BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

POSTA SEKTÖRÜNDE KİŞİSEL VERİLERİN GİZLİLİĞİ VE GÜVENLİĞİ: ÜLKE UYGULAMALARI VE TÜRKİYE İÇİN ÖNERİLER

Beray DİKİLİTAŞ

Bilişim Uzmanlığı Tezi

Eylül 2025

Ankara

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

POSTA SEKTÖRÜNDE KİŞİSEL VERİLERİN GİZLİLİĞİ VE GÜVENLİĞİ: ÜLKE UYGULAMALARI VE TÜRKİYE İÇİN ÖNERİLER

Beray DİKİLİTAŞ

Bilişim Uzmanlığı Tezi

Eylül 2025

Ankara

Beray DİKİLİTAŞ tarafından hazırlanan “Posta Sektöründe Kişisel Verilerin Gizliliği ve Güvenliği: Ülke Uygulamaları ve Türkiye İçin Öneriler” adlı bu tezin Bilişim Uzmanlığı tezi olarak uygun olduğunu onaylarım.

Bilişim Uzmanı, Çiğdem ÖZER GÜNDOĞAN
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlığı tezi olarak kabul edilmiştir.

Başkan : Kurul Üyesi, Mehmet KOÇYİĞİT

Üye : Kurum Başkan Yardımcısı, Müberra OĞUZ

Üye : Daire Başkanı, Muhammet GÜNGÖR

Üye : Bilişim Uzmanı, Çiğdem ÖZER GÜNDOĞAN

Üye : Bilişim Uzmanı, Uğur KAYDAN

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Posta Sektöründe Kişisel Verilerin Gizliliği ve Güvenliği: Ülke Uygulamaları ve Türkiye İçin Öneriler
Türü	Bilişim Uzmanlığı Tezi
Yazar	Beray DİKİLİTAŞ
Teslim Tarihi	23.09.2025
Anahtar Kelimeler	Kişisel veri, kişisel veri gizliliği, kişisel veri güvenliği, posta sektörü, posta güvenliği
Tez danışmanı	Çiğdem ÖZER GÜNDOĞAN
Sayfa Adedi	212 + viii

Geleneksel posta sektörü, kişilerin güvenli ve mahremiyet ilkesine dayalı bir biçimde iletişim kurmalarına olanak tanıyarak, haberleşme hürriyetinin sağlanmasında kritik bir rol üstlenmektedir. Öte yandan, dijitalleşmenin etkisiyle artan e-ticaret hacmi, posta sektöründe bir dönüşüm yaratarak sektörü daha dinamik bir yapıya kavuşturmuştur. Bu dönüşüm sürecinde posta hizmet sağlayıcıları, sundukları hizmetleri çeşitlendirerek yüksek miktarda kişisel veri işleyen aktörler haline gelmiştir. Posta sektörü bağlamında Türkiye'deki mer'i mevzuat, posta hizmetlerinin gizliliği ve güvenliğine ilişkin genel bir çerçeve sunmakla birlikte, kişisel verilerin korunmasına ilişkin olarak sektöre özgü ayrıntılı düzenlemeler içermemektedir. Her ne kadar 6698 sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde genel hükümler uygulanıyor olsa da sektörün kendine has yapısı özel düzenlemelere duyulan ihtiyacı gündeme getirmektedir. Bu tez çalışmasında, kişisel veri kavramı ele alındıktan sonra kişisel verilerin posta sektöründeki görünümleri ile kişisel verilerin gizliliği ve güvenliğine ilişkin uluslararası esas ve uygulamalar incelenmiş, Türkiye'deki mevcut durum analiz edilmiş ve sonuç itibarıyla posta sektörüne yönelik düzenleme önerilerinde bulunulmuştur.

ABSTRACT

INFORMATION TECHNOLOGIES AND COMMUNICATIONS AUTHORITY	
Thesis	Privacy and Security of Personal Data in the Postal Sector: Country Practices and Suggestions for Türkiye
Type	ICT Expertise Thesis
Author	Beray DİKİLİTAŞ
Submission Date	23.09.2025
Key Words	Personal data, personal data privacy, personal data security, postal sector, postal security
Advisor	Çiğdem ÖZER GÜNDOĞAN
Total Page	212 + viii

The traditional postal sector plays a critical role in ensuring freedom of communication by enabling individuals to communicate securely and confidentially. Meanwhile, the increasing volume of e-commerce driven by digitalization has transformed the postal sector, giving it a more dynamic structure. During this transformation, postal service providers have diversified their services and become actors processing large amounts of personal data. While current postal legislation in Türkiye provides a general framework for the privacy and security of postal services, it does not include detailed sector-specific regulations regarding personal data protection. While general provisions are implemented within the framework of 6698 numbered Personal Data Protection Law, the sector's unique structure brings forward necessities of specialized regulations. In this thesis, after addressing the concept of personal data, international principles and practices regarding personal data and the privacy and security of personal data in the postal sector were examined, the current situation in Türkiye was analyzed and as a result, regulatory recommendations for the postal sector were made.

TEŞEKKÜR

Tez çalışmam süresince engin bilgi birikimi, deneyimi ve vizyonuyla yolumu aydınlatan; yapıcı yaklaşımı, sabrı ve desteğiyle yanımda olan kıymetli danışmanım Sn. Çiğdem ÖZER GÜNDOĞAN'a, beni her zaman destekleyen Başkanım Sn. Müberra OĞUZ'a, değerli görüş ve katkılarıyla beni yönlendiren Sn. Burak Cesur AKÖZ, Sn. İdris GÜRBÜZ, Sn. Nurullah ÇAKMAK, Sn. Nuri AYGÜN ve Sn. Uğur KAYDAN'a, iş arkadaşı olmanın ötesinde, her daim yanımda olan ve gerçek bir dost olarak zamanını ve bilgisini paylaşan değerli arkadaşım Sn. Elçin Gökçen EFE'ye, destekleriyle bana güç veren sevgili arkadaşlarım Sn. Tuba Rabia UZUNOĞLU, Sn. Mert BATTAL, Sn. Ali Burak AKBULUT ile Sn. Gamze ÖZTÜRK DÜDÜKCÜ'ye ve sevgili aileme teşekkür ederim.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AB	Avrupa Birliği (European Union-EU)
ABAD	Avrupa Birliği Adalet Divanı (Court of Justice of the European Union)
ABD	Amerika Birleşik Devletleri
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AK	Avrupa Konseyi
ATHB	Avrupa Birliği Temel Haklar Bildirgesi
Aydınlatma Yükümlülüğü Tebliğ	Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ
AYM	Anayasa Mahkemesi
BGYS	Bilgi Güvenliği Yönetim Sistemi
BM	Birleşmiş Milletler
BTK	Bilgi Teknolojileri ve İletişim Kurumu
Çin	Çin Halk Cumhuriyeti
EDPB	Avrupa Veri Koruma Kurulu (European Data Protection Board)
EHK	5809 sayılı Elektronik Haberleşme Kanunu
ERGP	Avrupa Posta Hizmetleri Düzenleyicileri Grubu (The European Regulators Group for Postal Services)
GDPR	Genel Veri Koruma Tüzüğü (General Data Protection Regulation)
ICO	İngiltere Veri Koruma Kurumu (Information Commissioner's Office)
İHEB	İnsan Hakları Evrensel Beyannamesi
IP	Internet Protocol
KVKK	6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun

KVK Kurulu	Kişisel Verileri Koruma Kurulu
KVK Kurumu	Kişisel Verileri Koruma Kurumu
MDSA	UPU Çok Taraflı Veri Paylaşımı Anlaşması (Multilateral Data Sharing Agreement)
PİYY	Bilgi Teknolojileri ve İletişim Kurumu Posta Sektöründe İdari Yaptırımlar Yönetmeliği
OECD	Ekonomik İşbirliği ve Kalkınma Örgütü (The Organisation for Economic Co-operation and Development)
OECD Rehber İlkeleri	OECD tarafından yayımlanan "Kişisel Verilerin Sınır Aşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri" (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)
OFCOM	Birleşik Krallık Haberleşme Otoritesi (Office of Communications)
OIG	Birleşik Devletler Posta Hizmetleri Genel Müfettişlik Ofisi (USPS Office of Inspector General)
PHK	6475 Sayılı Posta Hizmetleri Kanunu
PHS	Posta Hizmet Sağlayıcısı
POC	Posta İşlemleri Konseyi (Postal Operations Council)
PHSİY	Posta Hizmetlerinin Sunulmasına İlişkin Yönetmelik
PSİYY	Posta Sektörüne İlişkin Yetkilendirme Yönetmeliği
PTT	Posta ve Telgraf Teşkilatı Anonim Şirketi
UAVT	Ulusal Adres Veri Tabanı
UPU	Uluslararası Posta Birliği (Universal Postal Union)
TBK	6098 sayılı Türk Borçlar Kanunu
T.C.	Türkiye Cumhuriyeti
TCK	5237 sayılı Türk Ceza Kanunu
TKHK	6502 sayılı Tüketicinin Korunması Hakkında Kanun
TMK	4721 sayılı Türk Medeni Kanunu
TRAFICOM	Finlandiya Ulaştırma ve İletişim Kurumu

TSE	Türk Standartları Enstitüsü
UK GDPR	Birleşik Krallık GDPR (United Kingdom General Data Protection Regulation)
USPS	ABD Posta Servisi (US Postal Service)
VERBİS	Veri Sorumluları Sicili
Veri Sorumlusuna Başvuru Tebliği	Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ
VKÇG	Madde 29 Veri Koruma Çalışma Grubu (Article 29 Working Group)
95/46/EC sayılı Direktif	Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi
108 sayılı Sözleşme	Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin korunmasına ilişkin 108 sayılı Avrupa Konseyi Sözleşmesi
181 sayılı Ek Protokol	181 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol
7499 sayılı Kanun	Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun

GİRİŞ

Günümüzde yaşanan teknolojik gelişmeler, verilerin toplanmasını, işlenmesini, depolanmasını, aktarımını ve erişilebilirliğini kolaylaştırmaktadır. Veriler, sistematik bir şekilde toplanarak çok hızlı bir biçimde analiz edilmekte ve çeşitli amaçlarla kullanılmaktadır. Bu çerçevede işletmeler de elde ettikleri verileri ticari esaslara dayalı iş modelleriyle kullanarak büyük kârlar elde edebilmektedirler. Sahip olduğu bu ekonomik değer nedeniyle veri, çağın "yeni petrolü" veya "yeni para birimi" olarak da tanımlanmaktadır.

Veri kullanımının bu denli yaygınlaşması ve katma değer yaratması, günümüzde insanların mahremiyetine ilişkin temel haklardan biri olarak görülen kişisel verilere yönelik tehditleri artırmış ve kişisel verilerin korunması ihtiyacını gündeme getirmiştir. Posta sektörü de teknolojide meydana gelen gelişmeler ve e-ticaretin yaygınlaşmasıyla kişisel verilerin yoğun olarak işlendiği bir alan olarak nitelendirilebilmektedir. Bu kapsamda posta gönderilerinin toplanması, tasnif edilmesi, taşınması ve teslim edilmesi gibi aşamalarda kişisel verilerin gizliliği ve bu verilerin güvenliğinin sağlanması yasal gerekliliklerin yerine getirilmesi açısından büyük önem taşımaktadır.

Bu çerçevede bu çalışmada temel olarak, posta sektöründe kişisel verilerin gizliliği ve güvenliği konusu esas alınmaktadır. Posta sektöründe kişisel verilerin gizliliği ve güvenliğine ilişkin sorunların ele alınması, bunlara yönelik öncül düzenleyici yaklaşımlar hakkında ayrıntılı incelemeler yapılması ve uluslararası gelişmeler ışığında Bilgi Teknolojileri ve İletişim Kurumu (BTK)'nun da rolü ortaya konularak Türkiye'deki posta sektörü için uygulanabilir düzenleyici öneriler teklif edilmesi bu tezin hedeflenen başlıca çıktısıdır.

Bu kapsamda, tezin birinci bölümünde kişisel veri kavramı ile bu kavramın unsurlarının neler olduğuna ilişkin bilgilere yer verilerek kişisel verinin kapsamı ortaya

konulacaktır. Ayrıca veri sorumlusu, veri işleyen, özel nitelikli kişisel veri kavramları ile kişisel verilerin işlenmesi ve bu verilerin imhasına dair genel esaslar ele alınacaktır. Devamında ise kişisel verilerin korunması hukukunun gelişim süreci de dikkate alınarak bu alana dahil uluslararası mevzuat hükümlerine yer verilecektir.

İkinci bölümde posta hizmeti, posta hizmetinin aşamaları ve çeşitleri açıklanacaktır. Devamında kişisel verilerin posta sektöründeki görünümleri ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) çerçevesinde posta sektöründe kişisel verilerin işlenmesine ilişkin temel ilkeler, hukuka uygunluk sebepleri ve kişisel verilerin yurt dışına aktarımı gibi başlıklar ele alınacaktır. Posta kullanıcısı hakları ve posta hizmet sağlayıcısı (PHS) yükümlülükleri ile hukuka aykırı veri işlenmesinden doğan sorumluluklar da bu bölümde tetkik edilecek konular arasındadır.

Üçüncü bölümde, posta sektöründe kişisel verilerin güvenliğiyle ilişkili olarak bilgi, bilgi güvenliği ve veri güvenliği kavramlarına yer verilecektir. Sonrasında kişisel veri güvenliğine dair alınabilecek idari ve teknik tedbirlere değinilerek PHS'lerin kişisel veri ihlallerine karşı alabilecekleri güvenlik önlemleri ve uygulamalar açıklanacaktır.

Dördüncü bölümde posta sektöründe kişisel verilerin gizliliği ve güvenliğine yönelik seçili ülke uygulamaları incelenecektir. Akabinde ise Türkiye'deki mevcut duruma yer verilecektir.

Son bölümde ise genel bir değerlendirme yapılarak ülkemize yönelik düzenleme önerileri sunulacaktır.

1 KİŞİSEL VERİ VE KİŞİSEL VERİLERİN GİZLİLİĞİ KAVRAMLARI

Bu bölümde öncelikle kişi, kişilik ve veri kavramlarına değinilerek, kişisel verinin tanımı, unsurları ve hukuki niteliği ile veri sorumlusu, veri işleyen, özel nitelikli kişisel veri başta olmak üzere kişisel veriyle ilişkili bazı önemli kavramlar ele alınmakta ve devamında ise kişisel verilerin işlenmesi ve imhasına ilişkin temel hususlar açıklanmaktadır.

1.1 Kişisel Veri Kavramı

Kişisel veri kavramı ele alınmadan önce, bu kavramın daha iyi anlaşılması adına, onun içerdiği terimlerin ayrı ayrı incelenmesi faydalı görülmektedir. Bunlar kişi, kişilik ve veri kavramlarıdır.

Kişi kavramı birçok hukuk sisteminin temelini oluşturmakta olup 08.12.2001 tarihli ve 24607 sayılı Resmî Gazete'de yayımlanan 4721 sayılı Türk Medeni Kanunu'nun (TMK) *"Hak ehliyeti"* başlıklı 8 inci maddesinde, *"haklara ve borçlara ehil olabilen varlıklar"* şeklinde ifade edilmektedir. Haklara ve borçlara ehil ya da hak ehliyetine sahip olma konusu genellikle insan kavramını akla getirmekle birlikte Türk hukukunda kişi kavramı yalnızca insanı kapsamamaktadır. Bir varlığın kişi olup olmadığını kararlaştıran kanun koyucu, insan dışında belirli bazı özelliklere sahip olan kişi veya mal topluluklarını da kişi kapsamında kabul edebilmektedir[1]. Bu kapsamda TMK, kişi ifadesiyle hem tek ve fiziki varlık olarak insanı hem de topluluk özelliği gösteren tüzel kişiyi ifade etmektedir. Gerçek kişi insanı tanımlamakta olup tüzel kişi insan olmayan ancak hukukun bir tür kişilik atfettiği soyut varlıkları açıklamaktadır[2].

---

[1] Gonca, Oktay, *Kişilik Haklarının Korunması*, (Yüksek Lisans Tezi, Akdeniz Üniversitesi, 2011), 4.

[2] Ömer, Özkaya ve İbrahim, Toprak, "Türkiye'de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi", *MANAS Sosyal Araştırmalar Dergisi,* Cilt: 11, Sayı: 3, (2022): 1292.

Kişilik, kişilerin tam ve sağ doğması koşuluyla kazandığı bir hak olarak karşımıza çıkmaktadır. Haklara ehil olmaktan daha geniş bir kavram olan kişilik, "kişinin yaşamı, beden tümlüğü ve sağlığı gibi maddi bedensel değerleri; ehliyetleri, onuru, saygınlığı, giz alanı, inanç ve özgürlükleri, adı ve resmi üzerindeki hakkı gibi manevi değerleri; mesleki ve ticari onur ve saygınlığı, mesleki ve ticari gizleri ve kredisi gibi mesleki-ticari manevi değerleri"nin bütünüdür. Bu kapsamda en genel ifadeyle kişilik hakkı, kişiliği meydana getiren değerlerin tümü üzerindeki hak olarak ifade edilebilmektedir[3].

Veri kavramı ise üzerinde uzlaşılmış tek bir tanımı bulunmamakla birlikte Türk Dil Kurumu Bilişim Terimleri Sözlüğünde; *"Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi"* olarak tanımlanmaktadır[4]. Literatürde ise veri, *"herhangi bir işleme tabi tutulmadan, gözlem veya ölçüm yöntemleri ile ortamdan elde edilen her türlü değer[5]"* olarak ya da *"tek başına anlam ifade etmeyen veya kullanılamayan, bununla birlikte enformasyona ve bilgiye temel oluşturan ilişkilendirilmeye, gruplandırılmaya, yorumlanmaya, anlamlandırılmaya ve analiz edilmeye gereksinim duyulan ham bilgi[6]"* biçiminde tanımlanabilmektedir. Esasen günümüzde veri, araştırmalar, gözlemler, internet, sosyal medya ve sensörler gibi çeşitli kaynaklardan elde edilen bilgilerin genel terimini ifade etmektedir[7].

Bu açıklamalar ışığında kişi ile veri kavramlarının kesiştiği bir nokta olarak karşımıza kişisel veri kavramı çıkmaktadır. Kişisel veriler tarih boyunca hem kamusal hem de özel menfaatler gereği ve hukuki, iktisadi ya da siyasi amaçlarla çeşitli şekillerde toplanmış ve kullanılmıştır. Örneğin, bireyler ve haneler hakkında yaş, cinsiyet, meslek ve servet gibi bilgilerin toplanmasını içeren nüfus sayımları kişisel verilerin en eski kullanım alanlarından biri olarak karşımıza çıkmaktadır. Benzer biçimde, 19.

---

[3] Hüseyin Can, Aksoy, *Kişisel Verilerin Korunması,* (Yüksek Lisans Tezi, Ankara Üniversitesi, 2008), 49.
[4] Türk Dil Kurumu, Bilişim Terimleri Sözlüğü.
[5] Şadi Evren, Şeker, *İş Zekası ve Veri Madenciliği*, (İstanbul: Cinius, 2013).
[6] Malik, Yılmaz, "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi", *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi,* Cilt: 49, Sayı: 1, (2009): 98.
[7] Korcan, Doğan ve Sacit, Arslantekin, "Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum", *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, Cilt: 56, Sayı: 1, (2016): 16.

yüzyıldan itibaren bankalar, bireylerin kredi geçmişi, borçları ve ödeme alışkanlıklarına ilişkin bilgiler toplamaya başlamış ve bu verileri kredi değerlendirme süreçlerinde kullanmıştır. 20. yüzyılda ise devletler, vatandaşlarının vergi yükümlülüklerini ve sosyal yardım taleplerini takip edebilmek amacıyla sosyal güvenlik numarası sistemini hayata geçirmiştir. Aynı dönemde işletmeler müşterileri hakkında veri toplayarak bu bilgileri pazarlama stratejileri için kullanmaya başlamış, hükümetler de vatandaşların faaliyetlerini izlemek amacıyla çeşitli veri toplama yöntemleri geliştirmiştir[8]. 21. yüzyılda kişisel veriler; bireyin kimliği, etnik kökeni, sağlık durumu, finansal bilgileri, telefon rehberi kayıtları, SMS ve e-posta içerikleri, IP (Internet Protocol) adresi gibi dijital izleri ve sosyal medya aktiviteleri hakkında bilgi veren bir konuma gelmiştir.

1.2 Tanımı ve Unsurları

Kişisel veri kavramının üzerinde anlaşılmış, tek tip bir tanımı bulunmamaktadır. Bununla birlikte en genel anlamda kişisel veri; belirli ya da belirlenebilir olmak şartıyla bir bireye ait tüm bilgileri ifade etmektedir[9]. Birçok ulusal ve uluslararası mevzuatta yer verilen bu tanıma ilk defa Ekonomik İşbirliği ve Kalkınma Örgütü (*The Organisation for Economic Co-operation & Development*, OECD) tarafından 23.09.1980 tarihinde yayımlanan "Kişisel Verilerin Sınır Aşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri"nin (OECD Rehber İlkeleri) 1 inci maddesinde yer verilmiştir. Diğer yandan, kişisel veri kavramının tanımına başka uluslararası metinlerde de yer verildiği görülmektedir. Örneğin, *"*Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi*"* nin (95/46/EC sayılı Direktif) 2 nci maddesinin (a) bendinde kişisel veri, "*doğrudan veya dolaylı olarak tespit edilmiş veya tespit edilebilir gerçek kişiye ilişkin herhangi bir bilgi"*

---

[8] Özlem, Özsoy, *Kişisel Verilerin Korunması Hukukunda İlgili Kişinin Hakları*, (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, 2024): 3.

[9] Nevzat Ali, Anı, *Kişisel Verilerin İşlenmesi ve Açık Rıza*, (Yüksek Lisans Tezi, İstanbul Üniversitesi, 2018), 8.

olarak ifade edilmiştir[10]. 25.05.2018 tarihinde yürürlüğe giren Avrupa Birliği (AB) Genel Veri Koruma Tüzüğü'nün (*General Data Protection Regulation*, GDPR) 4 üncü maddesinin birinci fıkrasında ise bu kavram *"tanımlanmış/belirlenmiş veya tanımlanabilir/belirlenebilir olan bireye ilişkin her türlü bilgi"* şeklinde yer bulmaktadır.

Türk hukukunda 07.04.2016 tarihine kadar kişisel verilerin korunmasına ilişkin özel bir kanun bulunmamakla birlikte, bunun öncesinde başta 1982 tarihli Türkiye Cumhuriyeti (T.C.) Anayasası olmak üzere birtakım kanun ve yönetmelik hükümleriyle kişisel veriler koruma altına alınmıştır[11]. Örneğin; 2008 yılında yürürlüğe giren 5809 sayılı Elektronik Haberleşme Kanunu (EHK) öncesinde yürürlükte olan mülga Telgraf ve Telefon Kanunu ve bazı hükümleri yürürlükten kaldırılan Telsiz Kanunu'na dayanılarak hazırlanan "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" içerisinde kişisel veri; *"tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi*

---

[10]Avrupa Parlamentosu ve Avrupa Konseyi, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, (1995).

[11] KVKK yürürlüğe girmeden önce, kişisel verilerin korunmasına dair hükümlerin bir kısım mevzuat ile düzenlendiği görülmektedir. T.C. Anayasası, Türk Medeni Kanunu, İş Kanunu, Türk Borçlar Kanunu, Türk Ceza Kanunu, Türk Ceza Muhakemesi Kanunu, Elektronik Haberleşme Kanunu, Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, Elektronik Ticarette Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcılar Hakkında Yönetmelik, Elektronik İmza Kanunu, Banka Kartları ve Kredi Kartları Hakkında Yönetmelik, Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik, Mesafeli Sözleşmeler Yönetmeliği, Polis Vazife ve Salahiyet Kanunu, Bilgi Edinme Kanunu, Türkiye İstatistik Kanunu, Sosyal Güvenlik Kurumu Kanunu, Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun, İlaç ve Biyolojik Ürünlerin Klinik Araştırmaları Hakkında Yönetmelik, Anonim Şirketlerin Genel Kurullarında Uygulanacak Elektronik Genel Kurul Sistemi Hakkında Tebliğ, Ticaret Sicil Yönetmeliği, Özel İstihdam Büroları Yönetmeliği, Sermaye Şirketlerinin Açacakları İnternet Sitelerine Dair Yönetmelik, Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, Hasta Hakları Yönetmeliği, Bankaların İç Sistemleri Hakkında Yönetmelik gibi mevzuatlarda kişisel verilerin korunmasına dair hükümlere yer verilmiştir. (Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu ve Uygulaması,* 2024).

bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgi" olarak tanımlanmıştır. Daha sonra yürürlüğe giren EHK'de ise kişisel veri tanımı yer almamış, ancak BTK'nin görev ve yetkileri arasında; *"abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak"* sayılmıştır[12]. Bu sayede BTK'ye, elektronik haberleşme sektörü ile kişisel verilerin işlenmesi ve gizliliğinin korunmasına ilişkin usul ve esasları belirleme yetkisi verilmiştir. Ayrıca işletmecilere de kişisel verilerin gizliliğin korunması yükümlülüğü getirilmiştir[13].

KVKK ise kişisel verilere ve bu verilerin korunmasına dair hükümler içeren özel bir kanun olarak 07.04.2016 tarihli 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Anılan Kanun'un 3 üncü maddesinin birinci fıkrasının (d) bendinde GDPR'a benzer bir şekilde kişisel veri, *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* biçiminde tanımlanmıştır.

Diğer yandan literatür ile yargı kararlarında da bu kavrama ilişkin tanımlamalara gidilmektedir. Bazı yazarlara göre kişisel veri, bir gerçek kişinin özelliklerini ifade eden ve o kişiyi başkalarından ayırt etmeye yarayan bilgi olarak tanımlanabilmekteyken[14] Yargıtay kişisel veriyi, *"kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü veri"* olarak tanımlamıştır[15].

---

[12] 5809 sayılı Elektronik Haberleşme Kanunu, 2008.
[13] Habip, Oğuz, "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum", *Uyuşmazlık Mahkemesi Dergisi*, Sayı: 3, (2013): 14-16.
[14] Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi No: 1", *KVKK Yayınları*, (2019): 52; Akkurt, "Kişisel Veri Kavramının…": 20; Dülger, *Kişisel Verilerin Korunması Hukuku*: 44.
[15] Yargıtay 12'nci Ceza Dairesi Kararı, 05.09.2018 günlü, E:2018/2571, K:2018/7821 sayılı karar.

Bu kapsamda kişisel veri kavramının daha iyi anlaşılabilmesi adına, kişisel veri tanımında sıklıkça yer verilen unsurlara da değinilmesi önem arz etmektedir. AB ve Türk hukuku bakımından kişisel verilerden bahsedilebilmesi için üç unsurun bir arada var olması şartı aranmaktadır. Bu unsurlar, "*gerçek kişiye ilişkin olma, kişiyi belirli veya belirlenebilir kılma ve her türlü bilginin kişisel veri olabilmesi"*dir[16].

Bu kapsamda ilk unsur gerçek kişi kavramını içermektedir. KVKK'nin üçüncü maddesinin birinci fıkrasının (ç) bendinde ilgili kişi; *"kişisel verisi işlenen gerçek kişi"* biçiminde tanımlanmıştır. Bu itibarla kişisel veri, yalnızca gerçek kişiye ait bir bilgi olup ilgili mevzuat uyarınca tüzel kişilere dair veriler kişisel veri kapsamında kabul edilmemektedir[17]. GDPR'ın *"Başlangıç"* bölümünde yer alan 14 üncü madde hükmünde de uyruk ya da yerleşim yeri fark etmeksizin GDPR kapsamında kişisel verilerin işlenmesinde sağlanacak olan korumanın yalnızca gerçek kişilere uygulanacağı, tüzel kişilere ait verilerin işlenmesinde GDPR'ın uygulanmayacağı belirtilmiştir. Bununla birlikte tüzel kişinin verisinin elde edilmesi, gerçek kişinin verisinin de elde edilmesine sebep oluyorsa, bu verilerin de hukuksal koruma kapsamına alınması mümkündür. Keza bu durumda esasen tüzel kişinin verisi değil, gerçek kişinin kişisel verisi korunmaktadır[18]. Örneğin, tüzel kişinin isminin bir gerçek kişi isminden oluştuğu ya da bir şirket çalışanının isim ve soy ismini içeren kurumsal e-posta veya telefon kullanılması halinde bu korumadan yararlanılabilmesi mümkün olacaktır[19].

Diğer yandan KVKK'de sadece gerçek kişilerin verilerinin koruma altına alınması, sektörlere özgü yapılan düzenlemelerde tüzel kişi verilerinin koruma altına alınmasına dair bir hüküm getirilmesine engel teşkil etmemektedir. Nitekim AB'ye

---

[16] Çiçek, Ersoy Kekevi, *Genel Kavramlar, Kişisel Verilerin Korunmasına Akademik Bakış- KVKK Akademi Derleme Çalışması*, ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy, (Ankara: Ütopya Grafik, 2023): 104.

[17] Mesut Serdar, Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, (On İki Levha Yayıncılık, 2020): 44.

[18] Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Kanununa İlişkin…": 45.

[19] Avrupa Komisyonu, "Do the data protection rules apply to data about a company?".

üye ülkelerden Avusturya, Danimarka, İtalya ve Lüksemburg ile üye olmayan ülkelerden İzlanda, İsviçre ve Norveç veri koruma düzenlemeleriyle tüzel kişileri de koruma kapsamına dahil etmiştir[20].

Bu doğrultuda, "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik" ile "Posta Sektörüne İlişkin Yetkilendirme Yönetmeliği"nde kişisel veri tanımının içeriğinde tüzel kişilere de yer verilmiştir.

İkinci unsur olarak kişisel veri tanımı yapılırken bilginin, yalnızca "belirli veya belirlenebilir gerçek kişiye ilişkin" olması esas alınmaktadır. Buna göre, GDPR'ın 4 üncü maddesinin birinci fıkrasında bir kişiyi doğrudan ya da dolaylı olarak belirleyebilecek olan bilgilerin kişisel veri olduğu kabul edilmektedir. Bu madde hükmünün devamında örneklendirme yoluna gidilmiş olup kişinin kimlik numarası, konum bilgisi ya da çevrim içi tanımlayıcılara veya genetik, fiziksel, zihinsel, sosyal ve ekonomik kimliğe atıfta bulunulmuştur.

Kişisel Verileri Koruma Kurumu (KVK Kurumu) da benzer bir tanımlama yoluna gitmiştir. Buna göre ekonomik, sosyal, fiziksel, ailevi gibi niteliklere ilişkin bilgilerin, bireyi belirlenebilir kılması halinde, bu bilgiler kişisel veri olarak kabul edilmektedir[21]. Diğer yandan KVKK'nin gerekçesinde bir kişinin "belirli veya belirlenebilir" olması, *"mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder"* olarak belirtilmiştir. Bir başka deyişle gerçek kişinin halihazırda kimliğinin belirlenmediği; ancak kimlik tespitinin mümkün olduğu hallerde, kişinin belirlenebilir kılınacağı kabul edilmektedir[22].

---

[20] Esranur, Dülber, "*Türk Hukukunda Kişisel Verilerin Korunması Hakkı ve Basın Hürriyeti Çatışması"*, (Yüksek Lisans Tezi, Hacettepe Üniversitesi, 2024): 12

[21] Kişisel Verileri Koruma Kurumu, "Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü", *KVKK Yayınları*, (2019): 9.

[22] Doğan, Kılınç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 61, Sayı: 3 (2012).

Üçüncü unsur ise her türlü bilgiyi kapsamaktadır. Buna göre, KVKK'de kişisel veri tanımında geçen bilgi ifadesi "her türlü bilgi"yi işaret etmektedir. Böylece gerçek kişilerin KVKK kapsamındaki korumadan azami seviyede faydalanmasının sağlanması amaçlanmıştır. KVKK'nin 3 üncü maddesinin gerekçesi ile kişisel verinin yalnızca isim, soy isim, doğum tarihi ve doğum yeri gibi kişinin net olarak teşhis edilmesini sağlayan bilgilerinin değil, aynı zamanda kişinin fiziksel, ailevi, ekonomik, sosyal vs. özelliklerine dair bilgilerinin de kişisel veri olduğu belirtilmiştir[23]. Bu kapsamda kişinin; "cinsiyeti, dini inancı, etnik kökeni, fiziksel özellikleri, sağlık, eğitim, öğretim ve istihdam durumu, bireysel ve aile içi yaşantısı, iletişim bilgisi, pasaport numarası, özgeçmişi, fotoğrafı, görüntüsü, ses kaydı, parmak izi, IP adresi, motorlu araç plakası, hobi veya tercihleri, gündelik alışkanlıkları, etkileşim halinde bulunduğu bireyler" gibi bilgileri kişisel veri olarak sayılabilmektedir[24].

Bilginin gerçek olup olmamasının ise verinin kişisel veri niteliği taşımasının değerlendirilmesinde bir etkisi bulunmamaktadır[25]. Ayrıca kişiye ait olan "her türlü bilgi" gerek nesnel gerekse de öznel nitelik taşıyabilmektedir. Örneğin, kişinin mali durumuna ilişkin bilgi nesnel kişisel veri, kişinin dürüst kişilik özelliğine sahip olup olmadığı bilgisi ise öznel kişisel veri olarak kabul edilmektedir[26].

1.3 Kişisel Veriye İlişkin Temel Hukuki Kavramlar

Bu başlık altında kişisel veriye ilişkin temel hukuki kavramlar açıklanacaktır.

---

[23] Kişisel Verileri Koruma Kurumu, "Madde ve Gerekçesi ile…": 9.
[24] Zeynel T., Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, (İstanbul: On İki Levha Yayıncılık, 2019): 21-22.
[25] Avrupa Komisyonu, *Article 29 Data Protection Working Party Opinion 4/2007 on the Concept of Personal Data*, (2007): 6; Selen, Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, (İstanbul: Seçkin Yayıncılık, 2018): 33.
[26] Kangal, *Kişisel Verilerin Ceza…*, 22.

1.3.1 Veri sorumlusu

Veri sorumlusu, KVKK'nin 3 üncü maddesinin birinci fıkrasının (ı) bendinde, *"Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak, GDPR'ın 4 üncü maddesinin yedinci fıkrasında ise *"yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesinin amaçlarını ve yollarını belirleyen gerçek veya tüzel kişi, kamu makamı, kamu kurumu veya diğer organlar"* olarak tanımlanmıştır.

Madde 29 Veri Koruma Çalışma Grubu (*Article 29 Working Group*, VKÇG)[27] ise veri sorumlusu tanımının üç ana unsurunu "gerçek veya tüzel kişi, yetkili kamu kurumu, kuruluşu veya diğer organlar olma", "tek başına veya diğerleriyle birlikte gerçekleştirme" ve "verileri işleme amaç ve vasıtalarını belirleme" olarak belirtmiştir. İlk unsur, hangi kişilerin veri sorumlusu olabileceğine ilişkin olup ikinci unsur veri işlemenin birden çok kişinin kontrolünde olma olasılığına ilişkindir. Üçüncü unsur ise veri sorumlusunun, işleme faaliyetinin ana ögeleri hakkında karar veren taraf olduğunu, bu yetkinin hem idari hem de teknik unsurları kapsadığını göstermektedir[28].

Veri sorumlusu, gerçek ya da tüzel kişi olabilmektedir. Tüzel kişi, kişisel veriyi işleme konusunda gerçekleştirdiği faaliyetler çerçevesinde "veri sorumlusu" sıfatına sahiptir. İlgili düzenlemelerde yer alan hukuki sorumluluk da tüzel kişinin şahsında doğmaktadır. Bu konuda tüzel kişinin kamu ya da özel hukuk tüzel kişisi olması açısından bir ayrım gözetilmemekte olup bir şirketin, dernek ya da vakfın da veri sorumlusu olması mümkündür[29].

---

[27] 95/46/EC sayılı Direktif doğrultusunda kişisel verilerin korunmasına ilişkin tavsiye niteliğinde kararlar alabileceği hükme bağlanmış olan ve bağımsız hareket eden çalışma grubudur.
[28] Avrupa Veri Koruma Kurulu (EDPB), *"Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 1.0"*, (2020): 10-13.
[29] Kişisel Verileri Koruma Kurumu, "Veri Sorumlusu Kimdir?".

Veri sorumlusunca veri işleme faaliyetinin amaçları ve işlemede kullanılacak yolların belirlemesi ile sürecin organize edilmesi önem arz etmektedir. Kişisel Verileri Koruma Kurulu (KVK Kurulu)'nun 30.01.2020 tarihli ve 2020/71 sayılı kararında özetle; ilgili verilere kimlerin erişebileceği, hangi verilerinin işlenebileceği, bunların ne kadar süreyle ve ne şekilde saklanacağı gibi kişisel veri işlemeye ilişkin teknik ve kurumsal ana unsurların veri sorumlusu tarafından belirleneceği ifade edilmiştir. Anılan kararda ayrıca, işleme faaliyeti gerçekleştirirken veri sorumlusunun bağımsızlığı ve özerkliğinin önemine yer verilmiş; işleme faaliyetinin her aşamasında serbestçe karar alma yetkisine sahip olmasının gerekliliği vurgulanmıştır[30].

Veri sorumlusuyla ilgili bir başka kavram, hukuki sorumluluğun belirlenmesi aşamasında karşılaşılan ortak veri sorumlusudur. Buna göre, GDPR'da iki ya da daha fazla veri sorumlusu tarafından veri işleme amaç yöntemlerinin birlikte belirlenmesi halinde, "ortak veri sorumlusu"nun ortaya çıkacağı belirtilmiştir. KVKK'de ise bu konuda açık bir düzenleme bulunmamakla birlikte KVK Kurulu'nun 23.12.2021 tarihli ve 2021/1304 sayılı ilke kararında, ortak veri sorumlusundan bahsedilmektedir. İlgili karara göre, taşıt kiralama sektöründe faaliyette bulunan işletmelerin "kara liste" olarak bilinen ve kiralanan taşıtın kullanımı sırasında oluşan ödemelerin gecikmeleri ya da taşıttaki zararlara dair menfi durumların kayıt altına alınmasına yarar sağlayan bir yazılımın kullanıldığı, yazılıma ise müşterisi olunan taşıt kiralama şirketi haricinde, yazılımı kullanan diğer taşıt kiralama şirketlerinin de erişebilmesi, kişisel veriler üzerinde hakimiyetlerinin bulunması ve bu verileri kendi çıkarları çerçevesinde kullanan bu şirketlerin ortak veri sorumlusu olarak kabul edileceğine karar verilmiştir[31].

---

[30] Kişisel Verileri Koruma Kurulu Kararı, 30.01.2020 günlü, 2020/71 sayılı "Veri sorumlusu ve veri işleyenin tespitinde göz önünde bulundurulması gereken hususlar ile aydınlatma yükümlülüğünün kim tarafından yerine getirileceği" konulu karar.

[31] Kişisel Verileri Koruma Kurulu Kararı, 23.12.2021 günlü, 2021/1304 sayılı "Araç kiralama sektöründeki kara liste uygulamaları hakkında İlke Kararı" konulu karar.

1.3.2 Kişisel verilerin işlenmesi

Kişisel verilerin işlenmesi, KVKK'nin 3 üncü maddesinin birinci fıkrasının (e) bendinde tanımlanmıştır. Buna göre; *"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"*ne kişisel veri işleme denilmektedir.

Kişisel verilerin elde edilmesinden; silinmesi, yok edilmesi veya anonim hale getirilmesine kadar geçen süreçte yapılan tüm işlemler KVKK kapsamında kişisel verilerin işlenmesi olarak kabul edilmektedir[32].

GDPR'ın 4 üncü maddesinin ikinci fıkrasında ise işleme, *"otomatik yollarla olsun veya olmasın, kişisel veriler veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, geri getirme, danışma, kullanma, iletim yoluyla açıklama, yayma veya bir başka şekilde kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, kalıcı olarak silme veya yok etme gibi herhangi bir işlem veya işlem seti"* biçiminde tanımlanmıştır. GDPR'da KVKK'ye nazaran daha fazla eylem "işleme" olarak sayılsa da esasen tanımların birbirleriyle örtüştüğü görülmektedir[33]. Keza her iki tanımda da "gibi" ifadesine yer verilerek anılan faaliyetlerin sayılanlarla sınırlı olmadığı yani tahdidi olmadığı belirtilmiştir[34].

---

[32] Şehriban İpek, Aşıkoğlu, *Avrupa birliği ve Türk Hukuku'nda Kişisel Verilerin Korunması ve Büyük Veri*, (On İki Levha Yayıncılık, 2018): 110-111.
[33] Hüseyin Murat, Develioğlu, *Avrupa Birliği Genel Veri Koruma Tüzüğü*, (On İki Levha Yayıncılık, 2017): 40.
[34] Beste, Ekin, *Kişisel Verilerin Korunması ve Rekabet Hukuku Boyutuyla Büyük Veri*, (Yüksek Lisans Tezi, İhsan Doğramacı Bilkent Üniversitesi, 2020): 47.

GDPR ve KVKK'deki ilgili tanımlarda "otomatik işleme" ve "otomatik olmayan yolla işleme" ifadelerine yer verilmekte olup bu ifadelere yönelik bir değerlendirmenin yapılmasına ihtiyaç duyulmaktadır. Otomatik işlemenin ne olduğu konusunda GDPR'da ve KVKK'de bir tanım bulunmamaktadır. Bununla birlikte, OECD tarafından otomatik işlemenin; *"İnsan müdahalesi ya da yardımı konusundaki ihtiyacı asgari seviyeye indiren, kendi aralarında bağlantılı ve etkileşimli elektrikli veya elektronik bir sistem tarafından gerçekleştirilen veri işleme faaliyeti"* biçiminde tanımlandığı görülmektedir[35].

KVKK'de kısmen ya da tamamen otomatik yollar ile gerçekleştirilen işleme faaliyetlerinin KVKK kapsamında değerlendirilmesi herhangi bir tereddüde mahal bırakmaksızın mümkünken, otomatik olmayan yollarla gerçekleştirilen işleme faaliyetlerinin KVKK'ye tabi olabilmesi için, söz konusu faaliyetlerin bir veri kayıt sisteminin[36] parçası olarak yürütülmesi gerekmektedir. Bu durum, veri kayıt sisteminin varlığını işleme faaliyetinin anılan Kanun kapsamına alınması için bir ön koşul haline getirmektedir[37]. Örneğin; isim, soy isim, telefon numarası gibi kişisel veriler fihrist ya da indeks gibi bir veri kayıt sistemine yazıldığında bu durum KVKK'ye tabi olacaktır. Benzer şekilde, üzerinde bir işlem yapılmaksızın verilerin sadece depolama amacıyla dosya halinde tutulması halinde de bu faaliyet KVKK kapsamında kabul edilecektir. Öte yandan, gelişigüzel bir şekilde ve manuel yolla bir kâğıdın üzerine yazılan kişisel veriler KVKK kapsamına girmeyecektir[38].

Anonim hale getirilmiş veriler üzerinde gerçekleştirilen işlemler de kişisel veri işleme faaliyeti olarak değerlendirilmemektedir. Zira anonimleştirme işlemi neticesinde,

---

[35] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu ve Uygulaması*, 35.

[36] "Veri kayıt sistemi", KVKK'nin 3 üncü maddesinde, kişisel verilerin belirli kriterlere göre yapılandırılıp işlendiği kayıt sistemi olarak tanımlanmıştır.

[37] Seda, Kuyumcu, *6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması ve Aktarım Koşullarının Değerlendirilmesi*, (Yüksek Lisans Tezi, Galatasaray Üniversitesi, 2024): 26-27.

[38] Kişisel Verileri Koruma Kurumu, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar", *KVKK Yayınları*, No: 31, (2020):14.

veriyle ilgili kişi arasındaki bağlantının bütünüyle ortadan kalkması öngörülmektedir[39].

1.3.3 Veri işleyen

KVKK'nin *"Tanımlar"* başlıklı 3 üncü maddesinin birinci fıkrasının (ğ) bendinde veri işleyen*; "Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* olarak, GDPR'ın 4 üncü maddesinin sekizinci fıkrasında ise *"veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu makamı, kamu kurumu veya diğer organlar"* şeklinde tanımlanmıştır.

Bu kapsamda veri sorumlusunca verilen emir ve yönlendirmeler doğrultusunda ilgili kişilerin verileri, veri işleyen tarafından işlenebilmektedir. Esasen veri işleyen, veri sorumlusunun bir hizmet sağlayıcısı ya da taşeronu gibi işlev görmektedir[40].

Veri işleyen de veri sorumlusu gibi gerçek veya tüzel kişi olabilmektedir. KVKK'de yer almayan ancak GDPR'da açıkça düzenlenen "yazılı sözleşme ilkesi" gereği veri sorumlusu, veri işleyen ile bağlayıcı niteliği olan yazılı bir sözleşme imzalamalıdır[41]. Bu kişisel veri işleme sözleşmesi[42] kapsamında veri işleyen, veri sorumlusunun çalışanı ya da üçüncü bir kişi olabileceği gibi, veri işleme faaliyetini şahsen ya da bir alt işleyici üzerinden gerçekleştirebilir[43].

---

[39] Murat Volkan, Dülger, "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 3, Sayı: 2, (2016): 113.

[40] Emir Efe, Egemen, "Kişisel Verilerin İşlenmesinde "Doğru ve Gerektiğinde Güncel Olma" İlkesi ve Kişisel Verileri Koruma Kurulunun 2023/78 Sayılı Kararı", *Trabzon Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 1, Sayı: 1, (2023): 115.

[41] Zehra, Yürük, "Veri Sorumlusunun Veri Güvenliğine İlişkin İdari ve Teknik Tedbirleri Alma Yükümlülüğü", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, Cilt: 22, Sayı: 48, (2023): 911.

[42] Kişisel veri işleme sözleşmesi, veri işleyence veri sorumlusunun emir ve menfaatlerine uygun bir şekilde bir işlemenin taahhüt edildiği, veri sorumlusu tarafından da bu edim karşılığında ücret ödenmesinin üstlenildiği atipik bir sözleşmedir.

[43] Gamze, Turan Başara, "Kişisel Veri İşleme Sözleşmesi", *Uyuşmazlık Mahkemesi Dergisi*, Sayı: 16, (Aralık 2020): 59-66.

Diğer yandan bir kişi hem veri sorumlusu hem de veri işleyen sıfatına sahip olabilmektedir. Örneğin; bir şirket, çalışanıyla ilgili işlediği veriler açısından veri sorumlusu, müşterisi şirketlere dair işlediği veriler açısından ise veri işleyen olarak kabul edilebilmektedir[44].

1.3.4 Özel nitelikli kişisel veri

Başkalarının öğrenmesi durumunda ilgili kişinin ayrımcılığa uğramasına veya mağduriyetine sebep olabilecek nitelikteki veriler olarak tanımlanabilen özel nitelikli kişisel veriler (hassas veriler), KVKK'nin 6 ncı maddesinin birinci fıkrasında; *"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri"* şeklinde tahdidi olarak sayılmaktadır. Dolayısıyla yorum yolu ile genişletilememekte ve yasada sayılanlar haricinde bir veri, hassas veri olarak nitelendirilmemektedir[45]. Söz konusu durum hassas verilerin işlenmesinin, temel hak ve hürriyetler açısından ciddi riskler doğurabilmesi nedeniyle ayrıca koruma altına alınmasından kaynaklanmakta olup bu mahiyette bir verinin işlenmesi yalnızca istisnai durumlarda söz konusu olabilmektedir[46].

GDPR'ın 9 uncu maddenin birinci fıkrasında ise hassas verilere ilişkin; *"Irk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğini açığa çıkaran kişisel verilerin işlenmesi ve bir gerçek kişinin kimliğini benzersiz bir şekilde belirleyen genetik veriler ile biyometrik verilerinin işlenmesi, sağlık verilerinin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır."*

---

[44] Kişisel Verileri Koruma Kurumu, *Veri Sorumlusu ve Veri İşleyen*, 2.

[45] Kübra, Demir, "İşyeri Hekimlerinin İşçinin Sağlık Verilerinin İşlenmesinde Hukuki Statüsü ve Sorumluluğu", *Selçuk Hukuk Kongresi III*, ed: Doç. Dr. Alper Uyumaz- Dr. Öğr. Üyesi Hüseyin Tokat vd. (2024): 137-142.

[46] Jonas, Wanker, *GDPR vs. PUL, En förbättring av skyddet för anställdas integritet?*, (Yüksek Lisans Tezi, Lund Üniversitesi, 2018): 20.

düzenleme yer almaktadır. KVKK ve GDPR'ın ilgili hükümleri mukayese edildiğinde, KVKK'nin GDPR'dan farklı olarak ceza mahkumiyeti ve güvenlik tedbirleri, kılık kıyafet, dernek veya vakıflara üyelik haline dair bilgileri de hassas veri olarak kabul ettiği ve bu kapsamda Türk mevzuatında hassas verilerin daha geniş çapta ele alındığı tespit edilebilmektedir.

Bu çerçevede, bir işçinin sendika üyeliğine dair işveren tarafından alınan kayıt, bir uçak yolcusunun dini inanışa uygun olan yiyecek tercihlerine ilişkin bilgi, bir çalışanın ameliyat olmak amacıyla hastanede bulunduğunu belirten bilgi, bir şahsın yasaklı madde bağımlılığı olduğuna dair hastane kaydı ve bir şahsın işlediği suça dair kayıt, hassas verilere örnek olarak gösterilebilmektedir[47].

Diğer yandan KVKK'nin 6 ncı maddesinde, hassas veriler arasında genetik ve biyometrik verilere de yer verilmekle birlikte, bu verilerin ne olduğuna dair bir tanım bulunmamaktadır. Türkiye Cumhuriyeti Kimlik Kartı Yönetmeliği'nde ise biyometrik veri; *"Elektronik sistemler aracılığı ile kimlik tespiti ve kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla alınan kişiye özgü veriler"* olarak tanımlanmıştır. Ayrıca KVKK'nin yürürlüğe girmesinden önce Danıştay 15. Hukuk Dairesi'nin E.2014/4562 sayılı kararında biyometrik yöntemler; *"ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme tekniklerini ifade ettiği belirtilerek, bu yöntemler arasında parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, yüz tanıma, retina tanıma, DNA tanıma gibi yöntemler"*[48] olarak, Anayasa Mahkemesi (AYM)'nin bir kararında ise *"Biyometrik yöntemlerle kimlik doğrulama, hizmet talep eden bir kullanıcının, ölçülebilir fizyolojik ve bireysel özellikler yoluyla gerçekleştirilen ve*

[47] Cemil, Kaya, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", *Journal of Istanbul University Law Faculty*, Cilt: 69, Sayı: 1-2, (2011): 322.
[48] Danıştay 15. Hukuk Dairesi Kararı, E: 2014/4562.

otomatik olarak doğrulanabilen kimlik denetleme yoluyla gerçek kullanıcı olup olmadığının doğrulanması anlamına gelmektedir." olarak ifade edilmiştir[49].

GDPR'ın 4 üncü maddesinin on üçüncü fıkrasında genetik veri kavramı; özellikle ilgili kişinin biyolojik bir numunesinin analizinden kaynaklanarak ilgili kişinin fizyolojisi ya da sağlık durumu hakkında benzeri bulunmayan biçimde bilgi veren kalıtımsal özellikleri şeklinde belirtilmiştir. Aynı madde hükmünün on dördüncü fıkrasında ise biyometrik veri kavramı; yüz görüntüleri gibi özel bir teknik işlemden kaynaklanan ve kişinin benzersiz olarak tanınmasına yarayan, fiziksel, fizyolojik veya davranışsal özelliklerine dair veriler olarak ifade edilmiştir. Fizyolojik biyometrik veriler, bireyin vücuduna özgü ve değişmeyen fiziksel özellikleri temel alır. Bu kapsamdaki örnekler arasında iris ve retina desenleri, parmak izi, yüz hatları, avuç içi şekli ile damar yapısı gibi insan bedenine ait ayırt edici veriler bulunmaktadır. Davranışsal biyometrik veriler ise bireyin zaman, duygu durumu, yaş veya çevresel faktörler gibi değişkenlere bağlı olarak sergilediği alışkanlık ve hareket kalıplarına dayalıdır. Örneğin, bir kişinin yürüme tarzı, klavye kullanım alışkanlıkları, dokunmatik ekranlara uyguladığı basınç ve temas şekli ya da araç kullanma biçimi, davranışsal biyometrik veri niteliğindedir[50].

KVKK tarafından yayımlanan "Özel Nitelikli Kişisel Verilerin İşlenmesine İlişkin Rehber"de, GDPR'ın "*Başlangıç"* bölümünün 51 inci maddesi gereğince biyometrik fotoğraflar dahil olmak üzere bireylerin fotoğraflarının işlenmesinin doğrudan biyometrik veri işlenmesi olarak değerlendirilemeyeceği, yalnızca gerçek bir kişinin benzersiz bir biçimde tanımlanmasına ya da doğrulanmasına izin veren belli bir metotla işlendiğinde bu verilerin biyometrik veri kapsamında kabul edileceği belirtilmiştir. Dolayısıyla bir verinin biyometrik veri olarak kabul edilmesi için o verinin yalnızca o bireyi tanımlayabilme veya doğrulayabilme niteliğine haiz olması

[49] Anayasa Mahkemesi Kararı, 19.03.2015 günlü, E:2014/108, K:2015/30 sayılı karar.
[50] Kişisel Verileri Koruma Kurulu Kararı, 27.08.2020 günlü, 2020/649 sayılı karar.

gerekmektedir[51]. Örneğin; bir spor salonunda, üyelerin giriş ve çıkışınlarının avuç iziyle doğrulayan sistemler aracılığıyla takip edilmesi, hassas veri işleme faaliyeti kapsamında nitelendirilmektedir[52].

1.3.5 Kişisel verilerin imhası

KVKK'nin 7 nci maddesinde verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi düzenlenmiştir. Bu kapsamda kişisel veriler, ilgili mevzuata uygun bir şekilde işlenmiş olsalar dâhi işlenme gerekçelerinin ortadan kalkması halinde re'sen veya ilgili kişinin talebi doğrultusunda veri sorumlusu tarafından silinmeli, yok edilmeli ya da anonim hale getirilmelidir[53].

KVKK'nin 7 nci maddesinin üçüncü fıkrası ile 22 nci maddesinin birinci fıkrasının (e) bendine dayanarak hazırlanan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" ile de kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesine dair veri sorumlularının karar verme yetkisi kapsamında usul ve esasların belirli hale getirilmesi amaçlanmıştır. Anılan Yönetmeliğin 4 üncü maddesinde, her üç durum için de müşterek olarak "*imha*" kavramı kullanılmaktadır.

Kişisel verilerin silinmesi, bu verilerin ilgili kullanıcılar tarafından erişilemez ve bir daha kullanılamaz duruma getirilmesi olarak; yok edilmesi, silinmeye ek olarak bu verilerin geri getirilemez hale getirilmesi işlemi olarak; anonimleştirilmesi ise başka bir veri ile eşleştirilse dâhi verilerin hiçbir suretle kimliği belirlenebilir gerçek bir kişiyle ilişkilendirilemeyecek duruma getirilmesi işlemi olarak tanımlanabilmektedir. Bu

---

[51] Kişisel Verileri Koruma Kurumu, *Özel Nitelikli Kişisel verilerin İşlenmesine İlişkin Rehber*, (2025): 26-27.

[52] Kişisel Verileri Koruma Kurulu Kararı, 25.03.2019 günlü, 2019/81 sayılı karar; Kişisel Verileri Koruma Kurulu Kararı, 31.05.2019 günlü, 2019/165 sayılı karar.

[53] Ömer Fatih, Sayan, *Karşılaştırmalı Hukukta Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması ve Veri Güvenliği*, (Doktora Tezi, Ankara Yıldırım Beyazıt Üniversitesi, 2023).

kapsamda veri sorumlusu, bahse konu üç durumda da gerekli her türlü tedbiri almakla yükümlü kılınmıştır[54].

Diğer taraftan anonimleştirilmiş veri, kişisel veri olarak kabul edilmemekte ve dolayısıyla işlenmesi durumunda mevzuatta yer alan yükümlülüklerin yerine getirilmesinden muaf tutulmaktadır[55]. Örneğin, 50 ila 60 yaş arasındaki tüketicilerin çevrim içi alışveriş alışkanlıklarına dair veri, gerçek kişiler ile bir bağlantısı bulunmadığından ve kişilerin kimliklerini belirleyebilecek nitelikte bir bilgi olmadığından anonim veri olarak kabul edilmekte ve Kanun'un kapsamı dışında kalmaktadır[56]. Ancak bu verilerin, teknolojinin yardımıyla gerçek bir kişiye kadar izlenebildiği durumlarda kişisel veri olarak değerlendirilmesi ve dolayısıyla korunması gerekecektir[57].

1.3.6 Açık rıza ve unsurları

Türk hukukunda kişisel veriler anayasal düzeyde bir korumaya sahiptir. T.C. Anayasası'nın 20 nci maddesinde kişisel verilerin yalnızca kanunda öngörülen hâllerde ya da bireyin açık rızasıyla işlenebileceği hükme bağlanmıştır. Rıza, ilgili kişinin kendisine ilişkin olan veriler hakkında denetimini sağlamada önemli bir araç olup *"bilgilerin geleceğini belirleme"* fikrinin bir yansımasıdır[58].

---

[54] Çiğdem, Ayözger Öngün, *Kişisel Verilerin Korunması Hukuku (Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil,* İkinci Baskı, (Beta Basım Yayım Dağıtım: 2019): 196-197.

[55] Anonim veri ile anonimleştirilmiş veri aynı anlama gelmemekte olup anonim veri ilk andan itibaren belirli bir kişiyle ilişkilendirilmesi mümkün olmayan veriyi ifade etmektedir. Anonimleştirilmiş veri ise önceden bir kişiyle ilişkilendirilmiş olmakla birlikte bağlantısı sona ermiş veridir. https://www.linkedin.com/posts/kvkkurumu_kvkk-activity-7245311200354324480-q45W?utm_source=share&utm_medium=member_desktop (Erişim Tarihi: 04.11.2024)

[56] Ersoy Kekevi, *Genel Kavramlar, Kişisel…,* 108.

[57] Gintare, Surblyte, *Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy*, (2016).

[58] Elif, Küzeci, *Kişisel Verilerin Korunması*, 4. Baskı, (İstanbul: On İki Levha Yayıncılık, 2020): 264

Açık rıza, KVKK'de genel nitelikli ve hassas verilerin işlenmesinde temel bir hukuka uygunluk nedeni olarak düzenlenmiştir. Bu düzenleme TMK'nin 24 üncü maddesinin ikinci fıkrasında yer alan*; "Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır."* hükmü ile benzer nitelikte bir düzenlemedir. Buna göre rızanın geçerli olabilmesi, rızanın hukuka ve ahlaka uygun olmasının varlığına bağlıdır. Aksi takdirde rıza, 6098 sayılı Türk Borçlar Kanunu (TBK)'nun *"Sözleşmenin özgürlüğü"* başlıklı 26 ncı maddesi ve *"Kesin hükümsüzlük"* başlıklı 27 nci maddesi kapsamında geçersiz olmaktadır. Diğer taraftan TMK'nin 15 inci maddesi gereğince kanunda belirtilen istisnai hâllerin saklı kalması kaydıyla, ayırt etme gücü bulunmayan bir kimsenin fiillerinin hukuki sonuç doğurmayacağı, yani rızayı veren kişinin rızasının geçerli olmayacağı hükme bağlanmıştır[59].

GDPR'ın *"Tanımlar"* başlıklı 4 üncü maddesinin on birinci fıkrasında rıza, veri sahibi tarafından, bir beyan veya açık bir onay eylemiyle kendisi ile ilgili olan kişisel verilerin işlenmesinin kabul edildiğini belirttiği, özgür bir biçimde, bilinçli, spesifik ve açıkça ifade edilmiş istekler olarak tanımlanmaktadır. KVKK'nin *"Tanımlar"* başlıklı 3 üncü maddesinin birinci fıkrasının (a) bendinde ise GDPR'dan farklı bir şekilde rızanın değil, doğrudan açık rızanın tanımına yer verilmiştir. Buna göre açık rıza, belirli bir konuya ilişkin, bilgilendirilmeye dayalı ve özgür irade ile açıklanan rızadır.

Kişisel verilerin işlenmesinde açık rızanın mutlaka aranması gerekip gerekmediği konusunda farklı görüşler mevcuttur. Bunlardan birincisi, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesine imkân veren bir veri işleme şartının mevcut olup olmadığının tespitini gerekli gören görüştür. Buna göre böyle bir şart oluşmamışsa ilgili kişinin açık rızasına başvurulmalıdır[60]. Çünkü, diğer işleme

---

[59] Cemil, Kaya, *Kişisel Verilerin Korunması Hukuku ve Bilgi Edinme Hukuku: Çeşitli Açılardan Bakış*, (İstanbul: On İki Levha Yayıncılık, 2023): 153

[60] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, 5.

koşullarının mevcut olduğu durumlarda da ilgili kişinin rızasının aranması, rızanın geri alınması durumunda veri işleme sürecinin sona ereceği yönünde yanıltıcı bir algı oluşturabilir[61]. Diğer bir görüş ise açık rızanın ve diğer istisnalardan birisinin bir diğerinden üstün ve öncelikli olmadığı yönündedir. AYM 28.09.2017 tarihli ve E.2016/125, K.2017/143 sayılı kararında[62], bu görüşle benzer biçimde; açık rızanın yerine getirilmiş olan istisnaların, esas düzenleme haline gelmesinden ya da açık rızaya gerek duyulmasının imkânsız hale gelmesinden bahsedilemeyeceğini belirtmiştir[63]. Ayrıca KVKK'de belirtilen istisnai durumlarda dahi, veri sorumlusunun işleme faaliyeti çerçevesinde ilgili kişiyi bilgilendirme yükümlülüğünün ortadan kalkmayacağı ifade edilmektedir[64].

Diğer yandan açık rızanın, kişiye sıkı sıkıya bağlı haklardan olması sebebiyle geri alınabilmesi her zaman mümkündür. Buna göre, kişi dilediği zaman zarfında veri sorumlusuna verdiği açık rızasını geri alma hakkına sahiptir. Geri alma işlemi ise ileriye yönelik sonuç doğurmakta olduğundan, geri alma beyanı veri sorumlusuna ulaştığı andan itibaren hüküm doğurur[65].

Açık rızanın hangi tarihte verilmesi halinde geçerli olacağı hususunda ise KVKK'de bir düzenleme bulunmamaktadır. Bununla birlikte, 13 Temmuz 2011 tarihinde VKÇG tarafından kabul edilen "15/2011 Sayılı Görüş: Rızanın Tanımı" raporunda, rızanın kişisel verilerin işlenmesine başlanılmadan önce alınması gerektiği belirtilmektedir[66].

---

[61] Kaya, *Kişisel Verilerin Korunması Hukuku ve…,* 153.

[62] Anayasa Mahkemesi 2016/125 Esas, 2017/143 Karar ve 28.09.2017 tarihli Kararı *"… Dava konusu kurallarla ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesinin mümkün olmadığı bir kısım haller düzenlenmek suretiyle kişisel verilerin korunması hakkına müdahalede bulunulmuş ise de açık rıza olmaksızın işlenebilecek kişisel veriler, ilgilinin her türlü kişisel verisi olmayıp dava konusu kurallarda açıkça düzenlenen şartlardan birinin gerçekleşmesi durumu ile sınırlıdır. Bu bağlamda açık rıza kavramına getirilen istisnaların esas düzenleme haline getirildiği veya açık rızaya gerek duyulmasını imkânsız hale getirdiği söylenemez. (…)"*

[63] Anı, *Kişisel Verilerin İşlenmesi ve…,* 102.

[64] Mahmut Furkan, Balaban, *Elektronik Haberleşme Sektöründe İşlenen Kişisel Verilerin Korunması*, (Ankara: Adalet Yayınevi, 2023): 89.

[65] Kişisel Verileri Koruma Kurumu, "Açık Rıza Alırken Dikkat Edilecek Hususlar".

[66] Avrupa Komisyonu, *Article 29 Data Protection Working Party, Opinion 15/2011*, (2011): 9.

Öte yandan, açık rızanın şekline ilişkin olarak gerek KVKK'de gerekse GDPR'da bir düzenlemenin bulunmaması sebebiyle açık rızanın sözlü veya yazılı olarak alınabileceği kabul edilmektedir. Keza duruma göre, veri sahibi bir davranışıyla dâhi açık rıza vermiş olabilir[67]. Fakat bu durum, yalnızca susmaya anlam ve sonuç yüklememektedir. Somut durumda, açık rızanın varlığının kabulü için iradenin ortaya konulması, yani ilgili kişinin beyanı veya aktif bir davranışının bulunması gerekir[68]. Bununla birlikte ileride ortaya çıkabilmesi muhtemel uyuşmazlıklarda delil olması açısından ilgili kişinin beyanın yazılı olmasının ya da elektronik bir ortamda kayıt altına alınmasının, veri sorumlusunun yararına olacağı belirtilmektedir. Keza, rıza talebinin ve rızanın alınmasının hukuka uygun şekilde olduğuna yönelik ispat yükü veri sorumlusundadır[69].

Açık rızanın geçerli olabilmesi için rızanın, belirli bir konuya ilişkin olma, bilgilendirmeye dayanma ve özgür iradeyle açıklanmış olma unsurlarını kümülatif olarak taşıması gerekmektedir.

Buna göre rızanın geçerliliği için aranan unsurlardan birincisi, rızanın; belirli bir konuya ilişkin olması ve bu konuyla sınırlı verilmesidir. Zira rızanın hem açık ifadelerle verilmesi hem de belirli bir veri işleme amacına özgü olması esastır[70]. İlgili kişiden açık rızaya ilişkin beyanın hangi husus için istendiğinin veri sorumlusunca açıkça ortaya konulması gerekmektedir[71]. Söz konusu unsura, GDPR'ın 4 üncü maddesinin on birinci fıkrasında ve GDPR'ın "*Başlangıç*" bölümünün 32 nci maddesinde geçen *"specific"*

---

[67] Örneğin, "bu odaya girildiği takdirde kişisel veriler işlenecektir" biçiminde bir uyarının olmasına rağmen odaya girilmesi halinde, diğer koşulların da sağlanması durumunda açık rıza verilmiş sayılabilecektir.

[68] Sezen, Özbaşı, *Kişisel Sağlık Verilerinin İşlenmesinde Açık Rıza Kavramı*, (Yüksek Lisans Tezi, Hacettepe Üniversitesi, 2024): 101.

[69] Ömer Faruk, Kuntoğlu, "Elektronik Ticarette Kişisel Verilerin Korunması", *Bilişim Hukuku Dergisi*, (2021): 189.

[70] Avrupa Birliği Temel Haklar Ajansı ve Avrupa Konseyi, *Handbook on European Data Protection Law*, çev. İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, (2018).

[71] Kişisel Verileri Koruma Kurumu, *Açık Rıza*, 4; Bilgi Komiserliği Ofisi (ICO), "What is valid consent?"; Murat Volkan, Dülger, *Kişisel Verilerin Korunması Hukuku*, (Hukuk Akademisi Yayınları, 2020): 224.

ifadesiyle, KVKK'nin ise 3 üncü maddesinin birinci fıkrasının (a) bendinde geçen *"belirli bir konuya ilişkin"* ibaresiyle işaret edilmiştir.

Verilecek olan bu rıza beyanının, belirli bir duruma yönelik olması ve bu durum için kişisel veri işlemeye konu olan somut olayın açıkça tanımlanması gereklidir[72]. Sınırsız bir şekilde, tüm kişisel verilerin işlenmesine yönelik rıza gösterilmesi durumunda, anılan rızalar "battaniye rıza"[73] olarak ifade edilmekte ve geçerli olarak kabul edilmemektedir[74].

Rızanın geçerli olması için aranan unsurlardan ikincisi, bilgilendirmeye dayalı olmasıdır. Rızanın bireyler tarafından özgür bir biçimde verilebilmesi için hangi konu hakkında rıza gösterildiği ve bu rızanın sonuçlarının bilinmesi gerekir[75]. Bilgilendirilmiş rıza olarak da adlandırılan bu unsur, veri sahibinin bir eylemin gerçeklerini ve sonuçlarını takdir edip anlamasına dayanan rızası anlamına gelir. Buna göre veri sahibi; işlenen verilerinin niteliği, işlenme amaçları, olası aktarımlarda alıcıları ve diğer hakları gibi ilgili bütün hususlarda açık ve anlaşılır şekilde doğru ve eksiksiz bilgi sahibi olmalıdır. Bu bilgi, söz konusu işleme faaliyetine rıza göstermemenin sonuçlarının farkında olunmasını da içermektedir[76].

Söz konusu unsura KVKK'nin *"Veri sorumlusunun aydınlatma yükümlülüğü"* başlıklı 10 uncu maddesinde yer verilmiştir. Buna göre kişisel verilerin edinimi esnasında, veri sorumlusunca ya da onun yetkilendirmiş olduğu kişice ilgili kişiye yapılacak bilgilendirmede, veri sorumlusu ve varsa temsilcisinin kimlik bilgisi, kişisel verinin hangi amaç için işlenebileceği, işlenen bu kişisel verilerin kimlere, ne amaç için

---

[72] Anı, *Kişisel Verilerin İşlenmesi ve…,* 131.
[73] Kişisel Verileri Koruma Kurumu, "Açık Rıza Alırken Dikkat Edilecek Hususlar".
[74] Ozan, Selek, "Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 21, Sayı: 2, (2019): 927.
[75] Erdinç, "Ölçülülük İlkesi ve Açık…": 14.
[76] Avrupa Komisyonu, *Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR),* (2007): 9.

aktarılabileceği, kişisel verilerin toplanma yöntemi ve hukuki olarak sebebi ile ilgili kişinin 11 inci maddede bahsedilen hakları yer almaktadır[77].

Rızanın geçerli olması için aranan unsurlardan üçüncüsü, rızanın özgür iradeyle verilmiş olmasıdır. Söz konusu unsura, GDPR'ın 4 üncü maddesinin on birinci fıkrasındaki "özgürce verilen *(freely given)*" ifadesiyle, KVKK'nin ise 3 üncü maddesinin birinci fıkrasının (a) bendindeki "özgür iradeyle açıklanan" ibaresiyle yer verilmektedir.

Avrupa Veri Koruma Kurulu (*European Data Protection Board*, EDPB)'na göre, veri sahibi gerçek bir seçim ve kontrole sahipse rızanın özgürce verildiği kabul edilir. Rızanın, hizmet koşullarının müzakere edilemez nitelikte bir parçası olduğu durumda ise özgürce verilmediği düşünülmektedir. Aynı durum, rızanın reddedilmesi veya geri alınmasının veri sahibi için olumsuz sonuçlara yol açması durumunda da geçerlidir. EDPB yönergelerine göre özgürce verilen bir rıza, veri sahibiyle veri sorumlusu arasında bir güç dengesizliği içermemelidir. Ayrıca rıza, koşulsuz, ayrıntılı ve veri sahibine zarar vermeyecek nitelikte olmalıdır[78].

KVK Kurulu'nun 10.06.2025 tarihli ve 2025/1072 sayılı kararında da açık rızanın "neye" gösterildiği ile yalnızca konu özelinde değil, beraberinde rızanın neticesi hakkında da tam anlamıyla bilgili olunması gerektiği belirtilmiştir. Ayrıca rızanın hata, tehdit, cebir gibi rıza beyanını sakatlayıcı her türlü durumdan da sıyrılmış olmasının arandığı özellikle vurgulanmıştır[79]. Mezkûr kararda zikredilen diğer önemli husus ise; açık rıza alınmasının bir ürün ya da hizmetin sunulması veya ürün ya da hizmetten

---

[77] Serdar, Çelikel, *"Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif Ve GDPR'la Karşılaştırmalı Olarak İncelenmesi"*, Haziran 2021, Uyuşmazlık Mahkemesi Dergisi – Yıl: 9, Sayı: 17, s. 161-190, s. 182

[78] Daniela, Alaattinoğlu, "Rethinking Explicit Consent and Intimate Data: The Case of Menstruapps". *Fem Leg Stud*, Cilt: 30, (2022): 163

[79] Kişisel Verileri Koruma Kurulu Kararı, 10.06.2025 günlü, 2025/1072 sayılı ilke kararı.

faydalandırmanın ön koşulu olarak ileri sürülmesi halinde özgür irade unsurunun zarar gördüğünden bahisle artık geçerli bir açık rızadan söz edilemeyeceğidir.

Diğer taraftan belirli bir konuya ilişkin bireyin açık rızası alındıktan ve bu verinin kullanımının akabinde bir üçüncü tarafla paylaşılabilmesi, yurt dışına aktarılabilmesi gibi durumlar için bireyin açık rızasına tekrar başvurulması gerekmektedir[80].

1.4 Kişisel Verilerin Korunması Hakkının Tarihsel Gelişimi

İnsanlık tarihinin hemen hemen her döneminde, değişen şartlarda ve farklı boyutlarda, dinî, ahlaki ve geleneksel normlar çerçevesinde kişisel mahremiyetin korunmasına yönelik inanç ve kurallar oluşturulmuştur. Yani, insana dair bazı bilgilerin başkaları tarafından bilinmemesi gerektiğine dair güçlü bir anlayış her zaman var olmuştur[81]. Öte yandan, gizlilik ve güvenlik ihtiyacını ortaya koyan bazı özel uygulamalar bilhassa bilginin hızlı ve kitlesel bir biçimde yayılmasına yönelik araçların ortaya çıkmasıyla birlikte gelişmiştir. Örneğin, mektupların[82] mühürlenmesi veya devletler arası iletişimin şifrelenmesi gibi uygulamalar, bu ihtiyacın tarihsel izlerini göstermektedir. Dahası, kişisel verilerin güçlü bir hukuki koruma kalkanına alınması günümüzde artık hâkim bir yaklaşımdır.

Bu bakımdan tarihsel süreçte veri koruma düzenlemeleri, teknoloji ve toplumsal yapıdaki dönüşümlerden büyük ölçüde etkilenen dinamik bir alan olarak öne çıkmaktadır. Bu konuya ilişkin ilk düzenlemelerde, bireylerin gizliliğinin korunmasından çok, verilerin işlenmesinin toplumsal boyutu ön plandayken, son dönemde bilgi teknolojilerinin gelişimiyle bireylerin korunmasına yönelik ihtiyaç

---

[80] Göksu Hazar, Erdinç, "Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi", *Kişisel Verileri Koruma Dergisi*, Cilt: 2, Sayı: 1, (Haziran 2020): 14.

[81] Berrak, Yılmaz, *Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, (Doktora Tezi, Hacettepe Üniversitesi, 2019): 119.

[82] PHK'de "mektup" kavramına yer verilmemiş, bunun yerine mektubu da kapsayacak şekilde "haberleşme gönderisi" kavramı kullanılmıştır. İşbu tez kapsamında da "mektup" ve "haberleşme gönderisi" kavramları birbirinin yerine kullanılacaktır.

artmıştır. Bu değişimi daha iyi anlamak için, kişisel verilerin korunması konusundaki düzenlemeleri Avrupa temelinde dört döneme ayırmak mümkündür[83].

İlk dönem, 1970-1980 yılları arasında ulusal düzeyde veri koruma düzenlemelerinin uygulamaya konulduğu süreci kapsamaktadır. Bu dönemde, veri işlemenin insan eliyle gerçekleştirilmesinin geride bırakılarak bilgisayarlar aracılığıyla yapılması, kişisel verilerin toplanmasını ve depolanmasını kolaylaştırmıştır. Ancak bu geçiş, II. Dünya Savaşı sırasında verilerin kötü amaçlarla kullanılabileceği tecrübesini yaşamış Avrupa vatandaşları arasında endişelere yol açmıştır. Bu kaygılar neticesinde, 1970'li yıllarda kişisel verilerin güvenliğini sağlamaya yönelik ilk ulusal hukuki metinler kabul edilmeye başlanmıştır[84]. İkinci dönemin başlangıcı, 1980'lerin başında OECD ile Avrupa Konseyi (AK) tarafından hazırlanan uluslararası metinlerle işaret edilmektedir. Üçüncü dönem ise 1982-1994 yılları arasında, bu uluslararası metinlerde belirtilen yükümlülüklerin yerine getirilmesi amacıyla AB üyesi ülkelerin ilk kez ulusal düzeyde veri koruma yasalarını kabul ettiği süreçtir. Ancak, ülkelerin anayasal normları, benimsenen politikalar ve sosyal yapılarındaki farklılıklar nedeniyle mevzuatta bir uyum sağlanamamış ve bu durum AB açısından çeşitli sorunlara yol açmıştır. Son olarak, 1995-2016 yılları arasında, üye ülkelerin mevzuatının uyumlaştırılması çalışmaları sonucunda, bireylere tanınan haklar, veri işleyen bireylere yüklenen sorumluluklar, verilerin işlenmesi koşulları ve bireylerin korunma yöntemleri gibi konularda detaylı düzenlemeler getirilmiştir[85].

