T.C.
DOKUZ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU PROGRAMI
YÜKSEK LİSANS TEZİ

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNDA İLGİLİ KİŞİNİN HAKLARI

Özlem ÖZSOY

Danışman
Doç. Dr. Oğuz ŞİMŞEK

İZMİR – 2024

YÜKSEK LİSANS
TEZ ONAY SAYFASI

Üniversite	**:** Dokuz Eylül Üniversitesi
Enstitü	**:** Sosyal Bilimler Enstitüsü
Adı ve Soyadı	**:** ÖZLEM ÖZSOY
Öğrenci No	**:** 2020800847
Tez Başlığı	**:** Kişisel Verilerin Korunması Hukukunda Veri Sahibinin Hakları
Savunma Tarihi	**:**
Danışmanı	**:** DOÇ.DR. OĞUZ ŞİMŞEK

JÜRİ ÜYELERİ

Ünvanı, Adı, Soyadı	**Üniversitesi**	**İmza**
DOÇ.DR. OĞUZ ŞİMŞEK	-Dokuz Eylül Üniversitesi	.....
Dr.Öğr.Üyesi Lale Burcu ÖNÜT	-Dokuz Eylül Üniversitesi	.....
Dr.Öğr.Üyesi Cemal BAŞAR	-İzmir Katip Çelebi Üniversitesi	.....

ÖZLEM ÖZSOY tarafından hazırlanmış ve sunulmuş olan bu tez savunmada başarılı bulunarak oy birliği(x) / oy çokluğu( ) ile kabul edilmiştir.

Prof. Dr. Asuman ALTAY
Müdür

YEMİN METNİ

Yüksek lisans tezi olarak sunduğum "Kişisel Verilerin Korunması Hukukunda İlgili Kişinin Hakları" adlı çalışmanın, tarafımdan, akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

Tarih

...../...../.....

Özlem ÖZSOY

İmza

ÖZET

Yüksek Lisans Tezi

Kişisel Verilerin Korunması Hukukunda İlgili Kişinin Hakları

Özlem ÖZSOY

Dokuz Eylül Üniversitesi

Sosyal Bilimler Enstitüsü

Kamu Hukuku Anabilim Dalı

Kamu Hukuku Programı

Gelişen teknoloji dünyasında artan bilgisayar ve internet kullanımı, kişisel verilerin işlenmesinde büyük bir artışı meydana getirmiştir. Kişisel verilerin hemen hemen her alanda kullanılmasının birçok olumlu etkisi olduğu gibi olumsuz etkileri de ortaya çıkmıştır. Bu nedenle tıpkı diğer temel hak ve özgürlükler gibi, kişisel verilerin korunması hakkının da bu kapsamda güvence altına alınma zarureti doğmuştur.

Kişisel verilerin korunması hakkı, kişilerin verilerinin gizliliğinin ve güvenliğinin sağlanması gerekliliğini içeren genel ve üst bir konsepttir. Sadece bu hakkın varlığından yola çıkılarak korumanın ne şekilde sağlanacağı belirsizdir. İlgili kişilere tanınan haklar sayesinde; kişisel verilerin korunması hakkının felsefesi somut bir görünüm kazanmakta, veri işleme faaliyetleri üzerinde denetimi sağlanmakta, ilgili kişilere verileri üzerinde daha fazla farkındalık ve seçenek sunulmaktadır.

Bu çalışmada, "kişisel veri" ve "ilgili kişi" kavramları öncülüğünde; kişisel veri koruma hukukuna ilişkin kavramlar ve mevzuat açıklanmış, kişisel verilerin korunmasının önemi ve hukuki niteliği vurgulanmış, ilgili kişilerin haklarının içerikleri, esasları ve uygulanma usulleri Türk ve Avrupa hukuku açısından mukayeseli olarak ortaya konulmuştur. Elde edilen bulgular çeşitli idari ve yargısal kararlarla desteklenmiştir.

Anahtar Kelimeler: Kişisel Veri, İlgili Kişi, İlgili Kişinin Hakları, KVKK, GDPR, Veri Koruma Hukuku

ABSTRACT

Master's Thesis

Rights of the Data Subject in Personal Data Protection Law

Özlem ÖZSOY

Dokuz Eylül University

Graduate School of Social Sciences

Department of Public Law

Public Law Program

Increasing computer and internet use in the developing technology world has caused a great increase of personal data processing. The use of personal data in almost every field has many positive effects, as well as negative ones. Therefore, it became necessary to guarantee the right to protection of personal data, just as other fundamental rights and freedoms.

The right to protection of personal data is more general and superior concept that includes the necessity of ensuring the confidentiality and security of people's data. It is unclear how the protection will be provided based solely on the existence of this right. Through the instrumentality of the rights granted to data subjects; the philosophy of the right to protection of personal data gains a concrete appearance, control over data processing activities is ensured, and data subejcts are offered more awareness and options regarding their data.

In this thesis, spearheaded by the notions of "personal data" and "data subject"; notions and legislation regarding personal data protection law are explained, the importance and legal nature of the protection of personal data are emphasized, and the contents, principles and implementation procedures of data subjects' rights are presented comparatively in terms of Turkish and European law. The findings are supported by various administrative and judicial decisions.

Keywords: Personal Data, Data Subject, Rights of the Data Subject, KVKK, GDPR, Data Protection Law

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNDA İLGİLİ KİŞİNİN HAKLARI

İÇİNDEKİLER

İKİNCİ BÖLÜM
İLGİLİ KİŞİNİN HAKLARI

KISALTMALAR

AB	**:** Avrupa Birliği
ABAD	**:** Avrupa Birliği Adalet Divanı
ABİHA	**:** Avrupa Birliğinin İşleyişi Hakkında Anlaşma
AİHM	**:** Avrupa İnsan Hakları Mahkemesi
AİHS	**:** Avrupa İnsan Hakları Sözleşmesi
Bkz.	**:** Bakınız
CMK	**:** 5271 Sayılı Ceza Muhakemesi Kanunu
CNIL	**:** Commission nationale de l'informatique et des libertés (Fransız Ulusal Bilişim ve Özgürlükler Komisyonu)
Çev.	**:** Çeviren
Der.	**:** Derleyen
E.	**:** Esas
Ed.	**:** Editör
E.T.	**:** Erişim Tarihi
GDPR	**:** General Data Protection Regulation (Avrupa Birliği Genel Veri Koruma Tüzüğü)
K.	**:** Karar
KEP	**:** Kayıtlı elektronik posta
KVKK	**:** 6698 Sayılı Kişisel Verilerin Korunması Kanunu
m.	**:** madde
OECD	**:** Organisation for Economic Co-Operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)
s.	**:** Sayfa
ss.	**:** Sayfa Sayıları
TBK	**:** 6098 Sayılı Türk Borçlar Kanunu
TCK	**:** 5237 Sayılı Türk Ceza Kanunu
TMK	**:** 4721 Sayılı Türk Medeni Kanunu
vb.	**:** ve benzeri
VERBİS	**:** Veri Sorumluları Sicili
Yön.	**:** Yönetmelik

GİRİŞ

Günümüzde dijitalleşmenin her geçen gün hızla arttığı yadsınamaz bir gerçektir. Bu dijitalleşme kapsamında bireylere ilişkin veriler yoğun bir şekilde toplanmakta ve birçok çeşitli alanda kullanılmaktadır. Gitgide artan bu faaliyetler, kişilerin mahremiyeti ve güvenliğiyle ilgili endişelere neden olunca, kişisel verileri korumak ve bireylerin verilerinin nasıl toplandığı, paylaşıldığı ve kullanıldığı üzerinde kontrol sahibi olmasını sağlamak elzem hale gelmiştir. Bu nedenle bireylerin kişisel verilerinin korunması modern hukuk sistemlerinin önemli bir odak noktasını oluşturmaya başlamış, çok sayıda ulusal ve uluslararası çapta hukuki düzenlemenin yapılmasına yol açmıştır. Bu hususta bilhassa Avrupa'daki gelişmeler tüm dünyaya örnek olmaktadır. Avrupa Birliği genelinde etkili olan 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ve iç hukukumuzda yürürlükte olan 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ilgili kişilerin haklarının kapsamlarının, esaslarının ve uygulanma usullerinin anlaşılması hususunda oldukça önemli kaynaklardır.

İşbu tez iki temel bölüme ayrılmıştır. "Kişisel Veri, İlgili Kişi ve Kişisel Verilerin Korunması" adlı ilk ana bölümde, "kişisel veri" ve "ilgili kişi" kavramlarının öncülüğünde kişisel veri koruma hukukuna ilişkin diğer kavramlar da incelenecektir. Kişisel verilerin korunabilmesi için öncelikle kişisel verinin ne anlama gelip neleri kapsadığını ve kimlerin ilgili kişi olarak hak ileri sürebileceğini tespit etmek önem arz etmektedir. "Kişisel Veri" alt başlığı altında kavramın tanımı ve unsurları, türleri, korunmasının gerekliliği ve hukuki niteliği, korunmasına ilişkin ulusal ve uluslararası temel düzenlemeler detaylıca açıklanacaktır. "İlgili Kişi" başlığı altında ise, ilgili kişinin kimliği irdelenecek ve benzer bazı kavramlarla ilişkisi ortaya konulacaktır. "İlgili Kişinin Hakları" adlı ikinci ana bölümde, ilgili kişilerin kendilerine ilişkin verilerle ilgili olarak ileri sürebileceği hakların içerikleri, esasları ve uygulanma usulleri; KVKK ve GDPR'deki düzenlemelerle birlikte karşılaştırmalı olarak ortaya konulacaktır. Varılan sonuçlar; arasında Kişisel Verileri Koruma Kurulu, Yargıtay, Avrupa Birliği'nin yargı organı olan Adalet Divanı, Avrupa Konseyi bünyesinde kurulan Avrupa İnsan Hakları Mahkemesi, çeşitli Avrupa ülkelerinin veri koruma otoriteleri ve yerel mahkemeleri gibi birçok kurul, kuruluş ve yargı organlarının

verdiği kararlarla da desteklenecektir. Ayrıca ilgili kişilerin haklarını kullanmasına yönelik genel esaslar ile hakların genel kısıtlanma sebepleri de incelenecektir.

BİRİNCİ BÖLÜM
KİŞİSEL VERİ, VERİ SAHİBİ VE KİŞİSEL VERİLERİN KORUNMASI

I. KİŞİSEL VERİ

A. Genel Olarak

Tarih boyunca toplumsal hayatın sürdürülebilmesi ve yürütülebilmesi için bireylerin kişisel verileri, gerek kamu sektörü gerekse de özel sektör aktörleri tarafından çeşitli amaçlarla toplanmış ve kullanılmıştır. Örneğin, kişisel verilerin en eski kullanım alanlarından biri, geçmişi çok eskilere dayanan bir uygulama olan nüfus sayımıdır. Zira bir nüfus sayımı; yaşları, cinsiyetleri, meslekleri ve kişisel servetleri dahil olmak üzere bireyler ve haneler hakkında bilgi toplamayı içermektedir. Benzer şekilde bankalar 19. yüzyılda borçları ve ödeme geçmişleri de dahil olmak üzere insanların kredi geçmişleri hakkında bilgi toplamaya başlamıştır. Bu bilgiler, borç verenlerin bireylere borç para verip vermeme konusunda karar vermelerine yardımcı olmak için kullanılmıştır. Devletler 20. yüzyıl ile birlikte, vatandaşlara vergisel yükümlülükler veya sosyal yardımlar gibi takip amaçları[1] için sosyal güvenlik numaraları vermeye başlamıştır. İşletmeler müşteriler hakkında veri toplamaya ve bunları pazarlama amacıyla kullanmaya başlarken, hükümetler de vatandaşların faaliyetlerini izlemek için verileri kullanmıştır[2].

Zaman ilerledikçe gelişen teknolojiye bağlı olarak artan bilgisayar ve internet kullanımı, kişisel verilerin önemindeki artışa ek olarak, nitelik ve nicelik olarak da artışını beraberinde getirmiştir. Veriler ayrıca bu sayede dijital ortama aktarılmış olup toplanması, saklanması ve analiz edilmesi daha kolay hale gelmiştir. Zira isimler, adresler, telefon numaraları, e-posta adresleri, finansal bilgiler ve hatta konum verileri

[1] Devletin takip amacıyla oluşturduğu üç çeşit kayıt türü olduğu ifade edilmektedir. Bunlardan ilki, bireylerin bir yönetim birimiyle işlem yapması nedeniyle oluşan ehliyet başvurusu, vergi beyanı, öğrenci kaydı gibi kayıtlardır. Diğerleri de istihbarat ve istatistiksel amaçlarla oluşturulan kayıtlar olarak kabul edilir. (Elif Küzeci, **Kişisel Verilerin Korunması**, Turhan Kitabevi, Ankara, 2010, s. 21).

[2] American Social Security Administration, "Report to Congress on Options for Enhancing the Social Security Card Chapter 3: The Expansion of the SSN as an Identifier", **Social Security Administration Web Sitesi**, https://www.ssa.gov/history/reports/ssnreportc2.html, (E.T. 01.03.2022).

gibi kişisel veriler, kullanıcıların bilgisi veya onayı olmadan toplanmakta, saklanmakta ve kullanılmaktaydı. Gitgide artan bu faaliyetler gizlilik ve güvenlikle ilgili endişelere neden olunca, kişisel verileri korumak ve bireylerin verilerinin nasıl toplandığı, paylaşıldığı ve kullanıldığı üzerinde kontrol sahibi olmasını sağlamak için devletler tarafından yasal düzenlemeler yapılmıştır. Bu düzenlemelerde devletler, kişisel verileri kendi yasal ve kültürel bağlamlarına göre farklı şekillerde tanımlamış ve yorumlamışlardır. Fakat genel olarak, kişisel verilerin bir kişiyi doğrudan veya dolaylı olarak tanımlamak için kullanılabilecek her türlü bilgiyi ifade edeceği açıktır. Bu kavram; kişinin adını ve soyadını, adresini, telefon numarasını, doğum tarihini, tıbbi kayıtlarını, mali bilgilerini, parmak izlerini ve daha fazlasını içerebilir. Kişisel verilerin tanımı; teknoloji, iletişim ve mahremiyet endişelerindeki değişiklikleri yansıtacak şekilde zaman içinde gelişmiştir. Örneğin, dijital iletişim ve sosyal medya platformlarının yükselişiyle birlikte, kişisel veriler artık çevrimiçi etkinlikleri, arama geçmişlerini ve coğrafi konum verileri gibi verileri de içerebilir hale gelmiştir. Kişisel verilerin korunabilmesi için öncelikle kişisel verinin ne anlama gelip neleri kapsadığını tespit etmek önem arz etmektedir.

B. Kişisel Verinin Tanımı ve Unsurları

1. Kişisel Verinin Tanımı

Kişisel veri denilince akla birçok örnek gelse de, "kişisel veri" kavramının kapsamına nelerin girdiğini sınırlı sayıda sayabilmek mümkün değildir. Zira zamanın şartları değişip geliştikçe kişilerin üzerinde kişilik hakkına sahip olduğu şeylerin sayısı artmakta ve kapsamı genişlemektedir. Bu nedenle kişisel veri için genel ve yalın bir tanım yapmak en doğrusu olacaktır. Buna göre, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilginin" kişisel veri olduğunu söylemek yanlış olmayacaktır. Gerçekten de kişisel verilerin korunmasına ilişkin olarak çıkarılan 6698 Sayılı Kanun (KVKK) m. 3/1-d'de kişisel veri kavramı bu şekilde tanımlanmıştır[3]. Ancak hukukumuzda her zaman bu şekilde tanımlanmadığını da belirtmek gerekir.

[3] 07.04.2016 tarihli Resmi Gazete'de yayımlanan 6698 Sayılı Kişisel Verilerin Korunması Kanunu, **Resmi Gazete**, https://www.resmigazete.gov.tr/eskiler/2016/04/20160407.pdf, (E.T. 01.03.2022).

Elektronik Haberleşme Kanunu'nun[4] ilgili maddelerine dayanılarak çıkartılan Yönetmelik'in "Tanımlar ve kısaltmalar" başlıklı m. 3/1-h'de yer alan düzenlemesinde[5] "belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgilerin" kişisel veri olduğu ifade edilmişti. Bu yönetmelik şu anda mülgadır. Aynı adla yerine getirilen yeni düzenlemede[6] ise (m.4/1-f) "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" kişisel veri olarak tanımlanarak günümüz standartları yakalanmıştır.

Kişisel veri elbette sadece iç hukukta KVKK'deki gibi tanımlanmamış olup uluslararası hukukta da durum çok farklı değildir. 2016 yılında çıkartılan 679 Sayılı Tüzük'te (General Data Protection Regulation – "GDPR") "Tanımlar" başlıklı m. 4/1'de[7] "tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilginin" kişisel veri şeklinde tanımlandığını görmekteyiz. Avrupa Birliği (AB) özelinde biraz daha geriye gittiğimizde, 2018 yılında yürürlüğe giren GDPR'den önce yürürlükte olan, mülga 95/46/EC Sayılı Direktif'in "Tanımlar" başlıklı m. 2/a hükmünde[8] de temel olarak aynı tanım yapılmış, sadece nelerin kişisel veri sayılabileceğine dair fikir vermesi açısından birkaç örneğe de yer verilmişti. Buna göre, kişisel veri; "fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye ("veri öznesi") ilişkin herhangi bir bilgiyi" kastedecektir. Hükmün lafzından da anlaşılacağı üzere, yapılan sayım tahdidi değil, örnekleyici niteliktedir.

---

[4] 10.11.2008 tarihli Resmi Gazete'de yayımlanan 5809 sayılı Elektronik Haberleşme Kanunu, **Resmi Gazete**, https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5809.pdf, (E.T. 01.03.2022).

[5] Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, **Lexpera İçtihat Sitesi**, https://www.lexpera.com.tr/mevzuat/yonetmelikler/elektronik-haberlesme-sektorunde-kisisel-verilerin-islenmesi-ve-gizliliginin-korunmasi-hakkinda – (E.T. 01.03.2022).

[6] 04.12.2020 tarihli Resmi Gazete'de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, **Resmi Gazete,** https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm, (E.T. 01.03.2022).

[7] 04.05.2016 tarihli Avrupa Birliği Resmi Gazetesi'nde yayınlanan Genel Veri Koruma Tüzüğü (GDPR), **Avrupa Birliği Resmi Gazetesi**, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, (E.T. 01.03.2022).

[8] 23.11.1995 tarihli Avrupa Toplulukları Resmi Gazetesi'nde yayınlanan 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi, **Avrupa Toplulukları Resmi Gazetesi**, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5, (E.T. 01.03.2022).

Yine Avrupa Konseyi'nin bir düzenlemesi olan, KVKK'nin de temelini oluşturan ve genellikle "108 Sayılı Sözleşme" olarak bilinen sözleşmenin "Tanımlar" başlıklı m. 2/a hükmünde "tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilginin" kişisel veri olduğu belirtilerek GDPR ile birebir aynı tanıma yer verilmiştir. Uluslararası arenada bu hususta ilk düzenleme olan ve OECD tarafından kabul edilen 1980 tarihli Rehber İlkeler'in m. 1/b'de ise "belirli veya belirlenebilir bir kişiye ilişkin her türlü bilgi" kişisel veriyi belirtir.

Şimdiye kadar bahsedilen bu tanımlar ister ulusal ister uluslararası düzenlemelerde yer alsın, bu yerlerin yasama organlarının yaptığı tanımlardır. Halbuki, bu tanımlara uygun olarak, yargı organları da önüne gelen hukuki uyuşmazlıkları çözerken, verdiği kararlarda kişisel veriler hakkında kendilerince tanımlar yapmaktadır. Bu tanımlarda, soyut ve genelgeçer nitelikte olması gereken hukuki düzenlemelerin aksine, uygulamaya yön göstermek amacıyla bolca örneklemeye yer verilmektedir. Örneğin, Anayasa Mahkemesi çeşitli kararlarında[9] kişisel verinin tanımına şu şekilde yer vermiştir:

> *Belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler.*

Yargıtay bir kararında[10] kişisel veri hakkında şöyle bir değerlendirmede bulunmuştur:

> *Kişisel veri kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir.*

[9] Anayasa Mahkemesi, 09.04.2014 tarih ve E. 2013/122, K. 2014/74; 19.03.2015 tarih ve E. 2014/180, K. 2015/30 kararı, https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/, (E.T. 02.03.2022).

[10] Yargıtay 12. Ceza Dairesi, 29.06.2022 tarih ve E. 2022/1745, K. 2022/5271, https://kararara ma.yargitay.gov.tr/, (E.T. 02.03.2022).

Uluslararası yargı yeri olarak kabul ettiğimiz Avrupa İnsan Hakları Mahkemesi (AİHM) de dinamik yorum yaparak Avrupa İnsan Hakları Sözleşmesi (AİHS) m.8'de maddesinde yer alan özel yaşama saygı hakkı kapsamında değerlendirdiği kişisel verilerin korunmasına yönelik hakka ilişkin olarak verdiği bazı kararlarda[11] "görüntü, fotoğraf, parmak izi, DNA profili, hücre örnekleri, ev adresi, yaş, doğum tarihi ve fiziksel özellikler" mahiyetindeki hususları kişisel veri şeklinde değerlendirdiğini belirlemiştir.

Tüm bu tanımlardan yola çıkarak, bir verinin kişisel veri olarak addedilebilmesi için üç unsuru taşıması gerektiğini söylemek mümkündür. Öyleyse, kişisel verinin varlığından söz edebilmek için halihazırda bir verinin var olması, bunun gerçek bir kişiyi belirli veya belirlenebilir hale getirmesi ve gerçek bir kişiye ilişkin olması gerekmektedir.

2. Kişisel Verinin Unsurları

a. Veri

Verinin kelime anlamı; "olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimidir"[12]. Doktrinde de verinin, her türlü bilgiyi kapsayan bir kavram olduğu ve bilişim sistemleri tarafından işlenebileceği, depolanabileceği, okunabileceği ve diğer sistemlere aktarılabileceği ifade edilmektedir[13]. Veri aynı zamanda sözlükte bilgi sözcüğüyle de ilişkilendirilmektedir. Buna paralel olarak KVKK'de de kişisel verinin tanımı yapılırken bilgi kavramına yer verilmiştir. Bu kavramlar anlam olarak birbirlerine yakın kavramlar olsa da aralarında temel birtakım farklılıklar bulunmaktadır. Veri dediğimiz zaman, sayılar veya yazı gibi belirli bir biçimde yapılandırılmış ham ve işlenmemiş bilgiler akla gelir. Akıl süzgecinden geçmediği için herhangi bir bağlamsal yorum veya analizden yoksundur

[11] AİHM, 28.01.2003 tarih ve 44647/98 başvuru numaralı Peck/Birleşik Krallık kararı; 11.01.2005 tarih ve 50774/99 başvuru numaralı Sciacca/İtalya kararı, 04.12.2008 tarih ve 30562/04 başvuru numaralı S. Marper/Birleşik Krallık kararı; 09.10.2012 tarih ve 42811/06 başvuru numaralı Alkaya/Türkiye kararı; 02.12.2008 tarih ve 2872/02 başvuru numaralı K.U./Finlandiya kararı, https://hudoc.echr.coe.int/, (E.T. 02.03.2022).

[12] Türk Dil Kurumu, https://sozluk.gov.tr/, (E.T. 02.03.2022).

[13] Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, Hukuk Akademisi Yayınları, 3. Baskı, İstanbul, 2020, s. 152.

ve genellikle kendi başına anlamsız sayılabilir. Öte yandan bilgi, sorunları çözmek veya bir konuda karar vermek için verinin yorumlanması ve uygulanmasıyla ortaya çıkar. Var olan verileri doğru bağlamlarda kullanarak anlamlı çıkarımlar yapılmasını, eldeki soruna uygun düştüğü ölçüde uyarlanarak uygulanmasını ve bu yönde doğru adımlar atılmasını sağlar. Başka bir deyişle veri, bilginin temel yapı taşı iken[14]; bilgi, verilerden bir dizi analiz, yorumlama ve uygulama sonucunda elde edilen değeri temsil eder[15]. Nitekim 5651 Sayılı Kanun m. 2/1-k'de "bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer" şeklinde "veri", m.2/1-ç'de ise "verilerin anlam kazanmış biçimi" denilerek "bilgi" tanımları yapılmıştır[16]. Bilgi ve veri, kişisel verileri koruma hukukuna ilişkin düzenlemelerde birbiri yerine kullanılabildiğinden iki kavram arasındaki farkın ortaya konulması önemlidir. Düzenlemede "bilgi" kavramı kullanılmışsa da içine veriyi alacak şekilde geniş bir yorum yapılması gerektiği kanısındayız.

Verinin kelime anlamının ve bilgiden farklı yanlarının anlaşılmasının ardından, bir başka önemli konu ise, verinin kişisel veri olabilmesi için mahiyeti ile kişinin hangi alanına mahsus olması gerektiğinin belirlenmesidir. Bu konu, kişisel verilerin korunması hukuku açısından özellikle önemlidir çünkü farklı türdeki veriler, farklı düzenlemelere tabi olabilir ve sonuç olarak farklı düzeylerde korunabilir. Kişinin adı, soyadı, doğum tarihi[17] ve yeri, kimlik numarası[18], pasaport numarası[19], uyruğu, anne-baba adı, nüfusa kayıtlı olduğu yer, cilt numarası, aile sıra numarası, kütük numarası gibi kimliğini doğrudan ortaya koyan bilgilerin kişisel veri kategorisine gireceğine kuşku yoktur. Zira kişiyi diğerlerinden ayıran en temel bilgiler bunlardır. Yine, kişinin

[14] Cemile Turgut, **Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı**, On İki Levha Yayınları, İstanbul, 2021, s. 173; A. Çiğdem Ayözger Öngün, **Kişisel Verilerin Korunması Hukuku**, 2. Baskı, Beta Yayınevi, İstanbul, 2019, s. 8.

[15] Chaim Zins, "Conceptual approaches for defining data, information, and knowledge", **Journal of the American Society for Information Science and Technology**, Cilt: 58, Sayı: 4, 2007, s. 481.

[16] 23.05.2007 tarihli Resmi Gazete'de yayımlanan 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, **Resmi Gazete**, https://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm, (E.T. 04.03.2022).

[17] AİHM, 24.01.2019 tarih ve 43514/15 başvuru numaralı Catt/Birleşik Krallık kararı, https://hudoc.echr.coe.int/, (E.T. 05.03.2022). Bu kararda, başvurucunun adı, katılımı, doğum tarihi ve adresi gibi kişisel verileri sendika üyeliğinin kayıt altına alınması için polis tarafından toplanmıştır. Mahkeme bu bilgilerin kişisel veri olduğunu belirtmiştir.

[18] Bird & Bird Law Firm, **Guide to the General Data Protection Regulation**, 2020, s. 74.

[19] Anayasa Mahkemesi, 09.04.2014 tarih ve E. 2013/122, K. 2014/74 numaralı kararı https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/, (E.T. 05.03.2022).

kimlik bilgileri[20] haricinde özel yaşamına ilişkin olan diğer bilgiler de kişisel veri sayılacaktır. Örneğin, bireyin adresi[21], medeni durumu[22], cinsiyeti[23], akıl ve ruh sağlığı[24], cinsel hayatı[25] ve yönelimi[26], banka veya kredi kartı numarası[27], telefon numarası[28], dini inancı[29] bu kapsamda sayılabilir. Elbette bir verinin kişisel veri sayılması için illa ki kişinin, dilediği gibi yaşadığı ve dış dünyadan sakındığı bir mahrem alandan oluşan özel hayatına ilişkin olması gerekmez. Zira özel yaşam, bireyin sosyal ve ekonomik yaşamını da içine alacak şekilde geniş yorumlanması gereken bir kavramdır. Sonuçta insan sosyal bir varlıktır. Nitekim AİHM de bireyin maddi ve manevi varlığını geliştirmek için dış dünyayla ilişki kurma ihtiyacı olduğunu, kişinin kendini gerçekleştirebilmesi için topluma katılması gerektiğini ve bu yüzden de hayatının sosyal ve ekonomik yönlerinin de özel yaşam kapsamında değerlendirilmesi gerektiğini belirtmektedir[30]. Örneğin, bir avukatın mesleği gereği yazmış olduğu dilekçede geçen adı ve soyadı, büro adresi ve iş amacıyla kullandığı

[20] Ersan Şen, "Kişisel Verilerin Korunması Kanunu Tasarısının Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", **İstanbul Barosu Dergisi**, Cilt: 83, Sayı: 3, 2009, (KVKK Tasarısı), s. 1197.

[21] W. Gregory Voss ve Kimberly A. Houser, "Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies", **American Business Law Journal**, Cilt: 56, Sayı: 2, 2019, s. 316.

[22] Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Yetkin Yayınları, Ankara, 2004, s. 34; AİHM, 06.04.2021 tarih ve 5434/17 başvuru numaralı Liebscher/Avusturya kararı, https://hudoc.echr.coe.int/, (E.T. 05.03.2022). Söz konusu kararda; boşanma protokolünde yer alan mal rejiminin tasfiyesi, reşit olmayan çocukların velayeti ve ikametgahı, nafaka anlaşması ve başvurucunun mal varlığı ile geliri gibi hususlar kişisel veri olarak nitelendirilmiştir.

[23] Volkan Sırabaşı, **İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz**, Adalet Yayınevi, 2. Bası, Ankara, 2007, s. 195.

[24] AİHM, 27.02.2018 tarih ve 66490/09 başvuru numaralı Mockutė/Litvanya kararı; 31.05.2016 tarih ve 50405/06 başvuru numaralı Malanicheva/Rusya kararı, https://hudoc.echr.coe.int/, (E.T. 05.03.2022).

[25] AİHM, 27.08.1997 tarih ve 20837/92 başvuru numaralı M.S./İsveç kararı, https://hudoc.echr.coe.int/, (E.T. 05.03.2022).

[26] AİHM, 22.10.1981 tarih ve 7525/76 başvuru numaralı Dudgeon/Birleşik Krallık kararı; 27.05.2021 tarih ve 5671/16 başvuru numaralı J.L./İtalya kararı, https://hudoc.echr.coe.int/, (E.T. 05.03.2022).

[27] Voss ve Hauser, s. 324.

[28] Voss ve Hauser, s. 316.

[29] AİHM, 02.05.2010 tarih ve 21924/05 başvuru numaralı Sinan Işık/Türkiye kararı; 27.02.2018 tarih ve 66490/09 başvuru numaralı Mockutė/Litvanya kararı, https://hudoc.echr.coe.int/, (E.T. 05.03.2022). Bu kararlarda, bireyin felsefi inançları da dahil olmak üzere, dini veya diğer inançlarının açıklanması Mahkeme tarafından kişisel verilerin korunma hakkı kapsamında değerlendirilmiştir. Özellikle Sinan Işık başvurusunda, dinin inanç sahiplerinin hüviyetlerini ve dünya görüşlerini yansıtan en önemli unsurlarından birini oluşturduğu tespitinde bulunularak başvurucuların kimlik kartlarında din ibaresinin yer almasının kişisel verilerin korunması hakkı özelinde düşünce, vicdan ve din özgürlüğünü (AİHS m.9) ihlal ettiği sonucuna varılmıştır.

