e-ISSN: 2757 - 5489
TOPLUM, EKONOMİ VE YÖNETİM DERGİSİ
JOURNAL OF SOCIETY, ECONOMICS AND MANAGEMENT
Cilt 5 Volume Sayı 3 Issue Ay Ekim Month Yıl 2024 Years

DİJİTAL ÇAĞDA KİŞİSEL VERİLERİN KORUNMASINDA VERİ KORUMA OTORİTELERİNİN ROLÜ

Zehra ÇUBUKCU[1]

Öz

Veri koruma otoriteleri, kişisel verilerin korunması konusunda 'bekçi' vazifesi görürler. Bununla birlikte hukuki düzenlemelerin teknolojik gelişmelerin hızına yetişemediği günümüzde, etik sorunların görülmesi ve mahremiyetin göz ardı edilmesi kaçınılmaz olmuştur. Teknolojide yaşanan hızlı gelişmeler beraberinde veri koruma otoritelerinin rol ve sorumluluklarında meydana gelen değişimleri getirmektedir. Veri koruma otoriteleri veri ihlalleri karşısında inceleme ve soruşturma yapma, danışmanlık sunma ve tavsiyede bulunma, rehberlik etme, karar verme ve yaptırım uygulamakla yükümlüdürler. Bununla birlikte gelişen teknoloji karşısında nasıl bir yol izleyebilecekleri farklı açılardan tartışılabilir. Günümüzde teknolojideki hızlı değişmeler, yeni teknolojilerin günlük hayatımızın ayrılmaz bir parçası olmasına neden olmuştur. Büyük veri, nesnelerin interneti, yapay zekâ, dijital ikiz gibi teknolojilerle birlikte son yıllarda sıkça kullanılan ChatGPT gibi üretken yapay zekâ teknolojileri ve yeni gelişmekte olan nöroteknolojiler bu teknolojilere örnek olarak verilebilir. Bu çalışma, veri koruma otoritelerinin teknolojik gelişmeler karşısındaki mevcut uygulamalarını ele almakta ve neler yapabileceklerini tartışmaktadır. Bu doğrultuda farklı ülkelerin veri koruma otoritelerinin teknolojik gelişmeler karşısındaki geliştirdiği faaliyetlere değinmekte ve Türkiye'nin kişisel verileri koruma kurumu olan KVKK bu kapsamda değerlendirilerek öneriler sunulmaktadır. Alan yazında yer alan çalışmalardan ve çeşitli ülkelerin veri koruma otoritelerinin uygulamalarından hareketle, veri koruma otoritelerinin teknolojik gelişmelere uyum sağlamasında BİT uzmanlığına sahip personel kadrosunu arttırması, teknoloji birimi oluşturması ve üniversiteler, start-up'lar, kamu kurumları ve diğer paydaşlarla iş birlikleri kurmasının önemi vurgulanmaktadır.

Anahtar Kelimeler

Kişisel Verilerin Korunması
Teknoloji
Veri Koruma Otoritesi
KVKK

Makale Hakkında

Araştırma Makalesi

Gönderim Tarihi : 16.05.2024
Kabul Tarihi : 01.08.2024
E-Yayın Tarihi : 15.10.2024
DOI : 10.58702/teyd.1485163

[1]Dr. Öğr. Üyesi., Selçuk Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, e-posta: zehra.cubukcu@selcuk.edu.tr, ORCID: 0000-0001-8578-8615.

e-ISSN: 2757 - 5489

Cilt 5 Sayı 3 Ay Ekim Yıl 2024
Volume Issue Month October Years

TOPLUM, EKONOMİ VE YÖNETİM DERGİSİ
JOURNAL OF SOCIETY, ECONOMICS AND MANAGEMENT

THE ROLE OF DATA PROTECTION AUTHORITIES IN PROTECTING PERSONAL DATA IN THE DIGITAL AGE

Abstract

Data protection authorities serve as 'guardians' for personal data protection. However, in today's world, where legal regulations struggle to keep pace with technological advancements, ethical issues and the disregard for privacy have become inevitable. Rapid technological advancements are bringing changes to the roles and responsibilities of data protection authorities. These authorities are tasked with investigating and addressing data breaches, providing advice and recommendations, offering guidance, making decisions, and enforcing sanctions. Nevertheless, how they can navigate these challenges amid evolving technologies can be debated from various perspectives. In today's world, rapid changes in technology have caused new technologies to become an integral part of our daily lives. Technologies such as big data, the Internet of Things, artificial intelligence, digital twins, and recently prevalent generative AI technologies like ChatGPT, as well as emerging neurotechnologies, serve as examples. This study examines the current practices of data protection authorities in the face of technological advancements and discusses potential actions they can take. In this context, it highlights the activities developed by data protection authorities in different countries in response to technological progress and evaluates Turkey's personal data protection authority, KVKK, offering suggestions accordingly. Based on the literature and the practices of various countries' data protection authorities, the importance of increasing personnel with IT expertise, establishing technology units, and fostering collaborations with universities, startups, public institutions, and other stakeholders is emphasized to ensure data protection authorities adapt to technological advancements.

Keywords

Personal Data Protection
Technology
Data Protection Authority
KVKK

Article Info

Research Article

Received : 16.05.2024
Accepted : 01.08.2024
Online Published : 15.10.2024
DOI : 10.58702/teyd.1485163

Kaynakça Gösterimi: Çubukcu, Z. (2024). Dijital çağda kişisel verilerin korunmasında veri koruma otoritelerinin rolü. *Toplum, Ekonomi ve Yönetim Dergisi*, 5 (3), 454-469.

Citation Information: Cubukcu, Z. (2024). The role of data protection authorities in protecting personal data in the digital age. *Journal of Society, Economics and Management*, 5 (3), 454-469.

e-ISSN: 2757 - 5489
TOPLUM, EKONOMİ VE YÖNETİM DERGİSİ
JOURNAL OF SOCIETY, ECONOMICS AND MANAGEMENT
Cilt 5 Sayı 3 Ay Ekim Yıl 2024
Volume Issue Month October Years

GİRİŞ

Günümüzde 'veri'nin değeri, 'dijital yüzyılın petrolü' söylemi ile ortaya konulmaktadır. Veri, özel sektör açısından önemli bir rekabet avantajı sağlarken; kamu yönetimi açısından hizmet kalitesinin arttırılması ve verimliliğin sağlanması gibi önemli avantajlar sağlamaktadır.

Teknolojik imkanlar doğrultusunda veri toplama, işleme hızı ve veri saklama kapasitesindeki artış, verinin önemini daha da arttırmıştır. Bununla birlikte veri toplama ve işleme kapasitesindeki ilerlemeler, mahremiyetin göz ardı edilmesi sonucunu doğurmuştur. Teknolojideki hızlı değişmelerle birlikte kişisel verilerin korunması konusu daha fazla önem kazanmıştır. Bu doğrultuda veri koruma kurumları önem arz etmektedir. Veri koruma otoriteleri, ulusal ve uluslararası düzeyde kişisel verilerin korunmasına ilişkin yasal düzenlemeleri uygulamakla görevli kurumlardır. Bununla birlikte teknolojik gelişmeler bu kurumların önemini arttırmış ve bu doğrultuda kapasitelerini arttırmalarını da zorunlu hale getirmiştir.