Bu açıklamalar ışığında kişisel verilerin korunmasının öneminin, insan hakları ve bunların korunması bilincinin son elli sene içerisinde artmasıyla birlikte daha da belirgin hâle geldiği görülmektedir. Özetle kişisel verilerin korunmasına dair temel düzenlemeler, ilk kez bilişim teknolojilerinin gelişimi ve yaygınlaşması ile 1960'larda

---

[83] Brendan, Van Alsenoy, *Regulating Data Protection: The Allocation of Responsibility and Risk Among Actors Involved in Personal Data Processing*, (Doktora Tezi, KU Leuven, 2016): 103.
[84] Dilek, Yüksel Civelek, *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*, (Uzmanlık Tezi, Devlet Planlama Teşkilatı Müsteşarlığı, 2011): 9.
[85] Van Alsenoy, *Regulating Data Protection: The….*

ele alınmaya başlanmış, 1970'li yıllarda ise hukuki düzenlemelerin konusu hâline gelmiştir[86].

Kişisel verilerin korunmasına dair ilk spesifik yasal düzenleme, 30.09.1970'te Almanya'nın Hessen Eyaleti tarafından yürürlüğe konulmuş olan anılan eyalet ile sınırlı tatbik edilen Veri Koruma Kanunu'dur. Ülke bazında uygulanan ilk kapsamlı kanun ise, 1973 yılında İsveç tarafından çıkarılan Veri Kanunu'dur. Bunu, 1978 yılında yürürlüğe giren Fransa ve Almanya Veri Koruma Kanunları izlemiştir. Bu düzenlemeler, kişisel verilerin işlenmesinden kaynaklanabilecek olası risklere karşı hukuki güvence sağlamayı amaçlamaktadır. 1974 yılında kabul edilen Amerika Birleşik Devletleri (ABD) Gizlilik Kanunu, devlet kurumlarının bireylere ait kişisel verileri nasıl toplayıp işleyeceğine ilişkin kapsamlı kurallar getirmiştir[87]. Uluslararası düzeyde ise AK tarafından elektronik veri bankalarında tutulan kişisel verilerin korunması için gerekli standartları belirlemek amacıyla alınan 1973 ve 1974 tarihli kararlar önemli bir adım teşkil etmiştir. Bu kararlar, kişisel veri koruma alanında sonraki düzenlemeler için temel oluşturmuş ve referans kabul edilmiştir[88].

1.5 Uluslararası Hukukta Yer Alan Düzenlemeler

Çalışmanın bu bölümünde kişisel verilerin işlenmesi ve gizliliğin korunmasına yönelik olarak OECD, BM, AK ve AB gibi uluslararası kuruluşlarca alınan bazı kararlar ile yapılan düzenlemelere yer verilecektir.

---

[86] Dülger, "Kişisel Verilerin Korunması Kanunu ve…": 102.

[87] Sayan, *Karşılaştırmalı Hukukta Elektronik…,* 127-128; Amerika Birleşik Devletleri (ABD) Posta Hizmetleri, *Gizlilik Politikası*.

[88] OECD Legal Instruments, "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", (2013).

1.5.1 Ekonomik Kalkınma ve İşbirliği Örgütü

OECD, kurucu ülke sıfatıyla Türkiye'nin de aralarında bulunduğu toplam 38 üye ülkenin katılımıyla oluşan uluslararası bir ekonomi kuruluşudur[89]. OECD, 23.09.1980'de "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler (OECD Rehber İlkeleri)"i yayımlamıştır. Hukuki bağlayıcılığı olmayan, tavsiye niteliğindeki bu Rehber, kişisel verilerin otomatik işlenmesi için belirlenen temel ilkelerden oluşmaktadır. Veri koruma alanında ilk uluslararası düzenleme olması nedeniyle OECD'nin bu rehber ilkeleri büyük bir öneme sahiptir[90]. OECD Rehber İlkeleri, sekiz temel ilkeden oluşmaktadır. Bu ilkeler *"veri toplamanın sınırlı olması ilkesi, veri niteliği ilkesi, amacın belirli olması gerektiği ilkesi, kullanımın sınırlanması ilkesi, veri güvenliği ilkesi, açıklık ilkesi, bireyin katılımı ilkesi, hesap verme zorunluluğu ilkesi"* şeklindedir[91].

OECD üye ülkelerinin, bu ilkeleri kendi iç hukuklarına dahil etme konusunda serbest olduğu kabul edilmekle birlikte, ülkemiz özelinde, KVKK'nin 4 üncü maddesinde yer alan ve kişisel verilerin işlenmesinde dikkate alınması gereken temel ilkeler ile OECD Rehber İlkelerinin önemli ölçüde benzer olduğu görülmektedir[92].

1.5.2 Birleşmiş Milletler

Birleşmiş Milletler (BM), ülkeler arasındaki ekonomik iş birliğini teşvik etmek amacıyla 1945 yılında kurulmuş ve kuruluş anlaşması 50 ülke tarafından imzalanmıştır[93].

---

[89] OECD, "Members and Partners".
[90] OECD Legal Instruments, "Recommendation of the Council concerning…".
[91] Mehmet Bedii, Kaya, *"Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verilebilirlik İlkesi"*, İstanbul Hukuk Mecmuası Cilt: 78, Sayı: 4 (2021): 1859-97, s. 1866.
[92] Özbaşı, *Kişisel Sağlık Verilerinin İşlenmesinde…,* 34.
[93] Yasime, Hoşnut, "Uluslararası Düzenlemelerde ve Türkiye'de Kişisel Verilerin Korunması", *Yeni Medya Hakemlik, Akademi E- Dergi*, Sayı: 6, (2019): 37.

BM bünyesinde 1948 senesinde çıkarılan İnsan Hakları Evrensel Beyannamesi (İHEB), bireylerin mahremiyet hakkını koruma amacını taşımaktadır. Örneğin; Beyanname'nin 12 nci maddesi, herkesin özel yaşamına, ailesine, hanesine ve iletişimine saygı duyulmasını isteme hakkına sahip olduğunu belirtmektedir. Yine aynı maddede, özel hayatın, ailenin, meskenin ve haberleşmenin korunmasını vurgulamakta ve keyfi müdahalelere karşı koruma sağlama hakkını tanımaktadır. Bu madde, özel hayata yönelik saldırılara karşı yasal koruma sağlayan ilk uluslararası metin olma özelliği taşırken, kişisel verilerin korunmasına ilişkin gelecekteki çalışmalar için de temel oluşturmaktadır. Ancak, İHEB tavsiye niteliğinde bir beyanname olup bağlayıcı bir hukuki gücü bulunmamaktadır [94].

Diğer yandan 1966 yılında kabul edilen ve ülkemizde 1976 yılında yürürlüğe giren Kişisel ve Siyasi Haklar Sözleşmesi, bireylerin özel yaşamına müdahale edilmeyeceği ilkesini vurgulamaktadır. Bu Sözleşmenin 17 nci maddesinde, kimsenin keyfi olarak özel hayatına, ailesine veya konutuna müdahale edilemeyeceği ve herkesin kişisel verilerinin korunması hakkına sahip olduğu açıkça düzenlenmektedir[95].

1985 yılında BM, kişisel verilerin korunmasına yönelik bir yönerge yayımlamış ve 14 Aralık 1990'da "Kişisel Veri Dosyalarının Bilgisayar Aracılığıyla İşlenmesine Dair Genel İlkeler" kabul edilmiştir. Bu ilkeler, üye devletlerin belirli bir standartta buluşmasını hedefleyen maddelerden oluşmaktadır[96]. Ancak, İHEB gibi BM Rehber İlkeleri de bağlayıcı nitelik taşımamaktadır[97].

BM, veri koruma konusundaki temel ilkeleri belirleyerek, devletlerin bu ilkelere uygun olarak hareket etmesini teşvik etmektedir. Bu ilkeler, kişisel verilerin işlenmesinde

---

[94] Hayrunnisa, Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, (Ankara: Seçkin Yayıncılık, 2009): 21.
[95] Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi, 1976.
[96] Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği, "*Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler"*, (1990).
[97] Lee A., Bygrave, "Privacy Protection in a Global Context-A Comparative Overview", *Scandinavian Studies in Law,* Cilt: 47, (2004): 319-348.

şeffaflık, güvenlik ve bireylerin haklarına saygılı olma hususlarını içermektedir. Bu bağlamda, BM düzenlemeleri, kişisel verilerin gizliliği ve korunması konusunda uluslararası standartların belirlenmesine katkıda bulunmuş ve bireylerin mahremiyet haklarını güvence altına almayı hedeflemiştir[98].

1.5.3 Avrupa Konseyi

AK; hukukun, demokrasinin ve insan haklarının geliştirilmesi amacıyla Avrupa'da iş birliğinin artırılmasını hedefleyen en eski uluslararası organizasyonlardan birisi olarak, Londra Anlaşması ile kurulmuştur. Konseyin ana hedefi, Avrupa'da ortak bir yasal düzenin ile demokratik ortamın oluşturulmasıdır. Bu kapsamda hedeflerini Avrupa İnsan Hakları Sözleşmesi (AİHS) ile benzer nitelikteki insan hakları metinleri ile gerçekleştirme gayesindedir[99].

AK bünyesinde, kişisel verilerin korunmasına dair hükümler içeren birden çok uluslararası metin olup bunlardan AİHS, AK'nin Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin korunmasına ilişkin 108 Sayılı Avrupa Konseyi Sözleşmesi (108 sayılı Sözleşme) ve 181 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol (181 sayılı Ek Protokol) en önemlileridir.

---

[98] Anı, *Kişisel Verilerin İşlenmesi ve…,* 48-49.
[99] Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, *Avrupa Konseyine Genel Bir Bakış*.

1.5.3.1 Avrupa İnsan Hakları Sözleşmesi

AİHS, 04.11.1950'de kabul edilmiş, 03.09.1953'te ise yürürlüğe girmiştir. Bu Sözleşme, insan haklarının korunması açısından oldukça etkili ve işlevsel bir sözleşme olarak kabul edilmekte olup güçlü bir denetim mekanizmasına sahiptir[100].

Sözleşmedeki hükümlerin kapsamı ve sınırları ise Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatları ile belirlenmiştir. Bu bağlamda, kişisel verilerin korunması konusu Sözleşme'de bağımsız bir hak olarak yer bulmamakla birlikte, AİHS'in 8 inci maddesinde düzenlenen "Özel ve Aile Hayatına Saygı" başlığı altında ele alınmaktadır. Bu madde, bireylerin özel hayatlarını ve aile ilişkilerini koruma altına alırken, kişisel verilerin işlenmesi ve korunması konularına da önemli bir zemin oluşturmaktadır. AİHM'in kararları, bu maddenin yorumlanması ve uygulanmasında belirleyici bir rol oynamakta; dolayısıyla, kişisel verilerin korunması, özel hayatın gizliliği ile doğrudan bağlantılı bir hak olarak karşımıza çıkmaktadır. Bu durum, bireylerin haklarının güvence altına alınması açısından önemli bir adım teşkil etmekte ve insan hakları bağlamında çağdaş tartışmalara zemin hazırlamaktadır[101].

AİHM içtihatlarında 8 inci maddeye dayanarak, ilk olarak ilgili olayın özel veya aile hayatı, konut ve haberleşmenin gizliliği gibi haklar kapsamında değerlendirip değerlendirilemeyeceği üzerine bir inceleme yapılmaktadır. Şayet olayın, gizlilik hakkı kapsamına girdiği kabul edilirse, akabinde müdahalenin var olup olmadığına bir değerlendirme gerçekleştirilmektedir. Müdahalenin varlığı tespit edilirse, bu durumda müdahalenin meşruiyeti, yani hukuka uygunluğu sorgulanmaya başlanmaktadır. Hukuka uygun bir müdahale gerçekleştirebilmek için temel kriterler arasında; müdahalenin yasalarla öngörülmüş olması, meşru bir müdahale amacının

---

[100] Zehra, Gayretli, *Avrupa İnsan Hakları Mahkemesi (AİHM) ve Anayasa Mahkemesi (AYM) Tedbir Kararlarının Karşılaştırmalı Olarak Değerlendirilmesi*, (Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2020): 13-15.

[101] Ekin, *Kişisel Verilerin Korunması ve…*, 34.

bulunması ve demokratik toplum düzeninin bu müdahaleyi gerekli kılması yer almaktadır. Bu ölçütler, müdahalelerin kabul edilebilirliğini belirleyen temel unsurları oluşturmaktadır[102].

1.5.3.2 Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 sayılı Avrupa Konseyi Sözleşmesi

"108 sayılı Sözleşme" olarak da bilinen uluslararası belge, 01.10.1985'te yürürlüğe girmiştir. Türkiye, sözleşmeyi imzalayan ilk ülkelerden biri olmakla birlikte, Türk hukuk sistemine 17.03.2016 tarihli ve 29656 sayılı Resmî Gazete'de yayımlanarak dâhil edilmiştir[103].

Anılan Sözleşme, kişisel verilerin korunmasıyla ilişkin olarak kabul edilen ilk bağlayıcı uluslararası sözleşme olma özelliğine sahiptir[104]. Sözleşme ile amaçlanan, üye ülkelerde yaşayan bireylerin kişisel verilerini, uyruğu veya kimliği ne olursa olsun güvence altına almaktır. Sözleşme, kişisel verilerin korunmasındaki asgari gereklilikleri belirleyerek, sözleşmeyi imzalayan devletlerin daha geniş koruyucu tedbirler alabilmesine olanak tanımaktadır. Sözleşmenin 5 inci maddesinde, kişisel verilerin adil ve yasal bir şekilde elde edilmesi, belirli ve meşru amaçlarla kaydedilmesi gibi temel ilkeler düzenlenmiştir. Bu maddeler doğrultusunda kişisel verilerin doğru ve güncel tutulması, kaydedilme amaçlarıyla sınırlı süreyle saklanması gerekmektedir[105].

Hassas verilerin korunması açısından ise söz konusu Sözleşme, daha sıkı tedbirler öngörmektedir. Nitekim Sözleşme'nin 6 ncı maddesinde, ırksal köken, politik görüş,

---

[102] Furkan Kaan, Yüksek, "AİHM İçtihatlarında Kişisel Verilerin Korunması", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 25, Sayı: 1, (Mayıs 2023): 388.
[103] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler*.
[104] Songül, Atak, "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", *TBB Dergisi*, Sayı 87, (2010): 91-92.
[105] Küzeci, *Kişisel Verilerin Korunması*, 146.

dini inanç gibi verilerin otomatik olarak işlenmesi yasaklanmıştır. Bununla birlikte, iç hukukun yeterli güvence sağlaması durumunda bu verilerin işlenmesine izin verilebileceği de belirtilerek söz konusu yasağın mutlak olmadığı ifade edilmiştir. Ayrıca, Sözleşme'nin 7 nci maddesi ile kişisel verilerin yetkisi olmayan kişiler tarafından imhasını veya yanlışlıkla kaybedilmesini, erişilmesini, değiştirilmesini veya açıklanmasını önlemek için gereken önlemlerin alınmasına ilişkin taraf devletlere yükümlülük getirilmiştir[106].

1.5.3.3 181 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol

AK tarafından 2001 yılında, 108 sayılı Sözleşme için 181 sayılı Ek Protokol imzaya açılmıştır. Bu Protokol, Türkiye tarafından 08.11.2001 tarihinde imzalanmış, ancak 05.05.2016 tarihli ve 29703 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir[107].

Bu ek protokolde ilk olarak, kişisel verilerin korunması amacıyla ulusal düzenlemeler yapılması ile bu kapsamda gerekli denetim ve kontrol mekanizmalarının sağlanması gerektiği vurgulanmaktadır. İkinci olarak, bu denetim ve kontrol işlevlerine yönelik ulusal düzenlemelerin, 108 sayılı Sözleşme hükümleriyle uyumlu olması gerekliliği belirtilmiştir. Bu sayede 108 sayılı Sözleşme'ye taraf devletler, kişisel verilerin korunması hakkının güvence altına alınmasını ve bu güvencenin bağımsız kurum ve kuruluşlar tarafından yerine getirilmesini sağlama konusunda ortak bir irade ortaya koymuşlardır[108].

---

[106] Atak, "Avrupa Konseyi'nin Kişisel Veriler Açısından…": 96.
[107] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Alanında Uluslararası….*
[108] Yurdanur, Ural Uslan ve Samed, Değirmenci, "Avrupa Birliği Genel Veri Koruma Tüzüğü Işığında Türkiye'de Kişisel Verileri Koruma Kurumu", *Optimum Ekonomi ve Yönetim Bilimleri Dergisi*, Cilt: 10, Sayı: 1, (Ocak 2023): 26.

Anılan Protokolün gelişen teknoloji ile bilgi ve iletişim teknolojilerinin artan kullanımı sonucunda modernize edilmesi ihtiyacı hâsıl olmuş ve bu kapsamda hazırlanan yeni metin 223 sayılı Protokol ile 18.05.2018 tarihinde kabul edilmiştir[109]. Bu değişiklikler neticesinde, koruma standartları yükseltilerek sözleşmenin kapsamı genişletilmiştir[110]. Türkiye ise anılan sözleşmeyi onaylayan ülkeler arasında henüz yer almamaktadır[111].

1.5.4 Avrupa Birliği Düzenlemeleri

1.5.4.1 Avrupa Birliği Temel Haklar Bildirgesi

Avrupa Birliği Temel Haklar Bildirgesi (ATHB), 2000 yılında, AB Kurumlarının insan haklarına saygı duyulmasını sağlamak ve temel hak ve özgürlükleri güvence altına alarak etkin bir biçimde koruma amacıyla, bir başka ifade ile AB'nin yetkilerinin, temel haklar lehine sınırlandırılması amacıyla kabul edilmiştir[112].

Bildirge, AB üyesi ülkelerin vatandaşlarına yönelik hakların korunmasını hedeflerken aynı zamanda bu hakların evrenselliğini ve uluslararası standartlara uyumunu teşvik etmektedir[113]. Diğer yandan, AB üye ülkeleri tarafından saygı gösterilmesi gerekli olan temel hakların belirlendiği söz konusu düzenlemede kişisel verilerin korunması hakkı, "özel ve aile hayatına saygı" başlıklı 7 nci maddesinden ayrı bir hak olarak tanınmıştır.

---

[109] Nuri, Aygün, *Elektronik Haberleşme Sektörüne İlişkin Avrupa Birliği e-Gizlilik Tüzüğü'nün Yenileme Çalışmaları Kapsamında İncelenmesi ve Ülkemiz İçin Öneriler*, (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2022): 28, (Yayımlanmamış Tez).

[110] Berna, Akçalı Gür, "Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, Cilt 25, Sayı 2, (Aralık 2019): 856.

[111] Bkz. Onaylayan ülke listesi (Avrupa Konseyi, "Chart of signatures and ratifications of Treaty 223", 2025).

[112] Metin, Yüksel, "Avrupa Birliği Temel Haklar Şartı", *Ankara Üniversitesi SBF Dergisi*, Cilt:57, Sayı: 4, (Nisan 2002): 46.

[113] Avrupa Komisyonu, "Charter of Fundamental Rights of the European Union (2000/C 364/01)", *Official Journal of the European Communities*, (2000).

Bu şekilde ayrı bir düzenleme ile kişisel verilerin korunması hakkının önemine vurgu yapılmıştır[114].

1.5.4.2 Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki 95/46/EC sayılı Avrupa Parlamentosu ve Konseyi'nin Direktifi

OECD Rehber İlkeleri ile 108 sayılı Sözleşme tarafından belirlenen çerçeveye rağmen, ulusal hukuk sistemlerindeki çeşitlilik ve istikrarsızlık, AB'yi kişisel verilerin korunmasına ilişkin bir Direktif hazırlamaya yönlendirmiş ve bu Direktif 1995 yılında yürürlüğe girmiştir[115]. 95/46/EC sayılı Direktif, AB üye ülkelerinin ulusal sınırları arasında kişisel verilerin güvenli ve serbest dolaşımını garanti altına almak için düzenleyici bir çerçeve sağlamanın yanı sıra, kişisel bilgilerin saklandığı, iletildiği veya işlendiği her yerde kişisel bilgiler etrafında bir güvenlik temeli oluşturmak amacını taşımaktadır[116].

Anılan Direktifte; verinin kaynağını öğrenme, hatalı verilerin düzeltilmesi, hukuka aykırı işlemlere karşı itiraz hakkı ile kişisel verilerin doğrudan pazarlama amaçlı dolaşımını engelleme ve hassas verilere ilişkin düzenlemeler öne çıkmaktadır[117]. Ayrıca AB sınırları içinde veya dışında gerçekleşse dahi, Birlik kökenli verilerin toplanması, işlenmesi ve paylaşılması süreçlerine önemli sınırlamalar getirmiştir[118].
AB mevzuatının bir parçası olan bu Direktife uyum zorunlu olup AB üyesi olmayan ülkelerin de AB üyesi ülkelerle veri aktarımı yapabilmek için eşdeğer koruma

---

[114] Dülger, *Kişisel Verilerin Korunması Hukuku*, 63.
[115] Ayözger Öngün, *Kişisel Verilerin Korunması Hukuku…,* 78.
[116] Caroline, Sheedy ve Maria, Moloney, *Leveraging the Postal Infrastructure for the Authentication of Individuals Towards an Online Government Service Provision*, (2013): 4.
[117] Çağrı Zeybek, Ünsal, *"Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri ile Uyumluluğu ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Açısından Değerlendirilmesi"*, *Hacettepe Hukuk Fakültesi Dergisi,* Cilt: 3, Sayı: 1, (Haziran 2013): 106.
[118] Ayözger Öngün, *Kişisel Verilerin Korunması Hukuku…,* 79.

sağlamaları gerekmektedir[119]. Diğer yandan 95/46/EC sayılı Direktif, 25.05.2018 tarihinde GDPR ile yürürlükten kaldırılmıştır.

1.5.4.3 Genel Veri Koruma Tüzüğü

95/46/EC sayılı Direktif, yaşanan teknolojik gelişmeler neticesinde bireylerin ihtiyaçlarına cevap verememeye ve yeknesaklığı da sağlayamamaya başlamıştır. Bu kapsamda 12.03.2014 tarihinde GDPR'a ilişkin taslak, Avrupa Parlamentosunca kabul edilmiştir. Taslağa ilişkin görüşlerin müzakereleri neticesinde de 27.04.2016 tarihinde GDPR kabul edilerek 04.05.2016 tarihinde AB Resmî Gazetesi'nde yayımlanmıştır. GDPR'ın yürürlük tarihi olarak ise 25.05.2018 tarihi belirlenmiş ve bu tarihte yürürlüğe girmiştir[120].

95/46/EC sayılı Direktif'ten farklı olarak GDPR, "Tüzük (*Regulation*)" olma özelliği ile üye ülkelerin ulusal mevzuatlarında ayrıca bir düzenleme yapılmasını gerektirmeden doğrudan uygulanabilir güçtedir. Bu güç sayesinde üye ülkelerde farklı uygulamaların önüne geçilerek ve farklı bir uyum yasalarının çıkarılmasına da gerek olmadan AB üyesi ülkelerde kişisel verilerin korunması alanında yeknesaklık sağlanmıştır[121].

GDPR, uygulanma alanı itibarıyla üye ülkelere nazaran daha geniş bir kapsama sahiptir. Keza işleme faaliyetinin nerede yapıldığına bakılmaksızın, üye ülkelerde yaşayan gerçek kişilerin verilerinin işlenmesi, GDPR'da belirlenen hükümlere uygun bir biçimde yapılmalıdır. AB ülkesi vatandaşlarının veya vatandaş olmasalar bile AB sınırları dahilindeki kişilerin verilerinin veyahut herhangi bir sebeple bu üye

---

[119] Ünsal, "Google'ın Yeni Gizlilik Politikası…": 106.
[120] Murat Volkan, Dülger, "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması", *Yaşar Hukuk Dergisi*, Cilt: 1, Sayı: 2, (2019): 84.
[121] Özbaşı, *Kişisel Sağlık Verilerinin İşlenmesinde…,* 39.

ülkelerden geçen kişisel verilerin, AB üyesi olmayan ülkeler ile temasının olması hâlinde de söz konusu ülkelerin GDPR ile uyumlu olması gerekmektedir[122].

GDPR, bireylerin kişisel verilerinin korunmasını sağlamak amacıyla kapsamlı bir çerçeve sunmaktadır. Ayrıca GDPR, veri işleme süreçlerini şeffaf hale getirerek bireylerin haklarını korumayı, veri sorumlularının ve işleyicilerinin yükümlülüklerini netleştirmeyi hedeflemektedir. Bu Tüzük, veri koruma alanında uluslararası standartların belirlenmesine de katkıda bulunmaktadır. Ayrıca veri koruma otoritelerine denetim yetkileri vermekte ve veri koruma ihlâlleri için ciddi yaptırımlar öngörmektedir. Keza ihlal durumlarında kuruluşlara uygulanan yaptırımlar, kuruluşların yıllık cirolarının %4'üne veya 20 milyon Euro'ya kadar çıkabilmektedir[123].

1.5.5 Avrupa Veri Koruma Kurulu

EDPB, veri koruma alanındaki mevzuatın doğru şekilde uygulanmasını destekleyen ve AB'deki veri koruma otoriteleri arasında iş birliğini teşvik eden bağımsız tüzel kişiliğe sahip bir kuruluştur[124]. Kurul, üye devletlerin veri koruma otoritelerinin temsilcilerinden oluşmakta ve veri koruma düzenlemelerinin tutarlı bir şekilde uygulanmasını sağlamak için çalışmaktadır. Kurulun faaliyetleri arasında, veri koruma ile ilgili rehberlik ve tavsiyeler sunmak, uyum sağlamak için ortak stratejiler geliştirmek ve veri koruma yasalarının uygulanmasını izlemek yer almaktadır. Ayrıca EDPB, üyeler arasında iş birliği ve bilgi alışverişini teşvik ederek veri koruma standartlarının yükseltilmesine de katkıda bulunmaktadır[125].

EDPB, GDPR'ın 64, 65 ve 70 inci maddelerinde tanımlanan görevleriyle, üç ana faaliyet alanına ayrılmaktadır. Öncelikle, EDPB'nin temel sorumluluğu, GDPR'ın AB içinde

---

[122] Paul, Lambert, *Understanding the New European Data Protection Rules*, (CRC Press, 2018): 165-167; Dülger, *Kişisel Verilerin Korunması Hukuku*, 105.
[123] Ayözger Öngün, *Kişisel Verilerin Korunması Hukuku…,* 89.
[124] Avrupa Veri Koruma Kurulu (EDPB), "The European Data Protection Board".
[125] Sayan, *Karşılaştırmalı Hukukta Elektronik…,* 86-87.

tutarlı bir şekilde uygulanmasını sağlamaktır. Bu bağlamda, denetim otoriteleri arasında liderlik konusundaki ihtilaflar ve bir denetim otoritesinin tek otoriteye bağlı olduğu durumlar gibi yasal olarak bağlayıcı kararlar alabilmektedir. Ayrıca EDPB, Avrupa Komisyonunda, kişisel verilerin işlenmesine dair değişiklikler ve AB veri koruma kurallarıyla çelişen mevzuat değişiklikleri hakkında danışmanlık yapma görevlidir. Bu çerçevede, kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarımını düzenleyen yeterlilik kararları da dâhil olmak üzere, önemli bilgi sağlamaktadır[126].

[126] Avrupa Birliği Temel Haklar Ajansı ve Avrupa Konseyi, *Handbook on European Data….*

2 POSTA SEKTÖRÜNDE KİŞİSEL VERİLERİN GİZLİLİĞİ

Tezin bu bölümünde öncelikle posta hizmetlerine ilişkin temel kavramlar ortaya konularak anılan hizmetin genel mahiyeti, aşamaları ve çeşitleri hakkında genel bilgiler verilmektedir. Ardından posta hizmetlerinin sunumunda kişisel veri gizliliğinin önemi ve gelişimi ortaya konularak bu minvalde uluslararası düzenlemelerin yanı sıra ülkemiz ilgili mevzuatındaki hükümler incelenmektedir. 2.2 başlığı altında ise posta sektöründe kişisel verilerin korunması konusu detaylıca ele alınmaktadır. Posta sektöründe kişisel veri kavramı, KVKK çerçevesinde posta sektöründe kişisel verilerin işlenmesine ilişkin temel ilkeler, hukuka uygunluk sebepleri ve kişisel verilerin yurt dışına aktarımı gibi hususlara da bu başlık altında değinilmektedir. Son olarak, posta kullanıcılarının kişisel verilerinin işlenmesi sırasında karşılaşabilecekleri problemler, hukuka aykırı veri işleme hallerinde başvurabilecekleri yasal yollar ve PHS'lerin yükümlülükleri incelenmektedir.

2.1 Posta ve Posta Hizmetinin Tanımı

İtalyanca kökenli bir kelime olan "posta" Türk Dil Kurumu sözlüğünde *"bir yere gelen veya bir yerden gönderilen mektup ve emanetlerin tümü"*[127] ve Cambridge Sözlüğünde ise aynı köken dilinden İngilizceye geçen "post" "toplama, taşıma ve teslim etme sistemine dahil mektup, koli vb." şeyler[128] olarak tanımlanmaktadır

Daha teknik bir biçimde incelendiğinde Uluslararası Posta Birliği (*Universal Postal Union*, UPU)'nin "posta" tanımının "*posta hizmetleri vasıtasıyla gönderilen herhangi bir şey (mektup postası, paket postası, para havaleleri vb.)"* şeklinde olduğu görülmektedir[129].

[127] Türk Dil Kurumu, Güncel Türkçe Sözlük.
[128] Cambridge Dictionary.
[129] Dünya Posta Birliği (UPU), "UPU Terminology Database (TERMPOST)".

Diğer yandan, posta hizmeti kavramı da yaygın olarak kullanılan bir ifadedir. Bu çerçevede posta hizmetini AB Posta Direktifi, *"toplama, tasnif, nakliye ve dağıtımı kapsayan hizmetler"* olarak, OECD ise *"malların veya bilgilerin bir yerden bir yere teslim edildiği bir iletişim ve taşıma çeşidi"* olarak tanımlamıştır[130].

Türkiye'de posta mevzuatının temel kaynağı olan ve 23.05.2013 tarihli ve 28655 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6475 Sayılı Posta Hizmetleri Kanunu (PHK) 'nda doğrudan *"posta"* tanımına yer verilmemiş olmakla birlikte, bu kavramla ilişkili olarak *"posta gönderisi"* ibaresi kullanılmıştır. Buna ek olarak posta gönderisinin alt unsurları *"haberleşme gönderisi"* ve *"posta kolisi veya kargosu"* kavramları tanımlanmak suretiyle posta kavramına açıklık getirilmiştir[131]. Aynı Kanun'un 5 inci maddesinde posta hizmetlerinin kapsamı *"Posta gönderilerinin kabulü, toplanması, işlenmesi, sevki, dağıtımı ve teslimi"* olarak belirlenmiştir. Bahse konu tanımlamalardan yola çıkılarak posta hizmetlerinin; bilginin, haberin, maddenin, eşyanın veya paranın el ve yer değiştirmesi olduğu söylenebilecektir[132].

Diğer taraftan posta hizmeti kavramı üzerinde de anlaşılmış tek tip bir tanımının bulunmadığı görülmektedir. Bununla birlikte posta hizmetinin, gönderilerin belirli bir noktadan teslim alınması ile başlayan ve başka bir noktada bulunan alıcıya teslim edilmesi ile sona eren bir hizmet olduğu söylenebilecektir.

2.1.1 Posta hizmetinin aşamaları

Uygulamadaki genel kabul ve PHK kapsamında, posta hizmetlerinin sunumunu; kabul-toplama, tasnif (işleme), sevk ve dağıtım-teslim olmak üzere birbiriyle bağlantılı dört

---

[130] OECD, *Promoting Competition in Postal Services*, (1999): 7.

[131] Posta hizmetlerinin sınıflandırılmasında bazı kaynaklar tarafından ekspres gönderi tanımına da yer verildiği görülmektedir. Bununla birlikte işbu tezin yayımlandığı tarih itibarıyla PHK'de böyle bir tanım yer almamakta, ekspres gönderiler posta gönderisi olarak kabul edilmemektedir. Bu nedenle bu çalışmada ekspres gönderiler incelenmemiştir.

[132] Kevser, Aktaş Kuruçay, "Bir İletişim Aracı Olarak Posta Sanatı (Mail Art)", *The Turkish Online Journal of Design, Art and Communication,* Cilt: 12, Sayı: 3, (2022): 771.

aşamada incelemek mümkündür. Diğer yandan bahse konu aşamaların, sektörde sıklıkla başvurulan yöntemlerle, diğer bir ifade ile ticari örf ve adetlerle şekillenmekte olduğu kabul edilmektedir.

Posta hizmetleri sunumunun ilk aşaması, gönderilerin kabulü ve toplanmasıdır. Toplama işlemi, bir yerden alınan gönderinin başka bir noktada tasnif edilmek üzere kabul edilmesi işlemi olarak tanımlanabilir. Toplama faaliyeti; belli bölgelerde yer alan posta kutuları, posta şubeleri/acenteleri ya da posta göndericisi veya yetkili kıldığı kişi vasıtasıyla gerçekleştirilebilir[133]. Kabul işlemi, postanın PHS'ye teslimi ile gerçekleşmekte ve bu işlem posta hizmet sözleşmesinin kuruluşuna kanıt teşkil etmektedir.

Tasnif ya da PHK'de geçen ifade ile işleme faaliyeti ise posta hizmetlerinin sunumu için gönderilerin toplanmasının akabinde gönderilerin nakliyesi öncesi ve sonrasında dağıtıma çıkarılmadan önce yapılan sınıflandırma işlemidir[134]. PHS'lerin teknik ve ekonomik imkânları çerçevesinde elle (manuel) ya da teknolojik olanaklar ile (otomasyon sistemleri vb.) tasnif ve adresleme işlemlerinin yapılması mümkündür. Özellikle yüksek gönderi hacmine sahip PHS'ler, teknolojinin yaygın ve etkin biçimde kullanılması sayesinde önemli avantajlar elde edebilmektedir[135]. Bu bağlamda, tedarik zinciri süreçlerinin dijital dönüşüme tabi tutulması; gönderi takibi, envanter yönetimi, rota optimizasyonu ve müşteri etkileşimi gibi operasyonel alanlarda verimliliği artırmaktadır.

---

[133] Mehmet, Özcan, *Posta Hizmetlerinin Düzenlenmesi, Uluslararası Kuruluşlar ve AB Müktesabatı Çerçevesinde Türkiye'deki Durumun İncelenmesi ve Öneriler*, (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2011): 14.

[134] Gülşen, Eser, *Posta Hizmetleri Sektöründe Yapılan Reformlar, Posta Hizmetlerinin Serbestleştirilmesi "PTT AŞ Örneği",* (Yüksek Lisans Tezi, İzmir Üniversitesi, 2014): 5.

[135] Muhammed Can, Büyüktanır, *Posta Sektöründe Birleşme-Satın Almalar (Yatay-Dikey Birleşmeler) ve Posta Sektörüne Etkileri*, (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2022): 13, (Yayımlanmamış Tez)

Sevk veya diğer bilinen adıyla transfer faaliyeti, posta gönderilerinin bir tasnif merkezinden diğerine, dağıtıma hazırlanmak üzere taşınması işlemidir[136].

Posta hizmetinin son aşaması olan dağıtım-teslim aşaması, posta gönderilerinin alıcısına ulaştırılması olarak tanımlanabilmektedir[137]. Özellikle son yıllarda gönderici odaklılıktan alıcı odaklılığa evrilen posta pazarında dağıtım hizmeti, tüketici memnuniyeti açısından en önemli unsur olarak karşımıza çıkmakta olup hizmet kalitesinin arttırılmasını teminen yatırım yapılması gereken önemli alanlardan biridir.

2.1.2 Posta hizmetinin çeşitlerine göre sınıflandırılması

PHK'de posta hizmetleri; posta gönderisi, haberleşme gönderisi ve posta kolisi veya kargosu olarak sınıflandırılmış[138] olup aşağıda söz konusu kavramların PHK'deki tanımlarına yer verilmektedir.

PHK'nin "Tanımlar" başlıklı 3 üncü maddesinin (u) bendinde posta gönderisi; *"Göndericinin bizzat kendisi veya talimatıyla, üzerinde belirtilen yer ve adrese, gönderi türüne ve özel hizmetine göre teslim edilen haberleşme gönderileri ile kitap, katalog, gazete ve süreli yayınları, görme engellilere özgü yazıları, ticari değeri olsun veya olmasın eşya içeren en fazla beş kilogram ağırlığa veya elli desimetreküp hacme sahip posta maddesi ile posta kolisi veya kargosu,"* olarak tanımlanmıştır.

PHK'nin "Tanımlar" başlıklı 3 üncü maddesinin (j) bendine göre haberleşme gönderisi; *"Kitap, katalog, gazete ve süreli yayınlar hariç herhangi bir fiziksel araç üzerine yazılan veya elektronik ileti şeklinde hazırlanan, gönderici tarafından gönderi üzerinde belirtilen adrese sevk ve teslim edilmesi gereken telgraf da dâhil her türlü gönderi"*dir.

---

[136] Büyüktanır, *Posta Sektöründe Birleşme-Satın…,* 13.
[137] Büyüktanır, *Posta Sektöründe Birleşme-Satın…,* 13.
[138] Posta hizmetlerinin sınıflandırılmasında bazı kaynaklar tarafından ekspres gönderiye de yer verilmektedir. Bununla birlikte halihazırda PHK'de böyle bir tanım yer almamaktadır. Bu nedenle bu çalışmada ekspres gönderiler ayrı bir başlık altında incelenmemiştir.

PHK'nin "Tanımlar" başlıklı 3 üncü maddesinin (ü) bendinde posta kolisi veya kargosu; *"Hizmet sağlayıcısı aracılığıyla yollanan ve kapsamında haberleşme niteliği taşıyan yazılar bulunmayan en fazla otuz kilogram ağırlığa veya üç yüz desimetreküp hacme sahip her türlü madde"* şeklinde ifade bulmaktadır.

2.2 Posta Sektöründe Kişisel Verilerin Tarihsel Gelişimi

PHS'lerin güvenilir aracı kurumlar olarak çalışmaları, haberleşme hizmetlerinin temel gereksinimlerinden biridir. Zira, haberleşmenin gizliliği, birçok demokratik ülkenin anayasasında yer alan temel bir hukuki ilke olup haberleşme gönderilerinin kanuni istisnalar haricinde açılmaması, içeriğinin araştırılmaması ve açıklanmaması bu ilke çerçevesinde garanti edilmektedir. Dolayısıyla, gizliliğe saygı, veri koruma ve mahremiyet kavramları PHS'ler ile ilişkilendirilmekte olup esasen kişisel verilerin gizliliği kavramının yüzyıllardır PHS'lerin bir nevi "DNA"sında yer aldığı ifade edilmektedir[139].

Diğer yandan, evrensel PHS'lerin hâlâ birçok ülkede kamu kurumu veya devlet şirketi olarak faaliyet göstermekte olduğu bilinmekte olup anılan kurumlar aracılığıyla posta hizmetlerine dahil önemli kamusal faaliyetlerde bulunulmaktadır. Örneğin; Türkiye'de sermayesinin tamamı Türkiye Varlık Fonu'na ait olan ve evrensel PHS olarak faaliyet gösteren Posta ve Telgraf Teşkilatı Anonim Şirketi (PTT)[140] aracılığıyla kamu yönetiminde bilgi ve iletişim teknolojilerinin kullanımına imkân tanıyan e-Devlet platformunun şifresi alınabilmekte, benzer şekilde emekli maaş ödemeleri gerçekleştirilebilmektedir. Ayrıca Türkiye'de Covid-19 salgınının yaşandığı dönemde, yine PTT aracılığıyla vatandaşlara ücretsiz maske dağıtımı yapıldığı, 65 yaş üstü,

---

[139] Claire Borsenberger, Denis Joram, Olaf Klargaard, and Philippe Regnard, "Personal Data and Privacy Issues and Postal Operators Stand", *The Future of the Postal Sector in a Digital World*, (2016): 266.

[140] Türkiye'de PTT'nin sermayesinin tamamı, 05.02.2017 tarihli ve 29970 sayılı Resmî Gazete'de yayımlanan 24.01.2017 tarih 2017/9756 sayılı Bakanlar Kurulu Kararı ile Hazine Müsteşarlığı'ndan Varlık Fonuna devredilerek tescil ve ilan edilmiştir. (Resmî Gazete, *24.01.2017 tarih 2017/9756 sayılı Bakanlar Kurulu Kararı*, (2017)).

engelli ve bakıma muhtaç bireylerin maaş ödemelerinin "evde maaş ödemesi" uygulaması kapsamında bizzat konutlarında gerçekleştirildiği bilinmektedir[141].

Öte yandan, posta hizmetlerinin kamu ve kişisel hayata dair önemli bir hizmet olarak görülmesi nedeniyle posta hizmetlerinin sunumunda, PHS'lerin elde ettikleri verilerin gizliliğini sağlamaları ve bu konudaki gerekli tedbirleri almaları ile bu yükümlülüklere aykırı durumlarda sorumlu tutulmaları zorunluluğu doğmaktadır. Bu kapsamda bu bölümde öncelikle posta hizmetlerinde gizliliğin kapsamı ile görünümleri ele alınmaktadır. Daha sonra posta sektöründe kişisel verilerin korunması hususu irdelenmektedir. Bu doğrultuda posta sektöründe kişisel veri kavramı üzerinde durulmakta ve kişisel verilerin korunmasına ilişkin mevzuat çerçevesinde posta sektörü ele alınmaktadır.

2.2.1 Posta hizmetinde gizliliğin kapsamı

Posta hizmetlerinde gizliliğin kapsamının ortaya konulabilmesi için öncelikle tarihsel bir perspektiften konunun ele alınmasında fayda vardır. Posta hizmetlerinde gizlilik hakkının doğuşu da Avrupa menşeilidir. Orta Çağ'da Avrupa genelinde posta hizmetleri, tıpkı para basma yetkisinde olduğu gibi bir egemenlik imtiyazı olarak görülmüştür. Söz konusu çağa kadar posta hizmetlerine dair hukuki bir gizlilik teminatı bulunmamaktadır. Posta hizmetlerinin sunumunda sanayi devrimi gibi gelişmeler neticesinde, özel sektör devreye girmiş ve özel sektör eliyle özellikle Avrupa'nın büyük bir bölümünü kapsayan bir posta ağı kurulmaya başlanmıştır. Anılan hizmetlerin özel sektörce sunulmasına paralel olarak posta sektörünün gizliliği ve güvenliğine yönelik düzenleme yaklaşımı da ortaya çıkmaya başlamıştır. Ancak bu güvenceler başta, bireylere yönelik değil, ticari sırların korunması için gündeme getirilmiştir. Nitekim posta hizmetlerindeki niceliksel artış ticari hayattaki haberleşme

[141] Ulaştırma ve Altyapı Bakanlığı, "PTT, evde emekli maaşı ve yardım ödemeleri kapsamında 8,4 milyon işlem gerçekleştirdi."

ihtiyacının ivme kazanmasıyla aynı döneme gelmektedir. Özellikle, tacirlerin Avrupa ticaret merkezlerinde neler yaşandığına dair bilgilere ihtiyaç duymaları, posta hizmetini ticaretin ana girdilerinden biri haline getirmiş ve ticari bilgilerin gizliliğinin korunmasına ihtiyaç duyulmuştur[142].

Diğer yandan Avrupa monarşileri, posta hizmetinin iyi bir gelir kaynağı olduğunu fark ederek bu sektörü kamulaştırma faaliyetlerine başlamıştır. Bu durum posta hizmetlerinin devletleştirilerek tekelleşmesi geleneğinin bir başlangıcı olarak görülmektedir. Ancak bu durum özellikle mektupların gizliliği yönünde endişeleri de beraberinde getirmiştir[143].

Devletin mutlak posta tekeline sahip olması, ilerleyen dönemlerde bireylerin haberleşme gizliliğinin korunarak anayasal bir hakka dönüşmesi açısından belirleyici bir rol oynamıştır. Bu doğrultuda devletin mektuplara yönelik geniş çaplı müdahalesine yanıt mahiyetinde ilk olarak 1789 yılında "Fransız İnsan ve Yurttaş Hakları Bildirisi"nin ön taslaklarında haberleşmenin gizliliği hakkına yer verilmiştir. Bildiriyi hazırlayanlar haberleşmenin gizliliği hakkını gizlilik hakkının bir yönü olarak değil, fikir ve ifade özgürlüğünün bir yönü olarak kabul etmişlerdir. Ancak Bildiri'nin son haline, haberleşmenin gizliliği hakkı doğrudan dahil edilmemiştir. Bu hak, fikir ve ifade özgürlüğünün tanınması hakkının altında örtülü bir biçimde kabul görmüştür[144].

Avrupa için 19. yüzyıl, anayasal düzenlemelerin yoğun şekilde yaşandığı bir dönemdir. Bu anayasaların temel amacı, devletin yetkilerini sınırlandırarak bireylerin medeni haklarını devlete karşı güvence altına almaktır. Haberleşmenin gizliliği hakkı, bireylerin özel alanlarına devlet müdahalesini engelleyen klasik medeni haklardan biri

---

[142] Frederik Zuiderveen, Borgesius ve Wilfred, Steenbruggen, "The Right to Communications Confidentiality in Europe: Protecting Trust, Privacy, and Freedom of Expression", *Theoretical Inquiries in Law*, (2018): 295.

[143] David, Kahn, *The Codebreakers: The Comprehensive History Of Secret Communication From Ancient Times To The İnternet*, (1996).

[144] Borgesius ve Steenbruggen, "The Right to Communications…": 295.

olarak bu dönemde birçok Avrupa ülkesi anayasasına dahil edilmiştir. Bununla birlikte, bazı Avrupa ülkeleri, anayasal düzeyde haberleşmenin gizliliği hakkını, telefon ve telgraf gibi yeni iletişim teknolojilerini de kapsayacak şekilde genişletmiştir[145].

II. Dünya Savaşı'ndan sonra ise uluslararası insan hakları antlaşmaları, haberleşmenin gizliliğinin korunmasına yeni bir seviye getirmiştir. Bu antlaşmalarda, haberleşmenin gizliliği, gizlilik ile ilgili bir hak olarak ele alınmıştır. Örneğin, 1948 tarihli Evrensel İnsan Hakları Beyannamesi'nde bireylerin mahremiyet hakları ele alınmıştır. Posta hizmetleri de bu kapsamda değerlendirilmiş olup anılan Beyannamede bireylerin mahremiyet haklarına ilişkin düzenlemeye 12 nci maddede yer verilmiştir. Kişilerin posta ağını kullanmak suretiyle yararlandığı haberleşme hakkının güvence altına alınması konusu; *"Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır."* hükmüyle sağlanmıştır. Özetlenecek olursa tarihsel olarak haberleşmenin gizliliği hakkı, posta ve telekomünikasyon hizmetlerindeki eski devlet tekeliyle bağlantılı olarak görülmektedir[146].

Türkiye'de haberleşmenin gizliliği hakkına T.C. Anayasası'nın "Haberleşme hürriyeti" başlıklı 22 nci maddesinde;

> *"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır."* hükmü ile yer verilmiştir. Ayrıca aynı maddede; *"millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla*

[145] Borgesius ve Steenbruggen, "The Right to Communications…": 296.
[146] Borgesius ve Steenbruggen, "The Right to Communications…": 296-297.

yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşmenin engellenemeyeceği ve gizliliğine dokunulamayacağı"

hükmü ile haberleşme hürriyeti, bireylere bir hak olarak tanınmış ve bu hak doğrudan anayasal güvence altına alınmıştır.

Öte yandan PHK'nin "Posta hizmetlerinin gizliliği ve güvenliği" başlıklı 7 nci maddesinde posta hizmetlerinin gizliliğine yönelik hükümlere yer verilmiştir. Buna göre posta hizmetlerinin sunumunda PHS'lerin, bu hizmetlerde çalışan veya hizmetlere dair bilgiye sahip olan kişilerin bu bilgileri açığa çıkarmaları, ayrıca bu kişilerin posta gönderilerini açmaları, gönderi içeriğini araştırmaları, bu konularda üçüncü taraflara bilgi vermeleri, gönderileri zapt etmeleri ya da yok etmeleri de yasaklanmıştır.

2.2.2 Posta sektörüne ilişkin uluslararası düzenlemeler

2.2.2.1 I. Posta Direktifi

I. Posta Direktifi (97/67/EC sayılı Direktif), AB'deki posta hizmetlerinin serbestleşme sürecine en önemli katkıyı sağlayan Direktif olarak görülmektedir[147]. Bu Direktifin 2 nci maddesinin on dokuzuncu fıkrasında posta hizmetlerinin sunumuna dair *"temel gerekliliklere (essential requirements)*" yer verilmiştir. Buna göre; bir üye devleti posta hizmetlerinin sağlanması konusunda koşullar koymaya sevk edebilecek ekonomik olmayan genel nedenler "temel gereklilik" olarak tanımlanmaktadır. Maddenin devamında ise bu genel nedenlerin, haberleşmenin gizliliği, tehlikeli malların taşınmasıyla ilgili olarak ağın güvenliği ve haklı nedenlerin varlığı halinde veri koruma, çevre koruma ve bölgesel planlama olduğu belirtilmiştir. Ayrıca veri koruma

[147] Mark, Winkelmann, Torben, Schönershoven, Eva, Lauerbach, Olivia, Dihel, Tim, Ulrich, Antonia, Niederprüm, Alex, Dieke ve Petra, Junk, *The Evolution of the European Postal Market since 1997*, (2009): 12-13.

kavramının; kişisel verilerin korunması, iletilen veya saklanan bilgilerin gizliliği ve mahremiyetin korunmasını kapsayabileceği belirtilerek kişisel verilerin korunması alanına atıfta bulunulmuştur[148].

2.2.2.2 II. Posta Direktifi

I. Posta Direktifi 2002 yılında, II. Posta Direktifi (2002/39/EC sayılı Direktif) adını alarak güncellenmiştir. 2002/39/EC sayılı Direktif, üye devletlere, evrensel hizmet kapsamı dışında kalan hizmetlerin kullanıcıları ve evrensel hizmet sağlayıcısı tarafından sunulmayan evrensel hizmet kullanıcıları için şeffaf, basit ve düşük maliyetli şikâyet prosedürleri ile ulusal düzenleyici otoritelerin yetkilerinin genişletilmesi olanağını sağlamıştır[149]. Anılan Direktif'te verilerin gizliliği ve kişisel verilerin korunması alanına ilişkin I. Direktife ilave bir düzenleme bulunmamaktadır.

2.2.2.3 III. Posta Direktifi

2008 yılında III. Posta Direktifi (2008/06/EC sayılı Direktif) yürürlüğe girmiştir. Anılan Direktifin Başlangıç kısmında yer alan 35 inci madde hükmüne göre; üye Devletler, PHS'lerinin, 97/67/EC sayılı Direktif uyarınca kişisel verileri işlerken özellikle 95/46/EC sayılı Direktif'te belirtilenler olmak üzere, kişisel verilerin korunmasına ilişkin Topluluk ve ulusal hükümleri uygulamasını sağlamalıdır[150]. Bu düzenleme ile posta sektöründe kişisel verilerin korunmasına ilişkin ayrı bir düzenleme yoluna gidilmeksizin PHS'lerin, kişisel verileri işlerken kişisel verilerin korunmasına ilişkin genel nitelikte olan 95/46/EC sayılı Direktif'e uyum sağlaması gerektiğine vurgu yapılmıştır.

---

[148] Avrupa Parlamentosu ve Avrupa Konseyi, *Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service*, (1998).
[149] Winkelmann vd., *The Evolution of the…,* 16.
[150] Avrupa Parlamentosu ve Avrupa Konseyi, *Directive 2008/6/EC of the European Parliament and of the Council of 20 February 2008 amending Directive 97/67/EC with regard to the full accomplishment of the internal market of Community postal services*, (2008).

2.2.2.4 Evrensel Posta Sözleşmesi

26.08.2021 tarihinde imzalanan ve 01.07.2022 tarihinde yürürlüğe giren Evrensel Posta Sözleşmesi, uluslararası posta hizmeti boyunca geçerli kuralları ve mektup postası ile posta kolisi/kargosu hizmetleriyle ilgili hükümleri içermektedir[151]. Anılan Sözleşmenin 3 üncü maddesi uyarınca; üye ülkeler, evrensel PHS'lerinin[152] Evrensel Posta Sözleşmesi'nden doğan yükümlülükleri yerine getirmesini sağlamakla yükümlüdür.

Diğer yandan bu Sözleşmenin "Kişisel verilerin işlenmesi" başlıklı 10 uncu maddesinde, kişisel verilerin işlenmesine ilişkin birtakım hükümlere yer verilmiştir. Buna göre kullanıcılara ait kişisel veriler yalnızca, yürürlükteki ulusal mevzuata uygun olarak toplandıkları amaçlar için kullanılabilmekte ve yürürlükteki ulusal mevzuat tarafından erişim yetkisi verilen üçüncü taraflara açıklanabilmektedir. Üye ülkeler ve evrensel PHS'ler ise ulusal mevzuatına uygun olarak kullanıcılara ait kişisel verilerin gizliliğini ve güvenliğini sağlamakla yükümlü kılınmıştır. Ayrıca bu PHS'ler müşterilerini kişisel verilerinin kullanımı ve toplanma amacı hakkında bilgilendirecektir. Bununla birlikte sayılan bu yükümlülüklere halel gelmeksizin, evrensel PHS'ler, hizmeti yerine getirmek için bu verilere ihtiyaç duyan hedef veya transit ülkelerin belirlenmiş PHS'lerine elektronik olarak kişisel verileri aktarabilmektedir.

2.2.2.5 UPU Çok Taraflı Veri Paylaşım Anlaşması

UPU'nun daimî organlarından biri olan Posta İşlemleri Konseyi (*Postal Operations Council***,** POC) tarafından 2021 yılının Nisan ayında kabul edilen ve Türkiye'den PTT'nin

---

[151] Dünya Posta Birliği (UPU), "Evrensel Posta Sözleşmesi".

[152] "Designated operatör" olarak ifade edilen "atanmış PHS", işbu tez kapsamında "evrensel PHS" olarak ifade edilmiştir.

17.01.2022 tarihinde imzalayarak tarafı olduğu[153] UPU Çok Taraflı Veri Paylaşımı Anlaşması (*UPU Multilateral Data Sharing Agreement*, MDSA)[154], uluslararası posta hizmetlerinin işletilmesi için gerekli verilerin değişimini kolaylaştırmak ve bu değişimlerin UPU düzenlemelerine uygun olarak gerçekleştirilmesini sağlamak için oluşturulan yasal bir belgedir. MDSA, UPU üyesi ülkelerin evrensel PHS'ler tarafından akdedilen mevcut ve özel olarak kurulmuş çok taraflı veri paylaşımı düzenlemelerinin esas hükümlerini içermekte ve genişletmektedir. Amaç, Birlik Yasalarında yer alan ilgili veri paylaşımı yükümlülüklerini daha iyi yansıtmak ve küresel erişime sahip UPU tarafından yönetilen bir araç için ilgili koşulları oluşturmaktır[155].

MDSA'da, *"bir posta hizmeti kullanıcısını tanımlamak için ihtiyaç duyulan (adı ve adresi de dahil olmak üzere makul ölçüde kullanılması muhtemel araçlarla tanımlanabilen) belirli veya belirlenebilir bir gerçek kişiye ilişkin bilgiler (Evrensel Posta Sözleşmesi'nin 1.1.8. maddesinde öngörüldüğü şekilde) ve Evrensel Posta Sözleşmesi'nin 10. maddesi uyarınca işlenen bilgiler."* şeklinde kişisel veri tanımına yer verilerek kişisel verilerin gerçek kişilere ait bilgiler olduğu belirtilmiştir.

"Veri koruma ve gizlilik" başlıklı 10 uncu maddesinde; herhangi bir taraf tarafından başka bir tarafa iletilen kişisel verilerin "Gizli Bilgi" kapsamına girdiği, bu bilgilerin, UPU veya diğer ağlar aracılığıyla taraflarca değiştirilen verileri içerdiği, bu tür verilerin, yetkisiz erişim, kayıp veya yanlışlıkla iletimi önlemek için sektör standartlarında güvenlik teknolojileriyle korunacağı, kişisel veri içermeyen posta takip bilgilerinin ise gizlilik yükümlülükleri dışında tutularak UPU'nun Tüzüklerinde belirtilen prosedürlere uygun olarak erişime açılabileceği ifade edilmiştir.

---

[153]Dünya Posta Birliği (UPU), *Multilateral Data Sharing Agreement - Signatory countries*, (2025).
[154] Dünya Posta Birliği (UPU), *Multilateral Data Sharing Agreement, 2021, POC C 1 2021.1–Doc 2.Annex 1.Rev 1 Published in English 8.7.2021, 16.38 (Previous version published 23.3.2021, 09.44).*
[155] Dünya Posta Birliği (UPU), "Postal Supply Chain Integration", (2022).

Ayrıca Anlaşma'nın 10 uncu maddesi gereği, UPU Tüzüklerinde belirtilen yükümlülüklerine halel getirmeksizin her bir taraf; kendi ülkesinde kişisel verilerin gizliliğini ve güvenliğini sözleşmenin anılan maddesine uygun olarak sağlaması gerektiğini, göndericinin gizli bilgilerini her zaman gizli tutmayı ve yazılı açık rızası olmaksızın bu bilgileri açıklamamayı veya açıklanmasına izin vermemeyi kabul ettiğini, bu bilgileri yalnızca Anlaşma kapsamındaki yükümlülüklerini yerine getirmek için kullanmayı ve aksi yönde bir izin alınmadıkça başka bir amaçla işlememeyi taahhüt etmektedir.

Özetle; Anlaşmanın 10 uncu maddesi ile kişisel verilerin ve diğer gizli bilgilerin korunmasını garanti altına alınmakta, gizli bilgilerin nasıl kullanılacağı ve kimlerle paylaşılacağı belirlenmektedir. Maddede, yasal zorunluluklar gibi istisnai durumlar dışındaki bilgilerin gizli kalması hükme bağlanmıştır. Ayrıca taraflar, kişisel verilerle ilgili talepleri birbirlerine bildirmekle yükümlü olup bu gizlilik yükümlülükleri anlaşma sona erdikten sonra da devam etmektedir.

Söz konusu Anlaşma ile UPU üye ülkeleri, evrensel PHS'ler ve posta sektöründeki diğer paydaşlar tarafından, uluslararası posta hizmetlerinin işletilmesinde ve posta gönderilerinin işlenmesinde veri ve gizliliğin korunmasının önemi kabul edilmektedir.

2.2.3 Posta sektöründe kişisel veri tanımı ve unsurları

Kişisel veri; "Evrensel Posta Sözleşmesi"nde, posta hizmeti kullanıcısını tanımlamak için gerekli olan bilgi olarak ifade edilmiştir. MDSA'da ise bu kavram, Evrensel Posta Sözleşmesi'nin 1.1.8 ve 10 uncu maddelerindeki kişisel veri tanımını ve kişisel verilerin işlenmesini içerecek şekilde *"*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin bilgi*"* şeklinde tanımlanmıştır[156].

[156] Dünya Posta Birliği (UPU), *Multilateral Data Sharing Agreement.*

Diğer yandan, Türk posta mevzuatı kapsamında kişisel veri kavramı, 03.06.2014 tarihli ve 29019 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Posta Sektörüne İlişkin Yetkilendirme Yönetmeliği (PSİYY)'nin "Tanımlar" başlıklı 4 üncü maddesinin birinci fıkrasının (g) bendinde, *"Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler"* şeklinde ifade edilmiştir[157].

Anılan tanımlardan yola çıkıldığında GDPR ve KVKK'den farklı olarak Evrensel Posta Sözleşmesi'nde kişisel verinin, bireyin gerçek ya da tüzel kişi olup olmadığına ilişkin bir ayrıma yer verilmeksizin, "kullanıcı" terimiyle ilişkilendirildiği, ancak sözleşme kapsamında bu terimin bir tanımının yapılmadığı görülmektedir. Bununla birlikte, bir gönderici veya alıcının tüzel kişi olabilmesi mümkün olduğundan, sözleşme gereği tüzel kişilerin de kişisel verilerinin korunmasına yönelik haklardan yararlanabileceği değerlendirilmektedir. Öte yandan, MDSA'da kişisel verinin yalnızca gerçek kişilere ait bilgilerle sınırlandırılmış olduğu, tüzel kişilerin bu hukuki koruma kapsamına dahil edilmeyerek GDPR ve KVKK'ye benzer nitelikte bir tanım yapıldığı anlaşılmaktadır. PSİYY'nin kişisel veri tanımında ise *"gerçek ve tüzel kişi"* ifadesi ile posta sektöründe tüzel kişi verilerinin de koruma altına alındığı görülmektedir. Keza AYM'nin 04.12.2014 tarihli ve E.2013/84, K.2014/183 sayılı kararında tüzel kişilere ait elektronik ve fiziki adres bilgisinin tüzel kişinin rızası alınmaksızın bir PHS olan PTT tarafından toplanması ve bu hususta kanun ile PTT'ye yetki verilmesi, eşitlik ilkesine aykırı bulunmuş ve tüzel kişilerin de koruma kapsamına alınması gerektiği belirtilmiştir[158]. Anılan hüküm ve karardan da anlaşılacağı üzere tüzel kişilere ait kişisel veriler, KVKK kapsamında korunmasa dâhi, diğer düzenlemeler kapsamında korunabilmektedir[159]. Bu kapsamda posta sektörüne dair özel hükümler ile tüzel kişi verileri de koruma altına alınmıştır.

---

[157] Posta Sektörüne İlişkin Yetkilendirme Yönetmeliği, 2014

[158] Anayasa Mahkemesi, 04.12.2014 günlü, E:2013/84, K:2014/183 sayılı karar.

[159] Faruk, Bilir, "Kişisel Verilerin Korunması Yönündeki Uygulama ve Hukuki Düzenlemelerin Ortaya Çıkışı", *Adalet Dergisi*, Sayı: 71, (Kasım 2023): 643.

Öte yandan yukarıda yer verilen kişisel veri tanımlarında, kişilerin kimliğinin *"belirli veya belirlenebilir olması"* zorunluluğuna yer verilmiştir. Dolayısıyla ilgili veri ile bir gerçek veya tüzel kişi arasında bağlantı kurulabiliyorsa, bu kişi belirlenebilir olmaktadır. Bu bağlamda, posta sektöründe kişisel veri değerlendirmesi yapılırken verilerin doğrudan veya dolaylı olarak bir gerçek ya da tüzel kişiyle ilişkilendirilebilirliği dikkate alınmakta ve bu durum veri koruma yükümlülüklerinin kapsamını genişletmektedir. Örneğin; posta sektöründe bazı PHS'ler[160] tarafından kullanıcılara "müşteri numarası" verilmesi halinde bu müşteri numarası ile kullanıcının isim, soy isim, adres bilgisi, cep telefonu gibi kişisel verilerine erişim mümkün olabilmekte, bir başka deyişle bu numara ile kişinin kimliği belirlenebilmektedir. Bu sebeple "müşteri numarası" olarak adlandırılan numaranın kişisel veri olarak kabul edilmesi gerektiği değerlendirilmektedir. Ayrıca posta sektöründe, bazı e-ticaret siteleri aracılığı ile sipariş edilen ürünlerin iadesinde "iade kargo kodu"[161] ile gönderici ya da alıcı bilgisi verilmeksizin gönderi doğrudan PHS'ye teslim edilmektedir. PHS ise bu iade kodu ile gönderici ve alıcıya ait taraf bilgilerine ulaşılabilmektedir. Bu kapsamda iade kodunun da kişiye özgü oluşturulması ve tarafları belirlenebilir kılması nedeniyle kişisel veri olarak kabul edilmesi gerektiği düşünülmektedir.

Diğer taraftan posta sektöründe kişisel veri tanımı yapılırken, bireylere ait *"her türlü bilgi"*nin koruma kapsamına alındığı dikkat çekmektedir. Buna göre, kişinin yalnızca temel kimlik bilgileriyle sınırlı kalınmadığı, ayrıca sosyal ve mesleki yaşamına ilişkin verileri gibi daha geniş bir bilgi yelpazesini de içerdiği anlaşılmaktadır. Bu bağlamda, örneğin belirli meslek gruplarına[162] (avukatlara özel kampanyalar gibi) veya toplumsal hassasiyet taşıyan bireylere (engelli, şehit ve gazi yakınları gibi) yönelik hizmetlerin sunulması amacıyla toplanan bilgilerin de kişisel veri niteliği taşıdığı değerlendirilmektedir.

---

[160] MNG Kargo, "Genel Aydınlatma Metni".
[161] Trendyol, "Ürünümü Nasıl İade Ederim?".
[162] Kişisel Verileri Koruma Kurulu Kararı, 30.09.2021 günlü, 2021/993 sayılı karar.

2.2.4 Posta sektöründe veri sorumlusu

GDPR ve KVKK uyarınca veri sorumlusu; kişisel verilerin işlenme amaçlarını ve yollarını belirleyen, veri kayıt sisteminin kurulması ve yönetilmesinden sorumlu gerçek ya da tüzel kişidir. Bu minvalde posta sektöründe kişisel verilerin işlenmesi aşamasında, PHS'lerin hangi hukuki sıfata sahip olduğunun ortaya konulmasında fayda görülmektedir. PHS'lerin posta hizmeti sunumunda gönderici ile bir sözleşme imzalayarak kişisel veri işleme sürecine dâhil oldukları bilinmekte olup buna göre PHS'ler, gönderici veya alıcıya ait birtakım kişisel veriler üzerinde karar verme yetkisine sahip olmaları nedeniyle, posta hizmeti sunmak amacıyla elde ettiği veriler açısından veri sorumlusu olarak kabul edilmektedir[163].

Diğer yandan PHS'lerin taşıdıkları gönderiler için muttali olmadıkları içeriğe ilişkin bir veri işleme sürecine giremeyecekleri dikkate alındığında, bu kapsamdaki veriler bakımından veri sorumlusu statüsünde olmadıkları açıktır. Zira KVK Kurulu'nca yayımlanan "*Veri Sorumlusu ve Veri İşleyen*" başlıklı Rehber'in "Örnekler: Kargo Firmaları" başlıklı alt bölümünde, *"Bir kargo firması, bir banka ile müşterilerin kredi kartlarını ilgilisine ulaştırma hizmetini vermek üzere bir sözleşme yapmıştır. Kargo firması gönderenin adı, soyadı, alıcının adresi gibi sevkiyatı yönetmek için elde ettiği veriler bakımından veri sorumlusudur. Ancak, kargo firması her ne kadar kredi kartlarını fiziksel olarak elinde bulundursa da, söz konusu kredi kartı ile ilgili bilgilere ulaşması mümkün değildir. Bu durumda, dağıtım hizmeti sunucusu olarak hizmet veren kargo firması ne veri sorumlusu, ne de veri işleyen statüsündedir. Dolayısıyla, yalnızca taşıdığı fiziksel eşyanın güvenliğini sağlamakla yükümlü olup, kişisel verilerin işlenmesiyle ilgili uyması gereken herhangi bir yükümlülük yoktur.*" denilmek suretiyle gönderi içeriğine tamamen hâkim olması kendisinden beklenemeyecek olan PHS'lerin, gönderi içeriği açısından veri sorumlusu ya da veri işleyen statüsünün

[163] Hasan Selçuk, Turan, "Veri Sorumlusu ve Veri İşleyen Farkı", (2017).

bulunmadığı ifade edilmiştir[164]. Aksi bir durumun kabulü, gönderi içeriğinde yer alan kişisel verilerin doğruluğu konusunda PHS'lerin sorumluluğuna yol açacaktır[165].

Öte yandan PHSİY'nin "Hizmetin kısıtlanması ya da durdurulması" başlıklı 21 inci maddesinin ikinci fıkrasında, *"Hizmet sağlayıcısı, posta yoluyla gönderilmesi yasak maddeler ile kabulü şarta bağlı gönderilere ilişkin yükümlülükleri kapsamında, haberleşmenin gizliliğine ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, gönderinin kabulü aşamasında kullanıcıdan gönderinin içeriğine ilişkin bilgi talep edebileceği gibi kullanıcıdan gönderiyi açmasını da isteyebilir."* hükmü yer almaktadır. Ayrıca BTK'nin, Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esaslar'nın (Güvenlik Usul ve Esasları) 4 üncü maddesi uyarınca posta gönderileri özel hayatın gizliliğine dikkat edilerek gönderici huzurunda kapsamı kontrol edildikten sonra kabul edilmekte ve kabul ve teslim aşamalarında gönderi içeriği kayıt altına alınmaktadır. Göndericinin, kabul aşamasında gönderiye ilişkin kapsam kontrolüne razı olmaması durumunda ise gönderi kabul edilmemektedir. Bu kapsamda esasen PHS'lerin gönderi içeriğini kayıt altına alması yükümlülüğü sonucu kişisel verileri işlemesi ve bu sayede gönderi içeriğini bilmesi (yani kişisel veriden muttali olması) durumları söz konusu olabilmektedir. Ancak, aynı düzenlemede özel hayatın gizliliği ifadesine yer verildiği göz önüne alındığında, haberleşme gönderileri gibi gönderilerin kapsamı hakkında bilgi sahibi olunması hukuken mümkün olmadığından, PHS'lerin bu verilere ilişkin veri sorumlusu sıfatına sahip olmadığı yorumu yapılabilecektir.

2.2.5 Posta sektöründe veri işleyen

GDPR ve KVKK uyarınca veri işleyen; veri sorumlusu tarafından verilen yetki doğrultusunda, veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişidir. Buna göre PHS'nin verdiği emir, yetki ve yönlendirmeler doğrultusunda onun adına

---

[164] Kişisel Verileri Koruma Kurumu. Veri Sorumlusu ve Veri İşleyen, 6.
[165] Kişisel Verileri Koruma Kurulu Kararı, 24.03.2022 günlü, 2022/277 sayılı "İlgili kişiye ait kişisel verileri içeren bir kargo paketinin üçüncü bir şahsın eline geçmesi" konulu karar.

kişisel verileri işleyen gerçek veya tüzel kişilerin veri işleyen sıfatına sahip olacağı, ayrıca veri sorumlusu ile veri işleyen sıfatlarının aynı kişide birleşmesi mümkün olacağından PHS'lerin de veri işleyen sıfatına sahip olabileceği değerlendirilmektedir.

Veri sorumlusunun bağımlı çalışanları ile kişisel veri işleyen ilgili birimleri ise veri işleyen statüsünde kabul edilmemekte olup veri işleyenin mutlaka veri sorumlusunun organizasyon yapısı dışında yer alması gerekmektedir[166]. Örneğin veri sorumlusu tarafından verilen yetkiye dayanarak veri sorumlusu adına faaliyette bulunan, dışarıdan hizmet alınması yoluyla çağrı merkezi hizmeti veren bir şirket, bu faaliyet kapsamında veri işleyen olarak kabul edilmektedir[167]. Bununla birlikte şirket bünyesinde faaliyet gösteren çağrı merkezi personeli veri işleyen konumunda değildir.

Posta sektöründe de PSİYY'nin 16 ncı maddesinin üçüncü fıkrası uyarınca, PHS'ler üçüncü taraflar ile yapacağı anlaşmalar doğrultusunda farklı iş sunum modelleriyle hizmet verebilmektedir. Bu kapsamda Türkiye'de esnaf kurye olarak tabir edilen modelde bireyler, kendi şahıs şirketlerini kurarak ve iş ortaklığı sözleşmeleri yaparak posta hizmeti sunmakta, veri sorumlusu olan PHS'nin bağımlı çalışanı olmamaktadır. Bununla birlikte hizmet sunumunun gereği olarak gönderi teslimatında gönderici, alıcı bilgileri, teslimat kodu gibi birtakım verileri işlemektedir. Bu halde esnaf kuryelerin de veri işleyen statüsünde olduğu değerlendirilmektedir.

Diğer yandan BTK'nin 28.03.2023 tarihli ve 2023/DK-SRD/115 sayılı kararı[168] ile yayımlanan "Teslimat Hizmetlerinin Uygulanmasına Yönelik Usul ve Esaslar"ın (Teslimat Usul ve Esasları) "fiziki ve teknik gereklilikler" başlıklı 6 ncı maddesinin ikinci fıkrasında PHS'ler ile sözleşme ilişkisi kuran üçüncü taraflara; PHS'ler ile anlık olarak

---

[166] Kişisel Verileri Koruma Kurumu, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında…": 17.
[167] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular,* (2025): 34.
[168] Bilgi Teknolojileri ve İletişim Kurulu Kararı, 28.03.2023 günlü ve 2023/DK-SRD/115 sayılı karar

veri paylaşımının sağlanması için gerekli yazılım ve sistemleri kullanmaları ve kullanılan bu yazılım ya da sistemler üzerinden alıcı ve göndericilerin kişisel verilerinin gizliliğini sağlamaları yükümlülüğü getirilmiştir. Anılan yükümlülük ile esasen posta sektöründe alternatif teslimat hizmeti yoluyla bir PHS'nin iş ortağı ya da taşeronu gibi faaliyet göstererek teslimat noktası hizmeti sunan üçüncü tarafların da veri işleme faaliyetleri nedeniyle "veri işleyen" statüsü kapsamına alındığı düşünülmektedir.

Bu bağlamda, KVKK'de öngörülmeyen ancak GDPR'da açıkça düzenlenen yazılı sözleşme ilkesine benzer biçimde, özellikle uluslararası hizmet sunan PHS'lerin veri işleyen statüsündeki üçüncü taraflarla bağlayıcı nitelikte bir kişisel veri işleme sözleşmesi imzalamasının faydalı olacağı değerlendirilmektedir.

2.2.6 Posta sektöründe kişisel verinin işlenmesi

Kişisel verilerin işlenmesi, diğer sektörlerde olduğu gibi posta sektöründe de yaygın bir uygulamadır. Posta hizmeti almayı talep eden bir kullanıcı, posta gönderisini PHS'ye teslim ederken çeşitli bilgilerini de paylaşmakta ve PHS'ler bu verileri sistemlerine kaydederek, kullanıcıların ileride yeniden hizmet talep etmeleri halinde bu bilgilere kolayca erişebilmektedir. Bu sayede PHS'ler operasyonel süreçlerde zaman tasarrufu sağlamaktadır[169].

Diğer yandan posta hizmetinin alıcıya teslimat aşaması, elektronik haberleşme ve elektrik gibi şebeke endüstrilerindeki altyapı kurulumuna benzer bir biçimde, maliyetli bir safha olup yeterli ölçek ekonomisine ulaşmak PHS'ler için stratejik bir önem taşımaktadır. Bu kapsamda günümüzde, PHS'ler posta hizmetlerinin sunumundan elde edilen verileri, maliyet azaltıcı bir fırsat olarak değerlendirebilmektedir. Büyük posta verilerinin analiziyle kullanıcı ihtiyaçlarının

---

[169] Nurullah, Çakmak, *Posta Sektöründe Kullanıcı Düzenlemeleri: Ülke Uygulamaları ve Türkiye İçin Öneriler*, (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2016): 96, (Yayımlanmamış Tez).

ortaya çıkarılması, PHS'lerin yeni hizmetler ve inovasyonla gelişmesini sağlayabilmektedir[170].

Öte yandan, PHS'ler tarafından işlenen kişisel veriler, PHS ile kullanıcı arasındaki ilişkinin niteliği, kullanılan iletişim yöntemleri ve kişisel veri işleme amaçlarına bağlı olarak farklılık göstermektedir. Kişisel veri, GDPR ve KVKK'de tahdidi olarak sayılmayarak kişinin belirlenebilir kılınmasında rol oynayan her türlü bilgi olarak kabul edilmiş olup bu çerçevede kargo göndericisi ya da alıcısının; "kimlik bilgileri (adı, soyadı, imzası, T.C. kimlik veya pasaport numarası, uyruk bilgisi, doğum tarihi), iletişim bilgileri (telefon numarası, e-posta adresi, ev ve/veya iş yeri adresi, işyeri ismi-ünvanı, il, ilçe, ülke bilgisi), hukuki işlem bilgileri (adli ve idari makamlarla yazışmalardaki bilgiler, ihtarname/ihbarname kapsamındaki bilgilerinin dava ve icra dosyasındaki bilgiler) yanı sıra, müşteri işlem bilgileri (kargo gönderisi ve kargo gönderi numarası, gönderi adedi, gönderi türü, gönderi tipine ilişkin sipariş bilgileri, talep ve şikâyet bilgileri, müşteri numarası, iade bilgileri, fatura bilgisi, tazmin talep bilgileri), görsel ve işitsel kayıt bilgileri (işitsel kayıtlar/çağrı merkezi kayıtları), finans bilgileri (banka hesap bilgileri, IBAN numarası) ve pazarlama bilgileri (anket yanıtları)[171]" gibi verilerinin kişisel veri olarak kabul edilerek bu verilerin işlenmesinin belirli ilke ve kurallara uygun bir biçimde gerçekleştirilmesi gerekmektedir[172].

