarabileceği riskler, algoritmik yönetim, Avrupa Birliği'nde geçerli olan yasal çerçeve ile Avrupa Parlamentosu'nun konuya ilişkin yaklaşımı gibi hususlar incelenmekte ve önümüzdeki süreçlere yönelik değerlendirmelerde bulunulmaktadır.

» Avrupa İnsan Hakları Mahkemesi, "kitlesel gözetim" konusundaki başlıca kararlara ilişkin özetlerin yer aldığı bilgi notunun güncellenmiş versiyonunu yayımladı[15].

» Yükseköğretim Kurulu, üretken yapay zekâ alanındaki riskleri ve fırsatları anlamaya, değerlendirmeye ve bu risklere karşı önlem almaya katkı sağlamak üzere yükseköğretim kurumlarını bilgilendirme amacıyla hazırlandığı belirtilen rehberini yayımladı[16]. Bu çerçevede bahse konu Rehber'de; üretken yapay zekânın bilimsel araştırma ve yayınlarda kullanılmasının etik boyutu ile üretken yapay zekâ kullanımında karşılaşılabilecek önemli birtakım riskler ve etik sorunlar ele alınmış ve üretken yapay zekâ sistemlerinin kullanımına yönelik tavsiyelerde bulunulmuştur. Diğer yandan, üretken yapay zekâ kullanımında temel etik değerler; (1) Şeffaflık, (2) Dürüstlük, (3) Özen, (4) Adalet ve Saygı, (5) Gizlilik ve Mahremiyetin Korunması, (6) Hesap Verebilirlik ve Sorumluluk Üstlenme ile (7) Etik İklime Katkıda Bulunma şeklinde sayılmıştır.

» İspanya Veri Koruma Otoritesi (AEPD) ile Avrupa Veri Koruma Denetçisi (EDPS), nörolojik verilerin işlenmesinin bireylerin temel hak ve özgürlüklerinin korunması açısından ortaya çıkarabileceği zorlukların ele alındığı bir çalışma yayımladı[17]. Bu kapsamda bahse konu çalışmada; nörolojik veriden ne anlaşılması

9 https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2024)762294, 25.04.2024.

10 https://www.oecd-ilibrary.org/science-and-technology/artificial-intelligence-data-and-competition_e7e88884-en, 24.05.2024.

11 https://www.oecd.org/newsroom/oecd-updates-ai-principles-to-stay-abreast-of-rapid-technological-developments.htm, 03.05.2024.

12 https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence, 17.05.2024.

13 https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-guidelines-generative-ai-embracing-opportunities-protecting-people_en, 03.06.2024.

14 https://www.europarl.europa.eu/thinktank/es/document/EPRS_BRI(2024)762323, 03.06.2024.

15 https://www.echr.coe.int/documents/d/echr/FS_Mass_surveillance_ENG, Haziran 2024.

16 https://www.yok.gov.tr/Sayfalar/Haberler/2024/yuksekogretim-kurumlari-bilimsel-arastirma-ve-yayin-faaliyetlerinde-uretken-yapay-zeka-kullanimina-dair-etik-rehber.aspx, 07.05.2024.

17 https://www.edps.europa.eu/system/files/2024-06/techdispatch_neurodata_en.pdf

gerektiği, bu verilerin işlenme şekilleri, bu verilerin işlenmesinin veri koruma hukuku açısından ortaya çıkarabileceği zorluklar ile bu alana ilişkin olarak önümüzdeki süreçte karşılaşılabilecek gelişmeler gibi hususlar ele alınmaktadır.

» Dünya Ekonomik Forumu, yükselmekte olan on teknolojinin incelendiği serinin bu yılki sayısını yayımladı[18]. Yapay zekâ ve bağlantılı teknolojilerdeki atılımların öne çıkarıldığı çalışmada, diğer yandan çevresel sürdürülebilirliği artıran teknolojilere de yer verilmekte ve bu çalışmada ele alınan teknolojilerin inovasyonu ve küresel iş birliğini güçlendirerek dünyayı daha iyi bir hale getirmeyi amaçladığı belirtilmektedir. Bu çerçevede raporda yer verilen teknolojiler şunlardır: -Bilimsel keşif için yapay zekâ, -Mahremiyet artırıcı teknolojiler, -Yeniden yapılandırılabilir zeki yüzeyler, -Yüksek irtifa platform istasyonları, -Entegre algılama ve iletişim inşa edilmiş dünya için sürükleyici/sarmal teknoloji, -Elastokalorikler, -Karbon yakalayan mikroorganizmalar, -Alternatif hayvan yemleri, -Nakil için genomik.