Veri koruma yasasının uygulanmasından sorumlu olan veri koruma otoriteleri, yeni teknolojilerle ilgili olarak mevcut yasal çerçevenin gerekliliklerini değerlendirmek ve/veya rehberlik sağlamak için kilit bir konumdadır (Wills, 2016, s. 1). Bununla birlikte teknolojinin hızlı ilerlemesi doğrultusunda veri koruma otoritelerinin kapasitelerini incelemeye ilişkin çalışmaların artırması önem arz etmektedir (Hiçkök, 2023, s. 8).

Teknolojik gelişmelerin hızla gelişmesi beraberinde hukuki düzenlemelerin de gelişmesini zorunlu kılmaktadır. Bununla birlikte yasal düzenlemeler haricinde yapay zekâ gibi teknolojilerin dinamik yapısı gereği gelişmelere uyum sağlayabilecek düzenlemelere ve mahremiyetin korunmasına yönelik gelişmelere uyum sağlayabilecek teknik, idari tedbir, yöntem ve araçlar gerekmektedir. Ortaya çıkan yönlendirme ihtiyacı ile birlikte pek çok ülkede açıklayıcı rehberler düzenlenmiştir (Burhan, 2023, s. 51).

Bu doğrultuda pek çok veri koruma otoritesi tarafından yeni teknolojilerin anlaşılmasını geliştirmek ve bu teknolojilerin uygulanması sırasında ortaya çıkabilecek gizlilik risklerinin önlenmesi için adımlar atılmıştır. Bazı otoriteler yeni teknolojilere odaklanan tavsiye rehberleri hazırlamışlardır (Fransa Veri Koruma Otoritesi, Kanada Veri Koruma Otoritesi, İspanya Veri Koruma Otoritesi, Kişisel Verileri Koruma Kurumu (KVKK), bazı otoriteler yeni teknolojilere ilişkin özel birimler oluşturmuşlardır (Fransa Veri Koruma Otoritesi). Oluşturulan rehberler, yeni teknolojileri geliştirenlerin ve servis sağlayıcıların rehber doğrultusunda hareket etmesi, tasarımdan itibaren veri koruma ilkesine uygun hareket edilmesi açısından önem arz etmektedir (Burhan, 2023, s. 51).

Yukarıda ifade edilen bilgiler doğrultusunda bu çalışmanın araştırma soruları şu şekilde ifade edilebilir. Hızla gelişen teknoloji karşısında kişisel verilerin korunması konusunda karşılaşılan riskler nelerdir? Teknolojik gelişmeler karşısında kişisel verilerin daha iyi korunması adına veri koruma otoriteleri tarafından hangi uygulamalar yapılmaktadır? Türkiye'de KVKK kapsamında hangi uygulamalar yapılmaktadır, neler yapılabilir?

Araştırma sorularına cevap bulabilmek adına öncelikle birinci başlıkta kişisel verilerin korunmasına yönelik gelişmeler ele alınmıştır. İkinci başlıkta teknolojik gelişmeler ve kişisel

verilerin korunmasına etkisi ele alınmaktadır. Üçüncü başlıkta ise teknolojik gelişmeler karşısında veri koruma otoritelerinin uygulamaları başlığı ve dördüncü başlıkta teknolojik gelişmeler karşısında KVKK uygulamaları yer almaktadır.

1. Kişisel Verilerin Korunmasına Yönelik Gelişmeler

Tarihsel süreç içerisinde kişisel verilerin insanoğlunun varoluşu ile ortaya çıktığı söylenebilir. Bununla birlikte kişisel verilerin zaman içerisinde pozitif hukuk içerisinde düzenlenmesine ihtiyaç duyulma nedenlerinden en önemlisi teknolojik gelişmelerde yaşanan hızlı değişimlerdir (Dülger, 2018, s. 75). 1970'li yıllardan itibaren bilgi ve iletişim teknolojisi alanındaki gelişmeler, kişisel verilerin toplanması ve işlenmesini artırmıştır. Bu durum karşısında hükümetler ve uluslararası kuruluşlar önlem almak durumunda kalmışlardır (Sevinç ve Karabulut, 2020, s. 453).

1980 yılında 'Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler'i kabul ederek uluslararası alanda kişisel verilerin korunması konusunda düzenleme yapan ilk kuruluş Ekonomik Kalkınma ve İş birliği Örgütü (OECD)'dir (Dülger, 2018, s. 83). Ardından 1981 yılında Avrupa Konseyi tarafından 1981'de imzaya açılan 108 sayılı *Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi* kişisel verilerin korunmasına ilişkin olarak bağlayıcılığı bulunan ilk uluslararası sözleşmedir (Kişisel Verileri Koruma Kurumu [KVKK], b.t.). Kişisel verilerin korunmasına ilişkin yapılan bir başka önemli düzenleme ise 1990 yılında BM Genel Kurulu'nda kabul edilen 'Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler' olmuştur (General Assembly, 1990).

1995 yılında kişisel verilerin işlenmesi hususunda gerçek kişilerin hak ve özgürlüklerini korumak amacı ile Avrupa Birliği (AB) tarafından 96/46/EC Sayılı 'Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi' yayınlanmıştır (Kalkınma Bakanlığı, 2017, s. 6; Dülger, 2018, s. 90). Zaman içerisinde direktifin güncellenmesi gerekmiştir.

Direktifin güncellenmesini doğuran ihtiyaçlar çeşitlilik göstermektedir. Nedenlerden bir tanesi, ekonomik faaliyetlerin eğilimi doğrultusunda veri aktarımının ve veri kullanımının hızla değişmesi, daha yüksek standartlarda korumayı gerektirmesidir (Kalkınma Bakanlığı, 2017, s. 10). Bir diğer neden ise söz konusu Veri Koruma Direktifi'nin AB'de bütüncül bir kişisel verilerin korunması uygulamasının oluşturulması amacına ulaşamadığıdır (Dülger, 2018, s. 91).

90'lı yıllardan itibaren internetin ticarileşmesi düzenlemenin yenilenme ihtiyacını önemli bir şekilde ortaya koymuştur (Kalkınma Bakanlığı, 2017, s. 10). Gelişen teknolojik gelişmeler ile veri toplama, işleme süreçlerindeki değişiklerin ortaya çıkardığı risklerin büyümesi, yeni düzenleme yapılmasını zorunluluk haline getirmiştir.