2.3 Posta Sektöründe Kişisel Verilerin İşlenmesinde Temel İlkeler

Posta sektöründe kişisel verilerin işlenmesinde esas alınan temel ilkeler, KVKK başta olmak üzere, genel veri koruma mevzuatına dayanmaktadır. Bir başka deyişle, posta sektöründe kimlik doğrulama, hizmet ifası ve pazarlama faaliyetleri gibi işlemlerde kişisel verilerin işlenmesine uygulanabilecek esasların, bu genel çerçeveyle uyumlu ve

---

[170] Pier Luigi, Parcu and Virginia, Silvestri, *Lessons from the Postal Sector to Telecommunications and Vice Versa*, (Springer, 2017): 30.
[171] MNG Kargo, "Genel Aydınlatma Metni".
[172] Gubse, Özdemir Koçar, "Tüketici-Çevrimiçi Pazar Yerleri-Kargo Şirketleri Üçgeninde Kişisel Veri İşleme Faaliyetleri", *Kişisel Verileri Koruma Dergisi*, Cilt: 6, Sayı: 2, (2024): 108.

destekleyici nitelikte olması gerekmektedir. Bu nedenle bu tezin farklı bölümlerinde mükerrer açıklamalar yapılmaması adına, kişisel verilerin işlenmesinde esas alınan temel ilkelere, 1 inci bölümde değil, bu başlık altında yer verilmesi uygun görülmüştür.

Kişisel verilerin korunmasına ilişkin ulusal ve uluslararası metinlerde, kişisel verilerin işlenmesinde uyulması gereken bazı ortak temel ilkelere[173] yer verilmiş olup bu ilkeler, kişisel verilere yönelik işlemlerin başta insan onuru olmak üzere temel hak ve özgürlüklerine uygun bir biçimde gerçekleştirilebilmesi için belirlenmiş ve birbirlerini tamamlayıcı mahiyettedir[174]. Veri işleyenler, veri işleme faaliyetlerinde bu ilkeleri dikkate almakla yükümlüdür. Zira veri sahibinin kişisel verilerinin işlenmesine ilişkin açık rızası olsa bile, bu ilkelere aykırı bir şekilde veri işleme faaliyetinin gerçekleştirilmesiyle hukuka aykırı bir durum oluşabilecektir[175].

Bu kapsamda, GDPR'ın 5 inci maddesine göre kişisel verilerin; hukuka uygun, adil ve şeffaf bir biçimde, belirtilen, açık ve meşru amaçlarla, işlenme amaçlarına uygun, işlenme amaçlarıyla ilgili ve bunlarla sınırlı, doğru ve gerektiğinde güncel tutularak, veri öznelerinin, yalnızca kişisel verilerin işlenme amaçlarının gerektirdiği sürece kimliğinin belirlenmesini sağlayan bir şekilde tutularak, izinsiz veya hukuka aykırı işlemeye karşı ve kazara kayba, yok etmeye veya tahribe karşı koruma da dâhil olmak üzere, teknik veya düzenlemeye ilişkin uygun tedbirler kullanılarak kişisel verilerin uygun bir biçimde güvenliğini sağlayacak şekilde işlenebileceği belirtilmektedir[176].

Ülkemizde T.C. Anayasası'nın *"Özel hayatın gizliliği"* başlıklı 20 nci maddesinin üçüncü fıkrasında, kişisel verilerin yalnızca kanunda öngörülen hâllerde ya da ilgili kişinin açık rızasıyla işlenebileceği hükme bağlanmıştır. Bu anayasal hüküm ile kişisel verilerin

---

[173] Küzeci, *Kişisel Verilerin Korunması*, 227.
[174] Helin, Karakuş, *İş İlişkisinde Kişisel Verilerin Korunması*, (Yüksek Lisans Tezi, Hacettepe Üniversitesi, 2024): 50.
[175] Karakuş, *İş İlişkisinde Kişisel…,* 50.
[176] Veri Koruma Komisyonu*, Quick Guide to the Principles of Data Protection*. (Ekim 2019): 1.

işlenmesinin ayrıksı bir durum olduğu ortaya konulmuştur[177]. KVKK'nin 4 üncü maddesinde ise kişisel verilerin; "hukuka ve dürüstlük kurallarına uygun olma", "doğru ve gerektiğinde güncel olma", "belirli, açık ve meşru amaçlar için işlenme", "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ve "ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkelerine uygun olarak işlenebileceği düzenlenmiştir. Söz konusu temel ilkelere, yalnızca genel nitelikteki verilerin işlenmesinde değil, hassas verilerin işlenmesinde de uyulması gerekmektedir[178]. Temel ilkeler aşağıda inceleme konusu yapılırken, KVKK hükümleri dayanak alınmakla birlikte, daha doğru yorumlanması açısından GDPR düzenlemelerine de yer verilmektedir.

2.3.1 Hukuka ve dürüstlük kurallarına uygun olma

KVKK'nin 4 üncü maddesinin ikinci fıkrasının (a) bendinde düzenlenen bu ilke, iki unsurdan oluşmaktadır: Bunlardan birincisi kişisel verilerin hukuka uygun olarak işlenmesi, ikincisi ise dürüstlük kurallarına uygun işlenmesidir.

Kişisel verilerin hukuka uygun olarak işlenmesi ilkesi, verinin işlenmesi aşamasında, kanun ve diğer hukuki düzenlemelerde yer alan ilkelere göre hareket edilmesi gerekliliğini ifade etmektedir. Bir başka deyişle bu ilke ile kişisel verinin işlenmesi, açık rıza veya diğer hukuka uygunluk hâllerinden birinin varlığının yanında sair mevzuata da aykırı olunmaması gerekliliğine vurgu yapılmaktadır[179].

GDPR'ın 5 inci maddesinin birinci fıkrasının (a) bendinde de kişisel verilerin hukuka uygun bir şekilde işlenmesi gerektiği belirtilmekte, ancak "hukuka uygun işleme" ifadesinin tanımı yapılmamaktadır. Bununla birlikte, GDPR'ın 6 ncı maddesi

---

[177] Nafiye, Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", *Kişisel Verileri Koruma Dergisi*, Cilt: 1, Sayı: 1, (2019): 48.
[178] Kuyumcu, *6698 Sayılı Kişisel Verilerin…,* 51.
[179] Küzeci, *Kişisel Verilerin Korunması*, 229.

"İşlemenin hukuka uygunluğu" başlığı altında hukuka uygun sayılacak işleme durumlarını göstermektedir. GDPR'ın "*Başlangıç*" bölümünde yer alan 40 ıncı maddesinde ise kişisel veri işlemenin hukuka uygun olması için ilgili kişinin rızasına veya GDPR ve atıf yapılan diğer AB ya da üye ülke hukuki düzenlemelerinde tanımlanan başka meşru sebeplere dayandırılması gerektiği vurgulanmıştır. Bu çerçevede GDPR'a göre hukuka uygunluk, 6 ncı maddede belirtilen ilgili kişinin rızası, yasal yükümlülüklerin yerine getirilmesi gibi dayanakların varlığıyla ilişkilidir[180].

İkinci olarak kişisel verilerin işlenmesine ilişkin her türlü eylemde, dürüstlük kuralına uyulması bir gerekliliktir. Bununla birlikte bu kurala göre hareket etmenin kapsamını belirleyebilmek güçtür. Keza dürüstlük ifadesi ile kastedilen her durum somut olaya göre değişebilmektedir[181].

Literatürde çeşitli tanımlamalar yapılmakla birlikte, dürüstlük kuralı *"orta zekalı, normal, makul kimselerin, toplum içerisinde karşılıklı güvene, ahlaka ve dürüstlüğe dayalı davranışları sonunda meydana gelmiş ve toplum ihtiyaçları ile iş hayatının ihtiyaçlarına cevap veren, bu nedenle de herkesçe benimsenen yazılı olmayan kurallar bütünüdür[182]"* şeklinde ifade edilmiştir. Ayrıca Türk hukukunda, TMK'nin *"Dürüst davranma"* başlıklı 2 nci maddesinde; *"Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır. Bir hakkın açıkça kötüye kullanılmasını hukuk düzeni korumaz."* hükmü ile dürüstlük kurallarına uygunluk kavramına yer verilmiştir.

Kişisel verilerin korunması kapsamında değerlendirildiğinde; kişisel veriler işlenirken hakkın kötüye kullanılmasına ilişkin yasağa, yani dürüstlük kuralına uyulması bir zorunluluktur. Ayrıca bu kurala göre veri işleme konusunda, kişilerin kendilerine izin veren veya emir içeren hukuk normlarına dayanarak gerçekleştirdikleri eylemlerde,

---

[180] Nafiye, Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında…": 48.
[181] Küzeci, *Kişisel Verilerin Korunması*, 229.
[182] Bilge, Öztan, *Medeni Hukukun Temel Kavramları*, 38. Bası (Ankara: Turhan Kitabevi, 2013): 173.

bu hukuk normunun amacı doğrultusunda mümkün olan en az seviyede verinin işlenmesi, ilgili kişilerin öngöremeyeceği biçimde hareket edilmemesi gerekmektedir[183]. Örneğin; gönderici tarafın bir sendika ya da siyasi parti olduğu posta gönderilerinde, PHS'nin gerekli olmadığı halde, alıcının da bu sendika ya da siyasi partiye üye olduğu ya da ilgisinin bulunduğuna yönelik işleme faaliyetinde bulunması uygun olmayacaktır.

Diğer taraftan dürüstlük kuralına uygunluk ile şeffaflık ilkesinin birbiri ile bağlantısı bulunmaktadır. Nitekim KVKK'de şeffaflık ilkesine açıkça yer verilmese de GDPR'ın 5 inci maddesinin birinci fıkrasının (a) bendinde hukuka uygunluk, adillik ilkelerinin yanında şeffaflık ilkesine de yer verilmiştir[184]. İşlemenin oldukça şeffaf olmasını sağlayan şey, veri sahibinin kendisiyle ilgili veri işleme süreci ve bu işlemenin temel özellikleri hakkında gerçek bir bilgiye sahip olmasıdır[185].

Bu ilkenin uygulanmasına ilişkin bir örnek mahiyetinde olmak üzere KVK Kurulu tarafından verilen bir kararda, sadakat programı kullanmakta olan bir havayolu taşımacılık şirketi tarafından (veri sorumlusu), kullanıcı ismi ve parolasını değiştirmek isteyen ilgili kişinin kimlik belgesinin fotoğrafının talep edilmesinin, veri işleme şartlarına uygun olmayan bir işleme faaliyeti olması sebebiyle, hukuka uygunluk ilkesine aykırı olduğu değerlendirilmiştir. Ayrıca veri sorumlusunca, ilgili kişinin kimlik görüntüsünün saklanmadığı yönünde verilen yanlış cevap nedeniyle; işleme faaliyetinin, şeffaf olmadığı ve bu bağlamda dürüstlük kuralına da aykırı işlem gerçekleştirildiği kanaatine ulaşılmıştır[186].

---

[183] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*.
[184] Anı, *Kişisel Verilerin İşlenmesi ve…,* 90.
[185] Gianclaudio, Malgieri, "The Concept of Fairness in the GDPR: : A Linguistic and Contextual Interpretation", *FAT* '20: Conference on Fairness, Accountability, and Transparency*, (2020).
[186] Kişisel Verileri Koruma Kurulu Kararı, 01.10.2019 günlü, 2019/294 sayılı karar.

2.3.2 Doğru ve gerektiğinde güncel olma

Doğru ve gerektiğinde güncel olma ilkesi, temelde iki boyuta sahiptir: İlk olarak söz konusu ilkeye göre kişisel verisi işlenen ilgili kişinin verileri, hatalı veya yanlış değil, doğru bir biçimde işlenmelidir. Yani ilgili kişi hakkındaki kayıtlar, doğru bilgileri içermeli aynı zamanda da gerçeğe uygun şekilde işlenmelidir. İkinci olarak ilgili kişiye ait kişisel veriler, ihtiyaç duyulduğu anda ya da verinin kullanılacağı vakitte güncel olmalıdır. Bir başka ifade ile zamanla değişikliğe uğrayabilen veriler için gerekli güncelleme işlemleri yapılmalıdır. Kişisel verilerin eski hali değil, mevcut haldeki güncelliği korunmalıdır[187].

Söz konusu ilke temelde kişisel verilerin ait olduğu bireyin yanlış temsil edilmemesini ve yanlış temsil edilmenin sonuçlarından korunmasını sağlamayı amaçlamaktadır. Nitekim AİHM'nin bir kararında, bir avukatın öğrenci olduğu dönemde yazmış olduğu mektuplar sebebiyle mahkûm edilmesi hakkında elli yıldan daha uzun süre saklanan kişisel bilgilerin doğru saklanmamasının avukatın itibarına zarar verdiği gerekçesiyle AİHS'nin "Özel ve aile hayatına saygı hakkı" başlıklı 8 inci maddesinin ihlal edildiğine karar verilmiştir[188].

Doğru ve gerektiğinde güncel olma ilkesi, GDPR'ın 5 inci maddesinin birinci fıkrasının (d) bendinde genel veri koruma ilkelerinden biri olarak şu şekilde belirtilmektedir: *"Kişisel veriler (...) doğrudur ve gerektiğinde güncel tutulur; işlenme amaçları göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeksizin kalıcı olarak silinmesi veya düzeltilmesinin sağlanmasıyla ilgili makul tüm adımlar atılmalıdır ("doğruluk")."*

---

[187] Egemen, "Kişisel Verilerin İşlenmesinde…": 119.
[188] Aydın, Akgül, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, (İstanbul: 2014).

Doğru ve gerektiğinde güncel olma ilkesinin, verilerin doğruluğu ile güncelliğinin saptanması ve denetlenmesi bağlamında verilere erişim hakkı ve verilerin ilgili kişi tarafından düzeltilmesi hakkı ile yakın bir ilişkisi vardır[189].

Türk hukukunda da KVKK'nin "Genel ilkeler" başlıklı 4 üncü maddesinin ikinci fıkrasının (b) bendinde; kişisel verilerin doğru ve gerektiğinde güncel olması gerektiğine yer verilmiştir. Bu kapsamda veri sorumlusu, kişisel verilerin doğru ve güncel bir şekilde tutulması için gerekli tüm tedbirleri almakla yükümlüdür. Ayrıca KVKK'nin 11 inci maddesinin birinci fıkrasının (d) bendinde yer alan; *"Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; … Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme… hakkına sahiptir."* hükmü, ilgili kişilere, kendileri hakkında doğru olmayan kişisel verilerin düzeltilmesini talep hakkı tanımıştır[190].

Posta sektöründe de kişisel verilerin doğru ve güncel olması kullanıcı hakları ve kullanıcı memnuniyeti açısından büyük önem taşımaktadır. Doğru ve güncel veriler, posta hizmetlerinin etkin ve güvenli bir şekilde yürütülmesini sağlamaktadır. Örneğin; kullanıcıların adres bilgilerinin doğru ve güncel olması, gönderilerin doğru yerlere ulaşmasını sağlamaktadır. Adres bilgisinin doğru ve güncel olmaması gibi aksi bir durumda ise bir kişiye gönderilen tebligatın tebliğ edilememesi ya da yanlış kişiye tebliğ edilmesi, kişinin maddi/manevi zararına sebebiyet verebilecek durumlar olarak ortaya çıkabilmektedir[191].

---

[189] Aygün, *Elektronik Haberleşme Sektörüne İlişkin…,* 16.
[190] Seda, Uzunal, *Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması*, (Yüksek Lisans Tezi, Marmara Üniversitesi, 2023): 49; Anı, *Kişisel Verilerin İşlenmesi ve….*
[191] Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Kanununa İlişkin …": 66.

2.3.3 Belirli, açık ve meşru amaçlar için işlenme

Kişisel verilerin korunması alanında temel ilkelerden biri verilerin toplanması ve işlenmesi amacının sınırlandırılmasıdır. Bu ilke, kişisel veri işleme faaliyetlerinin ilgili kişi tarafından açık ve net bir biçimde anlaşılır olmasını, kişisel veri işlemenin hangi hukuki işleme şartına dayanarak gerçekleştirildiğinin tespit edilmesini, bu işleme faaliyeti ile bu faaliyetin gerçekleştirilmesi amacının belirliliğini sağlayacak şekilde ortaya konulmasını sağlamaktadır. Ayrıca, veri sorumlusunun veri işleme amacını açık ve kesin olarak belirlemesini ve bu amacın meşru olmasını zorunlu kılmaktadır[192]. Bu ilkenin amacı, veri sorumlularının kişisel veri işlemesi faaliyetinde en baştan itibaren açık ve net olması ile amaçların bireylerin makul beklentileriyle uyumlu olmasını sağlamaktır. İlkenin veri sorumlularınca değerlendirilmesi ve tam olarak uyulması, verilerin işlendikleri amaçla sınırlı olma ilkesi ve hesap verebilirlik konularında da olumlu etkileri olacaktır[193].

GDPR'ın 5 inci maddesinin birinci fıkrasının (b) bendinde ilke şu şekilde belirtilmektedir: *"kişisel veriler (...) belirtilen, açık ve meşru amaçlarla toplanır ve bu amaçlara uygun olmayacak şekilde sonradan işlenmez; kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları veya istatistiki amaçlarla sonraki işleme, 89(1) maddesi uyarınca, baştaki amaçlara uygun olmadığı yönünde değerlendirilmez ("amacın sınırlandırılması")"*. Buna göre veri sorumluları, yeterli güvenlik önlemlerinin mevcut olduğu durumlarda, başlangıçtaki amaçlarla uyumlu oldukları düşünüldüğünde, kamu yararına arşivleme amaçları, bilimsel veya tarihsel araştırma amaçları veya istatistiksel amaçlar için daha fazla işleme yapabilmektedir. Daha fazla işleme faaliyetinin gerçekleştirilmesi ise yalnızca yeni işleme amacının asıl

---

[192] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*.
[193] An Coimisiún um Chosaint Sonraí (İrlanda Veri Koruma Kurumu), *Quick Guide to the Principles of Data Protection*. (2019).

amaç ile uyumsuz olmadığı durumlarda uygundur[194]. Diğer yandan madde üç temel gereklilik içerir:

İlk gereklilik, amacın belirli olmasıdır. Buradaki "belirli" kavramı, veri işleme sürecine başlamadan önce, amacın net bir şekilde ortaya konulmasını ifade etmektedir. Bir başka ifade ile amacın veri toplama işleminden önce belirlenmiş olması ve bu amacın kapsamının hangi veri işleme faaliyetlerini kapsadığı, hangilerini kapsamadığının açıkça belirlenmesi gerekmektedir. Eğer kişisel veriler birden fazla amaç için toplanıyorsa, her bir amaç ayrı ayrı belirlenmelidir[195].

İkinci gereklilik, amacın veri işlenmesi sırasında açık bir şekilde ifade edilmesidir. Bu, ilgili kişiye amacın net bir şekilde iletilmesi ve her bireyin amacın kapsamını aynı biçimde anlamasını sağlamaktadır. Amacın açıklığı, veri sahibine yapılan bir bildirim veya denetleyici bir otoriteye yapılan bir bildirimin ardından da sağlanabilmektedir[196].

Üçüncü gereklilik ise amacın meşru olmasıdır. Bu gereklilik yalnızca işleme için geçerli olan yasal dayanakları değil, aynı zamanda tüm veri koruma mevzuatını ve genel hukuki düzenlemeleri de kapsamaktadır. Buna göre, belirli bir amaç için toplanan kişisel veriler uyumlu amaçlar için kullanılmalı veya farklı bir yasal temel altında işlenmelidir[197]. Ayrıca bu kavram, yürürlükteki yönetmelikler, gelenekler ve sözleşmesel yükümlülükler gibi diğer hukukî ve toplumsal hükümleri de dikkate almayı gerektirmektedir[198].

---

[194] Juanita, Goicovici, *Granularity And Specificity Of Consent And Implications Thereof For The Data Controller In The Light Of The Principle Of 'Purpose Limitation'*, (2022): 53.
[195] Hannes, Westermann, *Change of Purpose: The effects of the Purpose Limitation Principle in the General Data Protection Regulation on Big Data Profiling*, (Yüksek Lisans Tezi, Lund University, 2018).
[196] Avrupa Komisyonu, *Article 29 Data Protection Working Party (Çalışma Grubu), No. 203 (2013). Opinion 03/2013 on purpose limitation*, (2013).
[197] Catherine, Jasserand, *Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?,* (2018).
[198] Hannes, Westermann, *Change of Purpose: The effects….*

KVKK'nin "Genel ilkeler" başlıklı 4 üncü maddesinin ikinci fıkrasının (c) bendinde de kişisel verilerin belirli, açık ve meşru amaçlar için işlenmesi gerektiği yer almaktadır.

Diğer yandan, Evrensel Posta Sözleşmesi'nin "kişisel verilerin işlenmesi" başlıklı 10 uncu maddesinin birinci fıkrasına göre kullanıcılara ilişkin kişisel veriler yalnızca yürürlükteki ulusal mevzuata uygun olarak toplanma amaçları doğrultusunda kullanılabilmektedir. Örneğin, PHS'ler tarafından, çağrı merkezleri aracılığıyla posta kullanıcılarına hizmet sunulmakta ve kullanıcıların birtakım kişisel verileri işlenebilmektedir. Bu işlenen veriler, kullanıcı taleplerine hızlı ve etkili bir biçimde cevap vererek kullanıcı şikâyetlerinin çözümlenmesi ve hizmet kalitesinin artırılması için kullanılabilmektedir. Bununla birlikte, posta sektöründe bu verilerin kullanıcılara yeni hizmetler ve teklifler hakkında bilgi vermek suretiyle reklam ve pazarlama amacıyla da kullanıldığı görülmektedir. Ancak bu tür veri işleme faaliyetlerinin, toplanma amacına uygun olmadığı ve hizmetin sunumu için gerekli olmadığı kabul edildiğinde, bu yönde bir işleme faaliyeti için ilgili kişinin açık rızasının aranmasının gerekli olacağı düşünülmektedir. Ayrıca, PHS'ler tarafından kullanıcıların verileri işlenirken bu işlemin posta hizmetinin sunumu için gerekli olduğunun belirtilmesinin yeterli olmadığı, işleme amacının daha net bir biçimde ortaya konulması gerektiği değerlendirilmektedir.

2.3.4 İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma

Kişisel verilerin korunması alanındaki ilkelerden biri kişisel verilerin "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması" ilkesidir. Bu ilke, veri sorumlularının, verilerin ilk toplanma aşamasından itibaren ve işleme boyunca yalnızca işleme amaçlarını gerçekleştirmek için gerekli olan verilerle sınırlı kalmalarını gerektirmektedir[199]. Veri sorumluları yalnızca gerçekten ihtiyaç duydukları kişisel

[199] Paul, De Hert ve Juraj, Sajfert, "The Fundamental Right To Personal Data Protection In Criminal Investigations And Proceedings: Framing Big Data Policing Through The Purpose Limitation and Data

verileri toplamalı ve bu verileri yalnızca ihtiyaç duydukları süre boyunca muhafaza etmelidir[200].

GDPR'ın 5 inci maddesinin birinci fıkrasının (c) bendinde ilke şu şekilde belirtilmektedir: *"kişisel veriler (...) işlenme amaçlarına uygun, işlenme amaçlarıyla ilgili ve bunlarla sınırlı olmalıdır ("veri minimizasyonu")".* GDPR kapsamında bu ilke, kişisel veriler işlenirken yalnızca gerekli verilerin işlenmesini ve bunların en az seviyede tutulması gerekliliğinin altını çizmektedir[201].

Buna göre söz konusu ilkenin üç temel gerekliliği içerdiği görülmektedir: İlk olarak, veriler, güdülen amaç açısından yeterli olmalıdır. Yeterlilik, somut olaya göre, çok ya da az verinin işlenmesini gerektirebilir. Örneğin; belirli bir veri eksikliği, bir veri setinin yararlılığını ve bu veri seti üzerinde yapılan analizlerin doğruluğunu sınırlayabilir. İkinci olarak, kişisel veri, amaç ile alakalı olmalıdır. Bir başka deyişle yalnızca amaca uygun veriler işlenebilir[202]. Üçüncü olarak ise GDPR, verilerin gerekli olan veri ile sınırlı olmasını şart koşmaktadır. Yani veri sorumluları, belirtilen amacı yerine getirmek için gereken en az miktarda kişisel veriyi belirlemelidir. Ulaşılması gereken doğru sonuçlara daha az kişisel veri işlenerek elde edilebiliyorsa, kişisel verilerin işlenmesi gerekli olarak kabul edilmemektedir[203]. Örneğin, yalnızca haber bülteninin teslim edilmesi amacıyla kişisel verilerin toplanması gibi bir durumda, abonelerin adlarına

---

Minimisation Principles of The Directive (EU) 2016/680", *Brussels Privacy Hub Working Paper,* Cilt: 7, Sayı: 31, (2021): 13.

[200] Rekabet Kurumu, *Dijital Dönüşümün Rekabet Hukukuna Yansımaları*, (2023): 86.

[201] Uzunal, *Elektronik Haberleşme Sektöründe…,* 51.

[202] Örneğin, bir e-ticaret aracı hizmet sağlayıcısının, kullanıcıların satın alma teklifleri için doğum günü bilgisini talep etmesi halinde, bu verinin büyük bir ihtimal ile (öneriler astrolojik temelli olmadıkça) ilgili olmayacağı söylenebilmektedir. Bu nedenle sadece veri toplamak amacıyla veri biriktirmenin önüne geçilmektedir.

[203] Asia J., Biega, Peter, Potash, Hal, Daumé III, Fernando, Diaz ve Michèle, Finck, "Operationalizing the Legal Principle of Data Minimization for Personalization", *In Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR '20), July 25–30, 2020, Virtual Event. China, ACM, New York, NY, USA*, (2020).

ve e-posta adreslerine ihtiyaç duyulabilse de iş ünvanlarının bilinmesine gerek yoktur[204].

KVKK'nin "Genel ilkeler" başlıklı 4 üncü maddesinin ikinci fıkrasının (ç) bendinde; kişisel verilerin "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü" olması gerektiğine yer verilmiştir. Bu kapsamda veri sorumlusu tarafından işlenen veriler, işleme amacının gerçekleştirilebilmesine elverişli olmalıdır. Ayrıca işleme amacıyla ilgisi bulunmayan veya amacın gerçekleştirilebilmesi için gerekli olmayan verilerin işlenmemesi gerekir[205].

2.3.5 İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

Kişisel verilerin, öngörülen ya da işlenme amacı için gerekli olan süre kadar saklanması, GDPR'ın 5 inci maddesinin birinci fıkrasının (e) bendinde şu şekilde belirtilmektedir: *"kişisel veriler (...) veri öznelerinin, yalnızca kişisel verilerin işlenme amaçlarının gerektirdiği sürece kimliğinin belirlenmesini sağlayan bir şekilde tutulur; kişisel veriler, veri öznesinin hakları ve özgürlüklerinin güvence altına alınması için bu Tüzük'ün gerektirdiği uygun teknik ve düzenlemeye ilişkin tedbirlerin uygulanmasına tabi olmak kaydıyla, 89(1) maddesi uyarınca yalnızca kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla ya da istatistiki amaçlarla işlendikleri sürece, daha uzun sürelerle depolanabilir ("depolamanın sınırlandırılması")."*

Bu ilke KVKK'de ise "Genel ilkeler" başlıklı 4 üncü maddesinin ikinci fıkrasının (d) bendinde ifade bulmaktadır. Gereken önlemlerin alınması, veri işleyenin sorumluluğunda bulunmakla birlikte; işlenecek veriler ilgili mevzuatta öngörülen veya

---

[204] İsmail, Özkan, "Data Protection Principles: The 7 Principles Of GDPR Explained", (2024).
[205] Uzunal, *Elektronik Haberleşme Sektöründe…,* 51.

işleme amacı için gereken süre kadar muhafaza edilebilir. Sürenin sona ermesi durumunda verilerin imhasının gerçekleştirilmesi gerekir[206]. Bununla birlikte kişisel veriler, işlenme amacının veya mevzuatta öngörülen sürenin sona ermesi halinde veri sahiplerinin kimliğinin belirlenmesinin mümkün olmayacağı şekilde, bir başka ifade ile anonim hale getirilerek saklanabilir. Bu sürenin uzunluğu somut bir değerlendirmeye bağlıdır[207].

Görüleceği üzere, GDPR hükmü ile KVKK'den farklı olarak kişisel verilerin, belirli bir amaç için gerekli olandan daha uzun bir süre saklanmasına bir istisna getirilmektedir. Buna göre GDPR'ın 89 uncu maddesinin birinci fıkrasında öngörülen, kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda kişisel veriler daha uzun bir süre depolanabilmektedir. Bununla birlikte bu amaçlar, veri sahiplerinin kimliğinin belirlenmesine izin vermeyen veya artık izin vermeyen daha fazla işlemle yerine getirilebiliyorsa, amaçlar bu şekilde yerine getirilmelidir. Kişinin belirli olan kimliğinin silinmesi mümkünse, meşru depolama amacı tehlikeye atılmadığı sürece belirli bir kişinin kimliğini gizleme yükümlülüğü uygulanmaktadır. Bu gizleme, takma ad kullanılmasını gerektirebilmektedir[208].

Mevzuatta öngörülen süreye ilişkin olarak posta sektöründe de bazı düzenlemeler bulunmaktadır. PHSİY'nin *"Kullanıcı şikâyetleri çözüm mekanizması"* başlıklı 22 nci maddesinin ikinci fıkrasında yer alan*; "Kullanıcı şikâyetleri ve bu şikâyetlere verilen cevaplar ile ilgili süreç hizmet sağlayıcılar tarafından kayıt altına alınır ve bu kayıtlar güvenlik tedbirleri alınarak asgari iki yıl muhafaza edilir."* hükmü ile kullanıcı şikâyetleri ile bunlara verilen cevapların muhafaza süresi düzenlenmiştir.

---

[206] Aygün, *Elektronik Haberleşme Sektörüne İlişkin…,* 18.
[207] Tanja Kammersgaard, Christensen, "Pre-installed cameras in vehicles—New technology from a data protection law perspective", *Computer Law & Security Review*, Cilt 53, (2024): 8.
[208] Mikuláš, Čtvrtník, *The Right to (Not) Be Forgotten, Right to Know, and Model of Four Categories of the Right to Be Forgotten,* Palgrave Macmillan, Cham, (2023).

Diğer yandan Güvenlik Usul ve Esaslarının *"Posta gönderilerinin kabulü ve teslimi aşamasında yapılacak işlemler"* başlıklı 4 üncü maddesi gereğince; PHS'ler tarafından haberleşme gönderileri dışındaki posta gönderilerinin kabulü sırasında gönderici ve/veya alıcının gerçek kişi olması durumunda; göndericinin kimlik bilgileri (isim, soy isim, T.C. kimlik bilgisi, pasaport numarası gibi), açık adres ve telefon numarası bilgisi, gönderinin üzerindeki gönderici olarak belirtilen kişiden farklı bir kişi tarafından PHS'ye teslim edilmesi halinde bu kişinin kimlik bilgileri ile açık adres ve telefon numarası bilgisi, alıcının ismi, soy ismi ve açık adres bilgisi kayıt altına alınmaktadır. Gönderici ve/veya alıcının tüzel kişi olması durumunda ise gönderici tüzel kişinin tam ünvanı, vergi kimlik numarası ya da mersis numarası, açık adres ve telefon numarası bilgisi, tüzel kişinin gönderisini göndermeye yetkili gerçek kişinin kimlik bilgileri ile adres ve telefon numarası bilgisi, alıcının adı-soyadı (alıcı tüzel kişiyse ünvanı ve açık adres bilgisi) kayıt altına alınmaktadır. Ayrıca gönderinin cinsi, gönderinin farklı ürünler içermesi halinde her ürün için cins bilgisi ve göndericinin kimlik bilgisi ile gönderi içeriğinin kontrolünü yapan PHS personelinin kimlik bilgisi kayıt altına alınarak, gerektiği durumda ilgili mercilere sunulması amacıyla PHS'ler tarafından en az iki yıl süreyle bu verilerin gizliliği sağlanarak muhafaza süresi düzenlenmiştir. Bununla birlikte aynı maddede, PHS ile yapılan sözleşme kapsamında fatura veya irsaliyeyle taşıttırılan posta gönderileri için gönderi cinsine dair bilgilerin kayıt altına alınmayabileceği belirtilmiştir.

Yine Güvenlik Usul ve Esaslarının 6 ncı maddesinin ikinci fıkrası uyarınca PHS'ler tarafından, gönderilerin kabul edildiği merkezlerde gönderilerin kabul-teslim, depolama ve yükleme işlemlerinin yapıldığı yerin açık biçimde görüntülenebildiği açı, mesafe ile en az iki megapiksel çözünürlükteki bir kamera sisteminin kurulması ve bu kamera kayıtlarının, ihtiyaç duyulduğunda ilgili makamlara sunulması amacıyla asgari olarak bir ay süreyle saklanması gerektiği ifade edilmiştir.

Anılan mevzuat hükümleri doğrultusunda, bu verilerin muhafazasının PHS açısından bir yükümlülük teşkil ettiği anlaşılmaktadır. Ancak, muhafaza sürelerinin sona ermesi

durumunda bu verilerin ne şekilde imha edileceğine dair yükümlülük içeren bir özel bir düzenlemeye yer verilmemiştir. Bu kapsamda, KVKK'nin 7 nci maddesinin birinci fıkrasının uygulanması ve bu verilerin işlenme süresinin bitimiyle birlikte imha edilmesi gerekliliği gündeme gelecektir.

Öte yandan, veri sahibi tarafından muhafaza süresi içerisinde verilerin silinmesi PHS'den talep edilirse, PHS'nin bu talebi reddetmesinin herhangi bir ihlal teşkil etmeyeceği değerlendirilmektedir. Nitekim KVK Kurulu'nun 22.06.2021 tarihli ve 2021/603 sayılı kararında, PHK'nin 7 nci maddesi uyarınca PHS tarafından muhafaza edilmesi gereken verilere ilişkin veri sahibinin bu verilerin imhasına yönelik talebinin, işleme sebebinin ortadan kalkmaması nedeniyle yerine getirilmemesinde bir hukuka aykırılık oluşmadığına hükmedilmiştir[209].

2.4 Posta Sektöründe Kişisel Verinin İşlenmesinde Hukuka Uygunluk Nedenleri

Kişisel verilerin işlenmesinde açık rıza ve açık rızayı gerektirmeyen haller, KVKK'de düzenlenmiş olup anılan hükümler posta sektöründe işlenen kişisel veriler için de geçerlidir. Söz konusu başlıklar, mümkün olduğu ölçüde posta sektörüyle ilişkilendirilerek açıklanmaktadır.

2.4.1 Kullanıcının açık rızasının olması

KVKK'nin 5 inci maddesinin birinci fıkrası gereğince kişisel veriler esas olarak, ilgili kişilerce verilmiş bir açık rıza olmadığı müddetçe veri sorumlusu tarafından işlenememektedir. KVKK'nin 3 üncü maddesinin birinci fıkrasında açık rıza, *"belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* şeklinde tanımlanmıştır.

---

[209] Kişisel Verileri Koruma Kurulu Kararı, 22.06.2021 günlü, 2021/603 sayılı karar.

İlgili tanım uyarınca açık rızanın 1.3.6 başlığı altında detaylıca açıklanan üç öğesi bulunmaktadır ve bu öğelerin posta hizmetleri için ele alınış biçimleri şu şekildedir: Öğelerden birincisi "belirli bir konuya ilişkin olma"dır. Buna göre, posta kullanıcısından alınacak rızanın genel nitelikte olmaması ve belirli bir konuya ilişkin verilmesi gerekmektedir. Ayrıca kullanıcının rızasının istendiği konu, kullanıcıya net bir biçimde açıklanmalıdır. Bu kapsamda, PHS'ler tarafından posta kullanıcısından, bütün verilerinin işlenmesinin kabul edildiğine dair alınan rıza, hukuken geçerli olmayacaktır[210].

İkinci olarak açık rızanın "bilgilendirmeye dayanan" rıza olması gerekmektedir. Posta kullanıcısı bilgilendirilirken anlaşılmayan ifadeler kullanılmamalıdır. Söz konusu bilgilendirmenin ise işleme faaliyetinden önce yahut en geç işleme anında yapılması gerekmektedir[211].

Üçüncü olarak açık rızanın "özgür iradeyle" verilmesi gerekir. Posta kullanıcısı rızasını baskı altında olmaksızın özgür iradesiyle vermelidir. Özgürce verilen rıza, veri sahibi olan posta kullanıcısı ile veri sorumlusu PHS arasında bir güç dengesizliği içermemelidir. Ayrıca verilen rıza koşulsuz, ayrıntılı ve kullanıcıya zarar vermeyecek nitelikte olmalıdır[212].

Posta sektöründe belirli verilerin işlenmesinde açık rızaya ihtiyaç duyulduğunun en belirgin örneği, PHK'nin *"Tanımlar"* başlıklı 3 üncü maddesinin birinci fıkrasının (a) bendinde yer almaktadır. Buna göre; *"adres bilgi kayıt sistemi: 25/4/2006 tarihli ve 5490 sayılı Nüfus Hizmetleri Kanunu ve ilgili mevzuatı saklı kalmak kaydıyla, (…) kişilerin rızası alınarak gerçek ve tüzel kişiler ile kamu kurum ve kuruluşlarına ait fiziki ve elektronik adreslerin, reklam ve tanıtım amacıyla PTT hizmetlerinden*

---

[210] Kişisel Verileri Koruma Kurumu, "Açık Rıza Alırken Dikkat Edilecek Hususlar".
[211] Kişisel Verileri Koruma Kurumu, *Açık Rıza*, 6.
[212] Alaattinoğlu, "Rethinking Explicit Consent…": 163.

yararlananlara ücret karşılığı kullandırılmasına yönelik olarak oluşturulan PTT'ye ait veri tabanı" olarak adres bilgi kayıt sistemi tanımlanmıştır. Tanımda posta hizmetinin sunulması amacıyla işlenen fiziki ve elektronik adreslerin, reklam ve tanıtım amacıyla PTT'nin hizmetlerinden yararlananlara kullandırılması için kişilerin açık rızasına ihtiyaç duyulduğu belirtilmiştir.

Diğer yandan Teslimat Usul ve Esaslarının 8 inci maddesinin ikinci ve üçüncü fıkrası uyarınca alıcıdan kaynaklı nedenlerle gönderinin teslim edilememesi halinde gönderi, alıcının onayı alınarak en yakın kilitli teslimat dolabına bırakılabilmektedir. Bu onayın diğer gönderiler için de geçerli olması için alıcıdan ayrıca onay alınması gerekmektedir. Hükümde "onay" şeklinde ifade edilen kavramın henüz gönderinin teslim edilmediği safhada alınması nedeniyle "icazet" mahiyetinde değil esasen "rıza" anlamı taşıdığı değerlendirilmektedir. Burada alıcının gönderinin teslim edileceği yer hususundaki talebine ilişkin bir kişisel verisi işlenmekte olup bu konuya ilişkin açık rızanın gönderinin teslimi anında alınmasının KVKK ile de uyumlu olduğu görülmektedir.

2.4.2 Kanunlarda açıkça öngörülmesi

Kişisel verilerin hukuka uygun bir şekilde işlenmesini sağlayan bir diğer hal, veri işlemenin kanunlarda açık bir şekilde belirtilmiş olmasıdır. Kişisel verilere ilişkin ortaya çıkan koruma, tüm temel hak ve hürriyetlerde olduğu gibi mutlak bir hak olarak görülmemekte olup Anayasa çerçevesinde başka temel hak ve hürriyetler lehine sınırlandırılabilmektedir[213]. Nitekim T.C. Anayasası'nın *"Temel hak ve hürriyetlerin sınırlanması"* başlıklı 13 üncü maddesinde yer alan; *"Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar,*

[213] Metin, Turan, *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması*, 2. Baskı, (Ankara: Seçkin Yayıncılık, 2019): 79.

Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz." hükmü gereği bu hürriyetler ancak kanunla ve özel sınırlama sebeplerine dayanılarak sınırlandırılabilmektedir.

Diğer yandan T.C. Anayasası'nın 20 nci maddesinde kişisel verilerin ancak kanunda öngörülen hallerde ya da kişinin açık rızasıyla işlenebileceği hükme bağlanmıştır. Hükmün lafzından da anlaşılacağı üzere temel hak ve özgürlükler, kanun hükmünde kararname ya da yönetmelik, tebliğ, karar gibi ikincil düzenleyici işlemler ile düzenlenememekte ya da sınırlandırılamamaktadır[214].

Bu kapsamda söz konusu madde ile bu hakkı ilgilendiren düzenlemelerin hukuki çerçevesi çizilmiş olup anlaşılabilir, açık, kişilerin özel hayatlarını ilgilendiren ve haklarını kullanabilmelerine elverişli olan kişisel veri, bilgi ve belgelerin yetkili makamların keyfî müdahalelerine karşı korunması amaçlanmıştır[215].

Anayasal düzenlemeye benzer olarak KVKK'nin 5 inci maddesinin ikinci fıkrasının (a) bendi uyarınca, kişisel verilerin, kanunlarda açıkça öngörülmesi halinde veri sahibinin açık rızası olmaksızın işlenebileceği hüküm altına alınmıştır. "Kanunda açıkça öngörülmüş olma" ifadesiyle hangi veri sorumlusu tarafından, hangi kişisel verilerin hangi amaç ile işlenebileceğinin ilgili hükümde açık bir şekilde düzenlenmiş olması ve işlenecek olan veri kategorilerinin, işleme amaçlarının ve veri gruplarının ilgili yasa hükmünden veya onun atıf yapmış olduğu ikincil mevzuattan anlaşılması gerekmektedir[216]. GDPR'da ise kanunlarda açıkça öngörülme hali bir hukuka uygunluk sebebi olarak düzenlenmemiştir.

---

[214] Kişisel Verileri Koruma Kurumu, *Kanunlarda Öngörülme Kişisel Veri İşleme Şartına İlişkin 05.08.2024 tarihli Bilgi Notu*.
[215] Anayasa Mahkemesi Kararı, 28.09.2017 günlü, E:2016/125, K:2017/143 sayılı karar.
[216] Kuyumcu, *6698 Sayılı Kişisel Verilerin…,* 60-61.

Türk hukukunda veri sahibinin rızasına başvurulmaksızın kişisel verilerin kayıt altına alınmasına; polis tarafından bir soruşturma kapsamında şüpheliden parmak izinin alınması ve 28.03.2013 tarihli ve 28835 sayılı Resmî Gazete'de yayımlanan 6502 sayılı Tüketicinin Korunması Hakkında Kanun (TKHK)'un ilgili alt düzenlemeleri uyarınca mesafeli satış sözleşmelerinin saklanmasının zorunlu olması örnek olarak gösterilebilmektedir[217].

Posta hizmetlerinin sunumunda ise PHK'de kayıtlı gönderi tanımına yer verilmiştir. Buna göre kayıtlı gönderi; *"kabulünden teslimine kadar kayda tabi tutulan gönderiyi"* ifade etmekte olup bu tanım kapsamında, dolaylı olarak, anılan gönderilerin PHS tarafından kayıt altına alınması zorunluluğuna işaret edilmektedir. Dolayısıyla posta sektörüne özel olarak, kayıtlı mahiyetteki gönderilerin de rıza aranmaksızın kişisel verilerin kayıt altına alınmasına örnek teşkil ettiği söylenebilecektir.

2.4.3 Fiili ve hukuki imkânsızlık nedeniyle açık rızanın verilememesi

Fiili imkânsızlık nedeniyle rızasını açıklaması mümkün olmayan halde bulunan veya rızasına hukuki bir geçerlilik tanınmayan bireyin kendisinin veya başka birinin yaşamı veya vücut bütünlüğünün korunması için işleme faaliyetinin gerekli olması, GDPR'ın 6 ncı maddesinin birinci fıkrasının (d) bendinde, KVKK'nin ise 5 inci maddesinin ikinci fıkrasının (b) bendinde düzenlenmiştir. Bu düzenlemelere göre verilerin işlenmesi, veri sahibinin veya başka bir gerçek kişinin yaşamı için hayati olan bir çıkarın[218] korunmasının gerekli olduğu durumlarda da yasal olarak kabul edilmelidir[219]. Kişisel verilerin başka bir gerçek kişinin hayati çıkarına dayalı olarak işlenmesi, kural olarak

---

[217] Süleyman, Yılmaz ve Gökçe Filiz, Çavuşoğlu, *Kişisel Verileri Koruma Hukuku*, (Ankara: Yetkin Yayınları, 2020): 89.

[218] Hayati çıkarlar, yalnızca bir kişinin hayatı için elzem olan çıkarları kapsamayı amaçlamaktadır. Bu nedenle, bu yasal temelin kapsamı oldukça sınırlıdır. Genellikle yaşam ve ölüm konularına ilişkin uygulanmaktadır. (Bilgi Komiserliği Ofisi (ICO), "Vital Interests")

[219] GDPR Text, "Article 6 GDPR: Lawfulness of processing", (2019).

yalnızca işlemenin açıkça başka bir yasal temele dayandırılamadığı durumlarda gerçekleşmelidir[220].

Bu hukuka uygunluk nedeninde kişinin kendisi veya bir başkasının "üstün yararı" gözetildiğinden veri sahibinin açık rızası aranmamaktadır. Örneğin, kişinin bir trafik kazası sonucu bilinci kapalı şekilde hastaneye götürülmesi halinde kişinin ismi, soy ismi, kan grubu, kaza yeri gibi kişisel verilerinin rıza aranmaksızın işlenmesi mümkündür[221].

2.4.4 Bir sözleşmenin kurulması veya ifası amacıyla gönderici verisinin işlenmesi

GDPR kapsamında kişisel verilerin işlenmesi faaliyetinin hukuka uygunluk nedenlerinden birisi, veri sahibinin tarafı bulunduğu sözleşmenin uygulanması ya da sözleşmenin kurulmasından önce veri sahibinin talebi ile işleme faaliyetinin sözleşme süreci için gerekli olmasıdır. Bu hukuka uygunluk nedeni, GDPR'ın 6 ncı maddesine paralel şekilde KVKK'nin 5 inci maddesinin ikinci fıkrasının (c) bendinde de düzenlenmiştir[222]. Bu bağlamda kişisel verinin işlenmesi faaliyetinin hukuka uygun olması, veri sahibi ile veri sorumlusu arasında sözleşmenin bulunmasına veya sözleşmenin müzakere aşamasında olmasına bağlıdır[223].

Diğer yandan genel ilkeler uyarınca anılan hukuka uygunluk sebebi için getirilen sınırlama, veri işlemenin hem işlemeye konu olan veriler hem de işleme amaçları açısından amaçla sınırlılık ve ölçülülük ilkelerine uygun olunmasını gerektirmektedir. Bu kapsamda sözleşmenin kurulması veya ifası için gerekli olmayan bir kişisel verinin

---

[220] Bilgi Komiserliği Ofisi (ICO), "Vital Interests".

[221] Yılmaz ve Çavuşoğlu, *Kişisel Verileri Koruma Hukuku*, 89-90.

[222] KVKK m.5/2(c)'ye göre kişisel veriler, *"Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması"* halinde işlenebilir.

[223] Şehriban İpek Aşıkoğlu vd., "Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebepleri", *Türk Hukukunun Avrupa Birliği Hukukuna Uyumu Özel Hukuk*, İstanbul Üniversitesi Hukuk Fakültesi Avrupa Hukuku Uygulama ve Araştırma Merkezi, (2020): 1065.

işlenmesi mümkün değildir. Kişisel verinin işlenmesi, sözleşmenin kurulması yahut ifasıyla doğrudan doğruya ilişkili olmalıdır[224]. Aksi durumda, işleme amacını aşan faaliyetler diğer veri işleme faaliyetlerine konu edilemeyecektir[225].

İlgi madde hükmünde yer alan "gerekli" ifadesi ise işleme faaliyetinin zorunlu olmasının sözleşmenin ifası ve sözleşme kurulmadan evvel yapılan hazırlıklar için bir ön koşul olduğunu belirtmektedir. Nitekim işlemede hedeflenen amacın, alternatif seçeneklerle kıyaslandığında daha baskın olup olmadığını değerlendirmek, işleme faaliyetinin gerekliliğinin tespitinde önemli bir unsurdur. Bu gerekliliğin, taraflara ilişkin olması ve sözleşmenin kurulması veya ifasıyla doğrudan bağlantılı olması koşullarının sağlanması halinde bu şartın varlığı kabul edilmelidir. Örneğin e-ticaret sitesi üzerinden ürün siparişi veren tüketicinin iletişim ve konum bilgileri, mesafeli satış sözleşmesinin ifası amacıyla işlenmektedir[226].

Burada önemli olan husus, verinin işlenmesinin esas sözleşme hükümlerinin ifası ile doğrudan ilişkisinin olup olmadığıdır. Yani, işleme faaliyeti gerçekleşmeden sözleşmesel bir yükümlülüğün yerine getirilmesi mümkün olmamalıdır[227]. Örneğin; sözleşme gereği satıcı tarafından, malın tesliminin yerine getirilmesi için alıcının adresinin kaydedilmesi, işveren tarafından ücret ödemesinin gerçekleştirilmesi için işçinin banka bilgilerinin kaydedilmesi gerekir[228].

---

[224] Sözleşmenin kurulması ile doğrudan doğruya ilişkili olunması, sözleşme kurmaya yönelik bir teklif, icap veya kabul işlemeleri ile bağlantılı olmayı ifade eder.
[225] Murat Volkan, Dülger, *Sözleşme Gereğince Veri İşleme ile Açık Rıza Alınmasının Gerektiği Hallerin Karşılaştırılması: Uygulamadaki Karışıklığa İlişkin Çözüm Önerileri*, (2021): 2; Şehriban İpek Aşıkoğlu vd., "Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebepleri": 1065.
[226] Avrupa Veri Koruma Denetçisi (EDPS), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, (2017): 5.
[227] Dülger, *Sözleşme Gereğince Veri…,* 3-4.
[228] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, 8.

Posta sektöründe de PHS ile gönderici arasındaki sözleşme gereği göndericinin kimlik, iletişim ve adres bilgileri gibi kişisel verilerinin işlenmesinin sözleşmenin ifası için gerekli olduğu açıktır.

Bu kapsamda, KVK Kurulu'na intikal eden bir şikâyet başvurusunda veri sahibi tarafından, herhangi bir hizmet alınmamasına rağmen, PHS tarafından veri sahibinin e-posta adresine kendisinin namına düzenlenen bir fatura gönderildiği, PHS'ye başvuru üzerine verilen cevapta, faturalandırma işleminin sehven veri sahibi adına yapıldığı, veri sahibinin bilgilerinin ise kayıtlı olduğu meslek kuruluşundaki üyelerin indirimli olarak gönderi ücretlerinden faydalanmasını sağlayan sözleşme çerçevesinde işlendiği ve PHS arşivinde bulunduğu belirtilmiştir. Veri sahibi tarafından bu cevabın akabinde KVK Kurulu'na PHS tarafından kanuni işleme şartlarına dayanılmaksızın veri işleme faaliyetinde bulunulduğu ve bu verilerin silinmesi talebinin PHS tarafından yerine getirilmediği gerekçesiyle başvuruda bulunulmuştur. KVK Kurulu tarafından yapılan inceleme sonucunda ise veri sahibinin söz konusu meslek kuruluşu ile yapılmış olan kampanya kapsamında veri sahibinin üyeliğinin tespiti için kullanılan sistem nezdinde işlenen kişisel verilerin sözleşmenin ifası ile doğrudan ilgili olması hukuki şartına dayanarak işlendiği, bu kapsamda veri sorumlusunun kişisel veri işlemesinde bu noktada bir hukuka aykırılığın bulunmadığına karar verilmiştir[229].

2.4.5 Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için verisinin işlenmesi

KVKK'nin 5 inci maddesinin ikinci fıkrasının (ç) bendi uyarınca, kişisel veriler, "*Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması"* halinde işlenebilir. GDPR'ın 6 ncı maddesinin birinci fıkrasının (c) bendi uyarınca ise veri sorumlusu tarafından, tabi olunan bir kanuni yükümlülüğe uyulması amacı ile

[229] Kişisel Verileri Koruma Kurulu Kararı, 30.09.2021 günlü, 2021/993 sayılı karar.

işlemenin gerekli olması halinde, bu işleme faaliyetinin hukuka uygun olduğu kabul edilmektedir.

Veri sorumlusu tarafından bir hukuki yükümlülük nedeniyle işlenecek olan veride yükümlülüğün kaynağı kural olarak Türk hukuku olarak görülmektedir. Bu itibarla, veri sorumlusunun başka bir ülkedeki yasal yükümlülüklerini yerine getirmek amacıyla veri işlemesi, bu madde kapsamında bir hukuka uygunluk sebebi olarak kabul edilmemektedir[230].

Hukuki sorumluluğun kapsamına, kanun ile sözleşmeden kaynaklanan sorumlulukların dahil edilip edilmeyeceği ise tartışmalı bir konu olarak karşımıza çıkmaktadır. Bu bent ile düzenlenen hukuka uygunluk sebebi, KVKK'nin 5 inci maddesinin ikinci fıkrasının (a) bendinde düzenlenen kanunen zorunlu olma ve aynı fıkranın (c) bendinde düzenlenen, sözleşmenin ifası yahut kurulması için gerekli olması haricindeki hukuki yükümlülükler için öngörülmektedir. Bu itibarla, anılan maddenin (a) bendi çerçevesinde ifade edilen Cumhurbaşkanlığı Kararnamesi, yönetmelik gibi biçimsel olarak kanun kapsamı dışında kalan düzenleyici işlemler, mahkeme kararları yahut usulüne uygun olarak verilmiş resmi kurum talimatları veri sorumlusunun hukuki bir yükümlülüğü olarak kabul edilir[231].

Buna göre, PHSİY'nin 22 nci maddesinin ikinci fıkrası uyarınca kullanıcı şikâyetleri ve bunlara verilen cevapların iki yıl süreyle saklanması, Teslimat Usul ve Esaslarının 7 nci maddesinin ikinci fıkrası uyarınca gönderilere ilişkin bilgilerin kilitli teslimat dolabı ve teslimat noktasına bırakılmasından itibaren iki yıl süreyle saklanması, Güvenlik Usul ve Esasları uyarınca gönderiler, kullanıcılar ve posta personeli ile ilgili gerekli bilgilerin iki yıl ve posta merkezlerindeki kamera kayıtlarının bir ay süreyle saklanması

---

[230] Furkan Güven, Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 2. Baskı, (İstanbul: On İki Levha Yayıncılık, 2017): 171.
[231] Kuyumcu, *6698 Sayılı Kişisel Verilerin…,* 63.

gerekmekte olup PHS'lerin bu verileri saklaması bir başka ifadeyle işlemesi, hukuka uygun bir veri işleme faaliyetidir.

Diğer taraftan posta sektöründe sözleşmesel bir yükümlülüğün ifası amacıyla sözleşmenin tarafları dışındaki üçüncü kişilere ait veriler de işlenebilmektedir. Örneğin; bir PHS'nin gönderici ile arasındaki sözleşmeden doğan hukuki yükümlülüklerini yerine getirmek amacıyla alıcının ad-soyad ve adres bilgisini işlemesi faaliyeti, hukuki yükümlülüğün yerine getirilmesinin zorunlu olmasından kaynaklanmaktadır[232].

2.4.6 İlgili kişinin kendi verisini alenileştirmesi

KVKK'nin 5 inci maddesinin ikinci fıkrasının (d) bendi uyarınca, "*İlgili kişinin kendisi tarafından alenileştirilmiş olması.*" halinde kişisel veriler, ilgili kişinin açık rızasının aranmasına gerek olmaksızın işlenebilmektedir. Veri sahibince kendisine ait kişisel verilerin, herkesin erişimine açılması ve bilinebilir hale gelmesi durumunda bu verilerin açık rıza aranmaksızın işlenmesi mümkündür. GDPR'da ise kişisel verilerin ilgili kişilerce aleni hale getirilmesine herhangi bir hukuki değer atfedilmemiştir.

Esas itibarıyla "alenileştirme" ifadesi, ilgili şahsın ait kişisel verilerinin, kendisi tarafından kamuoyuna açıklanması şeklinde ifade edilmektedir. Bununla birlikte alenileştirmenin varlığının kabulü için kişisel verilerin herhangi bir biçimde kamuoyuna açıklanmış ve alenileştirme işleminin veri sahibinin iradesiyle yapılmış olması şartı aranmaktadır. Dolayısıyla kişisel verilerin herkese açık bir ortamda bulunması alenileştirilmesi yeterli görülmemekte, ayrıca alenileştirme iradesinin varlığı aranmaktadır[233]. Örneğin; bir kişinin acil durumlarda müdahaleyi kolaylaştırmak amacıyla kan grubu bilgisini, sürücüsü olduğu motorlu taşıtın veya

[232] Kişisel Verileri Koruma Kurulu Kararı, 22.06.2021 günlü, 2021/603 sayılı karar.
[233] Kişisel Verileri Koruma Kurulu Kararı, 02.12.2021 günlü, 2021/1217 sayılı karar.

bisikletin herkes tarafından görülebilecek bir yerine yazdırması durumunda, bu kişisel verinin işlenmesi yalnızca ilgili kişinin alenileştirme iradesi ve belirlediği amaç doğrultusunda, yani acil bir durumun varlığı halinde hukuka uygun kabul edilecektir. Ancak, ilgili kişinin alenileştirme niyeti ve amacı dışında bu bilginin işlenmesi hukuka aykırı sayılacaktır[234].

Diğer yandan, verilerin alenileştirilmesi durumunda, özel yaşama ilişkin bilginin mahremiyeti de kaldırılarak hukukun sağladığı belirli korumalardan da ilgili kişi kendi iradesiyle vazgeçmiş olmaktadır. Nitekim, alenileştirilmiş verilerin işlenmesi hususunda ilgili kişi hakkında, KVKK'nin *"Veri sorumlusunun aydınlatma yükümlülüğü"* başlıklı 10 uncu maddesi, *"İlgili kişinin hakları"* başlıklı 11 inci maddesi ve *"Veri Sorumluları Sicili"* başlıklı 16 ncı maddesinde yer alan hükümler uygulanmamaktadır[235].

2.4.7 Bir hakkın tesisi, kullanılması veya korunması için verinin işlenmesi

KVKK'nin 5 inci maddesinin ikinci fıkrasının (e) bendi uyarınca, kişisel veriler, *"Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması"* halinde işlenebilmektedir.

Bu işleme şartının temelinde, verinin işlenmesinde veri sorumlusunun hakkının kaynağı ve türü konusunda bir sınırlama getirilmemiştir. Sınırlandırmanın, belirtilen amaçlar ile veri işlemenin zorunlu olması kriteriyle sağlanması öngörülmüştür. Buradaki zorunluluk ifadesinin, "kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesi çerçevesinde değerlendirilmesi konuyu daha net bir hale getirecektir. Tüm kanuni işleme şartları doğrultusunda yürütülen işleme faaliyetinde, uyulması gerekli ilke gereğince, işlenen verilerin belirlenmiş olan saik veya saiklerin

---

[234] Kişisel Verileri Koruma Kurumu, *Özel Nitelikli Kişisel verilerin İşlenmesine…,* 41.
[235] Mahmut, Koca ve İlhan, Üzülmez, "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Prof. Dr. Durmuş TEZCAN'a Armağan*, Cilt 21, Özel S. (2019): 83.

gerçekleştirilebilmesi açısından elverişli olması ve ilgisiz ya da saikin gerçekleştirilmesi için ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılması gerekmektedir[236].

Bu konuda uygulamada en fazla karşılaşılan durum, işveren tarafından çalışana ait verilerin, iş akdi sonlandıktan sonra bir süre daha işlenebilmesidir. Bunun sebebi, çalışan tarafından işverene dava açılması halinde bu verilerin davada bir ispat aracı vasfı taşıyacak olmasıdır[237].

KVK Kurulu'nun söz konusu hukuka uygunluk sebebine ilişkin 25.06.2020 tarihli ve 2020/494 sayılı kararı kapsamında yapılan değerlendirmede; ilgili kişi tarafından Kuruma iletilen şikâyette, çalışmakta olduğu PHS tarafından iş akdinin feshedilmesi ardından açtığı işe iade davasında, kendisine ait kamera kayıtlarının mahkemeye delil olarak sunulmasının KVKK'ye aykırı olduğu ileri sürülmüştür. İlgili kişi, söz konusu kamera kayıtlarının açık rızası olmaksızın işlendiğini ve bu yönde herhangi bir rıza beyanı bulunmadığını ifade etmiştir. Buna karşılık veri sorumlusu, ilgili kamera kayıtlarının daha önce imzalanan bir aydınlatma metni çerçevesinde ve hukuki gerekçelere dayanılarak işlendiğini; ayrıca kayıtların işe iade davası kapsamında, iş akdinin haklı nedenle feshedildiğini ispatlamak amacıyla mahkemeye sunulduğunu belirtmiştir. KVK Kurulu tarafından yapılan inceleme sonucu kamera kayıtlarının kişisel veri niteliğinde olduğu, bununla birlikte KVKK'nin 5 inci maddesinin ikinci fıkrasının (e) bendi uyarınca *"bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması"* hâlinde açık rıza aranmaksızın veri işlenmesinin mümkün olduğu, ayrıca, BTK'nin "Posta Gönderilerine İlişkin Güvenlik Tedbirlerine Yönelik Usul ve Esaslar"ı uyarınca PHS'lerin kamera kayıtlarını tutmasına yönelik yasal yükümlülüğünün bulunduğu, bu itibarla somut olayda kamera kayıtlarının mahkemeye sunulmasının KVKK kapsamında hukuka uygun bir veri işleme faaliyeti

---

[236] Fatma, Esenyel Hanaz, "Çevrimiçi Eğitimde Üniversite Öğrencilerinin Kişisel Verilerinin İşlenmesinin Hukuki Sebepleri", *Türkiye Barolar Birliği Dergisi*, Sayı: 155, (2021): 424-425.
[237] Murat Volkan, Dülger, *Anayasa Mahkemesi'nin Kişisel Verilerin Korunması Kanunu'nun Konu Edildiği İptal Davası Kararına İlişkin Bir Değerlendirme*, (2021): 4.

olduğu belirtilerek PHS hakkında yapılacak bir işlem bulunmadığına karar verilmiştir[238].

2.4.8 Veri sorumlusunun meşru menfaati için verinin işlenmesi

KVKK'nin 5 inci maddesinin ikinci fıkrasının (f) bendi uyarınca, kişisel veriler, *"İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"* halinde de işlenebilir. GDPR'ın 6 ncı maddesinin birinci fıkrasının (f) bendi uyarınca ise veri sorumlusu yahut üçüncü kişi tarafından hedeflenen menfaatlere varılmak amacıyla işlemenin gerekli olması halinde, bu işleme faaliyetinin hukuka uygun olduğu kabul edilir[239].

Kişisel verilerin bu istisna kapsamında işlenmesinin hukuka uygun olması için üç kümülatif koşul öngörülmektedir: Birincisi, veri sorumlusu veya üçüncü bir kişi tarafından meşru bir menfaatin gözetilmesi, ikincisi, kişisel verilerin veri sorumlusu tarafından işlenmesinin gerekliliği ve üçüncüsü, veri sahibinin çıkarlarının veya temel hak ve özgürlüklerinin üstün gelmemesi koşuludur[240].

Bu bağlamda ilk olarak meşru menfaat kavramını ele almak gerekmektedir. İlgili düzenlemelerde "meşru menfaat" kavramına ilişkin bir tanım yapılmamaktadır. Bununla birlikte, işleme faaliyeti sonucunda elde edilecek olan çıkar ve faydanın hukuka uygun, önemli ve ciddi olması aranmaktadır[241]. Nitekim AYM, 28.09.2017 tarihli ve E.2016/125, K.2017/143 sayılı Kararında, *"…Ancak bu kavramın çalışanların temel hak ve özgürlüklerine zarar vermemek kaydıyla gerekçede ifade edilen temel ilkelere uyulması ve veri sorumlusu ile ilgili kişinin menfaat dengesinin gözetilmesi*

---

[238] Kişisel Verileri Koruma Kurumu, "Kişisel Verileri Koruma Kurulu Kararları 2018-2021", *KVKK Yayınları,* No: 39, (2021): 323-326.

[239] Ancak ilgili kişinin çocuk olması hallerde, temel hak ve hürriyetlerin korunması gerekliliğinin daha ağır bastığı ifade edilmektedir.

[240] Avrupa Birliği Adalet Divanı, "07.12.2023 tarihli Karar, Birleştirilmiş Davalar C-26/22 ve C-64/22, SCHUFA Holding (Libération de reliquat de dette) (ECLI:EU:C:2023:958)", m.75.

[241] Ekin, *Kişisel Verilerin Korunması ve…*, 88.

çerçevesinde değerlendirilmesi gereken bir kavram olarak anlaşılması gerektiği dikkate alındığında belirsiz olduğu söylenemez." ifadesi ile "meşru menfaat" kavramını, hükmün gerekçesini temel alarak yorumlamıştır[242].

Diğer yandan, meşru menfaatte esas alınan çıkar kavramı, GDPR'ın 5 inci maddesinin birinci fıkrasının (b) maddesinde belirtilen "amaç" kavramıyla yakından ilişkili olsa da aynı anlama gelmemektedir. Amaç, verilerin işlenmesinin belirli nedenidir. Çıkar ise bir veri sorumlusunun veya üçüncü kişinin belirli bir işleme faaliyetinde bulunmada sahip olabileceği daha geniş fayda olarak tanımlanmaktadır. Tüm çıkarlar, bir veri sorumlusunun meşru menfaati için veri işlemesini yasal bir dayanak olarak ileri sürmesini sağlamamaktadır. Meşru menfaat kavramı, yasada yer alan ve yasayla belirlenen menfaatlerle sınırlı olmamakla birlikte, iddia edilen meşru menfaatin hukuki olmasını gerektirmektedir. Bu kapsamda meşru çıkarın çerçevesi açıkça tanımlanmalıdır. İlgi gerçek ve mevcut olmalı, spekülatif olmamalıdır. Meşru ilgi, veri işleme faaliyetinin gerçekleştiği tarihte mevcut olmalı ve varsayımsal olmamalıdır. GDPR ve Avrupa Birliği Adalet Divanı (ABAD), çevrim içi bilgilere erişim, kamuya açık internet sitelerinin sürekli işleyişini sağlama, birinin malına zarar veren bir kişinin kişisel bilgilerini elde etme gibi çeşitli çıkarları açıkça meşru olarak kabul etmiştir[243].

İkinci olarak kişisel verilerin veri sorumlusu tarafından işlenmesinin gerekliliği önem arz etmektedir. Kişisel verilerin işlenmesinde temel ilkelerden biri olan, verinin işlenme amacına uygun, işlenme amaçlarıyla ilgili ve bunlarla sınırlı olması ilkesiyle birlikte incelendiğinde, sadece belirlenen meşru çıkar için kesinlikle gerekli olması halinde bu hukuka uygunluk nedenine başvurulmalıdır. Bir başka ifade ile kişisel verilerin işlenmesi, veri sorumlusu için zorunluluk arz eden hususlar ile

---

[242] Kadir, Yıldız, "Veri Sorumlusunun Meşru Menfaati (5/2-f)", *Medeni Hukuk Dergisi,* 1/2, (2024): 214-237.

[243] Avrupa Veri Koruma Kurulu (EDPB), "Kişisel Verilerin İşlenmesine İlişkin 1/2024 Sayılı Kılavuz Madde 6(1)(f) GDPR, Versiyon 1.0", 7-8.

sınırlanmamalı, veri sorumlusu açısından mutlak surette "gerekli" olan durumlarda verinin işlenmesine izin verilmelidir[244].

Üçüncü ve son olarak ise kişisel verilerin veri sorumlusu tarafından işlenmesinde, veri sahiplerinin temel hak ve özgürlüklerinin meşru menfaatin önüne geçmemesi gereklidir. Yani, menfaat dengesinin sağlanması esas olup veri sorumlusunun menfaati ile veri sahibinin yaşayacağı etki birlikte değerlendirilmelidir. Yapılacak değerlendirme neticesinde veri sahibinin menfaatinin daha ağır basması halinde, kişisel verilerin bu hukuka uygunluk nedenine dayanarak işlenmesi mümkün olmamalıdır[245].

Sonuç olarak diğer yasal dayanakların uygulanamayacağı düşünülen sınırlı hallerde "son çare" olarak bu hukuka uygunluk nedenine başvurulmalı ve kullanımı genişletilmemeli, bir diğer ifadeyle istisna, kural haline getirilmemelidir[246].

2.5 Posta Sektöründe Hassas Veriler ve İşlenme Koşulları

KVKK'nin yürürlüğe girmesinin ardından ortaya çıkan yeni uluslararası düzenlemeler ve uygulama tecrübeleri nedeniyle, bu Kanun'un bazı konuları ve güncel gelişmeleri kapsamadığı yolunda eleştiriler ortaya konulmuştur[247]. Bu konulardan biri de hassas verilere ilişkindir.

Ülkemizde 2021 senesinde açıklanan "İnsan Hakları Eylem Planı"[248] ve diğer eylem planlarıyla KVKK ile GDPR'ın uyumu hedeflenmektedir. Bu kapsamda, 12 Mart 2024

---

[244] Dursun, Saat, "Kişisel Verilerin Korunması Kanunu'nda Öngörülen Meşru Menfaat Kavramının Ticaret Şirketleri Bakımından Değerlendirilmesi", *Anadolu Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 10, Sayı: 2, (2024): 635.
[245] Umniyahasghar, Yosif, "Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler", *SÜAMYOD*, Cilt: 4, Sayı: 1, (2021): 15-16.
[246] Avrupa Veri Koruma Kurulu (EDPB), "Kişisel Verilerin İşlenmesine İlişkin 1/2024 Sayılı…": 2.
[247] Turan Başara, "Kişisel Verilerin Korunması Kanunu'nun…": 54.
[248] Adalet Bakanlığı, "İnsan Hakları Eylem Planı", (2021): 80.

tarihli ve 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (7499 sayılı Kanun)'un 33 üncü maddesi ile KVKK'nin hassas verilerin işlenmesine ilişkin düzenlemeler içeren 6 ncı maddesinde kapsamlı değişiklikler gerçekleştirilmiştir. Bu değişiklik ile KVKK'nin 6 ncı maddesinin ikinci fıkrası yürürlükten kaldırılmış, aynı maddenin üçüncü fıkrasında değişikliğe gidilerek, hassas verilerin işlenebileceği nedenler yeniden düzenlenmiştir.

Yapılan bu değişiklikler ile başta hassas verilerin işlenmesinde, sağlık ve cinsel yaşam dışındaki veriler ile bunlara dair ayrımının kaldırıldığı, tüm hassas verilerin işlenmesinde hukuka uygunluk sebeplerindeki farklılığın giderildiği görülmektedir[249]. Bu bağlamda hassas verilerin işlenme sebepleri;

- *"Açık rıza*
- *Kanunlarda açıkça öngörülme*
- *Fiili imkânsızlık*
- *Alenileştirme*
- *Bir hakkın tesisi, kullanılması veya korunması için zorunluluk*
- *Sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işleme*
- *İstihdam, iş sağlığı ve güvenliği, iş ve sosyal güvenlik veya sosyal hizmetler ile sosyal yardım alanındaki hukuki yükümlülükler için işleme*
- *Siyasi, felsefi, dini veya sendikal amaçlarla kurulan vakıf, dernek veya diğer kâr amacı gütmeyen kuruluş ya da oluşumlara ilişkin özel işleme sebebi"*

olarak Kanun'un 6 ncı maddesinin ikinci fıkrasında tahdidi olarak sayılmıştır. Bu değişiklikler ve 5 inci maddedeki hukuki işleme sebepleri arasında uyum gözetilmiştir.

---

[249] Ömer, Ekmekçi, Nafiye, Yücedağ, Elif Beyza, Akkanat-Öztürk ve Şehriban İpek, Aşıkoğlu, "Ceza Muhakemesi Kanunu ile Bazı Kanunlarda ve 659 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılmasına Dair Kanun Teklifi ile 6698 Sayılı Kanun'da Yapılan Değişiklikler", (2024).

Posta sektöründe PHS'ler özellikle gönderi içeriğinde yer alan sağlık raporları, adli belgeler (tebligat/ihtarname gibi) veya siyasi içerikli belgelerin bulunması hâlinde bu tür verilere dolaylı olarak temas edilebilmektedir. Bunun yanı sıra, engellilere yönelik özel teslimat veya destek hizmetlerinde kişilerin sağlık durumuna ilişkin veriler de işlenebilmektedir. Diğer yandan uygulamada görülmemekle birlikte gönderinin kabulü veya teslimi sırasında biyometrik imza tabletleri veya yüz tanıma gibi sistemlerin kullanılmasının, hassas verilerin işlenmesine yol açabileceği değerlendirilmektedir.

Diğer taraftan hassas veri niteliğindeki biyometrik veriler, posta sektörü bağlamında değerlendirildiğinde; özellikle müşteri kimliğinin teyidine yönelik kullanılan "imza" ile çağrı merkezi işlemleri sırasında kaydedilen "ses kayıtları" dikkat çeken unsurlar arasında yer almaktadır. Zira Teslimat Usul ve Esaslarında yer alan hükümlerin halihazırda haberleşme gönderilerine uygulanmaması nedeniyle haberleşme gönderilerinin teslimatında alıcılardan imza alınmakta, PHS'lerin çağrı merkezleri aracılığıyla ilgili kişilerin sesleri kayıt altına alınmaktadır.

Öte yandan kullanıcıların imzası ve ses kayıtları tek başına biyometrik veri kabul edilmemektedir. Zira söz konusu verilerin biyometrik veri olarak nitelendirilmesi, ancak kişinin kimliğinin belirlenmesine yönelik teknik analizlerin uygulanması ve bu analizler sonucunda kimliğin tespit edilmesi durumunda mümkündür. Bununla birlikte, veri işleme süreci kimlik tespiti amacı taşımıyorsa, ancak ilgili kişi doğrudan ya da dolaylı olarak tanımlanabiliyorsa, bu durumda söz konusu veri hassas veri kapsamında değerlendirilmemektedir[250]. Örneğin, bir PHS'nin kullanıcıların kimliklerini ses tanımlama yöntemiyle saptaması durumunda, ses kaydı biyometrik veri olarak kabul edilirken; kullanıcı memnuniyetini sağlamak ile sunulan hizmet ve yapılan işleme ilişkin ispat aracı olarak ses kaydı verisinin tutulması halinde bu veriler genel nitelikte kişisel veri olarak kabul edilmektedir.

---

[250] Erdinç, "Ölçülülük İlkesi ve Açık…": 8.

2.6 Posta Sektöründe Kişisel Verilerin Aktarılması

Kişisel verilerin aktarımında veri sahibinin açık rızasının aranması, temel prensip olarak hüküm altına alınmaktadır. Bununla birlikte bazı istisnai hallerde veri sahibinin açık rızası aranmaksızın veri aktarımı gerçekleştirilebilmektedir. Bu istisnai haller, kanun ya da yönetmelik hükümleriyle belirlenmektedir[251].

Posta sektöründe de kullanıcı verilerinin korunması, PHS'lerin kullanıcılar ile olan ilişkisinde temel bir unsurdur. Bu doğrultuda PHK'nin 7 nci maddesinin üçüncü fıkrası gereğince PHS'ler, kullanıcı verilerini kanunla yetkilendirilmiş merciler dışında kalan kişi veya kuruluşlar ile paylaşamamakta, bir başka ifade ile aktaramamaktadır. Bununla birlikte KVKK'nin *"Kişisel verilerin yurt dışına aktarılması"* hususunu düzenleyen 9 uncu maddesinde 7499 sayılı Kanun ile 01.06.2024 tarihinde yapılan değişiklik sonucunda bu bilgilerin aktarımının hangi koşullarla sağlanacağı konusunda bazı tereddütler yaşanabilmektedir.

Bu başlıkta, posta sektöründe kişisel verilerin yurt içi ve yurt dışına aktarım süreçleri incelenecektir. Ardından kişisel verilerin yurt dışına aktarımına ilişkin olarak 7499 sayılı Kanun ile yapılan değişiklikle yürürlüğe giren KVKK hükümlerine uygunluğun sağlanması ve bu süreçlerin posta mevzuatı ile uyumlu bir şekilde yürütülmesine ilişkin dikkat edilmesi gereken hususlar ele alınacaktır.