» Küresel Gizlilik Uygulama Ağı (GPEN), kullanıcıların gizlilik tercihlerini etkilemek üzere aldatıcı tasarım kullanımına ilişkin bulgularını yayımladı[19]. Uluslararası Tüketiciyi Koruma ve Uygulama Ağı'nın (ICPEN) yanı sıra dünya genelindeki 26 veri koruma otoritesi ile iş birliği içerisinde gerçekleştirilen ve bu kapsamda 1.000'den fazla internet sitesi ve mobil uygulamayı içeren küresel taramada; - Aldatıcı tasarım modellerinin, kullanıcılardan daha fazla kişisel veri toplanmasıyla sonuçlanabilecek seçeneklereyönlendiren özellikler kullandığı, -Gizlilik politikalarının %89'undan daha fazlasının uzun olduğu veya bunlarda üniversite eğitimi almış kişilere uygun karmaşık bir dil kullanıldığı, -İnternet sitelerinin ve uygulamaların %42'sinde kullanıcıların gizlilikleri ile ilgili kararlarını etkilemek için duygu yüklü bir dil kullanılırken; %57'sinde gizliliğin en az korunacağı seçeneğin en belirgin ve seçmesi en kolay seçenek olarak sunulduğu, -İnternet sitelerinin ve uygulamaların %35'inde, kullanıcıların hesaplarını silme yönündeki niyetlerini sürekli bir şekilde yeniden düşünmelerinin istendiği, -Vakaların yaklaşık %40'ında, gizlilik seçeneklerine veya gizlilik bilgilerine erişimde engeller ile karşılaşıldığı, -İnternet sitelerinin ve uygulamaların %9'unda, kullanıcıların hesaplarını silmeye çalışırken, hesaplarını açarken sağlamaları gerekenden daha fazla kişisel veri sağlamalarının zorunlu kılındığı yönünde bulgulara ulaşıldı. Bu bağlamda kuruluşları, gizliliği koruyan tasarım ve varsayılan ayarlar geliştirmeye teşvik eden GPEN; -Gizlilik seçeneklerine vurgu yapılması, -Gizlilik seçimlerinin adil ve şeffaf bir şekilde sunulmasını sağlamak üzere nötr bir dil ve tasarım kullanılması, -Gizlilik bilgilerini bulmak, oturumu kapatmak veya bir hesabı silmek için daha az tıklama yapılmasının sağlanması, -"Tam zamanında" bağlamsal olarak ilgili rıza seçeneklerinin kullanıcılara sunulması yönünde önerilerde bulundu.

HABERLER

» Birleşik Krallık Veri Koruma Otoritesi (ICO), kuruluşların gizlilik politikası oluşturabilmelerine yönelik hazırlanan şablonun, "gizlilik bildirimi oluşturucu" ile değiştirildiğini duyurdu[20]. Kuruluşların mevzuata uygun şekilde faaliyette bulunduklarından emin olmalarına yardımcı olması amacıyla tasarlandığı belirtilen bu yeni aracın; bireysel olarak faaliyette bulunan kişiler ve start-up'ların yanı sıra küçük ve orta ölçekli işletmeler ile hayır kurumları tarafından da kullanılabileceği ifade edilmektedir. Buna ek olarak 2024 yılının yazında, profesyonel hizmetler (finans, sigorta, hukuk hizmetleri vb.), eğitim ve çocuk bakımı, sağlık ve sosyal hizmetler ile gönüllü çalışmalarda kullanılmak üzere aracın farklı versiyonlarının da sunulacağı belirtilmektedir. Söz konusu araca Otorite'nin internet sitesinden ulaşılabilmektedir.

» Colorado Gizlilik Yasası kapsamında, kullanıcıların beyin aktivitelerine ilişkin verilerin korunmasını düzenleyen bir değişiklik onaylandı[21]. Bu doğrultuda Yasa'nın mevcut hâlinde yer alan "hassas veri" tanımı, "biyolojik veriler" ile beyin, omurilik ve mesajları tüm vücuda ileten sinir ağları tarafından üretilen "nöral veriler"i içerecek şekilde genişletildi.

» New York'ta, sosyal medya platformlarının "bağımlılık yapıcı" algoritmik içeriklerinin, ebeveynlerinin rızası olmaksızın 18 yaş altındaki kullanıcılara gösterilmesini yasaklayan Yasa kabul edildi[22]. Ayrıca, internet sitelerinin reşit olmayan kullanıcıların kişisel verilerini toplamasını ve satmasını kısıtlayan Yasa tasarısı da onaylandı. Bu çerçevede bahse konu düzenlemeler, gençlerin ruh sağlığını koruma ve onlar için daha güvenli bir dijital ortam yaratma çabalarında tarihi bir adım olarak nitelendirildi.

» Birleşik Krallık'ta, siber suçlara karşı dayanıklılığı güçlendirmeyi amaçlayan ürün güvenliği ve telekomünikasyon altyapısı rejiminin bir parçası olarak yürürlüğe giren yeni düzenlemeler uyarınca, akıllı cihazlarda minimum güvenlik standartlarının karşılanması gerektiği ve bu kapsamda "admin" veya "12345" gibi zayıf parolaların kullanımının yasaklandığı bildirildi[23]. Kullanıcıların bilgisayar korsanlığı ve siber saldırılardan korunmasına yönelik alınan bu önlemler kapsamında; telefon, televizyon ve akıllı kapı zili gibi ürünlerin üreticilerinin, internete bağlı bu cihazları siber suçluların erişimine karşı korumaları gerektiği ve bu çerçevede yaygın şekilde kullanılmakta olan parolaların değiştirilmesinin isteneceği ifade edildi. Bunun yanı sıra, hataların ve sorunların bildirilebilmesi için markaların iletişim bilgilerinin yayınlanması ve güvenlik güncellemelerinin zamanlaması konusunda şeffaf olunması gerektiği de belirtildi.