Bu gelişmelerin sonucunda, 2016 yılında Genel Veri Koruma Tüzüğü (*General Data Protection Regulation-GDPR)* kabul edilmiştir (Dülger, 2018, s. 96-97). GDPR ile önemli temel değişiklikler getirilmiştir. Tüzük ile AB üyesi ülkeler arasında üst seviye bir uyum sağlanmıştır. Bununla birlikte veri işleyenlerin tamamının veri işlemeden sorumlu tutulması, GDPR hükümlerinin küresel ölçekte etkiyi haiz olması, verisi işlenenlere tazminat talebi

imkanı sağlaması, AB Vatandaşlarına Ait Kişisel Verilerin Sınır-Ötesi Aktarımının Daha Sıkı Kurallara Bağlanması, Kullanıcı haklarının uyumlulaştırılması, unutulma hakkı, kullanıcı haklarına ilişkin veri kontrolörüne bilgilendirme yükümlülüğü verilmesi, daha sıkı yaptırımların ve uygun mekanizmaların öngörülmesi, rızanın güçlendirilmesi, verinin taşınabilirliği hakkının getirilmesi, hassas verilerin işlenmesi adına veri koruma görevliliği zorunluluğu getirilmesi, riskli veri işleme faaliyetleri açısından zorunlu veri koruma etki değerlendirilmesi getirilmesi, tasarımdan itibaren veri koruması yaklaşımı getirilmesi, yüksek veri ihlali riski durumunda veri koruma otoritesine ve veri sahibine bildirimde bulunma zorunluluğu ve veri kontrolüne kurtuluş hakkı gibi değişiklikler getirmiştir (Kalkınma Bakanlığı, 2017, s. 14-19).

Kişisel verileri korumaya ilişkin gelişmelerin Türkiye'de yansımalarına baktığımızda, Avrupa Konseyi'nin 1981 yılında imzaya açtığı *Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi* Türkiye tarafından 1981 yılında imzalanmasına rağmen, 2016 yılında çıkarılan kanun ile Türkiye açısından bağlayıcı olmuştur. Bu anlamda Türkiye'de kişisel verilerin korunmasına yönelik en önemli adımın 2010 yılında yapılan anayasa değişikliği ile birlikte kişisel verilerin korunmasının anayasal hak olarak tanınması olduğu söylenebilir. Sonrasında ise 2016 yılında 6698 sayılı Kişisel Verileri Koruma Kanunu'nun yayınlanması ve Kişisel Verileri Koruma Kurumu'nun oluşturulması ile Türkiye'de kişisel verilerin korunması konusunda yeni bir aşamaya geçilmiştir (Resmî Gazete, 2016).

2. Teknolojik Gelişmelerin Kişisel Verilerin Korunması Konusunda Oluşturduğu Riskler

Günümüzde saniyeler içerisinde büyük veriler bilgisayar ortamına kaydedilebilmekte ve başka bilgisayarlara aktarılabilmektedir. Teknolojik gelişmelerle veri aktarım hızında yaşanan artış kişisel verilerle ilgili tehlikelerin de riskini artırmıştır (Dülger, 2018, s. 75). Büyük verilerin toplanması ve işlenmesine yönelik artan ilgi, verilerin korunması noktasında yeni zorluklar ortaya çıkarmıştır (McDermott, 2017, s. 4).

Büyük veri, nesnelerin interneti, dron teknolojileri, mahremiyet ve veri koruma açısından etkileri olan teknolojilerdir (Wills, 2016, s. 2). Günümüzde söz konusu teknolojiler pek çok alanda kullanılmaktadır. Yapay zekâ teknolojileri sağlık, ticaret, ulaşım gibi pek çok alanda karşımıza çıkarken; nesnelerin interneti, sağlık, akıllı ev, akıllı şehirler, ulaşım gibi pek çok alanda karşımıza çıkmaktadır. Teknolojilerin her alanda hayatımıza dahil oluşu kişisel verilerin korunmasını zorlaştırmaktadır.

Teknolojik araçlar insanlar tarafından kasti ve kötü amaçlı olarak veri sızdırmak amacı ile kullanılabilir. Veya teknik bir hata sonucu güvenli olmayan uygulamalar çalıştırabilir. Bu durum verileri riske atmaktadır. Bu nedenle verilerin korunması adına belirli kurallar/düzenlemeler bulunmalı ve kullanıcılar doğru şekilde yönlendirilmelidir (Gündüz ve Daş, 2018, s. 332).

Günümüz dünyasında, mevcut ekonomik koşullar doğrultusunda tüketim alışkanlıklarının belirlenmesinde teknoloji önemli ölçüde kullanılmaktadır. Sensörler, işaretçiler, kameralar, akıllı gözlükler gibi teknolojiler her yerde bulunduğunda ve topladıkları veriler ağa bağlı bir sisteme aktarıldığında, kişilerin hayat tarzı öğrenilebilmekte

ve davranış kalıpları ve tüketim alışkanlıkları kamusal bilgi haline gelebilmektedir (Greengard, 2021, aktaran Ertan, 2022, s. 56).

Teknolojideki hızlı değişimlerle birlikte kısa aralıklarla yeni gelişmelerle karşı karşıya kalınmaktadır. Son zamanlarda kullanılmaya başlanan üretken yapay zekâ (GenAI) bu gelişmelerden bir tanesidir. Genel olarak üretken yapay zekâ, teknolojik, toplumsal, yasal veya etik açıdan fırsatlar ve zorluklar sunar (Ooi ve ark., 2023, s. 4). Üretken yapay zekâ (GenAI), görüntüler, videolar, ses ve metin içeriği gibi çeşitli verilerden elde ettiği kalıpları kullanarak ve derin öğrenme tekniklerinden faydalanarak çeşitli içerikler üretir (Jovanovic ve Campbell, 2022, s. 107).

Üretken yapay zekâ modelleri (*Generative AI-GAI*), mevcut veri setlerinin gelişmiş istatistik yöntemlerle analiz edilmesi yolu ile içerik sağlamaktadır. Söz konusu modellerin geliştirilmesi için yüksek hacimli veri işlemesi kullanılması gerekmektedir. Kullanıcılar tarafından girilen yeni veriler işlenmektedir. Bu durum ise mahremiyet açısından bazı sorunların ortaya çıkmasına neden olmaktadır (Güçlütürk, 2023, s. 9).

Son zamanların popüler uygulaması olan 'ChatGPT', üretken yapay zekâ modeline bir örnektir. OpenAI'nin popüler sohbet robotu olan ChatGPT, piyasaya sürüldükten iki ay sonra aylık 100 milyon aktif kullanıcıya ulaşmış ve bu sayı ile en hızlı büyüyen tüketici uygulaması olarak anılmıştır (Hu, 2023). ChatGPT gibi teknoloji modelleri, insanlar için önemli olumlu ve olumsuz etkileri beraberinde getirmektedir. Politika yapıcılar, üretici yapay zekâ kullanımı için etik kılavuzlar ve en iyi uygulama geliştirme seçeneği ile güvenilir üretici yapay zekâ uygulamalarına uyumlu bir geçiş sağlayabilirler (Leboukh ve ark., 2023, s. 5).

Yine son yıllarda ortaya çıkan yeni teknolojik gelişmelerden bir tanesi nöroteknolojidir. Nöroteknolojiler, son on yılda sağlık ve araştırma sektöründe hızlı bir şekilde kullanılmaya başlamıştır. Nöroteknoloji, kişiselleşmiş hizmet sunumu noktasında önemli bir potansiyel barındırmaktadır. Bu bağlamda yakında günlük hayatın bir parçası olma potansiyeli taşımaktadır (Information Commissioner's Office [ICO], b.t.). Nöroteknoloji, farklı sektörlerde önemli avantajlar sağlamakla birlikte, karmaşık yapısıyla ve yanlış bilgi sunma potansiyeli nedeni ile kişisel verilerin korunması noktasında bazı riskler barındırmaktadır (ICO, b.t.).