[30] AİHM, 25.09.2018 tarih ve 76639/11 başvuru numaralı Denisov/Ukrayna kararı, https://hudoc.echr.coe.int/, (E.T. 05.03.2022); ABAD, 09.11.2010 tarih ve C-92/09 numaralı Volker und Markus Schecke. GbR ve C-93/09 numaralı Hartmut Eifert v. Land Hessen kararları, https://curia.europa.eu/juris/document/document.jsf?docid=79001&doclang=en, (E.T. 05.04.2022).

cep telefonu numarası, o avukat açısından kişisel veridir. İsteyenlerin bir engelle karşılaşmaksızın ulaşabileceği, kişinin kendisinin aleniyet kazandırarak paylaştığı veriler de kişisel veri olma niteliğini korumaya devam eder[31]. Yahut kişinin sosyal yaşamında severek iştigal ettiği hobileri[32], günlük çalışma, mola saatleri ve maaş bilgisi gibi çalışma koşullarına ilişkin bilgiler[33], aktif ve pasif malvarlığına ilişkin bilgiler[34], vakıf, dernek ve sendika üyelikleri[35] hep birer kişisel veridir. Sosyal medya aracılığıyla paylaşılan gönderiler başta olmak üzere benzer türdeki çevrimiçi davranış bilgileri de hala kişisel veridir[36]. Yargıtay da doktrin de aynı noktadan hareketle, kişisel verileri koruyan ceza hukuku normlarında, korunan hukuki değerin sırrın kendisinin değil, ilgilinin kişilik hakları olduğunu ifade etmektedir[37].

Çeşitli ölçüm ve gözlemler ile kişi hakkında edinebileceğimiz bilgiler kişisel veridir. Örneğin kişinin yaşı, boyu, kilosu, saç, göz ve ten rengi, kıyafet bedeni, ayakkabı numarası gibi nesnel bilgiler kişisel veridir. Fakat öyle veriler de vardır ki herkes tarafından aynı şekilde algılanmaz. Verinin kapsamına, karşı tarafı belirli veya belirlenebilir kılabilen duygu ve düşünceler de dahil olabilir. Birinin güzel veya çirkin olması, uzun veya kısa olması, güvenilir olup olmadığı gibi subjektif nitelendirmeler de kişisel veri sayılabilmektedir[38]. Örneğin, işverenin performans değerlendirmesinde işçinin çalışkan olup olmadığı, iş yapma kalitesinin ne olduğu, güvenilirliği, saygılı olup olmadığı ve görev sorumluluk bilincinin olup olmadığı gibi niteliklerini belirtmesi artık bu bilgileri de işçinin kişisel verisi haline getirecektir. Ya da sigortacının hayat sigortası yaparken sigortalı adayının genç olduğu için önünde uzun bir ömür olduğunu ve sağlık problemi yaşamayacağını not alması durumu da buna bir

---

[31] Dülger, s. 155.

[32] ABAD, 06.11.2003 tarih ve C-101/01 numaralı Bodil Lindqvist kararı, https://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=EN, (E.T. 05.04.2022).

[33] ABAD, 30.05.2013 tarih ve C-342/12 numaralı Worten Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT) kararı, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0342, (E.T.05.04.2022).

[34] ABAD, 16.12.2008 tarih ve C-73/07 numaralı Satakunnan Markkinapörssi and Satamedia kararı, https://curia.europa.eu/juris/liste.jsf?num=C-73/07&language=en, (E.T. 05.04.2022).

[35] Aydın Akgül, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, 2. Baskı, Beta Basım Yayın, İstanbul, 2016, s. 9.

[36] Turgut, s. 174; Voss ve Hauser, s. 324.

[37] Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, Seçkin Yayınevi, 4. Bası, Ankara, 2014, (Bilişim Suçları), ss. 579, 588-593; Yargıtay Ceza Genel Kurulu, 17.06.2014 tarih ve E.2012/12-1510, K. 2014/331 sayılı kararı, https://kararara ma.yargitay.gov.tr/, (E.T. 08.03.2022).

[38] Hüseyin Can Aksoy, **Kişisel Verilerin Korunması**, Çakmak Yayınevi, Ankara, 2010, ss. 14-15'ten aktaran Habip Bozkurt, **Kişisel Verilerin İşlenmesinin Hukuki Boyutu**, Yetkin Yayınları, Ankara, 2021, s. 8; Dülger, s. 155; Turgut, s. 175.

örnek teşkil eder[39]. Üstelik verinin, ister nesnel ister öznel nitelikte olsun, doğru olmasına gerek yoktur[40]. Yanlış veriler kişiye zarar verebileceği için yasal düzenlemenin koruma alanına dahil edilmesi elzem olduğundan kişisel veri sayılacaktır[41]. Ayrıca kişi bu sayede, söz konusu yanlış veriler üzerinde silme veya düzeltme hakkını da kullanabilecektir.

Bilginin formatı da kişisel veri olarak nitelendirilmesini etkilemez. Yani söz konusu bilgi, yazıyla veya sayıyla ifade edilebileceği gibi; fotoğraf, video, resim, grafik, ses vb. şeklinde de olabilir[42]. Örneğin, telefon bankacılığında, müşterinin banka memuruna sesi ile verdiği komutlar kayıt altına alınır. Bu kayıtlar sesin sahibini belirli veya belirlenebilir hale getiriyorsa kişisel veri sayılmalıdır. Bunun yanı sıra, kamera kaydı alınarak gözetlenen bir yerde, videodaki kişilerin yüzleri tanınabilecek durumdaysa bu görüntüler kişisel veridir. Bir toplantı veya gösteride yer alan kişilerin çekilen fotoğrafları, diğer koşulları da sağlıyorsa, benzer şekilde kişisel veri sayılır[43]. Bir çocuğun, velayet davası için yapılan psikiyatrik değerlendirmesinde, anne ve babası hakkında ne hissettiğini anlamak için, değerlendirmenin bir parçası olarak yaptığı çizimler, söz konusu resim çocukla ilgili akıl ve ruh sağlığı gibi bilgileri ortaya koyduğu sürece kişisel veri olarak kabul edilebilir[44]. Zira pedagog bu resimden çıkaracağı sonuçla ilgili bir rapor hazırlayacaktır. Kişinin, bir belgenin kendinden sadır olduğunu veya belgedeki ifadeleri onayladığını gösteren karakteristik işareti olan ıslak imzası da kişisel veri sayılır[45]. Günümüzde hayatın çeşitli alanlarında kullanılmaya başlayan elektronik ve mobil imza, PIN kodlarıyla birlikte olsun veya olmasın, bir kişinin kimliğini belirleme ve doğrulamaya muktedir bir araç olduğundan tıpkı ıslak imza gibi kişisel veri sayılabilir[46]. İmzaya ek olarak zaman zaman onun yerine

[39] Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data", **Avrupa Komisyonu Web Sitesi**, 2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm, (E.T. 08.03.2022), (Opinion 4/2007), s. 6; Turgut, s. 176.

[40] Selen Uncular, **İş İlişkisinde İşçinin Kişisel Verilerinin Korunması**, 2. Baskı, Seçkin Yayıncılık, Ankara, 2018 s. 33.

[41] Dülger, s. 156. Turgut, s. 174.

[42] Yargıtay Ceza Genel Kurulu, 17.06.2014 tarih ve E.2012/12-1510, K.2014/331 sayılı kararı; Article 29 Data Protection Working Party, Opinion 4/2007, s. 7; Dülger, s. 156; Turgut, s. 175.

[43] AİHM, 24.01.2019 tarih ve 43514/15 başvuru numaralı Catt/Birleşik Krallık kararı, https://hudoc.echr.coe.int/, (E.T. 09.03.2022). Bu kararda, başvurucunun adı, doğum tarihi ve adresi gibi kişisel verileriyle birlikte gösteri sırasında çekilen fotoğrafları da polis tarafından kayıt altına alınıştır. Mahkeme bu bilgilerin kişisel veri olduğunu belirtmiştir.

[44] Article 29 Data Protection Working Party, Opinion 4/2007, s. 8; Turgut, s. 178.

[45] Article 29 Data Protection Working Party, Opinion 4/2007, s. 8.

[46] Fundamental Rights Agency, **Handbook on European Data Protection Law**, 2018, s. 95.

geçebilen parmak izi[47], avuç izi[48], DNA profili[49], el geometrisi[50], retina deseni, avuç içi damar izi, kulak kanalı[51] ve hatta kişinin adımlama tarzı gibi kişide yer edinmiş diğer karakteristik özellikler de biyometrik veri sayılmakta, dolayısıyla kişisel veri olarak kabul edilmektedir[52]. Ancak biyometrik verinin üretildiği kaynak, mesela parmağın kendisi, kan ve tükürük örneği, saç teli vb. bu kapsamda değerlendirilemez.

Kişisel verinin kavramının kapsamı belirlenirken değinilmesi gereken bir başka önemli konu ise, verinin tutulduğu ortamın bu bağlamda etkili olup olmayacağıdır. Bilginin kağıt üzerinde, bilgisayar gibi elektronik bir ortamda, yedekleme ve arşivleme amacıyla kullanılan bir taşınabilir bellek içerisinde veya bir çevrimiçi veri tabanında bulunması, kişisel veri olma mahiyetini değiştirmez[53]. Örneğin, kişinin bilgisayardaki bir metin belgesinde yer alan kan grubu bilgisi, arkadaşına gönderdiği bir e-posta, bulut sisteminde yedeklenmiş vesikalık fotoğrafı ve taşınır belleğe yedeklediği çocukluk videoları, diğer koşulları da haiz olduğu sürece birer kişisel veri niteliğindedir.

Tüm bu ayrım ve örneklemlerden yola çıkarak, bazı verilerin işlendiğinde ilgili kişiler için risk oluşturabilecek ve daha gelişmiş korunmaya ihtiyaç duyan nitelikte olduğu sonucuna varmak kaçınılmazdır. Bu nedenle gerek uluslararası gerekse de ulusal hukuki düzenlemelerde, kişisel veriler genel ve özel (hassas) nitelikli olarak bir sınıflandırmaya tabi tutulmuştur. Ayrıca doktrin ve çeşitli yargı mercileri, kişinin yaşamının farklı yönlerine göre kolaylaştırıcı bir tasnif yoluna da gitmiştir. Buna göre

---

[47] AİHM, 24.03.1982 tarih ve 8022/77, 8025/77 ve 8027/77 başvuru numaralı McVeigh, O'Neill ve Evans/Birleşik Krallık kararı; 18.04.2013 tarih ve 19522/09 başvuru numaralı M.K./Fransa kararı; 13.02.2020 tarih ve 45245/15 başvuru numaralı Gaughran/Birleşik Krallık kararı, https://hudoc.echr.coe.int/, (E.T. 10.03.2022).

[48] 11.07.2020 tarih ve 74440/17 başvuru numaralı P.N./Almanya kararı, https://hudoc.echr.coe.int/, (E.T. 10.03.2022).

[49] 13.02.2020 tarih ve 53205/13 ve 63320/13 başvuru numaralı Trajkovski ve Chipovski/Kuzey Makedonya kararı; 14.04.2020 tarih ve 75229/10 başvuru numaralı Dragan Petrović/Sırbistan kararı, https://hudoc.echr.coe.int/, (E.T. 10.03.2022).

[50] Kişisel Verileri Koruma Kurulu, 07.07.2022 tarih ve 2020/662 sayılı kararı, https://www.kvkk.gov.tr/Icerik/7399/2022-662, (E.T. 28.03.2023).

[51] Metin Bulut, "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", **Ankara Barosu Dergisi**, Cilt: 78, Sayı: 3, Ankara, 2020, s. 114.

[52] Article 29 Data Protection Working Party, Opinion 4/2007, s. 7; Dülger, s. 157; AİHM, 04.12.2008 tarih ve 30562/04 başvuru numaralı S. Marper/Birleşik Krallık kararı, https://hudoc.echr.coe.int/, (E.T. 10.03.2022).

[53] Article 29 Data Protection Working Party, Opinion 4/2007, s. 7; Dülger, s. 156.

kişinin yaşam şekli, ekonomik ve finansal, bilişimsel, sağlıksal ve politik kişisel veriler olmak üzere gruplamalar yapılmıştır[54].

b. Kişiyi Belirli veya Belirlenebilir Kılma

Kişisel verinin tanımı yapılırken bahsedildiği üzere, eldeki verinin kişisel nitelikte sayılması için bir gerçek kişiyi belirlemesi veya belirlenebilir kılması gerekmekteydi. En yalın haliyle ifade etmek gerekirse, bir bireyi diğerlerinden ayırdığımızda, o bireyi belirlemiş oluruz. Belirleme; o bilginin kişiyi diğerlerinden ayırt etmeye, derhal veya bir araştırma sonucunda yaramasıyla gerçekleşecektir. Bir başka deyişle, iki durumda kişisel verinin varlığından bahsetmek mümkündür: Eldeki bilgiler kişiyi belirli veya belirlenebilir hale geliyorsa veya kimliği belirlenememiş olsa da, araştırma sonucu ilgili kişinin kimliğini tespiti mümkün kılıyorsa. Örneğin, birine "Zeynep" diye adıyla seslendiğimizde onu belirlemiş oluruz. Zira insanın adı, onun doğrudan tanınmasını sağlayacak şeylerin başında gelir[55]. Fakat aynı isimde başkaları da olabileceği göz önüne alındığında; kişinin fotoğrafı, kimlik numarası, araç plakası, mesleği veya fiziksel özellikleri gibi tanımlayıcılar olmaksızın kişinin belirlenebilmesi mümkün olmayabilir. Ülkemizde kullanılan en yaygın kadın isimlerinden biri olduğu için binlerce Zeynep vardır[56]. Ancak o an karşımızda oturan Zeynep'e sesleniyorsak artık bu kişi, çok sayıda Zeynep'ten biri olmayacaktır. Bu durumda Zeynep'in "konumu", onu belirlemekte kullandığımız ek bir bilgidir[57]. İşte bu şekilde, kişiyle yakından ilgili olan ve onun topluluk içerisinde diğerlerinin arasından sıyrılmasını sağlayacak türden olan her bilgiye "tanımlayıcı" denir. Bu bilgiler, ilgili olduğu kişiye özel ve sıkı bir bağla bağlıdır[58]. GDPR m. 4/1'de tanımlayıcıların; "kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre doğrudan veya dolaylı

---

[54] Fundamental Rights Agency, ss. 325-343; Turgut, ss. 177-178.

[55] Article 29 Data Protection Working Party, Opinion 4/2007, s. 13.

[56] İçişleri Bakanlığı'nın açıklamasına göre, sadece 2022 yılında kız bebeklere en çok verilen isim Zeynep olmuştur. (İçişleri Bakanlığı, "2022 Yılında Türkiye'de En Çok Tercih Edilen İsimler Belli Oldu", **İçişleri Bakanlığı Web Sitesi**, 01.01.2023, https://www.icisleri.gov.tr/2022-yilinda-turkiyede-en-cok-tercih-edilen-isimler-belli-oldu#:~:text=Kız%20bebeklere%20en%20çok%20verilen,bebeğe%20ise%20Asel%20ismi%20konuldu, (E.T. 30.09.2023).

[57] Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Basım Yayın, İstanbul, 2008, s. 122.

[58] İlke Gürsel, **İşçinin Kişisel Verilerinin Korunması Hakkı**, Adalet Yayınevi, Ankara, 2016 s. 7.

olarak atıfta bulunduğu isim, kimlik numarası, konum verileri ve çevrim içi nitelikli" (IP adresi, çerezler[59], radyo frekansı[60] gibi[61]) bilgiler olabileceği ifade edilmişse de elbette bu sayım tahdidi değildir. Bu hükümden anlaşılacağı üzere, tanımlayıcılar doğrudan veya dolaylı nitelikte olabilir.

Doğrudan tanımlayıcılar, eldeki bilgilerden başka bir şey kullanmadan kişiyi direkt olarak ayırt etmeye yarar. Önceki örnekte, adını ve yerini bildiğimiz için Zeynep'i doğrudan teşhis etmek mümkündü. Fakat ismini bilmeseydik de konumu ve başka bir özelliğinden (örneğin saç ve göz rengi gibi) yola çıkarak Zeynep'i doğrudan tanımlamak yine mümkün olacaktı. Dolaylı tanımlayıcılarla, bir kişiyi sadece o bilgilerden yola çıkarak belirlemek mümkün değildir. Yani, bu durumda kişiyi belirlemek için, sahip olunan diğer verileri veya başka bir kaynaktan makul yollarla erişebilecek verileri kullanmak gerekmektedir. Başka bir kaynaktan erişilmesi gereken bilgilere ulaşan kişi, elinde halihazırda veri bulunan kişi veya bu kişi dışında üçüncü bir şahıs olabilir. Örnek vermek gerekirse, diyelim ki aracını park yasağı olan yere bırakan birini şikayet etmek için araç plakasının fotoğrafını çektik ve emniyet güçlerine çevrim içi yoldan ihbar amacıyla gönderdik. Bu durumda aracın sahibinin kim olduğunu bilmediğimiz açıktır. Fakat polisin elindeki veri tabanı aracılığı ile plaka sahibinin Zeynep olduğunu öğrenmesi mümkündür. Bu durumda aracın plakası, kimliğini biz bilemeyecek olsak da üçüncü şahıslar için Zeynep'i belirlenebilir kılmaktadır. Benzer şekilde, belirli bir kurumun müdürü ile toplantı yapmamız gerektiğini varsayalım. Müdürün kimliğini bilmiyor olsak da mevzubahis kurumun internet sitesine girerek müdürün Zeynep olduğunu öğrenmemiz mümkündür. Fark edileceği üzere, Zeynep'in kimliği dolaylı yoldan ve elimizin altında bulunan makul

[59] Çerezler (cookies) basitçe ifade etmek gerekirse, ziyaret edilen internet siteleri tarafından kullanıcıların birtakım bilgilerinin cihazlarında depolandığı küçük dosyalardır (Kişisel Verileri Koruma Kurumu, **Çerez Uygulamaları Hakkında Rehber**, KVKK Yayınları, Ankara, 2022, (Çerez), s. 8).

[60] RFID (Radyo Frekansıyla Tanımlama), nesnelerin tanımlanması ve izlenmesi için kullanılan eski bir teknolojidir. Nesnelere etiket yerleştirilir ve bu etiketler nesnenin benzersiz kimlik bilgilerini taşır. Bu bilgiler, bir RFID okuyucu veya tarayıcı tarafından radyo frekansı sinyali kullanılarak okunabilir. (Fatih Maraşlı ve Musa Çıbuk, "RFID Teknolojisi ve Kullanım Alanları", **Bitlis Eren Üniversitesi Fen Bilimleri Dergisi**, Cilt: 4, Sayı: 2, 2015, s. 252).

[61] GDPR 30 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr.eu/recital-30-online-identifiers-for-profiling-and-identification/, (E.T. 11.03.2022).

bir yolla artık belirli hale gelmiştir. Bu noktada önemli olan verinin kişiyi belirleme potansiyelidir[62].

Burada dikkat edilmesi gereken başka bir konu da "makul yolun" ne olduğudur. Zira zaman ilerleyip teknoloji geliştikçe bir kişiyi belirli veya belirlenebilir kılacak yöntemler de artmaktadır. Bugün var olmayan bir yöntem, gelecekte bulunup kullanılmaya başlanabilir. Bu nedenle uzun süre saklanan verilerin, yeni teknolojiyle birleştirilerek kişilerin dolaylı yoldan tanımlanmasını önlemek için sürekli gözden geçirilmesi gerekmektedir[63]. Kişinin ileride belirlenebilir hale gelmesi illa bir teknolojik gelişme ile de olmayabilir. Örneğin faili meçhul bir cinayette, olay yerinde katilin parmak izi ve DNA örneğinin bulunduğunu düşünelim. Kişinin kimliği şu an kimliği bilinmese de ileride yakalanması veya kimliğinin bir şekilde ortaya çıkması mümkündür. Bu nedenle söz konusu biyometrik veriler katili belirlenebilir kılar, polisin de bu verileri sisteme kaydetmesi veri işleme sayılır.

Avrupa Birliği Adalet Divanı'nda (ABAD) görülen bir davada[64]; bir menajerlik şirketi olan SABAM, bir internet servis sağlayıcısı olan Scarlet'tan servis kullanıcılarının kendi müşterilerine ait eserlerin telif haklarını ihlal eden dosya paylaşımını önlemek için elektronik iletişimleri filtreleyecek bir sistem kurmasını istemiştir. Sistemin (statik) IP adreslerini işleyerek çalışacağı ve IP adresleri de kullanıcıların kimliklerini açıkça belirli kılacağı için böylesi bir sistemin varlığının kişisel verilerin korunması hakkını ihlal edeceği sonucuna varılmıştır[65]. Hatta ABAD, başka bir kararında[66] internete her bağlanıldığında değişen "dinamik IP adreslerini" de kişiyi belirlenebilir kıldığı için kişisel veri olarak kabul etmiştir. Zira Alman devlet kurumları, siber saldırıları önlemek için internet sitelerine erişenlerin dinamik IP adreslerini saklamakta ve gerektiğinde cezai işlem başlatmak için internet servis

---

[62] İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayınları, Ankara, 2017, s. 43; Turgut, s. 183.

[63] Article 29 Data Protection Working Party, Opinion 4/2007, s. 15; GDPR 26 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-26/, (E.T. 11.03.2022).

[64] ABAD, 24.11.2011 tarih ve C-70/10 numaralı Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) kararı, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62010CJ0070, (E.T. 15.03.2022).

[65] Virginia Keyder, "Introductory Note To The European Court Of Justice: Scarlet Extended SA v. Société Belge Des Auteurs, Compositeurs, Et Editeurs SCRL (SABAM)", **International Legal Materials**, Cilt: 51, Sayı: 2, 2012, s. 391.

[66] ABAD, 19.10.2016 tarih ve C-582/14 numaralı Patrick Breyer v Bundesrepublik Deutschland kararı, https://curia.europa.eu/juris/liste.jsf?num=C-582/14, (E.T. 15.03.2022).

sağlayıcılarından kişinin kimliğini öğrenebilme imkanına sahiptir[67]. Fakat kararda kişinin belirli veya belirlenebilir kılınmasının, kanunen izin verildiği yahut makul olmayacak derecede çok zaman, emek ve kaynak gerektirdiği için fiilen imkansız sayılabileceği durumlarda, artık verinin bu nitelikten yoksun olabileceği belirtilmektedir. Elbette bu husus; işlemenin amacı, tanımlamanın ekonomik yükü ve yararları, veri kontrolörünün niteliği ve yararlanılan teknolojik imkanlar gibi kriterler göz önünde bulundurularak her vaka için ayrı bir şekilde titizlikle değerlendirilmelidir. ABAD yakın tarihli başka bir kararında daha benzer şekilde düşündüğünü göstermiştir[68]. Divan'ın bu yaklaşımının GDPR'nin 26 No'lu Gerekçesi ve Madde 29 Çalışma Grubu'nun yetkili olarak hazırladığı kılavuzla uyuşmadığını savunanlar da mevcuttur. Zira her iki kaynak da özellikle "geri alınması mümkün olmayan anonimleştirme" ve "kimliğin belirlenmesinin makul biçimde imkansızlığı" konusunda vurgu yapmakta ve bu hususta koşullar ne olursa olsun risk almayı uygun bulmamaktadır[69]. Gerçekten de söz konusu verinin nerede, ne amaçla ve ne kadar süreliğine saklanacağı bilinmediği, gelecekte yaşanabilecek teknolojik gelişmeler sonucunda bu hususta kabul edilen "makul" tanımının değişebileceği ve kişisel verileri suç işlemekte kullanma gibi saiklerdeki hızlı ilerlemenin, belirlenebilirliğin kapsamını genişletebileceği göz önüne alındığında bu görüşe katılmak mümkündür.

Elbette bunun tam tersi de yaşanabilir. Kişi, belirlenebilir değilken belirlenebilir hale gelebildiği gibi, belirlenebilir nitelikteyken belirlenemez hale de gelebilir. Örneğin kişisel veriler üzerinde anonimleştirme işlemi yapılması buna bir örnektir. Anonimleştirme, KVKK m. 3/1-b'de tanımlandığı üzere, "kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini" ifade eder. Kişisel verilerin resmi istatistik ile anonim duruma getirilmek marifetiyle araştırma, planlama ve

[67] Ayrıca bkz. ABAD, 20.12.201 tarih ve C-434/16 numaralı Peter Nowak v Data Protection Commissioner kararı, https://curia.europa.eu/juris/liste.jsf?num=C-434/16, (E.T.15.03.2022). Söz konusu kararda, belirlenebilirliğin sağlanması için kişiye ait verilerin illa tek bir kişinin elinde olmasına gerek olmadığı ifade edilmektedir.

[68] ABAD, 17.07.2021 tarih ve C-597/19 numaralı Mircom International Content Management & Consulting (M.I.C.M.) Limited v Telenet BVBA kararı, https://curia.europa.eu/juris/liste.jsf?num=C-597/19, (E.T. 15.03.2022).

[69] Sophie Stalla-Bourdillon ve Alison Knight, "Anonymous Data v. Personal Data – A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data", **Wisconsin International Law Journal**, Cilt: 34, 2016, s. 284; Michèle Finck ve Frank Pallas, "They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR", **International Data Privacy Law**, Cilt: 10, Sayı: 1, 2020, s. 7.

istatistik gibi gayelerle işlenmesi durumunda GDPR ve KVKK düzenlemeleri uygulanmaz. Zira bu halde kişisel veri olma özelliğini kaybederler[70]. Anonimleştirme işlemi için çeşitli rastgele hale getirme ve genelleştirme teknikleri uygulanır[71]. Fakat hangi teknik kullanılmış olursa olsun anonimleştirme işleminin geri alınamaz yani kişiyi yeniden belirli veya belirlenebilir kılamaz nitelikte olması gerekir. Aksi takdirde eldeki veriler yeniden kişisel veri sayılacaktır[72]. Örneğin, GDPR m. 11'den yola çıkarak; verileri anonimleştirilmiş bir kimsenin verileri üzerindeki haklarını kullanmak için kontrolöre kimliğinin teşhisine imkan veren ek bilgiler sağlarsa, o zaman daha önce anonim hale getirilen verilerin, tekrar kişisel veri haline geleceğini söylemek mümkündür.

Kişiyi belirli veya belirlenebilir olmaktan korumak için kullanılan bir diğer yöntem ise psödonimleştirmedir. İlgili kişilere yönelik riskleri azaltmanın bir yolu ve bilimsel, tarihsel veya istatistiksel araştırmalar için kullanılan verileri koruma aracı olarak kullanılır[73]. Yalnız dikkat edilmelidir ki psödonimleştirme, anonimleştirmeden farklı olarak bilgiyi kişisel veri olmaktan çıkarmaz, dolayısıyla söz konusu veriler hala KVKK ve GDPR hükümlerine tabidir. Bu işlemde veri öyle bir işlenir ki ek bir bilgi olmaksızın sırf o veriden hareketle verinin sahibini teşhis etmek mümkün olmaz. İşleme esnasında veri setindeki bir kısım rumuz niteliğindeki verilerle değiştirilir[74]. Bunu yaparken anahtar kodlama[75], takma isim kullanma, maskeleme[76] ve karartma[77]

---

[70] Gökçe Filiz Çavuşoğlu, **Kişisel Verilerin Yapay Zekayla İşlenmesinden Doğan Özel Hukuk Sorunları**, Yetkin Yayınları, Ankara, 2021, s.28.

[71] Bu hususta detaylı bilgi için lütfen bkz. Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, https://commission.europa.eu/index_en, (E.T. 17.03.2022).

[72] Bozkurt, s. 31.

[73] Miranda Mourby, Elaine Mackey, Mark Elliot, Heather Gowans, Susan E. Wallace, Jessica Bell, Hannah Smith, Stergios Aidinlis ve Jane Kaye, "Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK", **Computer Law & Security Review**, Cilt: 34, Sayı: 2, 2018, s. 223.

[74] Dülger, s. 165.

[75] Kişisel bilgileri içeren örneğin isim, doğum tarihi veya adres gibi kimlik bilgilerinin kod veya takma adlarla değiştirilmesi anlamına gelen psödonimleştirilmiş verileri ifade eder. İlgili anahtar, takma adı orijinal kimlik bilgileri ile eşleştiren bilgi ayrı bir yerde saklanır. (Article 29 Data Protection Working Party, Opinion 4/2007, s. 18)

[76] "Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemlerdir." (Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi**, KVKK Yayınları, Ankara, 2018, s. 3).

[77] "Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması gibi işlemlerdir." (Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi**, s. 3).

gibi yöntemler kullanılır. Mevzubahis ek bilgiler de teknik ve organizasyonel önlemler alınarak bunlardan ayrı tutulur[78]. Anlaşılacağı üzere geri alınabilecek şekilde psödonimleştirilmiş veriler, daha önceden belirlenmiş koşullar altında, kişilerin kimliğinin dolaylı olarak belirlenebilirliğini sağlar[79].

Son olarak, yanlış ve eksik veriler de kişiyi belirli veya belirlenebilir kıldığı sürece kişisel veri sayılmaktadır. Örneğin, bir şirketin İzmir şubesinde çalıştığı düşünülen Zeynep Kaya, gerçekte Ankara şubesinde çalışıyorsa ve İzmir şubesinde de bu isimde başka biri yoksa, o zaman Zeynep hakkındaki bu bilgi yanlış olsa da onu belirli veya belirlenebilir kılmaktadır. Belirlilik veya belirlenebilirliğin herkes tarafından algılanmasına gerek yoktur. Bir grup insan tarafından ve hatta tek bir kişi tarafından bile tespit edilebiliyorsa yine kişisel veri niteliğini haizdir.