» Colorado'nun; işe alım, konut ve tıbbi bakım da dahil olmak üzere önemli kararların alınmasında yapay zekânın kullanımında karşılaşılabilecek ön yargıların ele alınmasını amaçlayan yasayı geçiren ilk eyalet olduğu bildirildi[24]. Henüz tasarı halinde olan ve yapay zekâ kullanımında şeffaflık ile hesap verebilirliği artırmayı amaçladığı belirtilen Yasa, şirketlerin yapay zekâdan kaynaklanan ayrımcılık riskini değerlendirmesini ve önemli kararların alınmasında yapay zekâ sistemlerinden faydalanıldığında kişilerin bilgilendirilmesini gerektiriyor. Çekince koymak suretiyle Yasa'yı imzaladığı belirtilen Eyalet Valisi tarafından konuya ilişkin yapılan açıklamada; yapay zekânın düzenlenmesine yönelik metinlerin inovasyonun önüne geçmemesinin önem taşıdığı ve bu düzenlemelere ihtiyatlı bir şekilde yaklaşılması gerektiği ifade edilerek yürürlüğe girmesinden önce söz konusu düzenlemenin iyileştirilmesi önerildi.

» Birleşik Krallık'ta milletvekillerinin, 16 yaşın altındaki çocukların akıllı telefon kullanımının tamamen yasaklanması ve çocukların

18 https://www.weforum.org/publications/top-10-emerging-technologies-2024/, 25.06.2024

19 https://www.privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns, 09.07.2024.

20 https://ico.org.uk/for-organisations/advice-for-small-organisations/create-your-own-privacy-notice/, Nisan 2024.

21 https://www.nytimes.com/2024/04/17/science/colorado-brain-data-privacy.html, 17.04.2024.

22 https://www.reuters.com/world/us/new-york-lawmakers-pass-measure-protect-youths-social-media-2024-06-08/, 08.06.2024.

23 https://www.theguardian.com/technology/2024/apr/29/devices-with-weak-passwords-to-be-banned-uk, 29.04.2024.

24 https://www.cbsnews.com/news/ai-colorado-law-algorithms-bias-antidiscrimination/, 24.05.2024.

ekran başında geçirdikleri sürenin azaltılmasının bir parçası olarak okullarda cep telefonu kullanımına yönelik hukuki bir yasak getirilmesi yönünde çağrıda bulundukları bildirildi[25]. Bu kapsamda konuya yönelik olarak Avam Kamarası Eğitim Komitesi tarafından hazırlanan raporda, çocukların ekran karşısında geçirdikleri sürenin eğitim ve refah üzerindeki etkilerinin incelendiği ve sosyal medya hesabı açabilmede yaş sınırının 16 yaşa çıkarılması yönünde bir önerinin de yer aldığı belirtilmektedir.

» Avrupa Komisyonu, Meta'nın "ödeme veya rıza" reklam modelinin Dijital Pazarlar Yasası'na uygun olmadığına dair ön bulguların Şirket'e bildirildiğini duyurdu[26]. Hatırlanacak olursa 2023 yılının kasım ayı içerisinde Meta, AB'deki Facebook ve Instagram kullanıcılarının şu iki seçenekten birini seçmek zorunda olduğu bir ikili "ödeme veya rıza" teklifini sundu: (i) Bu sosyal ağların reklamsız bir sürümüne aylık ücret karşılığında abonelik veya (ii) Bu sosyal ağların kişiselleştirilmiş reklamlar içeren versiyonlarına ücretsiz erişim. Diğer yandan, Dijital Pazarlar Yasası'nın 5(2) maddesi uyarınca; geçit bekçilerinin, belirlenmiş ana platform hizmetleri ile diğer hizmetler arasında kişisel verilerini birleştirmek için kullanıcılardan rıza istemesi gerekmektedir. Kullanıcının rıza vermeyi reddetmesi durumunda ise kullanıcının daha az kişiselleştirilmiş olmakla birlikte eş değer bir alternatif hizmete erişim sağlayabilmesi gerekmekte olup geçit bekçileri, hizmetin veya belirli işlevlerin kullanımını kullanıcıların rızasına bağlı kılamayacaktır. Konuya ilişkin olarak Komisyon tarafından yapılan açıklamada; Şirket tarafından sunulan iki seçeneğin, kişisel verilerinin birleştirilmesine rıza gösterme konusunda kullanıcıları zorladığı ve Meta'nın sosyal ağlarının daha az kişiselleştirilmiş fakat eş değer bir sürümünün sunulmadığı belirtildi. Dijital Pazarlar Yasası'nın anılan maddesinin ihlal edildiği yönündeki ön görüşün nihai olarak doğrulanması durumunda Komisyon, Meta'nın modelinin ilgili maddeye uymadığını belirten bir karar alacak ve Şirket'in dünya genelinde sahip olduğu cironun %10'una kadar para cezası uygulayabilecektir. Tekrarlanan ihlaller durumunda bu cezalar %20'ye kadar çıkabilecek ve sistematik uyumsuzluk durumunda ise birtakım ek yaptırımlar uygulanabilecektir.