2.6.1 Yurt içinde aktarılması

KVKK'nin *"Kişisel verilerin aktarılması"* başlıklı 8 inci maddesi uyarınca kişisel verilerin aktarımı kişilerin açık rızası ile gerçekleştirilebilecektir. Bununla birlikte, açık rıza olmasa da hassas olsun olmasın, tüm kişisel verilerin işlenmesinde uygulanabilir olan

---

[251] Begüm, Becer, *Kişisel Verilerin Korunması Kanunu Kapsamında Kişilik Haklarının Korunması,* (Yüksek Lisans Tezi, Başkent Üniversitesi Sosyal Bilimler Enstitüsü, 2021): 104-110.

hukuka uygunluk nedenlerinin varlığı, bu verilerin aktarılması faaliyetinin de hukuki olarak kabul görmesini sağlayacaktır.

Bu kapsamda posta hizmetinin yürütülmesi sırasında gerçekleştirilen veri aktarımlarının çoğunluğunun da kullanıcıların açık rızasına gerek duyulmaksızın, hukuka uygunluk nedenleri çerçevesinde gerçekleştirilebileceği değerlendirmektedir. Bununla birlikte, hukuka uygunluk nedenlerine dayanılarak yapılan veri aktarımlarında, amaca bağlılık unsurunun özenle değerlendirilmesi gerekmektedir[252]. Bu bağlamda aşağıda posta hizmeti sunumunda veri aktarımının söz konusu olabileceği durumlar ele alınarak konu değerlendirilmektedir.

2.6.1.1 Bilgi ve belge talep etmeye yetkili mercilere gerçekleştirilen kişisel veri aktarımları

PHK'nin *"Posta hizmetlerinin gizliliği ve güvenliği"* başlıklı 7 nci maddesinin üçüncü fıkrası ve PHSİY'nin *"Posta hizmetlerinin gizliliği ve güvenliği"* başlıklı 18 inci maddesinin üçüncü fıkrası kapsamında posta gönderi içeriği ve dolayısıyla kullanıcıların kişisel verileri kanunen yetkili kılınan mercilere açıklanabilmektedir. Bu sayede kanun ve diğer ikincil düzenlemelerde belirlenen yetki çerçevesinde bilgi ve belge talep edebilecek yetkili mercilere kişisel verinin aktarımında ilgili kişilerin açık rızasına ihtiyaç duyulmamaktadır. Bununla birlikte, bilgi ve belge talep etmeye kişi ve/veya kurumların kim olduğu PHK ve ikincil düzenlemelerde yer almamaktadır. Bu nedenle PHS'lerden veri talebinde bulunan mercilerin kanunen yetkili merci sayılıp sayılmayacağı hususunda ilgili merci ve yasal dayanağı özelinde değerlendirme yapılmalıdır[253]. Örneğin; 5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) *"bilgi isteme"* başlıklı 332 nci maddesi uyarınca mahkemeler, hakimlikler ve cumhuriyet savcıları tarafından talep edilen bilgilerin verilmesi mecburiyeti nedeniyle bu

[252] Göknil, Özcan, *Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması*, (Yüksek Lisans Tezi, İstanbul Üniversitesi, 2019): 106.
[253] Özcan, *Bankacılık İş ve İşlemlerinde…,* 110.

kapsamda aktarılan kişisel verilerde ilgili kişilerin açık rızasının aranmasına gerek bulunmamaktadır. Ayrıca Güvenlik Usul ve Esaslarının *"Hizmet sağlayıcılar tarafından Kuruma bilgi gönderilmesi ile ilgili hükümler"* başlıklı 7 nci maddesinin birinci fıkrasındaki, *"Hizmet sağlayıcıları, posta gönderilerine ilişkin olarak iş bu Usul ve Esasların 4 üncü maddesinin birinci ve ikinci fıkraları ile 5 inci maddesinde yer alan bilgi ve belgeleri, Kurum tarafından belirlenecek usul, esas ve standartlarda eksiksiz ve zamanında tüm harcamaları kendilerine ait olmak üzere elektronik ortamda kuruma teslim etmekle yükümlüdür."* hükmü gereği atıf yapılan maddelerde yer alan bilgi ve belgelerin BTK'ye teslim edilmesi gerekliliği bulunmaktadır.

2.6.1.2 Üçüncü kişilerden hizmet alımına yönelik veri aktarımları

PHS'ler, veri sorumlusu sıfatıyla işlemiş oldukları kişisel verileri, sözleşme kapsamında üçüncü kişilerden elde edeceği ürün veyahut hizmetlere ilişkin olarak; acil durum yönetimi, görevlendirme, iletişim, denetim ve etik süreçlerinin yürütülmesi, iş sağlığı ve güvenliği faaliyetlerinin sürdürülmesi, ilgili faaliyetlerin mevzuata uygun biçimde gerçekleştirilmesi, lojistik ve iş faaliyetlerinin yürütülmesi ve denetimi, sözleşme süreçlerinin yönetimi, muhasebe ve finans işlemlerinin gerçekleştirilmesi, talep ve şikayetlerin takibi, tedarik zinciri yönetimi süreçlerinin yürütülmesi, hukuk işlerinin takibi ve yürütülmesi ile mal ve hizmet satın alım süreçlerinin yürütülmesi amaçlarıyla sınırlı olmak kaydıyla üçüncü kişiler ile veri paylaşımı gerçekleştirilebilmektedir[254]. Örneğin; PHS'nin çağrı merkezi hizmeti aldığı, veri işleyen statüsünde bulunan bir şirket ile kullanıcılarının kimlik, iletişim bilgileri veya işlem kayıtları gibi kişisel verilerini paylaşmasının veri aktarımı kapsamına dahil olduğu söylenebilecektir. Bir başka örnek olarak da bir PHS'nin, tedarik zinciri yönetimi sürecinin yürütülmesi amacıyla operasyonel kapasitesinin dışında kalan belirli yerleşim bölgelerine gönderi teslimatı gerçekleştirmek için bir başka PHS ile iş birliği yapabildiği durumlar verilebilecektir. Bu durumlarda, teslimatın gerçekleştirilebilmesi amacıyla

[254] MNG Kargo, "Genel Aydınlatma Metni".

kullanıcılara ait kişisel veriler bir diğer PHS ile paylaşılmaktadır. Ancak, kişisel verilerin PHS'nin kendi tüzel kişiliği haricindeki başka bir PHS ile paylaşılmasının, KVKK ile uyumlu olmayabileceği ve bu nedenle kullanıcıların açık rızasına başvurulması gerektiği düşünülmektedir. Bu kapsamda açık rıza alınırken gönderinin tesliminden önce, teslim için bir başka PHS ile çalışılması zorunluluğu da bilgilendirme yükümlülüğü kapsamında kullanıcıya aktarılmalıdır.

Bununla birlikte, kullanıcılara ait kişisel verilerin şirket bünyesinde çalışan kişiler veya PHS'nin Türkiye'de faaliyet gösteren şubelerine veri aktarımının veri sorumlusunun meşru menfaati kapsamında paylaşılabileceği düşünülmektedir. Zira benzer bir gerekçe ile GDPR'ın *"Başlangıç"* bölümünde yer alan 48 inci maddesinde şirket içinde idari amaçla veri sorumlusunun meşru menfaatine dayanılarak kişisel verilerin paylaşılabileceği düzenlenmektedir.

2.6.2 Yurt dışına aktarılması

Kişisel verilerin yurt dışına aktarılması kavramına KVKK'de yer verilmemiştir. KVKK'nin 9 uncu maddesinde yalnızca yurt dışına aktarımın usulü belirlenmiş olup hangi faaliyetin yurt dışına aktarım sayılacağına ilişkin bir belirleme yer almamaktadır. KVK Kurumu tarafından yayımlanan rehberde ise işleme usullerinin bazıları belirtilirken kişisel verilerin çeşitli usullerle devralınması/aktarılması halinin işleme faaliyeti olduğu belirtilmiş ancak yine bir tanım yapılmamıştır[255].

Diğer yandan, KVKK'nin *"Kişisel verilerin yurt dışına aktarılması"* konusunu düzenleyen 9 uncu maddesinde 7499 sayılı Kanun ile yapılan değişiklikle kişisel verilerin yurt dışına aktarılması imkânı, esas olarak aktarımın yapılacağı ülke hakkında bir yeterlilik kararı bulunup bulunmadığı ayrımı geçerli kalmak üzere, GDPR ile uyumlu

[255] Kişisel Verileri Koruma Kurumu, *6698 Sayılı Kanunda Yer Alan Temel Kavramlar*, 17.

olacak biçimde yeniden düzenlenmiştir[256]. Böylece veri sorumlularını, kişisel verilerin yurt dışına aktarıldığı hallerde zorlayan "açık rıza" öncelikli yaklaşım terkedilmiş ve ilgili kişilerin daha fazla korunduğu bir yapı oluşturulmuştur[257].

Yeni düzenleme, aşamalı ve alternatifli bir aktarım sistemi getirmiştir. Bu düzenleme kapsamında, kişisel verilerin yurt dışına aktarılmasında üç farklı yöntem öngörülmüştür: Bunlardan ilki, yeterlilik kararına dayalı aktarım, ikincisi, uygun güvencelere dayalı aktarım, üçüncüsü ise arızi durumlara dayalı aktarımdır.

Bununla birlikte, söz konusu düzenlemenin, posta sektörü açısından uygulanabilirliğinde bazı zorluklar söz konusu olabilmektedir. Zira PHK'nin 13 üncü maddesi gereği evrensel hizmet yükümlüsünün evrensel hizmetleri sunma yükümlülüğü bulunmaktadır. Ancak KVKK'deki bu düzenleme ile veri sorumlusu olan PHS'nin, yasal yükümlülüklerini yerine getirme zorunluluğu ile kişisel verilerin yurt dışına aktarılmasına ilişkin veri sahibinin rızası olmaksızın işlem yapma yasağı arasında bir ikileme düşülebilir. Bu durum, veri sorumlularının faaliyetlerini kısıtlamalarına veya faaliyetlerinin, verileri yurt dışına aktarılacak kişilerin onayına orantısız şekilde bağımlı hale gelmelerine sebebiyet verebilir[258]. Bu bağlamda, verilerin yurt dışına aktarımında kullanılan yöntemler, posta sektörüne özgü uygulamalar çerçevesinde aşağıda daha ayrıntılı olarak ele alınmaktadır.

2.6.2.1 Yeterlilik kararına dayalı aktarımlar

7499 sayılı Kanun ile getirilen yeni düzenlemeye göre, KVKK'nin 5 ve 6 ncı maddelerinde belirtilen işleme şartlarından birinin sağlanması ile verilerin aktarılacağı ülke, uluslararası kuruluş ya da ülke içerisindeki belirli sektörler hakkında yeterlilik kararı bulunması durumunda, veri sorumluları ve veri işleyenler kişisel

---

[256] Kuyumcu, *6698 Sayılı Kişisel Verilerin…,* 94.
[257] Ekmekçi vd., "Ceza Muhakemesi Kanunu ile Bazı Kanunlarda ve…".
[258] Kuyumcu, *6698 Sayılı Kişisel Verilerin…,* 47.

verileri yurt dışına aktarabilecektir. Ayrıca, yurt dışına veri aktarımının da bir veri işleme faaliyeti olduğu göz önünde bulundurularak, bu süreçte de 5 inci ve 6 ncı maddelerdeki hukuki işleme nedenlerinin aranması gerekmektedir. Bu değişiklik, GDPR düzenlemeleriyle uyumlu niteliktedir[259].

Kişisel verilerin aktarılması amacıyla yeterlilik kararı verilirken hangi hususların dikkate alınacağı, anılan Kanun maddesinin üçüncü fıkrasında belirtilmiştir. Buna göre yeterlilik kararı;

> *"a) Kişisel verilerin aktarılacağı ülke, ülke içerisindeki sektörler veya uluslararası kuruluşlar ile Türkiye arasında kişisel veri aktarımına ilişkin karşılıklılık durumu.*
> *b) Kişisel verilerin aktarılacağı ülkenin ilgili mevzuatı ve uygulaması ile kişisel verilerin aktarılacağı uluslararası kuruluşun tâbi olduğu kurallar.*
> *c) Kişisel verilerin aktarılacağı ülkede veya uluslararası kuruluşun tâbi olduğu bağımsız ve etkin bir veri koruma kurumunun varlığı ile idari ve adli başvuru yollarının bulunması.*
> *ç) Kişisel verilerin aktarılacağı ülkenin veya uluslararası kuruluşun, kişisel verilerin korunmasıyla ilgili uluslararası sözleşmelere taraf veya uluslararası kuruluşlara üye olma durumu.*
> *d) Kişisel verilerin aktarılacağı ülkenin veya uluslararası kuruluşun, Türkiye'nin üye olduğu küresel veya bölgesel kuruluşlara üye olma durumu.*
> *e) Türkiye'nin taraf olduğu uluslararası sözleşmeler"*

dikkate alınarak verilmektedir[260].

---

[259] Mehmet Bedii, Kaya, *KVKK Reformu: 2024 Değişiklikleri*, (2024): 30.

[260] Bu fıkrada sayılan bu ölçütler tahdidi nitelikte değildir. Kurul yeterlilik kararı verirken gerekli gördüğü başkaca hususları da dikkate alabilecektir (Furkan Güven, Taştan, "Kişisel Verilerin Korunması Kanunu - 2024 Değişikliklikleri", 2025).

Yeni düzenleme ile yeterlilik kararına dayalı aktarım korunmuş ve yeterlilik kararına, ülkeler haricinde uluslararası kuruluşlar ile sektörlerin de dahil olmasına imkân tanınmıştır. Bu sayede ülke içerisindeki belirli bir sektör hakkında da yeterlilik kararı alınabileceği hükme bağlanmıştır. Bu kapsamda, aktarımın yapılacağı bir uluslararası kuruluşun Türkiye sınırları dahilinde bulunması durumunda, bu madde hükümlerinin uygulanacağı değerlendirilmektedir[261]. Örneğin; yurt dışında da faaliyet gösteren bir PHS'nin Türkiye'de bulunan temsilciliğine aktarımın yapılacak olması durumunda KVKK'nin 9 uncu maddesinde yer alan hükümlerin uygulanması mümkündür.

Yurt dışına kişisel verilerin aktarılması sürecinde veri sorumlusunun yanı sıra, veri işleyenlere de yer verilmiştir. Ayrıca yeterlilik kararının en geç dört yıl içerisinde yeniden değerlendirileceği ve yeterlilik kararının KVK Kurulu tarafından verilerek Resmî Gazete'de yayımlanacağı belirtilmiştir. Bununla birlikte işbu tezin yayımlanma tarihi itibarıyla KVK Kurulu tarafından halihazırda yeterlilik kararı verilmiş bir ülke, uluslararası kuruluş ya da sektör bulunmamaktadır[262].

2.6.2.2 Uygun güvenceye dayalı aktarımlar

Kişisel veriler, KVK Kurulu tarafından verilmiş bir yeterlilik kararının bulunmaması halinde, 5 ve 6 ncı maddelerde yer alan işleme şartlarından birinin varlığı, ilgili kişinin aktarım yapılacak ülkede de haklarını kullanma ve etkin yasal yollara başvurma imkânının bulunması şartıyla Kanun'un 9 uncu maddesinin dördüncü fıkrasında belirtilen;

> *"a) Yurt dışındaki kamu kurum ve kuruluşları veya uluslararası kuruluşlar ile Türkiye'deki kamu kurum ve kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşları arasında yapılan uluslararası sözleşme niteliğinde olmayan anlaşmanın varlığı ve Kurul tarafından aktarıma izin verilmesi.*

---

[261] Kuyumcu, *6698 Sayılı Kişisel Verilerin…,* 91.
[262] Kişisel Verileri Koruma Kurumu, "Yurt Dışına Aktarım", (2025).

b) Ortak ekonomik faaliyette bulunan teşebbüs grubu bünyesindeki şirketlerin uymakla yükümlü oldukları, kişisel verilerin korunmasına ilişkin hükümler ihtiva eden ve Kurul tarafından onaylanan bağlayıcı şirket kurallarının varlığı.

c) Kurul tarafından ilan edilen, veri kategorileri, veri aktarımının amaçları, alıcı ve alıcı grupları, veri alıcısı tarafından alınacak teknik ve idari tedbirler, özel nitelikli kişisel veriler için alınan ek önlemler gibi hususları ihtiva eden standart sözleşmenin varlığı.

ç) Yeterli korumayı sağlayacak hükümlerin yer aldığı yazılı bir taahhütnamenin varlığı ve Kurul tarafından aktarıma izin verilmesi."

şeklindeki uygun güvencelerin birisinin taraflarca sağlanması durumunda, veri sorumluları ve veri işleyenler tarafından yurt dışına aktarılabilmektedir.

Uygun güvencelerle aktarım faaliyetinde de aynı yeterlilik kararındaki gibi KVKK'nin diğer hükümlerinin de göz önüne alınması gerekmektedir. Nitekim uygun güvenceye dayalı aktarımda da 5 ve 6 ncı maddelerdeki hukuki işleme nedenlerinin varlığı bir ön koşul olarak aranmaktadır[263].

Bu aktarım yöntemi posta sektörü açısından değerlendirildiğinde, örneğin; evrensel posta hizmet yükümlüsünün haberleşme gönderileri açısından yurt dışı hizmet yükümlülüğüne sahip olması nedeniyle, veri aktarımı yapılan ülkelerdeki veri sorumluları ve veri işleyenlerle tek tek taahhütname imzalaması gerektiği gibi bir çıkarıma varılması mümkündür. Ayrıca anılan çıkarıma göre, bu aktarım için KVK Kurulu'nun onayının alınması da gerekecektir[264]. Ancak, anılan düzenlemenin bu

[263] Furkan Güven, Taştan, "Kişisel Verilerin Yurt Dışına Aktarılmasında Açık Rıza", *Terazi Hukuk Dergisi*, Cilt: 0, Sayı: 217, (Eylül 2024): 5.

[264] Şehriban İpek, Aşıkoğlu ve Fatih Burak, Uzun, "Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri", *Prof. Dr. Türkan Rado'nun Anısına Armağan*, (2020): 928.

şekilde anlaşılarak uygulanmasının; posta sektörünün ve hizmetlerinin doğasıyla tam uyumlu olmayacak negatif sonuçlara sebebiyet verebileceği düşünülmektedir.

2.6.2.3 Arızi hallere dayalı aktarımlar

Veri sorumluları ve veri işleyenler tarafından, yeterlilik kararının veya uygun güvencelerden birinin bulunmaması durumunda son çare olarak başvurulması gereken arızi haller kavramı, 7499 sayılı Kanun ile Türk hukukuna dahil olmuştur. *"Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik"*in 16 ncı maddesinde arızilik kavramı, *"düzenli olmayan, tek veya birkaç sefer gerçekleşen, süreklilik arz etmeyen ve olağan faaliyet akışı içinde bulunmayan aktarımlar"* şeklinde tanımlanmaktadır. Bir başka ifade ile arızi aktarım, yalnızca tek seferde gerçekleşen aktarım anlamı taşımamaktadır. Bu ifadeden anlaşılması gereken, sistematik ve düzenli veri aktarımı yapılmamasıdır. Bu durumun ise her somut olayda ayrıca değerlendirilmesi gerekmektedir[265].

KVKK'nin 9 uncu maddesinin altıncı fıkrasına göre kişisel verilerin, arızi olmak şartıyla yalnızca aşağıdaki hâllerden birinin varlığı durumunda yurt dışına aktarabilmesi mümkündür. Buna göre;

> *"a) İlgili kişinin, muhtemel riskler hakkında bilgilendirilmesi kaydıyla, aktarıma açık rıza vermesi.*
> *b) Aktarımın, ilgili kişi ile veri sorumlusu arasındaki bir sözleşmenin ifası veya ilgili kişinin talebi üzerine alınan sözleşme öncesi tedbirlerin uygulanması için zorunlu olması.*
> *c) Aktarımın, ilgili kişi yararına veri sorumlusu ve diğer bir gerçek veya tüzel kişi arasında yapılacak bir sözleşmenin kurulması veya ifası için zorunlu olması.*

---

[265] Kaya, *KVKK Reformu: 2024 Değişiklikleri*, 44.

ç) Aktarımın üstün bir kamu yararı için zorunlu olması.

d) Bir hakkın tesisi, kullanılması veya korunması için kişisel verilerin aktarılmasının zorunlu olması.

e) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin aktarılmasının zorunlu olması.

f) Kamuya veya meşru menfaati bulunan kişilere açık olan bir sicilden, ilgili mevzuatta sicile erişmek için gereken şartların sağlanması ve meşru menfaati olan kişinin talep etmesi kaydıyla aktarım yapılması."

hâllerden birinin varlığı durumunda kişisel veriler yurt dışına aktarabilmektedir.

Diğer iki aktarım yönteminin aksine, arızi durumlar için ön koşul olarak 5 ve 6 ncı maddelerde belirtilen hukuka uygunluk sebeplerine atıfta bulunulmamıştır. Bunun yerine, arızi durumlar için veri işleme şartları, özel bir düzenleme niteliğinde yukarıda yer verilen yedi bent halinde Kanunda sıralanmıştır[266].

Posta sektöründe yurt dışına veri aktarımında kanaatimizce, arızi hallerin varlığından söz edilemeyecektir. Arızi durumların, düzenli olmayan, tek seferlik veya sınırlı sayıdaki, süreklilik göstermeyen ve olağan faaliyet akışı içinde yer almayan durumlar olarak tanımlanması, posta sektörü açısından uygun olmayacaktır. Zira PHS'ler tarafından gerçekleştirilen veri aktarımı, sektörün olağan faaliyet süreçlerinin bir parçası olup süreklilik arz etmektedir.

[266] Taştan, "Kişisel Verilerin Yurt Dışına Aktarılmasında Açık Rıza": 6.

2.7 Posta Kullanıcı Hakları ve Posta Hizmet Sağlayıcısının Yükümlülükleri

Kişisel verilerin işlenmesi aşamasında ilgili kişiye çeşitli haklar tanınırken, veri sorumlusuna da belirli yükümlülükler getirilmiştir. T.C. Anayasası'nın 20 nci maddesi uyarınca bilgi edinme, erişim, düzeltme ve silme talepleri anayasal birer hak olarak güvence altına alınmıştır. Ayrıca KVKK'nin 11 inci maddesi, ilgili kişiye bilgi edinme, verilere erişim sağlama, düzeltme talebinde bulunma, verilerin silinmesini veya yok edilmesini isteme, bildirim talep etme, işleme faaliyetlerine itiraz etme ve uğranılan zararın giderilmesini isteme gibi haklar tanımaktadır.

Veri sorumluları bakımından ise KVKK'nin 10 uncu maddesi aydınlatma yükümlülüğünü, 12 nci maddesi veri güvenliğinin sağlanmasına ilişkin yükümlülükleri ve 16 ncı maddesi ise veri sorumluları siciline kayıt yükümlülüğünü düzenlemektedir. Buna ek olarak, anılan Kanunda açıkça belirtilmemekle beraber, ilgili kişilerin başvurularına yanıt verme ve Kurul kararlarına uyma gibi yükümlülüklerin de veri sorumlularının sorumlulukları arasında olduğu değerlendirilmektedir. Bu kapsamda aşağıda söz konusu haklar ve yükümlülükler incelenmektedir.

2.7.1 Posta kullanıcı hakları

Bu başlık altında, veri koruma mevzuatı kapsamında posta kullanıcılarının hakları incelenmektedir.

2.7.1.1 Bilgi edinme ve öğrenme hakkı

Kişisel verilerin işlenmesinde ilgili kişinin korunma isteminin temelinde *"bilgi edinme ve öğrenme hakkı"* yer almaktadır. Bu hak kapsamında ilgili kişi, ilk olarak kendisine ait kişisel verilerin işlenip işlenmediğini öğrenme hakkına sahiptir. Kişisel verilerinin işlenmesi durumunda ise veri kategorileri, işleme amaçları ve işlemenin hukuki dayanakları hakkında bilgi talep edilebilmektedir.

İlgili kişi, bu bilgiler ışığında işleme faaliyetlerinin belirli, açık ve meşru amaçlarla uyumlu olup olmadığını, aynı zamanda işlemenin amaç ile bağlantılı, sınırlı ve ölçülü şekilde gerçekleştirilip gerçekleştirilmediğini değerlendirebilmektedir. Ayrıca, kişisel verilerin yurtiçi veya yurt dışına aktarılması söz konusu ise verilerin aktarıldığı üçüncü taraflar hakkında bilgi alma hakkına da sahiptir. Bilgi edinme talebine karşı veri sorumlusu tarafından sunulan yanıt açık ve anlaşılır olmalıdır. İlgili kişi, bu yanıt doğrultusunda yaptığı değerlendirme neticesinde KVKK'nin 11 inci maddesinde düzenlenen diğer haklarını ileri sürebilmekte ve gerekli taleplerde bulunabilmektedir[267].

2.7.1.2 Kişisel verinin düzeltilmesini isteme hakkı

Bireyin kendine ait verileri üzerindeki kontrolünün bir tezahürü olarak görülen bu hak, KVKK'nin 11 inci maddesinin birinci fıkrasının (d) bendi ile ilgili kişiye; "kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme" hakkı olarak düzenlenmiştir. Benzer biçimde, bu hak GDPR'ın 16 ncı maddesinde kendine yer bulmuştur.

Bu hak KVKK'nin 4 üncü maddesinin ikinci fıkrasının (b) bendinde önemli bir ilke olarak yer alan, verilerin "doğru ve gerektiğinde güncel olması" ilkesi çerçevesinde ilgili kişiye, kişisel verilerinin eksik veya yanlış işlenmesi durumunda veri sorumlusundan bu verilerin düzeltilerek eksik verilerin tamamlanmasını veya hataların giderilmesini talep etme hakkı tanımaktadır. İlgili kişilerin bu taleplerini iletmelerinde ise herhangi bir şekil şartı bulunmamaktadır. Hatta taleplerin doğrudan "düzeltme talebi" olarak ifade edilmesi de zorunlu değildir. Kişisel verilerin eksik yahut yanlış işlenmesi hâlinde ortaya çıkabilecek zararların önlenmesi amacıyla verilerin doğru ve güncel olması gerekmektedir[268]. Veri sorumlusu da herhangi bir

[267] Yasemin, Avcı, *Kişisel Verilerin Korunması*, (Yüksek Lisans Tezi, Selçuk Üniversitesi, 2019): 83.
[268] AİHM 2. Dairesi Kararı, 18.11.2018 günlü, 22427/04 başvuru numaralı karar.

şart aramaksızın talebi yerine getirmelidir. Aksi takdirde veri işleme faaliyeti, hukuka aykırı duruma gelecektir.

Diğer yandan KVKK kapsamında; ilgili kişinin kimlik, iletişim veya adres bilgisi gibi kişisel verilerinin düzeltilmesini talep etmesi halinde veri sorumlusunun yine bu talebi yerine getirmesi gerekmektedir. Ancak bazı sektörlerde, bu tür değişiklik taleplerinin müşteri tanımlama ve güvenlik süreçleri açısından önemli olması nedeniyle belirli koşullara tabi tutulduğu görülmektedir. Örneğin; isim değişikliği taleplerinin, kişinin yasal kimlik bilgileriyle doğrudan ilişkili olması nedeniyle, bankalar tarafından bu taleplerin kanuni bir dayanağa dayandırılması talep edilebilmektedir. Bu bağlamda, banka değişiklik talebinin doğruluğunu teyit edebilmek amacıyla ilgili kişiden kimlik belgesi, ehliyet gibi gerekli kanıtları sunması istenebilmektedir[269].

Posta sektörü bağlamında değerlendirildiğinde, veri sorumlusunun, verileri gerektiğinde yetkili mercilere aktarma yükümlülüğü ve diğer yasal sorumlulukları çerçevesinde bu verilerin doğru ve güncel biçimde tutulmasından sorumlu olduğu görülmektedir. Bu doğrultuda, ilgili kişilerin düzeltme taleplerinin yerine getirilebilmesi için birtakım kanıtların sunulmasının gerekli olduğu ifade edilebilir. Ancak talep edilen kanıtların makul sınırlar içerisinde olması ve ilgili kişilerin düzeltme haklarının etkin kullanımını engellememesine dikkat edilmelidir.

2.7.1.3 Kişisel verinin düzeltilmesi, silinmesi veya yok edilmesini isteme hakkı

Teknolojik ilerlemeler sonucunda verilerin kayıt altına alınması ve paylaşım hızının sürekli artması, kişisel verilere erişimin daha kolay ve hızlı hale gelmesine neden olmuştur. Bu durum, kişisel verilerin bireylerin yaşamları üzerinde kalıcı etkiler yaratmasına zemin hazırlamaktadır. Bireylerin toplumsal alandan geri çekilme veya yayılan bilgilerinin gölgesinde bir yaşam sürdürmeme talepleri, günümüzde

---

[269] Özcan, *Bankacılık İş ve İşlemlerinde…,* 95.

"unutulma hakkı" olarak da adlandırılan kavrama olan ihtiyacı doğurmuştur. Modern teknolojik gelişmeler ışığında, bu hak artık kişisel verilerin korunmasına ilişkin ilkelerin dijital ortamda uygulanabilir hale getirilmesiyle ilişkilendirilmektedir[270].

KVKK'de "unutulma hakkı" ile ilgili doğrudan bir hüküm yer almamaktadır. Bununla birlikte, genel veri işleme kuralları ile yasal düzenlemelerin uygulanması suretiyle verisi işlenen kişinin mevzuat ile tanınan koşulları sağlaması durumunda verinin silinmesi ve yok edilmesi mümkün olmaktadır[271].

GDPR'ın 17 nci maddesinin birinci fıkrası uyarınca ise veri sahibinin kendisiyle ilgili kişisel verilerin herhangi bir gecikme olmaksızın silinmesini talep etme hakkı bulunmaktadır. Bunun yanı sıra belirli hallerin varlığı durumunda veri sorumlusuna bu verileri gecikmeksizin silme yükümlülüğü de getirilmiştir. Bu durumlar arasında ilk sırada, "kişisel verilerin toplandıkları veya işlendiği amaçlar doğrultusunda artık gerekli olmaması" yer almaktadır. Bu hak, kişisel verilerin yanlış olma veya güncelliğini yitirme riskine karşı silinmesine olanak tanımakta ve veri işlemenin belirli ve sınırlı bir amaç çerçevesinde gerçekleştirilmesi ilkesine uygunluğu sağlamaktadır[272].

Posta sektörü açısından bu hak, ilgili düzenlemeler çerçevesinde işlenen kişisel verilerin, işleme amacının ortadan kalkması durumunda silinmesini veya yok edilmesini talep etme imkânı sunmaktadır. Buna göre, mevzuattan doğan yükümlülüklerin sona ermesi hâlinde PHS'lerin, veri sahiplerinin taleplerini belirlenen süreler içinde değerlendirerek gerekli işlemleri yerine getirmekle yükümlü olduğu değerlendirilmektedir. İlaveten, artık güncel olmayan kimlik ve adres bilgisi gibi kişisel verilerin PHS kayıtlarından re'sen silinmesi ya da bunların düzeltilmesine yönelik kullanıcı taleplerinin de olumlu sonuçlandırılması gerektiği düşünülmektedir.

---

[270] Aydın, Akgül, "Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" ve AB Adalet Divanı'nın "Google Kararı"", *Türkiye Barolar Birliği Dergisi*, Sayı: 116, (2016): 14.
[271] Bkz. 1.1.6 Kişisel verilerin imhası başlığı
[272] Özsoy, *Kişisel Verilerin Korunması…,* 96.

2.7.1.4 Düzeltme ya da silme veya anonim hale getirme taleplerinin üçüncü kişilere bildirilmesi hakkı

Veri sorumlusu, ilgili kişinin başvurusu üzerine, doğru olmayan kişisel verileri düzeltse dahi veri aktarılan üçüncü taraf doğru olmayan veriyi kullanabilir. İlgili kişinin isteği neticesinde silinen kişisel veri, bu durumdan haberdar olmayan üçüncü tarafça kullanılmaya devam edilebilir. Bu olasılıkları dikkate alan kanun koyucu, ilgili kişiye, üçüncü kişilere taleplerin bildirilmesi hakkını tanımıştır[273]. Bu kapsamda KVKK'nin 11 inci maddesinin birinci fıkrasının (f) bendi gereğince; ilgili kişi, kişisel verilerinin düzeltilmesini, silinmesini veya anonim hale getirilmesini, verilerin aktarıldığı üçüncü kişilere bildirilmesini isteyebilmektedir.

GDPR'da ise bu hak, ayrıca düzenlenmemiş, veri sorumlusuna bir yükümlülük olarak getirilmekle yetinilmiştir. Düzenleme gereği veri sorumlusu, her türlü düzeltme, silme yahut işleme faaliyetini kısıtlama talebini bu verilerin açıklandığı kişilere bildirmekle yükümlüdür. Veri sahibinin bu doğrultuda bir isteğinin bulunması durumunda, veri sahibini bu verilerin açıklandığı kişiler hakkında bilgilendirir. Ancak GDPR'ın 19 uncu maddesi uyarınca bu durumun "imkânsız olmaması veya ölçüsüz bir çabayı gerektirmemesi" gerekmektedir[274].

Söz konusu hak posta sektörü bağlamında değerlendirildiğinde, gönderici veya alıcıya ait kişisel verilerin, hizmetin sunumu sırasında üçüncü taraflarla (örneğin taşeron firmalar ya da iş ortaklarıyla) paylaşılması halinde, veri sahibinin düzeltme, silme ya da anonimleştirme taleplerinin yalnızca PHS nezdinde uygulanmasının yeterli olmayacağı, aynı zamanda bu verilerin paylaşıldığı üçüncü taraflara da iletilmesi gerektiği değerlendirilmektedir.

---

[273] Oğulcan, Özkan, *Kişisel Verilerin Korunması*, (Yüksek Lisans Tezi, Ankara Üniversitesi, 2020): 192.
[274] P.T.J., Wolters, "The Control by and Rights of the Data Subject Under the GDPR", *Journal of Internet Law*, Cilt: 22, Sayı: 1, (2018): 8.

2.7.1.5 Veri taşınabilirliği hakkı

Veri taşınabilirliği hakkı, kişisel verilerin korunması alanında ilk kez GDPR'ın 20 nci maddesinde düzenlenmiştir[275]. Bu hak; kişisel verilerin işlenmesinin otomatik araçlarla gerçekleştirildiği hallerde "veri öznesinin kendisi ile ilgili olarak bir veri sorumlusuna sağladığı kişisel verileri; yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek" formatta alabilmesine ve bir engelle karşılaşmaksızın başka bir veri sorumlusuna iletebilmesine yönelik bir haktır[276].

Hakkın kullanımına örnek olarak Amsterdam Bölge Mahkemesi'nin "Ola's Driver App" kararı verilebilir. Mahkeme tarafından, davacıların şoför olarak çalıştığı taksi uygulamasından veri taşınabilirliği hakları kapsamındaki taleplerinin yerine getirilmediği iddiası değerlendirilmiştir. Şoförler, kişisel verilerinin belirli bir format aracılığıyla bir kâr amacı gütmeyen kuruluş olan WIE'ye aktarılmasını talep etmiş ancak davalı tarafından yalnızca verilerin bir kısmı talep edilen formatta sağlamıştır. Mahkeme ise GDPR'ın 20 nci maddesi uyarınca, kişisel verilerin yalnızca talep edilen formatta değil, makine tarafından okunabilir başka uygun formatlarda da sağlanabileceğine dikkat çekmiştir. Ayrıca, veri sahiplerinin isteklerinde hangi verilerin talep edildiğinin açık bir biçimde belirtilmediği nedeniyle davalının, başkalarının temel hak ve hürriyetlerine zarar vermemek için şoförlerin kişisel verilerinin tümünü sağlamamasının GDPR'a aykırı olmadığına yönelik karar vermiştir[277].

KVVK'de ise GDPR'dan farklı olarak veri taşınabilirliği hakkına yer verilmemiştir. Posta sektörü açısından bakıldığında da bu hakka örnek teşkil edebilecek bir uygulama

---

[275] Paul, De Hert, Vagelis, Papakonstantinou, Gianclaudio, Malgieri, Laurent, Beslay ve Ignacio, Sanchez, "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", *Computer Law & Security Review*, Cilt: 34, Sayı: 2, (2018): 194.
[276] Özsoy, *Kişisel Verilerin Korunması…,* 111.
[277] Hollanda Yargı Konseyi (de Rechtspraak) Kararı. InstantieRechtbank Amsterdam, 11.03.2021 günlü, C/13/689705 sayılı Ola's Driver App Kararı.

bulunmamaktadır. Çünkü her bir PHS kendi veri havuzunu, adres bilgi sistemini kendisi oluşturmaktadır. Söz konusu uygulamanın posta sektörüne uyarlanabilirliği konusunun; taşınacak olan verinin, veri sahibinin sıfatı, açık rızasının olup olmadığı gibi kriterler çerçevesinde ayrıca çalışılması gerekli bir husus olduğu değerlendirilmektedir.

Zira, veri taşımaya yönelik Türk hukukunda yer alan tek örnek uygulama, elektronik haberleşme sektöründe görülmektedir. Bu konu, Avrupa'daki Evrensel Hizmet Direktifine benzer olarak hazırlanan 02.07.2009 tarihli ve 27276 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren "Numara Taşınabilirliği Yönetmeliği" ile düzenlenmektedir[278].

2.7.1.6 İtiraz hakkı

KVKK'nin 11 inci maddesinin birinci fıkrasının (g) bendi uyarınca ilgili kişilere tanınan itiraz hakkı; *"işlenen verilerin otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkması"* halinde kullanılabilmektedir. Bu düzenlemede itiraz hakkının yalnızca otomatik veri işleme süreçlerinde geçerli olduğu, manuel veri işlemenin bu kapsamda değerlendirilmediği belirtilmektedir.

Teknolojinin yaşamımızda kullanımının artmasının etkisiyle birlikte bireylerin bilgilerini geniş kitlelere hızla iletebilmesi ve akıllı telefon tabanlı uygulamaların yaygınlaşması, niteliği bakımından farklılık gösteren otomatik veri sistemlerinin gelişimini teşvik etmiştir. Bu sistemler aracılığıyla bireylerin gerçekleştirdiği işlemlere dair veriler kayıt altına alınmakta ve böylece gelecekteki alışkanlık ve davranışlarının öngörülebileceği bir yapı oluşturulmaktadır. Bu yapı, bireye özgü bir profil oluşturulmasına imkân tanımaktadır. Otomatik veri kaydı gerçekleştiren ve

---

[278] Beste, Yılmaz, *Kişisel Verilerin Korunması ve Rekabet Hukuku Bağlamında Veri Taşınabilirliği Hakkı*, (Yüksek Lisans Tezi, İhsan Doğramacı Bilkent Üniversitesi, 2022): 10.

günümüzde "profilleme" olarak adlandırılan bu sistem, KVKK'nin ilgili maddesinde yer alan tanıma en uygun örneklerden biri olarak değerlendirilmektedir[279].

Diğer yandan itiraz hakkı, GDPR kapsamında daha detaylı olarak ele alınmıştır. GDPR'ın 21 nci ve 22 nci maddesinde iki bölüm halinde düzenlenen bu hak; otomatik kararlara yapılacak itiraz hakkını, ilgili kişinin özel durumu nedeniyle itiraz hakkını ve kişisel verilerin doğrudan pazarlama amacı ile kullanılmasına itiraz hakkını kapsamaktadır. GDPR'ın 21 nci maddesi uyarınca ilgili kişinin kendisine ait özel durumlardan kaynaklı nedenlere dayalı olarak, profil çıkarma dâhil olmak üzere, her daim itiraz hakkı bulunmaktadır.

Posta sektöründe ise profilleme uygulamaları, kişilerin teslimat alışkanlıkları ile işlem geçmişlerine dayalı olarak farklı otomatik değerlendirme süreçlerini içerebilmektedir. Örneğin, PHS'ler tarafından teslimat tercihleri analiz edilerek bir alıcının sıklıkla bulunduğu teslimat adresinin veya teslimat için tercih ettiği zaman aralıklarının sistem tarafından tespit edilebilmesi mümkündür. Bu sayede posta hizmeti sunumunda teslimat zamanı, kullanıcıların alışkanlıklarına uygun şekilde belirlenebilmektedir. Örneğin; bir alıcının genellikle akşam saat 17.00'dan sonra evde olduğu bilgisi dikkate alınarak bir planlama yapılabilir. Diğer yandan güvenlik amacıyla da profilleme yapılabilir. Belirli bir gönderim sıklığı ya da içeriğine sahip kullanıcıların (örneğin kurumsal gönderiler) davranışları sistemde normal olarak tanımlanabilirken, aksi işlemler (kurumsal gönderi niteliğinde olmayan birden fazla yüksek değerli gönderi veya göndericinin daha önce kabulü yasak madde göndermek amacıyla PHS'ye gönderi bırakması) riskli veya şüpheli olarak işaretlenebilir.

Diğer yandan kullanıcıların gönderi türü, sıklığı ve teslimat biçimi gibi veriler analiz edilerek pazarlama amacıyla kişiselleştirilmiş teklifler ve kampanyalar

---

[279] Özcan, *Bankacılık İş ve İşlemlerinde…,* 100.

sunulabilmektedir[280]. Bu tür işlemlerin, posta sektöründe otomatik karar alma kapsamında değerlendirilebileceği ve bu ilgili kişinin bu kararlardan olumsuz etkilenmesi halinde itiraz hakkının doğabileceği düşünülmektedir. Kullanıcı şikâyetlerin bu alanda belirgin bir biçimde yoğunlaşması halinde gerekli düzenlemeler yapılabilir.

2.7.1.7 Tazminat hakkı

Tazminat hakkı, ilgili kişinin kişisel verilerinin ihlali halinde; diğer haklarının kullanımıyla giderilemeyecek zararlarının giderilmesi hususunda güvence sağlayan bir haktır. İlgili kişi bu hak ile açık rızayı geri alma olanağının ötesine uzanan bir bireysel kontrol mekanizmasına dahil edilmektedir[281]. Genel hükümlere göre hakları ihlal edilen veri sahiplerinin maddi veya manevi tazminat talep etme hakkı bulunmakla birlikte, veri koruma kurallarının etkinliğini sağlamak amacıyla ilgili kişilere, özel ve doğrudan zararlarının giderilmesini talep etme hakkı da tanınmıştır. Tazminat sorumluluğu sayesinde, veri sorumluları; kanuni düzenlemelere uymaya, güvenlik önlemlerini artırmaya ve kişilerin haklarına saygı göstermeye teşvik edilmektedir.

KVKK'de düzenlenen *"ilgili kişinin hakları"* başlıklı 11 nci maddenin son bendi kapsamında yer verilen tazminat hakkı uyarınca; *"herkes, veri sorumlusuna başvurarak kendisiyle ilgili kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir"*. Bununla birlikte KVKK'nin *"Kurula şikâyet"* başlıklı 14 ncü maddesinin üçüncü fıkrasına göre kişilik hakları ihlâl edilenlerin genel hükümlere göre tazminat hakkı saklıdır.

---

[280] MNG Kargo, "Genel Aydınlatma Metni".

[281] Gabriela, Zanfir-Fortuna, *"Article 82. Right to compensation and liability", The EU General Data Protection Regulation (GDPR): A Commentary,* ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler, (Croydon: Oxford University Press, 2020): 1164.

Tazminat hakkına örnek olarak, ABAD tarafından 2023 yılında bir PHS'ye ilişkin verilen karar gösterilebilir. Anılan kararda, kişisel verilerin hukuka aykırı işlenmesi nedeniyle tazminat taleplerine ilişkin önemli bir değerlendirme yapılmıştır. Karara konu olayda, bir PHS, veri sorumlusu sıfatıyla Avusturya vatandaşlarının çeşitli sosyal ve demografik verilerini analiz eden bir algoritma kullanmıştır. Bu analizler sonucunda vatandaşların hassas verisi olan siyasi eğilimleri tahmin edilmiş ve "hedef grup adresleri" oluşturularak üçüncü kişilere pazarlanmıştır. Üçüncü kişiler ise bu bilgileri siyasi reklam faaliyetlerinde kullanmıştır. Somut olayda başvuru sahibi, algoritmanın kendisini belirli bir siyasi partiye yüksek düzeyde yakınlık gösteren bir birey olarak tahmin ettiğini belirtmiştir. Başvuru sahibi, kişisel verilerinin bu şekilde işlenmesine rızası olmadığını ifade etmiş ve bu durumun üçüncü kişilerle paylaşılmamış olsa dahi kendisinde ciddi bir üzüntü duygusuna yol açtığını ileri sürmüştür. Bu bağlamda duygusal zarar gördüğünü iddia ederek tazminat talebinde bulunmuştur. Talep sonucu verilen Kararda tazminata hükmedilebilmesi için bir zararın oluşması, GDPR ihlalinin olması ve zararla ihlal arasında nedensellik bağının olması biçiminde üç temel şartın sağlanması gerektiği belirtilmiştir. Ayrıca Karar'da, zarar meydana gelmeden yalnızca GDPR ihlalinin tespit edilmesi durumunda tazminata hükmedilmesinin mümkün olmadığını vurgulamıştır. Bu tür durumlarda yalnızca idari para cezasının uygulanabileceği, GDPR uyarınca manevi tazminat taleplerinde zararın belirli bir ağırlık eşiğini aşması koşulunun da aranmayacağı, her türlü zarar için hakkaniyete uygun bir tazminata karar verilebileceği belirtilmiştir[282].

2.7.2 Posta hizmet sağlayıcısının yükümlülükleri

Posta sektöründe kişisel verinin korunması kavramına, KVKK'nin yürürlüğe girmesinden önce PHK'nin 12 nci maddesinin (b) bendinde PHS'lerin yükümlülükleri arasında *"Kişisel veri ve bilgilerin gizliliğinin korunması yükümlülüklerine uymak"*

[282] Avrupa Birliği Adalet Divanı Kararı, 04.05.2023 günlü, C-300/21 numaralı Österreichische Post kararı.

hükmü ile yer verilmiştir. Diğer yandan, KVKK'nin yürürlüğe girmesiyle kişisel veriler konusunda temel ve kişilik haklarının korunmasına ilişkin özel bir kanun olma[283] niteliğini haiz bir düzenleme ortaya çıkmış ve posta sektöründe kişisel veri koruma esasları bu Kanuna tabi hale gelmiştir. Diğer yandan bu bölümde, posta sektörüne ilişkin düzenlemelerde yer alan spesifik konularda PHS'lere yönelik bazı yükümlülüklerin de altı çizilecektir.

2.7.2.1 Aydınlatma yükümlülüğü

Aydınlatma yükümlülüğü ile kişisel verilerin elde edilmesi esnasında ilgili kişilerin bilgilendirilmesi amaçlanmaktadır. Bu doğrultuda veri sorumlusu ya da yetkilendirdiği kişiler, KVKK'nin 10 uncu maddesinde belirtilen; *"veri sorumlusunun ve varsa temsilcinin kimliği, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel verileri toplamanın yöntemi ve hukukî sebebi ile 11 inci maddede sayılan ilgili kişinin diğer hakları*" hususlarında ilgili kişiye bilgi vermekle yükümlüdür[284].

Aydınlatma yükümlülüğü, veri sorumluları bakımından bir yükümlülük olmakla birlikte veri sahibi açısında da bir haktır. Veri sahibinin, işlenen kişisel verilerine ilişkin bilgilendirilmesini açıklayan bu yükümlülük, kişisel verilerin hukuka uygun biçimde işlenmesi için elzemdir[285]. Ayrıca kişisel veriler, hangi hukuki işleme sebebine dayanılarak işlenirse işlensin, veri sorumlusu tarafından aydınlatma yükümlülüğü her durumda yerine getirilmelidir[286].

---

[283] Ali Haydar, Doğu, "Kişisel Verilerin Korunmasına Genel Bir Bakış", *Karadeniz Teknik Üniversitesi*, (2017).
[284] Avcı, *Kişisel Verilerin Korunması*, 86.
[285] Kişisel Verileri Koruma Kurumu, "Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu Duyurusu", (2020).
[286] Kişisel Verileri Koruma Kurumu, "6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında…": 35.

Söz konusu yükümlülük gereğince ilgili kişi veya kurum ile paylaşılacak bilginin anlaşılır, kolay ulaşılabilir, basit ve sade bir dille hazırlanması, kesin olmayan muğlak ifadelerden uzak durulması gerekir. Bu durum "dürüstlük kurallarına uygun olarak işleme ilkesi" ile KVKK'de yer verilmemiş olsa dahi "şeffaflık ilkesi"nin bir gereği olarak görülmektedir[287].

Diğer yandan aydınlatma yükümlülüğünün yerine getirilmesinde 10.03.2018 tarihli ve 30356 sayılı Resmî Gazete yayımlanarak yürürlüğe giren *"Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ* (Aydınlatma Yükümlülüğü Tebliğ)"e de uyulması gerekir. Söz konusu Tebliğ'in 5 inci maddesinde, veri sorumlusu yahut yetkilendirmiş olduğu kişi tarafından yazılı, sözlü, çağrı merkezi, ses kaydı gibi fiziki veya elektronik ortam kullanılarak anılan yükümlülüğünün yerine getirilmesi sırasında uyulması gerekli kurallar düzenlenmiştir. Buna göre, ilgili kişinin açık rızasının veya kanundaki diğer kişisel veri işleme koşullarının bulunması halinde veri sorumlusu, aydınlatma yükümlülüğünü yerine getirmelidir. Ayrıca bu yükümlülük, ilgili kişinin talebine bağlı olmadığı gibi, yükümlülüğe uyulduğunun ispatı veri sorumlusundadır. Bununla birlikte veri sorumlusu, kişisel verilerin hangi üçüncü taraflara aktarılacağını tek tek belirtmekle yükümlü olmayıp bu kişilerin faaliyet ve sektör alanlarına (örneğin; *"işlenen kişisel verileriniz, sözleşme ilişkisi içerisinde bulunduğumuz PHS'lere, sanal POS ile ödeme yapılması için ilgili bankalara, e-ticaret aracı hizmet sağlayıcılarına, tedarikçilerimiz ile kanunen yetkili kamu kurum ve kuruluşlarına aktarılabilecektir"* gibi yapılarak) yer vermesi yeterlidir[288].

Bunun yanı sıra KVKK'de aydınlatma yükümlülüğünün nasıl yerine getirileceği konusunda bir düzenleme bulunmamaktadır. Yükümlülük, sözlü ya da yazılı olarak

---

[287] Şehriban İpek, Aşıkoğlu, "Veri Sorumlularının Aydınlatma Yükümlülüğü, -Avrupa Birliği ve Türk Hukukunda-", *Kişisel Verileri Koruma Dergisi*, Cilt: 1, Sayı: 2, (2019): 45-46.
[288] Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanunu Hakkında Sıkça…,* 82.

yerine getirilebileceği gibi katmanlı aydınlatmanın[289] da yapılması da mümkündür. Zira, çeşitli sektörler tarafından verilen hizmetler farklı kanallardan takip edilmekte olup çağrı merkezi gibi kanallarda ilgili kişilerin aydınlatma metinlerinin tamamını dinlemesinin doğru bir yöntem olmayacağı nedeniyle ön bilgilendirmeyle katmanlı aydınlatma yöntemi kullanılabilecektir. İnternet sitesi aracılığıyla yapılacak olan işlemlerde ise ilgili kişinin bir bağlantıyla aydınlatma metnine yönlendirilmesi uygun olacaktır[290]. PHS'ler tarafından verilen posta hizmetinin aşamaları da SMS, internet sitesi, mobil uygulama veya çağrı merkezi gibi kanallardan takip edilebilmekte olup posta kullanıcısının aydınlatma metninin tamamını okuması ya da dinlemesinin uygulanabilir bir yöntem olmayacağı hallerde, ön bilgilendirme yoluyla katmanlı aydınlatma yönteminin uygulanmasının doğru bir yaklaşım olacağı değerlendirilmektedir. Genellikle çağrı merkezleri arandığında *"kişisel verilere ilişkin aydınlatma yükümlülüğümüze dair bilgilendirme için …. numarasını tuşlayın"* şeklinde yapılan bilgilendirmeler katmanlı aydınlatmaya örnektir.

Öte yandan doktrindeki bir görüşte, aydınlatmanın yazılı olarak yapılacağı hallerde, TKHK gereği, ilgili kişinin belirli nitelikteki bir yazıyla aydınlatılması gerektiği belirtilmektedir. Bu durumda, ilgili kişiyi bilgilendiren yazının puntosunun asgari on iki olması, anlaşılır bir dilinin olması ile okunabilir, sade ve açık şekilde düzenlenmesi gerekmektedir[291]. Bu kapsamda 23.09.2019 tarihli ve 2019/DK-SRD/206 sayılı Bilgi Teknolojileri ve İletişim Kurulu Kararında;

---

[289] Katmanlı aydınlatma: Kişisel verilerin elde edilmesi sırasında ilgili kişiye, kişisel verilerinin elde edildiği konusunda ön bilgilendirme yapılarak, ilgili kişinin Kanun'un 10 uncu maddesine uygun aydınlatmaya yönlendirilmesidir (Kişisel Verileri Koruma Kurumu, *Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi*).

[290] Merve, Arslanhan, "Bankaların Bilgi Güvenliği Yönetimi Kapsamında Banka Müşterilerinin Kişisel Verilerinin Korunması", *Kişisel Verileri Koruma Dergisi*, Cilt: 6, Sayı: 2, (2024): 38.

[291] Arslanhan, "Bankaların Bilgi Güvenliği Yönetimi…": 38.

"…

Posta hizmet sağlayıcılarının;

1. Kayıtlı gönderilere ilişkin yetkilendirmeleri kapsamındaki hizmetler için düzenlemekle yükümlü oldukları hizmet sunumunu ispatlayan belgede en az 12 (on iki) punto siyah harfler ile açık, sade ve anlaşılabilir olarak belirtilecek şekilde kullanıcılar (gönderici ve alıcı) ile mevzuattan kaynaklanan karşılıklı hak ve yükümlülüklerine dair asgari;

- Hizmetin kapsamı (adrese teslim, şubede teslim gibi), gönderinin azami teslim süresi ve mevzuata dayalı mücbir haller dışında azami teslim süresinin sağlanamaması durumunda tazminat ve/veya geri ödemeye ilişkin prosedür başta olmak üzere kullanıcı haklarını içeren hizmet seviyesi taahhüdüne,

- Gönderinin çalınması, kaybı, hasarı veya eksik teslimatı halinde hizmet sağlayıcı tarafından uygulanacak tazminat ve/veya geri ödeme prosedürüne,

- Kullanıcının, kimlik bilgileri ve gönderinin içeriği konusunda hizmet sağlayıcıyı doğru bilgilendirme yükümlülüğü olduğu ve aksi durumda doğacak sorumluluğun kullanıcıda olduğu bilgisine,

- Uyuşmazlık hallerinde yargı yolu da dâhil olmak üzere uygulanacak çözüm prosedürü ve başvurulacak yetkili merci bilgisine

yer vermeleri,

…"

ile PHS'lerin aydınlatma yükümlülüğü kapsamında, hizmet sunumunu ispatlayan belge düzenlerken yer verilmesi gereken temel hususlar düzenlenmiştir[292].

Diğer yandan 03.08.2021 tarihli ve 2021/DK-SRD/212 sayılı Bilgi Teknolojileri ve İletişim Kurulu kararıyla PHS'lerin;

[292] Bilgi Teknolojileri ve İletişim Kurulu Kararı, 23.09.2019 günlü, 2019/DK-SRD/206 sayılı karar.

"...

*2. Hizmet sunumunu ispatlayan belgeleri göndericinin bilgi ve onayı dâhilinde dijital olarak düzenleyebilmeleri; bahse konu belge ve gerekli bilgilendirme metinlerini kullanıcılar (gönderici ve alıcı) ile SMS, internet sitesi bağlantısı veya benzeri yöntemler vasıtasıyla paylaşabilmeleri, anılan belgenin fiziksel olarak talep edilmesi halinde ise kullanıcılara bu imkânı sağlamaları,"*na

olanak tanınmıştır[293].

2.7.2.2 İlgili kişilerin başvurularının cevaplanması ve KVK Kurulu kararlarının yerine getirilmesi yükümlülüğü

KVKK'nin 13 üncü maddesi ile 22 nci maddesinin birinci fıkrasının (e) ve (g) bentlerine dayanılarak hazırlanan ve 10.03.2018 tarihli ve 30356 sayılı Resmî Gazete'de yayımlanan *"Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ"* (Veri Sorumlusuna Başvuru Tebliği) uyarınca, ilgili kişiler veri sorumlusuna başvuruda bulunabilir.

Veri Sorumlusuna Başvuru Tebliğinin 6 ncı maddesi gereğince veri sorumluları, ilgili kişi tarafından iletilen başvuruları, taleplerin niteliğine göre mümkün olan en kısa vakitte ve en geç otuz gün içerisinde sonuçlandırmakla yükümlüdür. Veri sorumlusu, başvuruya ilişkin olarak talebi kabul etmesi veyahut gerekçesini açıklamak suretiyle reddetmesi durumunda, bu yanıtını yazılı ya da elektronik ortamda ilgili kişiye bildirmekle yükümlüdür. Talebin kabulü hâlinde, veri sorumlusunca söz konusu talep yerine getirilmelidir.

Başvurunun reddedilmesi, verilen yanıtın yetersiz bulunması ya da süresi içinde herhangi bir yanıt verilmemesi hâlinde; ilgili kişi, veri sorumlusunun yanıtını öğrendiği

---

[293] Bilgi Teknolojileri ve İletişim Kurulu Kararı, 03.08.2021 günlü ve 2021/DK-SRD/212 sayılı karar.

tarihten itibaren otuz gün ve her durumda başvuru tarihinden itibaren en geç altmış gün içerisinde KVK Kurulu'na şikâyet yoluyla başvurabilir. KVK Kurulu, yapılan şikâyet sonucu yahut re'sen inceleme başlatabilir. İnceleme sonucunda bir hukuka aykırılık tespit edilmesi durumunda Kurul, veri sorumlusunun ilgili ihlali gidermesine karar verir ve bu kararı taraflara tebliğ eder. Veri sorumlusu, Kurul tarafından verilen kararı tebliğ tarihinden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirmekle yükümlüdür[294].

Posta sektöründe de PHS'ler tarafından, kullanıcıların yaptığı başvurulara zamanında ve usulüne uygun şekilde cevap verilmesi ile KVK Kurulu tarafından verilen kararların yerine getirilmesinin hem yasal bir sorumluluk hem de kullanıcı memnuniyetini etkileyen bir unsur olduğu düşünülmektedir.

2.7.2.3 Veri sorumluları siciline kayıt yükümlülüğü

KVKK'nin 16 ncı maddesinin ikinci fıkrasında Veri Sorumluları Siciline (VERBİS) kayıt yükümlülüğü düzenlenmiştir. Bu hükme göre; *"Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt yükümlülüğüne istisna getirilebilir".* Ayrıca Kurulun "Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili 19.07.2018 Tarihli ve 2018/87 Sayılı Kararı" ile "yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 Milyon TL'den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar", VERBİS'e kayıt yükümlülüğünden

[294] Kişisel Verileri Koruma Kurumu, *Kanun Kapsamındaki Hak ve Yükümlülükler*, 8.

istisna tutulmuşlardır[295]. Bununla birlikte bu muafiyet, veri sorumlusu sıfatını ve mevzuata uygun davranma yükümlülüğünü ortadan kaldırmamaktadır.

VERBİS'e kayıt yükümlülüğü, ilgili kişilerin kişisel verileri üzerindeki denetim ve kontrol imkânlarını güçlendirmesi açısından büyük önem arz etmektedir. Zira, kişisel verileri işlenmek üzere açık rızaları talep edilen ilgili kişiler, kamuya açık bu sicil üzerinden veri sorumlusunun yükümlülüklerini, veri işleme amaçlarını ve veri kategorilerini inceleyerek rıza verip vermeyeceklerine dair daha bilinçli bir değerlendirme yapma olanağına kavuşmaktadır. Bu çerçevede uygulamada zaman zaman yanlış yorumlanan ve karmaşaya neden olan bir hususun altının çizilmesi gerekmektedir: KVKK'nin 16 ncı maddesinin birinci fıkrasının (c) bendi uyarınca, sicile veri işleme faaliyetleri bildirilirken, verisi işlenen kişilere ait isim ya da benzeri doğrudan tanımlayıcı herhangi bir kişisel veri beyan edilmemeli; bunun yerine yalnızca işlenen veri kategorilerine yer verilmelidir. Bu ayrımın gözetilmesi hem hukuki uyumluluk hem de kişisel veri güvenliğinin temini açısından kritik bir gerekliliktir[296].

[295] Kişisel Verileri Koruma Kurulu Kararı, 19.07.2018 günlü, 2018/87 sayılı karar.
[296] Serdar, Çelikel, *Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri*, (Doktora Tezi, Ankara Üniversitesi, 2021): 122.

3 POSTA SEKTÖRÜNDE KİŞİSEL VERİLERİN GÜVENLİĞİ

Kişisel verilerin korunmasına dair temel ilkeler arasında veri güvenliğinin sağlanması önemli bir yer tutmaktadır. Kişisel verilerin korunması, bireylerin temel hak ve özgürlüklerinin güvence altına alınmasını, veri güvenliği ise verilerin olası tehdit ve risklere karşı korunmasını hedeflemektedir. Bu bağlamda, veri güvenliği, kişisel verilerin hukuki koruma çerçevesinde güvenli bir şekilde işlenmesini ve muhafaza edilmesini sağlamaya yönelik kritik bir araç niteliği taşımaktadır[297].

Veri güvenliği, bir organizasyonun veya bireyin sahip olduğu verilerin doğruluğunu, gizliliğini ve bütünlüğünü koruma sürecidir. Bu süreç, verilerin saklanması, işlenmesi ve aktarılması sırasında alınan önlemleri kapsamaktadır. Siber güvenlik ve bilgi güvenliği kavramları ile yakından ilişkili olan veri güvenliği, olası siber saldırılar ve veri kaybı durumlarında zararların en aza indirilmesini hedefler. Yani, dijital ekonomide veri güvenliği hem bireyler hem de kurumlar için stratejik bir öncelik olup teknoloji, politika ve farkındalık unsurlarını bir araya getiren çok boyutlu bir çabayı gerektirmektedir[298].

Türkiye'de kişisel verilerin güvenliğinin korunmasına ilişkin genel düzenleme, yine KVKK ile yapılmıştır. Bu düzenleme ile veri sorumluları, kişisel verilerin hukuka aykırı biçimde işlenmesi, kişisel verilere hukuka aykırı şekilde erişilmesinin engellenmesi ve kişisel verilerin güvenli bir şekilde muhafazasının sağlanması için gerekli idari ve teknik tedbirleri almakla yükümlüdür.

Bu kapsamda bu bölümde öncelikle bilgi ve bilgi güvenliği kavramlarına yer verilmektedir. Ardından GDPR ve KVKK kapsamında kişisel veri güvenliğinden bahsedilerek, BTK düzenlemeleri de dikkate alınarak posta sektöründe PHS'lerin

---

[297] Serhat Erdem, Aydın, *AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu*, (Yüksek Lisans Tezi, İstanbul Üniversitesi, 2014): 111.
[298] Sayan, *Karşılaştırmalı Hukukta Elektronik…,* 94.

kişisel veri güvenliğinin sağlanması konusundaki yükümlülükleri ve alması gereken önlemler açıklanmaktadır. Ayrıca 19.03.2025 tarihli ve 32846 sayılı Resmî Gazete'de yayımlanan 7545 sayılı Siber Güvenlik Kanunu ile kurulan Siber Güvenlik Kurulu hakkında bazı bilgilere yer verilerek, bu yeni Kanun'un posta sektöründeki veri güvenlik düzenlemeleri üzerindeki etkileri ortaya konulmaktadır.

3.1 Bilgi ve Bilgi Güvenliği

"Information" sözcüğünün Türkçe karşılığı olarak kimi zaman "enformasyon", kimi zaman ise "bilgi" kavramları kullanılmaktadır. Özellikle "bilgi" kavramı genellikle hem "information" hem de "knowledge" anlamında kullanılmakta ve bu iki kavram arasında net bir ayrım yapılmamaktadır. Ancak bu iki kavram, çeşitli farklılıklar barındırmaktadır. Zira Paul S. Myers, "information"ı anlam kazanan veri, "knowledge"ı ise değer kazanan enformasyon olarak tanımlamaktadır[299].

Diğer organizasyon varlıkları gibi, bir organizasyonun işleyişine önemli katkı sağlayan temel unsurlardan biri olan bilgi; evrak üzerine basılı ya da yazılı, elektronik ortamda depolanmış, posta yoluyla iletilmiş, elektronik olarak aktarılmış, filmlerde gösterilmiş ya da konuşmalarda ifade edilmiş şekilde olabilmektedir. Bilginin biçimi, işlevi veya paylaşım ya da depolama yöntemi ne olursa olsun, her zaman uygun şekilde korunması gerekmektedir[300].

Bilgi güvenliği kavramı ise elektronik ortamlarda verilerin yahut bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğünün bozulmaksızın izinsiz erişimlerden

---

[299] Hakan, Çetin, "Kişisel Veri Güvenliği ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi", *Akdeniz İ.İ.B.F. Dergisi*, Cilt: 29, (2014): 88-89.

[300] Uluslararası Telekomünükasyon Birliği, *ITU-T Recommendation X.1051, SERIES X: Data Networks, Open System Communications And Security Telecommunication security, Information technology-Security techniques-Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*, (2008): 3.

korunması amacıyla, güvenli bir bilgi işleme platformu oluşturma çabalarının tümü biçiminde tanımlanabilmektedir[301].

Bilgi güvenliği; bütünlük, gizlilik, kullanılabilirlik, kimlik doğrulama, yetkilendirme, şifreleme ve güvenlik politikaları olmak üzere yedi temel ilkeden oluşmaktadır. Bu ilkeler özetle aşağıdaki şekilde ifade edilebilmektedir:

- Bütünlük: Verilerin güvenilirliğinin ve doğruluğunun garanti edilmesi ile yetkisiz değişikliklerden uzak tutulması anlamına gelir.
- Gizlilik: Hassas bilgilere yalnızca yetkilendirilmiş kişilerin erişimini sağlama sürecini ifade eder.
- Kullanılabilirlik: Sistemler ve verilerin gereklilik hâlinde kullanılabilir ve erişilebilir olmasını sağlamayı belirtir.
- Kimlik Doğrulama: Kullanıcılar yahut varlıkların kimliklerinin doğrulanması için temel bir adımdır.
- Yetkilendirme: Kullanıcıların rollerine ve ayrıcalıklarına göre bilgilere erişimlerini kontrol etmeyi içerir.
- Şifreleme: Verileri okunamayacak bir şekle dönüştürerek güvenliğini sağlama yöntemidir.
- Güvenlik Politikaları: Bilgi güvenliğini sağlama uygulamalarına yönelik yönerge ve kuralların belirlenmesidir[302].

3.2 Kişisel Veri Güvenliği

Kişisel verilerin güvenliği, bilgi güvenliğinin bir alt kategorisi olması nedeniyle kendine özgü nitelikler ve gereklilikler barındırmaktadır. Bu doğrultuda, kişisel verilerin

---

[301] Gürol, Canbek ve Şeref, Sağıroğlu, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Politeknik Dergisi*, Cilt: 9, Sayı: 3. (2006): 165.

[302] Erdal, Bayrakcı ve Mehmet Ali, Koçman, "Bilgi Güvenliği ve Elektronik Harp", *Necmettin Erbakan Üniversitesi Siyasal Bilgiler Fakültesi Dergisi,* 5 (Özel Sayı), (2023): 186.

güvenliğinin sağlanması aşamasında genel bilgi güvenliği önlemlerinin yanı sıra, veri koruma hukuku ile öngörülen özel ilke ve kuralların da dikkate alınması gerekmektedir[303].

Bu kapsamda güvenlik ilkesi, kişisel verilerin korunması alanının temel ve ayrılmaz bir unsurudur. Bu verilerin korunması, kişilerin mahremiyeti ile temel hak ve hürriyetlerini garanti altına almayı hedeflemekte olup bu hedeflerin etkin bir şekilde sağlanabilmesi için veri güvenliğine ilişkin önlemlerin titizlikle uygulanması şarttır. Veri güvenliği, yetkisiz erişim, veri sızıntıları ve veri kaybı gibi riskleri önlemeyi amaçlayan kapsamlı bir güvenlik çerçevesi sunarak kişisel verilerin korunmasını mümkün kılmaktadır. Bu bağlamda veri güvenliği, kişisel verilerin mahremiyetini ve bütünlüğünü sağlamak için temel bir gereklilik olup bu mekanizmalar olmaksızın verilerin etkin biçimde korunabilmesi mümkün değildir[304].

Verilerin her türlü tehdit ve tehlikeden korunması olarak tanımlanan kişisel veri güvenliği esas olarak üç temel bileşenden oluşmaktadır: Birincisi, kişisel verilerin sadece yetkili kişiler tarafından erişilebilir olması ile bu verilerin yetkisiz kişilerce ele geçirilmemesini amaçlayan "gizlilik" ilkesidir. İkincisi, kişisel verilerin yetkisiz kişilerce değiştirilmesi, silinmesi veya herhangi bir biçimde zarar verilmesi tehditlerine karşı doğruluğunun ve tamlığının korunmasını belirten "bütünlük" ilkesidir. Üçüncü ve son unsur ise kişisel verilerin ihtiyaç duyulan her anda yetkili kişiler tarafından ulaşılabilecek ve kullanılabilecek halde olması şeklinde ifade edilen "erişilebilirlik" ilkesidir. Bu üç unsurun korunması amacıyla alınması gerekli önlemleri ifade etmekte olan veri güvenliğinde bu unsurlardan birinin zarar görmesi durumunda veri ihlalleri ortaya çıkmaktadır[305]. Bu konudaki başlıca uluslararası düzenlemelere bakıldığında; OECD Rehber İlkelerinin 11 inci, 95/46/EC sayılı Direktif'in 17 nci ve GDPR'ın 32 nci

---

[303] Sayan, *Karşılaştırmalı Hukukta Elektronik…,* 96.
[304] Kişisel Verileri Koruma Kurumu Bülteni, "Genel Olarak Kişisel Veri Güvenliğine İlişkin Tedbirler", *Kişisel Verilerin Korunması ve Siber Güvenlik*, Sayı: 6, (Ağustos- Kasım 2024): 20.
[305] Kişisel Verileri Koruma Kurumu Bülteni, "Genel Olarak Kişisel Veri Güvenliğine İlişkin…": 20.

maddesinde veri sorumlusu ve veri işleyenler tarafından, risklerin göz önünde bulundurarak gerekli idari ve teknik tedbirlerin uygulanması gerektiği belirtilmiştir. Bu kapsamda, GDPR'ın 32 nci maddesi, veri sorumlusu ve veri işleyenlerin, veri işleme süreçlerinde uygun güvenlik düzeyini sağlama yükümlülüğünü açıkça ortaya koymaktadır.

Teknolojik gelişimin geldiği nokta, uygulanacak güvenlik önlemlerinin maliyeti, işleme faaliyetinin kapsamı ve amaçları ile gerçek kişilerin hak ve hürriyetlerine yönelik olası riskler, bu değerlendirme sürecinde temel belirleyiciler olarak öne çıkmaktadır. Risk temelli bu yaklaşımda, olasılık ve ciddiyet açısından farklılaşabilen risklerin doğru bir şekilde analiz edilmesi ve bu analize uygun önlemlerin uygulanması esastır. Özellikle kişisel verilerin korunması sürecinde, yalnızca risklerin tespit edilmesi değil, aynı zamanda bu risklerin etkilerinin azaltılması ve mümkün olduğunda tamamen ortadan kaldırılması hedeflenmelidir.

3.3 Posta Sektöründe Bilgi ve Kişisel Veri Güvenliği

Günümüzde kurum ve kuruluşlar açısından sürdürülebilirliğin sağlanması ve rekabet avantajının korunması ihtiyacı; bilgiye hızlı, güvenli ve kesintisiz erişim gerekliliğini ön plana çıkarmıştır. Bu bağlamda, bilgi sistemlerinin güvenliği yalnızca operasyonel sürekliliğin değil, aynı zamanda ekonomik istikrarın, kamu hizmetlerinin etkinliğinin ve özel sektör performansının temel unsurlarından biri hâline gelmiş ve modern ulusal ekonomiler ile dijitalleşen kamu ve özel sektör yapıları için büyük bir öneme sahip olmuştur.

Posta sektörü de gelinen bu aşamada, önemli yapısal ve teknolojik dönüşüm fırsatları elde etmiştir. Özellikle e-ticaretin küresel ölçekte hızlı bir ivme kazanması, posta hizmetlerine yönelik talebi artırmış; bu artış, sektörde müşteri beklentilerine daha hızlı ve etkin yanıt verebilecek yenilikçi teslimat yöntemlerinin, dijital çözümlerin ve esnek iş modellerinin geliştirilmesini zorunlu kılmıştır. Bu çerçevede posta sektörü,

geleneksel hizmet anlayışından veri odaklı, teknoloji destekli ve kullanıcı merkezli bir yapıya dönüşmüştür[306]. Sektördeki bu dönüşüm PHS'leri, veri yönetimi ve kişiselleştirilmiş hizmet sunma gibi alanlara odaklanarak dijitalleşmeyle ortaya çıkan ihtiyaçlara yanıt vermeye çalışmaya yöneltmiştir[307].

Günümüzde en çok kullanılan dijital dönüşüm teknolojilerinden biri büyük veri teknolojisi olup bu teknoloji, posta sektöründe veri analizine dayalı stratejilerin temelini oluşturmaktadır. Depo yönetimi, rota optimizasyonu, araç takibi gibi süreçlerde büyük veri sistemlerinden yararlanılmakta; bu sistemler yalnızca depolama değil, aynı zamanda hızlı ve otomatik analiz işlevi de görmektedir[308]. Gönderici ve alıcı bilgileri analiz edilerek bu veriler üzerinden fayda sağlayacak planlamalar yapılabilmektedir[309]. Bu teknoloji sayesinde gönderi konsolidasyonu ve nakliye süreçlerinin optimizasyonunu gerçekleştirerek gelir artışı sağlanmakta ve rekabet avantajı elde edilmektedir[310]. Ayrıca lojistik faaliyetlerinin etkin bir biçimde yürütülmesinin yanı sıra lojistik faaliyetler tamamlandığında ortaya çıkan sonuçların değerlendirilmesinde de büyük veri teknolojisine ihtiyaç duyulmaktadır[311].

Öte yandan bu dönüşüm sürecinde öne çıkan dijital dönüşüm teknolojilerinden biri de yapay zekâ teknolojisidir. Marvin Minsky tarafından *"insan zekâsı ile yapılabilecek işleri makinelere yaptırma bilimi"* olarak tanımlanan yapay zekâ teknolojisi[312]; posta

---

[306] Ali Burak, Akbulut, *Posta Sektöründeki Dijital Dönüşümün Rekabetçi Bakış Açısıyla İncelenmesi, Uluslararası Uygulamalar ve BTK İçin Öneriler*, (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2023): 50.

[307] Anna, Otsetova, *"Digital Transformation of Postal Operators – Challenges and Perspectives",* Department of Management in Communications, University of Telecommunications and Post, Sofia, 2019: 1

[308] Annette, Hillebrand vd., *Technology and change in postal services impacts on consumers,* (WIK-Consult, 2016): 39.

[309] Barış, Karabay ve Mustafa, Ulaş, "Büyük Veri İşlemede Yaygın Kullanılan Araçların Karşılaştırılması", *8th International Advanced Technologies Conference*, (2017): 3.

[310] Bilgi Teknolojileri ve İletişim Kurumu, *Büyük Veri ve Yapay Zekâ Araştırma Raporu*.

[311] İsmail, İyigün, "Lojistik ve Tedarik Zinciri Süreçlerinde Büyük Veri Kullanımı ve Etkilerinin Analizi", *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi*, (2019): 98.

[312] Elçin Gökçen, Efe, *Yapay Zekâ Teknolojileri ve Rekabet İlişkisi: Elektronik Haberleşme Sektöründe Algoritmaların Kullanımının Rekabet Üzerindeki Olası Etkileri* (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2024): 4 (Yayımlanmamış Tez)

sektöründe envanter yönetimi, talep tahmini, rota optimizasyonu gibi alanlarda kullanılarak teslimat süreçlerinin hızlandırılmasına, doğruluğun artırılmasına ve maliyetlerin düşürülmesine katkı sağlayan temel araçlardan biri olarak karşımıza çıkmaktadır[313]. Zira posta sektöründe yapay zekâ destekli sistemler sayesinde, kullanıcıya gönderi sürecine dair tahmini zamanlamalar iletilmekte; siparişin hazırlanmasından teslimatına kadar tüm adımlar e-posta veya SMS aracılığıyla kullanıcıya bildirilmektedir.