Tüm bu açıklamalardan çıkarılacak sonuç, kişisel verinin zaman içerisinde değişen dinamik bir kavram olduğudur. Çünkü imkanlar geliştikçe kişilerin belirli veya belirlenebilir kılınma yöntemleri değişip gelişmektedir. Fakat unutulmamalıdır ki kişisel verilerin korunması hukukunda amaç veriyi değil, verinin ilişkin olduğu kişiyi korumaktır[80]. Bu nedenle söz konusu *kişinin* belirli veya belirlenebilir olması önem arz etmektedir.

c. Kişiye İlişkin Olma

Kişisel verinin tanımından çıkarılan üçüncü koşul, verinin gerçek bir kişiye ilişkin olması kriteridir. Yalın bir şekilde ifade etmek gerekirse; eldeki bilgi, bir kişiyle ilgili olduğunda, o kişiye "ilişkin" olarak kabul edilir. Yani kişiyi belirli veya belirlenebilir kılan şey, esasında kişi ve veri arasındaki bu "ilgi" bağıdır. Çoğu zaman ikisi arasındaki bağı tespit etmek kolaydır. Bireyin adı, doğum yeri, kimlik numarası, işyerinde hakkında tutulan özlük dosyasında yer alan performans bilgileri, adli sicil kaydında yer alan mahkumiyet kaydı gibi bilgileri doğrudan kişinin şahsıyla alakalıdır. Fakat bazı durumlarda, aradaki bağ bu kadar net olmayabilir. Örneğin araç şase numarası, doğrudan kişiye değil, kişinin maliki olduğu eşyaya atfedilen bir bilgidir. Kişi ile şase numarası arasındaki bağı, kişinin araç üzerinde sahip olduğu mülkiyet

[78] Finck ve Pallas, s. 17.
[79] Article 29 Data Protection Working Party, Opinion 4/2007, s. 18.
[80] Turgut, s. 182.

hakkı kurar. Yahut şahsın evinde akıllı termostat veya hava kalitesi monitörü gibi bir akıllı cihaz olduğunu düşünelim. Bu cihaz tarafından toplanan veriler, kişinin günlük rutini ve yaşam tarzı hakkında bilgi verecek cinsten olacaktır. Bu durumda kişi ile günlük rutini ve yaşam tarzına ilişkin verileri arasındaki bağı, kişinin akıllı cihaza olan fiziksel yakınlığı kurmuş olur. Görüldüğü üzere, bu hallerde kişi ile veri arasındaki alaka dolaylı türdendir.

Hakkındaki bilgiden bahsedilirken kişinin adı geçmemesi veya kimliğinin belirli olmaması, bu bilginin ona ilişkin olmadığı anlamına gelmez. Kişinin kimliği belirlenebilir olduğu sürece de, önceki başlıkta izah edildiği üzere, söz konusu veri kişiye ilişkin sayılacaktır. Yine, bir veri bazen birden çok kişiyle de ilgili olabilir[81]. Örneğin, orak hücreli anemi hastasının bu durumuna ilişkin verinin, hastalık kalıtsal yollarla aktarıldığı için aynı zamanda ailesinin diğer üyelerine de ilişkin olma ihtimali vardır. Bu durumda bilgilere erişim ve kullanım konusunda dikkat edilmelidir.

Verinin "kişiye ilişkin olması" ile "kişi hakkında" olması aynı şey değildir. Önceki ifade sonrakini kapsar[82]. Esasen verinin şahsa ilişkin olma kriterinin tayininde üç farklı ve birbirine alternatif[83] olabilen unsurdan en az birinin varlığı aranır[84]. Bunlardan birincisi ve akla ilk geleni "içerik" unsurudur. Eğer eldeki veriler; kişinin kimliğine, özelliklerine veya davranışlarına atıfta bulunuyorsa[85], "içerdiği bilgiler" nedeniyle o kişi hakkında ve dolayısıyla o kişiye ilişkin olacaktır. Örneğin, bir süpermarketin indirim kartı üyeliği için topladığı müşteri verileri; o müşterilerin isimleri, adresleri, telefon numaraları ve sipariş geçmişleri gibi bilgileri içermektedir. Bu verilerin içerikleri nedeniyle bir kişiye ilişkin olduğu açıktır.

İkinci unsur, "amaç" unsurudur. Veri, bir kişinin durumunun veya davranışının değerlendirilmesinde ya da etkilenmesinde yahut bunlara göre muamele görmesinde kullanılıyor veya kullanılması muhtemel oluyorsa, kişiyle amaç bakımından ilgilidir[86]. Örneğin, bir banka, kredi başvurusunda bulunanların kredi notlarını hesaplamak bir algoritma geliştirmiş olsun. Algoritma maaş, borç ve aktif malvarlığı gibi çeşitli

[81] Article 29 Data Protection Working Party, Opinion 4/2007, s. 12.
[82] Nadezhda Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law", **Law, Innovation and Technology**, Cilt: 10, Sayı: 1, 2018, s. 53.
[83] Article 29 Data Protection Working Party, Opinion 4/2007, s. 11.
[84] Aksoy, s. 28.
[85] Article 29 Data Protection Working Party, Opinion 4/2007, s. 10.
[86] Article 29 Data Protection Working Party, Opinion 4/2007, s. 10.

bilgileri göz önüne alarak kişinin kredi başvurusunun onaylanıp onaylanmayacağını belirlesin. Bu durumda, algoritmanın kullandığı bu veriler, kişinin mali durumu ile davranışını değerlendirmek ve ona göre muamele görmesini amacıyla kullanıldığı için artık açıkça kişiye ilişkindir.

"Sonuç" unsuru ise bu hususa ilişkin üçüncü ve son unsurdur. Buna göre; eldeki verinin kullanılmasının, kişinin hakları ve menfaatleri üzerinde etkili olma ihtimali varsa, yine o kişiye ilişkin olarak kabul edilir. Üstelik bu etkinin büyük olmasına da gerek yoktur[87]. Diyelim ki bir sosyal medya platformu, kullanıcısının arama geçmişi ve konumu gibi bilgilerini kullanarak ona kişiselleştirilmiş reklamlar gösteriyor olsun. Kişi de arama motoruna "böbrek taşı ameliyatı" yazıp sonuçları görüntülesin. Platform bu bilgiyi, kişinin evine yakın mesafede yer alan ve söz konusu ameliyatı yapabilecek hastanelere ilişkin reklamları göstermek için kullanırsa, kişinin sağlık durumuyla ilgili hassas bilgileri üçüncü şahıs reklamcılara ifşa etmiş olabilir. Bu durum da kullanıcının kişisel sağlık bilgileriyle ilgili olarak özel yaşamın gizliliği ve mahremiyet haklarını etkileyebilir.

ABAD ilk defa Y.S. ve diğerleri kararında[88], kişisel veri tanımında yer alan "ilişkin olma" kriterinin anlamını detaylı bir şekilde tartışmıştır. Kararın konusu şudur: Y.S. ve beraberindeki iki ayrı şahıs Hollanda'ya iltica başvurusu yapmışlardır. Başvurularını incelemek amacıyla yapılan mülakat sırasında görevli memur tarafından bir tutanak tutulmuştur. Tutanağın birinci kısmında adı, telefon numarası ve dahilisi gibi memura ilişkin bilgiler; ikinci kısmında isim, doğum tarihi, cinsiyeti, uyruğu, etnik kökeni, dili, dini, başvuru geçmişi ve sunduğu belgeler gibi başvuruculara ilişkin bilgiler; üçüncü kısmında ise devam eden başvuruya ilişkin olarak yürürlükte olan hukuk uyarınca yapılan değerlendirmeler yer almaktadır. Başvurucular haklarında verileri içeren tutanağın kopyasını istemişse de yetkili makam tarafından kendilerine sadece tutanakta yer alan verilerin bir listesi verilmiş, hukuki değerlendirmeyi içeren kısmı ise tamamen kapsam dışı bırakılmıştır. ABAD önüne gelen bu dosyada, söz konusu hukuki değerlendirmenin kişisel veri sayılıp sayılamayacağını değerlendirmiş ve değerlendirme metninin kişilerle ilgili birtakım bilgiler içerse de kişisel veri olarak

[87] Article 29 Data Protection Working Party, Opinion 4/2007, s. 11.

[88] ABAD, 17.07.2014 tarih ve C-141/12 numaralı Y.S. and others v. Minister voor Immigratie, Integratie en Asiel kararı, https://curia.europa.eu/juris/liste.jsf?num=C-141/12&language=en, (E.T. 05.04.2022).

değerlendirilemeyeceği sonucuna varmıştır. Halbuki yukarıda izah edildiği üzere; söz konusu metin, kişilerin hukuki statüsünün değerlendirilmesinde kullanılacağı ve 1951 tarihli Cenevre Sözleşmesi'nde sayılan durumlar sonucunda kaçarak oraya sığındıkları düşünüldüğünde, temel hak ve özgürlüklerini etkileyeceği için amaç ve sonuç bakımından kişiye ilişkin olarak kabul edilmeliydi. Fakat Divan ilişkin olma kriterini burada dar anlamda, yani sadece içerik bakımından yorumlayarak hatalı bir karar vermiştir.

Yeni tarihli Peter Nowak kararında[89] ise, Divan bu dar kapsamlı yorumunu terk etmiştir. Muhasebeci olmak amacıyla aşamalı bir dizi sınava tabi tutulan başvurucu, kitap açmanın serbest olduğu yazılı sınavda dördüncüye başarısız olmuştur. Bu nedenle kişisel veriye erişim hakkı kapsamında, nerede hata yaptığını görmek için değerlendirilmiş sınav cevap kağıdını incelemek istemişse de, talepte bulunulan makam tarafından sınav cevaplarının kişisel veri niteliğini haiz olmadığı gerekçesi ile talebi reddedilmiştir. En nihayetinde Divan'ın önüne gelen bu uyuşmazlıkta, başvurucunun mesleki yeterlilik sınavında verdiği yazılı cevapların ve kağıdı değerlendiren sınav görevlisinin bu cevaplara ilişkin yorumlarının GDPR kapsamında kişisel veri teşkil edip etmediği hususunda karar vermek zorunda kalınmıştır. İşte tam bu noktada Divan Y.S. ve diğerleri kararındaki görüşünden vazgeçerek söz konusu kağıttaki cevapların başvurucunun zihinsel sürecinin ürünü olduğu, el yazısını içerdiği, istediği mesleğe girme şansını etkilediği için içerik, amaç ve sonuç bakımından kişiye ilişkin olduğu doğrultusunda hüküm kurmuştur. Divan ayrıca sınav görevlisi tarafından yapılan değerlendirmelerin de adayın sınav performansı, o alandaki bilgisi ve yeterliliği hakkındaki görüşünü içerdiği için kişisel veri olduğunu belirtmiştir. Görüleceği üzere, tıpkı önceki kriterler gibi, kişiye ilişkin olma kriteri de kişisel veri tanımını geniş kapsamlı[90] ve değişken kılmaktadır.

[89] ABAD, 20.12.2017 tarih ve C-434/16 numaralı Peter Nowak v Data Protection Commissioner kararı, https://curia.europa.eu/juris/liste.jsf?num=C-434/16, (E.T. 05.04.2022).

[90] 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, (Ceza Normları), s. 102.

C. Kişisel Verilerin Türleri

1. Özel Nitelikli (Hassas) Kişisel Veriler

Kişisel verilerin korunmasına ilişkin belgelerde, bazı verilerin diğerlerine göre daha çok korumaya muhtaç olduğu belirtilerek hassas veya özel niteliği haiz kişisel veriler olarak nitelendirilmiştir. KVKK'nin 6. maddesinin 1. fıkrasına göre; "kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri" özel niteliği olan kişisel veridir. Bu sayım tahdidi niteliktedir, kıyas yoluyla genişletilmesi mümkün değildir[91]. Yine GDPR'nin m. 9/1'de; "ırk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğine ilişkin bilgiler, genetik ve biyometrik veriler, sağlıkla ilgili olan veriler, cinsel yaşam veya cinsel eğilime ilişkin veriler" özel kategorideki veriler olarak düzenlenmiştir.

Bu ayrımın temelinde, bu tür verilerin kişilerin temel hak ve özgürlükleri ile daha yakından alakalı olması yatmaktadır. Hassas kişisel verilerin ifşa olması, ilgili kişi hakkında ayrımcılık yapılmasına veya çeşitli yönlerden ağır mağduriyetlere neden olabilir[92]. Örneğin, kişinin tıbbi geçmişi veya sağlık durumu gibi hassas tıbbi verilerinin ifşası, kişinin işini kaybetmesine veya sağlık hizmetlerine erişimini kaybetmesine neden olabilir. Yahut cinsel yönelimi hakkında yapılan ifşa, kişinin ayrımcılığa uğramasına, tacize maruz kalmasına veya toplumda dışlanmasına yol açabilir. Etnik kökeninin ifşası, kişinin ırkçılığa uğramasına veya ayrımcılığa maruz kalmasına sebep olabilir. Cezai geçmişi hakkında yapılan ifşa, kişinin iş bulmasını veya toplum içinde kabul görmesini zorlaştırabilir. Parmak izi veya retina taraması gibi biyometrik verilerin ifşası, kimlik hırsızlığına yol açabilir. Bu örneklerin arttırılması elbette mümkündür. İşte bu nedenlerle bu verilerin işlenmesi, ilgilisinin açık rızası olmaksızın yasaktır.

Nelerin özel nitelikli veri olarak kabul edildiği mevzuatlarda açıkça ve sınırlı olarak yazılsa da, sayılan kategorilerin kapsamına nelerin dahil edilip edilemeyeceği

[91] Ersan Şen, Mert Maviş, Alperen Gözükan, M. Enes Efe ve Fırat Çetintaş, **Savunma Hakkının Kişisel Veriler Karşısında Korunması**, Seçkin Yayıncılık, Ankara, 2022, (Savunma Hakkı), s. 27.
[92] Dülger, s. 177.

tartışma konusudur. Örneğin, kişinin adı, doğum yeri veya ikametgahı, etnik kökeni hakkında bazı ipuçları verebilir. Selanik'te doğmuş Kostas isimli birinin, yüksek ihtimalle Yunan kökenli olduğunu söyleyebiliriz. Yahut bir havayolunun rezervasyon kaydında, rezervasyonu yaptıran yolcunun helal veya koşer gıda tercih ettiğinin yazması[93], kişinin dini inancı hakkında bize bilgi verebilir. Benzer şekilde, çeşitli internet mecralarında yayınlanan veya güvenlik kameraları tarafından çekilen fotoğraflar ve görüntülerin durumu da tartışmalıdır. Bu görüntülere bakılarak, kişinin etnik kökeni veya sağlık durumuna ilişkin bilgiler edinilebilir[94]. Bu nedenle, bu tarz özel nitelikli olmayan verilerin de özel nitelikli olarak kabul edilip edilmeyeceği sorusunun akıllara gelmesi son derece doğaldır. Bu durumda dikkat edilecek husus, söz konusu verilerin işleme amacı olmalıdır. Yani veri doğrudan özel nitelikli olmadığı halde, işleme şekli ve amacı sebebiyle özel nitelikli veri işlenmesine hizmet ediyorsa, artık özel nitelikli kişisel veri işlendiğinin kabul edilmesi gerektiği ifade edilmektedir[95]. Bu bağlamda, kişinin beslenme alışkanlıkları, normalde özel nitelikli bir veri değilse de, bu veri kişinin anoreksiya veya obezite tedavisi için bir sağlık profesyoneli tarafından işleniyorsa, işlenme amacı sağlıkla ilgili olduğundan bu veri özel nitelikli bir kişisel veri olarak kabul edilebilecektir.

Ayrıca özel nitelikli veri olarak sayılan kategoriler de eleştiri konusu olmaktadır. Örneğin, felsefi inancın ne olduğunu tanımlamak zordur. İngiltere'de bir mahkeme, kişinin iklim değişikliğine olan inancını, felsefi bir inanç olarak kabul etmiştir[96]. Farklı ülkelerdeki mahkemeler, hatta aynı ülkede başka bir mahkeme, aynı görüşü paylaşacak mıdır? KVKK'de özel nitelikli veriler için hem tahdidi bir sayım yapılmış hem de "kişilerin diğer inançları" denilerek hükmü yorum yoluyla genişletmeye açık kapı bırakılmıştır. Bu muğlaklığa başka bir örnek de sağlık verileri üzerinden verilebilir. Kişinin sağlığına ilişkin veriler, basit bir soğuk algınlığı veya

[93] Nicola Fulford ve Peter Carey, "Special Categories of Data", (ed. Peter Carey), **Data Protection: A Practical Guide to UK and EU Law**, 5. Edition, Oxford University Press, Croydon, 2018, s. 67.

[94] Article 29 Data Protection Working Party, "Advice paper on special categories of data ("sensitive data")", **Avrupa Komisyonu Web Sitesi**, 2011, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf, (E.T. 29.08.2023), (Sensitive Data), s. 8.

[95] Dülger, s. 179; Paul Quinn ve Gianclaudio Malgieri, "The Difficulty of Defining Sensitive Data- The Concept of Sensitive Data in the EU Data Protection Framework", **German Law Journal**, Cilt: 22, Sayı: 8, 2021, s. 1592.

[96] Article 29 Data Protection Working Party, Sensitive Data, s. 8.

beslenme ve spor alışkanlıkları hakkındaki bilgilerden, daha ciddi ve kronik hastalık tanıları, kan tahlili sonuçları veya engellilik hakkındaki bilgilere kadar değişebilmektedir. Hatta İtalya'da bir davada, aşılamadan kaynaklanan yaralanmaların mağdurlarına tazminat ödenmesini düzenleyen yasa uyarınca devletin düzenli şekilde ödeme yaptığı kişi olma bilgisi de bu kapsamda değerlendirilmiştir[97]. Akıllı telefonlarımız gün içerisinde attığımız adımları, yaktığımız kalorileri, uykuda ve ekrana bakarak geçirdiğimiz saatleri hesaplamaktadır. Bu bilgi setlerinden yola çıkılarak kişilerin sağlık durumu hakkında bilgi edinilebilmektedir. Bu gibi durumlar, hem bu tür basit verilerin sorunsuz bir şekilde işlenmesi için bile bireyin rızasının alınması gerektiğinden, uygulamada zorluklara yol açmakta[98] hem de kişilerin sıradan verilerinden yola çıkılarak özel nitelikli verilerinin ifşa edilmesi riskini doğurmaktadır. Yine, KVKK özelinde, kişilerin kılık ve kıyafetinin de özel nitelikli veri olarak yer alması eleştirilmektedir. Zira kanun lafzına bakıldığında, giyim mağazalarının internet sitelerinde müşterilerinin eski kıyafet siparişlerinin görünmesi de özel nitelikli kişisel verilerinin işlenmesi olarak sayılabilecektir ki bunun oldukça geniş ve düzenlemenin amacından sapan bir yorum olduğu ifade edilmektedir. Düzenlemenin kişinin kendi inancının ve dünya görüşünün tezahür etmesine sebep olacak şekilde giyinmesi nedeniyle herhangi bir ayrımcılığa uğrama ihtimaline karşı getirildiği ve bu kapsamda dar yorumlanması gerekmektedir[99]. Ancak kanaatimiz, bu kategorinin çok fazla geniş yorumlanmaya müsait olması nedeniyle kanundan çıkarılması yönündedir. Var olan kategorilerin muğlaklığının veya gerekli olup olmadığının yanı sıra, bazı kategorilerin de eksik olduğu düşünülmektedir. Örneğin, kişilerin konum ve ekonomik durumlarına ilişkin veriler ile çocukların verilerinin de özel nitelikli kişisel veriler içerisine dahil edilmesi önerilmektedir[100].

2. Genel Nitelikli (Hassas Olmayan) Kişisel Veriler

Veri, kanunda sayılan türden özel nitelikli bir veri değilse, genel nitelikli veri kategorisindedir. Bu başlık altında, bu hususa ilişkin olarak yeniden açıklama

[97] Quinn ve Malgieri, s. 1598.
[98] Article 29 Data Protection Working Party, Sensitive Data, s. 8.
[99] Dülger, s. 180.
[100] Article 29 Data Protection Working Party, Sensitive Data, s. 10.

yapılmayacak olup kişisel verinin unsurları ve özel nitelikli veriler başlıkları altında yapılan açıklamalara atıf yapılmakla yetinilmektedir.

D. Kişisel Verilerin Korunması

1. Genel Olarak

Dar anlamda kişisel verilerin korunmasının, veri güvenliği ve bunun sağlanması için alınan önlemleri ifade ettiği söylenebilir. Hem GDPR hem KVKK, üzerinde bağlayıcı etkisi olduğu kişi ve kurumların; kişisel verilere erişme, kullanma ve koruma şekillerini dikkatlice planlamaları hususunda biz dizi kural öngörmüştür. Verilerin yeterli şekilde korunmaması sonucu ihlallerin ortaya çıkması durumlarında da veri koruma otoriteleri tarafından yüksek meblağda para cezaları kesilmektedir. Örneğin, İrlanda Veri Koruma Komisyonu, 2023 yılının mayıs ayında, AB'deki kullanıcılarının kişisel verilerinin yeterli veri koruma mekanizmaları olmadan ABD'ye aktarması nedeniyle Meta'ya (eski adıyla Facebook) 1,2 milyar euro tutarında para cezası vermiştir[101]. Benzer şekilde, 2021 yılında Lüksemburg Ulusal Veri Koruma Komisyonu tarafından, kullanıcılardan gerekli izinler alınmadan kişiselleştirilmiş reklamlar göstererek GDPR'a aykırı surette veri işlediği gerekçesiyle Amazon'a 746 milyon euro para cezası verilmiştir[102]. Ülkemizde ise Kişisel Verileri Koruma Kurulu, 21 milyonu aşkın üye verisinin ihlale uğradığına dair yaptığı ihlal bildiriminin incelenmesine yönelik olarak, gerekli teknik ve idari tedbirler alınmadığı için Yemeksepeti'ne 1,9 milyon Türk Lirası para cezası vermiştir[103]. Facebook'a ise; bazı üçüncü taraf uygulamaların, Türkiye'den yaklaşık 300 bin kişinin fotoğraflarına, 12 gün boyunca yetkisini aşan düzeyde erişim sağlayan bir yazılım bozukluğunun sebep

[101] European Data Protection Board Web Sitesi, https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_en, (E.T. 10.10.2023).

[102] Data Privacy Manager Web Sitesi, https://dataprivacymanager.net/luxembourg-dpa-issues-e746-million-gdpr-fine-to-amazon/, (E.T. 10.10.2023).

[103] Kişisel Verileri Koruma Kurulu, 23.12.2021 tarihli ve 2021/1324 sayılı kararı, https://www.kvkk.gov.tr/Icerik/7168/2021-1324, (E.T. 10.10.2023).

olduğu veri ihlali sonucunda, gerekli tedbirlerin alınmadığı ve ihlalin bildirilmediği gerekçesiyle toplam 1,65 milyon Türk Lirası para cezası verilmiştir[104].

GDPR m. 24'te veri sorumlusunun, veri işleme faaliyetinin kurallara bağlı olarak yerine getirilmesini için "uygun teknik ve organizasyonel önlemleri" alma ve uygulama yükümlülüğü hüküm altına alınmıştır. Veri sorumlusu bu yükümlülüğünü yerine getirebilmek için, özellikle tasarımla veri koruma[105] ve varsayılan ayarlarla veri koruma[106] ilkelerini karşılayan iç politikalar ve önlemleri benimseyerek uygulamalıdır[107]. Bu önlemler; kişisel verilerin işlenmesinin en aza indirilmesi, verilerin mümkün olan en kısa sürede psödönimleştirilmesi, şifreleme gibi çeşitli siber güvenlik önlemleri alınması, çalışanlara veri güvenliği hakkında eğitimler verilmesi, toplanan kişisel verilere sadece gerekli personelin ulaşabilmesini sağlamak gibi birtakım fiziksel önlemlerin alınması, verilerin belirli süreliğine saklanması, veri ihlali protokolü oluşturulması gibi önlemler olabilir.

Geniş anlamda kişisel verilerin korunması ise, çeşitli hukuki düzenlemelerde bireylere tanınan kişisel verilerin korunması hakkıdır. Burada ayrıca, kişisel veri korumasının sadece hak düzeyinde koruma açısından; verilerin korunmasının önemi, korunmasına ilişkin temel hukuki düzenlemeler ve korunmasının hukuki niteliğinden oluşan üç ana başlık altında incelenecektir.

2. Kişisel Verilerin Korunmasının Önemi

Verilerin bilişsel süreçten geçirilerek anlam kazandırılmış hali olan bilgi, çok yönlü bir öneme sahiptir. Bireylerin kimliklerini şekillendirmenin ve toplumların kültürel mirasını koruyup aktarmanın yanı sıra, iletişimi güçlendirir, eğitim ve

---

[104] Kişisel Verileri Koruma Kurulu, 11.04.2019 tarih ve 2019/104 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5481/2019-104, (E.T. 10.10.2023).

[105] Bu ilke; kişisel verilerin, işleme faaliyetleri esnasında etkili bir şekilde korunabilmeleri için, işleme sistemi ve süreçleri henüz hayata geçirilmemişken yani tasarlanırken, veri işleme faaliyetleri esnasında ortaya çıkabileceği öngörülebilen risklere karşı, veri mahremiyetini güçlendirici nitelikte uygun ve yeterli teknik ve organizasyonel önlemlerin alınması anlamına gelmektedir. (İpek Çimen Bulut, "Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları", **Anadolu Üniversitesi Sosyal Bilimler Dergisi**, Cilt: 20, Sayı: 2, 2020, s. 132).

[106] Bu ilke de, veri sorumlusunun, işleme faaliyetine başlamadan önce belirleyerek ilgili kişiye bilgisini verdiği amaçla sınırlı olarak yapılmasını sağlayacak mahiyetteki önlemlerin alınması anlamına gelmektedir. (Bulut, s. 132).

[107] GDPR Gerekçe 78, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-78/, **(**E.T. 29.06.2023).

farkındalığı artırır. Yine bilgi, demokratik katılımın temelini oluşturur; bireylerin hükümet faaliyetlerini denetlemesine ve bilinçli kararlar almasına yardımcı olur. Ayrıca yeniliklerin ve rekabetin itici gücüdür, iş dünyasını dönüştürür ve ekonomik büyümeyi destekler. Amerikalı yazar Alvin Toffler, 1980 yılında yayımlanan "Üçüncü Dalga" adlı kitabında, bilgi ve iletişim teknolojilerinin hızla geliştiği ve bilgiye dayalı ekonomik, toplumsal ve kültürel değişimlerin öne çıktığı bu çağı "bilgi çağı" olarak tanımlamıştır[108]. Gerçekten de günümüzde bilgi, gelişim ve karar alma süreçlerinin temelini oluşturur. Bilgiye ulaşmak için ise bilginin hammaddesi olan verilerin ve özellikle de kişisel verilerin toplanıp işlenmesinin ve anlamlandırılmasının önemi yadsınamaz.

Kişisel veriler kullanılarak bireylere özelleştirilmiş ürün ve hizmetler sunulup daha iyi deneyimler yaşamaları sağlanabilir. Yahut sağlık verileri, hastalıkların teşhis ve tedavisinde kullanılabilir. Kişisel veriler ayrıca, yeni ürünlerin ve hizmetlerin geliştirilmesi için değerli bir kaynaktır. Araştırmacılar, toplumsal yarar amacıyla bu verileri analiz ederek yeni eğilimleri ve ihtiyaçları belirleyebilir. Kişisel veriler, kameralar, sensörler ve diğer teknolojiler aracılığıyla suçun önlemesi ve güvenlik amaçları için de kullanılabilir. Bu örnekleri çoğaltmak mümkündür. Ancak kişisel verilerin, her zaman yararlı şekilde kullanıldığına rastlamayız. Zira her durumda olduğu gibi, kişisel ve zararlı amaçlar için kullanıldığı da olmaktadır. 2016 yılında tüm dünyanın gündemine oturan Facebook ve Cambridge Analytica skandalı akla ilk olarak gelen örneklerden biridir. Hatırlanacağı üzere, siyasi kampanyalar için veri analizi yapan ve danışmanlık sağlayan bir şirket olan Cambridge Analytica, Facebook kullanıcılarının kişisel verilerini toplamak ve analiz etmek amacıyla bir uygulama geliştirmiş ve kişileri profillemiştir[109]. Elde edilen bu bilgiler, kişiselleştirilmiş reklamlar ve içeriklerin üretilmesinde kullanılarak Amerika Birleşik Devletleri'nin

---

[108] Jennifer Sharkey ve D. Scott Brandt, "Integrating Technology Literacy and Information Literacy", **Technology Literacy Applications in Learning Environments**, (Ed. David D. Carbonara), 2005, s. 65.

[109] "Profilleme, özellikle bir bireyle ilgili kararlar alınması ya da mevzubahis bireyin kişisel tercihlerini, davranışlarını ve tutumlarını analiz veya tahmin etmek amacıyla bir "profil"in bir bireye uygulanmasını içeren otomatik veri işleme tekniğidir." (Avrupa Konseyi Bakanlar Komitesi, "Profilleme Uygulamaları Kapsamında Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Üye Devletlere Yönelik Bakanlar Komitesi CM/Rec(2010)13 sayılı Tavsiye Kararı", **Avrupa Konseyi Web Sitesi**, https://rm.coe.int/profilleme-uygulamalar-kapsam-nda-kisisel-verilerin-otomatik-isleme/1680a4396d, (E.T. 30.09.2023).

2016 yılında yapılan başkanlık seçimlerinde ve İngiltere'nin Brexit referandumunda, seçmenlerin karar alma mekanizmalarının etkilenmesinde ve sonuçların manipüle edilmesinde kullanılmıştır. Yine e-posta hizmeti veren Yahoo'nun 2013 ve 2014 yıllarında gerçekleşen iki büyük veri sızıntısı sonucu toplamda üç milyardan fazla kullanıcısının, e-posta adresleri, şifreleri ve güvenlik sorularına verdikleri cevaplar dahil olmak üzere hesap bilgileri çalınmış ve kimlik hırsızlığı riski yaşanmıştır[110]. Benzer şekilde 2017 yılında yapılan siber saldırı sonucunda, kredi raporu şirketi Equifax'in müşterilerinin adlarını, sosyal güvenlik numaralarını, kredi kartı bilgilerini, doğum tarihlerini ve adreslerini içeren veri tabanına erişilmiş ve aynı risk doğmuştur[111].

Kişisel verilerin kötüye kullanıldığına dair bunlar gibi birçok örnek verilebilir. Kişisel verilerin korunmasına ilişkin hak, bireylerin haklarıyla gizliliklerini korumayı amaçlayan bir gerekliliktir. Bu hak, kişinin maddi ve manevi varlığını korunmasına ve geliştirilmesine yönelik hakkı, insan onuru, özel hayatın gizliliği, din ve vicdan özgürlüğü, düşünce ve kanaat özgürlüğü, düşünceyi açıklama ve yayma özgürlüğü, bilgi edinme hakkı gibi birçok hakla yakından ilgilidir[112]. Dikkat edilmelidir ki esasen korunan verinin kendisi değil, bireyin kendisidir[113]. Bu nedenle bireylerin mahremiyetini ve kişisel verilerini korumaya yönelik önlemler alma konusunda, devletlere ve veri işleyenlere büyük görev düşmektedir. Öncelikle devletlerin, kişisel verilerin korunması için veri işleme süreçlerini düzenleyen, veri işleyenlerin sorumluluklarını belirleyen ve bireylerin haklarını güvence altına alan etkili ve kapsamlı hukuki düzenlemeler oluşturması gerekmektedir. Böylece kişilerin kendilerine ait veriler üzerinde kontrol sahibi olması sağlanmalıdır. Veri işleyenlerse, bu hukuk kurallarına uygun hareket etmeli, gerekli veri güvenliği önlemlerini almalı ve veri ihlali risklerini en aza indirgemek için çaba göstermelidir. Ayrıca devletler ve sivil toplum kuruluşları, bireyleri veri koruma konusunda bilgilendirmeli ve eğitimler düzenlemelidir. Bireylerin bu konuda bilinçli olmaları, kuralların etkinliğini ve

[110] BPB Online, "Yahoo Data Breach: What Actually Happened?", **BPB Online Web Sitesi**, 23.11.2020, https://bpbonline.medium.com/yahoo-data-breach-what-actually-happened-54cf8f3f7c93, (E.T. 30.09.2023).