» Google DeepMind araştırmacıları tarafından hazırlanan bir raporda, yapay zekâ destekli asistanların ön yargı içermeleri ve amaçlarının belirli bir kullanım durumu ile uyumsuz olması durumunda bu araçların etik sorunlara yol açabileceği ortaya konuldu[27]. Bahse konu raporda, *"işlevi, kullanıcının beklentileri doğrultusunda bir veya daha fazla alanda kullanıcı adına eylem dizileri planlamak ve yürütmek olan, doğal dil arayüzlerine sahip yapay aracılar"* şeklinde tanımlanmakta olan yapay zekâ asistanlarının daha fazla gelişmesi ve kişiselleştirilmesinin bireyler için çeşitli faydalar sağladığı belirtilmekle birlikte bu durumun, bireyleri bu araçların "uygunsuz etkilerine karşı savunmasız" hâle getirdiği ve bunun da güven, mahremiyet ve yapay zekâya insan özellikleri atfetme gibi konularda yeni sorunlar ortaya çıkardığı ifade edilen hususlar arasındadır.

» Bir sonraki yapay zekâ modelini eğitmeye başladığı belirtilen OpenAI bünyesinde, "Güvenlik ve Emniyet Komitesi" kurulduğu duyuruldu[28]. Şirket'in projeleri ile faaliyetlerinde güvenliğin sağlanmasına ilişkin olarak yönetim kuruluna tavsiyelerde bulunmaktan sorumlu olacak Komite'nin ilk görevinin, önümüzdeki 90 gün boyunca Şirket'in mevcut güvenlik uygulamalarını değerlendirmek/geliştirmek olacağı, ardından buna yönelik önerilerin yönetim kurulu ile paylaşılacağı ve devamında kabul edilen önerilere ilişkin güncellemenin kamuoyu ile paylaşılacağı belirtildi.

» Çin'de Tsinghua Üniversitesi araştırmacıları tarafından geliştirilen ve dünyanın ilk yapay zekâ hastanesi olan "Agent Hospital" tanıtıldı[29]. 2024'ün ikinci yarısında faaliyete geçmesi planlanan Hastane'nin günde 3.000 hastayı tedavi edebilecek kapasiteye sahip robot doktorlarla çalışacağı, mevcut durumda 14 doktor ve 4 hemşireden oluşan bir yapılandırmanın hazırda bulunduğu, başlıca solunum yolu hastalıklarına yönelen sanal tıp uzmanlarının hastaların teşhis ve tedavisine yönelik tüm süreci başarı ile simüle edebildiği ve hastalıkların teşhis ve tedavisinde %93.06 doğruluk oranına sahip olunduğu açıklandı.

25 https://www.theguardian.com/technology/article/2024/may/25/mps-urge-under-16s-smartphone-ban-statutory-ban-schools, 25.05.2024.

26 https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582, 01.07.2024.

27 https://www.axios.com/2024/04/19/ai-agents-assistants-ethics-alignment-google, 19.04.2024. Bahse konu raporu görüntülemek için bkz. https://storage.googleapis.com/deepmind-media/DeepMind.com/Blog/ethics-of-advanced-ai-assistants/the-ethics-of-advanced-ai-assistants-2024-i.pdf.

28 https://www.reuters.com/technology/openai-sets-up-safety-security-committee-2024-05-28/, 28.05.2024.

29 https://www.thesun.co.uk/tech/28190601/worlds-first-ai-hospital-china/, 29.05.2024.

KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASINA İLİŞKİN USUL VE ESASLAR HAKKINDA YÖNETMELİK

"Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" 10.07.2024 tarih ve 32598 sayılı Resmî Gazete'de yayımlandı. Bu çerçevede Yönetmelik kapsamında, Kanunun 9'uncu maddesi uyarınca gerçekleştirilecek yurt dışına kişisel veri aktarımına ilişkin esaslar, yeterlilik kararına dayalı aktarımlar, uygun güvencelere dayalı aktarımlar ile istisnai aktarım hâlleri düzenlendi.

STANDART SÖZLEŞMELER VE BAĞLAYICI ŞİRKET KURALLARINA İLİŞKİN DOKÜMANLAR HAKKINDA KAMUOYU DUYURUSU

Kişisel Verilerin Korunması Kanununda yapılan değişiklik kapsamında, "standart sözleşmeler" ve "bağlayıcı şirket kuralları" kişisel verilerin yurt dışına aktarımında veri sorumluları ve veri işleyenlerin başvurabileceği birer uygun güvence sağlama yöntemi olarak öngörülmüştür.