Mevcut düzenleyici çerçevelerdeki boşluklar, aslında, nöro verilerin sınırsız bir şekilde ticaretine izin vermektedir (Yuste, 2023, s. 2869). Nöroteknoloji aracılığı ile artan veri ihlallerine yönelik olarak düzenleyici kurumlar ek tedbirler almalıdırlar. Yuste'ye göre (2023, s. 2873), tüm tedbirlerle birlikte ayrıca nöroteknoloji uygulayıcıları için tıpta yer alan Hipokrat yeminin temsiline benzer bir deontoloji aşılanabilir. Kişisel verilerin korunmasının tarihçesine bakıldığında ilk olarak tıp etiği ile ilgili ilkeler içerisinde hasta gizliliği ve mahremiyetini de kapsayan Hipokrat yemini ile başlatan kaynaklar olduğu görülmektedir (Dülger, 2018, s. 75).

Veri koruma otoriteleri, temel bir hak olarak sahip olduğumuz mahremiyetin korunmasında önemli bir rol oynamaktadır. Bu otoritelerin kurumsal düzenlemeleri, bağımsızlıkları ve performansları bu haktan yararlanmamız için çok önemlidir. Ancak veri koruma otoriteleri yeterince incelenmemektedir (Raab ve Szekely, 2017, s. 421). Bu çalışma, teknolojik gelişmeler doğrultusunda kişisel verilerin korunması hususunu veri koruma otoritelerinin rolü açısından inceleyerek alana katkı sunmaya çalışmaktadır.

e-ISSN: 2757 - 5489
TOPLUM, EKONOMİ VE YÖNETİM DERGİSİ
JOURNAL OF SOCIETY, ECONOMICS AND MANAGEMENT
Cilt 5 Volume Sayı 3 Issue Ay Ekim Month Yıl 2024 Years

3. Teknolojik Gelişmeler Karşısında Veri Koruma Otoritelerinin Uygulamaları

1970'li yıllardan itibaren kişisel verilerin korunmasına ilişkin yasal düzenlemeler yapılmaya başlanmıştır. Veri koruma yasaları, bu yasaların uygulanmasından sorumlu olacak olan otoritelerin kurulmasını da zorunlu kılmıştır. Dünyadaki mevcut veri koruma otoriteleri farklı özellikler göstermektedir. AB'ye üye ülkelerin çoğunluğunda tek bir ulusal ver koruma kurumu bulunmaktadır. Bununla birlikte üniter ve federal devletler arasında farklı yapılanmalar mevcuttur (Civelek, 2011, s. 93). Ayrıca veri koruma otoriteleri yetkinin ait olduğu kişi ve kurum açısından da farklılaşmaktadır (Komiser, komisyon, ajans modeli) (Civelek, 2011, s. 93-95).

Komisyon (kurul) modeli şeklinde örgütlenmiş olan Fransa veri koruma otoritesi CNIL, 1978 yılında kurulan 40 yıllık bir kurumdur. CNIL'in diğer otoritelerden farklılaşan noktası teknolojik gelişmelerin kişisel verilerin korunması konusunda öngörülerde bulunma ve önlem alma amacı ile yürüttükleri faaliyetler açısından dikkat çekici bir kurum olması açısından önemli olmasıdır (Tansuğ, 2018, s. 335).

Son yıllarda teknolojideki hızlı gelişmeler, kişisel verilerin korunması açısından belirli riskler oluşturmaktadır. Bu kapsamda dünyadaki veri koruma otoriteleri yeni teknolojik gelişmelerin yasalar çerçevesinde hareket etmesini kontrol altında tutmaktadırlar. Literatürde veri koruma otoritelerini yeni teknolojiler kapsamında ele alan çalışmalardan bazıları şunlardır: Raab ve Szekely (2017), Wills (2016), Sarlet ve Rodriguez (2023).

Raab ve Szekely (2017, s. 425), veri koruma otoritelerinin yeni teknolojileri kavramada yaşadıkları sorunları ve bunlarla nasıl başa çıktıklarını araştıran otoriteler arasında yapılan bir anketin sonuçlarını rapor etmektedir. Sonuçlar arasında veri koruma otoritelerindeki BİT uzmanı personel eksikliği nedenlerine de yer verilmektedir. Bu nedenler arasında en çok belirtilen bütçe kısıtlamaları nedeni olurken; diğer nedenler nitelikli personel bulmadaki zorluklar; BİT ile ilgili konularda sınırlı eğitim süresi ve veri koruma otoritelerinin BİT uzmanlarını işe almak yerine hukuk personelini işe almayı tercih etmesi; kamu sektöründeki BİT uzmanlarının maaşlarının özel sektöre göre önemli ölçüde düşük olması ve veri koruma otoritelerindeki bu tür pozisyonları daha az cazip hale getirmesi; ve son olarak, eğitimli BT personeline olan ihtiyacın mevcut arzdan çok daha fazla olması yer almaktadır.

Wills (2016, s. 1-9) çalışmasında, Avrupa Birliği veri koruma otoritelerinin teknoloji öngörü faaliyetlerini, bu faaliyetlerin kurumlar için önemini, karşılaşılan zorlukları ve iş birlikleri ele almaktadır. Wills'in bu çalışması, 2015 yılında gerçekleştirilen Pheadra II projesi kapsamında yürütülen araştırmaya dayanmaktadır. Bu proje kapsamında, veri koruma otoriteleri yetkilileri ile yapılan görüşmelerde yetkililerin potansiyel gizlilik ve veri koruma sorunlarına ilişkin gelişmekte olan teknolojilerin analizini yapılıp yapılmadığı sorulmuştur. Analiz sonucunda, bu otoritelerin bu tür faaliyetleri sistematik olarak yürütecek personele ve kaynağa sahip olmadığı belirlenmiştir (Wills, 2016, s. 3-4). Bu durum her ülkenin otoritesinin kapasite farklılıkları nedeni ile farklı sonuçlar gösterebileceğini göstermektedir. Bununla birlikte çalışmada veri koruma otoriteleri arasında teknoloji öngörü faaliyetlerini entegre etmenin önemi vurgulanmıştır.

Sarlet ve Rodriguez (2023) çalışmalarında Brezilya veri koruma otoritesinin (ANPD) yapılandırılmasına yönelik çıkarımlarda bulunmuşlardır. Sarlet ve Rodriguez (2023, s. 208),

ANPD'nin kurum içi bilgi kapasitesini geliştirmesi önemli olduğu için kurum bünyesinde BİT eğitimi almış kamu görevlilerinin bulunduğu ancak kurumun aynı zamanda kurumsal iş birliği araçlarından vazgeçmediğini belirtmektedir.