[111] Wikipedia, "2017 Equifax data breach", **Wikipedia Web Sitesi**, https://en.wikipedia.org/wiki/2017_Equifax_data_breach, (E.T. 30.09.2023).

[112] Şimşek, s. 111.

[113] Şimşek, s. 4.

denetimini artıracaktır. Son olarak devletler, veri koruma otoriteleri aracılığıyla veri işleyenleri denetlemeli ve gerektiğinde cezai yaptırımlar uygulamalıdır.

3. Kişisel Verilerin Korunmasına İlişkin Temel Düzenlemeler

a. Uluslararası Hukuktaki Düzenlemeler

(1) OECD Rehber İlkeleri

Kuruluş amaçlarından biri, üye ülkelerde insan hakları ve hürriyetlerinin korunup geliştirilerek demokratik sistemlerin sağlıklı bir şekilde sürdürülmesini desteklemek olan Ekonomik Kalkınma ve İşbirliği Teşkilatı (OECD), aynı zamanda kişisel verilerin korunmasını sağlamak için uluslararası arenada ilk düzenlemeyi yapan örgüttür[114]. Türkiye'nin de kurucu üyelerinden olan olduğu bu kuruluşun, 1980 senesinde "Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler"i belirleyerek kişisel veri koruma hukukuna yeni bir soluk gelmiştir. Bu ilkeler esasen üye ülkelerin iç hukuklarında yapacağı yasal düzenlemelerin yeknesaklığına yönelik tavsiyeler niteliğinde olup veri korumaya ilişkin temel kuralları içerse de, zaman içerisinde amacına ulaşmış ve hem ulusal hem de uluslararası çapta birçok düzenlemenin öncüsü olmuştur. Rehberde kişisel verilerin hukuka aykırı şekilde ele geçirilmesi, yanlış depolanması, yetkili olmayanlar tarafından kötü amaçlarla kullanılması gibi risklerin ortadan kaldırılması amaçlanmış ve kişisel verilerin akışının nasıl olması gerektiğine yönelik ilkelere yer verilmiştir[115]. OECD Rehber İlkeleri sekiz tane ilkeden oluşmaktadır. Metnin 7-14. maddeleri arasında yer alan bu ilkeler sırasıyla şunlardır: Kişisel veri toplanmasının sınırlılığı, veri kalitesi, veri toplamada amacın belirliliği, kişisel veri kullanımının sınırlı olması, veri güvenliği, açıklık, kişisel verilerin korunmasına bireysel katılım ve hesap verilebilirlik[116]. Burada dikkat edileceği üzere, kişinin kendisine ilişkin tutulan verilere

[114] Bilal Toprak, **KVKK ve GVKT Açısından İşçinin Kişisel Verilerinin Korunması**, Yetkin Yayınları, Ankara, 2021, s. 47.
[115] Dülger, s. 87.
[116] Şimşek, ss. 15, 16.

erişim hakkının sağlanması temel amaçtır[117]. Metin 2013 yılında revize edilerek ilgili kişilerin haklarını koruma hususunda temel bir ölçüt olarak kalmaya devam etmiştir.

(2) Birleşmiş Milletler Teşkilatı Düzenlemeleri

(i) İnsan Hakları Evrensel Bildirgesi

İkinci Dünya Savaşı'nın ardından kurulan ve Türkiye'nin de kurucu üyelerinden biri olduğu Birleşmiş Milletler Teşkilatı, 1948 senesinde İnsan Hakları Evrensel Bildirgesi'ni kabul etmiştir. Bildirge m. 12'de "Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır." denilerek özel hayatın gizliliği korunmuş olup dolayısıyla kişisel verilerin korunması da bu kapsamda koruma altında bulunmaktadır.

(ii) Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme

1976 senesinde yürürlüğe giren Birleşmiş Milletler Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme m. 17'de de benzer biçimde "Hiç kimsenin özel hayatına, ailesine, evine ya da haberleşmesine keyfi ya da yasa dışı olarak müdahale edilemez; hiç kimsenin şeref ve itibarına yasal olmayan tecavüzlerde bırakılamaz. Herkesin, bu gibi müdahalelere ve tecavüzlere karşı yasalarca korunma hakkı vardır." hükmü suretiyle kişinin özel hayatı ve dolayısıyla da kişisel verileri koruma altına alınmıştır.

Birleşmiş Milletler İnsan Hakları Komitesi, söz konusu düzenlemeye ilişkin olarak bazı yorumlarda bulunmuştur[118]. Buna göre;

> *Kamu otoritelerinin, özel kişi veya kurumların bilgisayarlarda, veri bankalarında veya benzeri cihazlarda kişisel bilgileri toplaması veya saklaması hukuki düzenlemeye tabi olması gerekmektedir. Devletlerin, bir kimsenin özel hayatına dair bilgilerin hukuken bu bilgilere sahip olma ve kullanma yetkisine sahip olmayanların eline geçmesini ve bu bilgilerin Sözleşme'nin amaçlarına*

[117] Aksoy, s.99; Toprak, s. 48.

[118] UN Human Rights Committee (HRC), "CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation", **United Nations High Commissioner for Refugees Web Sitesi**, 08.04.1988, https://www.refworld.org/docid/453883f922.html, (E.T. 10.08.2022).

aykırılık teşkil edecek şekilde kullanılmasını engellemek için etkili tedbirler alması lazımdır. Her birey kişisel dosyalarda veya veri tabanlarında kendisiyle ilgili bilgiler saklanmışsa bu bilgilerin ne tür bilgiler olduğunu, ne amaçla saklandığını ve bunlara kimlerin erişebileceğini öğrenme hakkına sahiptir. Söz konusu dosyaların, yanlış kişisel bilgilere yer vermesi halinde veya bu bilgilerin hukuka aykırı şekilde toplanması veya kullanılması halinde her birey düzeltme veya bilgilerin ortadan kaldırılmasını talep etme hakkına sahiptir[119].

Görüleceği üzere tüm bu tespitler, Birleşmiş Milletler Teşkilatı'nın kişisel verilerin korunmasına ilişkin hakkı, özel hayatı ve mahremiyeti korumaya alan 17. madde kapsamında takdir ettiğini göstermektedir.

(iii) Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler

Birleşmiş Milletler Teşkilatı'nın 1990 yılında yapmış olduğu bu düzenleme, direkt olarak kişisel verilerin korunmasına ilişkin olup artık bu koruma sadece özel yaşamın gizliliğinin geniş yorumlanmasıyla ulaşılabilecek bir sonuç olmaktan çıkmıştır. Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler de tıpkı OECD Rehber İlkeleri gibi tavsiye niteliğinde olup üye ülkeler açısından bağlayıcı değildir. Yayınlanma amacı üye devletlerin ulusal düzeyde yapacağı yasal düzenlemeler için asgari standartlar belirlemektir[120]. Belirlenen ilkeler özetle şunlardır: Yasal ve dürüst yollarla toplanması ve işlenmesi, verilerin doğruluğu, amacın belirliliği, ilgili kişinin erişimi ilkesi, ayrımcılık yasağı, veri güvenliği, denetim ve yaptırıma tabi olunması, verilerin sınır ötesine akışı. OECD Rehber İlkeleri'nden en önemli farkı ve genel anlamda en büyük önemi, kişisel verilerin korunması gayesiyle yetkilendirilmiş otonom bir otoritenin oluşturulmasını gerekli kılan ilk belge olmasıdır[121]. Ancak etkisi, OECD Rehber İlkeleri kadar geniş olmamıştır. Her iki metnin de tavsiye niteliğinde olduğu düşünüldüğünde, OECD Rehber İlkeleri'nin daha fazla yankı yapmasının, bu alanda hazırlanan ilk belge olmasından kaynaklandığı sanılmaktadır[122].

---

[119] Dülger, s. 88; Lema Uyar (Der. ve Çev.), **Birleşmiş Milletler'de İnsan Hakları Yorumları İnsan Hakları Komitesi ve Ekonomik, Sosyal ve Kültürel Haklar Komitesi, 1981-2006**, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2016, s. 35, 36.

[120] Aksoy, s. 6.

[121] Küzeci, s. 124; Toprak, s. 50.

[122] Küzeci, s. 124.

(3) Avrupa Konseyi Düzenlemeleri

(i) Avrupa İnsan Hakları Sözleşmesi

Türkiye tarafından 1950 yılında imzalanmış ve 1953 yılında yürürlüğe girmiş olan Avrupa İnsan Hakları Sözleşmesi, doğrudan kişisel verilerin korunmasına yönelik bir hüküm içermemektedir. Ancak Avrupa İnsan Hakları Mahkemesi, 8. maddede düzenlenmiş olan özel hayatın ve aile hayatının korunmasına ilişkin hükmü dinamik bir şekilde yorumlayarak kişisel verilerin korunmasına yönelik kararlar verebilmektedir. AİHS'in 8. maddesinde yer alan düzenlemeye göre;

> *Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.*

Mahkeme, kişisel verilerin toplanması, işlenmesi ve paylaşılmasının bireylerin özel hayatına ve aile hayatına müdahale anlamına gelebileceğini kabul eder. Madde metninden anlaşılacağı üzere, AİHS'in sağladığı koruma mutlak değildir. Dolayısıyla, bu tür işlemler ancak yasal bir temele dayanıyorsa, meşru bir amaca hizmet ediyorsa ve orantılı bir şekilde gerçekleştiriliyorsa kabul edilebilir. Mahkeme aynı zamanda kararlarında sıklıkla bilgilerin geleceğini belirleme hakkına vurgu yapar[123]. Tezin diğer kısımlarında sıkça AİHM içtihadına yer verildiği ve verileceği için bu kısımda mahkeme kararı örneklerine girilmeyecektir.

(ii) 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ve Modernize Edilen 108 Sayılı Sözleşme

AİHS'te ayrıca bir hak olarak düzenlenmeyen kişisel verilerin korunması hakkına yönelik olarak Avrupa Konseyi tarafından ayrıca bir düzenleme yapma ihtiyacı hasıl olmuştur[124]. Kişilerin verilerinin otomatik işleme tabi tutulmasının insan

[123] Toprak, s. 53.
[124] Şimşek, s. 21.

haklarına saygılı bir şekilde gerçekleştirilmesini sağlamak ve veri koruma standartlarını belirlemek amacıyla hazırlanan ve 1 Ekim 1985 tarihinde yürürlüğe girerek uygulanmaya başlayan 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (kısaca "108 Sayılı Sözleşme"), bu konuda hukuki bağlayıcılığı olan ilk metindir ve bu açıdan kendisinden önceki konuya ilişkin metinlerden bu açıdan ayrılır. Türkiye, 28.01.1981 tarihinde imzaya açılır açılmaz sözleşmeyi imzalamışsa da iç hukukta bağlayıcı olması 17 Mart 2016 tarihli Resmi Gazete'de onaylamasına ilişkin kararının yayınlanmasına kadar gerçekleşmemiştir[125]. Sözleşmenin kapsamı AİHS'in sağladığı koruma alanına göre daha geniştir. Zira AİHS imzacı devletlerin kamu hizmeti sunumunda ve kamusal alanda insan haklarının korunmasını sağlamak amacıyla uygulandığı bir uluslararası hukuk belgesi olduğu için Sözleşme'nin etkisi de nispeten sınırlı kalmaktadır. Fakat 108 Sayılı Sözleşme, kişisel verilerin otomatik olarak işlenmesiyle ilgili olarak sadece kamusal alanda değil, aynı zamanda özel sektörde de bağlayıcı nitelikte kurallar içermektedir. 108 Sayılı Sözleşme, ayrıca üye devletlere sözleşme hükümlerini iç hukuklarına aktarma yükümlülüğü de getirmiş olup bu husus devletlerin kendi kişisel verilerin korunması kanunlarını yapmak veya doğrudan Sözleşme'yi iç hukukun parçası haline getirmekle gerçekleştirilebilecektir[126]. Sözleşme tarafından sağlanan kişisel veri koruması asgari bir düzeydedir, bu nedenle üye devletler bu standardın ötesine geçerek daha kapsamlı ve yüksek düzeyde güvenlik sağlama imkanına sahiptirler[127]. Ancak unutulmamalıdır ki, mevzubahis Sözleşme sadece otomatik işlemeye tabi olan verileri koruma altına almaktadır yani otomatik olmayan yollarla işlenen verileri kapsam altına almadığından etkisi sınırlıdır[128].

108 Sayılı Sözleşme, verilerin niteliğine ilişkin meşru ve kanuni yollardan elde edilme ve işlenme, veri kaydetmenin ve kullanmanın belirli ve meşru amaçlara dayanması, uygun ve elverişli olma, doğru ve icabında güncel olma, belirli ve lazım oldukları süre boyunca muhafaza edilme gibi bazı ilkeler getirmiştir. Ayrıca hassas veri kategorisinden de bahsetmiş olup hangi verilerin bu kapsamda olduğuna dair örnekleyici ve asgari bir sayım yapmıştır. Yine ilgili kişilere otomatik olarak işlenmiş

[125] 17.03.2016 tarihli Resmî Gazete'de yayımlanan 2016/8576 Sayılı Karar, **Resmi Gazete**, https://www.resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf, (E.T. 11.08.2022).
[126] Şimşek, s. 23.
[127] Toprak, s. 55.
[128] Bozkurt, s. 62.

verilerine yönelik bilgi alma, işlemenin hukuka aykırı olması halinde silinmesi, yanlış verilerin düzelttirilmesi ve bu taleplerin karşılanmaması halinde hukuki yollara başvuru hakkı tanınması hususlarında ek güvence getiren haklar tanınmıştır[129].

Avrupa Veri Koruma Tüzüğü'nün (GDPR) kabul edilmesinden kısa bir süre sonra, 108 Sayılı Sözleşme'nin güncellenmesi ihtiyacı hasıl olmuş ve daha yeknesak uygulama sağlanması için GDPR'a paralel revizeler yapılarak "Sözleşme 108+" adıyla yeniden yayınlanmıştır[130]. Türkiye bu sözleşmeyi henüz onaylayarak iç hukukumuza entegre etmemiştir.

(iii) Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol

Bu düzenleme esasen 108 Sayılı Sözleşme'deki eksiklikleri gidermek üzere yapılmıştır. Örneğin, işlenen verileri denetleyecek yargı denetimine tabi bağımsız bir organın öngörülmemesi ve sınır aşan veri trafiğine ilişkin düzenlemelerin yokluğu problemleri böylece çözüme kavuşturulmuştur[131].

(4) Avrupa Birliği Düzenlemeleri

(i) 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi

108 Sayılı Sözleşme'nin kabulünden sonra, bilişim alanında yaşanan gelişmeler ve iç hukuklarındaki yasama süreçleri nedeniyle, Avrupa Birliği'ne üye devletlerin veri koruma kuralları arasında birlik sağlanamamıştı. AB sınırları içerisinde malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımı ilke olarak kabul edildiği için bu durum problem haline gelmişti. Şöyle ki, daha yüksek koruma

[129] Bozkurt, s. 63.
[130] Dülger, s. 92; Hande Seven, **Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (TCK M.136)**, Yetkin Yayınları, Ankara, 2021, s. 57.
[131] Dülger, s. 93; Şimşek s. 28.

sağlayan ülke, daha düşük koruma sağlayana veri transferi gerçekleştirmeyi reddedebilmekte yahut aynı seviyede asgari koruma sağlanana kadar geciktirebilmekteydi[132]. Bu da işlerin aksamasına ve ekonomik hayatın kan kaybetmesine neden olmaktaydı. İşte hem yeknesaklığın hem de ilgili kişilere yüksek korumanın sağlanması adına[133], 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi (kısaca "95/46/EC Sayılı Direktif") kabul edilmiş ve 24 Ekim 1995'te yürürlüğe girmişti[134]. Üye devletlere, 95/46/EC Sayılı Direktif hükümlerinin kabul edilmesinden itibaren üç sene içerisinde iç hukuklarına aktarmaları ödevi yüklenmişti. Ancak etkisi sadece Avrupa Birliği üyeleri ile sınırlı kalmamış, Birlik dışında yer alsa da Avrupa Ekonomik Alanı'nda bulunan diğer ülkelere de sıçramıştı[135].

Bu düzenlemenin amacı, günümüzde mülga olan 95/46/EC Sayılı Direktif m.1'de, "kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini korumak" olarak belirtilmiştir. Direktif bireylere kapsamlı bir koruma sağladığı için, ekonomik faaliyetlerin sorunsuz şekilde devam edebilmesi adına, üye devletler arasında kişisel veri akışının yasaklanması ya da engellemesi hususu yasaklanmıştır. Gerçekten de 95/46/EC Sayılı Direktif'in içeriği incelendiğinde, kendisinden önce yayınlanan kişisel verilerin korunması belgelerini kendine örnek aldığı ve hatta daha kapsamlı olduğu görülmektedir. Metinde, kişisel verilerin korunmasının sıklıkla diğer insan haklarıyla olan bağından ve bu hakların korunmasının öneminden bahsedilerek AİHS'e atıf yapılmaktadır. Yine kişisel verilerin meşru şekilde işlenebilmesi, belirli ve sınırlı amaçlarla toplanıp bu amaçlara aykırı kullanılamaması, ilgili kişilere karşı şeffaf davranılması, veri toplama ve işlemede amaçsal orantılılık, işleme faaliyetleri esnasında veri güvenliğinin sağlanması ve ulusal veri koruma otoriteleri tarafından

---

[132] Gürsel, s. 97.

[133] Yves Poullet, "EU data protection policy. The Directive 95/46/EC: Ten years after", **Computer Law & Security Review**, Cilt: 22, Sayı: 3, 2006, s. 206.

[134] 24.10.1995 tarihli Avrupa Birliği Resmî Gazetesi'nde yayınlanan 95/46/EC Sayılı Direktif, **Avrupa Birliği Resmî Gazetesi**, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:1995:281:TOC, (E.T. 12.08.2022).

[135] Avrupa Birliği üye ülkeleri ile birlikte İzlanda, Norveç ve Lihtenştayn; Avrupa Ekonomik Alanı ülkelerini oluşturmaktadır. Yani bu üç ülke, Avrupa Birliği'ne dahil olmadıkları halde, aynı ortak pazar kapsamında serbest ticaret ve ekonomik iş birliği yapabilmektedir.

denetim yapılması ilkeleri kendine yer bulmuştur. Veri sorumlusunun yükümlülükleri ve ilgili kişilerin hakları, sınır ötesi veri akışı, veri koruma ihlallerine karşı başvurulabilecek yasal yollar hüküm altına alınmıştır. Sağlık, cinsel yaşam, sendika üyeliği, dini ve felsefi inanç, siyasi görüş, ırk ve etnik köken gibi hususlara ilişkin verilerin özel mahiyetteki kişisel veriler olduğu belirtilerek, bunlar için ayrıca düzenleme yapılmıştır. Sadece otomatik araçlarla işlenen verileri koruma altına alan 108 Sayılı Sözleşme'den farklı olarak, otomatik araçlarla işlenmeyen verileri de korumaya dahil edilmiştir[136]. Direktif'in kabul edildiği ülkeler dışında üçüncü bir devlete veri aktarılacaksa ve o devlette verilerin korunmasına ilişkin yeterli garantiler öngörülmemişse, veri aktarımını yasaklamıştır[137].

ABAD tarafından görülen Rechnungshof v Österreichischer Rundfunk davasında, ulusal mevzuatların 95/46/EC Sayılı Direktif hükümlerine hem uygun olması hem de çelişecek şekilde uygulanmaması gerektiği vurgulanmıştır[138]. Benzer şekilde, Anayasa Mahkemesi de KVKK'nin bazı maddelerinin iptali istemiyle açılan davada[139], anayasaya aykırılık incelemesi yaparken Direktif hükümlerini dikkate almıştır. İptali istenen maddeler Direktif ile uyumluysa, iptal istemi bu gerekçeyle reddedilmiştir[140]. Gerçekten de KVKK hazırlanırken büyük ölçüde 95/46/EC Sayılı Direktif model alınmıştır. Böylece Avrupa düzenlemeleriyle uyum yakalanmaya çalışılmıştır.

---

[136] Seven, s. 66.

[137] Gürsel, s. 104.

[138] ABAD, 20.05.2003 tarih ve C-465/00 numaralı Rechnungshof v Österreichischer Rundfunk kararı, https://curia.europa.eu/juris/liste.jsf?num=C-465/00&language=en, (E.T. 12.08.2022). Avusturya yasalarına göre; denetime tabi kuruluşlar, aldıkları yıllık ücret belli bir meblağı aşan işçilerinin bilgilerini Sayıştay'a vermeye zorunludur. Sayıştay da yaptığı incelemeler sonucunda hazırladığı raporu, halka açık bir şekilde paylaşmaktadır. Bu uygulamanın 95/46/EC Sayılı Direktif hükümlerine aykırılık teşkil ettiği ileri sürülmüştür. ABAD önüne gelen bu uyuşmazlıkta, kişisel verilerin işlenmesinin söz konusu olduğu her türlü faaliyetin Direktif kapsamında olduğunu söylemiştir. İşçilerin ad-soyad ve maaş verilerinin kayıt altına alınmasında bir sakınca olmadığını belirtmekle, üçüncü kişilerle paylaşılmasını Direktif'e aykırı bulmuştur.

[139] Anayasa Mahkemesi, 28.09.2017 tarih ve E. 2016/125, K. 2017/143 kararı, https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/, (E.T. 12.08.2022).

[140] Dülger, s. 97; Murat Volkan Dülger, "Anayasa Mahkemesi'nin Kişisel Verilerin Korunması Kanunu'nun Konu Edildiği İptal Davası Kararına İlişkin Bir Değerlendirme", **SSRN Papers Web Sitesi**, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792249, (E.T. 12.08.2022), (KVKK İptal Davası).

(ii) Avrupa Birliği Temel Haklar Şartı

1 Aralık 2009'da bağlayıcılık kazanarak uygulanmaya başlayan Avrupa Birliği'nin temel hak düzenlemesi olan Temel Haklar Şartı'nın 8. Maddesinde şu şekilde bir düzenleme bulunmaktadır:

> *Herkes, kendisine ilişkin kişisel bilgilerin korunmasını isteme hakkına sahiptir. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir*

Her ne kadar Şart m. 7'de, özel ve aile yaşamına saygı hakkı düzenlenmişse de bu konuya ayrıca yer verilmesi, kişisel verilerin korunmasına bir temel hak olarak verilen önemi gözler önüne sermektedir. Zira kişisel verilerin korunmasına yönelik hak, özel yaşamın gizliliği çerçevesinde değerlendirilemeyecek bazı konuları da içermektedir[141]. Veri işlemeyi meşru kılacak koşullar, ilgili kişinin rızası gibi durumlar buna örnektir.

(iii) Avrupa Birliğinin İşleyişi Hakkında Andlaşma

Avrupa Birliği'nin İşleyişi Hakkında Andlaşma (ABİHA) ya da daha bilinen adıyla Lizbon Andlaşması, 2009 yılında yürürlüğe giren bir AB temel anlaşmasıdır. Avrupa Birliği'nin kurumsal yapısını, işleyişini ve temel değerlerini düzenleyen bu andlaşma, elbette kişisel verilerin korunmasına yönelik hükümler de içermektedir. ABİHA m. 16'ya göre; "herkes, kendisiyle ilgili kişisel verilerin korunması hakkına sahiptir. AB kurumları ve organları ile üye devletler tarafından kişisel verilerin işlenmesi sırasında bireylerin korunmasına ve bu bilgilerin serbest dolaşımına ilişkin kuralları olağan yasama usulü uyarınca belirlenir. Bu kurallara uyulması, bağımsız otoritelerin denetimine tabidir"[142]. Söz konusu düzenleme, AB'nin kişisel verilerin korunmasına, bağımsız bir temel hak olarak verdiği önemi göstermektedir.

---

[141] Küzeci, s. 162.

[142] Dışişleri Bakanlığı, "Avrupa Birliğinin İşleyişi Hakkında Andlaşma'nın Türkçe Çevirisi, **Dışişleri Bakanlığı Resmi Web Sitesi**, https://www.ab.gov.tr/files/pub/antlasmalar.pdf, (E.T. 10.10.2023).

(iv) 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

95/46/EC Sayılı Direktif'in amacı; ilgili kişilere yüksek düzeyde koruma sağlayan, kişisel verilerin serbest dolaşımına bir mani çıkmasını, dolayısıyla da ekonomik statükonun zarar görmesini engelleyen, Avrupa Birliği çapında yeknesak bir kurallar bütünü oluşturmaktı[143]. Ancak geçen zaman içerisinde, her ne kadar Direktif'in amacı ve ortaya koyduğu prensipler baki kalsa da, üye devletler arasında direktifi iç hukuklarına adapte edip uygulama biçiminde farklılıklar ve tutarsızlıklar yaşandığı tespit edilmiştir. Bu da AB genelinde veri koruma uygulanmasında parçalanmayı, yasal belirsizlikleri ve gerçek kişilerin korunmasına yönelik önemli riskler bulunduğuna dair yaygın bir kamuoyu algısını beraberinde getirmiştir[144]. Gerçekten de AB bünyesinde ikincil hukuk kurallarından olan direktifler, üye devletlere ulaşılması gereken amaca ilişkin uyulacak kuralları sunup, bu kuralları uygulamaları için kendi ulusal yasalarına aktarmalarını zorunlu tutar; ancak bunu nasıl yapacakları konusunda esneklik sağlar. Yani üye devletlere, iç hukuka aktarım sırasında, şekil ve yöntem açısından bir takdir yetkisi bırakılmaktadır[145]. Bu nedenle; üye devletlerde kişisel veriler, veri sorumlusu, rıza, hassas veriler gibi temel kavramları farklı yorumlanması, veri koruma kuralları ile üye ülkelerin yürürlükteki hukukları arasındaki uyumun sağlanmasında görüş ayrılıkları yaşanması, veri işlemeyi meşrulaştırma kriterleri ve ilgili kişinin erişim hakkına ilişkin sınırlamalarda farklılıklar gibi sıkıntılar ortaya çıkmıştır[146]. Dolayısıyla yeknesaklığın ancak bağlayıcı tek bir metinle sağlanabileceği anlaşılmış olup 95/46/EC Sayılı Direktif yürürlükten kaldırılıp 25 Mayıs 2018'de yürürlüğe girmek üzere GDPR kabul edilmiştir. Direktiflerden farklı olarak tüzükler, bütünüyle bağlayıcı olup tüm üye devletlere eş zamanlı ve doğrudan uygulanabilir nitelik taşırlar[147]. Yani tüzüklerin uygulanmasında üye devletlere takdir yetkisi verilmediği gibi iç hukuka aktarılmaları da gerekmez. Bu nedenle hem amaçlanan yeknesak uygulama sağlanmış olup hem de zamanın şartlarına daha uygun düşen bir modern kurallar bütünü kabul edilmiştir.

---

[143] Poullet, s. 207.
[144] GDPR 9 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-9/, (E.T. 15.08.2022).
[145] Mustafa T. Karayiğit, **Avrupa Birliği Anayasa Hukuku**, Seçkin Yayıncılık, Ankara, 2018, s. 70.
[146] Poullet, s. 207.
[147] Karayiğit, s. 69.

GDPR her ne kadar Avrupa Parlamentosu tarafından kabul edilse de sadece AB üyelerine özgü değildir. Yani AB sınırları içerisinde ikamet edip de AB vatandaşı olmayanların ve AB dışında yaşayıp da verileri herhangi bir sebeple AB'ye ulaşan kişisel verileri de bu korumadan yararlanır (m. 3). Ayrıca AB dışındaki üyeler de AB'de yaşayan kişilerin verilerini işlerken GDPR kurallarına uymak zorundadır. Böylece AB ile ilişkili verileri, kişisel verileri koruma hakkının düzenlenmediği veya GDPR'ye göre daha az korumanın sağlandığı ülkeler açısından da güvence altına alınmıştır[148].

GDPR'nin koruma alanı dışında getirdiği başka yenilikler de mevcuttur. Bu yeni metinle, kişisel verilerin işlenmesi için açık ve bilgilendirilmiş rızanın alınması gerekliliği vurgulanarak rıza koşulu güçlendirilmiştir (m. 7). Veri ihlalinin veya riskinin yaşanması halinde, yetkili makamlara ve ilgili kişilere 72 saat içerisinde bildirim yapılması zorunluluğu getirilmiştir (m. 33). Kişisel verilere erişim, düzeltme, silme, taşıma gibi haklar kuvvetlendirilmiştir (m. 15 vd.). Verilerin hukuka uygun, adil ve belirli amaç sınırlamalarına uygun bir şekilde işlenmesi gerekliliği vurgulanmıştır (m. 5). Hassas verilerin daha kapsamlı bir şekilde tanımlamış ve işlenmeleri için daha sıkı koşullar getirilmiştir (m. 9). Yine, hassas verilerin işlenmesi söz konusuysa buna ilişkin bir veri koruma görevlisi görevlendirme zorunluluğu getirilmiştir. Veri ihlallerine yönelik daha caydırıcı ve yüksek meblağda para cezaları öngörülmüştür. Riskli veri işleme faaliyetlerinde etki değerlendirmesi yapılmasının gerekliliği ifade edilmiştir (m. 35). Veri işleyenlerin tamamı işleme faaliyetini hukuka uygunluğundan sorumlu tutulmuştur. İşleme sürecinde zarara görenlere, toplu tazminat da dâhil olmak üzere ilk defa açıkça tazminat hakkı verilmiştir (m. 82). Benzer şekilde, ilk defa açıkça unutulma hakkı düzenlenmiştir (m. 17)[149]. İlgili kişiye, veri taşınabilirliği hakkı verilmiştir (m. 20). Veri sorumlusuna iç işleyiş ile alakalı politikalarını belirleyerek başlangıçtan itibaren veri koruması ve tasarımdan itibaren veri koruması prensiplerini karşılamaya yönelik tedbirleri alması yönünde bir sorumluluk yüklenmiştir (m. 24). İlgili kişi, paylaşılmasına rızası olsa dahi, verilerinin transfer edildiği devlette yeterli garanti sağlandığına ilişkin güvence verilmediği sürece verinin AB dışına

[148] Dülger, s. 105.
[149] Seven, s. 69.

aktarılmasını yasaklanmıştır (m. 46)[150]. Böylece kişisel verilerin sürekli dolaşımda olduğu günümüz dünyasında, kişilere veri güvenliği açısından insan hakları standartlarına uygun bir şekilde ileri koruma sağlanmaya çalışılmıştır.