Bu çerçevede Kişisel Verileri Koruma Kurulunun 04/06/2024 tarih ve 2024/959 sayılı kararı ile kişisel verilerin yurt dışına aktarılmasında kullanılacak standart sözleşme metinleri, bağlayıcı şirket kuralları başvuru formları ve bağlayıcı şirket kurallarında bulunması gereken temel hususlara ilişkin yardımcı kılavuzlar, Kurumumuzun internet sitesinde ilan edilmiştir.

TAAHHÜTNAME BAŞVURUSU HAKKINDA DUYURU

» Bosch Termoteknik Isıtma ve Klima Sanayi ve Ticaret Anonim Şirketi tarafından 15.02.2024 tarihinde Kurumumuza sunulan yurt dışına kişisel veri aktarımı yapılması hususundaki "taahhütname" başvurusu, Kişisel Verileri Koruma Kurulu tarafından Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin 2 nci fıkrasının (b) bendi kapsamında değerlendirilmiş ve söz konusu başvuruda usul ve esasa dair herhangi bir eksikliğin bulunmadığı görülmüş olup 02.05.2024 tarihinde Kurul tarafından söz konusu veri aktarımına izin verilmiştir.

» Huawei Telekomünikasyon Dış Ticaret Limited Şirketi tarafından Kurumumuza sunulan yurt dışına kişisel veri aktarımı yapılması hususundaki "taahhütname" başvurusu, Kişisel Verileri Koruma Kurulu tarafından Kişisel Verilerin Korunması Kanununun 9 uncu maddesinin 2 nci fıkrasının (b) bendi kapsamında değerlendirilmiş ve söz konusu başvuruda usul ve esasa dair herhangi bir eksikliğin bulunmadığı görülmüş olup 28.05.2024 tarihinde Kurul tarafından söz konusu veri aktarımına izin verilmiştir.

Böylelikle, yurt dışına kişisel veri aktarımı hususunda Kurul tarafından onaylanan taahhütname sayısı 10'a ulaşmıştır.

KURULA İLETİLEN ŞİKAYET VE İHBARLARDA SIK YAPILAN HATALAR DOKÜMANI

Kişisel Verilerin Korunması Kanunu ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e uygun biçimde şikayet ve/veya ihbarların Kişisel Verileri Koruma Kuruluna iletilebilmesi ve ilgili kişilerin bilgilendirilmesi amacıyla "Kurula İletilen Şikayet ve İhbarlarda Sık Yapılan Hatalar" dokümanı yayımlandı. Söz konusu dokümanda, Kurula intikal eden şikayet ve ihbarlarda usul şartlarına ilişkin sıkça yapılan hatalara yer verildi.

KİŞİSEL VERİLERİ KORUMA DERGİSİ

Kişisel Verileri Koruma Dergisi'nin yeni sayısı yayımlandı.

Dergi'nin yeni sayısında:

- İşe Alımda Adayın Kişisel Veri Güvenliği: Yapay Zekâ Destekli Video Mülakat Uygulamaları
- ChatGPT'nin Gölgesinde Kişisel Verilerin Korunması
- Blok Zincir Teknolojisinde Kişisel Verilerin Korunması

başlıklı makaleler, ilgililerin kullanımına sunuldu.

32. AVRUPA VERİ KORUMA OTORİTELERİ KONFERANSI

Avrupa Konseyi ülkelerindeki Veri Koruma Otoritelerini her yıl Mayıs ayında bir araya getiren "Avrupa Veri Koruma Otoritelerini Konferansı" kapsamında, bu sene Letonya'nın başkenti Riga'da Letonya Veri Koruma Otoritesi ev sahipliğinde, 14-16 Mayıs tarihlerinde gerçekleştirilen Konferans'a Kurumumuzu temsilen Kurum Başkanımız Prof. Dr. Faruk BİLİR tarafından katılım sağlandı.

Bu sene ele alınan temalar arasında; Avrupa Birliği Adalet Divanı'nda ve Avrupa İnsan Hakları Mahkemesi'nde kişisel veriler konusunda verilen güncel kararlar, AB'de yeni yürürlüğe giren mevzuatın (Dijital Hizmetler Yasası, Dijital Piyasalar Yasası ve Veri Yönetişimi Yasası) veri koruma otoriteleri açısından meydana getirdiği etkiler, veri koruma otoriteleri arasında olası iş birliği konuları yer almıştır. Ayrıca Konferans'ta, üye otoriteleri arasındaki iş birliğine dair İlke Kararı da kabul edildi.

VERİ KORUMA OTORİTELERİ İSTİŞARE TOPLANTISI

Veri Koruma Otoriteleri İstişare Toplantısı, 6 Haziran 2024 tarihinde Kurumumuz ev sahipliğinde İstanbul'da düzenlendi.