Bununla birlikte dijitalleşme süreci, veri ve bilgi güvenliği açısından birtakım riskler oluşturmaktadır[314]. Zira posta sektöründe hizmet sunumunun gerçekleştirilmesi sırasında çok çeşitli bilgiler üretilmekte ve işlenmektedir. Bu bilgiler arasında kullanıcıların ad, soyad, adres, telefon numarası gibi kişisel bilgileri; gönderi içerikleri, gönderi takip numaraları ve teslimat bilgileri gibi gönderi detayları; kurum içi yazışmalar, sözleşmeler gibi kurumsal bilgiler ile ödeme bilgileri, fatura ve tahsilat kayıtları gibi finansal veriler yer almaktadır. Ayrıca PHS'lerin internet sitesi veya mobil uygulamaları gibi dijital sistemlerin kullanımıyla birlikte kullanıcı hareketlerini izleyen sistem kayıtları (loglar) da önemli bilgi türleri arasında yer almaktadır. Elde edilen veriler ise içerdiği hassasiyet düzeyi ve çeşitlilik nedeniyle, bilgi güvenliği açısından önemli tehdit ve risk unsurları barındırmaktadır. Karşılaşılan güvenlik zafiyetleri arasında; veri sızıntıları, yetkisiz erişimler, fiziksel güvenlik eksiklikleri ve yetersiz veri yedekleme uygulamaları öne çıkmaktadır.

Bu kapsamda özellikle yeterli şifreleme yapılmaması sonucu, kişisel verilerin üçüncü kişilerin eline geçmesi, sistemlerde çalışanların görev alanları dışında verilere ulaşabilmesi ve sahte e-posta veya SMS yoluyla kullanıcıların dolandırılması gibi durumlar posta sektöründe ciddi güvenlik açıklarına neden olabilmektedir. Nitekim KVK Kurulu'nun 18.05.2023 tarihli ve 2023/845 sayılı kararında, bir PHS çalışanı

---

[313] Akbulut, *Posta Sektöründeki Dijital Dönüşümün…,* 89; Bilgi Teknolojileri ve İletişim Kurumu, *Büyük Veri ve Yapay Zekâ Araştırma Raporu*, (2025).
[314] Akbulut, *Posta Sektöründeki Dijital Dönüşümün…,* 175.

tarafından posta gönderisinin teslimi sonrasında ilgili kişinin telefonuna SMS gönderilmesi, kişisel verilerin hukuka aykırı olarak işlendiği şeklinde değerlendirilmiştir. Bu doğrultuda, veri sorumlusu PHS'nin kişisel verilerin korunmasına yönelik gerekli teknik ve idari tedbirleri almadığı gerekçesiyle Kurul tarafından idari para cezası uygulanmıştır[315].

Değinilen bu bilgi güvenliği risklerini bertaraf edebilmek için PHS'ler bünyesinde çok katmanlı kontrol mekanizmalarının oluşturulması gerekmektedir. Bu çerçevede, bilgi güvenliği politikalarının kurumsal düzeyde tanımlanması, güvenlik odaklı bir organizasyon yapısının benimsenmesi ve uluslararası standartlara uygun bir bilgi yönetim sisteminin (örneğin ISO/IEC 27001) tesis edilmesi bu sürecin temel taşları arasında yer almaktadır. Ayrıca, teknik güvenliğin sağlanması (örneğin ağ güvenliği, şifreleme sistemleri) gerekmektedir[316].

Bilgi güvenliği ihlallerinin tespiti, önlenmesi ve etkili kriz yönetimi süreçleriyle ele alınması ise hem hukuki yükümlülüklerin yerine getirilmesi hem de kurumsal itibarın korunması açısından kritik önemdedir. Dolayısıyla, posta sektöründe bilgi güvenliği yalnızca teknik bir konu değil; stratejik, organizasyonel ve hukuki boyutları bulunan bütüncül bir yönetim alanı olarak ele alınmalıdır.

3.4 Posta Hizmet Sağlayıcısının Yükümlülükleri

PHS'lerin bilgi güvenliği yükümlülükleri, muhtelif düzenlemelere dayanmaktadır. Buna göre, posta sektöründe veri sorumlusu sıfatını haiz PHS'lerin kişisel verilere yetkisiz erişimi engellemek ve bu verilerin güvenli bir biçimde muhafazasını sağlamak için, KVKK ve ilgili posta mevzuatı kapsamında bazı idari ve teknik tedbirleri alması gerekmektedir.

---

[315] Kişisel Verileri Koruma Kurulu Kararı, 18/05/2023 günlü, 2023/845 sayılı karar.
[316] Melis, Böke, Yazıcıoğlu, "ISO 27001, KVKK ve GDPR: Bilgi Güvenliği ve Veri Koruma Standartlarının Karşılaştırılması", *Mühendislik ve Teknoloji Dergisi*, 5(1), (2024): 17.

İlk olarak KVKK'nin 12 nci maddesinde veri sorumlusunun veri güvenliğine dair yükümlülükleri düzenlenmiştir. Anılan maddenin birinci fıkrasına göre veri sorumlusu;

> *"a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,*
> *b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,*
> *c) Kişisel verilerin muhafazasını sağlamak,*
> *amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak"*

ile yükümlüdür. Ancak bu yükümlülüklerin nasıl sağlanacağı noktasında bir açıklık bulunmamaktadır. Bununla birlikte bu noktada bir eksiklikten bahsetmenin mümkün olmadığı değerlendirilmektedir. Zira teknolojinin günden güne geliştiği ve değiştiği göz önünde bulundurulduğunda KVKK ile sınırlı sayıda olacak şekilde belirlenecek tedbirlerin zamanla yetersiz kalacağı ve her yeni değişim ve gelişime göre kanun değişikliğine gidilmesi gerekeceği aşikardır. Bu kapsamda KVK Kurumu tarafından uluslararası standartlar da göz önünde bulundurularak KVKK'nin uygulanabilirliğini sağlamak için *"Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)"* hazırlanmıştır[317].

Ayrıca KVKK'nin 18 inci maddesinin birinci fıkrasının (b) bendinde yer alan hüküm gereği veri güvenliğini sağlayamayan veri sorumluları hakkında idari para cezaları uygulanmaktadır. Dolayısıyla bu yükümlülük, veri sorumluları bakımından idari para cezası yaptırımı ile karşılaşmamak ve ticari saygınlığın zarar görmemesi için büyük önem taşımaktadır[318].

GDPR'ın 32 nci maddesinde de veri sorumlusunca alınması gerekli birtakım teknik ve idari tedbirlere yer verilmiş olup buna göre; *"kişisel verilerde takma ad kullanımı ve*

---

[317] Yürük, "Veri Sorumlusunun Veri…": 905-906.
[318] Cengiz, Paşaoğlu ve Emel, Cevheroğlu, "Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması", *Bilişim Teknolojileri Dergisi*, Cilt: 13, Sayı: 2, (2020): 192.

şifreleme; işleme sistemlerinin ve hizmetlerinin gizliliğini, bütünlüğünü, kullanılabilirliğini ve mukavemetini sürekli olarak sağlama kabiliyeti; fiziksel veya teknik bir olay durumunda, kişisel verilerin kullanılabilirliğinin ve kişisel verilere erişimin vakitlice yeniden sağlanma kabiliyeti; işlemenin güvenliliğinin sağlanmasına yönelik olarak teknik ve kurumsal tedbirlerin etkililiğinin düzenli olarak sınanmasına, ölçülmesine ve değerlendirilmesine ilişkin süreç" örnek olarak sayılmıştır.

Diğer yandan, Evrensel Posta Sözleşmesi'nin 8 inci maddesinde üye ülkeler ve bu ülkelerin PHS'lerinin, UPU güvenlik standartlarında tanımlanan güvenlik gerekliliklerine uymaları ve operasyonel aşamalarda önleyici bir güvenlik yaklaşımı benimsemeleri gerektiği belirtilmektedir[319].

Son olarak ise BTK'nin 23.09.2019 tarihli ve 2019/DK-SRD/206 sayılı kararının 2 nci maddesinde yer alan; "*Hizmetin sunumunu ispatlayan belgeyi düzenlerken, kullanıcıya (göndericiye ve alıcıya) ait kişisel verilerin gizliliğini ve güvenliğini sağlamaları; gönderinin taşınmak üzere kabulü ve alıcıya teslimi esnasında ve sonrasında kişisel verilerin ilgili mevzuatla yetkili kılınan merciler dışındaki üçüncü kişilerce görülmemesini ve işlenmemesini güvenceye alacak bir yöntem uygulamaları*" hükmü uyarınca PHS'lere, posta kullanıcılarına ait kişisel verilerin gizliliği ve güvenliğini sağlama ve bu verilerin güvenliğini sağlayacak bir yöntem uygulama yükümlülüğü getirilmiştir.

3.4.1 Kişisel veri güvenliğine ilişkin idari tedbirler

Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde kişisel veri güvenliğine ilişkin alınacak idari tedbirler; "mevcut risk ve tehditlerin belirlenmesi, çalışanların eğitilmesi ve farkındalık çalışmaları, kişisel veri güvenliği politikalarının ve

[319] Aikaterina, Papanikolaou, Eleni, Varvarousi ve Eirini, Gavala, *Postal sector digitalisation: security and vulnerabilities*, (2024): 48.

prosedürlerinin belirlenmesi, kişisel verilerin mümkün olduğunca azaltılması ve veri işleyenler ile ilişkilerin yönetimi" şeklinde belirtilmiştir[320]. Bu kapsamda aşağıda yer alan başlıklarda bu idari tedbirler açıklanmaktadır.

3.4.1.1 Mevcut risk ve tehditlerin belirlenmesi

Kişisel verilerin güvenliğini sağlamak amacıyla, veri sorumlusunca işlenen tüm kişisel verilerin kapsamlı bir biçimde analiz edilmesi gerekmektedir. Bu analiz; işlenen verilerin türleri, bu verilerin korunmasında karşılaşılabilecek riskler ve bu risklerin gerçekleşmesi halinde doğabilecek zararların kapsamını içermelidir. Risk değerlendirme sürecinde şu hususlar dikkate alınmalıdır:

- Kişisel verilerin hassas veri olup olmadığı,
- Verinin mahiyeti gereği ne seviyede gizlilik derecesi gerektirdiği,
- Güvenlik ihlali durumunda ilgili kişi üzerindeki olası zararların niceliği ve niteliği.

Bu değerlendirme, uygun teknik ve idari tedbirlerin seçilmesi ve uygulanmasına yönelik bir temel oluşturarak kişisel veri güvenliği risklerini en aza indirmeyi hedeflemektedir[321]. Bununla birlikte KVK Kurumu, yapılan risk değerlendirmesine göre veri sorumlusunun, riski azaltmak amacıyla gerekli tedbirleri almadığı ve veri işleme faaliyetinin gerçek kişilerin hak ve hürriyetleri açısından yüksek oranda risk oluşturacağının ortaya çıktığı hallerde, veri işleme faaliyetine başlamadan önce Kurumlarına danışılmasının gerekli olduğunu belirtmektedir[322].

---

[320] Kişisel Verileri Koruma Kurumu, "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", *KVKK Yayınları*, (Nisan 2025): 13-17.
[321] Kişisel Verileri Koruma Kurumu, "Kişisel Veri Güvenliği Rehberi…": 13.
[322] Öykü Beste, Bayram, "Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi", *Kişisel Verileri Koruma Dergisi*, Cilt: 4, Sayı: 1, (2022): 49.

3.4.1.2 Çalışanların eğitilmesi ve farkındalık çalışmalarının yapılması

Kişisel veri güvenliği ihlalleri çoğunlukla kullanıcıların dikkatsizlik, dalgınlık ya da deneyimsizlik gibi zayıf yönlerinin istismar edilmesiyle gerçekleşir. Örneğin; kötü amaçlı yazılım içeren bir e-postanın açılması ya da e-postanın yanlış bir alıcıya gönderilmesi bu ihlallere neden olabilir[323].

Bu kapsamda söz konusu ihlallere sebep olabilecek saldırılar karşısında, çalışanların ilk müdahaleyi yapmaları büyük önem taşımakta olup çalışanların bu tür durumlara karşı hızlı müdahale edebilmesi ve farkındalık sahibi olması için eğitimler düzenlenmeli, görev tanımları netleştirilmeli ve "İzin Verilmedikçe Her Şey Yasaktır" prensibi benimsenmelidir[324]. Ayrıca çalışanların gizlilik anlaşmaları imzalaması[325], güvenlik politikalarına uymayanlara yönelik disiplin süreçlerinin belirlenmesi ve politika değişikliklerinin düzenli eğitimlerle aktarılması da veri güvenliğini sağlamak için alınabilecek kritik önlemler arasındadır[326]. Nitekim KVK Kurulu tarafından verilen

---

[323] Kişisel Verileri Koruma Kurumu, "Kişisel Veri Güvenliği Rehberi…": 14.

[324] Kişisel Verileri Koruma Kurumu, "Kişisel Veri Güvenliği Rehberi…": 14-15.

[325] KVK Kurulu 26/12/2019 tarihli ve 2019/393 sayılı kararında; *"…Sonuç olarak; Anayasa, 657 sayılı Kanun ve ilgili ikincil mevzuat kapsamında Devlet memurunun başlıca ödevi (yükümlülüğü) Anayasaya, kanunlara sadık kalarak görevini ifa etmektir. Dolayısıyla, kişisel verilere ilişkin tesis edilen iş ve işlemlerde de 6698 sayılı Kanun hükümlerine uygun davranma yükümlülüğü, bu yükümlülüğe aykırı davranması halinde gerek idareye gerek kişilere verdiği zararlardan ötürü sorumluluğu söz konusudur. Bir başka ifadeyle, bu kişilerin yükümlülükleri hâlihazırda 657 sayılı Kanun ve ilgili yönetmeliklerle belirlenmiş olup; 6698 sayılı Kanun ve ilgili yönetmeliklere uygun hareket etmeleri görevlerini ifa ederken uymaları gereken başlıca yükümlülüklerindendir. Yukarıda yer verilen gerekçelerle, kamu kurumu nezdinde 657 sayılı Kanun kapsamında çalışan ve kişisel veri işleyen personele kişisel verilerin korunmasına yönelik ayrıca bir gizlilik sözleşmesi imzalatılması uygun olmayacaktır. Ancak bu noktada önemle belirtmek gerekir ki, kişisel verilerin korunması hakkının bir temel hak ve özgürlük olarak yakın tarihte iç hukukumuzda düzenleme altına alınmış olduğu gözetildiğinde, 657 sayılı Kanun kapsamında çalışan personele, kişisel verilerin korunması hakkı kapsamında uymaları gereken usul ve esaslara dair bilgilendirici mahiyette bir metin tebliğ edilmesi ve bu konuda periyodik eğitimler düzenlenmesi uygun olacaktır."* ile 657 sayılı Kanun kapsamında çalışmakta olan ve kişisel veri işleyen personele ayrıca bir gizlilik sözleşmesi imzalatılmasının uygun olmayacağını belirtmiştir (Kişisel Verileri Koruma Kurumu, "Kişisel Veri Güvenliği Rehberinde geçen "personel gizlilik sözleşmesi" imzalatılmasının 657 sayılı Devlet Memurları Kanununa tabii olarak çalışanlar için gerekli olup olmadığı ile ilgili Kişisel Verileri Koruma Kurulunun 26/12/2019 tarihli ve 2019/393 sayılı Karar Özeti").

[326] Kişisel Verileri Koruma Kurumu, "Kişisel Veri Güvenliği Rehberi…": 14.

bir kararda, hassas verilerin işlenmesi aşamasında görev alan personel ile gizlilik sözleşmesi yapılması zorunlu tutulmuştur[327].

Posta sektöründe kişisel veri güvenliğinin sağlanmasında da insan faktörü büyük önem arz etmekte olup çalışanların bilgi güvenliği konusunda yeterli donanıma sahip olmaması veri ihlallerinin temel sebeplerinden biridir. Bu bağlamda, PHS'ler nezdinde çalışanlara yönelik düzenli, güncel ve kapsamlı eğitim programlarının uygulanmasının faydalı olacağı düşünülmektedir.

3.4.1.3 Kişisel veri güvenliği politikalarının ve prosedürlerinin belirlenmesi

Kişisel verilerin güvenliğinin sağlanmasında veri sorumlusu olan PHS'lerin, kişisel verilere yönelik politikalar hazırlaması, risklere karşı önlemlerin alınabilmesinde büyük önem taşımaktadır.

Buna göre veri sorumluları, başta bilişim ağlarında kullanılan yazılım ve servislerin kontrol edilmesi, kullanıcı işlem hareketlerinin düzenli şekilde kayıt altına alınması gibi teknik önlemlerle sistemlerini içeriden ve dışarıdan gelebilecek tehditlere karşı korumalıdır.

Verilerin bulut teknolojilerinde depolanması durumunda da etkili güvenlik tedbirlerinin uygulanması gerekmektedir. Bunun için mevcut sistemlerin gözden geçirilmesi ve iyileştirilmesi süreçlerinde, mahremiyetin korunması odaklı bir yaklaşım benimsenmelidir. Öte yandan kişisel verilerin yalnızca siber ortamda değil, fiziksel ortamlarda da saklandığı göz önüne alındığında, fiziksel güvenlik önlemlerinin alınması da zorunlu bir husustur. Bu nedenle yedekleme işlemleri hem siber hem de fiziksel ortamlarda güvenli bir şekilde gerçekleştirilmelidir[328].

---

[327] Kişisel Verileri Koruma Kurulu Kararı, 31.01.2018 günlü, 2018/10 sayılı karar.
[328] Kişisel Verileri Koruma Kurumu Bülteni, "Genel Olarak Kişisel Veri Güvenliğine İlişkin…": 21.

Kişisel verilerin kaybı, çalınması veya zarar görmesi durumlarında ise veri sorumluları, hem gerekli hukuki bildirim süreçlerini işletmeli hem de yedeklenmiş verileri kullanarak hızlı bir şekilde operasyonel faaliyetlerine devam edebilecek teknik kabiliyete sahip olabilmelidir.

3.4.1.4 Kişisel verilerin asgari ölçüde işlenmesi

KVKK'nin 4 üncü maddesinin ikinci fıkrasının (b) ve (d) bentleri doğrultusunda *"kişisel verilerin, doğru ve gerektiğinde güncel olarak; ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi"* gerekmektedir. Bu sebeple veri sorumluları, toplamış oldukları verilerin kullanılmayan bölümünü yahut işlediği verilerin doğruluğu olmayan veya güncelliğini kaybetmiş olanlarını, *"Kişisel Veri Saklama ve İmha Politikası"* ile *"Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Yönetmeliği"*ne uygun olacak biçimde imha etmelidir[329]. Örneğin; internet sitelerinde üyelik işlemleri sırasında kişinin T.C. kimlik numarası gibi zorunlu olmayan bilgilerinin talep edilmemesi, bu kapsamda alınabilecek bir idari tedbir olarak gösterilebilmektedir. Keza posta sektöründe de Teslimat Usul ve Esaslarının *"Tanımlar"* başlıklı 3 üncü maddesinin birinci fıkrasının (c) bendinde temassız teslimat; gönderilerin teslimi sırasında T.C. kimlik numarası ve imza alınmaksızın gerçekleştirilen bir yöntem olarak tanımlanmıştır. Söz konusu düzenleme ile haberleşme gönderileri haricindeki gönderiler bakımından, kimlik numarası ve imza gibi kişisel verilerin toplanması uygulamasına son verilmiş ve bu sayede kişisel veri işleme faaliyetleri mümkün olduğunca azaltılmıştır.

Diğer taraftan uygulamada, gerekli olmayan kişisel verilerin toplandığı veya kişisel verilerin ihtiyaç duyulandan daha uzun süre saklandığı sıkça görülmektedir. Bu durum, şirketlerin kuruluşlarından itibaren çalışanlarına ilişkin tüm verileri imha

---

[329] Murat, Altındere, *Kişisel verilerin korunması hukuku ve uygulanması*, (Ankara: Adalet Yayınevi, 2020): 168.

etmeksizin saklaması gibi örneklerle kendini göstermektedir. Bu tür uygulamalar, kişisel verilerin işlenme amacıyla orantılı olarak saklanması gerektiği ilkesine aykırıdır. Bu nedenle, yalnızca işleme amacıyla uyumlu verilerin muhafazası ve bu verilere dair makul muhafaza sürelerinin belirlenmesi önemlidir[330].

3.4.1.5 Veri işleyenler ile ilişkilerin yönetilmesi

KVKK'nin 12 nci maddesinin ikinci fıkrasında, *"kişisel verilerin veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda veri sorumlusunun da bu kişilerle birlikte müştereken sorumlu olduğu"* hüküm altına alınmıştır. Bu kapsamda veri sorumlusu olan PHS'lerin, çeşitli alanlara dair ihtiyaçlarını gidermek için veri işleyenlerden hizmet alması hâlinde, kendilerince sağlanan düzeyde veri güvenliğinin sağlandığından emin olmaları gerekir.

Diğer yandan veri işleyenin, sahip olması gereken nitelikler konusunda KVKK'de açık bir düzenleme bulunmamaktadır. Bu nedenle veri sorumlusu tarafından ilgili kişi ve kuruluş hakkında araştırma yapılması, yeterli önlemlerin alındığına ve alınacağına ilişkin kanaat getirilmesi son derece önemlidir[331].

3.4.2 Kişisel veri güvenliğine ilişkin teknik tedbirler

Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)'nde kişisel veri güvenliğine ilişkin alınacak teknik tedbirler; *"siber güvenliğin sağlanması (ağ güvenliği, uygulama güvenliği, veri maskeleme, şifreleme, kriptografi, veri kaybı önleme yazılımları, yedekleme güvenlik duvarları vb.), kişisel veri güvenliğinin takibi (sızma testi, erişim logları, saldırı tespit ve önleme sistemleri, kullanıcı hesap yönetimi, log kayıtları),*

[330] Yürük, "Veri Sorumlusunun Veri…": 910.
[331] Yürük, "Veri Sorumlusunun Veri…": 911.

kişisel veri içeren ortamların güvenliğinin sağlanması (veri kaybı önleme yazılımları, güncel anti virüs sistemleri vb.), kişisel verilerin bulutta depolanması, sistemlerin tedariği, geliştirilmesi ve bakımı ile kişisel verilerin yedeklenmesi" olarak belirtilmiştir[332]. Bu kapsamda aşağıda yer alan başlıklarda bu teknik tedbirler açıklanmaktadır.

3.4.2.1 Siber güvenliğin sağlanması

Siber kavramı genel olarak, yalnızca internetle sınırlı olmayan, dijital verinin bulunduğu her ortamı kapsayan bir alan olarak tanımlanabilmektedir. Bu bağlamda, internet bağlantısı olsun ya da olmasın elektronik cihazlar da siber ortamın bir parçası sayılmakta olup bu dijital yapıların gün geçtikçe hayata entegre olması, siber güvenliğin dijital sistemlerin temel bir bileşeni haline gelmesine neden olmuştur. Zira dijital ortamda yer alan finansal bilgilerden müşteri kayıtlarına, kurumsal stratejilerden kritik altyapı verilerine kadar her tür veri siber ortam üzerinde bulunmakta ve bu verileri kötü niyetli şekilde ele geçirmek amacıyla siber saldırıda bulunan kişi veya gruplar her zaman var olmaktadır. Bu durum, siber güvenliğin dijital çağdaki önemini ortaya koymaktadır[333].

Bu çerçevede, posta hizmetleri alanında siber güvenliğin sağlanması hem bireysel hakların teminatı hem de kamu hizmetlerinin güvenilirliği açısından büyük önem arz etmektedir. Zira posta hizmeti, anayasal düzeyde güvence altına alınan haberleşme hürriyetinin hayata geçirilmesinde temel rol oynayan, kamu hizmeti niteliğindeki kritik bir hizmettir. Öte yandan, özellikle dijitalleşme süreci ve e-ticaret hacmindeki artışla birlikte, posta hizmetleri yalnızca bireyler arası iletişimi değil, aynı zamanda

---

[332] Kişisel Verileri Koruma Kurumu, "Kişisel Veri Güvenliği Rehberi…": 19-27.

[333] Muhammed Zekeriya, Gündüz ve Resul, Daş, "Kişisel Siber Güvenlik Yaklaşımlarının Değerlendirilmesi", *DÜMF MD*, Cilt: 13, Sayı: 3, (2022): 430.

ticari faaliyetlerin sürekliliğini destekleyen stratejik bir altyapı hizmeti olarak da öne çıkmaktadır.

Bu bağlamda siber güvenliğin sağlanmasında kritik bir sektör olarak karşımıza çıkan posta sektöründe çeşitli siber güvenlik saldırıları meydana gelebilmektedir. Bu saldırı yöntemlerinde verilerin kötüniyetli bireyler tarafından kurum dışına çıkarılması "veri sızıntısı" olarak ifade edilmekte ve veri güvenliğine dair kaygılanılan başlıca konular arasındadır. Karşımıza en çok çıkan saldırı yöntemlerinden biri "oltalama" olarak bilinen "phising" yöntemidir[334]. Bu yöntem ile posta sektöründe kullanıcılar, PHS'lerce gönderildiği izlenimi oluşturulan SMS veya e-posta vasıtasıyla aldatıcı internet sitelerine yönlendirilmektedir. Bunun sonucunda ise kullanıcıların kimlik ve kredi kartı şifresi gibi bilgileri üçüncü taraflarca elde edilmektedir. Örneğin; son yıllarda posta sektörünü de hedef alan dolandırıcılık girişimlerinde kötü niyetli kişiler tarafından vatandaşlara çeşitli iletişim kanalları aracılığıyla "Gönderiniz gümrükte bekletiliyor", "Teslimat için ek ücret ödemeniz gerekmektedir" ya da "Gönderinizde yasa dışı madde tespit edildi" gibi ifadelerle alıcıların bir hesap numarasına para yatırması ya da bir bağlantı linki üzerinden işlem yapması talep edilmektedir[335].

Bunun yanı sıra siber saldırılar sonucunda PHS'leri etkileyecek tehdit unsurlarından biri de bilgilerin çalınması ve/veya değiştirilmesidir. Kişisel veri içeren bilgi teknolojileri sistemlerinin dijital ortam kaynaklı yetkisiz erişim tehditlerine karşı korunmasında temel savunma önlemleri arasında güvenlik duvarları ve internet ağ geçitleri yer almaktadır. Bu unsurlar, dış kaynaklı siber saldırılara karşı sistemlerin ilk savunma hattını oluşturarak kritik bir rol üstlenmektedir. Uygun şekilde yapılandırılmış bir güvenlik duvarı, saldırı girişimlerinin kurumsal ağın derin katmanlarına ulaşmasını engelleyerek veri güvenliğini sağlayabilir. İnternet ağ geçitleri ise çalışanların güvenliği tehdit eden zararlı web sitelerine ya da kişisel

---

[334] Özcan, *Bankacılık İş ve İşlemlerinde…,* 169.

[335] Ticaret Bakanlığı, "Hızlı kargo ya da posta yoluyla gönderilen eşya konu edilerek yapılan dolandırıcılığa dikkat!", (2024).

verilerin sızdırılmasına neden olabilecek çevrimiçi hizmetlere erişimini kısıtlayarak kişisel veri güvenliği risklerini azaltmaya katkıda bulunabilir[336]. Ayrıca yazılım ve donanımların güncel tutulması, kullanılmayan uygulamaların sistemden kaldırılması ve sızma testleri ile yama yönetiminin düzenli yapılması da olası açıkların önlenmesi açısından kritik öneme sahiptir. Kişisel verilere erişimin görev tanımıyla sınırlı tutulması, güçlü parola politikalarının benimsenmesi ve erişim yetki kontrollerinin yapılandırılması gerekmektedir. Güvenlik ihlallerinin önüne geçilmesi için yönetici hesaplarının kontrollü kullanımı, işten ayrılan çalışanların erişimlerinin hızla sonlandırılması gibi önlemler alınmalıdır[337].

Bu kapsamda posta sektöründe ikincil düzenlemeler ile bilgi güvenliğinin ve dolayısıyla siber güvenliğin sağlanması amacıyla PHS'lere bazı yükümlülükler getirilmiştir. PHSİY'nin *"Posta hizmetlerinin gizliliği ve güvenliği"* başlıklı 18 inci maddesinin üçüncü fıkrasında yer alan; *"Hizmet sağlayıcısı, sunduğu posta hizmetlerinin gizliliği ve güvenliği ile ilgili olarak gerekli önlemleri almakla yükümlüdür."* hükmüne dayanılarak 29.12.2020 tarihli ve 2020/DKSRD/371 sayılı BTK kararı uyarınca tüm PHS'lere, TS ISO/IEC 27001 veya ISO/IEC 27001 uyum sağlama, ayrıca yıllık net satış tutarı on milyon Türk lirasını aşan hizmet sağlayıcılarına TS ISO/IEC 27001 veya ISO/IEC 27001 standardına göre uygunluk belgesi alma ve BTK'ye sunma yükümlülüğü getirilmiştir. PHS'lere söz konusu standarda uyum zorunluluğunun getirilmesi oldukça önem arz etmektedir. Zira 2022 yılında yayımlanan ve "NIS2 Direktifi" olarak anılan Siber Güvenlik Direktifi'nde posta ve kargo hizmetleri sektörüne "diğer kritik sektörler" arasında yer verilmiş olup bu Direktif'te belirlenen siber güvenlik tedbirlerinin büyük bölümü "TS ISO/IEC 27001" veya "ISO/IEC 27001 standardı" ile uyum halindedir[338].

---

[336] Kişisel Verileri Koruma Kurumu, "Kişisel Veri Güvenliği Rehberi…": 19.
[337] Kişisel Verileri Koruma Kurumu Bülteni, "Genel Olarak Kişisel Veri Güvenliğine İlişkin…": 10-12.
[338] Naci Soner, Payaslı, *Avrupa Birliği (AB) 2022/2555 Sayılı Birlik Genelinde Yüksek Düzeyde Ortak Siber Güvenlik Tedbirlerine İlişkin Direktifin (NIS2 Direktifi) İncelenmesi ve İlgili Direktif Kapsamında Ülkemiz Elektronik Haberleşme Sektörü Mevzuatının Değerlendirilmesi*, (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2023): 149-161.

Diğer yandan, 08.01.2025 tarihli ve 32776 sayılı Resmî Gazete'de yayımlanan 177 sayılı Cumhurbaşkanlığı Kararnamesi ile Siber Güvenlik Başkanlığı kurulmuştur. 19.03.2025 tarihli ve 32846 sayılı Resmî Gazete'de ise 7545 sayılı Siber Güvenlik Kanunu yayımlanmış ve bu kapsamda "Siber Güvenlik Kurulu" oluşturulmuştur. Bu Kurulun görevleri anılan Kanun'un 9 uncu maddesinin dördüncü fıkrasında aşağıdaki şekilde sayılmıştır:

> *"a) Siber güvenlikle ilgili politika, strateji, eylem planı ve diğer düzenleyici işlemlere yönelik kararları almak, alınan kararların tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek.*
> *b) Başkanlık tarafından hazırlanan siber güvenlik alanına ilişkin teknoloji yol haritasının ülke çapında uygulanmasına yönelik kararlar almak.*
> *c) Siber güvenlik alanında teşvik verilecek öncelikli alanları belirlemek, siber güvenlik alanındaki insan kaynağının geliştirilmesine yönelik karar almak.*
> *ç) Kritik altyapı sektörlerini belirlemek.*
> *d) Başkanlık ile kamu kurum ve kuruluşları arasında meydana gelebilecek ihtilaflar hakkında karar almak."*

Söz konusu hüküm gereği Siber Güvenlik Kurulu'nun kritik altyapı sektörlerini belirleme yetkisi mevcuttur. Bu doğrultuda "NIS2 Direktifi"nde "diğer kritik sektörler" arasında yer alan posta hizmetlerinin de kritik altyapı sektörleri kapsamında belirlenmesinin uygun olabileceği değerlendirilmektedir. Bu sayede Kanun'un 5 inci maddesinin birinci fıkrasının (ı) bendi uyarınca Siber Güvenlik Başkanlığı tarafından kamu hizmeti sunan PHS'lere ilişkin olarak gerekli altyapıları kurma, kurdurma, işletme, işlettirme, kamu kurum ve kuruluşlarına güvenli sistem ve altyapılar üzerinden barındırma hizmeti sunma veya sunulmasını sağlama ve bu faaliyetlere dair uygulama kurallarının belirlenmesi ile posta sektöründe siber güvenliğin sağlanmasında büyük yol kat edilebileceği değerlendirilmektedir.

3.4.2.2 Kişisel veri güvenliğinin takibi

Veri sorumluları, veri güvenliğini sağlamak amacıyla güvenlik sistemleri kursalar da bu sistemler her zaman içeriden ve dışarıdan gelen siber saldırılar, kötü amaçlı yazılımlar ve diğer siber tehditlere karşı tam anlamıyla güvenli olamamaktadır. Bu saldırıların önlenmesinde en önemli faktörlerden biri erken tespit ve müdahaledir. Bu kapsamda herhangi bir siber saldırının, özellikle kişisel verileri hedef alan saldırıların, hızla tespit edilip etkisiz hale getirilmesi için güvenlik sistemlerinin sürekli olarak izlenmesi ve güvenlik açıklarının düzenli olarak raporlanması ve denetlenmesi gerekmektedir[339].

Posta sektöründe işlenen kişisel verilerin güvenliğinin sağlanması da yalnızca teknolojik önlemlerle değil, aynı zamanda doğru yönetim süreçlerinin uygulanmasıyla mümkündür. Ayrıca sektörde kullanılan yazılım ve servislerin düzenli olarak kontrol edilmesi, kullanıcı hareketlerinin kaydedilmesi ve güvenlik açıklarının tespiti gibi önlemler önem arz etmektedir. İlgili sistemlerdeki her türlü güvenlik eksikliğinin tespiti ve raporlanması haricinde, kapsamlı bir bilgi güvenliği yönetim sistemi (BGYS) uygulamasının devreye alınması gerekmektedir. Bunlara ek olarak, düzenli gerçekleştirilen sızma testleri ve zafiyet analizleri sayesinde, sistemlerdeki potansiyel açıklar henüz kötüye kullanılmadan önce belirlenip giderilebilir. Bu teknik önlemlerin yanı sıra, çalışanlara yönelik siber güvenlik eğitimleri ve farkındalık programları da insan kaynaklı güvenlik zafiyetlerini minimize etmek açısından hayati önem taşımaktadır. Böylece posta sektöründe, kişisel veri güvenliği hem teknolojik hem de yönetsel boyutlarıyla bütüncül bir yaklaşımla ele alınarak sürdürülebilir ve etkin bir koruma mekanizması geliştirilebilir.

---

[339] Kişisel Verileri Koruma Kurumu, "Kişisel Veri Güvenliği Rehberi…": 21-22.

3.4.2.3 Kişisel veri içeren ortamların güvenliğinin sağlanması

Kişisel verilerin, veri sorumlusunun yerleşkesinde bulunan cihazlarda veya evrak üzerinde saklanması halinde, bunların kaybı veya çalınması gibi durumlara karşı fiziksel güvenlik önlemleri alınması suretiyle güvenliğinin sağlanması gerekmektedir. Ayrıca yangın, sel gibi dış tehditlere karşı da kişisel verilerin bulunduğu fiziki alanların uygun güvenlik yöntemleriyle korunması ve bu alanlara giriş-çıkışların denetim altında tutulması büyük önem taşımaktadır. Kişisel verilerin dijital ortamlarda saklanması halinde ise veri güvenliğini artırmak amacıyla ağ üzerindeki bileşenler arasında erişim kısıtlamaları getirilebilmesi ya da bileşenlerin birbirinden ayrıştırılabilmesi mümkündür. Örneğin; sadece kişisel verilerin işlendiği belirli bir ağ bölümü oluşturularak, bu alana özel güvenlik kaynaklarının tahsis edilmesi sağlanabilmektedir. Benzer güvenlik önlemlerinin, veri sorumlusunun yerleşkesi dışında yer alan ve kişisel veri barındıran tüm fiziki ortam, dijital ortam ve cihazlar için de uygulanması gerekmektedir[340].

Kişisel veri güvenliği ihlallerinin dizüstü bilgisayar, cep telefonu, taşınabilir bellek gibi cihazların kaybolması ya da çalınmasıyla gerçekleşebildiği göz önünde bulundurularak, bu tür durumlara karşı da gerekli tedbirler alınmalıdır. Ayrıca, kişisel verilerin posta yoluyla iletilmesi sürecinde de gerekli güvenlik önlemlerinin alınarak dikkatli olunması gerekmektedir. Çalışanların kendi kişisel cihazlarıyla kurumsal ağlara erişim sağlaması da ayrı bir risk teşkil ettiğinden, bu durumlar için de yeterli güvenlik politikaları uygulanmalıdır. Kâğıt ortamdaki belgeler, sunucular, yedekleme üniteleri, CD/DVD ve USB gibi veri taşıyıcıların güvenliği için bu ekipmanların ek önlemlerle korunan ayrı bir alanda saklanması, kullanılmadığı zamanlarda kilit altında tutulması ve bu alanlara yapılan giriş çıkışların kayıt altına alınması gereklidir. Cihazların kaybolması ya da çalınması durumlarında veri güvenliğinin korunması için erişim kontrolleri ile cihazın tamamını tam disk şifreleme ile koruma veya yalnızca

[340] Kişisel Verileri Koruma Kurumu, “Kişisel Veri Güvenliği Rehberi…”: 23-24.

belirli dosyaların şifrelenmesi gibi teknolojilerden yararlanılması faydalı olacaktır. Bu bağlamda şifre anahtarları, yalnızca yetkili kişiler tarafından erişilebilecek güvenli ortamlarda tutulmalı ve yetkisiz erişim engellenmelidir. Aynı şekilde, kâğıt ortamdaki belgeler de sadece yetkili personelin ulaşabileceği, kilitli alanlarda saklanmalıdır. Bu doğrultuda, fiziksel güvenlik önlemleri ile siber güvenlik politikalarının entegre biçimde uygulanması, kişisel veri güvenliğinin sağlanmasında temel bir gereklilik olarak kabul edilmektedir. ISO/IEC 27001 standardına göre, veri kaybını önleme stratejileri, şifreleme teknikleri, erişim kontrol politikaları ve mobil cihaz yönetimi gibi teknik ve yönetsel önlemlerin bir arada kullanılması, bilgi güvenliği yönetim sistemlerinin etkinliğini artırmaktadır. Bu kapsamda hem dijital ortamda hem de fiziksel veri taşıyıcılar üzerinde alınacak güvenlik tedbirleri, veri sızıntısı ve yetkisiz erişim risklerini minimize etmeyi amaçlamaktadır. Ayrıca, şifreleme anahtarlarının güvenli ortamlarda saklanması, biyometrik doğrulama ve CCTV destekli fiziksel erişim kontrolleri gibi önlemler de bu bütüncül yaklaşımın bir parçasını oluşturmaktadır[341].

Bu kapsamda posta sektörüne özgü bazı düzenlemeler de bulunmaktadır. Örneğin; PHS'lerin BTK'den alacağı yetki belgesine ilişkin başvuru şartı olarak PSİYY'nin *"Yetkilendirme başvuru şartları"* başlıklı 6 ncı maddesinin birinci fıkrasının (f) bendinde; *"Merkezinde veya şubelerinin bulunduğu il sınırları içinde en az 200 m²'lik kapalı ve yükleme, boşaltma, aktarma, istifleme, tasnif, etiketleme ile depolama gibi hizmetlere elverişli yapı ve donanımda, trafiği engellemeyen ve eşya taşımaya mahsus taşıtların yanaşıp yükleme, boşaltma yapabileceği bağımsız asgari bir adet taşınmazın kullanım hakkına sahip olmaları."* ve (g) bendinde; *"Her bir şubenin, (f) bendinde belirtilen nitelikleri haiz en az 20 m²'lik kapalı alana sahip bir taşınmazın kullanım hakkına sahip olmaları."* hükümlerine yer verilmiştir. Bu hükümlerle posta hizmetlerinin sunulduğu merkez ve şubelerin fiziksel koşulları belirlenmekte olup anılan hükümlerin temelinde, posta gönderilerinin yanı sıra kullanıcıların kişisel

[341] Uluslararası Standartlar Teşkilatı (ISO), *ISO/IEC 27001 (2022). Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*.

verilerinin güvenliğinin de sağlanması amacı bulunmaktadır. Zira belirtilen taşınmazların kapalı ve bağımsız alanlar olması, gönderi üzerinde yer alan kişisel verilere (örneğin; alıcı adı, soyadı, adres bilgisi, iletişim bilgisi) yetkisiz erişim riskini de azaltacaktır. Bu sayede kişisel verilerin üçüncü taraflarca görünmesi ihtimalinin azalacağı değerlendirilmektedir. Diğer yandan etiketleme ve depolama gibi faaliyetlerin bu alanlarda düzenli ve kontrollü biçimde yapılması, gönderilerin kaybolması veya yanlış kişiye teslimatı riskini bertaraf edecektir. Ayrıca gönderilerin aktarma ve yükleme işlemlerinin belirli standartlara uygun kapalı alanlarda yapılması, açık alanlarda veya ortak kullanıma açık bölgelerde gönderilerin zarar görmesi veya ifşa olması gibi ihlalleri önleyecektir**.** Öte yandan, söz konusu taşınmazlara yalnızca PHS personelinin erişiminin sağlanması ve kişisel verilere ilişkin işlemlerin yalnızca bu amaçla yetkilendirilmiş personel tarafından gerçekleştirilmesinin, posta sektöründe veri güvenliğinin sağlanması açısından önemli olduğu düşünülmektedir.

Bunun yanı sıra Teslimat Usul ve Esaslarının *"fiziki ve teknik gereklilikler"* başlıklı 6 ncı maddesinin ikinci fıkrasının (c) bendi uyarınca; PHS ile sözleşme ilişkisi kuran üçüncü tarafların, gönderilerin muhafazası amacıyla yeterli ve korunaklı bir alan tahsis etmesi gerekmektedir. Bu maddenin de yine posta sektöründe veri gizliliği ve veri güvenliğinin sağlanmasına katkı sunduğu değerlendirilmektedir.

3.4.2.4 Kişisel verilerin bulut ortamında depolanması

Kişisel verilerin dijital ortamda saklanmasında yaygın olarak kullanılan yöntemlerden biri de bulut depolama sistemleridir. Bu sistemler, verilerin fiziksel sunucular dışında, internet üzerinden erişilebilen sanal alanlarda korunmasına olanak sağlar. Ancak veri sorumlularının kendi bilişim altyapıları dışında yer alan bu tür platformlarda veri işlemesi, veri güvenliği bakımından çeşitli riskleri de beraberinde getirmektedir. Bu risklerin azaltılması amacıyla, veri işleme süreçlerinin envanterinin ayrıntılı şekilde oluşturulması, verilerin düzenli olarak yedeklenmesi, bulut ortamına erişimlerde iki aşamalı kimlik doğrulama mekanizmalarının uygulanması büyük önem taşımaktadır.

Ayrıca, verilerin saklanması sırasında kriptografik yöntemlerle şifrelenmesi, her bulut hizmeti için özgün şifreleme anahtarlarının kullanılması ve hizmet ilişkisi sona erdiğinde bu anahtarların tüm kopyalarının geri döndürülemez şekilde imha edilmesi, alınması gereken teknik tedbirler arasında yer almaktadır[342].

KVK Kurulu 16.04.2020 tarihli ve 2020/286 sayılı kararında, bir şirketin bulut tabanlı veri sistemine, kimliği belirsiz kaynaklardan elde edilen bilgilerle yetkisiz erişim sağlandığı ve bu durumun şirketin yeterli sızma testi yapmaması ile gerekli güvenlik önlemlerini almamasından kaynaklandığını tespit ederek şirket hakkında idari para cezası uygulanmasına karar vermiştir. Bu karar, bulut sistemleri kullanılırken idari ve teknik tedbirlerin eksiksiz biçimde uygulanmasının, veri güvenliğinin sağlanması açısından son derece önemli olduğunu ortaya koymaktadır[343].

Diğer yandan PHS'lerin posta hizmetleri kapsamında işlediği verilerin bulut tabanlı sistemlerde depolanması, fiziksel altyapı maliyetlerini azaltma, veri erişimini kolaylaştırma ve iş sürekliliğini sağlama gibi önemli avantajlar sunmaktaysa da yukarıda bahsedilen teknik tedbirlerin PHS'ler tarafından alınmasının gerekli olduğu değerlendirilmektedir.

3.4.2.5 Bilgi teknolojileri sistemlerinin tedariği, geliştirilmesi ve bakımı

Teknolojideki hızlı değişim göz önüne alındığında, bir veri sorumlusunun güvenlik gereksinimlerini dikkatlice değerlendirmesi ve en uygun, güncel sistemleri seçmesi gerekir. Kullanılan cihazların düzenli olarak kontrol edilmesi ve bakımlarının yapılması, cihazlarda bir arıza veya bakım durumu söz konusu olduğunda ve üçüncü bir tarafın müdahalesi gerektiğinde, veri güvenliğini sağlamak için cihazlardaki veri depolama ortamının sökülerek saklanması yahut yalnızca arızalı parçanın üçüncü

---

[342] Yürük, "Veri Sorumlusunun Veri…": 914.
[343] Kişisel Verileri Koruma Kurulu Kararı. 16.04.2020 günlü, 2020/286 sayılı karar.

tarafa verilmesi ve yetkisiz kopyalama veya veri erişimini engellemek amacıyla gerekli tüm önlemlerin alınması önem arz etmektedir[344].

Posta sektöründe de Güvenlik Usul ve Esaslarının *"Hizmet sağlayıcılar tarafından Kuruma bilgi gönderilmesi ile ilgili hükümler"* başlıklı 7 nci maddesinin ikinci fıkrasında; ***"****Hizmet sağlayıcıları, masrafları kendilerine ait olmak üzere her türlü sistemin işletilmesinden, bakımından, söz konusu sistemlerin çalışır vaziyette tutulması için gerekli donanım, yazılım, bakım, onarım, teknik destek gibi gerekli tedbiri almakla ve bunları etkileyen donanım, yazılım, altyapı ve şebekeye ilişkin değişiklikleri Kurum onayını alarak yapmakla yükümlüdürler."* hükmü ile veri güvenliğini teminen gerekli her türlü sistemin işletilmesi ve bakımı konusunda PHS'lerin yükümlü olduğu belirtilmiştir. Bu doğrultuda, PHS'lerin veri güvenliğini sağlamak amacıyla kullandıkları altyapı ve yazılımları güncel tutmaları, düzenli bakım ve kontrolleri gerçekleştirmeleri zorunludur.

3.4.2.6 Kişisel verilerin yedeklenmesi

Veri güvenliğini sağlamak amacıyla alınan bütün önlemlere rağmen, bilgi sistemleri zaman zaman beklenmedik olaylardan etkilenebilmektedir. Siber saldırılar, kötü amaçlı yazılımlar, veri hırsızlığı, doğal afetler ya da kullanıcı kaynaklı hatalar gibi çeşitli durumlar, sistemlerin zarar görmesine neden olabilmektedir. Bu gibi durumlarda, veri sorumlusunun önceden yedeklediği verilere hızla erişebilmesi ve hizmetlerine mümkün olan en kısa sürede devam edebilmesi büyük önem taşır[345].

Bu bağlamda, kişisel verilerin düzenli ve güvenli bir şekilde yedeklenmesi temel bir gereklilik olup yedeklenen verilerin güvenliği de ana sistemler üzerinde tutulan veriler kadar önemlidir. Bu verilerin, internet ağına doğrudan bağlı olmayan (ağ dışı)

---

[344] Kişisel Verileri Koruma Kurumu, "Kişisel Veri Güvenliği Rehberi…": 26-27.
[345] Yürük, "Veri Sorumlusunun Veri…": 915.

ortamlarda tutulması ve yalnızca yetkili sistem yöneticileri tarafından erişilebilir olması, veri ihlali ve kaybı riskini önemli ölçüde azaltabilecektir. Aksi halde, esas veriler ile birlikte yedeklerin de zarar görmesi söz konusu olabilir[346]. Nitekim KVK Kurulu'nun 16.06.2020 tarihli ve 2020/463 sayılı kararında; kritik sistem verileriyle birlikte yedek verilerin depolandığı bir sunucuda gerçekleşen veri kaybında, veri sorumlusunun gerekli tedbirleri almadığına kanaat getirilerek idari para cezası uygulanmıştır[347].

Posta sektörü için de çeşitli düzenlemeler doğrultusunda belirli bir süre boyunca saklanması gereken veriler bulunmaktadır. Bu verilerin ilgili süre boyunca erişilebilir, bütünlüğü korunmuş ve güvenli bir şekilde muhafaza edilmesi hem yasal yükümlülüklerin yerine getirilmesi hem de hizmetin kesintisiz devam edebilmesi açısından önemlidir.

3.4.3 Veri güvenliğinin ihlali halinde bildirim yükümlülüğü

Veri güvenliği ihlallerine ilişkin bildirim yükümlülüğü, kişisel veri ihlalinin gerçekleşmesinin akabinde veri koruma otoritelerinin gecikmeksizin haberdar edilmesi, gerekli tedbirlerin alınması ve veri sahiplerinin bilgilendirilmesi amacıyla veri sorumlularına getirilmiş olan bir yükümlülüktür. Yükümlülüğün temel amacı veri ihlali sebebiyle ortaya çıkan veya çıkabilecek zararın bir an evvel engellenmesi ya da oluşan zararın artmasını engelleyecek tedbirlerin alınmasıdır. Zira veri ihlali halinde, ilgili kişiler gerek ekonomik ve sosyal gerekse de fiziksel zararlara maruz kalabilmektedir[348].

---

[346] Kişisel Verileri Koruma Kurumu, "Kişisel Veri Güvenliği Rehberi…": 27.
[347] Kişisel Verileri Koruma Kurulu Kararı. 16.06.2020 günlü, 2020/463 sayılı karar.
[348] Nur Sena, Sevindi ve Muhammet Emin, Ordu, "AB ve Türk Hukukunda Veri İhlalinin Tespiti ve Bildirim Süresinin Karşılaştırmalı Değerlendirmesi", *Kişisel Verileri Koruma Dergisi*, Cilt: 5, Sayı: 1, (2023): 12-22.

KVKK'de veri ihlalinin ne olduğu ve türleri hakkında açık bir düzenleme bulunmamakta olup herhangi bir sayma veya örneklendirme yoluna da gidilmemiştir. Bununla birlikte KVKK uyarınca sayılan veri güvenliği tedbirleri kişisel verilerin muhafazasını sağlamakla beraber uygun güvenlik düzeyinin teminine yönelik gerekli her türlü idari ve teknik tedbirleri de içermekte olup bu bağlamda ihlalin önemli veya önemsiz olması, küçük veya büyük ölçekli boyutta bulunması fark etmeksizin; her türlü veri ihlalinin KVKK'nin 12 nci maddesi uyarınca KVK Kurulu'na ve ilgili kişilere bildirilmesi gerekmektedir. GDPR'da ise veri ihlali türleri; gizlilik, erişilebilirlik ve bütünlük ihlalleri[349] olmak üzere üç kategoride sayılmıştır. KVKK'den farklı olarak GDPR, her veri ihlalinin ilgili kişiye bildirilmesini zorunlu kılmamaktadır. Veri ihlali halinde, yalnızca veri koruma otoritesine bildirimi yeterli bulurken, GDPR'ın 34 üncü maddesi gereğince temel hak ve özgürlüklerin ihlalinin yüksek olasılığının bulunduğu veri ihlallerinde ilgili kişiye bildirim yapılması zorunluluğu getirilmiştir[350].

Diğer yandan veri ihlaline ilişkin bildirim yükümlülüğünün hangi süre zarfında yapılması gerektiği önemli bir konudur. İşlenen verilerin hukuki olmayan yollarla üçüncü kişiler tarafından elde edilmesi halinde veri sorumlusunun bildirim yükümlülüğü bulunmakta olup KVKK'nin 12 nci maddesinin beşinci fıkrası gereğince süre, ihlalin tespitiyle başlamaktadır. KVK Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı kararında[351] "ihlali öğrenme hali" bu yükümlülüğün başlangıcı olarak belirlenmiştir. GDPR'ın *"Başlangıç"* bölümünün 85 inci maddesi uyarınca da yine haberdar olma hali bildirimde bulunma süresi bakımından esas alınmıştır. Kişisel Veri İhlali Bildirim Formu Kılavuzu'nda ise ihlalin başlangıç tarihi, "veri sorumlusu tarafından yapılan incelemeler sonucunda veri ihlalinin başladığı tarih" olarak belirtilmiştir[352].

---

[349] Gizlilik ihlali; bir kişisel verinin ifşa edilmesi veya erişime açılmasını, erişilebilirlik ihlali; söz konusu verinin imhası veya kaybını, bütünlük ihlali ise kişisel verinin değiştirilmesini ifade etmektedir.
[350] Sevindi ve Ordu, "AB ve Türk Hukukunda Veri…": 12-22.
[351] Kişisel Verileri Koruma Kurumu, *Kişisel Veri İhlali Bildirim Formu Kılavuzu*.
[352] Kişisel Verileri Koruma Kurumu, *Kişisel Veri İhlali Bildirim Formu Kılavuzu*, 6.

KVKK'nin 12 nci maddesinin beşinci fıkrasında yer alan; *"İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir."* hükmü ile bildirimin en kısa sürede yapılması gerektiği düzenlenmiştir. Bu süre, KVK Kurulu'nun 24.01.2019 tarihli ve 2019/10 sayılı kararı ile 72 saat olarak belirlenmiştir. GDPR'ın "*Başlangıç*" bölümünün 85 inci maddesinde ise veri sorumlusunun veri ihlalinden haberdar olmasından itibaren gecikmeksizin, en geç ise 72 saat içinde veri ihlal bildirimi gerçekleştirmesi gerektiği hükme bağlanmıştır.

Bu kapsamda KVK Kurulu tarafından verilen bir kararda; PHS'nin posta gönderisini yanlışlıkla üçüncü bir kişiye teslim etmesi sonucu, ilgili kişinin gönderi içerisinde yer alan kişisel verilerinin kanuni olmayan yolla üçüncü bir kişi tarafından elde edilmesi nedeniyle gelecekte yaşanabilecek benzer olaylar için KVKK'nin 12 nci maddesinin beşinci fıkrası uyarınca en kısa sürede hem Kurula hem de ilgilisine bildirimde bulunması hususunda veri sorumlusunun talimatlandırılmasına karar verilmiştir[353].

KVK Kurulu tarafından verilen diğer bir kararda da bir PHS'nin çapraz barkodlama hatası nedeniyle ilgili kişinin kişisel verilerini hukuka aykırı olarak paylaşması nedeniyle veri güvenliği ihlaline sebep olduğu ancak ilgili ihlali KVKK'nin 12 nci maddesinin beşinci fıkrası gereği KVK Kurulu'na bildirmeyerek ihlale ilişkin bildirim yükümlülüğüne uygun hareket etmediğinden bahisle PHS hakkında idari para cezası uygulanmasına karar verilmiştir[354].

[353] Kişisel Verileri Koruma Kurulu Kararı, 24.03.2022 günlü, 2022/277 sayılı karar.
[354] Kişisel Verileri Koruma Kurulu Kararı, 05/01/2023 günlü, 2023/4 sayılı karar.

4 ÜLKE UYGULAMALARI VE TÜRKİYE'DEKİ MEVCUT DURUM

Bu bölüm kapsamında; başta seçili AB üye ülkeleri olmak üzere, kişisel verilerin korunması konusunda iyi uygulamalara sahip çeşitli ülkelerin, haberleşmenin gizliliği ile veri koruma mevzuatlarına ek olarak posta hizmetleri alanına özgü düzenlemelerine ve bu alanda karşılaşılan veri ihlallerine yer verilmektedir. Akabinde ise Türkiye'deki mevcut durum incelenmektedir.

4.1 Ülke Uygulamaları

4.1.1 Avrupa Birliği

2016 yılında yayımlanan GDPR, iki yıllık bir geçiş sürecinin akabinde, 25.05.2018 tarihinde AB'nin tüm üye devletlerinde, doğrudan uygulanabilir bir düzenleme haline gelmiştir. Ancak GDPR'da, üye devletlerin kendi yerel veri koruma yasaları ile GDPR'dan farklı şekilde düzenleme yapmalarına izin verilen bazı alanlar da bulunmaktadır.

4.1.1.1 Almanya

Almanya'da posta hizmetleri kapsamında verilerin korunması ve postanın gizliliği, çeşitli yasal düzenlemelerle güvence altına alınmıştır. 1949 yılında kabul edilen Alman Anayasası'nın (*Grundgesetz*) 10 uncu maddesi ile haberleşmenin gizliliği temel bir hak olarak tanımlanarak posta, telekomünikasyon ile diğer haberleşme araçlarının gizliliği koruma altına alınmıştır. Anılan Anayasanın 10 uncu maddesi ile *"Mektup, posta ve telekomünikasyon gizliliği"* başlığı altında, mektup ile posta ve telefon haberleşmelerinin gizliliğine dokunulamayacağı düzenlenmiştir. Bununla birlikte bu hakların ancak bir yasaya dayanarak sınırlandırılabileceği, sınırlandırmanın özgürlükçü demokratik temel düzeni veya Federasyon veya bir eyaletin varlık ve güvenliğini koruma amacını güttüğü takdirde, yasada, sınırlamaların ilgiliye

bildirilmemesi ve denetimin hukuk yolu yerine parlamento tarafından tayin edilen organ ve yardımcı organlarca yerine getirilebileceği hükme bağlanmıştır[355].

Alman Ceza Kanunu'nun 202 nci maddesinde, başkalarına ait kapalı mektupların veya benzer haberleşme araçlarının izinsiz açılması veya içeriğinin yetkisiz kişilere açıklanması haberleşmenin gizliliğinin ihlali olarak sayılmış ve bu gizliliğin ihlali durumunda para veya hapis cezası öngörülmüştür[356].

Diğer yandan Almanya, GDPR ile aynı zamanda yürürlüğe giren yeni Alman Veri Koruma Yasası aracılığıyla yasal çerçevesini GDPR ile uyumlu hale getirmiştir[357]. Bu kapsamda, posta hizmetlerini işletme olarak sağlayan veya bu hizmetlere aktif olarak dahil olan herkes posta gizliliğini korumakla yükümlü kılınmıştır[358].

GDPR ile uygulanmakta olan Alman Veri Koruma Yasası, kişisel verilerin işlenmesi, saklanması, aktarılması ve korunması ile ilgili kuralları belirlemektedir. Ayrıca özellikle Almanya'daki kamu kurumları ve özel kuruluşlar için ek düzenlemeler içermekte ve kamu kurumları ve özel şirketler için veri işleme süreçlerinde uyulması gereken yükümlülükleri belirleyerek ve veri sahiplerinin haklarını güvence altına almaktadır.

Alman Veri Koruma Yasası uyarınca veri sorumluları, kişisel veri işleme faaliyetlerinde hukuka uygunluk, şeffaflık, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, doğruluk ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uymakla yükümlüdür. Veri sahipleri ise; bilgi edinme, erişim, kişisel verilerin düzeltilmesini

---

[355] Almanya Federal Adalet ve Tüketiciyi Koruma Bakanlığı (Bundesministerium der Justiz und für Verbraucherschutz) ve Federal Adalet Ofisi (Bundesamt für Justiz), *Grundgesetz für die Bundesrepublik Deutschland*, (2025).

[356] Almanya Federal Adalet ve Tüketiciyi Koruma Bakanlığı (Bundesministerium der Justiz und für Verbraucherschutz) ve Federal Adalet Ofisi (Bundesamt für Justiz), *Strafgesetzbuch (StGB) 202 Verletzung des Briefgeheimnisses.*

[357] DLA Piper, "Collection and Processing in Germany", (2025).

[358] Almanya Federal Şebeke Ajansı (Bundesnetzagentur), *Merkblatt "Postgeheimnis und Datenschutz".*

isteme, unutulma, veri taşınabilirliği, itiraz, otomatik karar alma ve profillemeyle ilgili haklara sahiptir[359].

Ayrıca, Alman Veri Koruma Yasası'nın 22 nci maddesinde hassas veriler için özel koruma tedbirleri öngörülmektedir. Bu kapsamda alınacak tedbirler;

- işlemenin GDPR'a uygun olmasını sağlamak için teknik ve organizasyonel tedbirler,
- kişisel verilerin ulaşılıp ulaşılmadığı, değiştirildiğinin veya silindiğinin daha sonra doğrulanmasının ve tespit edilmesinin mümkün olmasını sağlayacak tedbirler,
- işleme operasyonlarında görev alan personelin farkındalığını artırmaya yönelik tedbirler,
- veri koruma görevlisinin atanması,
- denetleyici ve işlemciler tarafından kişisel verilere erişime ilişkin kısıtlamalar,
- kişisel verilerin takma adla işlenmesi,
- kişisel verilerin şifrelenmesi,
- kişisel verilerin işlenmesiyle ilgili sistem ve hizmetlerin işleyebilirliğini, gizliliğini, bütünlüğünü, erişilebilirliğini ve dayanıklılığını sağlamak için alınacak önlemler; ayrıca fiziksel veya teknik bir olay durumunda erişim ve erişilebilirliğin hızlı bir şekilde yeniden sağlanabilme yeteneği,
- işlemenin güvenliğinin sağlanması için teknik ve organizasyonel tedbirlerin etkinliğinin düzenli olarak test edilmesi, değerlendirilmesi ve ölçülmesine yönelik bir süreç,
- başka amaçlarla aktarılması veya işlenmesi durumunda Alman Veri Koruma Yasası ve GDPR'a uyumu sağlamak için belirli usul kuralları

olarak sayılmıştır. Ayrıca, kişisel veri ihlallerinde yetkili denetim makamına bildirim zorunlu kılınmıştır.

---

[359] Dünya Posta Birliği (UPU), *Country Name: Germany*.

Alman Veri Koruma Yasası, Federal Veri Koruma Komiserliği'nin yetkilerini belirleyerek, veri koruma ihlallerini denetleme, yaptırımlar uygulama ve kamu kurumları ile özel sektör kuruluşlarını denetleme yetkisi vermektedir. Posta hizmetleri alanında ise anılan Yasanın 16 ncı bölümünde Federal Veri Koruma Komiserliği'nin yetkilerinin, posta ve telekomünikasyon hizmetleri alanında yapılan veri işlemlerine erişim sağlama yetkisini de içerdiği düzenlenmiştir. Bu kapsamda Komiserlik, PHS'lerin sistemlerine ve ilgili verilere erişebilmekte, denetim yapabilmekte ve gerektiğinde yaptırım uygulayabilmektedir [360]. Bu noktada Alman Anayasası'nın 10 uncu maddesinde yer alan haberleşme ve posta gizliliği temel hakkı sınırlandırılmaktadır.

Almanya'da veri sorumluları veya veri işleyicilerin, veri koruma hukuku açısından yetkili denetim makamına işleme faaliyetlerini kaydettirmeleri konusunda genel bir gereklilik bulunmamaktadır; ancak her makam tarafından bir "veri koruma görevlileri sicili" tutulmaktadır. Alman Veri Koruma Yasası'nın 38 inci maddesi ise en az 20 kişinin, otomatik yollarla kişisel verilerin işlenmesiyle ilgili sürekli olarak çalıştırılması halinde bir veri koruma görevlisi belirlenmesini zorunlu kılmıştır.

Alman Veri Koruma Yasası'nın 85 inci maddesi uyarınca kişisel verilerin GDPR veya 2016/680 sayılı Kolluk Direktifi kapsamına girmeyen faaliyetler bağlamında üçüncü bir ülkeye veya uluslar üstü veya yabancı devletlere veya sair uluslararası kuruluşlara aktarılmasına, zorunlu savunma nedenleriyle kendi görevlerinin yerine getirilmesi veya kriz yönetimi veya çatışmanın önlenmesi veya insani önlemler alanında federal bir kamu kurumunun uluslarüstü veya uluslararası yükümlülüklerinin yerine getirilmesi için gerekli olması halinde de izin verilmektedir. Ayrıca verinin aktarıldığı tarafa, aktarılan verilerin yalnızca aktarıldıkları amaç için kullanılabileceği bildirilmektedir.

[360] DLA Piper, "Collection and Processing in Germany", (2025).

Diğer yandan posta gizliliğinin sağlanması Almanya'nın ulusal düzenleyici otoritesi Bnetza'nın posta sektörü alanındaki temel sorumlulukları arasında bulunmaktadır[361]. Nitekim 15 Temmuz 2024 tarihinde yayımlanan Alman Posta Kanunu (*PostG*)'nun 2 nci maddesinin altıncı fıkrasında Kanun'un amaçları arasında *"Kamu güvenliği ve posta gizliliği çıkarlarının korunması"* hükmü yer almaktadır. Bu çerçevede Almanya'da posta hizmetlerinin gizliliğine ilişkin hükümlere Alman Posta Kanunu'nun 2 nci bölümünün 64-66 ncı maddelerinde yer verilmektedir. Söz konusu hükümler kapsamında belirli gerçek veya tüzel kişilerin posta trafiğine ilişkin özel durumları ile posta gönderilerinin içerikleri, posta gizliliğine tabidir. Posta hizmeti sunanlar veya bu hizmetlerin sağlanmasına ticari amaçla katılan herkes, posta gizliliğini korumakla yükümlüdür. Bu yükümlülük, ilgili kişinin görev veya faaliyetinin sona ermesinden sonra da devam etmektedir. Ayrıca posta hizmetlerinde görevli kişilerin, hizmetin sağlanması için gerekli olanın da ötesinde, posta gönderilerinin içeriği veya posta trafiğine ilişkin özel bilgileri kendileri veya başkaları adına edinmeleri de yasaktır. Bu bilgiler yalnızca belirtilen hizmetin yerine getirilmesi amacıyla kullanılabilmektedir. Başka amaçlarla kullanılması veya üçüncü kişilere açıklanması ancak ilgili kanun veya yasal düzenlemeler kapsamında, açık bir şekilde posta gönderilerine veya posta trafiğine atıfta bulunulması durumunda mümkündür. Bu kapsamda belirli bir tarife ile gönderilen posta gönderilerinin söz konusu tarifeyi karşılayıp karşılamadığını kontrol etmek, hasarlı gönderilerin içeriğini güvence altına almak, başka bir şekilde tespiti mümkün olmayan posta gönderilerinin alıcısını veya göndericisini belirlemek amacıyla belirtilen yasaklara istisna getirilmiştir[362].

Alman Posta Kanunu'nun 65 inci maddesinde ise PHS'lerin, mahkemeler ve yetkili makamların talebi üzerine, posta trafiğine dahil olan bir kişinin tebligat yapılacak adresini paylaşmakla yükümlü olduğu düzenlenmiştir. Bu paylaşım, mahkemelerin

---

[361] Çakmak, *Posta Sektöründe Kullanıcı Düzenlemeleri: Ülke…,* 89.

[362] Almanya Federal Adalet ve Tüketiciyi Koruma Bakanlığı (Bundesministerium der Justiz und für Verbraucherschutz) ve Federal Adalet Ofisi (Bundesamt für Justiz), *Postgesetz (PostG).*

veya yetkili makamların posta trafiği ile ilgili gereksinimlerini karşılamak amacıyla gerçekleştirilmektedir.

Bir diğer önemli konu da kullanıcılara ait kişisel verilerin korunması olup konuya ilişkin mevzuat hükümlerine Alman Posta Kanunu'nun 3 üncü bölümünün 67-71 inci maddelerinde yer verilmektedir. Söz konusu maddelerde GDPR'ın Alman Posta Kanunu'nda yer alan madde hükümleriyle desteklendiği belirtilmektedir. Ayrıca posta gönderisinin içeriğine ek olarak, veri korumanın, posta hizmetleriyle ilgili tüm kişisel verileri (örneğin trafik verileri, teslimat verileri, fatura verileri ve adres verileri gibi) de içerdiği açıklanmıştır.

Alman Posta Kanunu'nun 68 inci maddesi kişisel verilerin işlenmesine izin veren veya bunu öngören bir madde olarak karşımıza çıkarmaktadır. Buna göre PHS'ler, gönderilerin usulüne uygun şekilde teslim edilmesi amacıyla gerekli olduğu hallerde adres değişikliğine ilişkin kişisel verileri diğer PHS'lere iletebilmektedir. Bu adres bilgisinde isim, teslimat veya teslim alma bilgileri ve posta yönlendirme bilgileriyle birlikte varış noktası da yer almaktadır. İlgili kişi, bir yönlendirme siparişi verirken, gelecekteki posta gönderilerinin doğru bir şekilde adreslenmesi amacıyla, veri sahibinin yanlış adresini içeren bir posta gönderisinin göndericisine talep üzerine adres değişikliğinin bildirilmesine onay vermişse, diğer hizmet sağlayıcılar, bu hüküm uyarınca kendilerine sağlanan bilgileri kullanabilmektedir.

Diğer taraftan posta kutusu sistemlerini[363] işleten hizmet sağlayıcılar, talep üzerine herhangi bir kişiye posta kutusu sahibinin posta kutusu adresini verebilmektedir. Bu posta kutusu sistemleri aracılığıyla posta teslimi faaliyetleri için gerekli olan veriler

[363] Posta kutusu sistemleri (Pick-Up Drop-Off, PUDO); posta kullanıcıların gönderilerini teslim alıp gönderebildikleri belirli teslimat noktalarını ifade etmektedir. Bu noktalar; marketler, toplu taşıma alanları ya da özel olarak oluşturulmuş merkezler gibi erişimi kolay yerlerde konumlandırılır. Bu sistem, gönderici veya alıcının paketlerini doğrudan bir adrese yönlendirmek yerine, daha erişilebilir ve esnek bir teslimat noktası olan PUDO noktasına yönlendirmesine olanak tanımaktadır. (Akbulut, *Posta Sektöründeki Dijital Dönüşümün…,* 116)

diğer PHS'lere de mevzuat kapsamında iletilebilmektedir. PHS'ler, posta gönderilerinin usulüne uygun şekilde teslimi için gerekli olduğu ölçüde, gönderinin alıcılarının ve yedek alıcılarının kişisel verilerini işleyebilmektedir. Bazı hallerde, gönderilerin usulüne uygun şekilde teslim edilmesini sağlamak amacıyla, teslimat sırasında dikkate alınması gereken özel durumlara ilişkin kişisel verileri de işleyebilmektedirler.

Öte yandan PHS'ler, posta trafiğinde yer alan bir tarafın verdiği adresin doğru olup olmadığına ilişkin bilgiyi, posta trafiği amaçları bakımından adres doğrulamasının gerekli olması halinde, üçüncü bir tarafın talebi üzerine sağlayabilir. Güncel adrese ilişkin verilen bilgilerdeki açık yazım hatası ve benzeri yanlışlıklar PHS'ler tarafından düzeltilebilir.

Alman Posta Kanunu'nun 69 uncu maddesine göre posta hizmetinin sunumunda PHS'ler kullanıcılardan hizmetin doğru bir şekilde yerine getirilmesini sağlamak amacıyla geçerli bir kimlik kartı, pasaport ya da resmi kimlik belgesi ibraz edilerek kimlik doğrulamasının yapılmasını talep edebilirler. Bu kapsamda kimliğin türü, kimliği veren makam, kimlik numarası, veriliş tarihi hizmetin usulüne uygun ifa edildiğine dair delil sağlamak amacıyla işlenebilmektedir. Bununla birlikte bu veriler yasal veya sözleşmeden kaynaklı zamanaşımı süresinin sona ermesinden itibaren en geç altı ay içerisinde silinmelidir.

Almanya'da yaklaşık 17 farklı Veri Koruma Otoritesi bulunmaktadır. Bunlardan biri, federal düzeyde PHS'ler ve telekomünikasyon kuruluşları üzerinde genel yetkiye sahiptir. Diğer 16 otorite ise federe düzeyde kendi yetki alanlarındaki özel şirketler üzerinde denetim yapmaktadır[364]. Alman Posta Kanunu'nda ise posta sektöründe veri koruma denetiminin nasıl yapılacağı hususu düzenlenmiştir. Buna göre Alman Posta Kanunu'nun 71 inci maddesinde kişisel verilerin posta hizmetlerinin ticari olarak

[364] Peter, Oladimeji, "Germany's data privacy protection laws: Everything you need to know", (2023).

sağlanması amacıyla işlenmesi durumunda, Alman Veri Koruma Kanunu'nun 40 ıncı maddesi uyarınca şirketlerin denetiminin, Federal Veri Koruma ve Bilgi Özgürlüğü Komiseri tarafından yapılan denetimle değiştirileceği hükme bağlanmıştır. Bu kapsamda Federal Veri Koruma ve Bilgi Edinme Özgürlüğü Komiseri, gözetim görevlerinin yerine getirilmesi için gerekli olduğu ölçüde, bilgi ve incelemeler yoluyla belirli kişilerin posta trafiğinin özel koşulları hakkında bilgi edinebilmektedir.

Son olarak, doğrudan Almanya posta sektörüne yönelik bir kişisel veri ihlali vakası şu ana kadar dikkat çekmemektedir.

4.1.1.2 Avusturya

Avusturya'da posta hizmetleri kapsamında posta gizliliği ve veri koruma hem ulusal mevzuat hem de AB mevzuatı ile güvence altına alınmıştır. Avusturya Anayasası (*Bundes-Verfassungsgesetz*)'nın 10 uncu maddesinde, federal hükümetin düzenleme yapma ve yürütme yetkileri belirlenmiştir. Bu madde uyarınca, bazı alanlarda yalnızca federal hükümetin düzenleme yapabileceği hükme bağlanmıştır. Posta hizmetleri de bu kapsamda yer almakta olup bu alanda düzenleme yapma yetkisi yalnızca federal parlamentoya aittir. Dolayısıyla, eyaletlerin posta hizmetlerine ilişkin düzenleme yapma yetkisi bulunmamaktadır[365]. Diğer yandan 1867 yılında kabul edilen Avusturya Temel Haklar Yasası (*Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger 1867*) Avusturya'da bireylerin temel hak ve özgürlüklerini düzenleyen anayasal belgelerden biridir. Bugün hâlâ yürürlükte olan Avusturya Temel Haklar Yasası, artık tek başına bir anayasa metni gibi değil, anayasanın bir parçası olarak kabul edilmektedir. Bu nedenle, Avusturya Anayasası yalnızca B-VG'den değil; Avusturya Temel Haklar Yasası, anayasal statü kazandırılmış Avrupa İnsan Hakları Sözleşmesi ve diğer bazı belgelerden oluşan daha geniş bir bütünden meydana

[365] Avusturya Federal Anayasası, 1930.

gelmekte olup Avusturya Temel Haklar Yasası'nın anayasal düzen içindeki yeri, Avusturya Anayasası'nın 149 uncu maddesinde de açıkça belirtilmiştir.

Avusturya Temel Haklar Yasası'nın 10 uncu maddesi gereği haberleşmenin gizliliği ihlal edilememektedir. Ayrıca mektuplara el konulması, kanuni yakalama veya arama halleri haricinde ancak savaş zamanında veya yürürlükteki kanunlara uygun olarak verilen yargı kararıyla mümkün olup Avusturya'da posta hizmetleriyle ilgili gizlilik koruması temel olarak bu hükme dayanmaktadır[366].

Diğer yandan Avusturya Ceza Kanunu (*Strafgesetzbuch*) 1974 yılında kabul edilmiş ve 01.01.1975'te yürürlüğe girmiştir. Kanun'un *"Mektup gizliliğinin ihlali ve mektupların alıkonulması"* 118 inci maddesi, kişinin bilgisi olmaksızın başkasına ait mühürlü bir mektubu veya benzeri bir belgeyi açan kişilere yönelik cezai yaptırımları düzenlemektedir. Anılan maddede bu tür belgelerin içeriğini öğrenmek amacıyla teknik bir yöntem kullanan veya mühürlü bir belgeyi açan kişilerin üç aya kadar hapis cezası veya 180 güne kadar para cezasıyla cezalandırılabileceği hükme bağlanmıştır. Ayrıca bir mektubu veya bir belgeyi alıcının haberi olmadan gizleyen veya alıkoyan kişinin de cezalandırılacağı belirtilmiştir. Söz konusu suçlar şikâyete tabi suç kapsamında olmakla birlikte suçun, kamu görevlisi tarafından görevinin ifası sırasında veya görevinin kendisine verdiği imkândan yararlanılarak işlenmesi halinde, Cumhuriyet savcısının, mağdurun izniyle fail hakkında kovuşturma yapmak zorunda olduğu belirtilmiştir[367].

Diğer yandan Avusturya'da, verilerin korunması alanında GDPR'ın uygulanmasına ilişkin yasalar kademeli olarak kabul edilmiştir. 2000 yılından itibaren yürürlükte olan

---

[366] Avusturya Federal Şansölyeliği (Bundeskanzleramt), "Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger, Fassung vom 08.05.2025".

[367] Avusturya Ceza Kanunu, 1975.