(v) Diğer Bazı Düzenlemeler

Avrupa Birliği bünyesinde kişisel verilerin korunmasına yönelik ihdas edilen diğer düzenlemelerin başında Avrupa Parlamentosu ve Avrupa Konseyi'nin 2002/58/EC Sayılı Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Direktifi gelmektedir. Bu Direktif, Avrupa Parlamentosu ve Avrupa Konseyi'nin 2002/58/AT Sayılı Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Yönergesi, 95/46/EC Sayılı Direktif'i tamamlamak üzere 12.07.2002'de kabul edilmiş ve kişisel verilerin telekomünikasyon ve iletişim hizmetleri alanında korunmasını amaçlamıştır. 2002/58/AT Sayılı Direktif hükmüne göre, üye devletler için bağlayıcı olup iç hukuka aktarılması gerekmektedir[151]. Ayrıca 2002/58/AT Sayılı Direktif'te herhangi bir konuda hüküm bulunmaması halinde 95/46/EC Sayılı Direktif uygulanır. 2002/58/AT Sayılı Direktif'ten farklı olarak tüzel kişilerin meşru menfaatlerini de korur[152].

Avrupa Birliği bünyesinde başka bir düzenleme olarak ise Kolluk Teşkilatında ve Ceza Yargılamalarında Kişisel Verilerin Korunmasına İlişkin 2016/680 Sayılı Direktif'ten bahsedilebilir. 2016/680 sayılı Direktif; kolluk teşkilatlarının suçu önleme, tespit etme, soruşturma faaliyetleri, ceza yargılamaları ve bu cezaların infazı esnasında yetkili mercilerin, kişisel verilerin korunması amacıyla uyması gereken prensipleri düzenler[153]. Aynı zamanda kişisel verilerin işlenmesindeki amaçlar, hukuki dayanaklar, veri konularının hakları ve veri güvenliği gibi konuları da kapsar. Bu sayede, adli ve cezai işlemlerde veri korumasının sağlanması ve bireylerin temel haklarına saygı gösterilmesi amaçlanmaktadır.

---

[150] Bozkurt, ss. 69-71; Dülger, ss. 106-109; Ayşe Nur Akıncı, **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, T.C. Kalkınma Bakanlığı Yayınları, Ankara, 2017, ss. 14-19.

[151] Dülger, s. 100.

[152] Gürsel, s. 153, 154.

[153] Juraj Sajfert ve Teresa Quintel, "Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities", **SSRN Papers Web Sitesi**, 2017, https://ssrn.com/abstract=3285873, (E.T. 12.08.2022), s. 3.

2006/24/EC Sayılı İletişim Trafik Verilerinin Saklanması Direktifi ise kamu güvenliği ve ulusal savunma amaçlarıyla, Avrupa Birliği üyesi ülkelerdeki iletişim hizmeti sağlayıcılarına, iletişim trafiği verilerini, belirli bir süre boyunca saklama yetkisi veren ve bu verilere yetkili makamlar tarafından erişme yetkisi sağlayan bir düzenlemeyi içermektedir. Bu veriler, yetkili makamların suç soruşturmalarını yürütmek ve kamu güvenliğini sağlamak amacıyla kullanılacaktır. Fakat ciddi suç kavramının yasal sınırlarını çizmemesi, veri saklama sürelerinin uzunluğu ve veri güvenliğinin eksikliği gibi hususlarda çok fazla tartışmaya yol açmıştır[154]. Nihayetinde ABAD'ın önüne gelen olayda, Digital Rights Ireland kararıyla, 2006/24/EC Sayılı Direktif'i geçersiz kılan bir karar verilmiş ve veri saklama sürelerinin ve kullanım amacının ölçülülük kıstasına uygun olması gerektiği vurgulanmıştır[155].

Avrupa Birliği bünyesinde bahsedilmesi gereken düzenlemelerden son ikisi de 45/2001 Sayılı ve 2018/1725 Sayılı Avrupa Birliği Kurumları Veri Koruma Tüzükleridir. 2001/45/EC Sayılı Avrupa Birliği Kurumları Veri Koruma Tüzüğü, adından da anlaşılacağı üzere, Avrupa Birliği kurumları ve organlarının kişisel verileri nasıl işleyeceğini düzenlemek amacıyla kabul edilmiştir. Ayrıca bu belgeyle, söz konusu faaliyetleri denetlemek ve gerektiğinde danışmanlık vermek için bağımsız bir kurum olan Avrupa Veri Koruma Denetçiliği kurulmuştur. Fakat 2018 yılında GDPR'ın yürürlüğe girmesinin ardından, GDPR ile olan yeknesaklığın sağlanması amacıyla 45/2001 Sayılı Tüzük kaldırılarak, yerine yine aynı ihtiyacı karşılamak üzere, 2018/1725 Sayılı Avrupa Birliği Kurumları Veri Koruma Tüzüğü kabul edilmiştir[156]. GDPR ile hükümleri büyük ölçüde benzese de birtakım farklılıklar içermektedir. Örneğin, GDPR AB üyesi devletlerce uygulanırken, 2018/1725 Sayılı Tüzük Avrupa Birliği kurumları ve organlarınca uygulanmaktadır. GDPR, kişisel verilerin işlenebilmesi için genelde açık ve özgür iradeye dayalı rıza alınmasını gerektirirken; 2018/1725 Sayılı Tüzük, AB kurumlarının işlemesi gereken verilerin özel ve hukuki amaçlarını belirlemiştir. Yine, GDPR, veri işleme amaçlarını genel ve geniş bir şekilde belirlerken; 2018/1725 Sayılı Tüzük, AB kurumlarının faaliyetlerinin özgün ihtiyaçlarına uygun olarak daha spesifik amaçlar öngörmüştür.

[154] Dülger, s. 101, Küzeci, s. 193.
[155] ABAD, 08.04.2014 tarih ve C-293/12 numaralı Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources kararı, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293, (E.T. 12.08.2022).
[156] Dülger, s. 101, 102.

b. Ulusal Hukuktaki Düzenlemeler

(1) Anayasa

Anayasa'nın 20. maddesine, 2010 yılında yapılan anayasa değişikliği referandumu ile;

> *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 ilave edilerek kişisel verilerin korunması hakkı teminata bağlanmıştır. Hükümde sayılan haklar, metnin lafzından da anlaşılacağı üzere, tahdidi nitelikte değildir. Kişiler, ilgili kanun kapsamında kendilerine sunulan diğer imkanlardan da yararlanabilir.

Esasen bu değişiklik yapılmadan önce de bireylerin kişisel verileri herhangi bir anayasal teminattan yoksun değildi. Aksine 2. maddede düzenlenen "hukuk devleti ilkesi", 17. madde kapsamında düzenlenen "bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı", 20. madde kapsamında düzenlenen "özel hayatın gizliliği hakkı", 21. maddedeki "konut dokunulmazlığı", 22. maddedeki "haberleşmenin gizliliği ilkesi", 24. maddede getirilen "dini ve vicdani kanaat hürriyeti", 25. maddede düzenlenen "düşünce ve kanaat hürriyeti" gibi hak ve hürriyetleri düzenleyen hükümler kişisel verilerin korunması hakkının temeli olarak kabul edilebilir[157]. Nitekim Anayasa Mahkemesi de, Anayasa'nın 20. maddesine bu düzenleme eklenmeden önce kişisel verilere ilişkin koruma, bahsedilen hak ve özgürlükler kapsamında yorumlamaktaydı[158]. Yine Anayasa'nın 40. maddesinde kişilere tanınan

[157] Küzeci, ss. 266-272; Şimşek, s. 111.

[158] Anayasa Mahkemesi, 25.06.2008 tarih ve E. 2006/167, K. 2008/86 kararı, https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/, (E.T. 16.08.2022). 5429 Sayılı Kanun m. 8 uyarınca, kişiler Türkiye İstatistik Kurumu'nun istediği verileri paylaşmak zorundaydı ve m. 54/2-b uyarınca bu yükümlülüğe aykırı davrananlara karşı uygulanacak bir para cezası bulunuyordu. Mahkeme, bu düzenlemeler belirsiz olduğundan kişisel veri olarak nitelendirilebilecek verilerin de Kurum tarafından talep edilebileceği, ülkede en güçlü veri tekelinin Kurum'un kendisi olduğu, bu düzenlemelerin bireyleri idare ve diğer kişiler karşısında korumasız bıraktığı, bu haliyle iptali istenen bu hükümlerin Anayasa'nın 20. ve 25. madde hükümlerine aykırı olacağı gerekçesi ile iptal edilmesine karar vermiştir.

temel hak tanınan hak ve özgürlüklere bir müdahale söz konusu olduğunda gecikmeksizin yetkili mercilere müracaat etme imkânının verilmesini talep etme hakkının olduğu ve devletin işlemlerinde kişilerin hangi kanun yollarına ve makamlara başvurabileceğini ve başvuru sürelerini göstermek mecburiyetinde olduğu düzenlenmiştir. Böylece kişisel verilerin korunması hakkı, dolaylı anlamda korunmaktaydı. Ancak Anayasa'nın m. 20/3'e yapılan ekleme ile kişisel verilerin korunması hakkı diğer haklardan bağımsız bir hak statüsüne kavuşarak bu hakkın temel, vazgeçilmez ve devredilemez bir hak olduğu kabul edilmiş ve böylece bu hakka yapılacak müdahalenin sınırları da oldukça daraltılmıştır[159].

Kişisel verilerin korunması hakkına yapılacak müdahale kapsamında, öncelikle Anayasa'nın 13. ve 15. maddeleri bağlamında gösterilen çerçeve dikkate alınmalıdır. Anayasa m. 13'e göre "temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir". Madde hükmünden de anlaşılacağı üzere temel hak ve hürriyetler, ilgili maddelerde hangi sınırlama sebebi öngörülmüş ise, yalnızca o sebeple sınırlandırılabilmektedir[160]. Ayrıca temel hak ve özgürlükler çağdaş demokrasilerde, hakka keyfi gerekçelerle müdahale edilmemesinin sağlanması adına, idari işlemlerle sınırlandırılamaz. Nitekim Anayasa'da kişisel verilerin, kişinin açık rızası ile ya da sadece kanunda öngörülen hallerde işlenebileceği düzenlenmiştir. Bu nedenle, anayasal teminat altına alınmış temel bir hak ve hürriyet olan kişisel verilerin korunması konusunda, idari makamlar tarafından getirilen sınırlamalar hukuka aykırı olacaktır[161].

Kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğine dair düzenlemenin Anayasa m. 13'e aykırılık tekvin ettiği ifade edilmektedir. Açıklandığı üzere, temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak sınırlandırılabilir. Her ne kadar bu sınırlama ancak bir kanunla yapılabilirse de

---

[159] Güray Dağ, **Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması**, (Yayınlanmamış Doktora Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2011, s. 59.

[160] Kemal Gözler, "Anayasa Değişikliğinin Temel Hak ve Hürriyetlerin Sınırlandırılması Bakımından Getirdikleri ve Götürdükleri: Anayasanın 13'üncü Maddesinin Yeni Şekli Hakkında Bir İnceleme", **Ankara Barosu Dergisi**, Sayı: 59 Cilt: 4, Ankara, 2001, (Anayasa M. 13), s. 64.

[161] Erhan Tanju, **AİHM Kararları Işığında İfade ve Basın Özgürlüğü**, Seçkin Yayıncılık, Ankara, 2012, s. 142.

kısıtlama sebeplerinin düzenlenmesi kanuna bırakılamaz. Fakat m. 20/3'teki düzenlemenin sınırlama nedenlerini belirleme yetkisini kanuna verdiği, bu yüzden bu düzenlemenin kişisel verilerin etkin şekilde korunmasına engel olabileceği belirtilmektedir[162].

Belirtildiği üzere, Anayasa'nın 13. maddesi kapsamında belirtilen sınırlamalar, "Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz". Anayasa Mahkemesi, kanunla getirilen sınırlamanın, o hakkın özüne müdahale etmediğinin kabul edilmesi için kullanımını mühim ölçüde zorlaştırıp amacına ulaşmasına engel teşkil edip etmediğini ve etkisini ortadan kaldıran bir nitelik taşıyıp taşımadığını önemsemektedir[163]. Bu husus elbette, temel haklardan biri olan kişisel verilerin korunmasını isteme hakkını ortadan kaldıran ya da kullanılmasını aşırı şekilde zorlaştıran sınırlandırmaların açısından da geçerlidir ve Anayasa Mahkemesi tarafından hakkın özüne dokunan sınırlamalar olarak kabul edilmektedir[164].

Eleştirilen yanları olsa da, Anayasa'ya kişisel verilerin korunması hakkının eklenmesiyle, kişilerin verilerinin geleceğini belirleme ve mahremiyet haklarını doğrudan güvence altına alma, teknolojik gelişmelere ayak uydurma, tarafı olduğumuz

---

[162] Küzeci, s. 266.

[163] Anayasa Mahkemesi, 18.06.2009 tarih ve E. 2006/121, K. 2009/90 kararı, https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/, (E.T. 17.08.2022).

[164] Mahkeme, kişisel verilerin korunmasına dair bazı hükümler içeren ve 703 sayılı KHK ile ilga edilen 5952 sayılı Kamu Düzeni ve Güvenliği Müsteşarlığı Teşkilat Kanununun ilgili maddesinin iptali talebiyle açılan davada, "hakkın özü" kavramı ile ilgili değerlendirme yaparak ilgili yasa hükümleri hakkında karar vermiştir. Gerekçede ise şu ifadeleri kullanmıştır: *Terörle mücadele alanında politikalar geliştirme konusunda yetkili olan Müsteşarlığın görevlerini ifa edebilmesi için bireylerin kişisel verileri de dahil olmak üzere bazı bilgi ve belgelere gereksinim duyması kaçınılmazdır. İptali istenen düzenlemede, veri ve bilgilerin terörle mücadele konusuyla sınırlı olacağı net bir şekilde ifade edilmiştir. Söz konusu düzenleme kişisel verilerin korunması konusunda Anayasa'nın 20. maddesi ile getirilen korumaya aykırı herhangi bir düzenleme de bulunmamaktadır. TCK'nın kişisel verilerin korunması konusunda getirdiği düzenlemelerin, Müsteşarlık personeli bakımından da geçerli olduğu açıktır. Bu yüzden, davaya konu teşkil eden düzenleme ile Kamu Düzeni ve Güvenliği Müsteşarlığına terörle mücadele konusu ile sınırlı olmak kaydıyla sağlanan veri ve bilgi toplama yetkisinin, özel hayatın gizliliği ilkesi kapsamında kişisel verilerin korunması hakkına ölçüsüz bir sınırlama olduğunu söylemek mümkün değildir. Ayrıca, bu kuralın kişisel verilerin korunması hakkını radikal şekilde güçleştiren ya da ortadan kalkmasına neden olan, dolayısıyla hakkın özüne dokunan bir sınırlama olmadığı da nettir.* Burada her ne kadar bir iptal kararı çıkmamışsa da kişisel verilere dair bir sınır çizmeden, kişisel veri toplanmasına dair koşullar belirlenmeden, kapsam tespit edilmeden her türlü kişisel verinin toplanabilmesine imkân verilmesinin, kişisel verilerin korunması hakkının özüne dokunulmasına yol açacağı ileri sürülmüştür. (Anayasa Mahkemesi, 19.01.2012 tarih ve E. 2010/40, K. 2012/8 kararı, https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/, (E.T. 17.08.2022)).

uluslararası belgelerle olan uyumu sağlama ve demokratik değerleri desteklemeye verilen önemi göstermeye verilen önem vurgulanmıştır.

(2) Kişisel Verilerin Korunması Kanunu

Tarafı olduğumuz kişisel verilerin korunmasına dair uluslararası belgelere ve çeşitli kanunlarda yer alan koruma hükümlerine rağmen iç mevzuatımızda ayrı bir kanun yapılması çok uzun zaman almıştır. 07.04.2016 tarihinde KVKK yürürlüğe girmeden önce, iki ayrı tasarı hazırlanmasına rağmen yasama dönemi içerisinde kanunlaştırılmadığı için tasarılar kadük kalmıştır[165]. Kanunun hazırlanmasında çoğunlukla 95/46/EC Sayılı Direktif esas alınmıştır[166]. Ancak kanunun yapılmasında o kadar gecikilmiştir ki, Avrupa Birliği aynı yıl Direktif zamanın ihtiyaçlarına cevap vermediği için daha kapsamlı korumalar ve yenilikler getiren GDPR'yi kabul etmiştir. KVKK'deki eksikliklerin GDPR'de yer alan ilke ve esaslar örnek alınarak mahkeme kararlarıyla veya yapılacak kanun değişiklikleriyle giderilebileceği düşünülmektedir[167].

Kanunun amacı ilk maddede, "kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek" olarak belirtilmiştir. Kanunun kapsamı olarak ise, "kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyenler" olarak belirlenmiştir. Bu düzenlemenin GDPR m. 2/1 ile paralel olduğu görülmektedir[168]. Bu bağlamda, bir veri kayıt sisteminin parçası olmaksızın otomatik olmayan yolla işlenen veriler, KVKK'nin uygulama alanına girmemektedir. Fakat

---

[165] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, KVKK Yayınları, Ankara, 2019, (Rehber), s. 23.

[166] 1/541 Esas Numaralı Tasarı gerekçesinin çeşitli yerlerinde doğrudan Direktif'e atıf yapılmıştır. (Türkiye Büyük Millet Meclisi, 117 Sayılı Kanun Tasarısı ve Rapor, https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf, (E.T. 25.08.2022)).

[167] Fatma Koç, **İş İlişkisinde Kişisel Sağlık Verilerinin İşlenmesi**, On İki Levha Yayınları, İstanbul, 2022, s. 81.

[168] GDPR m. 2/1: Bu Tüzük, kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesine ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesine uygulanır. (Avrupa Birliği Bakanlığı, "GDPR Çevirisi", https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-Türkçe-Çeviri-AB-Bakanlığı.pdf, (E.T. 25.08.2022).

Türk Ceza Kanunu'ndaki (TCK) düzenlemeler, bu verilere koruma sağlar[169]. Ayrıca KVKK m. 28'de; sayılan hususlar da KVKK kapsamı dışında bırakılmıştır. Bu düzenleme idarenin keyfi uygulamalarına yol açabileceği için eleştirilmiştir[170].

Kanunun sistematiğine bakıldığında, kişisel verilere ilişkin tanımları, veri işleme şartlarını ve ilkelerini, verilerin aktarılmasını, veri sorumlusu ve sahibinin hak ve yükümlülüklerini, veri türlerini, denetim mekanizmaları ve bunlara başvuru usullerini, veri sorumluları sicilini ve Kişisel Verileri Koruma Kurumu'nu düzenlediği anlaşılmaktadır.

Kanun, bağımsız bir otorite olması gereken Kişisel Verileri Koruma Kurumu'na Cumhurbaşkanı tarafından üye ataması yapılması gibi çeşitli açılardan eleştirilse de[171], kişisel verilerin korunması alanını kapsayıcı ve özerk bir biçimde düzenlemesi ve kişisel verileri işleyenlerin uymaları gereken usul ve esasları düzenlemesi bakımından hukukumuzda önemli bir yere sahiptir.

(3) Medeni Hukuk

Kişilerin ehliyetleri ve bu sebeple sahip oldukları maddi ve manevi çıkarları üzerindeki haklarının kişiliği oluşturduğu kabul edilmektedir[172]. Bu bağlamda kişinin adı, şerefi, vücut bütünlüğü, ekonomik ve düşünsel etkinliklerine, mülklerine ilişkin hakları da kişilik hakkı içerisinde olup bu kapsamda korunmaktadır[173]. Bu sayılanlardan kişinin ismi, kişisel sağlık bilgileri, ekonomik durum bilgileri gibi birçoğunun kişisel veri olarak kabul edildiği çeşitli başlıklar altında detaylı bir şekilde anlatılmıştı. Bahsedildiği üzere, Anayasa'da temel bir hak olarak ihdas edilen kişisel verilerin korunması hakkının, anayasalarda yer alan insan onuru, özel yaşamın gizliliği, maddi ve manevi varlığını geliştirme gibi birçok temel hak ve özgürlükle

[169] Koç, s. 83.
[170] Alaattin Bük, **Bilişim Alanında Kişisel Verilerin Korunması**, Yetkin Yayınları, Ankara, 2021, ss. 88, 89; Gürsel, s. 165.
[171] Seven, s. 78.
[172] Turgut Akıntürk, Jale Akipek ve Derya Ateş Karaman, **Medeni Hukuk**, Beta Yayıncılık, İstanbul, 2022, s. 341.
[173] Akıntürk, Akipek ve Ateş Karaman, s. 342, 343.

ilişkili olduğu, dolayısıyla kişilik hakkının da bir parçası olduğu su götürmez bir gerçektir[174].

Türk Medeni Kanunu (TMK) m. 24'te;

> *Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hakimden, saldırıda bulunanlara karşı korunmasını isteyebilir. 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.*

denilmek suretiyle kişilik hakları, dolayısıyla bireylerin kişisel verileri koruma altına alınmıştır. Ayrıca 25. maddede "kişilik hakkı saldırıya uğrayanın, hakimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebileceği" öngörülmüştür. Benzer şekilde, birey kişisel verisi olan adının da 26. maddedeki düzenleme ile korunmasını isteme hakkına sahiptir. Ayrıca kişiliği haksız bir şekilde saldırıya uğrayan kişiler, Türk Borçlar Kanunu (TBK) genel hükümlerine göre tazminat da talep edebilecektir.

(4) İş Hukuku

Hayatını idame ettirebilmek için iş sahibi olmak oldukça önemlidir. Bu nedenle iş hayatı, kişinin yaşamında oldukça geniş ve önemli bir yer kaplar. İşçilerin kişisel verileri, sadece iş ilişkisinin devam ettiği sürece değil, ilişkinin kurulmasından önce ve sonlanmasından sonra bile ihlallere açıktır[175]. Örneğin iş başvurusu için gönderilen özgeçmişler; adayın adı, doğum tarihi, önceki iş tecrübeleri, aldığı eğitimler, hobileri gibi konularda kişisel veri ihtiva etmektedir. İşe alındıktan sonra, işçinin performansına ilişkin değerlendirmeler birer kişisel veri olarak kabul edilmektedir. İş ilişkisinin sona ermesinden sonra, işçinin emekli olup olmadığı hakkında bilgi sahibi

[174] Almanya Anayasa Mahkemesi de 1983'te verdiği Nüfus Sayımı (Volkszahlung) kararında bu durumu vurgulamıştır. Karara göre, verilerin sınırsızca kaydedilmesi, bu verilere her zaman erişilebilir olması ve kişinin profillenmesi ihtimali; üzerinde psikolojik baskı kurulması ve kamusal yaşama katılımını olumsuz etkileme riski doğurabilir. Bu durum da bireyin kişisel gelişim hakkını ve kamu çıkarlarını tehlikeye atabilir. Gelecekte çeşitli yaşam ilişkilerinin nasıl şekilleneceği ve bu ilişkilerin sınırları konusunda kararlar, bireyin kendi iradesiyle alınmalıdır. Bu nedenle, "bilgilerin geleceğini belirleme hakkı" ilkesi, kişisel veriler üzerinde tam kontrole sahip olma hakkını vurgular (Şimşek, ss, 114, 115.)

[175] Küzeci, s. 280.

olabilir. Bu nedenle işçinin kişisel verilerin gizliliğinin ve güvenliğinin sağlanması büyük bir önem taşır.

Örnek olarak, İş Kanunu m. 75'teki hükümle işveren, "işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla" yükümlü kılınmıştır. Yine bu hükmü tamamlar şekilde[176], Türk Borçlar Kanunu m. 419'da işverenin, "işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabileceği" hüküm altına alınmıştır. İşverenin bu yükümlülüklere aykırı olarak hareket etmesi halinde, işçinin sözleşmeyi İş Kanunu m. 24/2 uyarınca haklı nedenle feshetme hakkı olduğu ileri sürülmektedir[177]. 6331 Sayılı İş Sağlığı ve Güvenliği Kanunu m. 15/5'te de "sağlık muayenesi yaptırılan çalışanın özel hayatı ve itibarının korunması açısından sağlık bilgilerinin gizli tutulacağı" düzenlenmiştir.

(5) Ceza Hukuku

Kişisel veriler ceza hukuku kapsamında geniş bir korumaya sahiptir. Türk Ceza Kanunu'nun 9. bölümü, özel yaşamı ve yaşamın gizli alanını korumaya yönelik ceza normlarını konu almıştır. Kanunun 132. ve 140. maddeleri arasında haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğini ihlal, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme fiilleri suç olarak düzenlenmiştir. Özel hayatın gizliliğini ihlal suçu, diğerlerine göre daha genel nitelikli bir suçtur. Ayrıca, TCK m. 239'da yer alan ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması suçu ve m. 258'de yer alan göreve ilişkin sırrın açıklanması suçları kişisel verilerin korunmasına yönelik düzenlemelerdir. Yine TCK m. 243 ve sonrasında düzenlenen bilişim alanındaki suçların da dolaylı yoldan bu amaca hizmet ettiği ifade edilebilir.

Kanunun en önemli eksiği, kişisel veri tanımını açıkça yapmamış olmasıdır. Bu nedenle ceza hukukuna hakim olan, kanunilik ve belirlilik ilkelerine aykırı hareket

[176] Koç, s. 87.
[177] Toprak, s. 168.

edilmiştir. KVKK, söz konusu cezai düzenlemelerin yapıldığı tarihten sonra yürürlüğe girdiği için her iki kanunun terminolojisi arasında farklılıklar bulunmaktadır. Bu nedenle KVKK'ye mugayir bazı eylemler, TCK'de suç olarak ihdas edilmediğinden cezalandırılamamaktadır[178]. TCK ve KVKK hükümlerinin uyumlu hale getirilmesi ve eksikliklerin giderilmesi gerekmektedir.

Benzer şekilde Ceza Muhakemesi Kanunu (CMK) da kişisel verilerin korunmasına yönelik kısıtlı bazı hükümler içermektedir. CMK m. 135/6'da "iletişimin tespitine yönelik sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde kayıtların derhâl imha edileceği" belirtilmiştir. Bireylerin vücut muayenesi, bedenden numune alınması ve moleküler genetik inceleme işlemlerinin sonuçları, CMK m. 80 uyarınca "kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez. Koşulları oluştuğunda ise Cumhuriyet savcısının huzurunda derhal imha edilir". Benzer bir düzenleme TCK m. 81'de "kişinin fotoğrafı, beden ölçüsü, parmak ve avuç içi izi, bedeninde yer alan ve teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri" için de öngörülmüştür.

(6) İdare Hukuku

Bilindiği üzere, idare hukuku kodifiye edilmemiş bir alandır; yani idare hukukuna ilişkin mevzuat tek bir çatı altında toplanmamıştır ve yargı içtihatları ile de gelişim göstermektedir. Kişisel verilerin idare hukuku alanında korunmasına ilişkin çeşitli kanunlarda birden fazla örnek bulunsa da bunların en belirgini, 4982 Sayılı Bilgi Edinme Kanunu 21. maddesinde yer alan düzenleme üzerinden verilebilir. Anılan hüküm gereğince, "kişinin izin verdiği haller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır". Yine 22. maddeye göre, "haberleşmenin gizliliği esasını ihlal edecek bilgi veya belgeler de, bu kanunun kapsamı dışındadır". Nitekim emniyet müdürlüğünde görevli iken ateşli silahla

[178] Uğur Orhan, "Kişisel Verilerin Korunmasına İlişkin Türk Ceza Hukuku Düzenlemeleri Üzerine Değerlendirmeler", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 70, Sayı: 4, Ankara, 2021, s. 1359.

intihara teşebbüs eden ve tedavi gördüğü hastanede hayatını kaybeden polis memurunun annesinin, avukatı aracılığı ile yaptığı başvuruda, memurun personel sicil ve özlük dosyası, ölüme ilişkin yürütülen idari soruşturma dosyası gibi birtakım evrakların kendisine verilmesini istemiştir. İdarenin verdiği ret cevabı nedeniyle Bilgi Edinme Değerlendirme Kurulu'nun önüne gelen başvuruda, başvurucunun talebinin karşılanması gerektiği ancak bu esnada üçüncü kişilere ait hüviyet bilgileri ile hüviyetlerinin saptanmasına olanak veren bilgi ve ifadeler karartılmak suretiyle özel hayatın korunmasına riayet edilerek yapılması gerektiği ifade edilmiştir[179].

4. Kişisel Verilerin Korunmasının Hukuki Niteliği

a. Temel İnsan Hakkı Görüşü

Özellikle Avrupa hukukunda baskın olan ve bizim de katıldığımız görüş, kişisel verilerin korunması hakkının temel bir insan hakkı olduğu yönündeki görüştür[180]. Bu görüşün temelinde, kişisel verilerin korunması hakkının insan onuru ve özel hayatın gizliliği gibi birçok temel hak ve özgürlükle yakından ilişkili olması yatmaktadır. Gerçekten de teknolojinin gelişmesi ve dijital iletişimin yaygınlaşmasıyla birlikte kişisel verilerin toplanması, işlenmesi ve paylaşılmasının arttığı bir döneme girilmiştir. Bu nedenle bireylerin temel haklarına ve özgürlüklerine yapılan müdahaleler çeşitlenmiş ve artmıştır. Kişisel verilerin korunması, bireylerin ifade özgürlüğü, düşünce özgürlüğü ve hareket özgürlüğü gibi temel özgürlüklerini desteklemektedir. Kişisel verilerin kötüye kullanılması veya ihlal edilmesi, bu özgürlükleri sınırlayabilir, bu da demokratik toplum yapısının tehlikeye girmesine yol açar. Tarihsel süreç boyunca, çeşitli ulusal ve uluslararası hukuk sistemlerinde kişilerin veri güvenliğini sağlamak için birçok düzenleme yapılmıştır. Türkiye'nin taraf olduğu birçok insan hakkı belgesi, veri korumayla ilişkilendirilebilecek hükümler içermektedir. 2010 yılında yapılan referandumla, kişisel verilerin korunmasını isteme hakkı, bir temel hak olarak Anayasa'ya eklenmiştir. Yine KVKK m. 1 mucibince, "kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel

[179] Bilgi Edinme Değerlendirme Kurulu, 04.08.2021 tarih ve 2021/959 sayılı kararı, https://bedk.adalet.gov.tr/SayfaDetay/kararlar13072021121109, (E.T. 20.08.2022).
[180] Dülger, s. 80; Küzeci, s. 67.

hak ve özgürlüklerini korumak" amacıyla söz konusu kanun yapılmıştır. Tüm bu nedenlerle, kişisel verilerin korunması hakkının temel bir insan hakkı olduğu kuşkusuzdur.