Toplantıya Azerbaycan, Cezayir, Fas, Katar, Malezya ve Mali'nin Veri Koruma Otoriteleri Başkanları ve temsilcileri katıldı. İki oturum olarak düzenlenen toplantının ilk oturumunda; açılış konuşmasını müteakiben toplantıya katılan ülkelerin temsilcileri, veri koruma otoritelerinin yapısı ve ülkelerindeki kişisel verilerin korunması mevzuatı ile ilgili bilgiler verdiler.

KUZEY KIBRIS TÜRK CUMHURİYETİ KİŞİSEL VERİLERİ KORUMA KURULU İLE İŞ BİRLİĞİ

Kurumumuz ile Kuzey Kıbrıs Türk Cumhuriyeti Kişisel Verileri Koruma Kurulu arasında, ülkelerin kendi kanun ve düzenleyici işlemlerine uyulmasını ve bunların uygulanmasını sağlamak ve özellikle kendi ülkelerindeki ve bölgelerindeki mahremiyet ve kişisel verilerin korunması alanında insan hak ve özgürlüklerinin daha kapsamlı bir şekilde korunmasına katkıda bulunmak için iş birliği ve bilgi alışverişinde bulunmak için iş birliği protokolü imzalandı.

7 NİSAN KİŞİSEL VERİLERİ KORUMA GÜNÜ ETKİNLİĞİ

Kurumumuz ile Ankara Üniversitesi Hukuk Fakültesi iş birliğinde düzenlenen "7 Nisan Kişisel Verileri Koruma Günü" etkinliği, KVKK Konferans Salonunda düzenlendi. Programa çok sayıda davetlinin yanı sıra öğretmenleri ile birlikte öğrenciler de katılım sağladı. Programın açılış konuşmalarını ise Ankara Üniversitesi Rektörü Prof. Dr. Necdet ÜNÜVAR ile Kurum Başkanımız Prof. Dr. Faruk BİLİR gerçekleştirdiler.

BİLİR, 7 Nisan 2016'da Kişisel Verileri Koruma Kanunu'nun yürürlüğe girdiğini, bu tarihten itibaren 7 Nisan'ın Kişisel Verileri Koruma Günü olarak kutlanmaya başlandığını anlattı. Kişisel Verilerin Korunması Kanunu'nun veri işlemeyi yasaklayan bir düzenleme olmadığını belirten BİLİR, "Kanunun getirdiği sistem, verilerin gelişigüzel veya keyfi olarak değil, belli ilke ve kurallar çerçevesinde işlenmesidir" değerlendirmesinde bulundu. BİLİR, "Kişisel Verilerin Korunması Kanunu aslında kişiye ait olan verilerin bizatihi kişinin kendisi tarafından yönetilebileceğini ve denetlenebileceğini öngören bir kanundur" dedi.

Kişisel verilerin korunması alanında mahremiyet kavramını önemsediklerini vurgulayan BİLİR, mahremiyetin kişiye ait bir değer olduğunu söyledi. Teknolojinin gelişmesinin mahremiyetin de yükselişini getirdiğine işaret eden BİLİR, "Kişilerin teknoloji karşısında mahremiyet beklentisinin düşeceği düşünülebilir. Ancak bunun tersine, teknoloji geliştikçe kişilerin mahremiyet beklentisi de yükselmektedir. Dolayısıyla teknoloji ve mahremiyeti bir arada düşünmek gerekir" şeklinde konuştu. Yapay zeka sayesinde çok geniş bir yelpazede önemli faydalar elde edildiğini belirten BİLİR, "Teknoloji ile veri koruma dengesini sağlamak için yapay zeka ve bu tür teknolojilerle çatışmak yerine işbirliği içinde olmak gerekir" ifadesini kullandı.

Ankara Üniversitesi Rektörü Prof. Dr. Necdet ÜNÜVAR ise dijital okuryazarlığın geliştirilmesinin kişisel verilerin korunması bakımından önemli olduğunu ifade etti.

Öte yandan program kapsamında Kurumumuz tarafından düzenlenen makale, slogan, karikatür ve kısa film yarışmasında dereceye girenlere ödülleri takdim edildi.

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNUNDA YAPILAN DEĞİŞİKLİKLER PANELİ

"6698 Sayılı Kişisel Verilerin Korunması Kanununda Yapılan Değişiklikler" paneli 24 Nisan 2024 tarihinde Kurumumuz Konferans Salonunda gerçekleştirildi.

Panel kapsamında Kurumumuz personeli ve alanında uzman akademisyenler tarafından bilgi paylaşımı yapıldı. Panelin açılışını Kurum Başkanımız Prof. Dr. Faruk BİLİR yaptı. BİLİR genel olarak Kişisel Verilerin Korunması Kanunu'nda yapılan değişikliklerden bahsetti.