Avusturya Veri Koruma Kanunu (*Datenschutzgesetz*)[368]**,** posta hizmetleri de dahil olmak üzere kamu ve özel sektördeki veri işleme faaliyetlerine ilişkin esasları belirlemektedir. 2017 yılında Avusturya Veri Koruma Kanunu, GDPR ile ilgili çeşitli düzenlemelerin ilk uygulamasını oluşturan ve GDPR ile aynı anda yürürlüğe girmesi amaçlanan Veri Koruma Değişiklik Yasası 2018 (*Datenschutz-Anpassungsgesetz 2018*) ile değiştirilmiştir. Gizlilik Deregülasyon Yasası 2018 (*Datenschutz-Deregulierungs-Gesetz 2018*) ise Avusturya Veri Koruma Kanunu'nu daha da değiştirmiş ve halihazırda yürürlükte olan düzenlemedir[369].

GDPR ve Avusturya Veri Koruma Kanunu uyarınca veri sorumluları; kişisel veri işleme faaliyetlerinde hukuka uygunluk, şeffaflık, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, doğruluk ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uymakla yükümlüdür. Veri sahipleri ise bilgi edinme, erişim, kişisel verilerin düzeltilmesini isteme, unutulma, veri taşınabilirliği, itiraz, otomatik karar alma ve profillemeyle ilgili haklara sahiptir[370].

Avusturya Veri Koruma Kanunu'nun 8 inci maddesi uyarınca kamu kurumları, belirli koşullarda adres bilgilerine ilişkin verileri, tebligatlar ya da bilgi talepleri için de kullanabilmektedir. Bu düzenleme, posta yoluyla haberleşme süreçlerinde adres bilgilerinin kamu yararına kullanımına imkân tanımaktadır.

Avusturya Veri Koruma Kanunu'nda veri ihlallerinin veri koruma otoritesine bildirilmesi hakkında GDPR hükümleri haricinde başka bir düzenlemeye yer verilmemiş ve GDPR'a atıfta bulunulmakla yetinilmiştir. Buna göre Kanun'un 55 inci maddesinde veri sorumlusunun, kişisel veri ihlallerini GDPR'ın 33 üncü maddesi

---

[368] Avusturya Federal Şansölyeliği (Bundeskanzleramt), *Bundesgesetz über den Schutz personenbezogener Daten*.
[369] Avusturya Cumhuriyeti Federal Hukuk Gazetesi, 5 inci madde, (15 Ocak 2019).
[370] Dünya Posta Birliği (UPU), *Country Name: Austria*.

uyarınca veri koruma otoritesine bildirmesi gerekmektedir. Diğer yandan Avusturya Veri Koruma Kanunu veri koruma görevlisinin hakları ve yükümlülükleri ile ilgili bazı ek düzenlemeler içermektedir. Buna göre, veri koruma görevlisi ve onun için çalışan tüm kişiler, veri koruma görevlisine başvuran kişilerin kimlikleri ve bu kişilerin kimliklerini ortaya çıkarabilecek tüm durumlar hakkında gizliliği korumakla yükümlüdür.

Avusturya'da, GDPR'nin uygulanmasından Avusturya Veri Koruma Otoritesi (*Österreichische Datenschutzbehörde*) sorumludur[371]. Avusturya Veri Koruma Kanunu'nun 11 inci maddesi uyarınca, Avusturya Veri Koruma Otoritesi, idari para cezalarını uygulamakla yükümlüdür. Ancak Otorite, özellikle ihlalin ilk kez yaşanması durumunda, para cezası uygulamak yerine GDPR'ın 58 inci maddesinde düzenlenen "uyarı" başta olmak üzere gerekli önlemleri de uygulayabilmektedir.

Avusturya Posta Kanunu (*Postmarktgesetz*) ise 2011 yılında yürürlüğe girmiş olup Avusturya'da posta hizmetlerinin düzenlenmesi, rekabetin sağlanması ve tüketici haklarının korunmasını amaçlamaktadır. Kanun'un *"Posta Gizliliği"* başlıklı 5 inci maddesi uyarınca posta hizmeti sunan kişiler, federal yasalarda aksi açıkça belirtilmedikçe faaliyetleri süresince ve faaliyetlerinin sona ermesinden sonra, gönderilere ilişkin her türlü bilgiyi gönderici ya da alıcı dışındaki üçüncü kişilere açıklamaktan kaçınmakla yükümlüdür. Aynı maddenin ikinci fıkrası uyarınca ise gizlilik yükümlülüğü, re'sen soruşturulması gereken adli suçlara ilişkin suç duyurusunda bulunulmasına engel teşkil etmemektedir. Diğer yandan yasada aksi açıkça belirtilmedikçe, teslimatın alıcının imzasıyla onaylaması gereken gönderilerde, gönderi yalnızca üzerinde belirtilen teslimat adresinde bulunan kişilere teslim edilebilir. Bu şekilde teslimat, gönderinin teslim edilmesinin başka türlü mümkün olmadığı ve ne gönderici ne de alıcı tarafından bu teslimat imkânının önceden açıkça reddedilmemesi halinde mümkündür. Ayrıca bu kişiler gönderileri ayrı bir teslim alma

[371] Avrupa Veri Koruma Kurulu (EDPB), "Our Members".

noktasından da alabilme imkânına sahiptirler. Bunun yanı sıra belirtilen teslimat adresinde teslim almaya yetkili kimsenin bulunmaması halinde, bir gerçek kişiye gönderilen paketler, gönderici ya da alıcı tarafından önceden açıkça reddedilmemiş ise komşulara da teslim edilebilmektedir. Bununla birlikte bu şekilde bir teslimat yapıldığı konusunda alıcı yazılı olarak bilgilendirilmelidir.

Diğer yandan Avusturya Posta Kanunu'nun 5 inci maddesinin beşinci fıkrası uyarınca PHS, kapalı bir gönderinin gönderici veya alıcıya tesliminin mümkün olmaması durumunda, gönderici ya da alıcının kimliğinin tespiti veya zararlarını önlemek amacıyla gönderiyi açabilir. Aynı maddenin altıncı fıkra uyarınca ise posta hizmetinin sunulması sırasında PHS'nin sorumluluğunda bulunan bir posta gönderisi, aksi kanunen açıkça belirtilmedikçe, herhangi bir icra takibine veya başka idari tedbire tabi tutulamaz. Ancak 1975 tarihli Ceza Muhakemesi Kanunu hükümleri ile mektup ve diğer gönderilere el konulması ve bunların açılmasına ilişkin hükümler istisna tutulmuştur.

Diğer yandan Avusturya Posta Kanunu'nun 35 inci maddesinin ikinci fıkrası gereğince gönderilerin teslimi ve iadesi süreçlerinde PHS'ler, diğer PHS'lerin adres verilerine erişim hakkına sahiptir. Bu erişimin şeffaf olması ve ayrımcı olmaması gerekmekte olup bu şekilde elde edilen veriler başka amaçlarla kullanılamamaktadır[372].

Bu kapsamda, yakın tarihte Avusturya posta sektöründe gerçekleşmiş bir kişisel veri ihlali dikkat çekmektedir. Buna göre söz konusu vakada; Avusturya'da posta hizmeti sunan ve pazar payı en yüksek olan Austrian Post (*Osterreichische Post AG*) şirketinin[373], müşterilerinin adres, yaş, cinsiyet gibi verilerini toplayarak siyasi eğilim tahmini yaptığı ve bu bilgileri üçüncü taraflara (örneğin pazarlama şirketlerine) sattığı

[372] Avusturya Yayıncılık ve Telekomünikasyon Düzenleme Kurumu, "Rechte und Pflichten von Postdiensteanbietern".
[373] IBIS World, "Postal & Courier Activities in Austria - Market Size, Industry Analysis, Trends and Forecasts (2025-2030)", (2025); Hazel, King, "Austrian Post delivers record 508 million parcels in 2024", (2025).

tespit edilmiştir. Avusturya Veri Koruma Otoritesi tarafından bu uygulamaların rızaya dayalı olmadığı ve GDPR'ı ihlal ettiği tespit edilmiş olup anılan şirkete 2019 yılında 18 milyon Euro para cezası uygulanmıştır. Bununla birlikte Avusturya'daki en yüksek idare mahkemesi, aynı zamanda evrensel hizmet sağlayıcısı da olan Austrian Post'un, Avusturya Veri Koruma Otoritesi tarafından kendisine kesilen 18 milyon Euro'luk para cezasını ödemek zorunda kalmayacağına hükmetmiştir. Anılan Mahkeme, Avusturya Veri Koruma Otoritesi'nin Austrian Post'un hanehalklarının "siyasi eğilimleri" hakkında bilgi derlemek ve satmak için GDPR kurallarını ihlal ettiği görüşüne katılmakla birlikte, Avusturya Veri Koruma Otoritesi'nin para cezasının verilmesinde usule aykırı davrandığına karar vererek para cezasını tamamen iptal etmiştir[374].

Aynı ülkede gerçekleşen bir başka veri ihlali ise Avusturya Veri Koruma Otoritesi tarafından verilen 28 Eylül 2021 tarihli ve 9,5 milyon Euro para cezası ile sonuçlandırılmıştır. Bu olayda, Veri Koruma Otoritesi'nin iddiasının temelini Austrian Post'un; posta, web iletişim formu ve müşteri hizmetleri aracılığıyla kullandığı iletişim seçeneklerine ek olarak, veri koruma sorularına e-posta yoluyla da izin verilmesi gerekliliğinin ihlal edildiği oluşturmaktadır[375]. Bu karar sonucu verilen para cezasının, 2025 yılının mart ayı itibarıyla Avusturya Veri Koruma otoritesi tarafından verilen ve onaylanan en yüksek para cezası olduğu belirtilmiştir[376].

4.1.1.3 Belçika

Belçika'da da posta gizliliği, yasal düzenlemelerle koruma altına alınmıştır. 1831 yılında kabul edilen ve son halini 2014 yılında alan Belçika Anayasası'nın 29 uncu maddesi, mektupların gizliliğinin ihlal edilemez nitelikte olduğunu hükme bağlamaktadır. Bununla birlikte aynı madde uyarınca posta hizmetlerinin teminatı

---

[374] Armen, Ghalumyan, "Fine on Posti for violation of data protection regulations", Cullen International, (2020).
[375] The Austrian Post, "Datenschutzverfahren Der Österreichischen Post", (2021).
[376] Marianna, Mattera, "Fines for Data Protection Infringements", (2025).

altında olan mektupların gizliliğinin hangi makamlar tarafından ihlal edilebileceğinin kanunla belirtileceğini düzenlemiştir[377].

Diğer yandan posta hizmetleri kapsamında olan mektupların gizliliğinin hangi makamlar tarafından bertaraf edilebileceğinin kanunlarla belirleneceği düzenlenmiştir. Buna göre postanın gizliliği her ne kadar ilgili Anayasa hükmüyle mutlak bir hak olarak düzenlenmiş olsa da Belçika AYM'si, suçla etkin mücadele amacıyla kamu otoriteleri tarafından ileri sürülen kamu güvenliği, suç ve terör tehditlerinin oluşturduğu tehlike gerekçelerini, bu hakkın sınırlandırılması için yeterli görerek bu hakkın kısıtlanabileceğine hükmetmektedir[378]. Anılan Mahkeme, söz konusu tehditlerin gerçek boyutunu derinlemesine incelemeksizin, kamu güvenliği gerekçesini bu tür müdahaleleri meşrulaştırmak adına geçerli bir temel olarak kabul etmektedir[379].

Yeni Belçika Ceza Kanunu ise 8 Nisan 2024 tarihinde Resmî Gazete'de yayımlanmış olup 8 Nisan 2026'da yürürlüğe girecektir. Söz konusu Kanun'un 347 nci maddesinde *"Mektup Gizliliğinin İhlali"* düzenlenmiştir. Anılan maddeye göre mektup gizliliğinin ihlali, PHS'lere emanet edilen bir mektubun kasıtlı olarak yok edilmesi veya gizliliğini ihlal etmek amacıyla açılması ile gerçekleşmektedir. Aynı şekilde, bir icra memuruna ait mektubun yok edilmesi veya gizliliğini ihlal etmek amacıyla açılmasının da bu kapsamda değerlendirildiği hükme bağlanmıştır. Ancak, ikinci durumda; mektubun ilgili çocuğun anne veya babası, eş, vasi, yönetici ya da kayyımı tarafından açılması gizlilik kuralına getirilen bir istisnadır[380].

---

[377] Belçika Anayasası, 1831.
[378] Belçika Anayasası, 1831.
[379] Patricia, Popelier ve Catherine, Van De Heyning, "Procedural Rationality: Giving Teeth to the Proportionality Analysis", *European Constitutional Law Review*, Cilt: 9, Sayı: 2, (2013):238.
[380] Belçika Adalet Bakanlığı (Service public fédéral Justice), "Loi Introduisant Le Livre II Du Code Pénal", (2024).

Diğer yandan 30 Temmuz 2018 tarihli Belçika Veri Koruma Kanunu (*Act on the protection of natural persons with regard to the processing of personal data*), GDPR'a uyumlu olarak kişisel verilerin işlenmesine ilişkin kuralları belirlemekte ve bireylerin veri koruma haklarını güvence altına almaktadır. Kanun, GDPR ile birlikte uygulanmakta olup kişisel verilerin işlenmesi, saklanması, aktarılması ve korunması ile ilgili kuralları belirlemekte, kamu kurumları, sağlık sektörü, işverenler ve çocuklara yönelik veri işlenmesi ile ilgili ek düzenlemeler içermektedir. GDPR'da yer alan tanımları temel almakla birlikte; "önemli kamu yararına veri işleme" ve "gazetecilik amaçlarıyla veri işleme" gibi bazı kavramları da netleştirmekte ve "ortak veri tabanı" gibi yeni kavramlar ortaya koymaktadır. Ayrıca güvenilir üçüncü taraf, kişisel verilerin açıklanması ve kişisel verilerin dağıtımı gibi kavramları, araştırma ve istatistiksel amaçlar için yapılan veri işleme istisnası bağlamında tanımlamaktadır[381].

Belçika'da veri sorumluları; kişisel veri işleme faaliyetlerinde hukuka uygunluk, şeffaflık, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, doğruluk ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uymakla yükümlüdür. Veri sahipleri ise bilgi edinme, erişim, kişisel verilerin düzeltilmesini isteme, unutulma, veri taşınabilirliği, itiraz, otomatik karar alma ve profillemeyle ilgili haklara sahiptir[382]. Ayrıca Kanunda hassas veriler için özel koruma tedbirleri de öngörülmüştür.

Belçika Veri Koruma Kanunu uyarınca Belçika Veri Koruma Otoritesi (*De Gegevensbeschermingsautoriteit*) kişisel verilerin korunmasının temel ilkelerinin doğru şekilde gözetilmesinin sağlanmasından sorumlu bağımsız bir kurum olarak görev yapmaktadır[383]. Anılan Kanun, GDPR'a ek olarak, belirli durumlarda veri koruma görevlisi atanmasını zorunlu kılmaktadır. Özellikle özel hukuk tüzel kişilerinin federal kamu otoriteleri adına veri işlemesi veya kolluğun görevleri kapsamında veri aktarımı

[381] DLA Piper, "Definitions in Belgium", (2024).
[382]Dünya Posta Birliği (UPU), *Country Name: Belgium.*
[383] Belçika Veri Koruma Kurumu (Gegevensbeschermingsautoriteit), "Organisatie".

yapılması durumunda veri koruma görevlisi atanması gerekmektedir. Ayrıca, kamu yararına yönelik arşivleme, bilimsel veya tarihsel araştırmalar ile istatistiksel amaçlarla veri işlenmesi hallerinde de benzer bir yükümlülük söz konusudur. Belçika Veri Koruma Otoritesi, veri koruma görevlisi atanmasına ve görevlerini yerine getirme biçimine ilişkin çeşitli kararlar almıştır. Bu bağlamda, veri koruma görevlisinin bağımsızlığı, en üst yönetim seviyesine doğrudan raporlama yükümlülüğü, görevlerini yerine getirebilmesi için yeterli kaynaklara ve alanında uzmanlığa sahip olması gerekliliği temel prensipler olarak belirlenmiştir[384].

Diğer yandan 14 Mart 2022 tarihli Posta Hizmetlerine İlişkin Kraliyet Kararnamesi'nin 3 üncü maddesinin üçüncü fıkrasında posta gönderilerinin teslimatının, göndericinin belirttiği adresin açık, net ve teslimat adresiyle tam uyumlu olması koşuluyla gerçekleştirileceği belirtilmiştir. Bununla birlikte gönderici tarafından beyan edilen adresin, belirlenen teslimat adresiyle açıkça veya araştırma yoluyla eşleşmemesi halinde PHS'nin, adrese ulaşmak amacıyla bazı gösterge unsurlarına veya kişisel verilerin otomatik işlenmesine başvurabileceği hüküm altına alınmıştır. Bu süreçte daha önce aynı alıcıya yapılan gönderiler bağlamında işlenmiş veriler veya PHS'lerin daha önce kullandığı adres veri tabanları gibi kaynakların da kullanılabileceği düzenlenmiştir[385].

Öte yandan, Belçika'da da bazı veri ihlallerine rastlanmaktadır. Örneğin; 2020 yılında Belçika'da faaliyet gösteren bir PHS olan Bpost, kullanıcıların takibi ve gönderilere ilişkin bilgilerin ifşasına yol açan bir veri ihlaliyle karşı karşıya kalmıştır. Söz konusu ihlalde, saldırganlar Bpost'un çevrim içi takip sisteminde bulunan güvenlik açıklarından faydalanarak teslimata dair verilere yetkisiz erişim sağlamıştır. Bu durum, binlerce gönderinin hırsızlık ve dolandırıcılık gibi risklerle karşı karşıya kalmasına neden olmuştur. Her ne kadar finansal verilerin tehlikeye atılmadığı

[384] DLA Piper, "Data protection officers in Belgium", (2024).
[385] Belçika Adalet Bakanlığı (Service public fédéral Justice), "Arrêté royal relatif aux services postaux", (2022).

bildirilmiş olsa da yaşanan ihlal, kamu hizmeti sunan kuruluşların veri güvenliği uygulamaları açısından ciddi endişelere yol açmış ve şirketin itibarını olumsuz etkilemiştir. Bu ihlal, özellikle zayıf uygulama programlama ara yüzlerinin doğurabileceği riskleri ve çevrim içi sistemlerde kullanıcı verilerinin şifrelenmesinin önemini ortaya koymuştur[386].

4.1.1.4 Finlandiya

Finlandiya'da postanın gizliliği, yasal düzenlemelerle koruma altına alınmıştır. 2000 yılında yürürlüğe giren Finlandiya Anayasası (*Suomen Perustuslaki*)'nın 10 uncu maddesi ile özel hayatın gizliliği temel bir hak olarak tanımlanmıştır. Maddede mektup, telefon görüşmeleri ve diğer haberleşmelerin gizliliğinin ihlal edilemeyeceği hükme bağlanmıştır. Bununla birlikte kişi veya toplumun güvenliğini veya iç barışını tehlikeye düşüren suçların soruşturulması, yargılama, güvenlik kontrolleri ve hürriyeti bağlayıcı cezalar sırasında yapılan haberleşmelerin gizliliğine, ayrıca askerî harekâtlara veya milli güvenliği ciddi şekilde tehdit eden diğer faaliyetlere ilişkin bilgi edinilmesine ilişkin olarak haberleşmenin gizliliğine gerekli sınırlamaların getirilebileceği düzenlenmiştir[387].

Finlandiya Ceza Kanunu (*Rikoslaki*)'nin 38 inci bölümünde, haberleşme gizliliğini ve kişisel verilerin korunmasını ihlal eden suçlar düzenlenmektedir. Anılan Kanuna göre bir kişinin mektuplarını, e-postalarını veya diğer haberleşme araçlarını izinsiz açan, okuyan veya içeriğini üçüncü şahıslara açıklayan kişilere para cezası veya en fazla 1 yıl hapis cezası tatbiki öngörülmektedir[388].

Diğer yandan Finlandiya'da posta sektöründe kişisel verilerin korunması, GDPR ve Finlandiya'nın ulusal mevzuatı çerçevesinde düzenlenmektedir. 1 Ocak 2019'da

---

[386] Vincent, Huysmans, "6 of the Most Infamous Data Breaches in Belgian History", (2025).
[387] Finlandiya Anayasası, 1999.
[388] Finlandiya Ceza Kanunu, 1889.

yürürlüğe giren Finlandiya Veri Koruma Yasası *(Tietosuojalaki, 1050/2018)* ile kişisel verilerin korunmasına dair düzenlemelere yer verilmiştir[389]. Bu yasa, Finlandiya'da GDPR'nin uygulanmasını destekleyici ve belirli sektörlere özgü ek kurallar getirerek kişisel verilerin korunmasını ve bireylerin mahremiyetinin güvence altına alınmasını amaçlamaktadır.

Finlandiya Veri Koruma Yasası'nın 8 inci maddesinde ulusal denetim otoritesinin Veri Koruma Ombudsmanlığı olduğu, Ombudsmanın ise faaliyetlerinde özerk ve bağımsız bir sıfat taşıdığı belirtilmiştir. Ayrıca Veri Koruma Ombudsmanı tarafından 22 nci madde uyarınca idari para cezası verilebilmektedir[390].

Finlandiya Veri Koruma Yasası, veri koruma görevlileri için belirli yerel gereklilikler içermemektedir. Ancak bazı özel kanunlar, veri koruma görevlilerinin zorunlu olarak atanmasını şart koşmaktadır[391].

Finlandiya Veri Koruma Yasası'nda ilgili kişinin haklarına ve veri sorumlusunun aydınlatma yükümlülüğüne ilişkin hükümlere de yer verilmiştir. Genel nitelikli ve hassas verilerin işlenme şartları GDPR ile paralel olmakla birlikte bu işleme faaliyetlerine ek olarak, ulusal hareket alanı, ceza mahkumiyetleri ve suçlarla ilgili işleme ve ulusal kimlik numaralarının işlenmesiyle ilgili olarak da kullanılmıştır. Örneğin, Finlandiya Veri Koruma Yasası'nın 29 uncu maddesinde ulusal kimlik numaralarıyla ilgili olarak, işlemenin yalnızca veri sahibinin rızasına dayanması veya veri sahibinin yasada tanımlanan bir görevi, veri sahibinin veya veri sorumlusunun hak ve sorumluluklarının gerçekleştirilmesi veyahut tarihsel ya da bilimsel araştırma veya istatistiksel amacıyla işlenebileceği belirtilmiştir. Ayrıca, kredi, borç, sigorta, borç

---

[389] DLA Piper, "Data protection laws in Finland", (2023).
[390] Finlandiya Veri Koruma Yasası, 2019.
[391] Örneğin, Finlandiya'da sağlık hizmetleri ve sosyal refahın tüm işlevsel birimlerinin yanı sıra eczaneler, 2007/61 Sayılı Elektronik Reçeteler Yasası ve Sağlık ve Sosyal Refah Alanında Müşteri Verilerinin Elektronik İşlenmesi Yasası (159/2007) uyarınca bir veri koruma görevlisi atamak zorundadır (DLA Piper, "Data protection officers in Finland", 2023).

tahsilatı, ödeme hizmeti ve kiralama amaçları, sosyal veya sağlık hizmetlerinde ve istihdam ilişkileriyle bağlantılı olarak işlenebileceği hükme bağlanmıştır[392].

Finlandiya Veri Koruma Yasası'nın 5 inci maddesinde çocuklara ilişkin kişisel verilerin işlenmesine dair düzenleme, GDPR'daki genel hükümden farklılık göstermekte olup çocuğun 13 yaş ve üzerinde olması durumunda kişisel verilerinin işlenmesinin hukuka uygun olduğu kabul edilmiştir[393].

Finlandiya'da veri sorumluları, kişisel veri işleme faaliyetlerinde hukuka uygunluk, şeffaflık, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, doğruluk ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uymakla yükümlü kılınmıştır. Veri sahipleri ise bilgi edinme, erişim, kişisel verilerin düzeltilmesini isteme, unutulma, veri taşınabilirliği, itiraz, otomatik karar alma ve profillemeyle ilgili haklara sahiptir[394].

Finlandiya Veri Koruma Yasası, kişisel verilerin aktarılmasına ilişkin ek maddeler içermediği gibi GDPR'ın 32 inci maddesinde yer alan işleme güvenliği kapsamında alınacak tedbirler için de doğrudan ek gereklilikler ihtiva etmemektedir. Diğer yandan anılan düzenlemede, hassas verilerin işlenmesi durumunda alınacak güvenlik tedbirleri yer almaktadır. Bu önlemler çoğunlukla GDPR'ın 32 nci maddesinde yer alan örneğin; takma adla işlenmesi, şifreleme, personel eğitimi, erişim yönetimi, oturum açma veri kullanımı gibi tedbirlerle aynıdır.

Finlandiya'da genel veri ihlal bildirim prosedürü GDPR tarafından belirlenen kurallara uyumludur. Yani veri sorumlusu, ihlali, makul olmayan gecikme olmaksızın ve mümkünse, ihlalin farkına vardıktan sonra 72 saat içinde denetleyiciye bildirmelidir.

---

[392] Finlandiya Veri Koruma Yasası, 2019.
[393] GDPR'ın 8 inci maddesi uyarınca çocuğun en az 16 yaşında olması hâlinde kişisel verilerinin işlenmesi hukuka uygundur.
[394] Dünya Posta Birliği (UPU), *Country Name: Finland*.

Bu kapsamda kişisel veri ihlalleri, Veri Koruma Ombudsman Ofisi'ne bildirilmektedir. Ancak, belirli özel ulusal mevzuat hükümleri ihlal bildirimleri konusunda ek gereklilikler içermektedir. Örneğin; Elektronik Haberleşme Hizmetleri Yasası, telekomünikasyon operatörlerinin abonelerini, kullanıcılarını ve Finlandiya Ulaştırma ve İletişim Kurumunu (*TRAFICOM*), iletişim hizmetlerini engelleyen veya ciddi şekilde aksatan her türlü önemli bilgi güvenliği ihlali ya da tehdidi konusunda bilgilendirmelerini zorunlu kılmaktadır. Ayrıca aynı yasa kapsamında; alan adı kayıt kuruluşları, alan adı hizmetlerinde meydana gelen önemli bilgi güvenliği ihlalleri ile bu hizmetleri kayda değer ölçüde kesintiye uğratan ya da bozan durumlar hakkında TRAFICOM'u gecikmeksizin bilgilendirmekle yükümlüdür[395].

Diğer yandan Finlandiya'da posta hizmetleri, Finlandiya Posta Kanunu (*Postilaki*, 415/2011) ile düzenlenmektedir. Bu Kanun, PHS'lerin yükümlülükleri ile haberleşmenin gizliliğinin korunmasının zorunluluğuna ilişkin hükümler içermektedir[396].

Finlandiya Posta Kanunu'nun 55 inci maddesi uyarınca PHS'lerin mühürlü bir gönderiyi açma yetkisi bulunmamaktadır. Bununla birlikte PHS'ler posta gönderisinin;

- Hasarlı olması veya içeriğinin korunması veya durumunun doğrulanması için açılmasının gerekli olması,
- Can ve mal güvenliği açısından risk oluşturabileceğinden şüphelenilmesi için gerekli sebeplerin bulunması,
- Teslim edilememesi nedeniyle satılması ya da imha edilmesi amacıyla açılmasının gerekli olması

hallerinde gönderiyi açma yetkisine sahiptir. Anılan gönderiler, Finlandiya Ulaştırma ve İletişim Ajansı tarafından yetkilendirilmiş bir kişi tarafından, başka bir kişinin

[395] DLA Piper, "Breach notification in Finland", (2023).
[396] Finlandiya Posta Kanunu, 2011.

huzurunda açılabilmektedir. Bununla birlikte bir posta gönderisinin içeriği, gönderinin açılma nedeninin gerektirdiğinden daha detaylı bir şekilde incelenememekte olup açılan gönderinin üzerine Finlandiya Ulaştırma ve İletişim Ajansı'nın öngördüğü işaretlemelerin yapılması zorunludur. Gönderinin açıldığı sırada hazırda bulunan kişiler tarafından imzalanan bir tutanak düzenlenerek durumun anılan Ajans'a sunulması gerekmektedir. Finlandiya Posta Kanunu'nun 56 ncı maddesinde ise gönderilerin saklanması ve imhası düzenlenmiş olup imha işleminin gizliliğin korunacağı şekilde yapılması gerektiği hükme bağlanmıştır.

Öte yandan Finlandiya Posta Kanunu'nun 57 nci maddesinde Finlandiya Ulaştırma ve İletişim Ajansı'nda teslim edilemeyen gönderilerin işlenmesi düzenlenmiştir. Buna göre teslim edilemeyen bir gönderiyi işlerken anılan Ajans;

- Gönderinin teslimi için alıcının adresinin, geri gönderilmesi için göndericinin adresinin belirlenmesinin zorunlu olması,
- Gönderinin can veya mal açısından risk oluşturabileceği açık olması,
- Gönderinin içeriğinin, güvenlik nedeniyle daha fazla taşınmasını engellemesi

halinde mühürlü mektupları açma yetkisine sahiptir.

Bunun yanı sıra Finlandiya Posta Kanunu'nun 62 nci maddesinde *"gizli mesajların güvenliğinin korunmasına"* ilişkin düzenlemelere yer vermektedir. Buna göre PHS'ler, gönderilerin mahremiyetini korumakla yükümlüdür. Aynı yükümlülük, PHS'ler ile yaptığı sözleşme çerçevesinde posta gönderilerini işleyen veya posta şirketinin hizmetlerini müşterilere sunan kişiler için de geçerlidir.

Finlandiya Posta Kanunu'nun 63 üncü maddesinde ise "bilgilerin ifşasına" ilişkin düzenlemelere yer verilmektedir. Buna göre bir PHS personeli, görevi sırasında edindiği kullanıcı ya da kullanıcının işleriyle ilgili herhangi bir bilgiyi ifşa edememektedir. Gizlilik yükümlülüğü, PHS'nin anlaşma yapması sonucu bilgi sahibi olan herkes için geçerlidir.

Yukarıdaki hükümlerden görüleceği üzere, posta gönderilerinin gizliliği ve güvenliğine ilişkin esaslar Finlandiya Posta Kanunu'nda ayrıntılı bir şekilde düzenlenmiştir. Bu ayrıntılı hükümlerin gerekçesi olarak; ülkenin bazı bölgelerinde nüfus yoğunluğunun düşük olması ve bu nedenle mahremiyetin özellikle korunması gerekliliği, ayrıca herkesin resmi olarak bilinen bir adresinin olmaması ve bu nedenle mektupların muhataplarına tespit edilememesinin sıklıkla yaşanması gösterilmektedir. Bunun yanı sıra postaların nasıl ele alınacağı konusunda son sözü söyleyen kurum olan TRAFICOM, alıcısı tespit edilemeyen mektuplardan sorumlu olup mektubun imhasına karar vermeden önce doğru adresi tespit etmek için bütün imkânları tüketmek zorundadır[397].

Finlandiya posta sektöründe kişisel verilerin korunmasına ilişkin yükümlülüklerin ihlali vakasının mevcut olduğu bilinmektedir. Buna göre veri koruma mevzuatı gereğine aykırı bir biçimde kişisel verilerin şeffaf bir şekilde işlenmemesi nedeniyle, Finlandiya Veri Koruma Ombudsmanlığı'nın 18 Mayıs 2020 tarihli kararı ile Finlandiya'da evrensel PHS olan Posti'ye yaptırım uygulanmasına karar verilmiştir. Kararda, Finlandiya'da taşınan kişilerin Posti'ye adres değişikliği bildirimi yapması gerektiği, bu bildirimde, kişisel verilerin üçüncü taraflarla paylaşılmasını engelleme seçeneği bulunsa da Posti'nin bu seçenek hakkında açık ve yeterli bilgilendirme yapmadığı anlaşılarak soruşturma neticesinde 161.000 kişinin söz konusu veri ihlalinden etkilendiği tespit edilmiştir. Bu tespit neticesinde Finlandiya'da, bir veri ihlali nedeniyle ilk kez idari para cezası verilerek, Posti'ye 100.000 Euro idari para cezası uygulanmıştır[398].

Finlandiya Veri Koruma Ombudsmanlığı tarafından 13 Kasım 2024 tarihinde Posti'ye uygulanan bir başka yaptırım da, Posti'nin müşterilerinin kişisel verilerini onların rızası

---

[397] Cornelia, Berger, *Liberalisierung des Postmarktes in Europa Utl: Umsetzung der Europäischen Richtlinie auf nationaler und supranationaler Ebene und die Rolle der politischen Akteure*, (2012): 56-57.

[398] Ghalumyan, "Fine on Posti for violation…".

olmaksızın dijital bir posta kutusu oluşturmak için kullanması, müşterilerini dijital posta kutusu hakkında yeterince bilgilendirmemesi ve çevrimiçi uygulaması olan OmaPosti'nin bazı teknik ayarlarının veri koruma yükümlülüklerine uymamasına dayanmaktadır. Anılan yaptırım kararında Posti'nin kullanıcılarını, dijital posta kutusunun OmaPosti uygulamasıyla birlikte otomatik olarak etkinleştirileceği konusunda yeterince açık bir şekilde bilgilendirmediği, müşterilere, OmaPosti dijital posta kutusunu etkinleştirdikten sonra yalnızca kâğıt formunda mektup almayı seçebilecekleri konusunda yanlış bilgi verdiği belirtilerek Posti'nin, veri sahiplerine, verilerinin nasıl işleneceğini anlamalarını sağlayacak yeterli bilginin verilmesini zorunlu kılan GDPR'nin 13 üncü maddesinin birinci fıkrasının (c) bendini, bilgilerin açık ve anlaşılır bir şekilde sunulmasını gerektiren 12 nci maddesini, temin edilen bilgilerin şeffaf bir şekilde işlenmesini gerektiren 5 inci maddesinin birinci fıkrasının (a) bendini ve 25 inci maddesinin birinci fıkrasını ihlal ettiği belirtmiştir. Bahse konu ihlal neticesinde Posti'ye 2,4 milyon Euro para cezası uygulanmıştır[399].

4.1.2 Birleşik Krallık

Birleşik Krallık'ta verilerin korunmasına yönelik müstakil bir Kanun olan Veri Koruma Kanunu esasen 1988'de yürürlüğe girmiş, bununla birlikte 1998'de güncellenmiş ve ardından 25 Mayıs 2018'de "2018 Veri Koruma Kanunu" (*Data Protection Act 2018*) olarak son halini almıştır. Anılan Kanun hem İngiltere'nin AB'den ayrılması öncesi hem de sonrasında İngiltere'de AB hukukunun gerekliliklerinin ülke düzeyinde karşılanmasını sağlamayı amaçlamaktadır[400].

Söz konusu Kanun genel bir mevzuat olup posta sektöründe de bu Kanun hükümleri uygulanmaktadır. Mezkûr Kanun'a göre veri sorumluları; kişisel veri işleme

---

[399] Finlandiya Veri Koruma Ombudsmanlığı, "Elektronik posta kutusu ve hizmetin etkinleştirilmesine ilişkin bilgilendirme amacıyla sözleşmeye dayalı kişisel verilerin işlenmesi", (2024).
[400] Paul F, Scott, *National Security, Data Protection, and Data Sharing after the Data Protection Act 2018*, (2019).

faaliyetlerinde hukuka uygunluk, şeffaflık, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, doğruluk ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkelerine uymakla yükümlüdür. Veri sahipleri ise bilgi edinme, erişim, kişisel verilerin düzeltilmesini isteme, unutulma, veri taşınabilirliği, itiraz, otomatik karar alma ve profillemeyle ilgili haklara sahiptir. Görüleceği üzere 2018 Veri Koruma Kanunu, veri koruma ve gizlilik yönetimi konusunda GDPR'a benzer ilkelere dayanmaktadır. Bununla birlikte aşağıda bazı önemli farklara da değinilmektedir:

Öncelikle 2018 Veri Koruma Kanunu'nun 21 nci maddesi, ulusal güvenliği veya savunma amaçlarını korumak ya da bilgi edinme mevzuatıyla belirlenmiş belirli devlet kurumları tarafından tutulan yapılandırılmamış manuel verilerle ilgili durumlarda, Birleşik Krallık GDPR (*United Kingdom General Data Protection Regulation*, UK GDPR)'ın uygulanmasına istisna getirmektedir. Söz konusu Kanun, kuruluşların, özel veri kategorilerinin işlenmesiyle ilgili uygun politika belgeleri tutmasını zorunlu kılmaktadır. Bu belgeler, veri sorumlusunun veri koruma ilkelerine nasıl uyduğunu ve bu tür verilerin nasıl saklanıp silindiğini açıklamaktadır. Belirli durumlarda kuruluşların, veri sahiplerinin erişim taleplerini reddetmesine olanak tanıyan istisnalar içermektedir[401]. Ayrıca anılan Kanun'un 9 uncu maddesinde çocukların verilerinin işlenmesi için asgari rıza yaşı 13 olarak belirlenmiştir.

Öte yandan UK GDPR, Birleşik Krallık'ın Genel Veri Koruma Tüzüğüdür[402]. 1 Ocak 2021'de yürürlüğe giren UK GDPR, AB'den ayrılması nedeniyle Birleşik Krallık'a uygulanan bir veri koruma düzenlemesi olup AB'nin GDPR düzenlemesi temel alınarak oluşturulmuştur[403]. Ancak mezkûr düzenlemede Birleşik Krallık'ın kendi yasal düzenlemelerine uyacak şekilde bazı farklılıklar bulunmaktadır. Örneğin UK GDPR, 9

[401] DLA Piper, "Collection and Processing the United Kingdom", (2025).
[402] Birleşik Krallık Genel Veri Koruma Tüzüğü, 2021.
[403] Halawi, Leila ve Makwana, Alpesh, "The GDPR and UK GDPR and its impact on US academic institutions", *Issues in Information Systems*, Cilt: 24, Sayı: 2, (2023): 235.

uncu maddesinde hassas verilerin ve 10 uncu maddesinde ise ceza mahkumiyetleri ve suçlara ilişkin kişisel verilerin işlenmesine ilişkin daha kısıtlayıcı kurallar belirlemektedir[404].

2018 Veri Koruma Kanunu'nun 51 inci maddesi uyarınca İngiltere Veri Koruma Kurumu (*Information Commissioner's Office*, ICO) Birleşik Krallık'ın denetim otoritesidir. ICO, belirli durumlarda ve/veya sektörlerde veri işleme konusunda uyumluluğun sağlanmasına yardımcı olacak uygulamaya yönelik kurallar hazırlamaktadır. Bu kurallar, kuruluşlara veri koruma düzenlemeleriyle nasıl uyumlu kalacakları konusunda rehberlik etmektedir[405]. UK GDPR'a göre, her veri sorumlusu veya işleyenin, kamusal bir otorite olması, temel faaliyetlerinin, nitelikleri, kapsamları veya amaçları gereği, veri sahiplerinin büyük ölçekte düzenli ve sistemli bir şekilde izlenmesini gerektiren işleme operasyonlarından oluşması veya temel faaliyetlerinin büyük ölçekte hassas verilerin işlenmesi şeklinde olması halinde bir veri koruma görevlisinin atanması gerekmektedir.

UK GDPR'ın 44 üncü maddesine göre, kişisel verilerin üçüncü ülkelere aktarımı yalnızca belirli şartların karşılanması halinde mümkündür. Birleşik Krallık Hükümeti bu Kanun'un 45 inci maddesi uyarınca üçüncü ülkeler hakkında yeterlilik kararı verme yetkisine sahiptir. Bu karar, ilgili ülkenin veri koruma konusundaki yeterliliğini onaylayarak kişisel verilerin serbestçe aktarılmasını sağlamaktadır. Aynı düzenlemenin 46 ncı maddesinde ise yeterlilik kararının bulunmadığı durumlarda, uygun güvenceler ve veri sahiplerine etkin haklar sağlanması koşuluyla veri transferine izin verilmektedir. Bu güvenceler arasında bağlayıcı şirket kuralları ve standart sözleşme maddeleri yer almaktadır.

---

[404] Birleşik Krallık Genel Veri Koruma Tüzüğü, 2021.

[405] Annie, Greenley-Giudici, "What's the Difference Between UK Data Protection Act & GDPR?", TrustArc.

AB açısından, Birleşik Krallık artık üçüncü ülke statüsünde olup AB Komisyonu 28 Haziran 2021'de Birleşik Krallık'a ilişkin yeterlilik kararları vererek veri aktarımının AB'den Birleşik Krallık'a serbestçe yapılmasını mümkün kılmıştır. Bununla birlikte söz konusu karar 2025 yılının Mart ayında Avrupa Komisyonu tarafından tekrar değerlendirilmiş olup Komisyon, Birleşik Krallık'a ücretsiz ve güvenli veri akışları için yeterlilik kararlarının altı ay uzatılmasını önermiştir. Bu uzatma ile Birleşik Krallık ile verilerin serbest akışının 27 Aralık 2025'e kadar sürdürüleceği belirtilmiştir[406].

UK GDPR'ın 32 nci maddesi, veri sorumlusu ve işleyenlerin veri işleme faaliyetleri kapsamında uygun güvenlik seviyesini sağlama amacıyla gerekli teknik ve organizasyonel önlemleri uygulayacaklarını belirtmektedir. İlgili madde uyarınca veri sorumlusu ve veri işleyenler, yeterli güvenliğin sağlanıp sağlanmadığını değerlendirirken;

- kişisel verilerin takma adla işlenmesi ve şifrelenmesi,
- işleme sistemlerinin ve hizmetlerinin sürekli gizliliğini, bütünlüğünü, kullanılabilirliğini ve dayanıklılığını sağlama yeteneği,
- fiziksel veya teknik bir olay durumunda kişisel verilere erişimin ve kullanılabilirliğin zamanında geri yüklenmesi yeteneği,
- işlemenin güvenliğinin sağlanması için teknik ve organizasyonel tedbirlerin etkinliğinin düzenli olarak test edilmesi, değerlendirilmesi ve ölçülmesine yönelik bir sürece ilişkin

hususları dikkate almalıdır[407].

UK GDPR'a göre veri sorumlusu, veri ihlali olması halinde, makul olmayan gecikme olmaksızın ve mümkünse, ihlalin farkına varıldıktan sonra 72 saat içinde ICO'ya bildirimde bulunmalıdır. Ayrıca veri sorumlusu, ihlalin gerçek kişilerin hakları ve

[406] Avrupa Komisyonu, "Daily News 18/03/2025", (2025).
[407] Birleşik Krallık Genel Veri Koruma Tüzüğü, 2021.

özgürlükleri için risk oluşturduğunu tespit ederse veri sahibine ayrıca bildirimde bulunmalıdır. İlgili düzenlemenin 33 üncü maddesine göre ise ICO'ya yapılacak bildirimde; mümkün olduğu takdirde ilgili kişilerin ve kayıtların kategorileri ve yaklaşık sayıları, kuruluşun veri koruma görevlisinin veya diğer irtibat kişisinin adı, ihlalin muhtemel sonuçları ve zararı azaltmak amacıyla alınan önlemler yer almalıdır.

Diğer yandan Birleşik Krallık'ın posta sektörüne ilişkin temel düzenlemelerin yer aldığı 2011 tarihli Posta Hizmetleri Kanunu'nda kişisel verilerin korunmasına yönelik doğrudan bir hüküm bulunmamaktadır. Bununla birlikte Kanun'un 49 uncu maddesinde Birleşik Krallık Haberleşme Otoritesi (*Office of Communications*, OFCOM)'nin, posta gönderilerinin taşınması ve teslimi esnasında gizliliğinin korunması ile iletilen bilgilerin gizliliğinin korunması hususuna riayet edilmesi için hizmet sağlayıcılarına belirli yükümlülükler getirebileceği düzenlenmiştir[408].

Birleşik Krallık'ta yürürlükte bulunan sıkı düzenlemelere rağmen, zaman zaman PHS'lerin siber saldırılarla karşılaştığı ve sonucunda kişisel veri ihlallerinin yaşandığı görülmektedir. Örneğin; İngiltere'de 2023'ün başlarında, fidye yazılımı grubu olan LockBit, İngiltere'de PHS olan Royal Mail verileri açısından veri ihlaline sebep olarak 80 milyon dolarlık fidye talep etmiştir.

Yine Mart 2025'te, Royal Mail ile ilişkili olduğu iddia edilen bir başka veri ihlali kamuoyuna yansımıştır. Saldırıya ilişkin olarak paylaşılan duyuruda saldırganlar; kullanıcıların kimlik bilgileri, adresleri ve gizli belgeler gibi yaklaşık 144 GB'lık kişisel veriyi ele geçirdiklerini iddia etmiştir. Royal Mail ise doğrudan sistemlerinin etkilenmediğini, bununla birlikte bir tedarikçilerinin saldırıya uğramış olabileceğini kamuoyu ile paylaşmıştır[409].

---

[408] Birleşik Krallık Haberleşme Otoritesi (Ofcom), "Conditions imposed on postal operators", (2024).
[409] Vilius, Petkauskas, "Royal Mail customer data stolen in massive attack, hackers claim", Cybernews, (2025).

Son olarak, İngiltere'de bir PHS olan Post Office, bir muhasebe yazılımında meydana gelen hata nedeniyle, yüzlerce PHS yöneticisinin zimmet iddiasıyla yargılanmasına sebep olmuştur. Bu süreçte, aynı zamanda söz konusu kişilerin kimlik ve adres bilgileri kurumun resmî internet sitesinde yayımlanmış olduğundan hem yaşanan mağduriyetler hem de veri ifşası nedenleriyle Post Office, ilgili kişilere tazminat ödemeyi kabul etmiştir[410].

4.1.3 Amerika Birleşik Devletleri

ABD'de posta gizliliği ve güvenliği, çeşitli yasal düzenlemelerle güvence altına alınmıştır. Bu düzenlemeler de diğer ülkeler ile benzer şekilde, bireylerin özel yazışmalarının korunmasını ve yetkisiz erişimlerin önlenmesini amaçlamaktadır.

Amerikan hukukunda posta gönderilerinin içerik ve trafik bilgilerinin gizliliği anayasal düzeyde korunmaktadır. Nitekim ABD Anayasası'nın Dördüncü Değişikliği (*Fourth Amendment*), kişilerin özel hayatına ve haberleşmesine yönelik makul olmayan arama ve el koymalara karşı koruma sağlamakta olup mahkeme kararı olmaksızın posta gönderilerine el konulmasını ya da içeriğinin incelenmesini yasaklamıştır[411]. Bu kapsamda ABD Yüksek Mahkemesi'nin 1878 yılında verdiği "Ex parte Jackson" kararında mühürlü mektupların dördüncü değişiklik kapsamında korunduğu açıkça belirtilmiştir[412].

Ayrıca posta yoluyla gönderilen gönderilerin gizliliğini doğrudan koruyan ve ihlali hâlinde cezai yaptırımlar öngören federal ceza hükümleri mevcuttur. 18 U.S. Code olarak ifade edilen Ceza Kanunu'nda başkasına ait bir mektubun veya postanın yetkisiz biçimde açılması, alıkonulması veya yok edilmesi federal suç olarak

---

[410] The Guardian, "Post Office data leak: hundreds of Horizon victims offered up to £5,000 compensation", (2025).
[411] Amerika Birleşik Devletleri (ABD) Anayasası.
[412] Amerika Birleşik Devletleri (ABD) Yüksek Mahkemesi Kararı, 1878 tarihli Ex parte Jackson Kararı.

düzenlenmiştir. Bu maddeye göre, herhangi bir kişinin posta gönderisini yetkisi olmadan alması veya engellemesi halinde para cezası ya da hapis cezası uygulanabilecektir[413].

Diğer yandan bu ülkedeki veri gizliliği konusundaki ilk yasal gelişme, 1966 yılında bilgiye erişim hakkını düzenleyen Bilgi Özgürlüğü Kanunu (*Freedom of Information Act*) ile başlamıştır. Bu yasa, kamuya ait bilgilerin şeffaf bir şekilde vatandaşlara sunulmasını öngörerek bilgi özgürlüğünü yasal güvence altına almıştır. Bunu takiben, 1974 yılında kabul edilen ABD Gizlilik Kanunu (*Privacy Act*), devlet kurumlarının bireylere ait kişisel verileri nasıl toplayıp işleyeceğine ilişkin kapsamlı kurallar getirmiştir. ABD Gizlilik Kanunu, kamu kurumlarının kişisel veri toplama ve kullanma süreçlerinde kişi haklarını koruma amacını taşımaktadır. PHS'ler tarafından işlenen veriler de bu kanun kapsamında korunmaktadır. Bununla birlikte bu düzenlemeler bugünkü anlamda kapsamlı ve merkezi bir veri koruma yapısı sunmamakta olup ABD halihazırda GDPR gibi temel bir düzenlemeye sahip değildir[414].

Diğer yandan ABD'de henüz yürürlüğe girmemiş olmakla birlikte, genel bir veri koruma rejimi kurulmasına ilişkin 2022 tarihli Amerikan Veri Gizliliği ve Koruma (*American Data Privacy and Protection Act*) Yasa tasarısı mevcuttur. Bu tasarı, posta hizmetleri de dâhil olmak üzere bütün sektörlerde kişisel verilerin işlenmesi ve korunmasına dair temel ilkeleri ortaya koymaktadır. Taslak yasa uyarınca PHS'ler; kişisel veri işleme faaliyetlerinde şeffaflık, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkelerine uymakla yükümlüdür. Veri sahipleri ise erişim, unutulma, veri taşınabilirliği haklarına sahiptir[415]. Bunun yanı sıra PHS'lerin kullanıcı bilgilerine ilişkin olarak başta adres doğrulama ve teslimatın doğru şekilde yapılabilmesi gibi amaçlarla sınırlı veri aktarımı yapabileceği hüküm

---

[413] Amerika Birleşik Devletleri (ABD) Ceza Kanunu, 1994.
[414] Sayan, *Karşılaştırmalı Hukukta Elektronik…,* 127-128; Amerika Birleşik Devletleri (ABD) Posta Hizmetleri, *Gizlilik Politikası*.
[415] Dünya Posta Birliği (UPU), *Country Name: United States of America.*

altına alınmıştır. Ayrıca, kullanıcıların rızaları olmadıkça, reklam, analiz veya profilleme amacıyla veri kullanımı yasaklanmakta olup bununla, posta üzerinden sağlanan hizmetlerin veri güvenliği açısından özel bir koruma rejimi oluşturulması öngörülmektedir[416].

Federal Düzenlemeler Yasası (*Code of Federal Regulations*) ise ABD'deki tüm federal düzenlemelerin resmi derlemesidir[417]. 50 başlık altında oluşan bu yasada, her başlık altında farklı bir konuya odaklanılmaktadır[418]. Anılan Yasanın 39 uncu başlığı altında yer alan 266 ncı Bölüm'de *"Bilgilerin Gizliliği (PART 266—Privacy of Information)"* düzenlenmektedir. Bu düzenleme, ABD Posta Servisi (*US Postal Service*, USPS) ile ilgilidir[419].

USPS, 1974 tarihli Gizlilik Yasası kapsamında bireylerin kişisel bilgilerinin toplanması, kullanımı, saklanması ve ifşa edilmesiyle ilgili sıkı kurallara uymakla yükümlüdür. Bu düzenleme, USPS'nin sahip olduğu kayıt sistemlerinde yer alan ve bireylerin adı ya da kişisel verileri ile ilişkilendirilebilecek tüm bilgileri kapsamaktadır. Bu kapsamda bireyler, USPS tarafından tutulan kayıt sistemlerinde kendi bilgilerine erişme, bunları inceleme, kopyalama, hatalı bilgileri düzeltme ve bu bilgilerin kime ve ne şekilde ifşa edildiğinin kaydını talep etme haklarına sahiptir[420].

USPS, yalnızca kanun veya yürütme emriyle yetkilendirilmiş durumlarda bireyler hakkında bilgi toplayabilir. Bilgiler mümkün olan en geniş ölçüde doğrudan bireyden alınmalıdır. Bilgi talep edilirken, kişinin bu bilgileri vermek zorunda olup olmadığı, hangi yetkiyle istendiği, nasıl kullanılacağı ve bilgi verilmemesinin muhtemel sonuçları açıkça belirtilmelidir. Ayrıca USPS, bireylerin ifade özgürlüğü gibi anayasal haklarını

---

[416] Amerikan Veri Gizliliği ve Koruma Yasası (ADPPA), 2022.
[417] University of Michigan Law Library, "Federal Regulations: FR vs CFR", (2024).
[418] Richard J., McKinney, *A Research Guide to the Federal Register and the Code of Federal Regulations*, (2016).
[419] Amerika Birleşik Devletleri (ABD) Federal Düzenlemeler Yasası (CFR), 2017.
[420] Amerika Birleşik Devletleri (ABD) Posta Hizmetleri, *Guide to Privacy, the Freedom of Information Act, and Records Management*, (2025).

kullanmalarıyla ilgili kayıt tutamaz ve sosyal güvenlik numarası gibi hassas bilgiler ancak federal yasa gerektiriyorsa talep edilebilir. Düzenlemenin 266.3 bölümünde "*Bireyler hakkında bilginin toplanması ve açıklanması"*na yer verilmiştir. Kişisel bilgilerin ifşası yalnızca belirli koşullar altında mümkün olup bunlardan biri veriyi talep eden kişinin, veri sahibinden önceden yazılı onay almasıdır. Bununla birlikte bu kişisel verilerin "posta hizmetleri görevlerinin yerine getirilmesinde bu tür bilgilere ihtiyaç duyan PHS çalışanları veya PHS'nin alt yüklenicisinin çalışanlarına açıklanmasında" olduğu gibi bazı istisnai durumlarda da açıklanabilmesi mümkündür. Kayıt sistemlerinde yapılan her açıklama ise düzenli şekilde belgelenerek en az beş yıl süreyle saklanmakta, elde edilen verilerin doğruluğu, güncelliği ve ilgili olup olmadığı sürekli denetlenmektedir. Değişiklik talepleri ise yazılı olarak yapılmalı ve makul süre içinde yanıtlanmalıdır. Kayıtların düzeltilmemesi durumunda, bireye itiraz etme ve kayıtlara itiraz açıklaması ekletme hakkı tanınmaktadır[421].

Bununla birlikte ABD posta sektöründe bazı veri ihlallerinin yaşandığı bilinmekte olup bazılarına aşağıda yer verilmektedir:

2018 yılında yaşanan bir veri ihlalinde, USPS internet sitesinin uygulama programlama ara yüzünden kaynaklanan bir hata nedeniyle; telefon numaraları, sokak adresleri, kullanıcı adları ve telefon numaraları gibi bazı kişisel verilere erişilmesine sebep olunmuştur[422].

Mart 2024'te yayımlanan bir habere göre ise USPS, çevrim içi hizmet kullanıcılarının posta adresleri dâhil bazı kişisel verilerini, farkında olmadan Meta, LinkedIn ve Snap gibi üçüncü taraflarla paylaşmıştır. Bu veri aktarımının, USPS internet sitesine yerleştirilen ve kullanıcı davranışlarını izlemeye yarayan izleme pikselleri aracılığıyla gerçekleştiği belirtilmiştir. Bu durum, izinsiz veri paylaşımı ve kişisel verilerin üçüncü

[421] Amerika Birleşik Devletleri (ABD) Federal Düzenlemeler Yasası (CFR), 2017.
[422] Annie, Palmer, "US Postal Service admits a 'catastrophic' flaw in its system exposed exactly what mail 60 million users were getting delivered", DailyMail, (2018).

taraflarla rıza dışında aktarımı açısından ciddi bir veri ihlali olarak değerlendirilmiştir[423].

4.1.4 Çin Halk Cumhuriyeti

1954 yılında kabul edilen ve değişikliğe uğrayarak son halini 2018 yılında alan Çin Halk Cumhuriyeti Anayasası devletin temel yapısı, vatandaşların hak ve yükümlülükleri gibi hükümler içerirken posta sektöründe kişisel verilerin korunmasını ele alan bir madde içermemektedir[424].

Öte yandan, Çin Kişisel Bilgilerin Korunması Kanunu (*Personal Information Protection Law of the People's Republic of China*)[425] ve Veri Güvenliği Kanunu (*Data Security Law*) 2021 yılında yürürlüğe girmiş[426] olup bu kanunlar ile kişisel veriler üzerindeki hak ve menfaatlerin korunması, kişisel veri işleme faaliyetlerinin düzenlenmesi ve kişisel verilerin makul şekilde kullanılmasının teşvik edilmesi amaçlanmıştır.

Çin KVKK'sinin 4 üncü maddesi uyarınca kişisel veri; kimliği belirli yahut belirlenebilir bir gerçek kişiye dair, elektronik ortamda veya diğer yollarla kaydedilen çeşitli bilgileri ifade etmektedir. Anılan Kanun tüm "kişisel veri sorumlularını" kapsamakta olup bu kapsama kamu kurumları ve şirketler de dahil edilmiştir. Kanun, Çin sınırları içinde bulunan gerçek kişilere ait kişisel verilerin işlenmesine uygulanmaktadır. Bununla birlikte Kanun'un 3 üncü maddesi uyarınca ülke içindeki gerçek kişilere ürün veya hizmet sağlama amacıyla, ülke sınırları içindeki gerçek kişilerin davranışlarının analiz edilmesi veya değerlendirilmesi veya herhangi bir kanun ya da idari düzenlemede öngörülen diğer bir durumun varlığı halinde, ülke sınırları içerisinde bulunan gerçek

---

[423] Zack, Whittaker, "USPS shared customer postal addresses with Meta, LinkedIn and Snap", TechCrunch, (2024).
[424] Çin Halk Cumhuriyeti Anayasası, 2018.
[425] Çin Halk Cumhuriyeti Kişisel Bilgilerin Korunması Kanunu (PIPL), 2021.
[426] Rogier, Creemers, "China's emerging data protection framework", *Journal of Cybersecurity*, Cilt: 8, Sayı: 1, (2022): 1.

kişilere ait kişisel bilgilerin ülke sınırları dışında işlenmesinde de söz konusu Kanun uygulanmaktadır.

Anılan Kanun'un 5 inci maddesine göre kişisel verilerin işlenmesi, hukuka uygun olarak, gerekli olduğu takdirde, haklı bir nedenle ve iyi niyetle işlenebilmektedir. Öte yandan kişisel verilerin işlenmesi Kanun'un 6 ncı maddesine göre açık ve makul amaçlara dayanmalı ve bu amaçlarla doğrudan ilişkili olmalı, kişilerin hak ve menfaatleri üzerinde asgari etkiyi yaratmalı ayrıca işleme amacının gerektirdiği asgari kapsamla sınırlı olarak ve aşırı miktarda kişisel veri toplanmasına izin vermeyecek nitelikte olmalıdır. Kanun'un 7 nci maddesine uyarınca ise işleme faaliyetinde açıklık ve şeffaflık ilkeleri gözetilerek kişisel verilerin işlenmesine ilişkin kuralların açıklanmasıyla işleme amaçları, araçları ve kapsamı açıkça belirtilmektedir.

Çin KVKK'sinin 13 üncü maddesinde kişisel verilerin işlenme şartları da düzenlenmiştir. Buna göre kişisel verilerin işlenmesi için bireylerin açık rızası aranmaktadır. Bu rıza gönüllü, açık ve tam bilgilendirilmeye dayalı olmalıdır. Kişisel veriler, bireyin açık rızası olmadan üçüncü taraflarla paylaşılamamakta ancak sözleşme gereklilikleri, yasal yükümlülükler veya kamu sağlığı gibi durumlarda rıza aranmaksızın verilerin işlenmesine izin verilebilmektedir. Ayrıca kişisel veriler habercilik ve kamu yararına yürütülen diğer faaliyetler ile bireylerin kendisi tarafından açıklanan veya bireylerin yasal olarak açıklanan kişisel verileri Kanuna uygun olarak makul şekilde işlenebilmektedir. Bireyler, verilerinin ne şekilde işlendiği konusunda bilgilendirilme hakkına sahip olup verdikleri bu rızayı geri alma hakkına da sahiptir. Kanun ve diğer düzenlemelerde aksi öngörülmedikçe, kişisel verilerin saklanma süresi, işlenme amacının gerçekleştirilmesi için gerekli olan asgari süre kadardır.

Çin KVKK'sinin 2 nci bölümünde hassas veriler de düzenlenmiş olup hassas verilerin işlenmesinde kişinin ayrıca rızasının arandığı belirtilmiştir. İlaveten bu Kanun hükümlerine göre zorunlu olmadıkça, ilgili kişiye hassas kişisel verilerinin işlenmesinin

gerekliliği ve bunun hak ve menfaatleri üzerindeki etkisi konusunda bilgi verme yükümlülüğü getirilmiştir.

Çin KVKK'sinde kişisel verilerin yurt dışına aktarımına dair düzenlemelere de yer verilmiştir. Kanun'un 41 inci maddesi kapsamında Çin yetkili makamları, Çin sınırları içinde saklanan kişisel bilgilere ilişkin yabancı yargı veya kolluk kuvvetlerinin taleplerini, ilgili yasalara ve Çin tarafından imzalanan veya katılım sağlanan uluslararası antlaşma ve sözleşmelere uygun olarak veya eşitlik ve karşılıklılık ilkesi uyarınca ele almaktadır. Çin yetkili makamlarının onayı olmaksızın hiçbir kuruluş veya birey, Çin topraklarında saklanan verileri herhangi bir yabancı yargı veya kolluk kuvvetine sağlayamamaktadır.

Diğer yandan Çin KVKK'sinin 4 üncü bölümünde kişisel veri işleme faaliyetinde bireylerin hakları, 5 inci bölümünde ise veri işleyenlerin yükümlülükleri düzenlenmiştir. Ayrıca kişisel verilerin korumasının genel planlaması ve koordinasyonu ile ilgili denetim ve idareden "Ulusal Siber Uzay Dairesi"nin sorumlu olacağı hükme bağlanmıştır. Kanunda ayrıca ihlale sebebiyet verenler hakkında uygulanacak yaptırımlara da yer verilmiştir[427].

Çin Halk Cumhuriyeti Posta Kanunu (*Postal Law of the People's Republic of China*)[428] ise posta yazışmalarının ve bilgilerinin güvenliğinin sağlanması, haberleşme özgürlüğü ve gizliliğinin korunmasını amaçlamaktadır. Kanun'un 3 üncü maddesi uyarınca vatandaşların haberleşme hürriyeti ve gizliliği kanun ile korunur. Hiçbir kurum veya kişi, herhangi bir gerekçeyle vatandaşların haberleşme özgürlüğüne ve gizliliğine müdahale edemez. Ancak, ulusal güvenliğin korunması veya suç soruşturmalarının yürütülmesi amacıyla; kamu güvenliği organları, ulusal güvenlik organları veya savcılık organları, kanunda belirtilen usuller çerçevesinde vatandaşların yazışmalarını

[427] Çin Halk Cumhuriyeti Kişisel Bilgilerin Korunması Kanunu (PIPL), 2021.
[428] Çin Halk Cumhuriyeti Posta Kanunu, 2009.

inceleyebilir. Ayrıca Kanun tarafından aksi belirtilmedikçe, hiçbir kurum veya kişi, posta gönderilerini veya havaleleri inceleyemez ya da alıkoyamaz. Bu kapsamda 7 inci madde uyarınca posta idare birimleri, kamu güvenliği organları, ulusal güvenlik organları ve gümrük birimlerinin birbirleriyle iş birliği yaparak etkili bir güvenlik koruma mekanizması kurma ve posta aracılığıyla haberleşme ile bilgilerin güvenliğini sağlamak amacıyla bu alanlarda güvenlik denetimi ve yönetimini güçlendirme yükümlülüğü bulunmaktadır.

4.2 Türkiye'deki Mevcut Durum

Bu bölümde, Türkiye posta sektörünün kişisel veriler odağında incelenmesi hedeflenmektedir. Bunun için öncelikle, daha önce çeşitli bölümlerde yeri geldikçe değinilmekle birlikte, Türkiye'de faaliyet gösteren PHS'lerin kişisel verilerin gizliliği ve güvenliğine ilişkin uymakla yükümlü oldukları genel ve posta sektörüne özgü düzenlemeleri içeren Türkiye kişisel veri mevzuatı ortaya konulmaya çalışılacaktır. Devamında ise Türkiye posta sektörüne ilişkin bazı güncel bilgilere özet bir biçimde yer verilerek ilgili pazarda üretilen veri kapasitesi hakkında bir fikir verilmesi amaçlanmaktadır. Bu bölümde ayrıca, Türkiye'de faaliyet gösteren bazı PHS'lere işbu tez kapsamında gönderilen sualnamenin sonuçları değerlendirilecektir. Son olarak, Türkiye'de gerçekleşen bazı kişisel veri ihlallerine değinilecektir.

Türkiye'de kişisel verilerin korunmasına ilişkin düzenlemeler T.C. Anayasası, çeşitli kanunlar ve diğer ikincil mevzuatta yer almaktadır. Anayasal hükümler, kişisel verilerin korunmasını temel bir kişi hakkı olarak konumlandırırken; bu hakkın kapsamı, nasıl kullanılabileceği ve sınırlandırılabileceği, ilgili temel kavramların neler olduğu ve bu hakkın ihlali halinde ne gibi tedbirlerin alınabileceği ise kanuni düzenlemelerin konusu olmaktadır. Bu düzenlemelerin her biri, kişilik haklarıyla bağlantılı olarak, kişisel verilerin korunmasının bütüncül bir şekilde sağlanmasına hizmet etmektedir.

Türkiye'de 2010 yılında yapılan referandum neticesinde, 5982 sayılı T.C. Anayasasında Değişiklik Yapılmasına Dair Kanunla, 1982 tarihli T.C. Anayasası'nın 20 nci maddesinin üçüncü fıkrasına; *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* hükmü eklenerek "özel hayatın gizliliği ve korunması hakkı" kapsamında kişisel veriler açık bir hüküm ile Anayasal güvence altına alınmıştır. Bu hukuki gelişme AB'nin "Türkiye 2010 Yılı İlerleme Raporu"nda kişisel verilerin korunması ile bilgiye erişim hususlarında kaydedilen önemli bir ilerleme olarak kabul görmüştür[429].

Kişisel verilerin korunması hakkının anayasal bir hak olarak kabulü büyük bir önem taşımakla birlikte, bu hakkın etkin bir biçimde korunabilmesi için ceza hukukunun da müdahalesi kaçınılmazdır. Bu doğrultuda değinilmesi gereken ceza hukuku düzenlemesi, söz konusu Anayasal hükmün öncesinde kabul edilerek 01.06.2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu (TCK)'nda kişisel verilerin korunmasını amaçlayan suç tiplerine yer verilmesine ilişkin kanun hükümleridir[430].

Buna göre TCK'nin 135 inci maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu, 136 ncı maddesinde verileri hukuka aykırı bir biçimde verilmesi veya ele geçirilmesi suçu ve 138 inci maddesinde ise yasalar tarafından belirlenen sürelerin geçmesine rağmen verilerin sistem içerisinde yok edilmemesi suçları düzenlenmiştir[431]. Bu hükümler, ülkemiz ceza hukuku açısından önemli bir boşluğu doldurmuştur. Bilişim suçları bağlamında ise kişisel verilere ilişkin suç tiplerinin

---

[429] Avrupa Komisyonu. Türkiye 2010 Yılı İlerleme Raporu. 2011.
[430] Koca ve Üzülmez, "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)": 73.
[431] Ömer, Ekmekçi, Nafiye, Yücedağ, Elif Beyza, Akkanat-Öztürk ve Şehriban İpek, Aşıkoğlu, *Kişisel Verilerin Korunması Hukuku*, İstanbul Üniversitesi Hukuk Fakültesi Ders Kitapları Dizisi, (İstanbul: On İki Levha Yayıncılık, 2024): 7.

“bilişim alanında suçlar” başlıklı bölümde değil, korunan hukuksal değere göre benzer hukuksal değerlerin yer aldığı “özel hayata ve hayatın gizli alanına karşı suçlar” bölümünde yer alması, düzenlemenin olumlu yönlerinden biri olarak görülmektedir[432].

Diğer yandan 5271 sayılı Ceza Muhakemesi Kanunu (CMK)’nun *“Postada elkoyma”* başlıklı 129 uncu maddesine göre; bir suçun delili olduğundan şüphe edilen ve hakikatin ortaya çıkarılması için soruşturma ve kovuşturma aşamasında incelenmesi gerekli olan posta gönderilerine, hâkimin veya gecikmesinde sakınca bulunan durumlarda Cumhuriyet savcısının kararı ile el konulabilmektedir. Ancak hâkim kararı veya Cumhuriyet savcısı emrinin taraflara bildirilmesi sonucu el koyma işlemini yerine getiren kolluk memurları, gönderinin içerisinde bulunduğu zarf veya paketleri doğrudan açamamaktadır. El konulan gönderiler, ilgili posta görevlilerinin huzurunda önce mühür altına alınmakta ve derhâl el koyma kararını veya emrini veren hâkim veya Cumhuriyet savcısına teslim edilmektedir. Bununla birlikte Kanun’da belirtilen belirli suçlara[433] ilişkin bu kararın verilmesi halinde gönderilerin bulunduğu zarf veya paketler Cumhuriyet Savcısının talimatı ile kolluk memurları tarafından da açılabilmektedir. Bununla birlikte, açılmamasına ya da açılıp da içeriği açısından yargı mercilerinin elinde bulunmasına gerek olmadığına kanaat getirilen gönderiler hemen ilgililerine teslim edilmektedir. CMK’de yer alan söz konusu düzenleme, posta sektöründe kişisel verilere yönelik önemli bir koruma hükmüdür.

Adalet Bakanlığı 2024 yılı adli istatistiklerine göre TCK kapsamında, Cumhuriyet Başsavcılıklarında kişisel verilerin korunmasına dair dosya sayısında bir önceki yıla göre artış yaşandığı görülmektedir. Bu kapsamda “özel hayata ve hayatın gizli alanına

---

[432] Dülger, “Kişisel Verilerin Korunması Kanunu ve…”: 119.

[433] 1. Tehlikeli maddelerin izinsiz olarak bulundurulması veya el değiştirmesi (madde 174),
2. Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188), suçları.
b) 10/7/1953 tarihli ve 6136 sayılı Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunun 12 nci ve 13 üncü maddelerinde tanımlanan suçlar.
c) 21/7/1983 tarihli ve 2863 sayılı Kültür ve Tabiat Varlıklarını Koruma Kanununun 67 nci ve 68 inci maddelerinde tanımlanan suçlar.

karşı suçlar" kapsamında 119.340 yeni dosyanın açıldığı ve en çok, verileri hukuka aykırı olarak verme veya ele geçirme (81.365), özel hayatın gizliliğini ihlal (31.319) ve kişisel verilerin kaydedilmesi (3.020) suçlarının olduğu belirtilmiştir[434].

Kişisel verilerin hukuka aykırı biçimde işlenmesi, yalnızca TCK kapsamında suç teşkil etmekle kalmamakta, aynı zamanda bireylerin kişilik haklarına yönelik bir müdahale anlamına da gelmektedir. Bu tür hukuka aykırı işlemler karşısında, mağdur bireylerin kişilik haklarını korumak amacıyla TMK ve TBK çerçevesinde çeşitli hukuki yollara başvurma imkânları bulunmaktadır[435].

TMK'nin 25 inci maddesi gereği, kişisel verileri hukuka aykırı biçimde işlenen kişiler, söz konusu işlemenin durdurulmasını, ortadan kaldırılmasını ve hukuka aykırılığın tespitini talep edebilir. Ayrıca, bu kişiler ihlal sonucu zarara uğramaları halinde hem maddi hem de manevi tazminat talebinde bulunabilecekleri gibi, hukuka aykırı saldırı neticesinde elde edilen kazançların kendilerine verilmesini de talep edebilir.

Öte yandan, TBK'nin 58 inci maddesi kapsamında, kişilik hakkının ihlal edilmesi durumunda zarara uğrayan kişilerin, uğradıkları manevi zararın karşılanması amacıyla tazminat talebinde bulunmaları mümkündür. Bu çerçevede, kişisel verileri ister otomatik yollarla isterse geleneksel yöntemlerle hukuka aykırı şekilde işleyen kişiler, kusur derecesine bakılmaksızın manevi tazminat ödeme yükümlülüğü altına girebilirler.

Türkiye'de kişisel verilerin korunmasına ilişkin temel ve özel bir kanun olarak KVKK'nin hazırlanma süreci, Türkiye'nin AK ile 1981 senesinde imzaladığı ancak 2016 yılında onaylanarak bağlayıcı hale gelen 108 sayılı Sözleşmeye dayanmaktadır. KVKK, 07.04.2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiş ve

---

[434] Adalet Bakanlığı, *Adalet İstatistikleri 2024*, (2024): 70.

[435] Osman, Şahin, *Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğinin Korunması*, (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2011): 122.

mevzuat sürecinin en önemli aşamalarından biri olarak hukuk sistemimizde yerini almıştır[436].

KVKK'nin birinci maddesinde düzenlendiği üzere *"kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek"* Kanun'un temel amacıdır. Keza madde gerekçesinde bu Kanun'un nihai amacının, *"kişisel verilerin işlenmesinin disiplin altına alınması ve Anayasada öngörülen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin korunması"* olduğu ve *"son yıllarda önem kazanan kişinin mahremiyet hakkı ile bilgi güvenliği hakkının"* korunmasının da yine bu çerçevede dikkate alındığı ifade edilmiştir. *"Ayrıca, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların"* düzenlenmesinin de düzenleme amaçları içerisinde yer aldığı belirtilmiştir[437].

KVKK, kişisel verilerin korunmasına dair temel kavramları tanımlamakta ve hangi koşullarda bu verilerin işlenebileceğini düzenlemektedir. Bu hakkı doğuran sebeplerin hâlâ gelişim sürecinde olduğu göz önünde bulundurulduğunda, KVKK'nin gelecekteki olası şartlara uyum sağlayabilmesi açısından çerçeve bir düzenleme olarak kabul edilmesi oldukça isabetlidir[438].

Türkiye'de kişisel verilerin korunmasına dair düzenleyici ve denetleyici yetki, KVKK uyarınca, KVK Kurumuna verilmiştir. KVK Kurumu, veri koruma alanındaki temel

---

[436] Bununla birlikte KVKK'nin, kendisi ile yakın zamanlarda AB'de yürürlüğe konulan GDPR yerine, GDPR'nin yürürlüğe konulmasıyla mülga olan 95/46/EC sayılı Direktif'i esas alması, ayrıntılı hükümler barındırmadığı, unutulma hakkı gibi mevcut sorunlara çözüm bulamadığı, KVK Kurulu üyelerinin seçilme yolları sebebiyle güvence sağlamadığı gibi gerekçelerle AK'de ve kamuoyunda eleştirildiği görülmüştür (Avrupa Komisyonu, *AB Genişleme Politikasına İlişkin 2020 Bilgilendirmesi*, (2020): 18; Tahir Hami, Topaç, *6698 Sayılı Kanun Kapsamında Kişisel Verilere İlişkin Suçlar*, (Doktora Tezi, Selçuk Üniversitesi, 2022): 203).

[437] Bilir, "Kişisel Verilerin Korunması Yönündeki…": 639.

[438] Bilir, "Kişisel Verilerin Korunması Yönündeki…": 648.

otorite olup KVKK'nin uygulanmasını sağlamak, kişisel verilerin işlenmesini denetlemek ve ihlalleri tespit etmekle yükümlüdür. Kurumun karar organı ise KVK Kurulu'dur. KVK Kurulu, kişisel veri ihlalleriyle ilgili idari yaptırımlar uygulama yetkisine sahip olup veri sorumlularının yükümlülüklerini yerine getirip getirmediğini denetlemektedir. Bu bağlamda, veri sorumlusu sıfatıyla faaliyet göstermekte olan PHS'lerin kişisel verileri KVKK'ye aykırı bir biçimde işlemesi hâlinde KVK Kurulu tarafından idari yaptırımlar uygulanabilmektedir.[439]

Kişisel verilerin gizliliği ve güvenliğine yönelik olarak posta sektörüne özgü düzenlemeler ise PHK ve bu kanuna dayanılarak hazırlanan ikincil mevzuatta bulunmaktadır.

PHK, posta sektörünün serbestleştirilmesi sürecinde, etkin düzenleme ve denetim mekanizmalarıyla rekabetçi bir piyasa oluşturmayı ve ilgili AB Direktifine uyum sağlamayı hedefleyerek 23.05.2013 tarihli ve 28655 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. PHK'nin *"Posta hizmetlerinin gizliliği ve güvenliği"* başlıklı 7 nci maddesi ile posta sektöründe gönderinin gizliliği ve güvenliğinin korunmasına yönelik düzenleyici çerçeve çizilmekle birlikte kişisel verinin ne olduğu hususunda bir tanıma yer verilmemiştir. Bununla birlikte Kanun'un *"Hizmet sağlayıcılarının yükümlülükleri"* başlıklı 12 nci maddesinin birinci fıkrasının (b) bendi uyarınca hizmet sağlayıcıların, kişisel verilerin ve bilgilerin gizliliğinin korunmasına ilişkin hükümlere riayet etmeleri zorunlu tutulmuş ve bu Kanun maddeleri ile BTK tarafından yetkilendirilmiş olan PHS'ler, posta sektöründe kullanıcılara ait verilerinin gizliliğini ve güvenliğini korumakla yükümlü kılınmıştır[440].