Bu konudaki temel soru, kişisel verilerin korunması hakkının yakinen ilişkili olduğu özel hayatın gizliliği ve mahremiyet hakkı şümulünde kalan bir hak mı yoksa bağımsız bir hak mı olduğudur. Zira AİHM, kişisel verilerle ilgili olarak verdiği çeşitli kararlarda, tarafı olduğumuz AİHS m. 8'de öngörülen özel yaşama saygı hakkı kapsamında değerlendirme yaparak ihlal olup olmadığını belirtmektedir[181]. Fakat Avrupa Birliği Temel Haklar Şartı'nda özel yaşama saygı (m. 7) ile kişisel bilgilerin korunması (m. 8) hakları ayrı ayrı düzenlenmiştir. O halde, kişisel verilerin korunması hakkı ile özel hayatın gizliliği ve mahremiyet hakkı arasındaki münasebet hala çözümlenmemiş bir sorun olarak durmaktadır.

Kanaatimizce kişisel verilerin korunması hakkı, diğerleriyle dirsek temasını sürdürse de onlardan bağımsız bir hak olarak kabul edilmelidir. Zira bu iki hak, bir verinin kişisel veri sayılabilmesi için illa ki kişinin giz alanına ait veya sır niteliğinde olması gerekmediği[182] için her durumda örtüşmez. Bilindiği üzere özel hayatın gizliliği, insan haklarının hukuksal açıdan gruplandırılmasında, Jellinek'in negatif statü hakları kategorisine girmektedir. Bu tip haklarda, hakkın yerine getirilmesi için devletten sadece karışmaması ve engellememesi beklenir. Yani devletin bir pozitif harekette bulunması gerekmez; kişi, haklarından devletin bir muaveneti olmaksızın kendisine yaratılan özerk alan sayesinde yararlanır[183]. Bu bağlamda özel hayatın gizliliği hakkının sağladığı korumanın, kişisel veriler gizli tutulduğu sürece geçerli olacağı sonucu çıkacaktır ki bu husus her koşulda geçerli değildir. Örneğin, kişinin alenileştirdiği verileri, hala kişisel verisi olma niteliğini haizken; artık herkese açık hale geldiği için mahremiyetini ihlal etmeyecektir. Yahut kişinin camide, kilisede ya

[181] Yuliia Kovalenko, "The Right To Privacy And Protection Of Personal Data: Emerging Trends And Implications For Development In Jurisprudence Of European Court Of Human Rights", **Masaryk University Journal of Law and Technology**, Cilt: 16, Sayı: 1, 2022, s. 41.

[182] Murat Volkan Dülger, "Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 1, Sayı: 2, 2014, (Hasta Mahremiyeti), s. 45; Yargıtay Ceza Genel Kurulu, 17.06.2014 tarih ve E.2012/12-1510, K.2014/331 sayılı kararı, https://kararara ma.yargitay.gov.tr/, (E.T. 28.08.2022). Söz konusu kararda, kişinin zaten onu tanıyan herkesçe bilinen ve kolaylıkla ulaşılabilen fotoğrafı, kişisel verisi olarak kabul edilmiştir.

[183] Aydın Turhan, "İnsan Hakkı Kuşakları Arasındaki Tamamlayıcılık İlişkisi", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 4, Sayı: 2, 2013, s. 368.

da havrada dua edip ibadet yapması veya desteklediği siyasi partinin mitingine katılması gibi kamuya açık platformlarda gerçekleşen faaliyetlere ilişkin bilgiler, hassas kişisel veri olma niteliğini kaybetmeyeceği gibi kişinin gündelik yaşamında farklı muameleye uğramasına yol açabileceği için korunması gerekmektedir[184]. Yine, yanlış veri, kişinin mahremiyetini ihlal etmezken; söz konusu veri üzerinden kimliği belli veya belirlenebilir bir kişiye ulaşılabiliyorsa, bu durumda yine kişisel veri olduğundan bahsedilebilecektir[185]. Kişi başvuru yaparak bu veriyi düzeltme veya silme hakkını kullanabilir. Tüm bu nedenlerle, klasik insan hakları öğretisi kapsamında, özel hayatın gizliliği hakkı ile kişisel verilere yeterli koruma sağlanamayacağı açıktır. Nitekim AİHM de verdiği kararlarda, AİHS'i günün koşullarına uygun şekilde dinamik yorumlanması gereken "yaşayan bir enstrüman" olarak uyguladığı için, kişisel verilerin korunması özelinde, özel hayatın gizliliğinin sağlanması hususunda devletlere pozitif yükümlülük yüklemektedir[186]. Başka bir deyişle, aslında hakkın negatif yükümlülüklerle sağladığı korumanın yetmediğini doğrulamaktadır. Devletler, kişisel verilerin korunması hakkını kurumsallaştırarak bu konuya ilişkin uluslararası belgelere taraf olmakta, kendi iç hukuklarında mevzuat yapmakta ve bu kuralların uygulanması için bağımsız denetim ve kontrol mekanizmaları kurmaktadır. Böylece hem kamu otoriteleri hem de özel kişiler bu kurallara uymak zorunda kalmaktadır. Zira AİHS, dinamik yorum ilkesi olmadığı zaman, sadece devletlere karşı müdahale etmeme yükümlülüğü açısından koruma sağlamaktadır. AİHM'in devletlere yüklediği pozitif yükümlülükle artık o hakkı hem koruma hem de gerçekleştirmeye yönelik edimlerde bulunma sorumluluğu da doğar[187].

Özel yaşamın gizliliği ile kişisel verilerin korunması hakkı arasındaki başka bir fark, özel kişilerin sorumluluklarında yatmaktadır. Açıklandığı üzere, özel hayatın gizliliği hakkı, genellikle kamu otoritelerinin müdahale etmemesi ve bireylerin de müdahale etmemesi için mevzuat yapma yükümlülüklerinden oluşurken, kişisel

[184] Hüseyin Can Aksoy, "The Right To Personality And Its Different Manifestations As The Core Of Personal Data", **Ankara Law Review**, Cilt: 5, Sayı. 2, Ankara, 2008, (Personal Data), s. 240.
[185] Aksoy, Personal Data, s. 241.
[186] Kovalenko, s. 43.
[187] Semih Batur Kaya, "İnsan Haklarında Devletin Pozitif Yükümlülüğü: Avrupa İnsan Hakları Mahkemesi ve Anayasa Mahkemesi Üzerine Bir Analiz", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 9, Sayı: 1, İstanbul, 2022, s. 56.

verilerin koruması hakkı hem kamu otoritelerine hem de özel kişilere oldukça benzer yükümlülükler yüklemektedir. Örneğin, veri güvenliğini sağlama, veri işleme amaçlarına uygunluk, veri işleme kuralları ve sınırlamaları gibi açılardan benzer kurallara tabidirler. Ayrıca kişisel verilerin koruması hakkının ilgili kişilere farklı veri türleri üzerinde özel hayatın gizliliğinin sağladığından daha fazla kontrol imkanı vermektedir[188]. Gerçekten de kişisel verilerin korunması kapsamında, ilgili kişilere erişim, bilgilendirilme, unutulma, düzeltme gibi çok yönlü ve kendine özgü ilkeler içeren haklar verilmiştir. Söz konusu haklar, kişisel verilerin korunması hakkının ayrı ve bağımsız bir hak olarak düzenlenmesi sonucunda ortaya çıkmış ve somutlaşmıştır.

Daha genel olarak bakıldığında Anayasa, ayrıca düzenlenen kişisel verilerin korunmasını isteme hakkıyla (m. 20/3), özel yaşamın gizliliği hakkına (m. 20/1) kıyasla çok daha ayrıntılı bir düzenleme sunmaktadır. Böylece ilgili kişilere sağlanması gereken bazı güvenceleri, yenilikçi bir şekilde anayasal teminat altına almıştır[189]. Kişinin verileri hususunda bilgilendirilme, bunlara erişme, yanlış veya eksik olması halinde düzeltilmesini veya silinmesini talep etme ve işleme gayelerine yönelik mi tutulduğunu öğrenme hakları bunlardan bazılarıdır. Buna ek olarak kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği de belirtilmiştir. Yani tahdidi olmayan sayımla ilgili kişilerin hakları ve veri işlemenin kanun veya açık rıza gibi meşru bir dayanağa ihtiyaç duyması şartı anayasal statü kazanmıştır. Özel hayatın gizliliği veya başka bir temel hakka ilişkin düzenlemeden yola çıkarak bu ilkelere ulaşılamayacağı göz önüne alındığında, kişisel verilerin korunması hakkının ayrı ve müstakil bir temel hak olarak kabul edilmesinin gerekliliği bir kez daha anlaşılmaktadır.

b. Mülkiyet Hakkı Görüşü

Mülkiyet hakkının sahibine verdiği tam tasarruf yetkisi ve geniş yasal koruma imkanları düşünüldüğünde, kişisel verilerin de bu korumadan yararlanması için bir mülkiyet türü olduğunun ileri sürülmesi, aslında çok da şaşırtıcı değildir. Özellikle

[188] Kovalenko, s. 43.

[189] Maja Brkan, "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning", **German Law Journal**, Cilt: 20, Özel Sayı 6: Interrogating the Essence of EU Fundamental Rights, 2019, s. 880.

Amerikan hukuku menşeili bu düşünceye göre, verilerin birer mal olduğu kabul edilirse, kişiler çeşitli anlaşmalarla verilerinin kullanımının karşılığını alabilecek ve bu sayede kişisel veriler pazarı daha adil işleyecektir[190]. Ayrıca toplama, işleme ve koruma faaliyetlerinin ekonomik açıdan bir hayli külfetli olacağından daha özenli davranmaya iteceği düşünülmüştür[191].

Ancak piyasa karşısında bireyin pozisyonu dikkate alınarak, durum biraz daha ince irdelendiği zaman bu yaklaşımın kabul edilemeyeceği anlaşılmaktadır. Zira herhangi bir işinin yapılması için devlet kurumlarına başvuracak kişinin, kişisel verileri üzerindeki mülkiyet hakkından vazgeçmesi mecburi olabilecektir. Benzer şekilde, özel sektörde de kişilerin, özel kuralları olan bir pazar olmaksızın, olası bir değiş-tokuş sürecinde eşit konumda olması zordur. Her iki durumda da yarar sağlayan, eli güçlü olan taraf olan özel ve kamu hukuku tüzel kişileri, zarar gören ise zayıf konumda olan bireyler olacaktır[192]. Ayrıca satıldıktan sonra verilerin mülkiyeti el değiştireceği için, yeni malik eskisinin rızasına ihtiyaç duymadan, bu verilerle istediğini yapma hakkına sahip olacaktır. Verilerin artık hangi sebeplerle kullanılacağı veya ne gibi üçüncü kişilerin eline geçeceği belirli değildir. Kişinin verilerinin geleceğini belirleme hakkı artık ona ait olmayacaktır. Verilerinin işlenmesi, kullanılması veya aktarılmasından ileride duyabileceği bir rahatsızlık konusunda yapabileceği bir şey kalmayacaktır. Bireyler sıradan bir veri objesi olmaktan ileri gidemeyecektir[193]. Bu nedenlerle, kişisel veriler üzerinde mülkiyet hakkı bulunduğu görüşü, "temel hakların ticaretinin yapılamaz ve devredilemez oluşu" ilkesinin doğasına uygun düşmemektedir[194].

---

[190] Küzeci, s. 62.

[191] Steven H. Hazel, "Personal Data as Property", **Syracuse Law Review**, Cilt: 70, Sayı: 1055, 2020, s. 1059.

[192] Küzeci, s. 63.

[193] Almanya Anayasa Mahkemesi de 1983'te kurduğu Nüfus Sayımı (Volkszahlung) hükmünde bu durumu vurgulamıştır. Mahkemeye göre, kişisel verilerin korunması hakkı, kişisel verilerinin hukuka mugayir ve sınırsızca işlenip paylaşılması hallerinde kişiye temel bir hak sunarak kişiyi alelade bir veri nesnesi olmaktan kurtarmaktadır. (Şimşek, ss. 114-115.)

[194] Dülger, s. 79.

c. Fikri Mülkiyet Hakkı Görüşü

Fikri mülkiyetin konusunu, fikir ve sanat eserleri oluşturur. Düşünsel bir uğraş sonucu ortaya çıkan, orijinal, estetik kıymeti haiz ve onu meydana getirenin karakteristiklerini taşıyan bilim ve edebiyat, müzik, güzel sanatlar ve sinema eserleri fikir ve sanat eseri olarak kabul edilir[195]. Kişisel veriler de ait olduğu bireyin özelliklerini yansıttığı ve korunmaya ihtiyaç duyduğundan fikri mülkiyet haklarına benzetilerek, hukuken bu kavrama tanınan imkanlardan yararlanması gerektiği ileri sürülmüştür[196]. Ancak fikri mülkiyet hakkında, korunan hukuki değerin, eser sahibinin eseri üzerindeki emeği ve emeği karşılığı elde edeceği maddi menfaat olduğu gözden kaçırılmıştır[197]. Oysa kişisel verilerin korunması hakkının özünde, ilgili kişinin temel hak ve özgürlüklerinin korunması düşüncesi yatar. Dolayısıyla mülkiyet hakkı görüşüne yapılan eleştiriler, bu görüş için de geçerlidir. Kişisel verilerin ekonomik bir hak olarak kabul edilip korunması mümkün değildir.

II. İLGİLİ KİŞİ

A. İlgili Kişi Kavramı ve Niteliği

1. Genel Olarak

Sahiplik, sözlükte "herhangi bir şey üstünde mülkiyeti olma, onu yasaya uygun bir biçimde dilediği gibi kullanabilme" olarak tanımlansa da[198], niteliği ve korunması bakımından mülkiyet hakkından ziyade temel hak olması nedeniyle, kişisel verilerin mal olarak kabul edilemeyeceği ve üzerinde alım-satım veya benzer bir ilişkiye konu olacak bir sahipliğin mümkün olamayacağı açıklanmıştı. Aslında GDPR da orijinal İngilizce metninde data owner (veri sahibi) yerine data subject (veri öznesi) terimini

[195] Nurbanu Erzurumlu, "Türk Hukukunda Fikri Mülkiyete Konu Malların Cebrî İcrası", **Yıldırım Beyazıt Hukuk Dergisi**, Sayı: 3, 2017s. 171.

[196] Fikri mülkiyet, hem mülkiyet haklarını hem de telif hakkı ve lisans anlaşmaları gibi sözleşmeye dayalı hakları içerebilir. (Leon Trakman, Robert Walters ve Bruno Zeller, "Is Privacy and Personal Data Set to Become the New Intellectual Property?", **International Review of Intellectual Property and Competition Law**, Cilt: 50, Sayı: 8, 2019, s. 951).

[197] Seven, s. 39.

[198] Türk Dil Kurumu, https://sozluk.gov.tr/, (E.T. 31.08.2023).

tercih etmiştir. Ancak metin dilimize çevrilirken "veri sahibi" şeklinde bir Türkçeleştirme öngörülmüştür[199]. KVKK'de ise "ilgili kişi" terimi tercih edilmiştir. Tez içerisinde de ilgili kişi ve veri öznesi terimleri birbirlerinin yerine ve aynı anlama gelecek şekilde kullanılacaktır.

OECD Rehber İlkeleri'nin "Tanımlar" başlıklı 1. maddesinde kişisel veri, "belirli veya belirlenebilir kişiye ilişkin herhangi bir bilgi" olarak tanımlanırken tanımdaki belirli veya belirlenebilir kişinin "veri öznesi" olduğu ifade edilmiştir. Burada dikkat edilmesi gereken veri öznesinin yalnızca gerçek kişi olabileceğine dair bir sınırlamanın getirilmemiş olmasıdır. Yani tüzel kişilerin de veri öznesi olarak kabul edilmesi mümkündür. Yine mülga olan 95/46/EC Sayılı Direktif'te ve 108 Sayılı Sözleşme'de de, OECD Rehber İlkeleri'nde yer alan tanım kullanılmış ancak tanımda veri öznesinin sadece gerçek kişi olabileceğine dair bir ibare yer almıştır. Ayrıca 108 Sayılı Sözleşme Türkçeye çevrilirken "ilgili kişi" terimi tercih edilmiştir[200]. Sözleşme 108+'da bu tanım aynen korunmuştur[201].

GDPR m. 4/1'de "özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak belirlenebilir bir gerçek kişinin" veri öznesi olduğu ifade edilmiştir. KVKK'de ise veri öznesi yerine ilgili kişi terimi kullanılmış olup m. 3/1-ç'de "kişisel verisi işlenen gerçek kişi" tanımı yapılmıştır. Anlaşılacağı üzere, çoğu yasal düzenlemede, bir verinin kişisel veri olma niteliğini haiz olması için gereken son şart, ilgili kişinin gerçek kişi olması olarak belirlenmiştir. Bu nedenle öncelikle gerçek kişi ve tüzel kişilerin ayrımının yapılarak bazı özel durumların ayrıca irdelenmesi önem arz etmektedir.

---

[199] Tezin tamamlanmasından sonraki bir tarihte Dışişleri Bakanlığı tarafından yeni bir GDPR çevirisi yapılmış ve bu metinde "veri sahibi" yerine, doğru çeviri olan "veri öznesi" terimi kullanılmıştır. Yeni çeviriye ulaşmak için lütfen bkz. T.C. Dışişleri Bakanlığı, "AB Genel Veri Koruma Tüzüğü (GDPR) Türkçeye çevrildi", **T.C. Dış İşleri Bakanlığı Web Sitesi**, https://www.ab.gov.tr/siteimages/resimler/Nihai-ABB-HCDB-GDPR.pdf, (E.T. 05.04.2024).

[200] Tüm metin için lütfen bkz. Adalet Bakanlığı Web Sitesi, https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf, (E.T.10.10.2023).

[201] Tüm metin için lütfen bkz. Avrupa Konseyi Web Sitesi, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf, (E.T.10.10.2023).

2. Gerçek Kişilerde İlgili Kişi Olma Durumu

TMK 28. maddesinde gerçek kişiliğin sağ ve tam doğumla başladığı belirtilmiştir. Çocuğun bütün organlarıyla ana rahminden ayrılarak dış aleme gelmesi tam doğum, bu gerçekleştikten sonra kısa bir zaman zarfında da olsa bağımlı olmadan hayatta kalması ise sağ doğum olarak görülmektedir[202]. Hatta ceninler, gerçek kişilerin sahip olduğu hak ehliyetini, "sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder". Gerçek kişiliğin sona ermesi ise ölümün gerçekleşmesiyle olur. Ancak ölümün gerçekleştiğinin kesin olduğu ancak tam olarak kanıtlanamadığı durumlarda, ölüm ve birlikte ölüm (TMK m. 29, 31) karineleri de uygulama alanı bulmaktadır[203]. Ayrıca ölümün yüksek ihtimalle gerçekleştiğinin kabul edildiği durumlar da vardır. TMK m. 32 uyarınca, hakim kararıyla "hakları bu ölüme bağlı olanların başvurusu üzerine mahkeme kişinin gaipliğine karar verilebilir".

KVKK m. 3/1-ç'de ancak kişisel verisi işlenen "gerçek kişilerin" ilgili kişi olabileceği belirtilmiştir. Yani iç hukukumuza göre, tüzel kişilerin ilgili kişi olması mümkün değildir. Yine, GDPR m. 4/1'de veri öznesinin doğrudan veya dolaylı olarak belirlenebilir bir "gerçek kişi" olduğu ifade edilmiştir. Gerçekten de GDPR tarafından sağlanan koruma, tabiiyeti veya ikametgahı fark etmeksizin, kişisel verilerinin işlenmesiyle ilgili olarak sadece gerçek kişilere ilişkin olup; tüzel kişileri ve özellikle bu şekilde kurulan teşebbüsleri ilgilendiren verilerin işlenmesini kapsamamaktadır[204].

Gerçek kişiler, yalnızca yaşadıkları sürece ilgili kişi olabilirler; zira gerçek kişilik, doğum anıyla başlar ve ölümle son bulur. Dolayısıyla, ilgili kişi olabilmek için bir bireyin fiziksel olarak yaşayan ve varlığını sürdüren bir gerçek kişi olması gereklidir. Nitekim Kişisel Verileri Koruma Kurulu bir kararında, ölmüş kişiye ait kişisel verilerin artık gerçek kişiye ilişkin olamayacağını belirtmiştir[205]. Benzer şekilde, GDPR'nin gerekçesinde de ölen kişilerin kişisel verilerinin bu tüzük kapsamında korunmayacağı belirtilmekle beraber, ölen kişilerin kişisel verilerine

---

[202] Şaban Kayıhan, **Medeni Hukuk Bilgisi**, 5. Baskı, Seçkin Yayıncılık, Ankara, 2022, s. 156; Zafer Zeytin ve Ömer Ergün, **Türk Medeni Hukuku**, 6. Baskı, Seçkin Yayıncılık, Ankara, 2022, s. 79.

[203] Ayşe Arat, "Gerçek Kişilerde Kişiliğin Sona Ermesi", **Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi**, Cilt: 9, Sayı: 1-2, 2006, s. 258.

[204] GDPR 14 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-14/, (E.T. 15.08.2023).

[205] Kişisel Verileri Koruma Kurulu, 18.09.2019 tarih ve 2019/273 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6710/2019-273, (E.T.28.03.2023).

ilişkin iç hukuklarında farklı kurallar öngörebilme hususunda üye devletlere takdir yetkisi verilmiştir[206]. Her ne kadar ölü kişiler, medeni hukuka göre gerçek kişi olarak kabul edilmeseler de verileri bazı durumlarda dolaylı olarak korunabilir. Mesela, veri sorumlusu elinde bulundurduğu kişisel verinin sahibinin ölü olduğunu bilemeyebilir. Yahut bilse bile, verilerin işlendiği sistemde yaşayan ve ölü kişilere ilişkin bilgiler, bu yönde bir ayrım gözetmeksizin ve aynı koruma sağlanarak işlenmeye devam ediliyor olabilir[207]. Dolaylı olarak koruma sağlanan durumlara bir başka örnek olarak, ölüye ait verinin, yaşayan başka gerçek kişilere ilişkin bilgi içermesi durumu gösterilebilir. Örneğin, orak hücreli anemi hastalığına sahip ölünün bu durumuna ilişkin verinin, hastalık kalıtsal yollarla aktarıldığı için aynı zamanda ailesinin diğer üyelerine de ilişkin olma ihtimali vardır. Bu durumda ölünün kişisel verisi korunmaya devam edilmelidir[208]. Son olarak, ölü kişilerin verileri, veri koruma mevzuatı hariç başka kurallarla da koruma altına alınmış olabilir[209]. Örneğin, Tıbbı Deontoloji Nizamnamesi'nin 4. maddesinde doktorlara ve Avukatlık Kanunu'nun 36. maddesinde avukatlara sır saklama yükümlülüğü yüklenmiştir. Bu meslek mensuplarının gizlilik yükümlülüğü, hastanın veya müvekkilin ölümü ile sona ermez. Yine, her ne kadar Kişisel Verileri Koruma Kurulu tarafından kişilerin yakınlarının ölenin kişisel verilerine KVKK m. 11 kapsamında erişim talep edemeyeceği ifade edilmekteyse de[210], Kişisel Sağlık Verileri Hakkında Yönetmelik m.11/1'de; ölenin sağlık verilerine erişmeye yasal mirasçıları yetkili kılınmıştır. Ayrıca TCK m. 130/1'de "kişinin hatırasına hakaret" suçu düzenlenmiş olmakla, bu düzenleme ile ölenin kişisel verileri kullanılarak anısına yapılabilecek saldırıların engellenmesi mümkündür. Yaşarken kasten öldürme suçundan yargılandığına dair gazete haberinden yola çıkarak ölüye "katil" diye hakarette bulunulması, suçun koşulları oluşmuşsa TCK m. 130/1 kapsamında cezalandırılabilecek ve kişinin anısına yaşamının sona ermesinden sonra koruma sağlayacaktır. Ayrıca ölenin yakınları, kendi saygı duygularının incindiğinden bahisle kendilerine yönelik saldırının durdurulmasını TMK m. 24 kapsamında

[206] GDPR 27 No'lu Gerekçe, https://gdpr-info.eu/recitals/no-27/, **Avrupa Birliği GDPR Resmi Web Sitesi**, E.T. 15.08.2023.

[207] Article 29 Data Protection Working Party, Opinion 4/2007, s. 22.

[208] Murat Uçak, "Kişisel Verilerin Ölümden Sonra Korunması", **İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 6, Sayı: 10, İstanbul, 2021, s. 113.

[209] Article 29 Data Protection Working Party, Opinion 4/2007, s. 22.

[210] Kişisel Verileri Koruma Kurulu, 30.06.2020 tarih ve 2020/507 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6926/2020-507, (E.T. 28.03.2023).

hakimden isteyebilir; böylece dolaylı yoldan ölenin kişisel verileri de korunabilir. ABAD'ın bileşenlerinden olan Avrupa Genel Mahkemesi MS v Commission kararında[211], veri öznesinin ölümünden önce yapılan ve reddedilen veri erişim talebine ilişkin davanın, veri öznesinin mirasçısı tarafından takip edilebileceğini tespit etmiştir. Yine Pérez Gutiérrez v Commission kararında[212], mahremiyetin bazı yönlerinin veri öznesinin ölümünün ötesine geçtiği de kabul edilerek, ölen kişinin görselinin izinsiz kullanımı nedeniyle dul eşinin başvurusu üzerine, tütün paketleri üzerindeki fotoğrafın kaldırılmasına ve AB sınırları içinde bu şekilde kullanımının yasaklanmasına karar verilmiştir. Benzer şekilde hukukumuzda, ölenin vasiyeti veya mirasçılarının/yakınlarının talepleri ile kişisel verileri koruma kuralları arasında, hakkaniyet açısından bir denge kurulması gerekmektedir.

Ölüler gibi ceninlerin durumu da ilgili kişi olma açısından irdelenmelidir. TMK m. 28/2'ye göre "çocuk hak ehliyetini, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder". Yani ceninin hak ehliyeti erteleyici koşula bağlıdır[213]. Bu nedenle TMK m. 582/1 ile cenine sağ doğmak koşuluyla mirasçı olma hakkı tanınmıştır. Yine TMK m. 643'e göre "mirasın açıldığı tarihte, mirasçı olabilecek bir cenin varsa paylaşımın doğuma kadar ertelenir." Hukukumuz ceninlerin kazanımlarını korumaktadır. Buradan yola çıkarak ceninin de tam ve sağ doğması koşuluyla kişisel verilerinin korunması gerektiğini söylemek yanlış olmayacaktır[214]. Bu veriler; ultrason görüntüsü, DNA profili, anne-babasının kimliği, kaç haftalık olduğu, cinsiyeti, ana rahmine düşme tarihi, embriyonun doğal yolla mı yoksa tüp bebek gibi yapay yolla mı döllendiği gibi veriler olabilir. Mevzuatta ceninlerin kişisel verilerinin korunması hususunda eksiklik olduğu için açık bir düzenleme yapılması gerekmektedir.

İlgili kişinin kişiliğinin ayrıcalık arz ettiği başka bir durum da çocuk olmasıdır. İnternet ve özellikle de sosyal medya platformlarının kullanımının artmasıyla hem çocukların kendilerinin hem de ebeveynlerin, çocuğa ait kişisel verileri sıklıkla

---

[211] Avrupa Genel Mahkemesi, 27.11.2018 tarih ve T-314/16 ve T-435/16 numaralı MS v Commission kararı, https://curia.europa.eu/juris/liste.jsf?language=en&num=T-314/16, (E.T. 10.08.2023).

[212] Avrupa Genel Mahkemesi, 09.09.2015 tarih ve T-168/14 numaralı Pérez Gutiérrez v Commission kararı, https://curia.europa.eu/juris/liste.jsf?num=T-168/14&language=en, (E.T. 10.08.2023).

[213] Burcu G. Özcan Büyüktanır, "Ceninin Bedensel Bütünlüğünün İhlalinde Maddi Zararının Tazmini", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 9, Sayı: 1, 2018, s. 278.

[214] Gamze Turan Başara, "Medeni Hukuk İlişkilerinde Kişisel Verilerin Korunması", **Kişisel Verilerin Korunmasına Akademik Bakış**, (Ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy), Arkadaş Basımevi, Ankara, 2023, s. 441.

işlenmeye başlamıştır. Çocuklar kırılgan gruplar içerisinde yer aldığı için kişisel verilerinin korunması özellikle önem arz etmektedir. GDPR m. 8'e göre; kişisel verileri işleyebilmek için çocuğun on altıdan büyük olması gerekmektedir. Ancak üye devletler, bu yaşı on üçe kadar indirebilecektir. Çocuğun on altı yaşından küçük olması halinde, işlenme faaliyetinin yasallığı, ancak kanuni temsilcisinin açık rızasıyla mümkün olmaktadır. Buradan hareketle on altı yaşından büyük çocukların verilerinin işlenmesinin neticelerini anlama kabiliyetini haiz olacağı ve verdiği rızanın geçerliliğinin kabul edildiği söylenebilir. KVKK'de ise çocukların kişisel verilerinin korunması hakkında spesifik bir düzenlemeye yer verilmemiştir. Dolayısıyla çocukların verileri de yetişkinlerin verilerine yönelik usul ve esaslara tabi olarak işlenecek ve aynı haklara sahip olacaklardır. Yine, çocuğun verilerinin işlenmesinde aranan rıza kavramı, medeni hukuk kurallarımız göz önüne alınarak değerlendirilmelidir. Hiçbir baskı altında kalmaksızın özgür irade ile açıkça rıza verilmesi, şahısla kaim bir hakkın kullanılması niteliğindedir[215]. Çocuk temyiz kudretine sahipse, işleme konusunda verdiği rıza geçerli olduğundan buna dayanılarak yapılan veri işleme faaliyeti hukuka uygundur[216]. Bu bağlamda, çocuğun kişisel verilerinin işlenmesine veli veya vasisi rıza göstermişse, çocuk her zaman bu rızayı geri alabilir. Ancak çocuk verdiği rızanın sonuçlarını anlama yetisinden yoksunsa, veli veya vasinin açık rızasının alınması gerekir[217]. Çocuk rıza açıklama ehliyetine

---

[215] İlknur Deniz, **Çocuklara Ait Kişisel Verilerin Türk Medeni Kanunu ve Kişisel Verilerin Korunması Kanunu Kapsamında Korunması**, Seçkin Yayıncılık, Ankara, 2021, ss. 134-137.