Bir kanunun iyi uygulanmasının her şeyden önce doğru anlaşılmasına ve doğru yorumlanmasına bağlı olduğunu dile getiren BİLİR, Kanun'da yapılan değişikliklerin amacına uygun yorumlanmasının son derece önem taşıdığını belirtti. Yapılan değişikliklerin 'sınırsız veri işleme' ya da 'yurt dışına veri aktarımının denetimsizliği' şeklinde yorumlanmaması gerektiğinin altını çizen BİLİR, "Kanun'un 6'ncı maddesinde yapılan değişiklikleri veri işlemede şartların genişletilmesi olarak; yurt dışına veri aktarımını da yeni yöntemlerin getirildiği, denetimli ve kontrollü bir aktarım rejimi olarak kabul etmek gerekir" dedi. Değişikliğin uygulamada ortaya çıkan ihtiyaçların karşılanmasını amaçladığını ifade eden BİLİR, bu çerçevede Kurum olarak gerekli çalışmaları yürüttüklerini söyledi.

KİŞİSEL VERİLERİN KORUNMASINDA İÇ DENETİMİN ROLÜ ETKİNLİĞİ

Kurumumuz ev sahipliğinde, Kamu İç Denetçileri Derneği (KİDDER) ve ICT Media tarafından düzenlenen "Kişisel Verilerin Korunmasında İç Denetimin Rolü" etkinliği 8 Mayıs Çarşamba günü Kurumumuz Konferans Salonunda gerçekleştirildi.

"Kişisel Veri Denetimi Kurum Uygulamaları" ve "Kişisel Veri Denetiminde İç Denetimin Yeri" olmak üzere iki panelden oluşan etkinliğin açılış konuşmasını Kurum Başkanımız Prof. Dr. Faruk BİLİR gerçekleştirdi.

BİLİR, nesnelerin interneti, yapay zeka ve bulut bilişim gibi teknolojiler sayesinde veri temelli hayatın insanlık tarihinde hiç olmadığı kadar etkili hale geldiğini ifade etti. Veri temelli hayatla birlikte tüm süreçlerde olduğu gibi denetim süreçlerinde de birtakım değişimlerin yaşandığını ve dijitalleşmenin etkilerinin görüldüğünü söyleyen BİLİR, "Denetim süreçleri risklerin değerlendirilmesi, risklere karşı kontrollerin belirlenmesi ve veri güvenliğinin temin edilmesi bakımından ciddiyetle ele alınmalıdır" dedi.

Kişisel Verilerin Korunması Kanunu'nun veri güvenliğine ilişkin yükümlülükleri düzenleyen 12'nci maddesinde; veri sorumlusunun, kendi kurum veya kuruluşunda, Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorunda olduğunun hükme bağlandığını hatırlatan BİLİR, bu çerçevede kişisel verileri işleyen gerçek ve tüzel kişilerin sürdürülebilir veri koruma politikaları oluşturması gerektiğini belirtti.

Öte yandan sosyal mühendislik saldırılarına da dikkat çeken BİLİR, sosyal mühendislik saldırılarının asıl hedefinin "insan" olduğunu dile getirerek, güvenlik zafiyetinin giderilmesinde çalışanların veri güvenliği konusunda yeterli farkındalığa sahip olmasının büyük önem taşıdığını ifade etti.

BİLİŞİM VE TEKNOLOJİ HUKUKU ZİRVESİ

"Anadolu Bilişim Buluşmaları" kapsamında çeşitli sektörlerden paydaşların bir araya getirilmesiyle düzenlenen "Bilişim ve Teknoloji Hukuku Zirvesi", 9 Mayıs Perşembe günü dijital konferans şeklinde gerçekleştirildi.

Zirve'nin açılış konuşmasını gerçekleştiren Kurum Başkanımız Prof. Dr. Faruk BİLİR, bilişim hukuku ve veri koruma hukuku arasındaki ilişkiden söz etti.

Dijital teknolojilerde yaşanan gelişmelerin insan yaşamını sanayi devrimi ile kıyaslanır ölçüde bir dönüşüme uğrattığını, bu gelişmelerin pek çok alanda yaşanan bir dönüşümü de beraberinde getirdiğini ifade eden BİLİR, bunun sonucunda bilişim hukukunun, hukukun yeni dallarından biri olarak gündeme geldiğini belirtti.

Bilişim hukukunun, gerek teknolojik yenilikleri yakından ilgilendirmesi, gerekse sürekli gelişen bir mevzuatının bulunması nedeniyle, son derece dikkatle takip edilmesi gereken bir alan olduğunu dile getiren BİLİR, bilişim hukukunun birçok hukuk dalıyla kesiştiğini söylemenin mümkün olduğunu ve bunlardan birinin de veri koruma hukuku olduğunu söyledi.