Diğer yandan, PHSİY, *"posta hizmeti verilebilmesi ve/veya bunun için gerekli altyapının kurulup işletilebilmesine yönelik usul ve esasları düzenlemek"* amacıyla

---

[439] Kişisel Verilerin Korunması Kanunu (KVKK).
[440] Posta Hizmetleri Kanunu, 2013, 12/1(b).

03.06.2014 tarihli ve 29019 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Yönetmeliğin *"Tanımlar"* başlıklı 4 üncü maddesinin birinci fıkrasının (g) bendinde "kişisel veri" tanımına yer verilmiştir. Bu bent uyarınca; *"Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler"* kişisel veri olarak kabul edilmektedir.

Burada dikkat çekilmesi gereken husus, Yönetmelikte yer alan kişisel veri tanımında gerçek ve tüzel kişilere ilişkin bütün bilgilerin kişisel veri olarak kabul edildiğidir. Keza KVKK kapsamında korunan veriler yalnızca gerçek kişilere ait kişisel verilerdir. Ancak tüzel kişilere ilişkin kişisel verilerin KVKK kapsamında korunuyor olmaması, hiç korunmayacakları manasına gelmemektedir. Tüzel kişiler de diğer yasalar kapsamında korunabilmektedir[441]. Nitekim, söz konusu Yönetmelik kapsamında kişisel veri tanımına tüzel kişiler de dâhil edilerek bu şekilde koruma kapsamına alındıkları görülmektedir. Bu husus AYM Kararı ile de uyumludur. Zira PHK'nin 3 üncü maddesinin birinci fıkrasının (a) bendinde yer alan; "adres bilgi kayıt sistemi" tanımı kapsamında, PTT tarafından ticari amaçla veri tabanı oluşturulurken gerçek kişilerden açık rıza alınmasının zorunlu olduğu, ancak tüzel kişilerden rıza alınmadığı belirtilmiştir. AYM, tüzel kişilerin fiziki ve elektronik adres bilgilerinin, rızaları olmaksızın reklam ve tanıtım amacıyla kullanılmasına imkân tanınmasının Anayasa'nın 20 nci maddesinde güvence altına alınan kişisel verilerin korunması hakkına aykırı olduğunu değerlendirmiş ve bu nedenle ilgili madde hükmünü iptal etmiştir[442].

Posta Hizmetlerinin Sunulmasına İlişkin Yönetmelik (PHSİY), *"posta hizmetlerine ilişkin tarife, kullanıcı menfaatleri, posta hizmetlerinin gizliliği ve güvenliği, hizmet kalitesi ve uzlaştırma prosedürü ile posta sektöründe rekabeti tesis etmeye ve korumaya yönelik usul ve esasları düzenlemek"* amacıyla 03.06.2014 tarihli ve 29019

---

[441] Bilir, "Kişisel Verilerin Korunması Yönündeki…": 643.
[442] Anayasa Mahkemesi, 04.12.2014 günlü, E:2013/84, K:2014/183 sayılı karar.

sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Yönetmeliğin 18 inci maddesinde, posta hizmetlerinin gizliliği ve güvenliği hakkında PHK'nin 7 nci maddesine benzer biçimde düzenlemeye gidilmiştir. Bununla birlikte anılan maddenin dördüncü fıkrasına mücbir nedenler haricinde ve ilgili mevzuat hükümlerinin saklı kalması kaydı ile, kayıtlı gönderilerin kaybının, çalınmasının ya da hasarının oluşması hâlinde sorumluluğun PHS'de olduğu düzenlenmiştir[443].

Diğer yandan bu Yönetmeliğin "Kullanıcı şikâyetleri çözüm mekanizması" başlıklı 22 nci maddesinde PHS'lere, kullanıcı şikâyetleri ile bu şikâyetler uyarınca verilen cevapların kayıt altına alınması ve asgari iki yıl saklanması yükümlülüğü getirilmiştir. Bu kapsamda PHS'ler söz konusu verileri işleyerek şikâyetin sebebine ilişkin olarak sınıflandırmakta ve talep edildiğinde şikâyetlere ilişkin bilgi ve belgeleri BTK'ye göndermekle yükümlü kılınmıştır[444].

Bilgi Teknolojileri ve İletişim Kurumu Posta Sektöründe İdari Yaptırımlar Yönetmeliği (PİYY) ise *"Kurum tarafından posta sektöründe uygulanacak idari yaptırımlara ve bunların uygulanmasına ilişkin usul ve esasları düzenlemek"* amacıyla 03.06.2014 tarihli ve 29019 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Anılan Yönetmeliğin kapsamı, PHK ve BTK düzenlemeleri dâhil olmak üzere, posta sektörüne dair ilgili mevzuatta yer verilen yükümlülüklerin yerine getirilmemesi halinde ya da ilgili mevzuata aykırılık durumunda uygulanacak olan idari para cezalarıyla diğer idari tedbirler ve yaptırım ve bunların uygulanmasına dair kurallardır. Buna göre PHS'lerin kişisel veri ve bilgilerin gizliliğinin korunmasına dair yükümlülükleri bulunmaktadır. Posta hizmetlerinin gizliliği ve güvenliğinin sağlanması hususunda yasal sorumluluğun, PHS'leri, bunlar tarafından istihdam edilen çalışanları ve posta hizmeti ile ilgili bilgiye sahip olan üçüncü kişileri kapsadığı belirtilmektedir[445]. Bu kapsamda

---

[443] Posta Hizmetlerinin Sunulmasına İlişkin Yönetmelik, 2014.
[444] Posta Hizmetlerinin Sunulmasına İlişkin Yönetmelik, 2014.
[445] M. Aytaç, Özelçi, "Posta Hizmetleri Sektöründe Uygulanan İdari Yaptırımların Bağlı Olduğu Hukuksal Düzen", *İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 20, Sayı: 1, (Ocak 2021): 205.

anılan Yönetmeliğin *"Kişisel veri ve bilgilerin korunmasına ilişkin ihlaller"* başlıklı 10 uncu maddesinde, PHS tarafından kişisel verilerin ve bilgilerin gizliliğinin korunmasına dair yükümlülüklerinin ihlal edilmesi durumunda PHS'ye, bir önceki takvim yılındaki net satışlarının yüzde üçüne (%3) kadar idari para cezası uygulanabileceği hükme bağlanmıştır. Bu oran, düzenlemedeki en yüksek oran olup bu konudaki ihlallere kritik düzeyde önem verildiğini vurgulamaktadır.

PHK ve PİYY'de yer alan düzenlemelere göre, kişisel verilerin gizliliğinin ihlali durumunda idari yaptırımlar öngörülmesi, KVK Kurulu'nun yaptırım uygulamaya ilişkin yetkisini etkilememektedir. Keza PHS'ler, KVKK kapsamında özel hukuk tüzel kişisi olarak değerlendirilmekte olup faaliyetlerinde KVKK'ye uygun hareket etme yükümlülüğü altındadır. Bu doğrultuda, BTK ve KVK Kurulu, PHS'lerin kişisel veri ve bilgilerin korunmasına dair yükümlülüklerini ihlal etmeleri halinde idari yaptırım uygulama yetkisine sahiptir. Ancak bu süreçte izlenecek yöntem ve prosedürlerin daha net bir biçimde belirlenmesi faydalı olacaktır[446].

BTK'nin kişisel veri ihlali gerekçesiyle uygulanabilecek idari yaptırım kararlarının hukuka uygunluğunun denetiminde, ihlalin ne olduğunun açıkça ortaya konulması önemlidir. PHS'nin kişisel verilere ilişkin düzenlemeleri ihlal etmesi halinde, ilgili yükümlülüğün belirlenmesi bakımından KVKK ile KVK Kurulu'nun düzenleyici işlemlerinin esas olarak alınması gerekmektedir. Böylelikle, hangi eylemin hukuka aykırı veya uygun olduğunun tespiti açısından KVKK hükümleri rehber olarak kullanılmalıdır[447].

İdari para cezasını gerektiren kabahat türünden eylemler veri sorumlusunun aydınlatma yükümlülüğünün ve veri güvenliğine ilişkin yükümlülüklerin ihlali; KVK Kurulu tarafından verilen kararların yerine getirilmemesi ve veri sorumluluğu siciline

---

[446] Özelçi, "Posta Hizmetleri Sektöründe Uygulanan…": 207.
[447] Özelçi, "Posta Hizmetleri Sektöründe Uygulanan…": 208.

kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesidir. Bu durumda KVKK kapsamında tesis edilen idari para cezası sadece veri sorumlusu hakkında uygulanacaktır; yani veri sorumlusu gerçek kişiyse bu kişi, tüzel kişi ise yine sadece bu tüzel kişi idari yaptırım kararının öznesi olacaktır. Posta hizmetleri sektörü için belirlenen kişisel veri koruma yükümlülüklerinin ihlali halinde BTK'nin yaptırım kararlarının öznesi PHS'ler olacaktır. KVKK, PHK'den sonra yürürlüğe giren ve kişisel verilerin korunmasında çerçeve yasa niteliğinde olan bir düzenleme olarak, genel denetim yetkisini KVK Kurulu'na tanımaktadır. Bununla birlikte, BTK'nin KVKK'de belirlenen sorumluluğun kapsamı haricinde kalan ve posta hizmeti sunma konusunda yetkilendirdiği PHS'lerin bu kapsamdaki iş ve işlemleri bakımından yaptırım yetkisine sahip olduğu konusunda duraksama bulunmamaktadır. Ayrıca, KVKK kapsamındaki bir ihlalin tespiti halinde BTK'nin, durumu KVK Kurulu'na bildirerek iki kurum arasında iş birliğinin sağlanması gereklidir. Bu ilişkinin hukuki belirlilik ilkesine uygun şekilde yasal düzenlemelerle veya ikincil mevzuatla netleştirilmesine ihtiyaç duyulmaktadır[448].

Son olarak, KVK Kurulu sektör bazlı somut tedbirlerden ziyade daha çok sektör üstü kriterler ve esaslar belirlemekte olduğundan, posta sektöründe gerek görülmesi halinde; kişisel verilerin toplanmasında, işlenmesinde ve imhasında kullanılabilecek daha spesifik düzenlemeler ile yine kişisel verilerin işlendiği sistemlerin güvenliğini sağlamak üzere PHS'lere veri koruma standartları getirmek konusunda BTK'nin yetkilerinin olduğu açıktır.

Sonuç itibarıyla 4. Bölüm içerisinde ülkemiz ve seçili diğer ülkelerde kişisel verilerin korunması mevzuatı incelenmiştir. İncelenen bu ülkeler ile ülkemizde geçerli olan ilgili mevzuatın karşılaştırılabilmesini teminen, "Veri Koruma İlkeleri" ve "Kullanıcı Hakları"nın mevcut durumunu belirlemek amacıyla UPU tarafından hazırlanan Ekim 2024 tarihli anketin özet sonuçlarına Tablo 4.1 ve Tablo 4.2'de yer verilmektedir:

---

[448] Özelçi, "Posta Hizmetleri Sektöründe Uygulanan…": 208-209.

Tablo 4.1 Veri Koruma İlkeleri

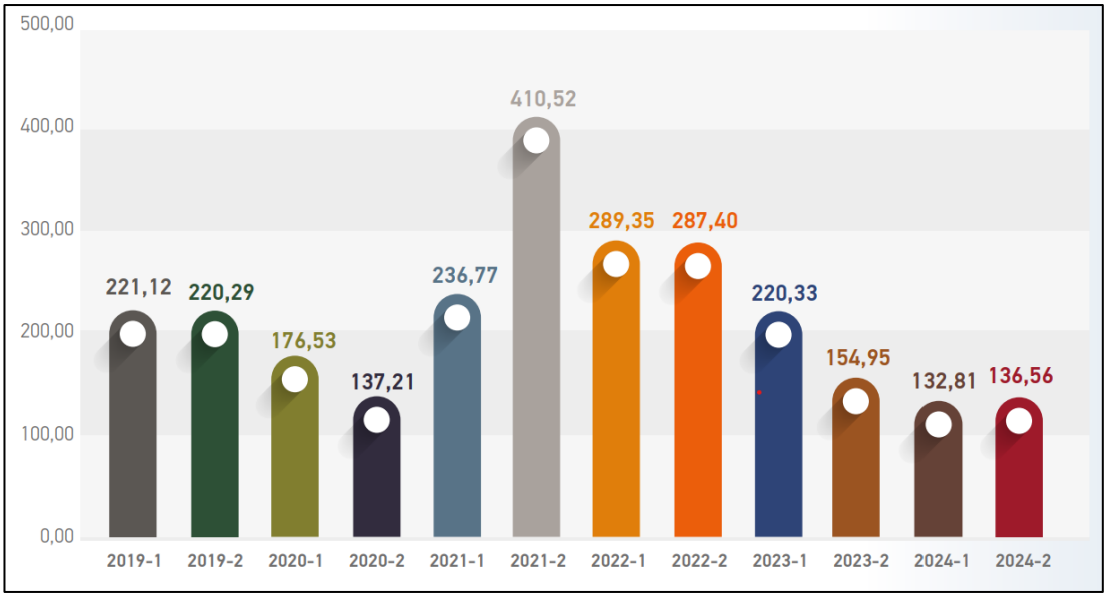
	Almanya	Avusturya	ABD	Belçika	Finlandiya	Birleşik Krallık	Çin	Türkiye
Hukuka Uygunluk	✓	✓		✓	✓	✓	✓	✓
Adillik	✓	✓		✓	✓	✓		✓
Şeffaflık	✓	✓	✓	✓	✓	✓	✓	✓
Belirli, Açık Meşru Amaçlar için İşleme	✓	✓	✓	✓	✓	✓		✓
İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma	✓	✓	✓	✓	✓	✓	✓	✓
Doğru ve Güncel Olma	✓	✓		✓	✓	✓	✓	✓
Gerekli Olan Süre Kadar Muhafaza Edilme	✓	✓		✓	✓	✓	✓	✓

Tablo 4.2 Kullanıcı Hakları

	Almanya	Avusturya	ABD	Belçika	Finlandiya	Birleşik Krallık	Çin	Türkiye
Bilgilendirilme Hakkı	✓	✓		✓	✓	✓	✓	✓
Erişim Hakkı	✓	✓	✓	✓	✓	✓	✓	✓
Düzeltme Hakkı	✓	✓	✓	✓	✓	✓	✓	✓
Silinme/Unutulma Hakkı	✓	✓	✓	✓	✓	✓	✓	✓
Veri Taşınabilirliği Hakkı	✓	✓	✓	✓	✓	✓	✓	
İtiraz Hakkı	✓	✓		✓	✓	✓	✓	
Otomatik Karar Verme ve Profil Oluşturma ile İlgili Haklar	✓	✓		✓	✓	✓	✓	

Ülkemizde uygulanan kişisel verilerin korunmasına ilişkin mevzuatın incelenmesinin akabinde, Türkiye'de posta sektörünün genel görünümüne bakılacak olunursa; son yıllarda artan dijital alışveriş alışkanlıkları, tüketici davranışlarını ve dolayısıyla posta hizmetlerine olan talebi önemli ölçüde değiştirmiştir. Bu dönüşüm neticesinde, Türk posta sektöründe posta koli/kargosu, bireysel ve kurumsal kullanıcıların artan talepleri doğrultusunda daha fazla ön plana çıkarken, haberleşme gönderilerinin hacminde bir azalma gözlemlenmektedir. Bu kapsamda Şekil 4.1'de, ülkemizde haberleşme gönderileri adetlerinin 2019-2024 yılları arasında 6'şar aylık dönemlere göre dağılımına yer verilmektedir:

Şekil 4.1 Haberleşme Gönderileri Adetlerinin Dönemlere Göre Dağılımı (Milyon Adet)



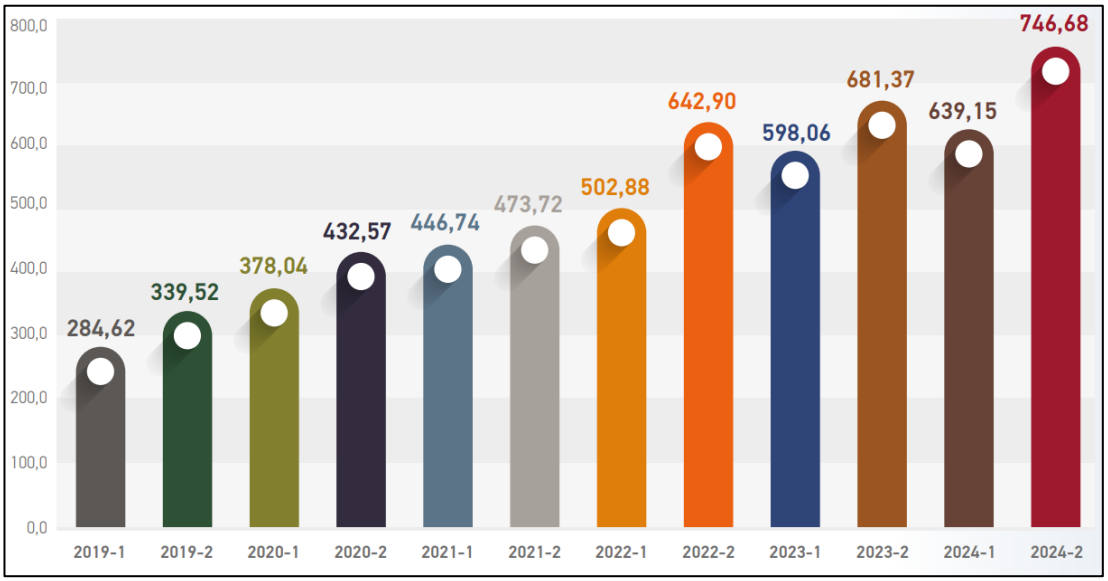
Kaynak: BTK[449]

Söz konusu şekilden görüleceği üzere, 2021 yılının ikinci 6 ayında haberleşme gönderi adetleri beş yılın en yüksek seviyesindedir.

[449] Bilgi Teknolojileri ve İletişim Kurumu. *Türkiye Posta Sektörü Pazar Verileri Raporu* 2024-2

Posta kolisi ve kargo gönderi adetlerinin 2019-2024 yılları arasında 6'şar aylık dönemlere göre dağılımı ise Şekil 4.2'de sunulmaktadır:

Şekil 4.2 Posta Kolisi/Kargosu Gönderi Adetlerinin Dönemlere Göre Dağılımı (Milyon Adet)



Kaynak: BTK[450]

Buna göre, posta kolisi ve kargo niteliğindeki gönderilerin sayısı, 2023 yılının ikinci altı ayında 681,37 milyon iken, 2024 yılının ikinci altı ayında %9,6 oranında artış göstererek yaklaşık 746,7 milyon adede ulaşmıştır.

Türkiye'de kişisel verilerin korunması ve güvenliğinin sağlanmasında posta sektöründe faaliyet gösteren PHS'ler tarafından kişisel veri güvenliğinin nasıl sağlandığını tespit etmeyi teminen, işbu Tez çalışmasında kullanılmak üzere, bir Sualname hazırlanmıştır. Söz konusu Sualname, pazar payları da dikkate alınarak 13 PHS'ye iletilmiş olup anılan Sualnameye 12 PHS tarafından cevap verilmiştir. Sualname aracılığıyla elde edilen yanıtlar, tüm katılımcılar açısından tamamıyla örtüşmemektedir. Ancak bu veriler, ortak ve farklı yönleriyle birlikte değerlendirilmiş

[450] Bilgi Teknolojileri ve İletişim Kurumu. *Türkiye Posta Sektörü Pazar Verileri Raporu* 2024-2

olup en yaygın ve etkili uygulamaları temsil eden iyi örneklerin bir araya getirilmesiyle sentezlenmiştir. Bu kapsamda, kişisel verilerin korunmasına ilişkin olarak posta sektöründe dikkat edilen önemli hususlar ile alınan güvenlik tedbirlerine; hukuki, idari ve teknik gerekliler şeklinde sınıflandırılarak aşağıda özet bir biçimde yer verilmektedir:

İlgili PHS'ler tarafından sunulan posta hizmeti kapsamında hukuki gereklilikler bakımından; mevzuatla zorunlu kılınan ve hizmetin doğrudan ifası için gerekli kişisel verilerin toplanması, bu verilerin, KVKK'nin genel ilkeleri çerçevesinde ve veri işleme şartlarına uygun olarak BTK'nin 2016/DK-YED/517 sayılı Posta Güvenlik Tedbirleri Usul ve Esasları kapsamındaki gönderici ve alıcıya ait verilerin işlenmesi,

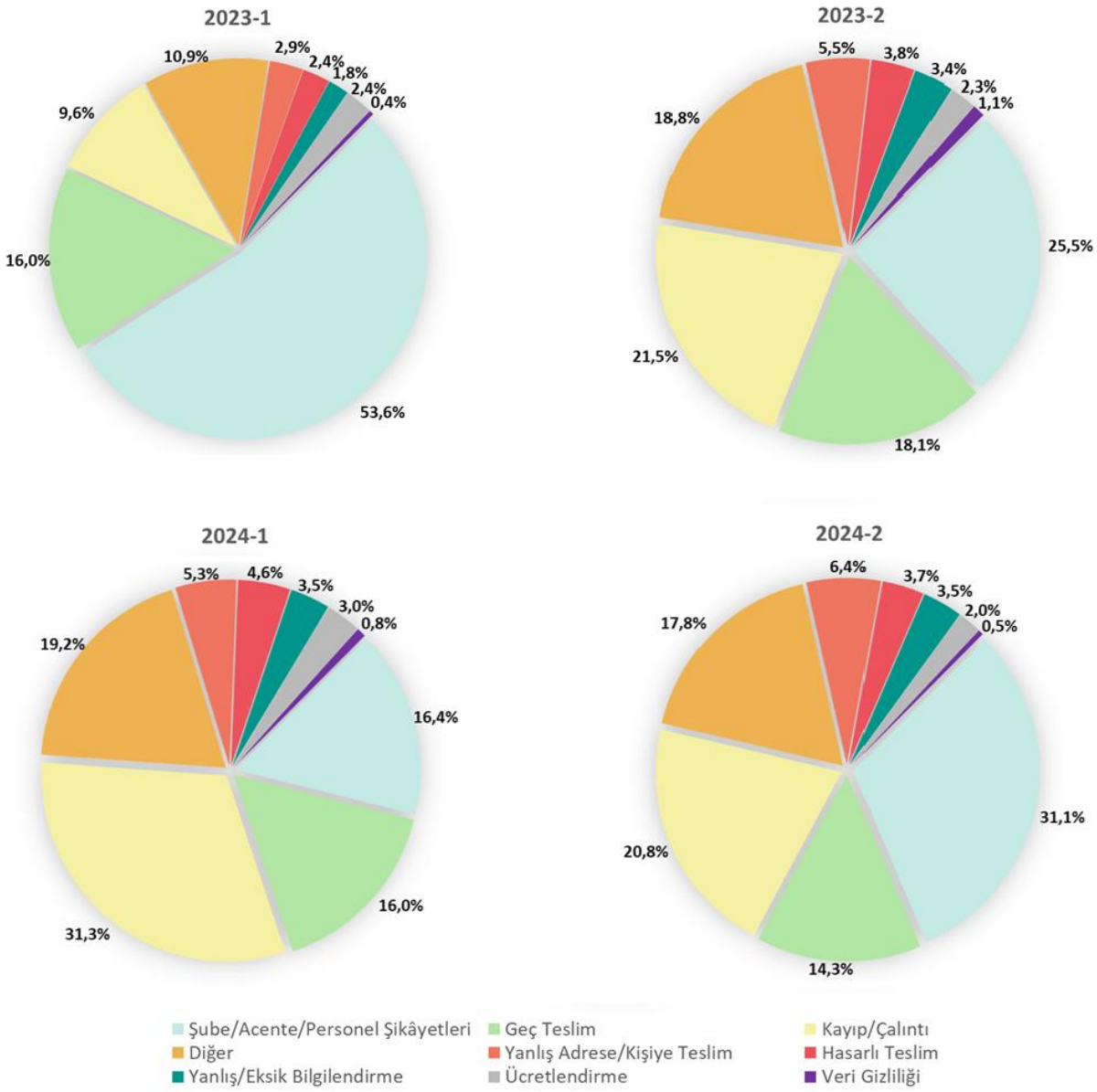
İdari tedbirler bakımından; aydınlatma yükümlülüğünün yerine getirilmesi ve ilgili kişilerin bilgilendirilmesi, şirket içinde kişisel verilerle ilgili özel politika ve prosedürlerin oluşturulması, kişisel verilerin işlenmesi, aktarılması, saklanması, imhası ve anonimleştirilmesine dair süreçlerin ayrıntılı prosedürlere bağlanması, kişisel verilerin korunması amacıyla komite/ekip kurularak veri işleme faaliyetlerinin düzenli olarak gözden geçirilmesi ve denetlenmesi, veri koruma görevlisi ile çalışılarak GDPR ile de uyum sağlanmaya çalışılması, çalışanlar, acenteler, tedarikçiler ve müşteriler ile gizlilik ve kişisel verilerin korunmasına ilişkin hükümler içeren sözleşmeler imzalanması, şirket içinde yaşanan ihlal durumlarının kayıt altına alınması ve takibini sağlayan sistemler oluşturulması, disiplin düzenlemelerine gizlilik ve veri güvenliği kurallarının dâhil edilmesi, çalışanlara yönelik eğitim faaliyetlerinin düzenlenmesi, ISO 27001 (Bilgi Güvenliği Yönetim Sistemi) ve ISO 27701 (Kişisel Veri Yönetim Sistemi) sertifikalarına sahip olunması,

Teknik gereklilikler bakımından; fiziksel ortamda, hizmet alanlarında, aynı anda birden fazla kişiye hizmet sunulurken veri sızıntısını engelleyecek şekilde fiziksel düzenlemeler yapılması, yetkisiz kişilerin bu alanlara girmesinin engellenmesi, şubelerde kişisel veri güvenliği konusunda bilgilendirici afişlerin yer alması, sistemsel

ve dijital ortamda ise kişisel verilere yalnızca görev tanımı ile uygun, sınırlı erişimin sağlanması, iki faktörlü kimlik doğrulama sistemleriyle hem çalışan hem de kullanıcı girişlerinin güvence altına alınması, çalışanların el terminalleri üzerinden sadece yetkili oldukları gönderilere ait maskelenmiş bilgilere erişim sağlayabilmesi, alıcı ile iletişimin sistemde maskelenmiş numaralar üzerinden sağlanması, teslimat anında kimlik teyidinin tek kullanımlık şifre veya alıcının dijital imzası ile gerçekleştirilmesi, gönderilerin üzerinde yer alan barkodlarda göndericinin açık adres bilgisi, telefon numarası gibi kişisel verilerinin maskelenmesi, teslimat sürecinde gönderinin durumunun sadece alıcıya özel şekilde; maskelenmiş veri üzerinden, internet sitesi veya SMS yoluyla takip edilebilmesi, kişisel veri içeren belgelerin tespit edilerek sınıflandırılması ve bu sınıflara özel güvenlik önlemlerinin uygulanması, sistemde yapılan tüm kritik işlemlerin (erişim, teslimat vb.) loglanarak izlenebilirliğinin sağlanması, gelişmiş şifreleme yöntemleri ve güçlü parola politikalarının uygulanması, antivirüs, zararlı yazılımdan koruma sistemleri, güvenlik duvarı, saldırı tespit/önleme sistemlerinin aktif bir şekilde kullanılması, periyodik sızma testleri ve zafiyet taramaları yapılarak sistem açıklarının analiz edilmesi

gibi tedbirlerin uygulandığı ifade edilmektedir. Söz konusu tedbirler ışığında uygulamadaki durumun görülebilmesi için, posta sektöründe kullanıcılar tarafından 2023-2024 yılları içinde BTK'ye yapılan şikâyet başvurularının kategori bazlı dağılımına Şekil 4.3'te yer verilmektedir:

Şekil 4.3 BTK'ye Ulaşan Kategori Bazlı Şikâyet Sayılarının Dağılımı



Kaynak: BTK[451]

[451] Bilgi Teknolojileri ve İletişim Kurumu, *Türkiye Posta Sektörü Pazar Verileri Raporu*, 2023-1; Bilgi Teknolojileri ve İletişim Kurumu, *Türkiye Posta Sektörü Pazar Verileri Raporu* 2023-2; Bilgi Teknolojileri ve İletişim Kurumu, *Türkiye Posta Sektörü Pazar Verileri Raporu* 2024-1; Bilgi Teknolojileri ve İletişim Kurumu. *Türkiye Posta Sektörü Pazar Verileri Raporu* 2024-2

Bu şikâyetlere ilişkin veriler incelendiğinde, “veri gizliliği” temelli şikâyetlerin tüm başvurular içerisindeki oranının %1’den aşağı seviyelerde olduğu dikkat çekmektedir. Bu kapsamda, posta sektöründe kişisel veri ihlallerine yönelik BTK’ye yapılan başvuruların yoğun olmadığı sonucuna varılabilecektir.

Son olarak ülkemizdeki PHS’lere ilişkin olarak KVK Kurulu’na yapılan ihlal bildirimleri neticesinde, anılan Kurulca verilen ve kamuoyuna açıklanan idari yaptırımlarda değinilmesinde fayda görülmektedir. Buna göre;

- MNG Kargo Yurtiçi ve Yurtdışı Taşımacılık AŞ tarafından KVK Kurulu’na iletilen veri ihlal bildiriminde, 15-23 Ağustos 2021 tarihleri arasında yetkisiz kişilerce kurumsal müşterilerin kullanıcı adı ve şifre bilgilerinin ele geçirilerek sistemlerine izinsiz erişim sağlandığı bildirilmiştir. Bu ihlal kapsamında, kargo alıcılarına ait ad, soyad, adres ve telefon numarası gibi kişisel verilerin etkilendiği, ancak etkilenen kişi sayısının tespit edilemediği belirtilmiştir. Bu kapsamda KVK Kurulu’nun 26.08.2021 tarihli ve 2021/875 sayılı kararıyla söz konusu veri ihlalinin KVK Kurumunun internet sitesinde kamuoyuna ilan edilmesine karar verilmiştir[452].
- Posta ve Telgraf Teşkilatı Biriktirme ve Yardım Sandığı tarafından KVK Kurulu’na iletilen veri ihlal bildiriminde, 29-30 Ağustos 2022 tarihleri arasında zararlı yazılımlar aracılığıyla sisteme yetkisiz erişim sağlandığı ve anne kızlık soyadı, cilt seri numarası gibi PTT çalışanlarına ait kişisel verilerin yanı sıra 3,2 GB büyüklüğünde veri tabanı yedeği ile site dosyalarının ele geçirildiği bildirilmiştir. İhlal sonucu yaklaşık 38.000 kayda ait kimlik ve üyelik bilgileri etkilendiği ve ihlalin 30 Ağustos 2022 tarihinde tespit edildiği belirtilmiştir. Bu kapsamda KVK Kurulu’nun 01.09.2022 tarihli ve 2022/891 sayılı kararıyla söz

[452] Kişisel Verileri Koruma Kurulu Kararı, 26.08.2021 günlü, 2021/875 sayılı karar.

konusu veri ihlalinin KVK Kurumunun internet sitesinde kamuoyuna ilan edilmesine karar verilmiştir[453].

- Asilkar Hızlı Kargo Taşımacılık Ticaret A.Ş. tarafından KVK Kurulu'na iletilen veri ihlal bildiriminde, 30 Ocak – 3 Şubat 2025 tarihleri arasında yetkisiz kişilerce sistem kullanıcılarının kullanıcı adı ve parola bilgilerinin ele geçirilerek Ajannet Bilişim Hizmetleri Sanayi Ticaret Ltd. Şti.'nin terminal sunucularına uzak bağlantı yoluyla erişim sağlandığı bildirilmiştir. Saldırı sonucu, yalnızca dosya isimlerinde yer alan 16 çalışanın ad ve soyad bilgilerine yetkisiz erişimin gerçekleştiği, dosyalara ilave kullanıcı adı ve parola olmadan erişim sağlanamadığı belirtilmiştir. Ajannet Bilişim tarafından alınan veriler arasında posta alıcılarının adı, soyadı, adresi ve gönderi içeriği bilgilerinin bulunabileceği bildirilmiştir. İnceleme devam etmekle birlikte KVK Kurulu'nun 13.02.2025 tarihli ve 2025/353 sayılı kararıyla söz konusu veri ihlalinin KVK Kurumunun internet sitesinde kamuoyuna ilan edilmesine karar verilmiştir[454].

[453] Kişisel Verileri Koruma Kurulu Kararı, 01.09.2022 günlü, 2022/891 sayılı karar.
[454] Kişisel Verileri Koruma Kurulu Kararı, 13.02.2025 günlü, 2025/353 sayılı karar.

SONUÇ VE ÖNERİLER

İşbu tez kapsamında; posta sektöründe kişisel verilerin korunması konusu ele alınmış olup bu konu, gizlilik ve güvenlik olmak üzere iki alt başlık altında detaylıca ele alınmıştır. Bunun için, kişisel verilerin gizliliği ve güvenliğine ilişkin temel kavram ve uygulamalar ile ulusal ve uluslararası düzenlemelerin yanı sıra, bu hususların posta sektöründeki görünümleri de incelenmiştir. "Sonuç ve öneriler" başlıklı bu son bölümde ise incelenen konu başlıklarına ilişkin çıkarımlara ve bu alanda Türkiye için düzenleme önerilerine yer verilmesi amaçlanmaktadır.

Kişisel veri kavramı, kişi ile veri kavramlarının kesiştiği bir nokta olarak karşımıza çıkmakta; dolayısıyla kişisel veri, veri işleme faaliyetlerinin yanı sıra, bireylerin kişilik haklarının korunması açısından da kritik bir önem arz etmektedir.

Bireylerin özel hayatları ve haberleşme özgürlüğü ile ilişkilendirilen özel hayatın gizliliği müessesesi, 19. yüzyılın sonundan itibaren, kişisel veriler başlığını da içine almaya başlamıştır. Bu çerçevede kişisel veri kavramı ve kişisel verilerin korunması, bireyin özel hayatına saygı ilkesinin bir uzantısı olarak modern hukuk sistemlerinde temel bir hak olarak yer bulmuştur.

Kişisel verilerin korunması alanındaki ilk kapsamlı düzenleme girişimi, 1980 yılında OECD tarafından yayımlanan ve veri korumaya ilişkin temel ilkeleri belirleyen Rehber İlkeler ile gerçekleşmiştir. Ardından BM'nin İHEB ile AK'nin AİHS gibi belgelerinde yer verilen özel hayatın gizliliğine ilişkin hükümleri, kişisel verilerin korunmasını da içerecek biçimde genişletilmiştir. Ancak bu hükümlerin yetersiz kalmasıyla, AK tarafından 1981 yılında 108 sayılı Sözleşme kabul edilmiştir. AB ise 1995 yılında yürürlüğe giren 95/46/EC sayılı Direktif ile kişisel verilerin korunmasının çerçevesini belirlemiştir. Ancak bu Direktifin uygulanması aşamasında üye devletler nezdinde bir birlik sağlanamaması üzerine, 2016 yılında GDPR kabul edilmiştir.

Türkiye'de T.C. Anayasası'nın "Özel hayatın gizliliği" başlıklı 20 inci maddesinin üçüncü fıkrasıyla kişisel verilerin korunması anayasal güvenceye kavuşturulmuş, 2016 yılında yürürlüğe giren ve 95/46/EC sayılı Direktif esas alınarak hazırlanan KVKK ile de kişisel verilerin işlenmesi, saklanması ve aktarılmasına dair kanuni esaslar düzenlenmiştir. 108 sayılı Sözleşme ise 17 Mart 2016 tarihli ve 29656 sayılı Resmî Gazete'de yayımlanarak Türk hukuk sistemine dâhil edilmiştir.

Gerek ulusal gerekse uluslararası mevzuatta kişisel veri *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* biçiminde tanımlanmakta olup bu kavramsal çerçeve, modern hukuk sistemlerinde veri koruma rejimlerinin temelini oluşturmuştur.

Diğer yandan dijitalleşmenin hızla geliştiği günümüzde, kişisel veri mahremiyetine ilişkin sorunlar yalnızca bireylerin değil, aynı zamanda sektörel düzenlemelerin de öncelikli gündem maddelerinden biri haline gelmiştir. Bu çerçevede, posta sektöründe gönderilerin gizliliği ve güvenliğinin nasıl sağlanacağı sorusu üzerinde önemle durulmalıdır.

PHS'lerin güvenilir işletmeler olması, posta hizmetlerinin temel gereksinimlerinden biri olup bu husus, kamu hizmeti mahiyetinde olan posta hizmetlerinin sunumunda söz konusu hizmet sağlayıcılarının bir yetkilendirme rejimi kapsamına girmelerini gerektirmektedir. Klasik posta hizmetlerine dahil haberleşme gönderileri açısından kişisel verinin korunması hem özel hayatın hem de haberleşmenin gizliliğiyle doğrudan ilişkilidir. Diğer yandan PHS'ler, haberleşme gönderileri haricinde e-ticaret gönderilerinin fiziksel dağıtım altyapısının da önemli bir parçasıdır. Artan e-ticaret gönderileriyle birlikte kapsam ve kapasitesi hızla artan posta sektöründe PHS'ler, kendi hizmet kalitelerini artırmak adına gelişen teknolojileri işletme organizasyonlarının çekirdek şebekelerine entegre etmek zorunda kalmaktadırlar. Çünkü katma değerli hizmetler ve geniş bir yelpazede sunulan ürünlerle birlikte her geçen gün artan müşteri beklentilerini karşılamak PHS'lerin en önemli öncelikleri

arasındadır. Dolayısıyla, PHS'ler hizmet sunumlarını çeşitlendirirken, artan gönderi trafiği daha fazla veri üretmekte ve bu da PHS'lerin aynı zamanda büyük hacimlerde kişisel veri işleyen aktörlere dönüşmesine sebebiyet vermektedir. Bu nedenlerle kişisel veri gizliliği, verilerin korunması ve mahremiyet kavramlarının posta sektöründeki etkisi oldukça genişlemektedir.

Türkiye'de posta gönderilerinin gizliliği ve güvenliği hususu çeşitli mevzuat hükümleriyle sağlanmaktadır. Bunlardan en temel olanı, T.C. Anayasası'nın 22 nci maddesinde yer alan haberleşme hürriyetiyle ilgili düzenlemedir. Bu maddede, herkesin haberleşme hürriyetine sahip olduğu ve haberleşmenin gizliliğinin esas olduğu hükme bağlanmıştır. Diğer yandan bu hakkın ancak millî güvenlik, kamu düzeni, genel sağlık ve ahlâkın korunması, suç işlenmesinin önlenmesi ya da başkalarının hak ve özgürlüklerinin korunması gibi özel sınırlama sebepleriyle kısıtlanabileceği; bununla birlikte, bu sınırlamaların ancak usulüne uygun şekilde verilmiş bir hâkim kararı ile mümkün olabileceği düzenlenmiştir. Gecikmesinde sakınca bulunan durumlarda ise yalnızca kanunla yetkilendirilmiş mercilerin yazılı emriyle bu hakka müdahale edilebileceği, aksi bir durumda haberleşmenin engellenemeyeceği ve gizliliğinin ihlal edilemeyeceği esasına dayanılmaktadır.

Yine PHK'de ve PHK'ye dayanılarak hazırlanan PSİYY'de, PHS'lerin ve posta hizmetlerinde görevli kişilerin, görevleri esnasında edindikleri bilgileri açığa vuramayacakları, gönderileri açamayacakları, içeriklerini araştıramayacakları ve bu bilgileri üçüncü kişilere aktaramayacakları hüküm altına alınmıştır. Aynı şekilde, bu tür eylemlere neden olunmasının veya gönderilerin alıkonulması ya da yok edilmesinin de yasak olduğu düzenlenmiştir. Ayrıca, posta gönderilerinin yalnızca kanunen yetkilendirilmiş merciler tarafından açılabileceği veya incelenebileceği; bunlar dışındaki kişiler tarafından gönderilerin alıkonulamayacağı, açılamayacağı ya da içeriğinin araştırılamayacağı belirtilmiştir. Diğer yandan, bu yetkili mercilerin kim olduğu aynı düzenlemede sayılmamış, yetkili kişi ve kurumların kendi mevzuatına

atıfta bulunulmakla yetinilmiştir. PHS'ler ise sundukları hizmet kapsamında gerekli güvenlik önlemlerini almakla yükümlü kılınmıştır.

PHK'de kişisel veri tanımı yapılmamakla birlikte, PHS'lerin yükümlülükleri arasında "Kişisel veri ve bilgilerin gizliliğinin korunması yükümlülüklerine uymak" da sayılmıştır. Bu kapsamda KVKK'nin yürürlüğe girmesinin posta sektörü açısından da oldukça önemli olduğu düşünülmektedir. Zira posta mevzuatında kişisel verilerin korunmasına ilişkin özel düzenlemeler bulunmasa dahi, PHS'lere genel hukuki düzenlemeler uygulanabilmektedir. Buna göre KVKK kapsamında PHS'ler, sundukları hizmetler doğrultusunda gönderici ile kurdukları sözleşme çerçevesinde gönderici veya alıcıya ait veriler üzerinde karar verme yetkisine sahip olmaları nedeniyle veri sorumlusu sıfatını haiz olmaktadır. PHS'lerin talimatları doğrultusunda kişisel verileri işleyen kişi veya kuruluşlar ise veri işleyen olarak değerlendirilmektedir. Bazı durumlarda bu iki sıfatın PHS nezdinde birleşmesi de mümkündür. Veri işleyen seçiminde de veri sorumlusu azami özeni göstermelidir. Zira her iki aktör de kişisel verilere dair ihlallerde müteselsil sorumluluk taşımaktadır.

Öte yandan PSİYY'de kişisel veri kavramı; kimliği belirli veya belirlenebilir gerçek ve tüzel kişilere dair bütün bilgiler olarak tanımlanmıştır. Bu düzenlemede yer alan tanım ile GDPR ve KVKK'den farklı olarak, posta sektöründe tüzel kişi verileri de kişisel veri olarak kabul edilmiş ve bu verilerin de koruma altına alınması sağlanmıştır.

Posta sektöründe veri işlemenin kapsam ve niteliğine bakılacak olunursa; hizmet talep eden kullanıcıların PHS'ler ile paylaştığı bilgiler, PHS'ler tarafından sistemlerine kaydedilmekte bu sayede hem hizmetin sunumu esnasında hem de daha sonraki hizmet sunumlarında kullanılmaktadır. Bu kapsamda işlenen veriler; kullanıcı ile PHS arasındaki ilişkinin niteliğine, kullanılan iletişim araçlarına ve veri işleme amaçlarına göre farklılık gösterebilmektedir. Hem GDPR'ın hem de KVKK'nin, kişisel veriyi tahdidi olarak sınırlamayarak "her türlü bilgi" şeklinde ifade etmesi ile posta sektöründe kimlik, iletişim, işlem, finans, görsel kayıt ve pazarlama gibi çeşitli bilgilerin kişisel veri

kapsamında değerlendirilmesi ve bu verilerin belirli ilke ve kurallara uygun bir biçimde işlenmesi mümkün olabilmektedir.

Posta sektöründe kişisel verilerin işlenmesi sürecinde, PHS'lerin KVKK'de belirtilen ilkelere uygun hareket etmeleri şarttır. Bu ilkeler; kişisel verilerin hukuka ve dürüstlük kurallarına uygunluğu, verilerin doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlarla işlenmesi, ilgili, sınırlı ve ölçülü olması ile amaç için gerekli süre kadar muhafaza edilmesini kapsamaktadır. Söz konusu ilkelerin BTK düzenlemelerine de yansıdığı görülmektedir. Örneğin, Teslimat Usul ve Esasları'nda yapılan düzenlemelerle temassız teslimat yöntemi benimsenerek haberleşme gönderisi hariç gönderilerin tesliminde alıcının imzasının alınmamasına karar verilmiştir. Benzer şekilde, 2023 yılında Güvenlik Usul ve Esaslarında yapılan değişiklikle haberleşme gönderileri haricindeki teslimatlarda alıcının T.C. kimlik numarasının talep edilmeyeceği düzenlenmiştir. Bu tür uygulamaların, kişisel verilerin korunmasına yönelik ilkelere uyum açısından yerinde ve önemli adımlar olduğu değerlendirilmektedir.

PHS'lerin veri işleme süreçlerinde yalnızca yukarıda belirtilen ilkelere uymaları yeterli olmamakta, ayrıca kişisel veri işleme faaliyetlerini KVKK'de düzenlenen hukuka uygunluk şartlarına da dayandırmaları gerekmektedir. Bu doğrultuda veri işleme faaliyetinden önce, işlemenin hangi hukuki sebebe dayandığı tespit edilmelidir. PHS'ler; açık rıza, kanuni yükümlülük, sözleşmenin ifası veya hukuki yükümlülüğün yerine getirilmesi gibi hukuka uygunluk nedenlerinden birine dayanarak veri işleme faaliyetinde bulunabilmektedir. Nitekim PHK'deki kayıtlı gönderi tanımı kapsamında gönderiye ilişkin veriler kanuni bir yükümlülük nedeniyle; göndericinin ad, soyad ve adres bilgileri ise PHS ile gönderici arasındaki sözleşmenin ifası amacıyla işlenmektedir. İlaveten, teslimatın yapılabilmesi için gereken alıcı verileri ile ikincil düzenlemeler nedeniyle ihtiyaç duyulan sair verilerin de yine PHS'lerin hukuki sorumluluklarını yerine getirebilmeleri adına işlenmesi mümkündür.

Posta hizmetlerinin sunumunda elde edilen verilerin üçüncü taraflara aktarılması hususuna ilişkin olarak; PHK'nin 7 nci maddesinin üçüncü fıkrası gereğince PHS'ler, kullanıcı verilerini kanunla yetkilendirilmiş merciler dışında kalan kişi veya kuruluşlar ile paylaşamamaktadır. Esasen posta verilerinin ilgili kişinin açık rızası olmaksızın PHS'ler aracılığıyla üçüncü taraflara aktarılmaması temel prensip olarak kabul edilmiştir. Bununla birlikte, bazı istisnai hallerde ilgili kişinin açık rızası aranmaksızın veri aktarımı gerçekleştirilebilmektedir. Yurt içine veri aktarımında bilgi ve belge talep etmeye yetkili mercilere kişisel veri aktarımında açık rıza aranmamaktadır. Diğer yandan PHS'ler, veri sorumlusu sıfatıyla işlemiş oldukları kişisel verileri, hizmet sözleşmesi kapsamında üçüncü kişilerden temin edeceği ürün veya hizmetlerle sınırlı olmak kaydıyla paylaşabilmektedir. Bununla birlikte KVKK'nin "Kişisel verilerin yurt dışına aktarılması"nı düzenleyen 9 uncu maddesinde 01.06.2024 tarihinde yürürlüğe giren 7499 sayılı Kanun ile yapılan değişiklikte, kişisel verilerin yurt dışına aktarıldığı hallerde "açık rızayı" önceleyen yaklaşım terkedilmiş ve veri sahiplerinin daha fazla korunduğu bir yapı oluşturulmuştur. Yeni düzenleme, aşamalı ve alternatifli bir aktarım sistemi getirmiştir. Bu düzenleme kapsamında, kişisel verilerin yurt dışına aktarılmasında; yeterlilik kararına dayalı aktarım, uygun güvencelere dayalı aktarım ve arızi durumlara dayalı aktarım olarak üç farklı yöntem öngörülmüştür. Oysa, posta hizmetlerinin uluslararası düzeyde sunumunda; bu faaliyetlerin doğası gereği veri aktarımının yapılması gerekliliği göz önüne alındığında, anılan gönderiler için yukarıda sayılan yöntemlerden hangisinin kullanılması gerektiği konusunda henüz net bir yaklaşım benimsenmemiş olduğu görülmektedir. Bu doğrultuda, sektörel bazda bir yeterlilik kararının alınmasının, bu alanda karşılaşılması muhtemel sorunların çözümüne fayda sağlayacağı değerlendirilmektedir.

Posta sektöründe kişisel veri güvenliği de oldukça önem arz eden bir konudur. Zira kişisel verilerin korunması, bireylerin temel hak ve özgürlüklerinin güvence altına alınmasını, kişisel veri güvenliği ise kişisel verilerin olası tehdit ve risklere karşı korunmasını hedeflemektedir. Bu bağlamda, kişisel verilerin hukuki koruma çerçevesinde güvenli bir şekilde işlenmesi ve muhafaza edilmesi kritik bir önem

taşımakta olup PHS'ler, kişisel verilerin hukuka aykırı biçimde işlenmesi ve erişilmesini önlemek ile kişisel verilerin güvenli bir şekilde muhafazasının sağlanması için gerekli idari ve teknik tedbirleri almakla yükümlüdür.

İşbu tez kapsamında; kişisel verilerin gizliliği ve güvenliğinin, bilgi toplumuna geçiş sürecinde tüm sektörler için hukuki, teknik ve ekonomik bir ikilem haline geldiği, zira hizmetlerin devamlılığı için veri işleme faaliyetinin kaçınılmaz olduğu, kişisel verilerin müşteri ilişkilerini geliştirmek, hizmetleri kişiselleştirmek ve yeni gelir modelleri oluşturmak açısından stratejik önem taşıdığı, ancak bu konuda kullanıcıların çoğunlukla korunmaya muhtaç taraf olduğu görülmektedir. Posta sektörü için de söz konusu hususlar geçerlidir. Posta sektöründe kişisel verilerin korunmasına yönelik olarak bazı düzenleyici kararlar alınmış olmakla birlikte, kullanıcıların kişisel verilerinin gizliliği ve güvenliğinin üst düzeyde teminine yönelik sektöre özgü, bir örnek ve kapsayıcı ilke, kural ve uygulama esaslarına ihtiyaç duyulduğu düşünülmektedir. Bu kapsamda, işbu tez çalışmasında yer alan tüm bilgi, açıklama ve değerlendirmeler ışığında, Türkiye için geliştirilen önerilere aşağıda yer verilmektedir:

PHK'de kişisel verilerin korunmasına ilişkin olarak yalnızca PHS'lerin kişisel veri ve bilgilerin gizliliğinin korunması yükümlülüklerine uyması gerektiğine yer verilmiş; ancak kişisel verilerin işlenmesi, aktarılması, muhafazası ve imha edilmesi gibi temel veri işleme faaliyetlerine dair açık hükümlere yer verilmemiştir. Buna karşılık uygulamada; gerekli olmamasına rağmen kişisel verilerin işlenmesi ya da mevzuatta öngörülen süreden daha uzun süre saklanması veya üçüncü taraflara aktarılması gibi problemlere rastlanma ihtimali vardır. Bu tür uygulamalar, kişisel verilerin işlenmesinde uyulması gereken temel ilkelere aykırılık doğurabilme riskini taşımaktadır.

Diğer yandan PHK'nin 12 nci maddesinde yer alan PHS'lerin kişisel verilerin korunmasına ilişkin yükümlülüklere uyması gerektiğine dair hükmün, sektöre özgü düzenlemelerin yapılmasına imkân tanıdığı düşünülmektedir. Zira anılan madde ile

BTK'nin düzenleyici yetkisi birlikte değerlendirildiğinde, BTK'nin posta sektöründe kişisel verilerin korunmasına yönelik ikincil düzenleme yapma yetkisine sahip olduğu sonucuna varılmaktadır. Nitekim BTK, PHK'ye dayanılarak hazırlanan Güvenlik Usul ve Esasları ile posta gönderilerine ilişkin güvenlik tedbirlerinin belirlenmesine yönelik kuralları belirlemiştir. Ancak kişisel verilerin işlenmesi, saklanması ve silinmesi gibi konularda daha ayrıntılı ve uygulamaya yön veren düzenlemelere de yer verilmesi mümkündür. Bu çerçevede, hizmet sağlayıcıların yükümlülüklerini somutlaştıracak, denetim süreçlerini destekleyecek ve veri sahiplerinin haklarını güçlendirecek nitelikte ikincil düzenlemelerin BTK tarafından hayata geçirilmesinin faydalı olabileceği değerlendirilmektedir.

Bu kapsamda, mevcut yasal mevzuatın tamamlayıcısı olacak şekilde, yalnızca posta sektörü özelinde uygulanacak ve sektördeki muhtelif uygulama ve tedbirleri en iyi örnekler çerçevesinde bir örnekleştirebilecek bir "Posta Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Usul ve Esaslar" hazırlanmasının, sektörel uyumu ve hukuki güvenliği artıracağı düşünülmektedir. Her ne kadar teknoloji hızla değişmekte de olsa, posta sektörü genelinde uygulanabilecek asgari güvenlik esas ve standartların belirlenmesi, hem kullanıcıların daha etkin bir biçimde korunmasına hem de sektörde faaliyet gösteren PHS'ler açısından ortak bir güvenlik anlayışının geliştirilmesine katkı sağlayacaktır. Bu nedenle Bir Yönetmelik ya da Tebliğ şeklinde çıkarılabilecek olan söz konusu düzenleme, PHK, KVKK ve ilgili ikincil mevzuata dayalı olarak hazırlanmalı; ayrıca posta sektörüne özgü operasyonel ihtiyaçlar ve teknoloji kullanımını da dikkate almalıdır. İlaveten söz konusu düzenlemenin hazırlanması aşamasında KVK Kurumu ile koordineli bir biçimde çalışılması ve anılan Kurumun görüşlerinin dikkate alınması da önemli bir gereksinim olacaktır.

Söz konusu Usul ve Esaslarda; öncelikle posta sektöründe kişisel verilerin toplanması, işlenmesi, saklanması ve imhası aşamalarında kullanılan temel kavramları tanımlayan bir "Tanımlar" bölümünün yer alması gerekecektir. Bu maddede "Kişisel veri, açık rıza, hizmet sağlayıcısı" gibi ilgili düzenlemelerde daha önce tanımlanmış olan kavramların

yanı sıra, “işlem kaydı, maskeleme, şifreleme” gibi hizmete özel teknik kavramlara da yer verilmesine ihtiyaç duyulacağı değerlendirilmektedir.

Diğer yandan, söz konusu düzenleme kapsamında, PHS’lere çeşitli yükümlülükler getirilebilecek olup bu yükümlülükler “teknik ve idari güvenlik önlemleri ile sistemsel yetkilendirmelerin yapılması; barkodlama ve gönderi üzeri bilgi güvenliğine dair özel tedbirlerin alınması; şube ve dağıtım noktalarında fiziksel güvenlik standartlarının belirlenmesi; insan kaynağına yönelik eğitim ve sorumluluk mekanizmaların oluşturulması; veri paylaşımı; üçüncü taraflarla ilişkiler ve bildirim sorumluluğu; yerli ve milli yazılımlarla veri işlenmesi ve saklanması; siber güvenlik çalışmaları kapsamında denetimlerin yapılması ve veri koruma görevlisi belirlenmesi” olmak üzere çeşitli başlıklar altında toplanabilecektir. Anılan başlıklara göre, söz konusu yükümlülüklerin kapsamının aşağıdaki ilke, esas ve usullere göre belirlenebileceği öngörülmektedir.

Teknik ve idari güvenlik önlemleri ile sistemsel yetkilendirmelerin yapılması

- Veri güvenliği açısından en temel önlemlerden biri, erişim kontrollerinin sıkı şekilde yapılandırılmasıdır. PHS çalışanlarının yalnızca görev tanımlarına uygun veri alanlarına erişebilmesi için sistemsel yetkilendirme süreçleri titizlikle tanımlanmalıdır. Erişim logları, sistem denetimleri kapsamında en az iki yıl süreyle saklanmalı ve yalnızca yetkili denetim birimleri tarafından erişilebilir olmalıdır.

- Kişisel verilerin görünürlüğünü azaltmak amacıyla yazılım sistemlerinde "veri maskeleme" teknikleri kullanılmalıdır. Bu sayede, yetkisiz erişimlerin veri ifşası riski azaltılacak, aynı zamanda sistem kullanıcılarının yalnızca gerekli bilgiye ulaşması sağlanacaktır.

- Kargo takip sistemlerinde, takip numarası ile erişilen bilgilerin yalnızca operasyonel durumu (gönderi yolda, şubede, teslim edildi vb.) göstermesi sağlanmalı; gönderici ve alıcı isimleri gibi kişisel veriler bu ekranlardan ayrıştırılmalıdır.

- Veri işleme süreçleri; hukuka uygunluk, ölçülülük ve amaca bağlılık ilkeleri çerçevesinde sınırlandırılmalı, posta hizmet sunumu haricinde herhangi bir amaçla işleme yapılmasına müsaade edilmemelidir. İşlenen veriler, yasal zorunluluklar ortadan kalktığında anonimleştirilmeli veya geri döndürülemez biçimde imha edilmelidir.

Barkodlama ve gönderi üzeri bilgi güvenliğine dair özel tedbirlerin alınması

- Posta gönderileri üzerindeki barkod etiketleri, bireylerin telefon, adres ya da diğer kişisel bilgilerini barındırmakta; bu durum, özellikle postanın teslim alınmasına kadar verilerin üçüncü kişilerce görülmesine neden olabilmektedir. Bu nedenle, gönderi üzerindeki barkodlar yalnızca teslimat için mutlak surette gerekli olan bilgileri içermeli, kişisel veri niteliği taşıyan diğer unsurlar (örneğin; alıcı telefon numarası) sistemsel erişim alanına alınmalı, fiziksel etiketlerde yer almamalıdır.

- Teslimatı gerçekleştiren personelin alıcı ile iletişimi, çağrı merkezi üzerinden yönlendirilerek veya doğrudan telefonla görüşme yerine, sistem üzerinden yönlendirilen anonim aramalar veya yazışmalar ile gerçekleştirilmelidir. Bu sayede alıcının iletişim bilgilerinin PHS personeli tarafından öğrenilmesi engellenmelidir.

- Gönderi üzerindeki QR kod sistemleri yalnızca yetkili personelin kimlik doğrulaması sonrası kullanılabilir hale getirilmelidir. Bu uygulama ile QR kodlar üzerinden erişilebilecek alıcı bilgileri veya gönderi detayları, sadece

görevli dağıtım personeli tarafından ve kimlik doğrulama işlemi gerçekleştikten sonra görüntülenebilir olacaktır. Böylece, gönderi üzerinde yer alan verilerin yetkisiz kişilerce okunması veya kötüye kullanılması riski azaltılacaktır. Kimlik doğrulama süreci; görevlinin mobil cihaz üzerinden kullanıcı adı/parola girişi yapması, personel kartı ile doğrulama gerçekleştirmesi ya da biyometrik sistemlerle erişim sağlaması gibi yöntemlerle uygulanabilir. Bu önlem sayesinde, hem dağıtım sürecinde veri güvenliği artırılabilecek hem de erişim işlemlerinin kim tarafından ve ne zaman yapıldığının kayıt altına alınması mümkün olabilecektir.

- Gönderiye iliştirilen irsaliye, fatura gibi belgeler ise alıcı bilgilerini doğrudan ifşa etmeyecek biçimde yerleştirilmelidir. Bu durum gönderi içeriğinin gizliliği açısından önemli bir adım olacaktır.

Şube ve dağıtım noktalarında fiziksel güvenlik standartlarının belirlenmesi

- Kişisel verilerin yalnızca dijital ortamlarda değil, fiziksel mekanlarda da ifşa riski taşıdığı unutulmamalıdır. Özellikle şube ve teslim noktalarında, gişe/banko düzenlemeleri, müşteri bilgilerinin çevredeki üçüncü kişiler tarafından duyulamayacağı veya görülemeyeceği biçimde tasarlanmalıdır.

- Veri paylaşımı, şube personeli ile gönderici arasında gerçekleştirilirken, bu bilgilere yalnızca yetkili personelin ulaşabileceği sistemler kullanılmalı, evrak teslimi gibi işlemler gizlilik ilkesine uygun şekilde yürütülmelidir.

- Aydınlatma yükümlülüğünün fiziksel ortamlarda da görünür şekilde yerine getirilmesi sağlanmalı; bunun için şubelerde, veri işleme süreçlerine ilişkin afişler, broşürler ya da dijital ekranlar aracılığıyla bireyler bilgilendirilmelidir.

İnsan kaynağına yönelik eğitim ve sorumluluk mekanizmaların oluşturulması

- Veri güvenliği kültürü, yalnızca teknik sistemlerle değil, çalışan davranışlarıyla da yakından ilişkilidir. Bu nedenle PHS bünyesindeki tüm çalışanlara yılda en az bir kez olmak üzere kapsamlı kişisel veri güvenliği eğitimleri verilmelidir. Eğitim içerikleri sadece yasal yükümlülükleri değil, aynı zamanda etik sorumlulukları da kapsamalıdır.

- Yeni işe başlayan personelin, işe başlamadan önce gizlilik ve veri koruma taahhütnamesi imzalaması zorunlu hale getirilmelidir.

- Veri ihlali gerçekleştiren ya da bu konuda şikâyet geçmişi olan personel için kademeli yaptırım mekanizmaları (yeniden eğitim, görev değişikliği, ihtar vb.) tanımlanmalıdır. Bu uygulamalar, çalışan farkındalığının artırılması ve kurumsal hesap verebilirliğin güçlendirilmesi açısından kritik önemdedir.

Kullanıcılara yönelik bilgilendirme ve güvenlik farkındalığını artırmaya yönelik mekanizmaların oluşturulması

- PHS'ler tarafından; kullanıcılara periyodik şekilde (örneğin; yılda bir kez) kişisel verilerinin hangi amaçla işlendiği, bu bilgilerin güncel ve doğru olması gerektiği, düzeltme ve itiraz hakları bulunduğu ile ilgili talepte bulunma haklarının olduğu hatırlatılmalıdır.
- PHS ile kullanıcılar arasında kullanılan bir uygulama, ara yüz vb. olması halinde giriş için kullanılan şifrelerin basitlikten uzak seçilmesi ve sıklıkla değiştirilmesi şeklinde yönlendirici bilgilendirmeler yapılmalıdır.

Veri paylaşımı, üçüncü taraflarla ilişkiler ve bildirim sorumluluğu

- PHS'ler, hizmet süreçlerinde üçüncü taraflardan destek aldığında bu firmalarla olan ilişkileri "veri sorumlusu-veri işleyen" bağlamında açık bir sözleşmesel çerçeveye oturtmalıdır. Veri işleyen konumundaki üçüncü taraflar, yalnızca verilen talimatlarla sınırlı olarak veri işleyebilmeli ve kendi amaçları doğrultusunda veriyi kullanamamalıdır.

- PHS'ler adına veri işleme faaliyeti yürüten tüm tedarikçi ve iş ortakları, PHS'ler tarafından belirli periyotlarla, örneğin; altı aylık dönemlerle BTK'ye raporlanmalıdır.

- Veri ihlali yaşanması durumunda ise en geç 72 saat içinde hem BTK'ye hem de KVKK'ye bildirim yapılmalı, ilgili veri sahipleri de bilgilendirilerek riskin etkileri azaltılmalıdır.

Yerli ve milli yazılımlarla veri işlenmesi ve saklanması

Kişisel verilerin mümkün olduğunca yurt içinde, yerli ve milli yazılımlar ile işlenmesi ve saklanması sağlanmalı; bunun için sektöre özel bulut hizmetlerinin ve yazılım sistemlerinin oluşturulması önceliklendirilmelidir.

Siber güvenlik çalışmaları kapsamında denetimlerin yapılması

PHS'lerin siber güvenlik kapasitelerini güçlendirmeye yönelik olarak, öncelikle düzenli ve kapsamlı sızma testleri ile bağımsız güvenlik denetimlerinin gerçekleştirilmesi sağlanmalıdır. Bununla birlikte, olası veri kayıplarına ve hizmet kesintilerine karşı, düzenli aralıklarla test edilen veri yedekleme süreçleri ile felaket kurtarma planlarının oluşturulması ve güncellenmesi zorunlu hale getirilmelidir. Ayrıca, PHS'lerin kullandığı yazılım ve sistemlerin güvenliği, yalnızca dış tehditlere karşı değil, aynı

zamanda geliştirme aşamasında ortaya çıkabilecek zafiyetlere karşı da korunabilmelidir.

Veri koruma görevlisi belirlenmesi

PHS'lerin otomatik yollarla kişisel verilerin işlenmesine ilişkin çalışan kapasitesine bağlı olarak, örneğin; en az 20 personel çalıştırması halinde, veri koruma görevlisi belirleme yükümlülüğü getirilmesi önerilmektedir.

Çalışanların çalışma süresiyle sınırlı veri işlenmesi

Platformlar aracılığıyla hizmet sunan bağımsız esnaf kuryeler ile bağımlı statüde çalışan diğer personelin kişisel verileri, PHS'ler tarafından hizmetle orantılı ölçüde işlenmelidir. Bu doğrultuda PHS'lere "çalışma süresiyle sınırlı veri işleme" yükümlülüğü getirilmesi önerilmektedir. Buna göre, PHS'ler çalışanlarının konum verilerini yalnızca fiilen hizmet sundukları zaman diliminde işleyebilmeli; mesai veya görev süresi dışında herhangi bir konum, hareket ya da benzeri kişisel veri takibinde bulunmamalıdır.

Diğer yandan, posta sektöründe kişisel verilerin yurt dışına aktarılması konusu da özel olarak ele alınması gereken bir konu başlığıdır. Zira, posta sektöründe uluslararası gönderi işlemleri kapsamında birtakım kişisel verilerin yurt dışına aktarılması kaçınılmazdır. Nitekim gönderici ve alıcı bilgilerini içeren barkodlar, gönderi etiketleri veya sistemsel kayıtlar, teslimatın sağlıklı biçimde gerçekleşebilmesi açısından alıcı ülkeye ya da uluslararası taşıyıcılara iletilmek zorundadır. 2024 yılında KVKK'de yapılan değişiklik ile posta verilerinin yurt dışına aktarımı, uygun güvencenin bulunmasına veya standart sözleşmenin bulunması halinde mümkün olabilmektedir. Ancak, söz konusu kararın posta hizmetlerinin doğasıyla uyumu itibarıyla yeniden ele alınması faydalı olabilecektir. Zira binlerce adet uluslararası gönderi taşıyan orta ölçekli bir PHS'nin yurt dışındaki alıcılarla teslimat öncesinde birebir sözleşme

yapması, alıcıyla ilk temasın genellikle teslimat anında gerçekleşmesi nedeniyle oldukça zorlaşmaktadır. Bu bağlamda, posta sektörünün yapısal özellikleri ve kamu hizmeti niteliği dikkate alınarak, KVK Kurumu ile BTK'nin koordinasyonunda özel bir "sektörel yeterlilik kararı" alınması önerilmektedir. Bu sayede posta sektörü özelinde bir yeterlilik kararının alınmasının, yurt dışına veri aktarımında yaşanan uygulama zorluklarını önemli ölçüde ortadan kaldıracağı değerlendirilmektedir.

Öte taraftan, her bir bağımsız bölüme özel olarak tanımlanan 10 haneli bir kodun açık adres bilgisi yerine kullanılması yöntemi, Ulusal Adres Veri Tabanı (UAVT) sistemi olarak adlandırılmaktadır. Söz konusu uygulama henüz çok yaygın olmamakla birlikte bu konuya ilişkin pilot uygulamalar gündeme gelmektedir. UAVT uygulamasının alıcının teslimat adresinin üçüncü kişilerce görülmesini engelleyebilecek mahiyette olması sebebiyle bu konudaki kişisel veri ihlallerini azaltabileceği düşünülmektedir. Bu kapsamda yapılabilecek düzenlemeler öncesinde BTK, Ticaret Bakanlığı ve Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü ve PHS'ler arasında koordineli bir çalışma yürütülmesinin söz konusu uygulamanın başarısı açısından faydalı olacağı değerlendirilmektedir.

Diğer taraftan, posta sektöründe kişisel verilerin korunması hususunda yetkili kurumlar olarak KVK Kurulu ile BTK koordinasyonu ve iş birliğinin oldukça önemli olduğu düşünülmektedir. Bu kapsamda "Posta Sektöründe Kişisel Verilerin Korunmasına İlişkin Uygulama Protokolü"nün hazırlanmasının, sektörde meydana gelen veri ihlallerine ilişkin idari soruşturmalarda karşılıklı görüş alışveriş usulünü netleştirerek, sürecin daha etkin bir biçimde sonuçlandırılmasına katkı sağlayacağı düşünülmektedir.

Öte yandan, 26 Haziran 2021 tarihli ve 31523 sayılı Resmî Gazete'de yayımlanan "Elektronik Haberleşme Sektöründe Başvuru Sahibinin Kimliğinin Doğrulanma Süreci Hakkında Yönetmelik"**,** elektronik haberleşme sektöründe abonelik sözleşmesi, numara taşıma, işletmeci değişikliği, nitelikli elektronik sertifika, kayıtlı elektronik

posta ve SIM değişikliği gibi başvuruların elektronik ortamda yapılması hâlinde, başvuru sahibinin kimliğinin doğrulanmasına ilişkin usul ve esasları düzenlemektedir. Ancak, PHS'ler bu düzenleme kapsamına dâhil değildir; zira posta sektöründe abonelik kavramı bulunmadığı gibi gönderinin kabulü veya teslimi sırasında biyometrik imza veya yüz tanıma gibi kimlik doğrulama sistemleri henüz kullanılmamaktadır. Bununla birlikte, PHS'ler tarafından gönderi teslimi aşamasında anılan Yönetmelik kapsamında bir doğrulama sürecinin (e-Devlet kapısından kimlik doğrulama, yapay zekâ veya yetkili ile görüntülü kimlik doğrulama ya da yüz yüze yapılan işlemlerde kimlik doğrulama) uygulanması halinde söz konusu Yönetmeliğe PHS'lerin de belirli kimlik doğrulama süreçleri bakımından dâhil edilmesini sağlayacak bir hüküm eklenmesinin, posta sektöründe güvenilirliğin artmasına katkı sağlayacağı değerlendirilmektedir.

Son söz olarak; posta sektöründe, kişisel verilerin korunması yalnızca mevzuatla sınırlı bir yükümlülük değil; aynı zamanda sosyal sorumluluk anlayışının da temel bileşenlerinden biri olmalıdır. PHS'lerin veri güvenliği konusundaki teknik tedbirler haricinde kullanıcıları bilinçlendirme, çalışan farkındalığını artırma ve şeffaflık politikaları geliştirme yönündeki faaliyetlerine ağırlık vermesinin faydalı olacağı düşünülmektedir. Bu kapsamda PHS şubelerinde afiş, broşürle, sosyal medyada ve televizyon reklamlarında bilgilendirici videolar hazırlanması ve dolandırıcılığın önlenmesine yönelik içeriklerin sunulması kişisel verilere yönelik farkındalığın artırılmasına katkı sağlayabilecektir.

KAYNAKLAR

Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü. *Avrupa Konseyine Genel Bir Bakış*. https://diabgm.adalet.gov.tr/Home/SayfaDetay/avrupa-konseyine-genel-bir-bakis27022020030011 (Erişim tarihi: 18.11.2024)

Adalet Bakanlığı. *Adalet İstatistikleri 2024.* 2024. https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/7042025092455Adalet_%C4%B0statistikleri_2024%20T%C3%BCrk%C3%A7e_Ingilizce.pdf (Erişim tarihi: 23.04.2025)

Adalet Bakanlığı. "İnsan Hakları Eylem Planı". 2021. https://insanhaklarieylemplani.adalet.gov.tr/resimler/eylemplani.pdf (Erişim tarihi: 09.10.2024)

AİHM 2. Dairesi Kararı, 18.11.2018 günlü, 22427/04 başvuru numaralı karar. https://www.kararara.com/aihm/turkce2/aihm11095.htm (Erişim Tarihi: 10.02.2025)

Akbulut, Ali Burak. *Posta Sektöründeki Dijital Dönüşümün Rekabetçi Bakış Açısıyla İncelenmesi, Uluslararası Uygulamalar ve BTK İçin Öneriler*. Bilişim Uzmanlığı Tezi. Bilgi Teknolojileri ve İletişim Kurumu. 2023. https://www.btk.gov.tr/uploads/thesis/ali-burak-akbulut-tez.pdf (Erişim Tarihi: 18.02.2025)

Akçalı Gür, Berna. "Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması". *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*. Cilt 25, Sayı 2. (Aralık 2019): 850-872. https://doi.org/10.33433/maruhad.665460 (Erişim Tarihi: 12.08.2024)

Akgül, Aydın. *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*. İstanbul: 2014.

Akgül, Aydın. "Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" ve AB Adalet Divanı'nın "Google Kararı"". *Türkiye Barolar Birliği Dergisi.* Sayı: 116. (2016). https://kutuphane.dogus.edu.tr/mvt/pdf.php?pdf=0016856 (Erişim Tarihi: 18.11.2024)

Aksoy, Hüseyin Can. *Kişisel Verilerin Korunması.* Yüksek Lisans Tezi. Ankara Üniversitesi. 2008. https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=P9q-Nq5ukBq9dT_yeUvx-Q&no=Aoy78eSDK17MIAoAGg_M7Q (Erişim Tarihi: 05.01.2025)

Aktaş Kuruçay, Kevser. "Bir İletişim Aracı Olarak Posta Sanatı (Mail Art)". *The Turkish Online Journal of Design, Art and Communication*. Cilt: 12, Sayı: 3. (2022): 764-780 https://dergipark.org.tr/tr/download/article-file/2388147 (Erişim Tarihi: 08.05.2025)

Alaattinoğlu, Daniela. "Rethinking Explicit Consent and Intimate Data: The Case of Menstruapps". *Fem Leg Stud.* Cilt: 30. (2022): 157–179. https://doi.org/10.1007/s10691-021-09486-y (Erişim Tarihi: 08.01.2025)

Almanya Federal Adalet ve Tüketiciyi Koruma Bakanlığı (Bundesministerium der Justiz und für Verbraucherschutz) ve Federal Adalet Ofisi (Bundesamt für Justiz). *Grundgesetz für die Bundesrepublik Deutschland*. 2025. https://www.gesetze-im-internet.de/gg/BJNR000010949.html (Erişim Tarihi: 26.05.2025)

Almanya Federal Adalet ve Tüketiciyi Koruma Bakanlığı (Bundesministerium der Justiz und für Verbraucherschutz) ve Federal Adalet Ofisi (Bundesamt für Justiz). *Postgesetz (PostG)*. https://www.gesetze-im-internet.de/postg_2024/BJNR0EC0B0024.html (Erişim Tarihi: 26.05.2025)

Almanya Federal Adalet ve Tüketiciyi Koruma Bakanlığı (Bundesministerium der Justiz und für Verbraucherschutz) ve Federal Adalet Ofisi (Bundesamt für Justiz). *Strafgesetzbuch (StGB) 202 Verletzung des Briefgeheimnisses*. https://www.gesetze-im-internet.de/stgb/__202.html (Erişim Tarihi: 26.05.2025)

Almanya Federal Şebeke Ajansı (Bundesnetzagentur). *Merkblatt "Postgeheimnis und Datenschutz"*. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Post/Unternehmen_Institutionen/PostgeheimnisDatenschutz/MerkblattPostgeheimnis.pdf?__blob=publicationFile&v=1 (Erişim Tarihi: 26.05.2025)

Altındere, Murat. *Kişisel verilerin korunması hukuku ve uygulanması*. Ankara: Adalet Yayınevi, 2020.