[216] Deniz, s. 136; AİHM bir kararında, 14 yaşındaki çocuğun aynı evde yaşadığı üvey babası tarafından çıplak görüntülerinin kameraya alınması durumunda, çocuğun rızasının yokluğunu AİHS m. 8'in ihlali olarak değerlendirmiştir. Bu tespit, 14 yaşındaki bir çocuğun kişisel verisi olan görüntülerinin kayda alınmasına rıza göstermesinin sonuçlarını anlama yetisine sahip olduğunun kabulü açısından önemlidir (AİHM, 12.11.2013 tarih ve 5786/08 başvuru numaralı Söderman/İsveç kararı, https://hudoc.echr.coe.int/, (E.T. 10.09.2023). Kişisel Verileri Koruma Kurulu ise bir kararında, çocuğun ayırt etme gücünü haiz olması koşuluyla kanunun kendisine tanıdığı hakları tek başına kullanabileceğini belirtmiştir. Ancak yasal temsilcisinin de çocuk adına aynı şekilde işlem yapabileceğine değinilmiştir (Kişisel Verileri Koruma Kurulu, 11.08.2020 tarih ve 2020/622 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6816/2020-622, (E.T. 10.09.2023).

[217] Emel Badur, **Çocuğun Kişisel Verilerinin Korunması Kvkk, Gvkt ve Aihm Kararları Çerçevesinde Bir İnceleme**, Seçkin Yayıncılık, Ankara, 2023, s. 179; AİHM bir kararında, yeni doğan bebeğin ebeveynlerinin rızası olmaksızın, özel hastane tarafından çekilen fotoğrafının silinme talebinin reddedilmesini AİHS m. 8'a aykırı bulmuştur. Buradan rıza verme ehliyeti bulunmayan çocuğun yerine velilerinin rıza vermeye yetkili olduğu anlaşılmaktadır (AİHM, 15.04.2009 tarih ve 1234/05 başvuru numaralı Reklos ve Davourlis/Yunanistan kararı, https://hudoc.echr.coe.int/, (E.T. 10.09.2023)). Başka bir kararında ise, 11 yaşında ebeveynlerinin izni olmadan röportaj veren çocuğun görüntülerinin kaldırılmamasını AİHS m. 8'in ihlali olarak değerlendirmiştir. Mahkemenin, karar metninden 11 yaşı rıza vermeye ehil bulmadığı anlaşılmaktadır (AİHM, 01.06.2022 tarih ve 35582/15 başvuru numaralı IVT/Romanya kararı, https://hudoc.echr.coe.int/, (E.T. 10.09.2023)).

ulaştıktan sonra rızayı geri çekmezse veli ya da vasisi tarafından verilen rızayı kabul ediyor demektir. Fakat işlenen veriler özel nitelikli ise, işlemeye devam edilebilmesi için çocuğun rızası alınmalıdır[218]. Veli veya vasinin verdiği rıza, hiçbir şekilde çocuğun zarar görmesine neden olmamalıdır. Olursa TMK m. 346 kapsamında hakimin müdahalesi istenebilir. Çocukların kişisel verilerine ilişkin GDPR'dekine benzer hükümlerin, hukukumuza hakim olan çocuğun üstün yararı ilkesi de gözetilerek KVKK'ye eklenmesi gerektiği kanaatindeyiz. Son olarak, kısıtlıların kişisel verilerinin korunmasında, çocuklara ilişkin yapılan açıklamaların uygun düştüğü sürece uygulama alanı bulacağını belirtmek gerekmektedir.

3. Tüzel Kişilerde İlgili Kişi Olma Durumu

Farklı toplumsal, ekonomik ve teknik gereksinimler, kişi olarak kabul edilen varlıkların sadece insanlarla sınırlı tutulmamasına neden olmuştur[219]. Tüzel kişi olarak adlandırılan bu varlıklar da, cinsiyet, yaş, akrabalık gibi yaradılış icabı gerçek kişilere atfedilebilen özelliklerle vabeste olanlar hariç, hakların ve borçların ehliyetine sahiptir. TMK m. 47/1'e göre, "başlı başına bir varlığı olmak üzere örgütlenmiş kişi toplulukları ve belli bir amaca özgülenmiş olan bağımsız mal topluluklarına" tüzel kişi denmektedir.

Bir önceki başlıkta açıklandığı üzere, tüzel kişilerin ilgili kişi/veri öznesi olması, KVKK ve GDPR hükümleri uyarınca mümkün değildir. Sadece belirli veya belirlenebilir gerçek kişiler bu sıfatı haiz olabilmektedir. Kişisel verilerin korunması hakkının, temel bir insan hakkı olduğu düşünüldüğünde, bu durum şaşırtıcı değildir. Ancak devletlerin yasama işlemleriyle tüzel kişileri de veri öznesi olarak düzenlemesi yasaklanmamıştır[220]. Nitekim İsviçre, İtalya, Avusturya ve Lüksemburg gibi ülkeler, ulusal mevzuatlarında tüzel kişilerin veri öznesi olmasına imkan sağlayan düzenlemeler benimsemişlerdir[221]. Benzer şekilde, KVKK'nin yürürlüğe girmesinden

[218] Turan Başara, s. 447.
[219] Fahri Erdem Kaşak, "Tüzel Kişilik Kavramı ve Tüzel Kişilik Perdesinin Kaldırılması", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt: 26, Sayı: 2, 2020, s. 1243.
[220] ABAD da bir kararında bu ifadeyi desteklemektedir (ABAD, 06.11.2003 tarih ve C-101/01 numaralı Bodil Lindqvist kararı, https://curia.europa.eu/juris/liste.jsf?num=C-101/01, (E.T. 05.09.2023)).
[221] Gianclaudio Malgieri, **Vulnerability and Data Protection Law**, Oxford University Press, Oxford, 2023, (Data Protection Law), s. 22.

önce, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik m. 3/1-h'de kişisel veriyi "belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler" olarak tanımlayarak tüzel kişilerin de ilgili kişi olmasına imkan vermişti. Söz konusu yönetmelik şu anda mülgadır[222].

Tüzel kişiler doğrudan ilgili kişi olamasa da, tüzel kişilere ilişkin verilerden hareketle gerçek kişiye ulaşılabiliyorsa artık bu verilerin de kişisel veri olarak değerlendirilmesi gerekecektir[223]. Örneğin, çalışanın adı soyadının geçtiği bir şirket mail adresi artık kişisel veri kapsamında değerlendirilmelidir. Benzer şekilde, işyeri kimlik kartları; çalışanların adı, soyadı ve fotoğrafını içerir[224]. Bu bilgiler, belirli bir çalışanın kimliğinin tespiti için kullanılabileceğinden kişisel veri sayılır. Yine, bazı şirketler çalışanları hakkında internet sitelerinde veya sosyal medya platformlarında bilgi paylaşmaktadır. Bu bilgiler, çalışanların adını, unvanını, mezun olduğu okulları ve bazen iletişim bilgilerini içerebilir. Tüm bu bilgiler artık kişisel veridir. Ancak tüzel kişiler hakkındaki verinin, gerçek kişilerle bağlantılı olması halinin her maddi vaka özelinde ayrı değerlendirilmesinin lazım geldiği durumlar da söz konusu olabilir. Kişisel Verileri Koruma Kurulu bir kararında, bu hususa dikkat çekmiştir[225]. Karar; unvanında, gerçek kişi ilgili kişinin ad ve soyadının geçtiği bir şirkete ilişkindir. Söz konusu şirkete yönelik icra takibi başlatılmış ve dosya içeriği sosyal medyada herkese açık olarak paylaşılmıştır. Yapılan paylaşımlarda her ne kadar gerçek kişinin adı yer alsa da, yapılan yorumda esasen tüzel kişiliğin hedeflendiği anlaşıldığından söz konusu veri, gerçek kişinin değil, tüzel kişinin verisi olarak değerlendirilmiş ve başvuru KVKK'nin uygulama alanının dışında bulunmuştur.

---

[222] Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, **Lexpera İçtihat Sitesi**, https://www.lexpera.com.tr/mevzuat/yonetmelikler/elektronik-haberlesme-sektorunde-kisisel-verilerin-islenmesi-ve-gizliliginin-korunmasi-hakkinda, (E.T. 01.09.2023). Aynı adla 2020 yılında başka bir yönetmelik yürürlüğe girmiş ve tüzel kişilerin ilgili kişi olabileceğine dair ifadeler içermemektedir.

[223] Başalp, s. 35; Ian Walden, "The Application of Directive 95/46/EC", **The EDI Law Review**, Cilt: 3, Sayı: 2, 1996, s. 88; Toprak, s. 25; ABAD, 09.11.2010 tarih ve C-92/09 numaralı Volker und Markus Schecke GbR ve C-93/09 numaralı Hartmut Eifert v. Land Hessen kararları, https://curia.europa.eu/juris/document/document.jsf?docid=79001&doclang=en, (E.T. 05.09.2023).

[224] Dülger, s. 172.

[225] Kişisel Verileri Koruma Kurulu, 10.02.2022 tarih ve 2022/103 sayılı kararı, https://www.kvkk.gov.tr/Icerik/7293/2022-103, (E.T. 08.09.2023).

Tüzel kişilere ilişkin veriler, KVKK ve GDPR kapsamında korunmasalar da tamamıyla hukuki korumadan yoksun değildir. Ticaret ve rekabet hukuku, sınai mülkiyet hukuku, ceza hukuku gibi alanlarla tüzel kişilere ait verilerin bazı yönlerden korunması sağlanmaktadır. Nitekim AİHM de özel yaşamın gizliliği hakkı kapsamında tüzel kişilere bir kısım koruma sağlamaktadır. Örneğin bir kararda[226], üç şirkete ortak kullandıkları sunucuda yer alan tüm verileri vergi denetmenleri ile paylaşmaları emredilmiştir. Mahkeme, vergi incelemesi bittikten sonra incelenen verilerin yok edilmesi ve şirketlerin gerekli hazırlıkları yapmak üzere önceden haberdar edilmesi gibi sebeplerle, işin önemi ve kişisel verilerin korunması arasında makul ve adil bir denge kurulduğundan, AİHS m. 8'in ihlal edilmediği sonucuna varmıştır. Buradan mevzubahis dengenin kurulmaması halinde, konuta ve haberleşmeye saygı hakkı özelinde, tüzel kişilerin özel hayatın gizliliğinin hakkının ihlal edilebilecek olduğu sonucuna ulaşılmaktadır.

B. İlgili Kişi Kavramının Benzer Kavramlarla Karşılaştırılması

1. Veri Sorumlusu ile Karşılaştırılması

Veri sorumlusunun kim olduğu, görev ve sorumluluklarından bahsetmeden önce veri işlemenin ne anlama geldiğini açıklamak gerekmektedir. KVKK m. 3/1-e'ye göre veri işleme;

> *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 işlemdir.*

GDPR m. 4/2'de de işleme faaliyetinin;

> *otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisi*

olduğu ifade edilmiştir. Her iki madde lafzından anlaşılacağı üzere, yapılan sayımlar tahdidi nitelikte değildir. Kişisel verilerin elde edilmesinden başlayarak ilerleyen

[226] AİHM, 14.03.2013 tarih ve 24117/08 başvuru numaralı Bernh Larsen Holding AS ve diğerleri/Norveç kararı, https://hudoc.echr.coe.int/, (E.T. 10.09.2023).

süreçte, verilere yapılan tüm muameleler bu kapsamdadır[227]. Tamamen veya kısmen otomatik olan işleme ise, "insan müdahalesi ya da yardımı konusundaki ihtiyacın asgari seviyeye" indirilmesiyle olur[228]. Örneğin, özel bir hastanenin hasta kayıtları oluşturması ve saklaması, bir e-ticaret şirketinin müşteri tercihlerini analiz ederek kişiselleştirilmiş öneriler sunması, bir bankanın kredi başvurularını değerlendirip kredi notu vermesi, bir özel okulun sınav sonuçlarının kaydedip öğrencilerin akademik gelişimini izlemesi, bir turizm işletmesinin konukların güvenliğini sağlamak için güvenlik kameralarıyla izleme yapması, bir insan kaynakları görevlisinin çalışanların performans değerlendirmesini yaparak eğitim ihtiyaçlarını belirlemesi gibi faaliyetleri veri işlemeye örnek olarak verilebilir. Bir veri kayıt sisteminin parçası olmaksızın yapılan ve otomatik olmayan işlemelerin, KVKK ve GDPR kapsamında veri işleme faaliyeti olarak kabul görmediğine dikkat edilmelidir. Fakat bu veriler, TCK'de yer alan suçların konusu olabilir[229].

İşte kısaca genel hatları açıklanmaya çalışılan "veri işleme faaliyetinin amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu gerçek veya tüzel kişilere" veri sorumlusu adı verilmektedir. GDPR da KVKK'ye benzer bir tanım yapmış; "yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organı" veri sorumlusu (kontrolör) olarak kabul etmiştir. Veri sorumlusu, veri işleme faaliyetlerini yönetmek ve hukuka uygunluğunu sağlamakla görevlidir. Eğer bir tüzel kişi veri işliyorsa, burada veri sorumlusu tüzel kişinin şahsen kendisidir. Tüzel kişiliğin bünyesinde veri işleme faaliyetlerini yürütmekle görevli gerçek kişiler veri sorumlusu sayılmazlar[230].

İlgili kişi sadece gerçek bir kişi olabilirken, veri sorumlusu KVKK'ye göre hem tüzel hem gerçek kişi olabilmektedir. GDPR ise bu kapsamı daha da genişletmiş ve tüzel kişiliği bulunmayan kuruluşlar ve birimleri de veri sorumlusu olarak kabul etmiştir[231]. Her ne kadar kanun, tüzüğe göre daha sınırlı bir veri sorumlusu profili

---

[227] Kişisel Verileri Koruma Kurumu, **100 Soruda Kişisel Verilerin Korunması Kanunu**, KVKK Yayınları, Ankara, 2019, (100 Soru), s. 21.

[228] Kişisel Verileri Koruma Kurumu, 100 Soru, s. 22.

[229] Dülger, s. 176.

[230] Kişisel Verileri Koruma Kurumu, 100 Soru, s. 29.

[231] ABAD, 10.07.2018 tarih ve C-25/17 numaralı Jehovan todistajat (Jehovah's Witnesses) kararı, https://curia.europa.eu/juris/document/document.jsf?docid=203822&doclang=EN, (E.T. 05.09.2023). Yehova Şahitleri adlı dini topluluk, Finlandiya'nın merkezinde propaganda amacıyla

çizmişse de Kişisel Verileri Koruma Kurulu verdiği kararlarla veri sorumlusunu hayatın olağan akışının bozulmaması için kuralı geniş yorumladığını göstermektedir. Bu bağlamda tüzel kişi olmasa da kat malikleri kurulu; apartman, site ve benzeri yapılar bakımından veri sorumlusu olarak kabul edilmiştir[232]. Benzer şekilde başka bir kararda, yurtdışında yerleşik yabancı şirketlerin şubelerinin, tüzel kişilikleri bulunmasa da veri sorumlusu olabileceğine hükmedilmiştir[233]. Kanaatimizce hem uygulamadaki benzer sorunları çözmek hem de kişisel veri mevzuatında AB ile uyumu sağlamak adına kanunda değişiklik yapılarak tüzel kişiliği olmayan kuruluşlar ve birimler de veri sorumlusu tanımına dahil edilmelidir.

İlgili kişi, kişisel verisi işlenen kişiyi temsil ederken; veri sorumlusu en basit ifadeyle bu kişisel verilerin nasıl işleneceğini ve neden işlendiğini belirleyen kişidir. Yani kişisel verilerin korunması hukukunda birbirine karşıt iki noktada bulunduklarını söylemek yanlış olmayacaktır. İlgili kişinin çeşitli haklara (verilerine erişme, bilgi alma, düzeltme, silme vb.) sahip olmasına karşılık; veri sorumlusunun bu verileri işlerken söz konusu haklara saygılı davranma ve işleme faaliyeti esnasında temel ilkelere uygun davranma (hukuka ve dürüstlük kurallarına uygunluk, belirli, açık ve meşru amaçlar için işlenme, İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma vb.) yükümlülüğü vardır. Veri sorumlusu işleme sürecini aktif bir şekilde yönetir ancak ilgili kişi kendisine tanınan haklarla bu sürece etkin bir şekilde katılım ve denetim sağlama olanağına sahiptir. İlgili kişinin sadece kendi kişisel verileri üzerinde belirli hakları varken; veri sorumlusu sistemdeki herkesin kişisel verilere erişebilir. Veri sorumlusunun, ilgili kişiden farklı olarak veri sorumluları siciline kayıt yükümlülüğü ve idari para cezası sorumluluğu da bulunmaktadır.

---

insanlarla görüşmekte ve bu kişilerle ilgili verileri not almaktadır. Notların kapsamı; kişilerin kimlik bilgileri, adresleri, ailevi durumları gibi bilgilerden, dini inançları ve topluluğa katılmaya sıcak bakıp bakmadıklarına dair hassas nitelikteki bilgilere kadar değişmektedir. Topluluğun yönetimi toplanan bu verileri, hazırlanan yayınlarda kullanmalarını da tavsiye etmektedir. Fin Danıştayı ve ABAD, bu faaliyetleri bir veri işleme faaliyeti ve tüzel kişiliği olmayan topluluğu da veri sorumlusu olarak kabul etmiştir; zira topluluk, mensuplarından bu notların alınmasını talep etmektedir ve işleme faaliyetine tesir edebilen bir kontrol sistemini haizdir. Yani istediği zaman bir talimatla bu uygulamayı sonlandırma veya toplanacak verilerin içeriğini değiştirme vb. imkanlara sahiptir. Ek olarak verilerin hangi amaçla ve nasıl işleneceğine dair mensuplarına yol göstermektedir.

232 Kişisel Verileri Koruma Kurulu, 22.07.2020 tarih ve 2020/560 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6798/2020-560, (E.T. 28.08.2023).

233 Kişisel Verileri Koruma Kurulu, 23.07.2019 tarih ve 2019/225 sayılı kararı, https://kvkk.gov.tr/Icerik/5545/2019-225, (E.T. 28.08.2023).

2. Veri İşleyen ile Karşılaştırılması

Veri işleyen, KVKK m. 3/1-ğ'de yer alan tanımına göre; "veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi" ifade eder. GDPR ise veri işleyeni, tıpkı veri sorumlusunda olduğu gibi biraz daha geniş kapsamlı tanımlamıştır. Buna göre, veri sorumlusu "(kontrolörü) adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ" veri işleyen sıfatını haiz olabilir. Anlaşılacağı üzere, veri işleyen faaliyetlerinde, veri işlemenin çoğunlukla teknik tarafıyla alakalı olup veri sorumlusundan aldığı talimatlarla kısıtlı olarak hareket etmektedir[234]. Örneğin, bir e-ticaret şirketinin müşteri siparişlerini işlemek ve müşteri hizmetleri sağlamak amacıyla müşteri verilerini topladığı bir senaryoda; şirketin kendisi, müşteri verilerini toplayan ve bu verilerin nasıl işlendiğinden sorumlu olan kuruluş olan veri sorumlusu olacaktır. Ancak e-ticaret şirketi, müşteri siparişlerini işlemek için bir lojistik şirketiyle anlaşırsa lojistik şirketi veri işleyen olarak kabul edilir, zira müşteri verilerini e-ticaret şirketi adına işlemekte ve saklamaktadır. Bu veri işleme hizmeti sağlayıcısı, e-ticaret şirketinin veri işleme politikalarına ve talimatlarına uymakla yükümlüdür. Eğer veri işleyen, veri sorumlusunun talimatlarına aykırı eylemlerde bulunursa artık veri sorumlusuna dönüşür. Çünkü bu durumda artık bağımsız kararlar alıp hareket etmeye ve süreçte aktif rol oynamaya başlamıştır[235].

İlgili kişi sadece gerçek bir kişi olabilirken, veri işleyen KVKK'ye göre hem tüzel hem gerçek kişi olabilmektedir. GDPR ise bu kapsamı daha da genişletmiş ve tüzel kişiliği haiz olmayan kuruluşlar ve birimleri de veri sorumlusu olarak kabul etmiştir. Kanaatimizce kişisel veri mevzuatında AB ile uyumu sağlamak adına

---

[234] Kişisel Verileri Koruma Kurumu, 100 Soru, s. 30.

[235] GDPR m. 28/10; Kişisel Verileri Koruma Kurulu kararında; araç kiralama firmaları, gerçek kişi müşterilerin kişilerin bilgilerinin ve bu kişilerin kullanımlarına ilişkin olumsuz deneyimlerin ve çeşitli yorumların paylaşıldığı ortak bir kara liste yazılımı kullanmaktadır. Buna göre, araç kiralama firmaları, gerçek kişi müşterilerden kişisel verilerini toplayan veri sorumlularıdır. Fakat kullandıkları sistemler, bir firmanın işlediği verilere, diğerlerinin de erişim sağlamasına imkan sağlayan sistemler olarak tasarlanmıştır. Bu nedenle artık yazılım şirketlerinin ortak veri sorumluluğunun ortaya çıkacağı belirtilmiştir. Anlaşılacağı üzere, yazılım şirketleri veri işleme sürecinde aktif rol oynamaya başlamış, sadece veri sorumlusu araç kiralama firmalarının talimatıyla hareket eden bir veri işleyen olarak kalmamıştır. (Kişisel Verileri Koruma Kurulu, 23.12.2021 tarih ve 2021/1304 sayılı ilke kararı, https://www.resmigazete.gov.tr/eskiler/2022/01/20220120-10.pdf, (E.T. 30.08.2023)).

kanunda değişiklik yapılarak tüzel kişiliği bulunmayan kuruluşlar ve birimler de veri sorumlusu tanımına dahil edilmelidir.

İlgili kişi, kişisel verisi işlenen kişiyi temsil ederken; veri işleyen, işleme faaliyetlerinde veri sorumlusunun talimatlarına göre davranan kişidir. Kişisel verilerin korunması hukukunda, tıpkı veri sorumlusunda olduğu gibi, birbirine karşıt iki noktada bulunmaktadırlar. Veri işleyenin tek farkı bağımsız hareket etme yetkisinin olmamasıdır. İlgili kişinin çeşitli haklara (verilerine erişme, bilgi alma, düzeltme, silme vb.) sahip olmasına karşılık; veri işleyenin de bu verileri işlerken söz konusu haklara saygılı davranma ve işleme faaliyeti esnasında temel ilkelere uygun davranma (hukuka ve dürüstlük kurallarına uygunluk, belirli, açık ve meşru amaçlar için işlenme, İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma vb.) yükümlülüğü vardır. Veri işleyen, işleme sürecini pasif bir şekilde yönetir ancak ilgili kişi kendisine tanınan haklarla bu sürece aktif bir şekilde katılım ve denetim sağlama olanağına sahiptir. İlgili kişinin sadece kendi kişisel verileri üzerinde belirli hakları vardır. Veri işleyen de, işleme sürecinde çoğu zaman sınırlıdır; sistemdeki her veriye erişimi olmaz ve bu veriler hakkında kendince bir işlem yapamaz. Aksi takdirde verilecek idari para cezalarının doğrudan muhatabı olabilir[236].

3. İrtibat Kişisi ile Karşılaştırılması

Türkiye'de yerleşik olan gerçek ve tüzel kişiler için veri sorumlusu tarafından, Türkiye'de yerleşik olmayan gerçek ve tüzel kişiler için de veri sorumlusu temsilcisi tarafından, KVKK ve ona dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kişisel Verileri Koruma Kurumu ile iletişimi sağlamak amacıyla Veri Sorumluları Sicili'ne (VERBİS) kayıt esnasında bildirilen gerçek kişiye "irtibat kişisi" denmektedir (Yön. m. 4/1-ç). İrtibat kişisi KVKK'de düzenlenmemiş, Veri Sorumluları Sicili Hakkında Yönetmelik'te kendine yer bulmuştur[237].

[236] Çiçek Ersoy Kekevi, "Genel Kavramlar", **Kişisel Verilerin Korunmasına Akademik Bakış**, (Ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy), Arkadaş Basımevi, Ankara, 2023, s. 129.

[237] 30.12.2017 tarih ve 30286 Sayılı Resmi Gazete'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelik,https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=24276&MevzuatTur=7&MevzuatTertip=5, (E.T. 07.09.2023).

GDPR'da ise tam olarak irtibat kişisine karşılık gelecek bir kavram bulunmamaktadır. Ancak kişisel verilerin korunması açısından denetim otoritesiyle iş birliği yapmak, danışmak ve iletişimi sağlamak, veri öznelerinin haklarının kullanılmasında muhatap yüz olma görevleri açısından "veri koruma görevlisi" (data protection officer) irtibat kişisine benzerlikler taşımaktadır. Veri koruma görevlisi, GDPR m. 37 ve devamında düzenlemiştir.

İrtibat kişisi veri sorumlusunu KVKK kapsamında temsile yetkili değildir. Dolayısıyla gerek Kurum gerekse de ilgili kişiler nezdinde sorumluluk veri sorumlusu olan tüzel kişiye aittir. "Kamu kurum ve kuruluşlarında irtibat kişisi, koordinasyonu sağlayacak üst düzey yönetici tarafından sicile kaydı yapılan daire başkanı veya üstü yöneticidir" (Yön. m. 11/5). Tıpkı ilgili kişide olduğu gibi, sadece gerçek kişiler irtibat kişisi olabilmektedir.

4. Veri Sorumlusu Temsilcisi ile Karşılaştırılması

KVKK'de veri sorumlusu temsilcisinden bahsedilmişse de tanımına yer verilmemiştir. Veri Sorumluları Sicili Hakkında Yönetmelik'te (m. 4/1-p), Türkiye'de yerleşik olmayan veri sorumlularını bazı konularda asgari temsile yetkili Türkiye'de yerleşik tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı gerçek kişinin veri sorumlusu temsilcisi olabileceği ifade edilmiştir. Türkiye'de yerleşik olmayan veri sorumluları, veri işlemeye başlamadan önce veri sorumlusu temsilcisi marifetiyle VERBİS'e kaydolmak zorundadır (Yön. m. 5/1-b). "Kanunun uygulanmasıyla ilgili olarak Kurum tarafından veri sorumlusuyla kurulacak her türlü iletişim; Türkiye'de yerleşik olmayan veri sorumluları için, sicile bildirilen veri sorumlusu temsilcisi aracılığıyla gerçekleştirilir" (Yön. m. 12).

GDPR'da ise veri sorumlusu temsilcisi, 27. maddede düzenlenmiştir. Eğer bir veri sorumlusu veya veri işleyen AB içinde yerleşik değilse ve AB içindeki veri öznelerinin kişisel verilerini işliyorsa, bir veri sorumlusu temsilcisi atama zorunluluğunu haizdir. Bu temsilci, AB içindeki veri koruma yetkilileri ve veri özneleri ile iletişim kurar.

KVKK ve GDPR kapsamındaki yükümlülükler ve yaptırımlar açısından veri sorumlusu temsilcisinin bir sorumluluğu yoktur. İlgili kişi sadece gerçek bir kişi olabilirken, veri sorumlusu temsilcisi hem tüzel hem gerçek kişi olabilmektedir.

İKİNCİ BÖLÜM
İLGİLİ KİŞİNİN HAKLARI

I. GENEL OLARAK

İlk bölümde izah edildiği şekliyle, kişisel verilerin korunması hakkı bir temel insan hakkıdır. İlgili kişiye, kişisel verileri üzerinde kontrol sağlamaya yönelik haklar verilmesi, insan onuruna gösterilmesi gereken saygının bir gereğidir. Zira kişiler, kendilerine ilişkin olan veriler söz konusu olduğunda, basit birer veri nesnesi olmaktan öteye geçebilmeli ve kendi verilerinin geleceğini kendileri belirleyebilmelidir. Aksi takdirde, özünde insan onuru yatan insan haklarına saygılı hukuk devleti düzeni ve demokrasi zarar görecektir.

Kişisel verilerin korunması hakkı bir insan hakkıdır ancak bu hak somut olarak nasıl korunacaktır? İşte bu noktada, ilgili kişilere tanınan haklar devreye girer. Zira daha üst ve genel bir konsept olan kişisel verilerin korunması hakkı, kişilerin verilerinin gizliliğinin ve güvenliğinin sağlanması hakkını içerirken; ilgili kişilere tanınan haklar da bu amacı güvence altına alan, veri işleme faaliyeti üzerindeki denetimi sağlayan ve ilgili kişilere verileri üzerinde daha fazla farkındalık ve seçenek sunan somut haklar olarak karşımıza çıkar. Yani kişilerin verileri üzerinde daha fazla bilgi ve kontrol sahibi olmalarını sağlayarak kişisel verilerin korunmasını destekler. Örneğin, bir bireyin sosyal medya platformunda paylaştığı bazı kişisel bilgilerin, izni olmadan reklam amaçlı kullanıldığını fark ettiğini varsayalım. Bu durumda, verilerini korumak için nasıl bir yol izleyebileceğini bilmiyorsa, kişisel veri koruma düzenlemeleri çerçevesinde bilgilendirme hakkına sahip olduğunu öğrenebilir. Bu hakkını kullanarak platformdan bilgilerinin kimlerle ve hangi amaçla paylaşıldığını hakkında bilgi alabilir. Ayrıca gerektiğinde düzeltme veya silme taleplerinde bulunma hakkına sahip olduğunun farkına varabilir. Bu da bireyin mahremiyetinin ve kişisel verilerinin korumasına yardımcı olacaktır.

Kişisel verilerin korunması hukuku alanında ilk düzenleme olan OECD Rehber İlkeleri'nde açıkça ilgili kişilere hak tanınmamıştır. Zira metinde ilkeler daha çok kişisel verilerin işlenmesi sırasında saygı gösterilmesi gereken temel değerleri ve yaklaşımları vurgulamaktadır. Ancak 13. maddede yer alan "bireysel katılım ilkesine"

yönelik düzenlemeden[238] ilgili kişilere bilgilendirilme, erişim, itiraz, silme veya düzeltme gibi bazı haklar tanınması gerektiğine yönelik tavsiyede bulunulduğu anlaşılmaktadır. Benzer şekilde 108 Sayılı Sözleşme'de de ilgili kişi haklarını açıkça düzenleyen özel bir madde bulunmamakta olup sadece 8. maddede ilgili kişilere birtakım ek güvenceler sağlanmıştır[239]. Bu güvenceler bilgilendirilme, düzeltme ve silme haklarının temellerini atmıştır. Ancak 2018 yılında Modernize Edilmiş 108 Sayılı Sözleşme'nin (Sözleşme 108+) 9. maddesinde, GDPR ile uyumu yakalamak açısından açıkça ve detaylıca ilgili kişinin hakları düzenlenmiştir[240]. Esas olarak ilk defa ilgili kişiye açıkça bazı haklar tanıyan düzenlemenin 95/46/EC Sayılı Direktif olduğu söylenebilir. Zira mülga olan bu Direktif'in 10-15. maddelerinde bilgilendirilme, erişim, düzeltme, silme, işleme faaliyetini kısıtlama, itiraz, otomatik karar alınmasını kısıtlama hakları ve 23. maddesinde zararın giderilmesini isteme hakkı güvence altına alınmıştı[241].