BİLİR, veri koruma hukukunun kişisel verilerin işlenmesi ve korunmasıyla ilgili özel düzenlemeler içerdiğini, bu hukuk alanının; kişisel verilerin toplanması, işlenmesi, saklanması ve aktarımına ilişkin kuralları belirlediğini ve bu kuralların genel olarak bireylerin verilerini korumayı ve kötüye kullanılmasını önlemeyi amaçladığını kaydetti. Bilişim hukuku ve veri koruma hukuku arasındaki ilişkinin, gün geçtikçe daha da önem kazandığını söyleyen BİLİR, "Dijital teknolojilerin kullanımı genellikle kişisel verilerin işlenmesiyle doğrudan ilişkilidir. Örneğin yapay zeka, blokzincir ve bulut bilişim gibi teknolojiler, her iki hukuk alanını da etkileyen konular arasındadır" dedi.

E-SAFE KİŞİSEL VERİLERİ KORUMA ZİRVESİ

Kurumumuz ev sahipliğinde bu yıl 7'nci kez düzenlenen e-Safe Kişisel Verileri Koruma Zirvesi, 22 Mayıs Çarşamba günü KVKK Konferans Salonunda gerçekleştirildi.

Alanında uzman birçok konuşmacının yer aldığı etkinlikte, kişisel verilerin korunması alanındaki gelişmeler hukuki, sektörel ve teknik açılardan ele alındı. Zirveyi, aralarında hukukçular ve bilişim uzmanlarının da bulunduğu sektör temsilcileri takip etti. Bu yılki teması "Türkiye'de ve Dünya'da Kişisel Verilerin Korunmasında Yeni Gelişmeler" olarak belirlenen Zirvenin açılış konuşmasını Kurum Başkanımız Prof. Dr. Faruk BİLİR gerçekleştirdi.

Konuşmasına kişisel verilerin korunmasına ilişkin hukuki düzenlemelerin önemini anlatarak başlayan BİLİR, söz konusu düzenlenmeler sayesinde kişisel verilerin hangi usul ve esaslara göre işlenebileceğinin, veri işlemede uyulması gereken kuralların ve bireylerin haklarının belirlendiğini ifade etti. Kişisel Verilerin Korunması Kanunu ile bireylerin bilgilendirilme, verilere erişim sağlama, silme ve düzeltme ile itiraz hakkı gibi haklara sahip olduğunu belirten BİLİR, bu tür haklar vasıtasıyla bireylerin verilerinin geleceğini belirleme imkanına kavuştuğunu söyledi. Kişisel Verilerin Korunması Kanunu'nda yapılan değişikliklerden bahseden BİLİR, Kanun'da yapılan değişikliklerin amacına uygun yorumlanmasının önem taşıdığını belirtti.

Kişisel verilerin korunmasının, teknolojik yenilikleri yakından ilgilendirmesi ve hukukun diğer alanlarına da temas etmesi nedeniyle dikkatle ve sürekli olarak takip edilmesi gereken bir alan olduğunu vurgulayan BİLİR, "kişisel verilerin korunmasını hem hukuki hem de teknik boyutuyla ele almak gerekir" dedi.

KVKK'DA YAPILAN DEĞİŞİKLİKLER VE YANSIMALARI KONFERANSI

Kurumumuz ve İstanbul 2 Nolu Barosu ortaklığında "KVKK'da Yapılan Değişiklikler ve Yansımaları Konferansı" 11 Haziran 2024 Salı günü İstanbul Kartal Anadolu Adalet Sarayı Konferans Salonu'nda gerçekleştirildi.

Konferans'ın açılış konuşmalarını İstanbul 2 No'lu Barosu Başkanı Yasin ŞAMLI, İstanbul 2 No'lu Barosu Bilişim Merkezi Başkanı Melik İslam ŞEKER ve Kurum Başkanımız Prof. Dr. Faruk BİLİR yaptı.

BİLİR sözlerine "Bir kanunun amacına uygun şekilde uygulanması, o kanunun doğru anlaşılmasına ve daha da önemlisi doğru anlatılmasına bağlıdır. Bu çerçevede Kişisel Verilerin Korunması Kanunu'na uyum konusunda yanlış algıların önüne geçilmesi bakımından hukukçuların sağlayacağı katkıların önemli olduğuna inanıyorum" diyerek başladı.

Kişisel verilerin korunması alanının gelişiminde, mahkemelerin ve Kurul'un kararlarıyla oluşacak içtihatlar ile hukukçuların ve akademisyenlerin görüşlerinin ciddi bir rol oynadığını belirten BİLİR, 6698 sayılı Kanun'un yorumlanmasında ve uygulanmasında ortaya çıkan soruların çözümü için yapıcı bir tutum benimsemek gerektiğini ifade etti.

Öte yandan Konferans'ta;

- Kişisel Verilerin Korunması Kanunu'nda Gerçekleştirilen Değişikliklere Genel Bakış
- Yurt Dışına Veri Aktarımda Uygun Güvenceler ve Yeterlilik Kararı
- İstisnai Aktarım Halleri
- KVKK Bakımından Sonraki Aktarım
- Kanun Değişikliğinin İş Hukuku Alanına Etkileri
- Değişen Veri İşleme Şartları ile Özel Nitelikli Kişisel Verilerin İşlenmesi

konuları ele alındı.

kvkkurumu

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

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