Amerika Birleşik Devletleri (ABD) Anayasası. https://constitution.congress.gov/constitution/amendment-4/#:~:text=The%20right%20of%20the%20people,and%20the%20persons%20or%20things (Erişim Tarihi: 06.06.2025)

Amerika Birleşik Devletleri (ABD) Ceza Kanunu, 1994. https://www.law.cornell.edu/uscode/text/18/1702 (Erişim Tarihi: 06.06.2025)

Amerika Birleşik Devletleri (ABD) Federal Düzenlemeler Yasası (CFR), 2017. https://www.ecfr.gov/current/title-39/chapter-I/subchapter-D/part-266 (Erişim Tarihi: 06.06.2025)

Amerika Birleşik Devletleri (ABD) Posta Hizmetleri. *Gizlilik Politikası*. https://about.usps.com/who/legal/privacy-policy/welcome.htm (Erişim Tarihi: 06.06.2025)

Amerika Birleşik Devletleri (ABD) Posta Hizmetleri. *Guide to Privacy, the Freedom of Information Act, and Records Management*. 2025. https://about.usps.com/policy/as353_pol.pdf (Erişim Tarihi: 06.06.2025)

Amerika Birleşik Devletleri (ABD) Yüksek Mahkemesi Kararı, 1878 tarihli Ex parte Jackson Kararı. https://supreme.justia.com/cases/federal/us/96/727/ (Erişim Tarihi: 06.06.2025)

Amerikan Veri Gizliliği ve Koruma Yasası (ADPPA), 2022. https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf (Erişim Tarihi: 06.06.2025)

An Coimisiún um Chosaint Sonraí (İrlanda Veri Koruma Kurumu). *Quick Guide to the Principles of Data Protection*. 2019. https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf (Erişim Tarihi: 01.09.2024)

Anayasa Mahkemesi Kararı. 04.12.2014 günlü, E:2013/84, K:2014/183 sayılı karar. https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-183-nrm.pdf (Erişim Tarihi: 27.10.2024)

Anayasa Mahkemesi Kararı. 19.03.2015 günlü, E:2014/108, K:2015/30 sayılı karar. https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2015-30-nrm.pdf (Erişim Tarihi: 18.01.2025)

Anayasa Mahkemesi Kararı. 28.09.2017 günlü, E:2016/125, K:2017/143 sayılı karar. https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2017-143-nrm.pdf (Erişim Tarihi: 10.03.2025)

Anı, Nevzat Ali. *Kişisel Verilerin İşlenmesi ve Açık Rıza*. Yüksek Lisans Tezi. İstanbul Üniversitesi. 2018. https://nek.istanbul.edu.tr/ekos/TEZ/58103.pdf (Erişim Tarihi: 28.07.2025)

Arslanhan, Merve. "Bankaların Bilgi Güvenliği Yönetimi Kapsamında Banka Müşterilerinin Kişisel Verilerinin Korunması". *Kişisel Verileri Koruma Dergisi.* Cilt: 6, Sayı: 2. (2024): 33-53. https://dergipark.org.tr/tr/pub/kvkd/issue/88721/1554932 (Erişim Tarihi: 06.05.2025)

Aşıkoğlu, Şehriban İpek. *Avrupa Birliği ve Türk Hukuku'nda Kişisel Verilerin Korunması ve Büyük Veri*. On İki Levha Yayıncılık, 2018.

Aşıkoğlu, Şehriban İpek. "Veri Sorumlularının Aydınlatma Yükümlülüğü, -Avrupa Birliği ve Türk Hukukunda-". *Kişisel Verileri Koruma Dergisi*. Cilt: 1, Sayı: 2. (2019): 41-65. https://dergipark.org.tr/tr/download/article-file/904836 (Erişim Tarihi: 18.05.2025)

Aşıkoğlu, Şehriban İpek ve Uzun, Fatih Burak. "Kişisel Verilerin Yurtdışına Aktarımının Açık Rızaya Dayandırılmasının Yarattığı Sorunlar ve Çözüm Önerileri". *Prof. Dr. Türkan Rado'nun Anısına Armağan*. (2020). https://ssrn.com/abstract=3683903 (Erişim Tarihi: 10.01.2025)

Aşıkoğlu, Şehriban İpek vd. "Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Sebepleri". *Türk Hukukunun Avrupa Birliği Hukukuna Uyumu Özel Hukuk*. İstanbul Üniversitesi Hukuk Fakültesi Avrupa Hukuku Uygulama ve Araştırma Merkezi, 2020. https://cdn.istanbul.edu.tr/file/JTA6CLJ8T5/BF53E3482BE0406290D5FF22FF94DDCE (Erişim Tarihi: 14.05.2025)

Atak, Songül. "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler". *TBB Dergisi*. Sayı 87. (2010): 90-120. https://tbbdergisi.barobirlik.org.tr/m2010-87-606 (Erişim Tarihi: 17.04.2025)

Avcı, Yasemin. *Kişisel Verilerin Korunması*. Yüksek Lisans Tezi. Selçuk Üniversitesi. 2019. https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=Tq-8gxclnXZS6QwCgseBQg&no=04JDuPDsp38MrQdFkqsZBA (Erişim Tarihi: 23.03.2025)

Avrupa Birliği Adalet Divanı, "07.12.2023 tarihli Karar, Birleştirilmiş Davalar C-26/22 ve C-64/22, SCHUFA Holding (Libération de reliquat de dette) (ECLI:EU:C:2023:958)". https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0026 (Erişim Tarihi: 15.10.2024)

Avrupa Birliği Adalet Divanı Kararı, 04.05.2023 günlü, C-300/21 numaralı Österreichische Post kararı. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021CJ0300 (Erişim Tarihi: 10.02.2025)

Avrupa Birliği Temel Haklar Ajansı ve Avrupa Konseyi. *Handbook on European Data Protection Law*. çev. İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü. rev. ed. 2020. https://itlaw.bilgi.edu.tr/media/2020/3/30/Bilgi_Avrupa_Veri_Koruma_Mevzuat%C4%B1_El_Kitab%C4%B1_2018_TR_v01_16022019.pdf (Erişim Tarihi: 24.07.2024)

Avrupa Komisyonu. *AB Genişleme Politikasına İlişkin 2020 Bilgilendirmesi*. 2020. https://www.ab.gov.tr/siteimages/trkiye_raporustrateji_belgesi_2020/enlargement_policy_nihai.pdf (Erişim Tarihi: 22.06.2025)

Avrupa Komisyonu. *Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data*. 2007. https://www.pdp.ie/docs/1030.pdf (Erişim Tarihi: 18.11.2024)

Avrupa Komisyonu. *Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR)*. 2007. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf (Erişim Tarihi: 27.01.2025)

Avrupa Komisyonu. *Article 29 Data Protection Working Party, Opinion 15/2011*. 2011. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (Erişim Tarihi: 16.03.2025)

Avrupa Komisyonu. *Article 29 Data Protection Working Party (Çalışma Grubu), No. 203 (2013). Opinion 03/2013 on purpose limitation*. 2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (Erişim Tarihi: 17.09.2024)

Avrupa Komisyonu. "Charter of Fundamental Rights of the European Union (2000/C 364/01)". *Official Journal of the European Communities*. 2000. https://www.europarl.europa.eu/charter/pdf/text_en.pdf (Erişim Tarihi: 14.11.2024)

Avrupa Komisyonu. "Daily News 18/03/2025". 2025. https://ec.europa.eu/commission/presscorner/detail/en/mex_25_812#5 (Erişim Tarihi: 16.06.2025)

Avrupa Komisyonu. "Do the data protection rules apply to data about a company?". https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en (Erişim Tarihi: 29.10.2024)

Avrupa Komisyonu. *Türkiye 2010 Yılı İlerleme Raporu.* 2011. https://www.ab.gov.tr/files/AB_Iliskileri/AdaylikSureci/IlerlemeRaporlari/turkiye_ilerleme_rap_2010.pdf (Erişim Tarihi: 16.06.2025)

Avrupa Konseyi. "Chart of signatures and ratifications of Treaty 223". 2025. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223&__cf_chl_tk=xCFk9DBcE7e8E9.9dNRicynhkcRHbfptKdrSOToYybg-1759235195-1.0.1.1-Sm3wdOnjFGI6973iiNuiaSrG8XoaGWNJcqDDT3lUlAM (Erişim Tarihi: 22.09.2025)

Avrupa Parlamentosu ve Avrupa Konseyi. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. 1995. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046&qid=1733605075285 (Erişim Tarihi: 29.11.2024)

Avrupa Parlamentosu ve Avrupa Konseyi. *Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service*. 1998. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31997L0067 (Erişim Tarihi: 29.11.2024)

Avrupa Parlamentosu ve Avrupa Konseyi. *Directive 2008/6/EC of the European Parliament and of the Council of 20 February 2008 amending Directive 97/67/EC with regard to the full accomplishment of the internal market of Community postal services.* 2008. https://eur-lex.europa.eu/eli/dir/2008/6/oj (Erişim Tarihi: 29.11.2024)

Avrupa Veri Koruma Denetçisi (EDPS). *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*. 2017. https://www.edps.europa.eu/sites/default/files/publication/17-04-11_necessity_toolkit_en_0.pdf (Erişim Tarihi: 19.10.2024)

Avrupa Veri Koruma Kurulu (EDPB). "Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Versiyon 1.0". https://www.edpb.europa.eu/system/files_en?file=2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf (Erişim Tarihi: 15.12.2024)

Avrupa Veri Koruma Kurulu (EDPB). "Kişisel Verilerin İşlenmesine İlişkin 1/2024 sayılı Kılavuz Madde 6(1)(f) GDPR, Versiyon 1.0". https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en (Erişim Tarihi: 08.10.2024)

Avrupa Veri Koruma Kurulu (EDPB). "Our Members". https://www.edpb.europa.eu/about-edpb/about-edpb/members_en (Erişim Tarihi: 28.05.2025)

Avrupa Veri Koruma Kurulu (EDPB). "The European Data Protection Board". https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en (Erişim Tarihi: 21.01.2025)

Avusturya Ceza Kanunu, 1975. https://www.gesetze-im-internet.de/englisch_stgb/index.html (Erişim Tarihi: 10.06.2025)

Avusturya Cumhuriyeti Federal Hukuk Gazetesi. 5 inci madde. 15 Ocak 2019. https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2019_I_14/BGBLA_2019_I_14.html (Erişim Tarihi: 10.06.2025)

Avusturya Federal Anayasası, 1930. https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1930_1/ERV_1930_1.pdf (Erişim Tarihi: 10.06.2025)

Avusturya Federal Şansölyeliği (Bundeskanzleramt). *Bundesgesetz über den Schutz personenbezogener Daten*. https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf (Erişim Tarihi: 10.06.2025)

Avusturya Federal Şansölyeliği (Bundeskanzleramt). "Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger, Fassung vom 08.05.2025". https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1867_142/ERV_1867_142.pdf (Erişim Tarihi: 10.06.2025)

Avusturya Yayıncılık ve Telekomünikasyon Düzenleme Kurumu. "Rechte und Pflichten von Postdiensteanbietern". https://www.rtr.at/TKP/was_wir_tun/post/betreiberservice/rechte_pflichten.de.html#heading__heading_Hinterlegung_und_Ruecksendung_von_PostsendungenHinterlegung_und_Ruecksendung_von_Postsendungen (Erişim Tarihi: 10.06.2025)

Aydın, Serhat Erdem. *AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu*. Yüksek Lisans Tezi. İstanbul Üniversitesi. 2014. (Erişim Tarihi: 16.10.2024) https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=MJASJNR_mAeCWBdCkC1VOg&no=5TpxUKB7aPsxPlY5ImVyww (Erişim Tarihi: 16.10.2024)

Aygün, Nuri. *Elektronik Haberleşme Sektörüne İlişkin Avrupa Birliği e-Gizlilik Tüzüğü'nün Yenileme Çalışmaları Kapsamında İncelenmesi ve Ülkemiz İçin Öneriler*. Bilişim Uzmanlığı Tezi. Bilgi Teknolojileri ve İletişim Kurumu. 2022. (Yayımlanmamış Tez)

Ayözger Öngün, Çiğdem. *Kişisel Verilerin Korunması Hukuku (Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil.* İkinci Baskı. Beta Basım Yayım Dağıtım: 2019.

Balaban, Mahmut Furkan. *Elektronik Haberleşme Sektöründe İşlenen Kişisel Verilerin Korunması*. Ankara: Adalet Yayınevi, 2023.

Bayrakcı, Erdal ve Koçman, Mehmet Ali. "Bilgi Güvenliği ve Elektronik Harp". *Necmettin Erbakan Üniversitesi Siyasal Bilgiler Fakültesi Dergisi.* 5 (Özel Sayı). (2023): 184-206. https://dergipark.org.tr/tr/pub/neusbf/issue/81358/1383441 (Erişim Tarihi: 18.04.2025)

Bayram, Öykü Beste. "Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi". *Kişisel Verileri Koruma Dergisi*. Cilt: 4, Sayı: 1. (2022): 38-53. https://dergipark.org.tr/en/download/article-file/2432499 (Erişim Tarihi: 11.12.2024)

Becer, Begüm. *Kişisel Verilerin Korunması Kanunu Kapsamında Kişilik Haklarının Korunması*. Yüksek Lisans Tezi. Başkent Üniversitesi Sosyal Bilimler Enstitüsü. 2021. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi: 24.11.2024)

Belçika Adalet Bakanlığı (Service public fédéral Justice). "Arrêté royal relatif aux services postaux". 2022. https://www.ejustice.just.fgov.be/cgi_loi/article.pl?language=fr&lg_txt=f&type=&sort=&numac_search=&cn_search=2022031401&caller=eli&&view_numac=2022031401nl (Erişim Tarihi: 12.06.2025)

Belçika Adalet Bakanlığı (Service public fédéral Justice). "Loi Introduisant Le Livre II Du Code Pénal". 2024. https://www.ejustice.just.fgov.be/eli/loi/2024/02/29/2024002088/moniteur (Erişim Tarihi: 12.06.2025)

Belçika Anayasası, 1831. https://www.constituteproject.org/constitution/Belgium_2014 (Erişim Tarihi: 12.06.2025)

Belçika Veri Koruma Kurumu (Gegevensbeschermingsautoriteit). "Organisatie". https://www.gegevensbeschermingsautoriteit.be/burger/de-autoriteit/organisatie (Erişim Tarihi: 12.06.2025)

Berger, Cornelia. *Liberalisierung des Postmarktes in Europa Utl: Umsetzung der Europäischen Richtlinie auf nationaler und supranationaler Ebene und die Rolle der politischen Akteure*. 2012. https://core.ac.uk/download/pdf/11597737.pdf (Erişim Tarihi: 14.06.2025)

Biega, Asia J., Potash, Peter, Daumé III, Hal, Diaz, Fernando and Finck, Michèle. "Operationalizing the Legal Principle of Data Minimization for Personalization". *In Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR '20), July 25–30, 2020, Virtual Event. China, ACM, New York, NY, USA.* 2020. https://doi.org/10.1145/3397271.3401034 (Erişim Tarihi: 08.08.2024)

Bilgi Komiserliği Ofisi (ICO). "What is valid consent?". https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/ (Erişim Tarihi: 02.10.2024)

Bilgi Komiserliği Ofisi (ICO). "Vital Interests". https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/vital-interests/ (Erişim Tarihi: 17.10.2024)

Bilgi Teknolojileri ve İletişim Kurulu Kararı, 23.09.2019 günlü, 2019/DK-SRD/206 sayılı karar. https://www.btk.gov.tr/uploads/boarddecisions/posta-sektorunde-kullanici-haklarina-yonelik-bazi-hususlarda-duzenleyici-tedbirlerin-alinmasi/206-2019-web.pdf (Erişim Tarihi: 06.02.2025)

Bilgi Teknolojileri ve İletişim Kurulu Kararı, 03.08.2021 günlü ve 2021/DK-SRD/212 sayılı karar. https://www.btk.gov.tr/uploads/boarddecisions/2019-dk-srd-206-nolu-kurul-karari-nin-tadili-posta-sektorunde-kullanici-haklarina-yonelik-bazi-hususlarda-duzenleyici-tedbirlerin-alinmasi/212-2021-web.pdf (Erişim Tarihi: 06.02.2025)

Bilgi Teknolojileri ve İletişim Kurulu Kararı, 28.03.2023 günlü ve 2023/DK-SRD/115 sayılı karar. https://www.btk.gov.tr/uploads/boarddecisions/alternatif-teslimat-modellerinin-uygulanmasina-yonelik-usul-ve-esaslar/115-2023-web.pdf (Erişim Tarihi: 07.07.2024)

Bilgi Teknolojileri ve İletişim Kurumu. *Büyük Veri ve Yapay Zekâ Araştırma Raporu.* 2025. https://www.btk.gov.tr/uploads/announcements/buyuk-veri-ve-yapay-zeka-arastirma-raporu-yayimlandi/buyuk-veri-ve-yapay-zeka-arastirma-raporu.pdf (Erişim Tarihi: 05.07.2025)

Bilgi Teknolojileri ve İletişim Kurumu. *Türkiye Posta Sektörü Pazar Verileri Raporu*. 2023-1 https://www.btk.gov.tr/uploads/pages/posta-sektoru-pazar-verileri-raporu/pazarverileri-2023-1-rev.pdf (Erişim Tarihi: 09.06.2025)

Bilgi Teknolojileri ve İletişim Kurumu. *Türkiye Posta Sektörü Pazar Verileri Raporu*. 2023-2 https://www.btk.gov.tr/uploads/pages/posta-sektoru-pazar-verileri-raporu/2023-2-phs-raporu-666a9cd8e5297.pdf (Erişim Tarihi: 09.06.2025)

Bilgi Teknolojileri ve İletişim Kurumu. *Türkiye Posta Sektörü Pazar Verileri Raporu*. 2024-1 https://www.btk.gov.tr/uploads/pages/posta-sektoru-pazar-verileri-raporu/posta-hizmetleri-pazar-verileri-raporu-2024-1-karekodlu.pdf (Erişim Tarihi: 09.06.2025)

Bilgi Teknolojileri ve İletişim Kurumu. *Türkiye Posta Sektörü Pazar Verileri Raporu*. 2024-2. https://www.btk.gov.tr/uploads/pages/posta-sektoru-pazar-verileri-raporu/2024-2-phs-raporu-final-versiyon-karekod.pdf (Erişim Tarihi: 09.06.2025)

Bilir, Faruk. "Kişisel Verilerin Korunması Yönündeki Uygulama ve Hukuki Düzenlemelerin Ortaya Çıkışı". *Adalet Dergisi.* Sayı: 71. (Kasım 2023): 631-651. https://doi.org/10.57083/adaletdergisi.1391733 (Erişim Tarihi: 22.05.2025)

Birleşik Krallık Genel Veri Koruma Tüzüğü, 2021. https://www.legislation.gov.uk/uksi/2019/419/schedule/1/made (Erişim Tarihi: 22.06.2025)

Birleşik Krallık Haberleşme Otoritesi (Ofcom). "Conditions imposed on postal operators". 2024. https://www.ofcom.org.uk/post/market-performance/conditions (Erişim Tarihi: 22.06.2025)

Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği. *Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler*. 1990. https://www.refworld.org/pdfid/3ddcafaac.pdf (Erişim Tarihi: 19.05.2025)

Borgesius, Frederik Zuiderveen ve Steenbruggen, Wilfred. "The Right to Communications Confidentiality in Europe: Protecting Trust, Privacy, and Freedom of Expression". *Theoretical Inquiries in Law*. (2018). http://dx.doi.org/10.2139/ssrn.3152014 (Erişim Tarihi: 16.08.2024)

Borsenberger, Claire, Joram, Denis, Klargaard, Olaf and Regnard, Philippe. "Personal Data and Privacy Issues and Postal Operators Stand". *The Future of the Postal Sector in a Digital World.* (2016). https://link.springer.com/book/10.1007/978-3-319-24454-9 (Erişim Tarihi: 28.08.2024)

Büyüktanır, Muhammed Can. *Posta Sektöründe Birleşme-Satın Almalar (Yatay-Dikey Birleşmeler) ve Posta Sektörüne Etkileri*. Bilişim Uzmanlığı Tezi. Bilgi Teknolojileri ve İletişim Kurumu. 2022. (Yayımlanmamış Tez)

Bygrave, Lee A. "Privacy Protection in a Global Context-A Comparative Overview". *Scandinavian Studies in Law.* Cilt: 47. (2004): 319-348. https://lawpub.se/en/artikel/5543 (Erişim Tarihi: 12.11.2024)

Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english/post (Erişim Tarihi: 11.07.2024)

Christensen, Tanja Kammersgaard. "Pre-installed cameras in vehicles—New technology from a data protection law perspective". *Computer Law & Security Review.* Cilt 53. (2024). https://doi.org/10.1016/j.clsr.2024.105980

Creemers, Rogier. "China's emerging data protection framework". *Journal of Cybersecurity*. Cilt: 8, Sayı: 1. (2022) https://doi.org/10.1093/cybsec/tyac011

Čtvrtník, Mikuláš. *The Right to (Not) Be Forgotten, Right to Know, and Model of Four Categories of the Right to Be Forgotten*. Palgrave Macmillan, Cham, 2023. https://doi.org/10.1007/978-3-031-18667-7_5

Çakmak, Nurullah. *Posta Sektöründe Kullanıcı Düzenlemeleri: Ülke Uygulamaları ve Türkiye İçin Öneriler*, Bilişim Uzmanlığı Tezi. Bilgi Teknolojileri ve İletişim Kurumu. 2016. (Yayımlanmamış Tez)

Çekin, Mesut Serdar. *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*. On İki Levha Yayıncılık, 2020.

Çelikel, Serdar. "Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR'la Karşılaştırmalı Olarak İncelenmesi". *Uyuşmazlık Mahkemesi Dergisi*. Yıl 9, Sayı 17. (Haziran 2021): 161-190. https://doi.org/10.18771/mdergi.957894 (Erişim Tarihi: 04.02.2025)

Çelikel, Serdar. *Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri*. Doktora Tezi. Ankara Üniversitesi. 2021. https://www.proquest.com/openview/8ddd746329a3dacfbd4b508b6b9508b2/1?pq-origsite=gscholar&cbl=2026366&diss=y (Erişim Tarihi: 10.10.2024)

Çetin, Hakan. "Kişisel Veri Güvenliği ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi". *Akdeniz İ.İ.B.F. Dergisi*. Cilt: 29. (2014): 86-105. https://dergipark.org.tr/tr/pub/auiibfd/issue/32333/359291 (Erişim Tarihi: 07.04.2025)

Çin Halk Cumhuriyeti Anayasası, 2018. https://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e9499913.html (Erişim Tarihi: 15.05.2025)

Çin Halk Cumhuriyeti Kişisel Bilgilerin Korunması Kanunu (PIPL), 2021. http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559_2.htm (Erişim Tarihi: 15.05.2025)

Çin Halk Cumhuriyeti Posta Kanunu, 2009. https://www.lawinfochina.com/display.aspx?lib=law&id=7435&CGid=#menu7 Erişim Tarihi: 15.05.2025)

Danıştay 15. Hukuk Dairesi Kararı, E: 2014/4562. https://www.istabip.org.tr/icerik/biyometrikyurutmeyidurdurma.pdf (Erişim Tarihi: 18.01.2025)

De Hert, Paul ve Sajfert, Juraj. "The Fundamental Right To Personal Data Protection In Criminal Investigations And Proceedings: Framing Big Data Policing Through The Purpose Limitation and Data Minimisation Principles of The Directive (EU) 2016/680". *Brussels Privacy Hub Working Paper*. Cilt: 7, Sayı: 31. (2021). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4016491 (Erişim Tarihi: 26.09.2024)

De Hert, Paul, Papakonstantinou, Vagelis, Malgieri, Gianclaudio, Beslay, Laurent ve Sanchez, Ignacio. "The right to data portability in the GDPR: Towards user-centric interoperability of digital services". *Computer Law & Security Review*. Cilt: 34, Sayı: 2. (2018). https://doi.org/10.1016/j.clsr.2017.10.003 (Erişim Tarihi: 21.02.2025)

Demir, Kübra. "İşyeri Hekimlerinin İşçinin Sağlık Verilerinin İşlenmesinde Hukuki Statüsü ve Sorumluluğu". *Selçuk Hukuk Kongresi III*. ed: Doç. Dr. Alper Uyumaz-Dr. Öğr. Üyesi Hüseyin Tokat vd. (2024). https://selcuk.edu.tr/contents/hukuk/icerik/29360/Selc%CC%A7uk%20Hukuk%20Kongresi%20O%CC%88zet%20Kitab%C4%B1%202024_638632981698978745.pdf (Erişim Tarihi: 14.12.2024)

Develioğlu, Hüseyin Murat. *Avrupa Birliği Genel Veri Koruma Tüzüğü*. On İki Levha Yayıncılık, 2017.

DLA Piper. "Breach notification in Finland". 2023. https://www.dlapiperdataprotection.com/?t=breach-notification&c=FI#insight (Erişim tarihi: 03.06.2025)

DLA Piper. "Collection and Processing in Germany". 2025. https://www.dlapiperdataprotection.com/?t=collection-and-processing&c=DE (Erişim tarihi: 02.06.2025)

DLA Piper. "Collection and Processing the United Kingdom". 2025. https://www.dlapiperdataprotection.com/?t=collection-and-processing&c=GB#insight (Erişim tarihi: 05.06.2025)

DLA Piper. "Data protection laws in Finland". 2023. https://www.dlapiperdataprotection.com/?t=law&c=FI (Erişim tarihi: 03.06.2025)

DLA Piper. "Data protection officers in Belgium". 2024. https://www.dlapiperdataprotection.com/?t=data-protection-officers&c=BE#insight (Erişim tarihi: 04.06.2025)

DLA Piper. "Data protection officers in Finland". 2023. https://www.dlapiperdataprotection.com/?t=data-protection-officers&c=FI#insight (Erişim tarihi: 03.06.2025)

DLA Piper. "Definitions in Belgium". 2024. https://www.dlapiperdataprotection.com/?t=definitions&c=BE#insight (Erişim tarihi: 04.06.2025)

Doğan, Korcan ve Arslantekin, Sacit. "Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum". *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi.* Cilt: 56, Sayı: 1. (2016): 15-36. https://dergipark.org.tr/tr/download/article-file/2153482 (Erişim Tarihi: 05.01.2025)

Doğu, Ali Haydar. "Kişisel Verilerin Korunmasına Genel Bir Bakış", *Karadeniz Teknik Üniversitesi.* 2017. https://ceur-ws.org/Vol-2045/34_Bilisim_2017_paper_23.pdf (Erişim tarihi: 03.03.2025)

Dülber, Esranur. "*Türk Hukukunda Kişisel Verilerin Korunması Hakkı ve Basın Hürriyeti Çatışması"*. Yüksek Lisans Tezi. Hacettepe Üniversitesi. 2024. https://openaccess.hacettepe.edu.tr/xmlui/bitstream/handle/11655/34905/10374282.pdf?sequence=1&isAllowed=y (Erişim Tarihi: 03.07.2025)

Dülger, Murat Volkan. *Anayasa Mahkemesi'nin Kişisel Verilerin Korunması Kanunu'nun Konu Edildiği İptal Davası Kararına İlişkin Bir Değerlendirme.* 2021. http://dx.doi.org/10.2139/ssrn.3792249

Dülger, Murat Volkan. "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması". *Yaşar Hukuk Dergisi*. Cilt: 1, Sayı: 2. (2019).

Dülger, Murat Volkan. *Kişisel Verilerin Korunması Hukuku*. Hukuk Akademisi Yayınları, 2020.

Dülger, Murat Volkan. "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması". *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*. Cilt: 3, Sayı:2. (2016): 101-168. https://dergipark.org.tr/en/download/article-file/1102227 (Erişim Tarihi: 12.02.2025)

Dülger, Murat Volkan. *Sözleşme Gereğince Veri İşleme ile Açık Rıza Alınmasının Gerektiği Hallerin Karşılaştırılması: Uygulamadaki Karışıklığa İlişkin Çözüm Önerileri.* 2021. http://dx.doi.org/10.2139/ssrn.3792325

Dünya Posta Birliği (UPU). "Evrensel Posta Sözleşmesi". https://www.upu.int/en/universal-postal-union/about-upu/acts (Erişim Tarihi: 02.07.2025)

Dünya Posta Birliği (UPU). *Country Name: Austria*. https://www.upu.int/UPU/media/wwwUpuIntMemberSCentrePoliciesAndRegulationDataCollectionAndProtectionPolicies/database/autEn.pdf (Erişim Tarihi: 28.06.2025)

Dünya Posta Birliği (UPU). *Country Name: Belgium*. https://www.upu.int/UPU/media/wwwUpuIntMemberSCentrePoliciesAndRegulationDataCollectionAndProtectionPolicies/database/belEn.pdf (Erişim Tarihi: 28.06.2025)

Dünya Posta Birliği (UPU). *Country Name: Finland*. https://www.upu.int/UPU/media/wwwUpuIntMemberSCentrePoliciesAndRegulationDataCollectionAndProtectionPolicies/database/finEn.pdf (Erişim Tarihi: 28.06.2025)

Dünya Posta Birliği (UPU). *Country Name: Germany*. https://www.upu.int/UPU/media/wwwUpuIntMemberSCentrePoliciesAndRegulationDataCollectionAndProtectionPolicies/database/deuEn.pdf (Erişim Tarihi: 28.06.2025)

Dünya Posta Birliği (UPU). *Country Name: United States of America*. https://www.upu.int/UPU/media/wwwUpuIntMemberSCentrePoliciesAndRegulationDataCollectionAndProtectionPolicies/database/usaEn.pdf (Erişim Tarihi: 13.04.2025) (Erişim Tarihi: 28.06.2025)

Dünya Posta Birliği (UPU). *Multilateral Data Sharing Agreement, 2021, POC C 1 2021.1–Doc 2.Annex 1.Rev 1 Published in English 8.7.2021, 16.38 (Previous version published 23.3.2021, 09.44)*. https://www.upu.int/UPU/media/upu/files/postalSolutions/programmesAndServices/postalSupplyChain/SupplyChainIntegration/mdsa/upuMdsa_EN.docx (Erişim Tarihi: 09.09.2024)

Dünya Posta Birliği (UPU). *Multilateral Data Sharing Agreement - Signatory countries*. 2025. https://www.upu.int/getmedia/0c6e3d13-a660-47dd-ab2c-7d1a184eda82/upuMdsaSignatories.pdf (Erişim Tarihi: 13.04.2025)

Dünya Posta Birliği (UPU). "Postal Supply Chain Integration". 2022. https://www.upu.int/en/Postal-Solutions/Programmes-Services/Postal-Supply-Chain/Postal-Supply-Chain-Integration (Erişim Tarihi: 20.06.2025)

Dünya Posta Birliği (UPU). "UPU Terminology Database (TERMPOST)". https://www.upu.int/en/Universal-Postal-Union/About-UPU/TERMPOST (Erişim Tarihi: 13.01.2025)

Efe, Elçin Gökçen, *Yapay Zekâ Teknolojileri ve Rekabet İlişkisi: Elektronik Sektöründe Haberleşme Algoritmaların Kullanımının Rekabet Üzerindeki Olası Etkileri* (Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2024) (Yayımlanmamış Tez)

Egemen, Emir Efe. "Kişisel Verilerin İşlenmesinde "Doğru ve Gerektiğinde Güncel Olma" İlkesi ve Kişisel Verileri Koruma Kurulunun 2023/78 Sayılı Kararı". *Trabzon Üniversitesi Hukuk Fakültesi Dergisi*. Cilt: 1, Sayı: 1. (2023): 105–133. https://dergipark.org.tr/en/pub/truhfd/issue/80765/1345375 (Erişim Tarihi: 14.10.2024)

Ekin, Beste. *Kişisel Verilerin Korunması ve Rekabet Hukuku Boyutuyla Büyük Veri.* Yüksek Lisans Tezi. İhsan Doğramacı Bilkent Üniversitesi. 2020. https://www.proquest.com/openview/db0b0004e485fe6215f8982c62f579ae/1?pq-origsite=gscholar&cbl=2026366&diss=y (Erişim Tarihi: 10.02.2025)

Ekmekçi, Ömer, Yücedağ, Nafiye, Akkanat Öztürk, Elif Beyza ve Aşıkoğlu, Şehriban İpek. "Ceza Muhakemesi Kanunu ile Bazı Kanunlarda ve 659 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılmasına Dair Kanun Teklifi ile 6698 Sayılı Kanun'da Yapılan Değişiklikler". 2024. https://blog.lexpera.com.tr/ceza-muhakemesi-kanunu-ile-bazi-kanunlarda-ve-659-sayili-kanun-hukmunde-kararnamede-degisiklik-yapilmasina-dair-kanun-teklifi-ile-6698-sayili-kanunda-yapilan-degisiklikler/ (Erişim Tarihi: 20.02.2025)

Ekmekçi, Ömer, Yücedağ, Nafiye, Akkanat Öztürk, Elif Beyza ve Aşıkoğlu, Şehriban İpek. *Kişisel Verilerin Korunması Hukuku*. İstanbul Üniversitesi Hukuk Fakültesi Ders Kitapları Dizisi. İstanbul: On İki Levha Yayıncılık, 2024.

5809 sayılı Elektronik Haberleşme Kanunu, 2008. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5809&MevzuatTur=1&MevzuatTertip=5 (Erişim Tarihi: 04.06.2025)

Erdinç, Göksu Hazar. "Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi". *Kişisel Verileri Koruma Dergisi.* Cilt: 2, Sayı: 1. (Haziran 2020): 1-19. https://dergipark.org.tr/tr/pub/kvkd/issue/55487/738174 (Erişim Tarihi: 08.09.2024)

Ersoy Kekevi, Çiçek. *Genel Kavramlar, Kişisel Verilerin Korunmasına Akademik Bakış-KVKK Akademi Derleme Çalışması*. ed. Pınar Çağlayan Aksoy, Hüseyin Can Aksoy. Ankara: Ütopya Grafik, 2023. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0cd33e96-77cf-4989-b29b-d331af6a463f.pdf (Erişim Tarihi: 22.11.2024)

Esenyel Hanaz, Fatma. "Çevrimiçi Eğitimde Üniversite Öğrencilerinin Kişisel Verilerinin İşlenmesinin Hukuki Sebepleri". *Türkiye Barolar Birliği Dergisi.* Sayı: 155. (2021): 424-425 https://tbbdergisi.barobirlik.org.tr/Dergi/Dergi155/8/ (Erişim Tarihi: 27.10.2024)

Eser, Gülşen. *Posta Hizmetleri Sektöründe Yapılan Reformlar, Posta Hizmetlerinin Serbestleştirilmesi "PTT AŞ Örneği"*. Yüksek Lisans Tezi. İzmir Üniversitesi. 2014. https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=pBJAK8CGmJSUxPy9Qemuow&no=S2SQo_R8p1KxAjgCUgydZA (Erişim Tarihi: 16.12.2024)

Finlandiya Anayasası, 1999. https://www.finlex.fi/api/media/statute-foreign-language-translation/240375/mainPdf/main.pdf?timestamp=1999-06-11T00%3A00%3A00.000Z (Erişim Tarihi: 28.05.2025)

Finlandiya Ceza Kanunu, 1889. https://www.finlex.fi/fi/lainsaadanto/1889/39-001 (Erişim Tarihi: 28.05.2025)

Finlandiya Posta Kanunu, 2011. https://www.finlex.fi/api/media/statute-foreign-language-translation/128621/mainPdf/main.pdf?timestamp=2011-04-29T00%3A00%3A00.000Z (Erişim tarihi: 28.05.2025)

Finlandiya Veri Koruma Ombudsmanlığı. "Elektronik posta kutusu ve hizmetin etkinleştirilmesine ilişkin bilgilendirme amacıyla sözleşmeye dayalı kişisel verilerin işlenmesi". 2024. https://finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2024/2363 (Erişim Tarihi: 28.05.2025)

Finlandiya Veri Koruma Yasası, 2019. https://finlex.fi/api/media/statute-foreign-language-translation/46200/mainPdf/main.pdf?timestamp=2018-12-05T00%3A00%3A00.000Z (Erişim tarihi: 28.05.2025)

Gayretli, Zehra. *Avrupa İnsan Hakları Mahkemesi (AİHM) ve Anayasa Mahkemesi (AYM) Tedbir Kararlarının Karşılaştırmalı Olarak Değerlendirilmesi*. Yüksek Lisans Tezi. Ankara Üniversitesi Sosyal Bilimler Enstitüsü. 2020. https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=viesM_GyX_0ajVGbGHpfdQ&no=u17eVOppr-YKPzm3NkmKMw (Erişim Tarihi: 16.04.2025)

GDPR Text. "Article 6 GDPR: Lawfulness of processing". 2019. https://gdpr-text.com/read/article-6/#recital_gdpr-a-06_1-1c (Erişim Tarihi: 17.10.2024)

Genel Veri Koruma Tüzüğü (General Data Protection Regulation, GDPR). https://gdpr-info.eu/ (Erişim Tarihi: 14.06.2024)

Ghalumyan, Armen. "Fine on Posti for violation of data protection regulations". Cullen International. 2020. https://www.cullen-international.com/client/site/documents/FLPOFI20200001 (Erişim Tarihi: 10.04.2025)

Goicovici, Juanita. *Granularity And Specificity Of Consent And Implications Thereof For The Data Controller In The Light Of The Principle Of 'Purpose Limitation'*. 2022. https://hrcak.srce.hr/file/424613 (Erişim Tarihi: 21.04.2024)

Greenley-Giudici, Annie. "What's the Difference Between UK Data Protection Act & GDPR?". TrustArc. https://trustarc.com/resource/uk-data-protection-act-gdpr/ (Erişim Tarihi: 27.05.2025)

Gündüz, Muhammed Zekeriya ve Daş, Resul. "Kişisel Siber Güvenlik Yaklaşımlarının Değerlendirilmesi". *DÜMF MD*. Cilt: 13, Sayı: 3. (2022): 429–438. https://doi.org/10.24012/dumf.1122997 (Erişim Tarihi: 10.04.2025)

Gürol, Canbek ve Sağıroğlu, Şeref. "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme". Politeknik Dergisi. Cilt: 9, Sayı: 3. (2006). https://dergipark.org.tr/tr/pub/politeknik/issue/33021/367110 (Erişim Tarihi: 12.04.2025)

Halawi, Leila ve Makwana, Alpesh. "The GDPR and UK GDPR and its impact on US academic institutions". *Issues in Information Systems*. Cilt: 24, Sayı: 2. (2023): 232-241. https://doi.org/10.48009/2_iis_2023_120 (Erişim Tarihi: 21.04.2025)

Hillebrand, Annette vd. *Technology and change in postal services impacts on consumers.* WIK-Consult, 2016.

Hollanda Yargı Konseyi (de Rechtspraak) Kararı. InstantieRechtbank Amsterdam, 11.03.2021 günlü, C/13/689705 sayılı Ola's Driver App Kararı. https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBAMS:2021:1019 (Erişim Tarihi: 05.04.2025)

Hoşnut, Yasime. "Uluslararası Düzenlemelerde ve Türkiye'de Kişisel Verilerin Korunması". *Yeni Medya Hakemlik, Akademi E- Dergi*. Sayı: 6. (2019): 32-45. https://dergipark.org.tr/tr/pub/yenimedya/issue/56862/798023 (Erişim Tarihi: 12.11.2024)

Huysmans, Vincent. "6 of the Most Infamous Data Breaches in Belgian History". 2025. https://infofarm.be/6-of-the-most-infamous-data-breaches-in-belgian-history/ (Erişim Tarihi: 15.06.2025)

IBIS World. "Postal & Courier Activities in Austria - Market Size, Industry Analysis, Trends and Forecasts (2025-2030)". 2025. https://www.ibisworld.com/austria/industry/postal-courier-activities/200069/#IndustryStatisticsAndTrends (Erişim tarihi: 28.05.2025)

İyigün, İsmail. "Lojistik ve Tedarik Zinciri Süreçlerinde Büyük Veri Kullanımı ve Etkilerinin Analizi". *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi*. 2019. https://dergipark.org.tr/tr/download/article-file/847106 (Erişim tarihi: 05.07.2025)

Jasserand, Catherine. *Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?.* 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230347 (Erişim Tarihi: 07.08.2025)

Kahn, David. *The Codebreakers: The Comprehensive History Of Secret Communication From Ancient Times To The İnternet*. 1996. https://archive.org/details/2.thecodebreakersthecomprehensivehistoryofsecretcommunicationfromancienttimestotheinternet/page/11/mode/2up (Erişim Tarihi: 09.08.2024)

Kangal, Zeynel T. *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*. İstanbul: On İki Levha Yayıncılık, 2019.

Karabay, Barış ve Ulaş, Mustafa. "Büyük Veri İşlemede Yaygın Kullanılan Araçların Karşılaştırılması". *8th International Advanced Technologies Conference*. 2017.

Karakuş, Helin. *İş İlişkisinde Kişisel Verilerin Korunması.* Yüksek Lisans Tezi. Hacettepe Üniversitesi. 2024. https://openaccess.hacettepe.edu.tr/handle/11655/34506 (Erişim Tarihi: 09.03.2025)

Kaya, Cemil. "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi". *Journal of Istanbul University Law Faculty.* Cilt: 69, Sayı: 1-2. (2011): 317-34. https://dergipark.org.tr/tr/pub/iuhfm/issue/9185/115031#article_cite (Erişim Tarihi: 25.07.2024)

Kaya, Cemil. "*Kişisel Verilerin Korunması Hukuku ve Bilgi Edinme Hukuku: Çeşitli Açılardan Bakış"*. İstanbul: On İki Levha Yayıncılık, 2023.

Kaya, Mehmet Bedii. "*KVKK Reformu: 2024 Değişiklikleri"*. 2024. https://mbkaya.com/hukuk/kvkk-reformu.pdf (Erişim Tarihi: 10.05.2025)

Kaya, Mehmet Bedii. *"Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verilebilirlik İlkesi"*. İstanbul Hukuk Mecmuası Cilt: 78, Sayı: 4 (2021): 1859-97, https://doi.org/10.26650/mecmua.2020.78.4.0005 (Erişim Tarihi: 05.07.2025)

Kılınç, Doğan. "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması". *Ankara Üniversitesi Hukuk Fakültesi Dergisi.* 61, Sayı: 3. (2012): 1089-1172. https://doi.org/10.1501/Hukfak_0000001684 (Erişim Tarihi: 24.02.2025)

King, Hazel. "Austrian Post delivers record 508 million parcels in 2024". 2025. https://www.parcelandpostaltechnologyinternational.com/news/parcels/austrian-post-delivers-record-508-million-parcels-in-2024.html (Erişim Tarihi: 28.05.2025)

Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi. 1976. https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020093321bm_05.pdf (Erişim Tarihi: 17.06.2025)

Kişisel Verileri Koruma Kurulu Kararı. 31.01.2018 günlü, 2018/10 sayılı karar. https://www.kvkk.gov.tr/Icerik/4110/2018-10 (Erişim Tarihi: 17.05.2025)

Kişisel Verileri Koruma Kurulu Kararı. 19.07.2018 günlü, 2018/87 sayılı karar. https://www.kvkk.gov.tr/Icerik/5271/2018-87 (Erişim Tarihi: 14.04.2025)

Kişisel Verileri Koruma Kurulu Kararı. 25.03.2019 günlü, 2019/81 sayılı karar. https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 (Erişim Tarihi: 06.04.2025)

Kişisel Verileri Koruma Kurulu Kararı. 31.05.2019 günlü, 2019/165 sayılı karar. https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 (Erişim Tarihi: 06.04.2025)

Kişisel Verileri Koruma Kurulu Kararı. 01.10.2019 günlü, 2019/294 sayılı karar. https://kvkk.gov.tr/Icerik/6556/2019-294 (Erişim Tarihi: 18.01.2025)

Kişisel Verileri Koruma Kurulu Kararı. 30.01.2020 günlü, 2020/71 sayılı karar. https://www.kvkk.gov.tr/Icerik/6874/2020-71 (Erişim Tarihi: 27.10.2024)

Kişisel Verileri Koruma Kurulu Kararı. 16.04.2020 günlü, 2020/286 sayılı karar. https://www.kvkk.gov.tr/Icerik/6763/2020-286 (Erişim Tarihi: 10.04.2025)

Kişisel Verileri Koruma Kurulu Kararı. 16.06.2020 günlü, 2020/463 sayılı karar. https://www.kvkk.gov.tr/Icerik/7030/2020-463 (Erişim tarihi: 01.07.2025)

Kişisel Verileri Koruma Kurulu Kararı. 27.08.2020 günlü, 2020/649 sayılı karar. https://www.kvkk.gov.tr/Icerik/6815/2020-649 (Erişim tarihi: 08.01.2025)

Kişisel Verileri Koruma Kurulu Kararı. 22.06.2021 günlü, 2021/603 sayılı karar. https://www.kvkk.gov.tr/Icerik/7131/2021-603 (Erişim Tarihi: 21.01.2025)

Kişisel Verileri Koruma Kurulu Kararı. 26.08.2021 günlü, 2021/875 sayılı karar. https://kvkk.gov.tr/Icerik/7042/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-MNG-Kargo-Yurtici-ve-Yurtdisi-Tasimacilik-AS (Erişim Tarihi: 01.06.2025)

Kişisel Verileri Koruma Kurulu Kararı. 30.09.2021 günlü, 2021/993 sayılı karar. https://www.kvkk.gov.tr/Icerik/7144/2021-993 (Erişim Tarihi: 24.06.2024)

Kişisel Verileri Koruma Kurulu Kararı. 02.12.2021 günlü, 2021/1217 sayılı karar. https://www.kvkk.gov.tr/Icerik/7271/2021-1217 (Erişim Tarihi: 22.06.2024)

Kişisel Verileri Koruma Kurulu Kararı. 23.12.2021 günlü, 2021/1304 sayılı "Araç kiralama sektöründeki kara liste uygulamaları hakkında İlke Kararı) konulu karar. https://www.resmigazete.gov.tr/eskiler/2022/01/20220120-10.pdf (Erişim Tarihi: 27.10.2024)

Kişisel Verileri Koruma Kurulu Kararı. 24.03.2022 günlü, 2022/277 sayılı "İlgili kişiye ait kişisel verileri içeren bir kargo paketinin üçüncü bir şahsın eline geçmesi" konulu karar. https://www.kvkk.gov.tr/Icerik/7559/2022-277 (Erişim Tarihi: 19.11.2024)

Kişisel Verileri Koruma Kurulu Kararı. 01.09.2022 günlü, 2022/891 sayılı karar. https://www.kvkk.gov.tr/Icerik/7435/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Posta-ve-Telgraf-Teskilati-Biriktirme-ve-Yardim-Sandigi (Erişim Tarihi: 01.06.2025)

Kişisel Verileri Koruma Kurulu Kararı. 05.01.2023 günlü, 2023/4 sayılı karar. https://www.kvkk.gov.tr/Icerik/7598/2023-4 (Erişim Tarihi: 20.02.2025)

Kişisel Verileri Koruma Kurulu Kararı. 18.05.2023 günlü, 2023/845 sayılı karar. https://www.kvkk.gov.tr/Icerik/7759/2023-845 (Erişim Tarihi: 20.02.2025)

Kişisel Verileri Koruma Kurulu Kararı. 13.02.2025 günlü, 2025/353 sayılı karar. https://www.kvkk.gov.tr/Icerik/8180/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Asilkar-Hizli-Kargo-Tasimacilik-Ticaret-Anonim-Sirketi (Erişim Tarihi: 01.06.2025)

Kişisel Verileri Koruma Kurulu Kararı, 10.06.2025 günlü, 2025/1072 sayılı ilke kararı. https://kvkk.gov.tr/Icerik/8338/2025-1072 (Erişim Tarihi: 01.07.2025)

Kişisel Verileri Koruma Kurumu. *6698 Sayılı Kanunda Yer Alan Temel Kavramlar*. https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun'da-Yer-Alan-Temel-Kavramlar (Erişim Tarihi: 14.12.2024)

Kişisel Verileri Koruma Kurumu. "6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar". *KVKK Yayınları.* No: 57. (2025). https://www.kvkk.gov.tr/Icerik/6722/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Dogru-Bilinen-Yanlislar (Erişim Tarihi: 15.01.2025)

Kişisel Verileri Koruma Kurumu. *Açık Rıza*. https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf (Erişim Tarihi: 02.10.2024)

Kişisel Verileri Koruma Kurumu. "Açık Rıza Alırken Dikkat Edilecek Hususlar". https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar (Erişim Tarihi: 03.10.2024)

Kişisel Verileri Koruma Kurumu. "Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu Duyurusu". 2020. https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU (Erişim Tarihi: 14.04.2025)

Kişisel Verileri Koruma Kurumu. *Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi*. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf (Erişim Tarihi: 14.04.2025)

Kişisel Verileri Koruma Kurumu. *Kanun Kapsamındaki Hak ve Yükümlülükler*. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/8662692a-80ff-49a8-9ce9-7aca5b69ccd7.pdf (Erişim Tarihi: 14.04.2025)

Kişisel Verileri Koruma Kurumu. *Kanunlarda Öngörülme Kişisel Veri İşleme Şartına İlişkin 05.08.2024 tarihli Bilgi Notu*. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/8d119dab-5886-4300-bd13-4eaf9bf15ea0.pdf (Erişim tarihi: 10.10.2024)

Kişisel Verileri Koruma Kurumu. "Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)". *KVKK Yayınları*. (Nisan 2025). https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf (Erişim Tarihi: 17.05.2025)

Kişisel Verileri Koruma Kurumu. "Kişisel Veri Güvenliği Rehberinde geçen "personel gizlilik sözleşmesi" imzalatılmasının 657 sayılı Devlet Memurları Kanununa tabii olarak çalışanlar için gerekli olup olmadığı ile ilgili Kişisel Verileri Koruma Kurulunun 26.12.2019 tarihli ve 2019/393 sayılı Karar Özeti". https://kvkk.gov.tr/Icerik/6868/2019-393 (Erişim Tarihi: 17.05.2025)

Kişisel Verileri Koruma Kurumu. *Kişisel Veri İhlali Bildirim Formu Kılavuzu.* https://kvkk.gov.tr/SharedFolderServer/CMSFiles/369d954a-aaee-44ca-9ca6-105e8b4102f9.pdf (Erişim tarihi: 17.05.2025)

Kişisel Verileri Koruma Kurumu. "Kişisel Verileri Koruma Kurulu Kararları 2018-2021". *KVKK Yayınları.* No: 39. (2021): 323-326. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/1d7c2f99-be2c-4971-a304-0a1eb3586bd1.pdf https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/1d7c2f99-be2c-4971-a304-0a1eb3586bd1.pdf (Erişim Tarihi: 16.08.2025)

Kişisel Verileri Koruma Kurumu. *Kişisel Verilerin İşlenme Şartları*. https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari (Erişim Tarihi: 29.09.2024)

Kişisel Verileri Koruma Kurumu. *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler*. https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler (Erişim Tarihi: 08.09.2024)

Kişisel Verileri Koruma Kurumu. *Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler*. https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler (Erişim Tarihi: 18.11.2024)

Kişisel Verileri Koruma Kurumu. *Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular*. 2025. https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular (Erişim Tarihi: 19.05.2025)

Kişisel Verileri Koruma Kurumu. *Kişisel Verilerin Korunması Kanunu ve Uygulaması*. 2024.https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf (Erişim Tarihi: 10.02.2025)

Kişisel Verileri Koruma Kurumu. "Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi No: 1". *KVKK Yayınları.* 2019. https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf (Erişim Tarihi 24.11.2024)

Kişisel Verileri Koruma Kurumu. "Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü". *KVKK Yayınları*. (2025). https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/062384e3-d18c-4c38-b108-3a7a2a28e849.pdf (Erişim Tarihi: 20.05.2025)

Kişisel Verileri Koruma Kurumu. *Özel Nitelikli Kişisel verilerin İşlenmesine İlişkin Rehber*. 2025. https://www.kvkk.gov.tr/Icerik/8184/Ozel-Nitelikli-Kisisel-Verilerin-Islenmesine-Iliskin-Rehber (Erişim tarihi: 12.03.2025)

Kişisel Verileri Koruma Kurumu. "Veri Sorumlusu Kimdir?". https://www.kvkk.gov.tr/Icerik/2032/Veri-Sorumlusu-Kimdir#:~:text=Kanuna%20g%C3%B6re%20veri%20sorumlusu%20ki%C5%9Fisel,yap%C4%B1laca%C4%9F%C4%B1%20sorular%C4%B1n%C4%B1n%20cevab%C4%B1n%C4%B1%20verecek%20ki%C5%9Fidir (Erişim Tarihi 01.08.2024)

Kişisel Verileri Koruma Kurumu. *Veri Sorumlusu ve Veri İşleyen*. https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen (Erişim Tarihi: 13.01.2025)

Kişisel Verileri Koruma Kurumu. "Yurt Dışına Aktarım". 2025. https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim (Erişim Tarihi: 22.09.2025)

Kişisel Verileri Koruma Kurumu Bülteni. "Genel Olarak Kişisel Veri Güvenliğine İlişkin Tedbirler". *Kişisel Verilerin Korunması ve Siber Güvenlik*. Sayı: 6. (Ağustos- Kasım 2024). https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/9a224548-1876-4065-aba8-24a0acb5bff6.pdf (Erişim Tarihi: 15.05.2025)

Kişisel Verilerin Korunması Kanunu (KVKK). https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5 (Erişim Tarihi: 05.06.2024)

Koca, Mahmut ve Üzülmez, İlhan. "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)". *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Prof. Dr. Durmuş TEZCAN'a Armağan*. Cilt 21, Özel S. (2019): 69-93. https://hukuk.deu.edu.tr/wp-content/uploads/2019/09/MAHMUT-KOCA-ILHAN-UZULMEZ.pdf (Erişim Tarihi: 14.08.2024)

Kuntoğlu, Ömer Faruk. "Elektronik Ticarette Kişisel Verilerin Korunması". *Bilişim Hukuku Dergisi.* 2021. https://dergipark.org.tr/tr/pub/bilisimhukukudergisi/issue/63317/747224 (Erişim Tarihi: 12.06.2024)

Kuyumcu, Seda. *6698 Sayılı Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması ve Aktarım Koşullarının Değerlendirilmesi*. Yüksek Lisans Tezi. Galatasaray Üniversitesi. 2024. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp (Erişim Tarihi: 03.07.2024)

Küzeci, Elif. *Kişisel Verilerin Korunması*. 4. Baskı. İstanbul: On İki Levha Yayıncılık, 2020.

Lambert, Paul. *Understanding the New European Data Protection Rules*. CRC Press, 2018. https://www.taylorfrancis.com/books/mono/10.1201/9781315115269/understanding-new-european-data-protection-rules-paul-lambert (Erişim Tarihi: 10.06.2024)

Malgieri, Gianclaudio. "The Concept of Fairness in the GDPR: : A Linguistic and Contextual Interpretation". *FAT* '20: Conference on Fairness, Accountability, and Transparency*. 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3517264 (Erişim Tarihi: 08.09.2024)

Mattera, Marianna. "Fines for Data Protection Infringements". 2025. https://www.cullen-international.com/client/site/documents/CTECEU20230033 (Erişim Tarihi: 19.06.2025)

McKinney, Richard J. *A Research Guide to the Federal Register and the Code of Federal Regulations*. 2016. https://www.llsdc.org/fr-cfr-research-guide (Erişim Tarihi: 14.06.2025)

MNG Kargo. "Genel Aydınlatma Metni". https://www.mngkargo.com.tr/genel-aydinlatma-metni (Erişim Tarihi: 14.01.2025)

OECD. "Members and Partners". https://www.oecd.org/en/about/members-partners.html (Erişim Tarihi: 11.11.2024)

OECD. *Promoting Competition in Postal Services*. 1999. https://www.oecd.org/en/publications/promoting-competition-in-postal-services_26e00ffc-en.html (Erişim Tarihi: 01.08.2024)

OECD Legal Instruments. "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data". 2013. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (Erişim Tarihi: 11.11.2024)

Oğuz, Habip. "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum". *Uyuşmazlık Mahkemesi Dergisi*. Sayı: 3. (2013): 1-38. https://dergipark.org.tr/en/pub/mdergi/issue/16883/175778 (Erişim Tarihi: 20.04.2025)

Oktay, Gonca. *Kişilik Haklarının Korunması.* Yüksek Lisans Tezi. Akdeniz Üniversitesi. 2011. https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=ak0nG_cWpCGF8hCAGlUfqQ&no=DpvSnbVFKQ11B_5trzzXoA (Erişim Tarihi: 05.07.2024)

Oladimeji, Peter. "Germany's data privacy protection laws: Everything you need to know". 2023. https://www.didomi.io/blog/germany-data-privacy-protection-laws-everything-you-need-to-know (Erişim Tarihi: 04.05.2025)

Otsetova, Anna. *"Digital Transformation of Postal Operators – Challenges and Perspectives".* Department of Management in Communications, University of Telecommunications and Post, Sofia, 2019: 1 https://tac.uniza.sk/artkey/tac-201902-0004_digital-transformation-of-postal-operators-challenges-and-perspectives.php (Erişim Tarihi: 02.06.2025)

Özbaşı, Sezen. *Kişisel Sağlık Verilerinin İşlenmesinde Açık Rıza Kavramı*. Yüksek Lisans Tezi. Hacettepe Üniversitesi. 2024. https://openaccess.hacettepe.edu.tr/xmlui/handle/11655/34613 (Erişim Tarihi: (07.02.2025)

Özcan, Göknil. *Bankacılık İş ve İşlemlerinde Kişisel Verilerin Korunması*. Yüksek Lisans Tezi. İstanbul Üniversitesi. 2019. https://nek.istanbul.edu.tr/ekos/TEZ/ET000709.pdf (Erişim Tarihi: 27.12.2024)

Özcan, Mehmet. *Posta Hizmetlerinin Düzenlenmesi, Uluslararası Kuruluşlar ve AB Müktesabatı Çerçevesinde Türkiye'deki Durumun İncelenmesi ve Öneriler.* Bilişim Uzmanlığı Tezi. Bilgi Teknolojileri ve İletişim Kurumu. 2011. https://www.btk.gov.tr/uploads/thesis/mehmet-ozcan.pdf (Erişim Tarihi: 14.07.2025)

Özdemir, Hayrunnisa. *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*. Ankara: Seçkin Yayıncılık, 2009.

Özdemir Koçar, Gubse. "Tüketici-Çevrimiçi Pazar Yerleri-Kargo Şirketleri Üçgeninde Kişisel Veri İşleme Faaliyetleri". *Kişisel Verileri Koruma Dergisi*. Cilt: 6, Sayı: 2. (2024): 92-116. https://dergipark.org.tr/tr/pub/kvkd/issue/88721/1577978 (Erişim Tarihi: 16.04.2025)

Özelçi, M. Aytaç. "Posta Hizmetleri Sektöründe Uygulanan İdari Yaptırımların Bağlı Olduğu Hukuksal Düzen". *İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi.* Cilt: 20, Sayı: 1. (Ocak 2021): 175-248. https://www.jurix.com.tr/article/22117?u=0&c=0 (Erişim Tarihi: 25.06.2025)

Özkan, İsmail. "Data Protection Principles: The 7 Principles Of GDPR Explained". 2024. https://www.cyberpilot.io/cyberpilot-blog/data-protection-principles-the-7-principles-of-gdpr-explained/# (Erişim Tarihi: 08.08.2024)

Özkan, Oğulcan. *Kişisel Verilerin Korunması.* Yüksek Lisans Tezi. Ankara Üniversitesi. 2020. https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=Fa6iDGNe_JFw7EiflIyQxg&no=L_LqELk7VAgugHHziEvuSg (Erişim tarihi: 23.11.2024)

Özkaya, Ömer ve Toprak, İbrahim. "Türkiye'de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi". *MANAS Sosyal Araştırmalar Dergisi* Cilt: 11, Sayı: 3. (2022): 1291-1305. https://doi.org/10.33206/mjss.1098009 (Erişim Tarihi: 30.05.2024)

Özsoy, Özlem. *Kişisel Verilerin Korunması Hukukunda İlgili Kişinin Hakları*. Yüksek Lisans Tezi. Dokuz Eylül Üniversitesi. 2024.

Öztan, Bilge. *Medeni Hukukun Temel Kavramları*. 38. Bası. Ankara: Turhan Kitabevi, 2013.

Palmer, Annie. "US Postal Service admits a 'catastrophic' flaw in its system exposed exactly what mail 60 million users were getting delivered". DailyMail. 2018. https://www.dailymail.co.uk/sciencetech/article-6430837/US-Postal-Service-admits-flaw-exposed-exactly-60-million-users-getting-delivered.html (Erişim tarihi: 03.06.2025)

Papanikolaou, Aikaterina, Varvarousi, Eleni, ve Gavala, Eirini. *Postal sector digitalisation: security and vulnerabilities*. 2024. https://dx.doi.org/10.1504/IJASS.2024.10064596 (Erişim Tarihi: 20.05.2025)

Parcu, Pier Luigi and Silvestri, Virginia. *Lessons from the Postal Sector to Telecommunications and Vice Versa*. Springer, 2017. https://core.ac.uk/download/pdf/156757432.pdf (Erişim Tarihi: 21.03.2025)

Paşaoğlu, Cengiz ve Cevheroğlu, Emel. "Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması". *Bilişim Teknolojileri Dergisi*. Cilt: 13, Sayı: 2. (2020). https://doi.org/10.17671/gazibtd.559235 (Erişim Tarihi: 21.11.2024)

Petkauskas, Vilius. "Royal Mail customer data stolen in massive attack, hackers claim". Cybernews. 2025. https://cybernews.com/security/royal-mail-data-breach-hackers-claim/ (Erişim Tarihi: 01.07.2025)

Posta Hizmetleri Kanunu, 2013. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6475&MevzuatTur=1&MevzuatTertip=5 (Erişim Tarihi: 19.11.2024)

Posta Hizmetlerinin Sunulmasına İlişkin Yönetmelik, 2014. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19739&MevzuatTur=7&MevzuatTertip=5 (Erişim Tarihi: 20.05.2025)

Posta Sektörüne İlişkin Yetkilendirme Yönetmeliği, 2014. https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=19740&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5 (Erişim Tarihi: 30.03.2025)

Payaslı, Naci Soner. *Avrupa Birliği (AB) 2022/2555 Sayılı Birlik Genelinde Yüksek Düzeyde Ortak Siber Güvenlik Tedbirlerine İlişkin Direktifin (NIS2 Direktifi) İncelenmesi ve İlgili Direktif Kapsamında Ülkemiz Elektronik Haberleşme Sektörü Mevzuatının Değerlendirilmesi*. Bilişim Uzmanlığı Tezi. Bilgi Teknolojileri ve İletişim Kurumu. 2023. https://www.btk.gov.tr/uploads/thesis/naci-soner-payasli-karartilmis-hali.pdf (Erişim Tarihi: 14.05.2025)

Popelier, Patricia ve Van De Heyning, Catherine. "Procedural Rationality: Giving Teeth to the Proportionality Analysis". *European Constitutional Law Review*. Cilt: 9, Sayı: 2. (2013): 230 – 262. https://doi.org/10.1017/S1574019612001137 (Erişim Tarihi: 24.04.2025)

Rekabet Kurumu. *Dijital Dönüşümün Rekabet Hukukuna Yansımaları*. 2023. https://www.rekabet.gov.tr/Dosya/dijital-piyasalar-calisma-metni.pdf (Erişim Tarihi: 26.09.2024)

Resmî Gazete. *24.01.2017 tarih 2017/9756 sayılı Bakanlar Kurulu Kararı*. 2017. https://www.resmigazete.gov.tr/eskiler/2017/02/20170205M1-1.pdf (Erişim Tarihi: 01.02.2025)

Saat, Dursun. "Kişisel Verilerin Korunması Kanunu'nda Öngörülen Meşru Menfaat Kavramının Ticaret Şirketleri Bakımından Değerlendirilmesi". *Anadolu Üniversitesi Hukuk Fakültesi Dergisi.* Cilt: 10, Sayı: 2. (2024). https://dergipark.org.tr/tr/pub/andhd/issue/86405/1491304 (Erişim Tarihi: 21.09.2024)

Sayan, Ömer Fatih. *Karşılaştırmalı Hukukta Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması ve Veri Güvenliği*, Doktora Tezi. Ankara Yıldırım Beyazıt Üniversitesi. 2023.

Scott, Paul F. *National Security, Data Protection, and Data Sharing after the Data Protection Act 2018*. 2019. http://dx.doi.org/10.2139/ssrn.3340543 (Erişim Tarihi: 14.06.2025)

Selek, Ozan. "Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması". *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*. Cilt: 21, Sayı: 2. (2019): 911-951. https://doi.org/10.33717/deuhfd.646330. (Erişim Tarihi: 19.06.2025)

Sevindi, Nur Sena ve Ordu, Muhammet Emin. "AB ve Türk Hukukunda Veri İhlalinin Tespiti ve Bildirim Süresinin Karşılaştırmalı Değerlendirmesi". *Kişisel Verileri Koruma Dergisi*. Cilt: 5, Sayı: 1. (2023): 12-22. https://dergipark.org.tr/tr/download/article-file/3116868 (Erişim Tarihi: 17.01.2025)

Sheedy, Caroline ve Moloney, Maria. *Leveraging the Postal Infrastructure for the Authentication of Individuals Towards an Online Government Service Provision*. 2013. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2245054 (Erişim Tarihi: 01.07.2024)

Surblyte, Gintare. *Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy*. 2016. http://dx.doi.org/10.2139/ssrn.2752989 (Erişim Tarihi: 19.06.2024)

Şahin, Osman. *Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğinin Korunması*. Bilişim Uzmanlığı Tezi. Bilgi Teknolojileri ve İletişim Kurumu. 2011. https://www.btk.gov.tr/uploads/thesis/osman-sahin.pdf (Erişim Tarihi: 23.04.2025)

Şeker, Şadi Evren. *İş Zekası ve Veri Madenciliği*. İstanbul: Cinius, 2013.

Taştan, Furkan Güven. "Kişisel Verilerin Korunması Kanunu - 2024 Değişikliklikleri". 2025. https://fgtastan.com/wiki/kvkk-degisiklikler/ (Erişim Tarihi: 14.04.2025)

Taştan, Furkan Güven. "Kişisel Verilerin Yurt Dışına Aktarılmasında Açık Rıza". *Terazi Hukuk Dergisi*. Cilt: 0, Sayı: 217. (Eylül 2024): 110-121. https://www.researchgate.net/publication/384329575_Kisisel_Verilerin_Yurt_Disina_Aktarilmasinda_Acik_Riza (Erişim Tarihi: 06.02.2025)

Taştan, Furkan Güven. *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*. 2. Baskı. İstanbul: On İki Levha Yayıncılık, 2017.

The Austrian Post. "Datenschutzverfahren Der Österreichischen Post". 2021. https://news.post.at/presse/de/post/id/1711838/DATENSCHUTZVERFAHREN%20DER%20%C3%96STERREICHISCHEN%20POST (Erişim Tarihi: 25.05.2025)

The Guardian. "Post Office data leak: hundreds of Horizon victims offered up to £5,000 compensation". 2025. https://www.theguardian.com/uk-news/2025/may/20/post-office-offers-compensation-to-horizon-it-victims-over-name-and-address-leak-report (Erişim Tarihi: 06.06.2025)

Ticaret Bakanlığı. "Hızlı kargo ya da posta yoluyla gönderilen eşya konu edilerek yapılan dolandırıcılığa dikkat!". 2024. https://ticaret.gov.tr/haberler/izli-kargo-ya-da-posta-yoluyla-gonderilen-esya-konu-edilerek-yapilan-dolandiriciliga-dikkat (Erişim Tarihi: 06.04.2025)

Topaç, Tahir Hami. *6698 Sayılı Kanun Kapsamında Kişisel Verilere İlişkin Suçlar*. Doktora Tezi. Selçuk Üniversitesi. 2022.

Trendyol. "Ürünümü Nasıl İade Ederim?". https://www.trendyol.com/s/trendyol-iade (Erişim Tarihi: 14.01.2025)

Turan Başara, Gamze. "Kişisel Veri İşleme Sözleşmesi". *Uyuşmazlık Mahkemesi Dergisi*. Sayı: 16. (Aralık 2020): 57-90. https://dergipark.org.tr/tr/download/article-file/1472674 (Erişim Tarihi: 06.06.2024)

Turan Başara, Gamze. "Kişisel Verilerin Korunması Kanunu'nun 6. Maddesinde Yapılan Değişiklik Bağlamında Özel Nitelikli Kişisel Verilerin İşlenmesi". *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*. Cilt: 28, Sayı: 4. (2024): 51-80. https://doi.org/10.34246/ahbvuhfd.1497257 (Erişim Tarihi: 12.07.2024)

Turan, Hasan Selçuk. "Veri Sorumlusu ve Veri İşleyen Farkı". 2017. https://kisiselveri.com/veri-sorumlusu-ve-veri-isleyen-farki (Erişim Tarihi: 16.01.2025)

Turan, Metin. *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması*. 2. Baskı. Ankara: Seçkin Yayıncılık, 2019.

Türk Dil Kurumu, Bilişim Terimleri Sözlüğü. https://sozluk.gov.tr/?ara=veri (Erişim Tarihi: 06.07.2025)

Türk Dil Kurumu, Güncel Türkçe Sözlük. https://sozluk.gov.tr/?ara=posta (Erişim Tarihi: 06.07.2025)

Türkiye Cumhuriyeti Anayasası, 1982. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5 (Erişim Tarihi: 15.08.2024)

Ulaştırma ve Altyapı Bakanlığı. "PTT, evde emekli maaşı ve yardım ödemeleri kapsamında 8,4 milyon işlem gerçekleştirdi." https://www.uab.gov.tr/haberler/ptt-evde-emekli-maasi-ve-yardim-odemeleri-kapsaminda-8-4-milyon-islem-gerceklestirdi (Erişim Tarihi: 01.02.2025)

Uluslararası Standartlar Teşkilatı (ISO). *ISO/IEC 27001 (2022). Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*.

Uluslararası Telekomünükasyon Birliği. *ITU-T Recommendation X.1051, SERIES X: Data Networks, Open System Communications And Security Telecommunication security, Information technology-Security techniques-Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*, 2008.

Umniyahasghar, Yosif. *"Kişisel Verilerin İşlenmesi Şartları ve 6698 Sayılı Kişisel Verilerin Korunması Kanununun Ruhu Olarak Genel İlkeler"*. *SÜAMYOD.* Cilt: 4, Sayı: 1. (2021): 1-22. https://dergipark.org.tr/tr/download/article-file/1748966 (Erişim Tarihi: 12.01.2025)

Uncular, Selen. *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*. İstanbul: Seçkin Yayıncılık, 2018.

University of Michigan Law Library. *"Federal Regulations: FR vs CFR"*. 2024. https://libguides.law.umich.edu/c.php?g=1005584&p=7284939 (Erişim Tarihi: 21.05.2025)

Ural Uslan, Yurdanur ve Değirmenci, Samed. *"Avrupa Birliği Genel Veri Koruma Tüzüğü Işığında Türkiye'de Kişisel Verileri Koruma Kurumu". Optimum Ekonomi ve Yönetim Bilimleri Dergisi*. Cilt: 10, Sayı: 1. (Ocak 2023): 23-38. https://doi.org/10.17541/optimum.1106817 (Erişim Tarihi: 14.06.2025)

Uzunal, Seda. *Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması*. Yüksek Lisans Tezi. Marmara Üniversitesi. 2023. https://tezara.org/theses/795477 (Erişim Tarihi: 20.11.2024)

Ünsal, Çağrı Zeybek. "Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri ile Uyumluluğu ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Açısından Değerlendirilmesi". *Hacettepe Hukuk Fakültesi Dergisi*. Cilt: 3, Sayı: 1. (Haziran 2013): 99-124. https://dergipark.org.tr/tr/pub/hacettepehdf/issue/44821/557498 (Erişim Tarihi: 19.10.2024)

Van Alsenoy, Brendan. *Regulating Data Protection: The Allocation of Responsibility and Risk Among Actors Involved in Personal Data Processing.* Doktora Tezi. KU Leuven. 2016. http://dx.doi.org/10.13140/RG.2.2.17593.98400 (Erişim Tarihi: 14.12.2024)

Veri Koruma Komisyonu. *Quick Guide to the Principles of Data Protection*. Ekim 2019. https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf (Erişim Tarihi: 08.10.2024)

Wanker, Jonas. *GDPR vs. PUL, En förbättring av skyddet för anställdas integritet?.* Yüksek Lisans Tezi. Lund Üniversitesi. 2018. https://lup.lub.lu.se/student-papers/search/publication/8967735 (Erişim Tarihi: 22.06.2024)

Westermann, Hannes. *Change of Purpose: The effects of the Purpose Limitation Principle in the General Data Protection Regulation on Big Data Profiling.* Yüksek Lisans Tezi. Lund University. 2018. https://lup.lub.lu.se/student-papers/search/publication/8941820 (Erişim Tarihi: 04.08.2024)

Winkelmann, Mark, Schönershoven, Torben, Lauerbach, Eva, Dihel, Olivia, Ulrich, Tim, Niederprüm, Antonia, Dieke, Alex ve Junk, Petra. *The Evolution of the European Postal Market since 1997*. 2009. https://www.wik.org/fileadmin/Studien/2009/2009-wik-evolution_en.pdf (Erişim Tarihi: 09.08.2025)

Whittaker, Zack. "USPS shared customer postal addresses with Meta, LinkedIn and Snap". TechCrunch. 2024. https://techcrunch.com/2024/07/18/usps-shared-customer-postal-addresses-with-meta-linkedin-and-snap/ (Erişim Tarihi: 03.06.2025)

Wolters, P.T.J. "The Control by and Rights of the Data Subject Under the GDPR". *Journal of Internet Law*. Cilt: 22 Sayı: 1. (2018). https://repository.ubn.ru.nl/bitstream/handle/2066/194516/194516pub.pdf?sequence=1&isAllowed=y (Erişim Tarihi: 12.02.2025)

Yargıtay 12'nci Ceza Dairesi Kararı, 05.09.2018 günlü, E:2018/2571, K:2018/7821 sayılı karar.

Yazıcıoğlu, Melis Böke. "ISO 27001, KVKK ve GDPR: Bilgi Güvenliği ve Veri Koruma Standartlarının Karşılaştırılması". *Mühendislik ve Teknoloji Dergisi.* 5(1). (2024): 11-21. https://dergipark.org.tr/en/pub/jetech/issue/85597/1488191 (Erişim Tarihi: 18.06.2025)

Yıldız, Kadir. "Veri Sorumlusunun Meşru Menfaati (5/2-f)". *Medeni Hukuk Dergisi*. 1/2. (2024): 214-237. https://dergipark.org.tr/tr/download/article-file/3796860 (Erişim Tarihi: 12.05.2025)

Yılmaz, Berrak. "Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması". Doktora Tezi. Hacettepe Üniversitesi. 2019. https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=pe4O665l35b5vefME-x8uQ&no=L3AlQ-9eMMm4vktT27Y-6A (Erişim Tarihi: 22.06.2024)

Yılmaz, Beste. "Kişisel Verilerin Korunması ve Rekabet Hukuku Bağlamında Veri Taşınabilirliği Hakkı". Yüksek Lisans Tezi. İhsan Doğramacı Bilkent Üniversitesi. 2022. https://repository.bilkent.edu.tr/server/api/core/bitstreams/d8e94fc2-2544-4cf2-91df-3f91cc1407bc/content (Erişim Tarihi: 14.01.2025)

Yılmaz, Malik. "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi". Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi. Cilt: 49, Sayı: 1. (2009): 95-118. https://dergipark.org.tr/tr/download/article-file/2153338 (Erişim Tarihi: 05.01.2025)

Yılmaz, Süleyman ve Çavuşoğlu, Gökçe Filiz. *Kişisel Verileri Koruma Hukuku*, Ankara: Yetkin Yayınları, 2020.

Yücedağ, Nafiye. "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler". *Kişisel Verileri Koruma Dergisi*. Cilt: 1, Sayı: 1. (2019): 47-63. https://dergipark.org.tr/tr/pub/kvkd/issue/45759/566993 (Erişim Tarihi: 17.10.2024)

Yüksek, Furkan Kaan. "AİHM İçtihatlarında Kişisel Verilerin Korunması". *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 25*. Sayı: 1. (Mayıs 2023): 371-420. https://doi.org/10.33717/deuhfd.1276294 (Erişim Tarihi: 12.07.2024)

Yüksel, Metin. "Avrupa Birliği Temel Haklar Şartı". *Ankara Üniversitesi SBF Dergisi*. Cilt:57, Sayı: 4. (Nisan 2002). https://doi.org/10.1501/SBFder_0000001806 (Erişim Tarihi: 14.07.2024)

Yüksel Civelek, Dilek. *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*. Uzmanlık Tezi. Devlet Planlama Teşkilatı Müsteşarlığı. 2011. https://afyonluoglu.org/PublicWebFiles/Reports-TR/Uzmanlik_Tez/2012-04-TEZ-Kisisel_Verilerin_Korunmasi.pdf (Erişim Tarihi: 16.01.2025)

Yürük, Zehra. "Veri Sorumlusunun Veri Güvenliğine İlişkin İdari ve Teknik Tedbirleri Alma Yükümlülüğü". *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*. Cilt: 22, Sayı: 48. (2023): 899-920. https://doi.org/10.46928/iticusbe.1218693 (Erişim Tarihi: 12.02.2025)

Zanfir-Fortuna, Gabriela. "*Article 82. Right to compensation and liability", The EU General Data Protection Regulation (GDPR): A Commentary*. ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler. Croydon: Oxford University Press, 2020. https://academic.oup.com/oxford-law-pro/book/41324/chapter-abstract/352305300?redirectedFrom=fulltext (Erişim Tarihi: 05.03.2025)

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Yönetmeliğine uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

23.09.2025

Beray DİKİLİTAŞ

ÖZGEÇMİŞ

08.05.1995 tarihinde Ankara'da doğdu. Lise eğitimini 2013 yılında Ankara Esenevler Anadolu Lisesi'nde, lisans eğitimini ise 2017 yılında Çankaya Üniversitesi Hukuk Fakültesi Hukuk bölümünde tamamladı. 2022 yılının Ocak ayında başladığı Bilgi Teknolojileri ve İletişim Kurumunun Sektörel Rekabet Dairesi Başkanlığında Bilişim Uzman Yardımcısı olarak hâlen görevine devam etmektedir.