Üretken yapay zekâ uygulamalarının hızla büyümesi ve oldukça fazla kullanıcı kitlesine ulaşması, veri koruma otoritelerinin bu konudaki çalışmalarını arttırmıştır. Bu konuda çalışma yapan veri otoritelerinden birisi Fransa Veri Koruma Otoritesi olan CNIL (*Commission Nationale de I'Informatique et des Libertés*) dir. CNIL, kişisel veri düzenlemesini destekleyen yapay zekâ kullanıma ilişkin ilk kılavuz ilkelerini yayınlamıştır (Commission Nationale de I'Informatique et des Libertés [CNIL], 2023a).

Ayrıca Fransa veri koruma otoritesi CNIL'in organizasyon yapısı içerisinde şikâyet direktörlüğü ve diğer direktörlüklerle birlikte Teknoloji ve İnovasyon Direktörlüğü bulunmaktadır. Son olarak Teknoloji ve İnovasyon Direktörlüğünün altında Yapay Zekâ Departmanı (AID) oluşturulmuştur. Yapay zekâ departmanı, yapay zekâ sistemlerinin anlaşılmasını geliştirmek, bu sistemlerin uygulanması sırasında karşılaşma ihtimali olan gizlilik risklerinin belirlenmesi ve önlenmesi için CNIL'in uzmanlığını geliştirmek, üniversiteler, start-up'lar ve diğer paydaşlarla ilişkiler geliştirmekle görevlidir (CNIL, 2023b).

İtalya Veri Koruma Otoritesi (*Garente per la protezione dei dati personali [GDDP]),* ChatGPT kullanımı sırasında kişisel verilerin hukuka aykırı olarak toplandığı ve çocuklar için herhangi bir yaş doğrulama sistemi kullanılmadığı gerekçesi ile ChatGPT'ye durdurma kararı vermiştir (Garante Per La Protezione Dei Dati Personali [GDDP], 2023). Durdurma gerekçesi olarak platformun dayandığı algoritmaları 'eğitmek' için kişisel verilerin büyük ölçüde toplanmasını ve işlenmesini destekleyen yasal bir dayanak olmaması ve ChatGPT tarafından sunulan bilgilerin her zaman gerçek durumlarla eşlenmemesi ve dolayısıyla yanlış kişisel veriler işlenmesini belirtilmektedir. Bununla birlikte kararda, OpenAI'nin hizmet şartlarına göre hizmetin 13 yaş üstü kullanıcılara yönelik olduğu iddia edilse de herhangi bir yaş doğrulama mekanizmasının olmamasının çocukları yaşlarına ve farkındalıklarına kesinlikle uygun olmayan yanıtlar almaya maruz bıraktığını vurgulamaktadır (GDDP, 2023).

Kanada Veri Koruma Otoritesi (*Office of the Privacy Commissioner of Canada*), üretken yapay zekâ teknolojilerinin güvenilir ve gizliliğe saygılı bir şekilde kullanımını sağlamak için ilkeler belirlemiştir (Office of the Privacy Commissioner of Canada [OIPC], 2023). Bu kapsamda öncelikle, kişisel bilgilerin toplanması ve kullanılması için yasal yetki sağlanması belirtilmiştir. Kişisel bilgilerin toplanması, kullanılması veya ifşa edilmesi için yasal yetkinin rıza istendiği durumlarda, rızanın geçerli ve anlamlı olduğundan emin olunması gerektiğini belirtmektedir. Rıza mümkün olduğunca spesifik olmalı ve aldatıcı tasarım modellerinden kaçınılmalıdır. Üretken bir YZ sistemi ile ilişkili kişisel bilgilerin toplanması, kullanılması veya ifşa edilmesinin uygun amaçlar için olduğundan emin olunması gerektiği belirtilmektedir. Üretken yapay zekanın potansiyel istenmeyen uygunsuz kullanımlarının tespit edilmesi için teknik önlemler alınmasını belirtmektedir.

Birleşik Krallık'ın veri koruma otoritesi olan ICO (*Information Commissioner's Office)*, nöroteknoloji ve nöro verilerin mahremiyet üzerindeki etkisine ilişkin inceleme yapmışlardır (ICO, b.t.). ICO, bu kapsamda akademi, sivil toplum, özel sektörden kilit paydaşlarla iş birliği halinde olacaklarını, bununla birlikte nöroteknoloji ve mahremiyet açısından bilgi düzeyleri

ve endişelerini anlamak adına halkla etkileşim halinde olacaklarını belirtmişlerdir. Bu doğrultuda uzun vadeli bir süreçte nöroteknolojiye ilişkin özel rehberlik sağlayacaklarını belirtmişlerdir (ICO, b.t.).

4. Teknolojik Gelişmeler Karşısında Kişisel Verileri Koruma Kurumu

Kanunda verilen görevleri uygulamakla yükümlü olan KVKK, idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz bir kurumdur. Kurum, Kurul ve Başkanlıktan oluşmaktadır ve Kurumun karar organı Kuruldur (6698/19). Kurum; düzenleme, denetleme, ihlal bildirimlerinin çözülmesi, yaptırım uygulanması yetkilerine sahiptir. Yükümlülüklerini yerine getirmeyenlere idari para cezası verme yetkisine sahiptir.

2022 yılında Kişisel Verileri Koruma Kurumu'na toplam 9.059 ihbar ve şikâyet gelmiştir. Şikayetlerin büyük bir çoğunluğunun e-posta veya kurumun e-şikâyet modülü yerine Cumhurbaşkanlığı İletişim Merkezi (CİMER) (%72) aracılığıyla geldiği belirtilmektedir (KVKK, 2022a, s. 34). KVKK raporuna göre, şikayetlerin konu dağılımına bakıldığında büyük bir çoğunluğun (%45,68), kişisel verilerin veri sorumlusu tarafından hukuka aykırı olarak işlenmesi nedeni ile olduğu görülmektedir (KVKK, 2022a, s. 35).

6698 sayılı Kanun'un 20. Maddesinde sayılan KVKK görevleri arasında, görev alanı itibarıyla, uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak; ihtiyaç duyulması hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak, kişisel verilerle ilgili uluslararası gelişmeleri izlemek ve değerlendirmek ve uluslararası kuruluşlarla iş birliği yapmak sayılmıştır.

Bu kapsamda KVKK kişisel verilerin korunmasına yönelik olarak toplumsal farkındalık kazandırmak ve bu kapsamda iş birlikleri oluşturmakla da sorumludur. Bu doğrultuda bakanlıklara bağlı, ilgili ve ilişkili kuruluşların temsilcilerine kişisel verilerin korunması konusunda eğitimler vermekte ve halka açık şekilde seminerler düzenlemektedir. Bununla birlikte yurtiçi ve yurtdışı paydaş kurum ve kuruluşların katılımı ile çalıştay, konferans, panel, toplantılar düzenlemektedir.

Yine bu kapsamda KVKK kişisel verilerin korunmasına ilişkin 6698 sayılı Kanun'un uygulanmasına yön vermek, toplumsal farkındalık oluşturmak, düzenleyici ve denetleyici işlem yapmak, veri sorumlularının şeffaf ve hesap verebilir olarak kişisel verisini işlemek amacıyla uygulamaya yön vermek, Kanun'un uygulanmasını ve farkındalık düzeyini arttırmak için kitap, rehber ve broşür gibi bilgilendirici dökümanlar hazırlamak ve internet sayfasında paylaşmaktadır (KVKK, 2022a, s. 85).

KVKK, diğer veri koruma otoriteleri gibi yeni teknolojiler karşısında kişisel verilerin korunmasına yönelik olarak tavsiyelerde bulunmaktadır. Kurum 'Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler' ile yapay zekâ alanında geliştiriciler, üreticiler, servis sağlayıcılar ve karar alıcıları kapsayan kişisel verilerin korunmasına dair tavsiyelere yer vermektedirler.

KVKK bünyesinde çalışan personelin unvana göre dağılımına ilişkin bilgiler kurum faaliyet raporunda (KVKK, 2022a, s. 22) yer almakla birlikte uzman ve uzman yardımcısı personelin alan bilgisi dağılımına yer verilmemiştir. Bununla birlikte Kişisel verileri koruma

uzmanlığı yönetmeliğinde (Resmi Gazete, 2018) kurumun kadro ve ihtiyaç durumuna göre "sosyal bilimler alanında siyasal bilgiler, iktisadi ve idari bilimler, iktisat, hukuk ve işletme fakültelerinden ya da sayılan fakültelerde yer alan denkliği Yükseköğretim Kurulunca kabul edilmiş yurt dışındaki yüksek öğretim kurumlarından" mezun olma ve "mühendislik alanında elektronik, elektrik-elektronik, elektronik ve haberleşme, endüstri, bilgisayar, bilişim sistemleri mühendisliği bölümleri ve fakültelerin istatistik bölümlerinden ya da sayılan bölümlerin denkliği Yükseköğretim Kurulunca kabul edilmiş yurt dışındaki yükseköğretim kurumlarından" mezun olma şartı bulunmaktadır.

Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği'ne göre KVKK'nın yedi birimi bulunmaktadır. Bunlar; Veri Yönetimi Dairesi Başkanlığı, İnceleme Dairesi Başkanlığı, Hukuk İşleri Dairesi Başkanlığı, Veri Güvenliği ve Bilgi Sistemleri Dairesi Başkanlığı, Rehberlik, Araştırma ve Kurumsal İletişim Dairesi Başkanlığı, İnsan Kaynakları ve Destek Hizmetleri Dairesi Başkanlığı, Strateji Geliştirme Dairesi Başkanlığı'dır.

KVKK içerisinde Fransa veri koruma otoritesi CNIL'in organizasyon yapısı içerisinde yer alan Teknoloji ve İnovasyon Direktörlüğü benzeri bir direktörlük ve alt departmanı olan bir Yapay Zekâ Departmanı oluşturulabilir. Böylece yapay zekâ sistemlerinin uygulanması sırasında karşılaşılabilecek gizlilik risklerinin belirlenerek önüne geçilmesi adına KVKK'nın uzmanlığı geliştirilebilir. Bununla birlikte yeni teknolojik gelişmeler karşısında gizlilik risklerinin önlenmesinde üniversiteler, start-up'lar, diğer paydaşlar arasında iş birlikleri geliştirmelidir.

CNIL internet sitesinde görevlerini dört başlık altında toplamıştır. Bunlar; bilgilendirme ve koruma, genel düzenleyici işlem yapma, görüş ve yardım verme ve teknolojik gelişmelerin kişisel veriler üzerindeki etkilerini araştırmak ve geleceğe yönelik önlem almak şeklindedir (CNIL, 2023c; Tansuğ, 2018, s. 346-347).

CNIL'in teknolojik öngörü kapsamındaki görevleri arasında özel hayat üzerinde önemli etkileri olabilecek teknolojileri ve kullanım alanlarını analiz etmeye çalışmaktadır ve bu amaçla oluşturulan laboratuvara sahiptir. Bununla birlikte *privacy by design* (tasarımdan itibaren mahremiyet) anlayışı ile mahremiyetin korunmasının ürünlerin tasarımından itibaren başlatılabileceğini savunmakta ve kişisel verilerin korunması aşamalarını teknolojik şirketlere entegre etmek için şirketlere danışmanlık rolünü üstlenmektedir (Tansuğ, 2018, s. 347).

SONUÇ

Kişisel veri "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" (6698/3d), "kişiyi tanımlayacak her türlü bilgi" (Bilir, 2021, s. 173) şeklinde tanımlanmaktadır. Kişisel verilerin işlenmesi ise "Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi" (6698/3e) olarak tanımlanmaktadır. Günümüzde hızla gelişen teknolojik gelişmeler, kişisel verilerin işlenmesini kolaylaştırmaktadır.

Bu çalışmada hızlı teknoloji koşullarında kişisel verilerin korunmasında veri koruma otoritelerinin rolü ve önemi ele alınmaya çalışılmıştır. Hızlı gelişen teknoloji ile kişisel verilerin korunmasında karşılaşılan riskler artmıştır. Alan yazında yer alan çalışmalarda veri koruma otoritelerinin teknoloji öngörülerini arttırmak ve gelişen teknolojiler karşısında veri korumayı sağlamak adına atılan adımlardan bahsedilmiş ve öneriler sunulmuştur. Raab & Szekely (2017) bütçe kısıtlamaları, hukuk personelinin işe alınmasının tercih edilmesi, BİT uzmanları için ilgili kadro maaşlarının cazip gelmemesi gibi nedenlerle BİT uzmanı personel eksikliği yaşanmasının veri koruma otoritelerinin yeni teknolojilere hazırlık sürecinde zorluk yaşamalarına neden olduğunu belirtmişlerdir. Wills'te (2016) Pheadra II projesi kapsamında yürüttüğü çalışmasında veri koruma otoritelerinin teknoloji öngörü faaliyetlerini yürütecek personele ve kaynağa sahip olmadığını belirtmiştir. Aynı zamanda veri koruma otoriteleri arasında teknoloji öngörü faaliyetlerine ilişkin iş birlikleri oluşturmanın önemini vurgulamıştır. Sarlet & Rodriguez (2023) çalışmalarında kurum bünyesinde BİT eğitimi almış kamu görevlilerinin istihdam edilmesinin kritik önemini belirtmişlerdir. Ayrıca kurumsal iş birliği süreçlerinin de önemine vurgu yapmışlardır.

Türkiye'de 2016 yılında 6698 sayılı Kişisel Verileri Koruma Kanunu'nun yayınlanması sonucu Kişisel Verileri Koruma Kurumu'nun oluşturulması ile kişisel verilerin korunması konusunda yeni bir aşamaya geçilmiştir. Kurum, kişisel verilerin işlenmesi ve korunması ile ilgili işlemlerin kanuna uygunluğunu denetlemek, ihlal tespiti durumunda yaptırım uygulamak yetkilerine sahiptir. Kurum, teknolojik gelişmeler karşısında kişisel verilerin korunması konusunda rehberler ve kılavuzlar hazırlayarak yol gösterici bir rol üstlenmektedir. Kurum 2022 yılında 44. Küresel Mahremiyet Konferansını gerçekleştirilmiştir. Konferans ana teması, kişisel veri işleme esaslı teknolojiler ile mahremiyet arasındaki dengenin kurulabilmesine yönelik olarak "Bir Denge Meselesi: Hızlı Teknolojik Gelişme Çağında Mahremiyet" şeklinde belirtilmiştir. Konferansta yapay zekâ, blok zincir, büyük veri, meta verse vb. teknolojilerdeki güncel gelişmeler mahremiyet açısından ele alınmıştır (KVKK, 2022b). Bununla birlikte kurumun yayınlamış olduğu 'Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler' belgesi ilgili alanda yer alan geliştiriciler, üreticiler, servis sağlayıcılar ve karar alıcılar açısından yol gösterici niteliktedir.

Veri koruma otoriteleri, veri koruma kanunlarının uygulanmasından sorumlu kurumlardır. Bununla birlikte yeni teknolojilerle ilgili durumlarda rehberlik ve danışmanlık işlevi görebilmekte ve böylece oluşabilecek veri ihlallerinin önceden önlenmesini sağlayabilmektedirler. Literatürden hareketle veri koruma otoritelerinin yeni teknolojiler karşısında kişisel verilerin korunması noktasında kapasitesini arttırabilecek BİT uzmanlığına sahip personel sayısını arttırmasının önem arz ettiği görülmektedir. Bu doğrultuda veri koruma otoriteleri BİT uzmanlığına sahip personel kadrosunu arttırabilir.

Türkiye açısından değerlendirildiğinde ise KVKK bünyesinde CNIL'de Teknoloji ve İnovasyon Direktörlüğü altında oluşturulan Yapay Zekâ Departmanı (AID) benzeri bir birim oluşturulabilir. KVKK bünyesinde BİT uzmanlığına sahip personel kadrosu arttırılabilir. Ayrıca yeni teknolojilerin oluşturabileceği gizlilik risklerinin erkenden önüne geçilebilmesi adına üniversiteler, start-up'lar, kamu kurumları ve diğer paydaşlarla iş birlikleri geliştirilebilir.

Bununla birlikte 1 Ağustos'tan itibaren yürürlüğe giren Avrupa Yapay Zekâ Yasası'nın uygulanması veri koruma otoritelerinin rolünde değişikliklere neden olabilecektir. Sonraki çalışmalarda, teknolojik gelişmeler karşısında veri koruma otoritelerinin rolüne ilişkin farklı ülke uygulamalarını ele alan karşılaştırmalı araştırmalara ve veri koruma otoritelerinde yapılacak alan araştırmaları ile derinlemesine inceleme imkânı sunan araştırmalara alan yazında yer verilmesi önem arz etmektedir.

Araştırma ve Yayın Etiği Beyanı

Bu çalışmada içerisinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, çalışmanın özgün olduğunu bildiririm. Aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Yazarların Makaleye Katkı Oranları

Bu çalışma tek yazar tarafından oluşturulmuştur. Makalenin tüm kısımlarında yazarın kararı ve yazımı vardır.

Etik Kurul İzni

Bu makalede etik kurul iznine gerek yoktur. Etik kurul kararı gerekmediğine ilişkin ıslak imzalı onam formu sistem üzerindeki makale süreci dosyalarında yer almaktadır.

Çıkar Beyanı

Bu çalışmada çıkar çatışması durumu yaşanmamıştır.

KAYNAKÇA

Bilir, F. (2021). Kişisel verilerin korunması kişinin kendisinin korunmasıdır. *TRT Akademi*, *6*(11), 173-179.

Burhan, B. T. (2023). Üretici yapay zekâ çağında mahremiyeti yeniden düşünmek. *KVKK Bülten*, (1), 48-57.

Civelek, D. Y. (2011). *Kişisel verilerin korunması ve bir kurumsal yapılanma önerisi* [Uzmanlık Tezi]. T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi Başkanlığı.

CNIL. (2023a, 16 Ekim). Artificial intelligence: CNIL unveils its first answers for innovative and privacy-friendly aI. https://www.cnil.fr/en/artificial-intelligence-cnil-unveils-its-first-answers-innovative-and-privacy-friendly-ai_adresinden 3 Ocak 2024 tarihinde alınmıştır.

CNIL. (2023b, 26 Ocak). The CNIL creates an artificial intelligence department and begins to work on learning databases. https://www.cnil.fr/en/cnil-creates-artificial-intelligence-department-and-begins-work-learning-databases_adresinden 2 Ocak 2024 tarihinde alınmıştır.

CNIL. (2023c, 05 Nisan). Status and composition. https://www.cnil.fr/en/cnil/status-composition adresinden 2 Ocak 2024 tarihinde alınmıştır.

Dülger, M. V. (2018). İnsan hakları ve temel hak ve özgürlükler bağlamında kişisel verilerin korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 5*(1), 71-144.

Ertan, A. (2022). Nesnelerin internetinin kişisel verilerin korunması kapsamında incelenmesi. *Kişisel Verileri Koruma Dergisi*, *4*(2), 48-68.

GDDP. (2023). Artificial Intelligence: Stop to ChatGPT by the Italian SA Personal data is collected unlawfully, no age verification system is in place for children. https://www.garanteprivacy.it/web/garante-privacy-en/main-decisions adresinden 7 Ocak 2024 tarihinde alınmıştır.

General Assembly. (1990). Guidelines for the regulation of computerized personal data files. https://digitallibrary.un.org/record/82456?ln=fr&v=pdf adresinden 10 Ocak 2024 tarihinde alınmıştır.

Güçlütürk, O. G. (2023). Üretken yapay zekâ riskler ve mahremiyet üzerine bir değerlendirme. *KVKK Bülten,* (1), 9-11.

Gündüz, M. Z. ve Daş, R. (2018). Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, *24*(2), 327-335.

Hiçkök, M. (2023). Üretici yapay zekâ neden mahremiyet, ön yargı ve siber güvenlik açısından bir kâbus oluşturuyor? *KVKK Bülten*, (1), 6-8.

Hu, K. (2023). ChatGPT record for fastest growing user base analyst note. https://www.cnil.fr/en/artificial-intelligence-cnil-unveils-its-first-answers-innovative-and-privacy-friendly-ai adresinden 20 Ocak 2024 tarihinde alınmıştır.

ICO. (b.t.). ICO tech futures: Neurotechnology. https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures-neurotechnology/ adresinden 10 Ocak 2024 tarihinde alınmıştır.

Jovanovic, M. ve Campbell, Ö. (2022). Generative artificial intelligence: Trends and prospects. *Computer*, *55*(10), 107-112.

Kalkınma Bakanlığı (2017). Avrupa birliği genel veri koruma tüzüğünün getirdiği yenilikler ve Türk hukuku bakımından değerlendirilmesi (Yayın no. 2968). http://www.bilgitoplumu.gov.tr/wpcontent/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf

KVKK. (2022a). KVKK 2022 yılı faaliyet raporu. www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aae3c721-9da4-43c7-95a6-8d14e6413a36.pdf adresinden 27 Ocak 2024 tarihinde alınmıştır.

KVKK. (2022b). 44. küresel mahremiyet konferansı ülkemiz ev sahipliğinde gerçekleştirilecek. https://www.kvkk.gov.tr/Icerik/7478/44-Kuresel-Mahremiyet-Konferansi-Ulkemiz-Ev-Sahipliginde-Gerceklestirilecek#:~:text=Konferans%2025%2D28%20Ekim%202022,Geli%C5%9Fme

%20%C3%87a%C4%9F%C4%B1nda%20Mahremiyet%E2%80%9D%20%C5%9Feklinde%20belirlenmi%C5%9Ftir adresinden 03 Şubat 2024 tarihinde alınmıştır.

KVKK. (b.t..). Kişisel verilerin korunması alanında uluslararası ve ulusal düzenlemeler. https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler adresinden 25 Ocak 2023 tarihinde alınmıştır.

Leboukh, F., Aduku, E. B. ve Ali, O. (2023). Balancing ChatGPT and data protection in Germany: Challenges and opportunities for policy makers. *Journal of Politics and Ethics in New Technologies and AI*, *2*(1), 1-8. https://doi.org/10.12681/jpentai.35166

McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data and Society*, *4*(1), 1-7. https://doi.org/10.1177/2053951716686994

OIPC (2023, 07 Aralık). Principle for responsible, trustworthy and privacy-protective generative AI technologies. https://www.priv.gc.ca/en/privacy-topics/technology/artificial intelligence/gd_principles_ai/ adresinden 10 Ocak 2024 tarihinde alınmıştır.

Ooi, K. B., Tan, G. W. H., Al-Emran, M., Al-Sharafi, M. A., Capatina, A., Chakraborty, A. ve Wong, L. W. (2023). The potential of Generative Artificial Intelligence across disciplines: Perspectives and future directions. *Journal of Computer Information Systems*, 1-32. https://doi.org/10.1080/08874417.2023.2261010

Raab, C. ve Szekely, I. (2017). Data protection authorities and information technology. *Computer Law and Security Review*, *33*(4), 421-433.

Resmi Gazete. (2016, 24 Mart). 6698 sayılı Kişisel Verileri Koruma Kanunu. https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf adresinden 8 Şubat 2024 tarihinde alınmıştır.

Resmi Gazete. (2018, 9 Şubat). Kişisel Verileri Koruma Uzmanlığı Yönetmeliği. https://www.resmigazete.gov.tr/eskiler/2018/02/20180209-3.htm adresinden 11 Şubat 2024 tarihinde alınmıştır.

Sarlet, G. B. S. ve Rodriguez, D. P. (2023). Alternatives for an adequate structuring of the national data protection authority (ANPD) in its independent profile: Proposals to overcome the technological challenges in the age of digital governance. *International Cybersecurity Law Review*, *4*, 197-211.

Sevinç, İ. ve Karabulut, N. (2020). A review on the personal data protection authority of Turkey. *Akademik Hassasiyetler*, *7*(13), 449-472.

Tansuğ, Ç. (2018). Fransız hukukunda kişisel verileri koruma otoritesi: CNIL. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, *14*(2), 335-354.

Yuste, R. (2023). Advocating for neurodata privacy and neurotechnology regulation. *Nature Protocols*, *18*(10), 2869-2875. https://doi.org/10.1038/s41596-023-00873-0

Wills, B. D. (2017). The technology foresight activities of European Union data protection authorities. *Technological Forecasting and Social Change*, *116*, 142-150.

e-ISSN: 2757 - 5489
TOPLUM, EKONOMİ VE YÖNETİM DERGİSİ
JOURNAL OF SOCIETY, ECONOMICS AND MANAGEMENT
Cilt 5 Sayı 3 Ay Ekim Yıl 2024
Volume Issue Month October Years

EXTENDED ABSTRACT

Since the 1970s, it has been observed that governments and international organizations have begun to take measures regarding the protection of personal data. In this context, the first international treaty with binding force on the protection of personal data, namely Convention No. 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data, was opened for signature by the Council of Europe in 1981. Although Turkey signed the treaty in 1981, it became binding for Turkey with the law enacted in 2016. The enactment of Law No. 6698 on the Protection of Personal Data and the establishment of the Personal Data Protection Authority in 2016 are significant developments in Turkey regarding the protection of personal data. This study examines the role of data protection authorities in the protection of personal data against technological developments and attempts to make recommendations for the KVKK (Personal Data Protection Authority) in this regard.

Data protection authorities are institutions responsible for enforcing legal regulations concerning the protection of personal data. These authorities play a significant role in safeguarding privacy, which is a fundamental right. However, there is not enough research available regarding the activities of data protection authorities, which play a key role in protecting this right. Particularly, the rapid advancements in technology complicate the protection of personal data and, in this sense, impose a greater role on data protection authorities.

The rapid advancement of technological developments necessitates the development of legal regulations as well. Especially big data, the Internet of Things, and drones are new technologies that have implications for privacy and data protection. Nowadays, these new technologies are being used in many fields. It is observed that next-generation technologies are being used in various fields such as healthcare, commerce, transportation, smart homes, and smart cities. Additionally, recently introduced productive artificial intelligence (GenAI) technologies have reached a large user base. Like other technologies, these technologies also have advantages and disadvantages for individuals.

Nowadays, data can be processed at a very rapid pace. The speed and convenience of data processing increase the risk of personal data protection. Changes in consumer habits and the effort to learn consumer preferences have led to the widespread use of technology in all areas, making it much easier to access data about individuals' lifestyles and habits. One of the recently popular technologies is Generative Artificial Intelligence (Generative AI-GAI). These technologies have reached a significant user base. Data protection authorities have prepared advisory guidelines regarding the risks that these technologies may pose to the protection of personal data.

In this context, the research questions of the study can be formulated as follows: What are the risks faced in the protection of personal data in the face of rapidly advancing technology? What practices are data protection authorities implementing to better protect personal data against technological advancements? What practices are implemented under the scope of KVKK in Turkey, and what can be done? In order to find answers to the research questions, the studies on the subject in the literature were examined and the practices of data protection

authorities of various countries were examined. Turkey's personal data protection authority, KVKK, is also evaluated in this context, and recommendations are presented.

Data protection authorities are responsible for enforcing data protection laws, but they can also serve as guides and consultants against the risks posed by new technologies, thereby preventing potential data breaches in advance. In this sense, data protection authorities have obligations such as conducting examinations and investigations, providing counselling and advice, providing guidance, making decisions and imposing sanctions in order to take measures against the risk of data breaches brought by technological developments. In this regard, many countries' data protection authorities are creating informative guidelines.

The studies in the field indicate that the shortage of IT expert personnel contributes to the challenges faced by data protection authorities in preparing for new technologies (Raab & Szekely, 2017; Wills, 2016; Sarlet and Rodriguez, 2023). They also emphasize the importance of institutional cooperation processes. In this regard, it is seen as crucial for data protection authorities to increase their capacity to protect personal data in the face of new technologies by increasing the number of personnel with IT expertise. Accordingly, it may be important to increase the number of personnel with IT expertise within the structure of KVKK. Additionally, a unit similar to the Artificial Intelligence Department (AID) established under the Technology and Innovation Directorate at CNIL could be formed within KVKK. Furthermore, collaborations with universities, startups, public institutions, and other stakeholders could be developed to proactively address the privacy risks posed by new technologies.