2018 yılında yürürlüğe giren GDPR ile bu hakların kapsamı daha da genişlemiş ve bunlara ek olarak tüzük veri öznelerine yönelik bazı yeni hakları beraberinde getirmiştir. Tüzüğün 3. bölümünde görüleceği üzere bu haklar; bilgilendirilme, erişim, düzeltme, silme (unutulma), işleme faaliyetini kısıtlama, veri taşınabilirliği, itiraz ve otomatik karar alınmasını kısıtlama haklarıdır. Bunlardan veri taşınabilirliği ve unutulma hakkı yeni nesil haklar olup ilk defa GDPR ile kişisel veri koruma hukukunun bir parçası haline gelmiştir. Ayrıca GDPR m. 82'de kendisine yönelik bir

---

[238] *OECD Rehber İlkeleri m. 13- Bireysel Katılım İlkesi*
Bireylere aşağıdaki haklar tanınmalıdır:
a) Veri sorumlusundan veya başka bir kaynaktan, veri sorumlusunun kendisine ilişkin veriye sahip olup olmadığını teyit ettirme hakkı;
b) Kendileriyle ilgili verilerin, aşağıdaki koşullarda iletilmesi hakkı:
i. Makul bir süre içinde,
ii. Öngörülmüşse, abartılı olmayan bir ücret karşılığında,
iii. Makul bir şekilde ve
iv. Kolayca anlaşılabilir bir biçimde.
c) (a) ve (b) bentleri kapsamındaki bir talep reddedildiyse, reddin gerekçelerinin verilmesi ve böyle bir redde itiraz hakkı ve
d) Kendileriyle ilgili verilere itiraz hakkı ve itirazın başarılı olması durumunda verilerin silinmesi, düzeltilmesi, tamamlanması veya değiştirilmesi hakkı. (OECD Web Sitesi, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188, (E.T. 05.10.2023)).

[239] Tüm metin için lütfen bkz. Adalet Bakanlığı Web Sitesi, https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf, (E.T. 05.10.2023).

[240] Tüm metin için lütfen bkz. Avrupa Parlamentosu Web Sitesi, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf, (E.T. 05.10.2023).

[241] Tüm metin için lütfen bkz. Avrupa Birliği Web Sitesi, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046, (E.T. 05.10.2023).

ihlal sonucu maddi veya manevi zarar gören kişilere tazminat hakkı da verilmiştir. Bu haklar yalnızca veri sorumlusuna karşı ileri sürülebilmektedir. Ancak veri işleyen ile veri sorumlusunun yapmış olduğu sözleşmede, veri işleyene de bu sorumluluk yüklenmişse, bu durumda veri öznesi haklarını veri işleyene karşı da ileri sürebilecektir[242].

KVKK'de ise ilgili kişinin, kişisel verilerine yönelik olarak bilgilendirilme, erişim, düzeltme, silme, itiraz ve tazminat hakları bulunmaktadır. Bu haklardan veri taşınabilirliği GDPR'da bulunup KVKK'de bulunmazken; işlemlerin üçüncü kişilere bildirilmesini isteme hakkı da KVKK'de yer alıp GDPR'da mevcut değildir. Ayrıca KVKK'nin ilgili kişinin haklarını düzenleyen 11. maddesinde doğrudan yer almasa da genel olarak metinden sonuç olarak çıkarılan bazı haklar da bulunmaktadır. İlgili kişiye tanınan bu hakların ayrı ayrı ne anlama gelip hangi hususları kapsadığını tespit etmek önem arz etmektedir.

II. HAKLARIN KAPSAMI, ESASLARI VE ÖZEL KULLANILMA USULLERİ

A. Bilgilendirilme Hakkı

1. Bilgilendirilme Hakkının Kapsamı ve Esasları

Basit şekilde ifade etmek gerekirse, GDPR kapsamında bilgilendirilme hakkı; veri öznelerine kişisel verilerinin nasıl işlendiği ve hakları hakkında şeffaf ve kolayca anlaşılır bilgilerin sağlanmasını kapsamaktadır. Bu sebeple diğer haklardan önce geldiği yani daha öncül nitelikte olduğu söylenebilir. Şöyle ki bilgilendirilme hakkı doğrultusunda, verilerinin işlenmesine ve bu hususlaki haklarına ilişkin bilgisi olmayan kişi, diğer haklarını da bilmediği için ileri süremeyecektir[243]. Nitekim bu husus, ABAD'ın Smaranda Bara kararında da şu şekilde ifade edilmiştir: "Veri öznelerini kişisel verilerinin işlenmesi konusunda bilgilendirme gerekliliği, veri

[242] Heledd Lloyd-Jones ve Peter Carey, "The Rights of Individuals", (ed. Peter Carey), **Data Protection: A Practical Guide to UK and EU Law**, 5. Edition, Oxford University Press, Croydon, 2018, s. 122.

[243] Helena U. Vrabec, **Data Subject Rights under the GDPR: With a Commentary through the Lens of the Data-driven Economy**, Oxford University Press, 2021, s. 64.

öznelerinin işlenen verilere erişim, düzeltme ve itiraz haklarını kullanmalarını etkilediği için daha da önemlidir[244]."

GDPR'da hem doğrudan veri öznesinden kişisel verilerin toplandığı (m. 13) hem de alınmadığı (m. 14) hallerde sağlanacak bilgiler için kapsamlı iki ayrı düzenleme yapılmıştır. Her iki durumda da, söz konusu kişiye derhal, yani hemen verinin elde edildiği anda bilgi verilmelidir. Veri sorumlusu kişiyi; kendisi ile temsilcisinin kimliği ve iletişim bilgileri, ayrıca varsa veri koruma görevlisinin iletişim bilgileri, veri işleme amacı, işleme faaliyetinin yasal dayanağı, verisi işlenen kişinin çocuk olması halinde çocuğun temel hak ve özgürlüklerine ağır basan ve veri işlemeyi gerekli kılan bir meşru menfaatin bulunup bulunmadığı, kişisel verilerin iletilmesi durumunda alıcıların kim olduğu ve kişisel verilerin üçüncü ülkelere aktarılma niyetinin bulunup bulunmadığı, eğer aktarılacaksa bu ülkelerin münasip güvencelere sahip olup olmadığı konularında bilgi paylaşmakla yükümlü kılmıştır (m. 13/1, 14/1). Ayrıca, adil ve şeffaf bir veri işleme süreci için bilgilendirme hakkının; verilerin depolanma süresi ve bu süreyi belirlerken kullanılan kriterlerin neler olduğu, veri öznesinin hakları, rızanın geri çekilmesi hakkı, bir denetim makamına şikayet hakkı, kişisel verilerin sağlanmasının yasadan mı yoksa sözleşmeden mi kaynaklanan bir gereklilik olduğu ve verilerin sağlanmamasının hukuki sonuçları, profilleme de dahil otomatik karar alma hususunun uygulanıp uygulanmadığı ve varsa bu faaliyetlerin veri öznesi açısından önemi ve öngörülen sonuçları gibi konuları da içermesi gerektiği ifade edilmiştir (m. 13/2, 14/2). Zira otomatik karar verme, özellikle de profilleme işlemi, kişiler hakkında ön yargı oluşmasına, etiketlenmeye ve hatta ayrımcılığa varan olumsuz sonuçlar doğrulabilmektedir[245]. Örneğin, bir bankanın kredi verip vermeme kararı otomatik olarak bir algoritma tarafından yapılıyorsa ve bu algoritma, özellikle finansal geçmişi kötü olan kişilere düşük kredi notları verme eğilimindeyse, bu durum ihtiyaç sahibinin zor duruma düşmesine neden olarak hakkaniyetten uzak sonuçlar doğurabilir. Bu da veri işlemede adil olma ilkesine aykırılık teşkil edecektir. Yine, veri sorumlusu topladığı kişisel verileri, toplanma amacı dışında bir amaçla işleyecekse, yeni amaca ilişkin bilgilerle beraber bahsedilen konularda bilgilendirme de yapmalıdır

[244] ABAD, 01.10.2015 tarih ve C-201/14 numaralı Smaranda Bara and Others v Casa Naţională de Asigurări de Sănătate and Others kararı, https://curia.europa.eu/juris/liste.jsf?num=C-201/14, (E.T. 10.10.2023).
[245] Vrabec, s. 77.

(m. 13/3, 14/4). Her iki durumda da, veri sorumlusuna yüklenen bu yükümlülüklerin yerine getirilmesi için veri öznesinin bir talepte bulunması gerekmemektedir. Zira veri sorumlusu kendiliğinden harekete geçerek bilgilendirme görevini yerine getirmelidir[246]. Ancak "veri öznesinin halihazırda bu bilgilere sahip olduğu hallerde ve ölçüde" bu yükümlülüğün yerine getirilmesi gerekmez (m. 13/4). Kanaatimizce, pratikte bu durumu ispat yükünün veri sorumlusuna düştüğünün kabul edilmesi; dolayısıyla ikna edici bir kanıt olmaksızın, genel varsayımın veri sorumlusu tarafından kişisel verinin elde edildiği anda bilgilendirme yapılmadığının veya veri öznesinin halihazırda bu hususlarda bilgi sahibi olmadığının kabulü gerekmektedir.

Kişisel verilerin bizzat veri öznesinden alınması durumundan farklı olarak, bizzat alınmadığı hallerde; veri sorumlusunun kişisel verileri sağlama yükümlülüğüne ilişkin açıklama yapması gerekmez, çünkü bu hususta karar alma yetkisine sahip değildir[247]. Ek olarak, veri öznesine üçüncü bir taraftan elde edilen kişisel verilerin kategorilerinin de (adres, cinsiyet, sağlık vb.) bilgisi verilmelidir (m. 14/1-d). Bu farklılık muhtemelen böyle durumlarda, veri öznesinin paylaşılan veriler üzerinde detaylı bir fikre veya kontrole sahip olmamasından ileri gelmektedir. Elde edilen veri kategorilerini paylaşmak, işleme faaliyetinin kapsamını daha iyi anlamasına yardımcı olacaktır[248]. Yine bir başka farklılık olarak GDPR veri sorumlusuna, kişisel verilerin kaynağı ve bunların kamuya açık olup olmadığı konusunda da bilgi verme yükümlülüğü yüklemiştir (m. 14/2-f). Ayrıca veri öznesinin halihazırda bu bilgilere sahip olması durumuna ek olarak başka bazı koşullarda da bilgilendirilmesine gerek olmadığı ifade edilmiştir. Bunlardan birincisi, kişisel verilerin kaydedilmesinin yahut açıklanmasının veri öznesine bilgi sağlama yükümlülüğü yerine getirilmesinin herhangi bir sebeple imkansız veya orantısız bir çaba gerektirecek olmasıdır. Bu sebepler; veri işlemenin kamu yararına arşivleme, bilimsel veya tarihi araştırma ya da istatistiki amaçlarla yapılması gibi sebepler olabilir (GDPR m. 14/5-b). Bu örnekler tahdidi nitelikte değildir. Bu durumda veri öznesinin hakları ile özgürlükleri ve meşru menfaatlerinin korunması amacıyla uygun tedbirlerin alınması gerekmektedir. Bu tedbirler alınırken veri öznelerinin sayısı ve verilerin ne kadar zaman önce elde edilmiş

[246] Dülger, s. 529; Fundamental Rights Agency, s. 207.
[247] Vrabec, s. 67, 68; GDPR Bilgilendirme Hakkı Bilgi Notu, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/issues/right-to-be-informed/, (E.T. 11.10.2023).
[248] Vrabec, s. 67.

olduğu gibi faktörler göz önüne alınmalıdır[249]. Kişisel verinin bizzat verinin sahibinden elde edilmemesi halinde, bilgilendirilme hakkının gerekliliklerinin yerine getirilmesine gerek olmayan durumlardan ikincisi ise, veri işlemenin kanunda açıkça öngörülmesidir. Bunun için söz konusu yasal düzenlemenin veri sorumlusunun uymaya zorunlu olduğu ve veri öznesinin meşru menfaatlerinin korunması için uygun tedbirler öngören bir düzenleme olması şarttır (GDPR m. 14/5-c). Üçüncüsü ise, kişisel verinin işlenmesinin kanunen düzenlenen bir mesleki yükümlülük sebebiyle gizli kalmasının gerekmesidir (GDPR m. 14/5-d). Örneğin, bir avukatın müvekkilinin kişisel verilerini işlerken, avukatlık meslek kanunu gereği bu verilerin gizli tutulması yasal bir yükümlülüktür. Bu nedenle avukat, GDPR kapsamında verilerin işlenmesi hususunda veri öznesine bilgilendirme yapmak zorunda değildir.

KVKK'de ise ilgili kişinin bilgilendirilme hakkı, ayrıca ve açıkça düzenlenmiş bir hak değildir. Zira kanunda bilgilendirilme hakkı veri sorumlusunun aydınlatma yükümlülüğü adı altında hüküm altına alınmıştır. Buna göre, kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere şu konularda bilgi vermekle yükümlüdür: Veri sorumlusunun ve varsa temsilcisinin kimliği, verilerin işlenme amacı, kimlere ve hangi amaçla aktarılabileceği, veri toplamanın yöntemi ve hukuki sebebi ile ilgili kişinin diğer hakları (KVKK m. 10). Buna ek olarak, aydınlatma yükümlülüğünün yerine getirilmesi esnasında uyulacak usul ve esasları detaylıca belirlemek amacıyla, Kişisel Verileri Koruma Kurumu tarafından 2018 yılında "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ" yayınlanmıştır[250]. Tebliğin içeriği incelendiğinde, genel olarak GDPR'a benzer hükümler içerdiği görülmektedir. Kişisel verilerin ilgili kişiden elde edilip edilmediği ayrımları GDPR'da olduğu kadar kapsamlı olmasa da burada da yapılmıştır.

Tebliğin 5. maddesine göre, aydınlatma yükümlülüğü yani bilgilendirilme hakkının gereklilikleri, ilgili kişinin kişisel verilerinin işlendiği her durumda yerine getirilmelidir. Yani ilgili kişinin açık rızası alınmış olsa veya KVKK'deki diğer işleme şartları mevcut olsa bile bilgilendirilme hakkının gereklerinin yerine getirilmesinden

[249] GDPR 62 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-62/, (E.T. 11.10.2023).

[250] 10.03.2018 tarihli Resmi Gazete'de yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, **Resmi Gazete**, https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm, (E.T. 10.10.2023).

kaçınılamaz[251]. "Kişisel veri işleme amacı değiştiğinde, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmelidir" (Tebliğ m. 5/1-b). Bu yükümlülüğün yerine getirilmesi özellikle genel nitelikli verilerden yola çıkılarak özel nitelikli verilere ulaşma konusunda önem arz etmektedir[252]. Örneğin, kişinin zayıflamak için kullandığı bir egzersiz uygulamasını ele alalım. Doğal olarak, kullanıcının egzersiz türü ve süresi, konum bilgisi ve kalp atış hızı gibi bilgileri içeren verileri başta egzersiz rutinlerini takip etmek için toplanacaktır. Ancak bu verilere bakılarak kişinin genel sağlığı hakkında çıkarımlar yapmak veya kalp sorunları gibi potansiyel sağlık sorunlarını tespit etmek için kullanılıyor ve kişiye uygulama içinde hastane veya kalp damar hastalıklarında uzman doktor reklamları gösteriliyorsa, artık kişinin bu sebeple de rızasının alınması ve bu hususta da bilgilendirilmesi gerekecektir. Yine, "veri sorumlusunun farklı birimlerinde kişisel veriler farklı amaçlarla işleniyorsa, aydınlatma yükümlülüğü her bir birim nezdinde ayrıca yerine getirilmelidir" (Tebliğ m. 5/1-c). Örneğin, bir e-ticaret şirketinin satış departmanı müşteri siparişlerini işlemek ve ürünleri göndermek için kişisel verileri kullanırken; pazarlama departmanı, müşterilere özel teklifler sunmak ve tanıtım yapmak için kişisel veri işleyecektir. Bu sebeple her iki departman da ilgili kişiyi kendi faaliyetlerinin özelliklerine uygun olarak ve ayrı ayrı bilgilendirmelidir. Aydınlatma yükümlülüğünün yerine getirilmesi, tıpkı GDPR'de olduğu gibi ilgili kişinin talebine bağlı değildir ve "yerine getirildiğinin ispatı veri sorumlusuna aittir" (Tebliğ m. 5/1-e). Aydınlatma yükümlülüğünün yerine getirilmesi esnasında, "verilerin KVKK'nin 5. ve 6. maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiği yani veri işleme faaliyetinin hukuki sebebinin açıkça belirtilmesi gerekmektedir" (Tebliğ m. 5/1-h). Böylece ilgili kişiler, veri sorumlularının niyetlerinin daha fazla farkına vararak işleme faaliyetinin kapsamını daha kolay değerlendirebilirler. Bu durum da veri sorumlularına, kendi çıkarları ile ilgili kişilerin menfaatleri arasında adil bir denge kurulduğunu, ilgili kişilerin temel hak ve özgürlüklerinin risk altında olmadığını ispat konusunda bir motivasyon sağlamaktadır[253]. Ayrıca "kişisel verilerin aktarılma amacı ve aktarılacak alıcı grupları" ile "verilerin tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerden

[251] Dülger, s. 530.
[252] Vrabec, s. 73.
[253] Vrabec, s. 69.

hangisiyle elde edildiği" bu yükümlülük kapsamında belirtilmelidir (Tebliğ m. 5/1-ı, i). Söz konusu alıcı gruplarına iş ortağı, tedarikçi, iştirakler, hissedarlar, kanunen yetkili kamu kurum ve kuruluşları, kanunen yetkili özel hukuk kişileri vb. örnek olarak verilebilir[254]. Yükümlülük yerine getirilirken asla yükümlülüğü eksik, yanıltıcı ve yanlış bilgilere yer verilmemelidir. Dikkat edilmesi gereken bir husus, kanunda ve yönetmelikte, bilgilendirme yükümlülüğüne istisna hallerinin öngörülmediğidir. Dolayısıyla her durumda, belirtilen bilgilerin ilgili kişilere verilmesi gerekmektedir. Bu açıdan KVKK ve Yönetmelik, GDPR'dan daha katı bir nitelik göstermektedir. Bununla birlikte, KVKK m. 28'de belirtilen faaliyetler kapsamında veri işleme faaliyetinde bulunuluyorsa, aydınlatma yükümlülüğünün yerine getirilmesi zorunlu tutulmamıştır. Bunlar, bilgilendirilme hakkının istisnaları olarak kabul edilebilir[255].

Anlaşılacağı üzere, bilgilendirilme hakkı ile aydınlatma yükümlülüğü ve verilerin hukuka uygun, adil ve şeffaf bir şekilde işlenmesi ilkesi, bir madalyonun iki yüzünü oluşturmaktadır. Veri sorumlusu, kişisel veri işleme faaliyeti esnasında, kanundaki ilkelere uygun hareket eder ve üzerine düşen aydınlatma yükümlülüğünü eksiksiz bir şekilde yerine getirirse, aynı zamanda ilgili kişinin bilgilendirilme hakkının gereklerini de yerine getirmiş olur[256].

2. Bilgilendirme Usulü

Kural olarak veri sorumlusunun, GDPR m. 13/1'e göre, kişisel verilerin veri öznesinden elde edildiği anda, derhal ve gecikmeksizin bilgilendirme yükümlülüğünün yerine getirmesi gerekmektedir. Bu husus elbette kişisel verilerin bizzat veri öznesinden elde edildiği durumlarda geçerlidir. Eğer kişisel veri, bizzat verinin sahibinden elde edilmediyse, söz konusu bilgiler; veri öznesine makul bir süre içinde ve işleme koşulları göz önünde tutularak her halükarda bir ay içinde verilmelidir. Toplanan bilgilerin veri öznesi ile iletişim kurmak için kullanılacağı hallerde veri öznesi, kendisiyle temas sağlandığında derhal bilgilendirilme hakkına

[254] Kişisel Verileri Koruma Kurumu, **Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi**, Ankara, 2019, s. 10.
[255] Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğü, s. 12. Madde hükmünde sayılan istisna halleri, esasen tüm ilgili kişi hakları ve veri sorumlusu yükümlülükleri için geçerli olup; doğrudan KVKK'nin kapsamı dışında bırakılmıştır.
[256] Dülger, s. 473.

sahiptir. Yine, verileri başka bir alıcıya açıklanmışsa, en geç kişisel veriler ilk kez açıklandığı zaman bilgilendirme hakkının gereğinin yerine getirilmiş olması gerekir (m. 14/3).

Veri öznesine, özellikle de veri öznesi bir çocuksa; bilginin "öz, şeffaf, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanılarak" verilmesi gerekmektedir (m. 12/1). Bu hüküm aslında genel olarak tüm hakların kullanılmasına ilişkin olup en çok da bilgilendirilme hakkıyla yakından ilişkilidir. Madde hükmünde esasen, veri sorumlusuna bilgilendirmenin içeriğinin ve bilgilendirmede kullanılan dilin niteliği hakkında yükümlülükler verilmiştir.

Öncelikle bilgilendirmenin içeriği, öz yani kısa ve kapsamlı olmalıdır. Dolayısıyla veri öznesine sağlanan bilgiler, gereksiz kelimeler olmadan ve uygun düzeyde ayrıntıyla, veri öznesinin kafasının karışmasına mahal vermeyecek şekilde kaleme alınmalıdır. Bu sayede bilgilendirme metni, daha açık ve dikkat dağılmadan okunabilir hale gelir. Bilgilendirme metni aynı zamanda anlaşılır da olmalıdır. Burada veri öznesinin yetişkin mi yoksa çocuk mu olduğu önem taşır. Zira yaş itibarıyla hareketinin sonuçlarını anlama yeteneği çocuklarda daha düşük olduğundan, çocuklara yapılan bilgilendirmelerde bir yetişkine göre teknik terimlerden daha ari ve basit ifadeler kullanılması gerektiği tartışılmaz bir gerçektir. Ancak yetişkinler için de anlaşılırlık kriteri yüksek tutulmamalıdır. Çünkü kişisel verilerin korunması konusu son derece karmaşık ve teknik bir konu olabilir. Bir başka husus olarak, bilgilendirmenin içeriğinin kolayca erişilebilir olması da gerekmektedir. Bu nedenle, GDPR m. 12/1'de bilgilerin "yazılı olarak veya uygun olduğu hallerde, elektronik yollar da dahil olmak üzere diğer yollarla" sağlanması hüküm altına alınmıştır. Gerçekten de "Söz uçar, yazı kalır." mantığından hareketle, yazılı bilgilerin daha kalıcı ve ihtiyaç halinde bu bilgilere ulaşmanın kolay olacağını söylemek mümkündür. Özellikle de gelişen teknoloji sebebiyle kişi, dünyanın diğer ucunda olsa da kendisine gönderilen bir elektronik iletiyi yahut veri işleme faaliyetini yürüten kişinin internet sitesindeki gizlilik politikasını içeren gönderiyi istediği zaman ve sayıda okuma şansına sahiptir. Yahut kişinin verileri bir mobil uygulama (app) üzerinden işleniyorsa, gerekli bilgilendirmeler uygun zamanlarda bildirim şeklinde de gönderilebilir[257].

[257] Future of Privacy Forum and the Center for Democracy & Technology, Best Practices for Mobile Application Developers, **Future of Privacy Forum Web Sitesi**, 2018, https://cdt.org/wp-content/uploads/pdfs/Best-Practices-Mobile-App-Developers.pdf, (E.T. 13.10.2023), s. 3; Mobil

Ayrıca bilgilendirmenin yazılı bir şekilde yapılması, veri sorumlusunun bilgilendirme yükümlülüğünü yerine getirdiğine dair kanıt teşkil edecektir. Ancak bu husus, bilgilendirmenin sözlü olarak yapılamayacağı anlamına gelmez. Nitekim veri öznesi tarafından talep edilmesi halinde, bilgiler sözlü olarak da sağlanabilir. Ancak bu durumda veri öznesinin kimliğinin diğer şekillerde doğrulanması gerekmektedir (m. 12/1). Son olarak bilgilendirmenin içeriği şeffaf olmalıdır. Veri işleme sürecine hakim olan yaklaşımlardan biri olan bu ilke, aslında yukarıda açıklanan hususların tamamını kapsar; yani kişisel verilerin işlenmesine ilişkin olarak sağlanacak tüm bilgilerin ve kurulacak diyalogların kolayca erişilebilir ve anlaşılır olmasını gerektirmekle beraber, bu süreçte açık ve anlaşılır bir dil kullanılmasını şart koşar[258].

Bilgilendirme yükümlülüğünün yazılı, elektronik veya koşulları oluşmuşsa sözlü olarak yerine getirilebilmesinin yanı sıra, "standartlaştırılmış görsel semboller" olarak adlandırılan sembollerle de yerine getirilebileceği belirtilmiştir. Böylece anlatılmak istenen işlem, bir çırpıda ve bilgilendirme yükümlülüğünün yerine getirilmesinde uyulması gereken usullere uyularak anlatılabilecektir (m. 12/7). Örneğin, bir e-ticaret sitesi, müşterilerine kişisel verilerin korunmasıyla ilgili bilgi vermek için web sitesinde "kilit" sembolü kullanabilir. Bu sembol, verilerin güvende olduğunu göstereceğinden, kullanıcılar verilmek istenen mesajı açıkça anlayabilir[259]. "Simgelerin elektronik olarak sunulduğu hallerde, simgeler makine tarafından okunabilecek şekilde" sağlanmalıdır (m. 12/7).

KVKK'de bu hususta detaylı bilgi yer almasa da, iç hukukumuz uyarınca bilgilendirme/aydınlatma yükümlülüğünün yerine getirilmesine ilişkin kurallar, çoğunlukla GDPR'dekine paraleldir. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'de söz konusu yükümlülüğün yerine getirilirken, "genel nitelikte ve muğlak ifadelere yer verilmemesi" hüküm altına alınmıştır. Ayrıca "gündeme gelmesi muhtemel başka

---

uygulamalarda bilgilendirme yükümlülüğünün nasıl yerine getirebileceğine ilişkin detaylı bilgi için ayrıca bkz. Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", **Avrupa Komisyonu Web Sitesi**, 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf, (E.T. 08.10.2023), (Opinion 02/2013), s. 23.

[258] GDPR 39 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-39/, (E.T. 13.10.2023).

[259] Kişisel Verileri Koruma Kurumu'nun aydınlatma için kullanılacak sembol, işaret ve ikonları için lütfen bkz. Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğü, s. 21.

amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır" (Tebliğ m. 5/1-g). Veri sorumlusu kötü niyetle hareket etmese bile, kullandığı ifadeler muğlaksa, yükümlülüğünü ihlal etmiş sayılabilir[260]. Örneğin, bir şirkete iş başvurusunda bulunan kişinin özgeçmişi, ileride açılabilecek pozisyonlara alım için kullanılmak amacıyla saklanacağının bilgisi açıkça verilmelidir. "Kişisel verilerinizi yeni alımlar için kullanabiliriz." şeklinde muğlak ifadelerden kaçınılmalıdır[261]. "Aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak bildirimin anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir" (m. 5/1-ğ). Bu kapsamda yukarıda GDPR hükümleri için yapılan açıklamalar aynen geçerlidir.

Kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüğü, bu verilerin "elde edilmesinden itibaren makul bir süre içerisinde" yerine getirilmelidir. Elde edilen bu kişisel veriler ayrıca ilgili kişiyle iletişim amacıyla kullanılacaksa, ilk iletişim kurulması esnasında, ilgili kişi bilgilendirilmelidir. "Kişisel verilerin aktarılacak olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada ilgili kişiyi aydınlatma yükümlülüğünün yerine getirilmesi" gerekmektedir (Tebliğ m. 6). Bilgilendirmenin gereken zamandan önce veya sonra yapılan bilgilendirmenin etkisinin olmayacağı unutulmamalıdır[262]. Ayrıca bilgilendirmenin sadece başlangıçta değil, veri işlemenin devam ettiği sürece belirli aralıklarla yapılması gerektiği ifade edilmektedir[263]. Son olarak bilgilendirme, "veri sorumlusu ya da onun temsilcisi tarafından sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle" yapılabilir (Tebliğ m. 5/1). Örneğin, bir sitenin muhtelif yerlerine asılmış ve o bölgenin güvenlik amacıyla kamera görüntülerinin kaydedildiği yazısı (yazılı), operatörün müşteri temsilcisine bağlanmadan önce dinletilen ses kaydı (çağrı merkezi), bir çevrim içi alışveriş sitesinin internet sayfasında yer alan bir belgede soru-cevap şeklinde katmanlı aydınlatma

[260] Dülger, s. 530.
[261] Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğü, s. 10.
[262] Dülger, s. 473.
[263] Çalışma Grubu'nun verdiği örneğe göre; bir hizmetin konum verilerinin sürekli olarak işlenmesini gerektirdiği durumda, hizmet sağlayıcı veri öznesine aracının yerinin daha önce belirlenip belirlenmediğini, şu anda bu durumun devam edip etmediğini ya da gelecekte belirlenmeye devam edilip edilemeyeceğini bildirmelidir. (Article 29 Data Protection Working Party, "Opinion 15/2011 on the definition of consent", **Avrupa Komisyonu Web Sitesi**, 2011, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, (E.T. 10.10.2023), (Opinion 15/2011), s. 33).

yapılması (elektronik ortam) mümkündür. Ayrıca görme engelliler açısından bu yükümlülüğün yerine getirilebilmesi için ilgili mevzuatta (5378 Sayılı Kanun vb.) yer alan uygulamaların yapılması da mümkündür[264]. Veri sorumlusu, bu metotlardan hangisini izleyeceğini, işin mahiyetine göre kendisi seçmelidir.

3. Bilgilendirilme Hakkına İlişkin Örnek Kararlar

Kişisel Verileri Koruma Kurulu bir kararında[265], ilgili kişinin KVKK m. 11'de belirtilen hakları kapsamındaki taleplerini içeren başvurusuna hiçbir suretle cevap vermeyen ve banka olan veri sorumlusunun internet sitesinde yer alan aydınlatma metnini de incelemiştir. Metinde; veri işleme amaçlarının, KVKK'de belirtilen işleme koşullarından hangisine dayandığına yönelik hukuki sebep açıkça belirtilmeksizin sıralandığı tespit edilmiştir. Bu husus, Aydınlatma Yükümlülüğü Hakkında Tebliğ'in m. 5/1-h hükmüne aykırı bulunmuştur. Ayrıca bankanın aydınlatma metninde, kişisel veri işleme amaçları belirtildikten sonra, "gibi amaçlar kapsamında işlenmektedir" ifadesinin Tebliğ'de aynı maddenin (g) bendinde yer verilen ve "gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıracak" türden bir ifade olduğundan metnin gözden geçirilerek düzeltilmesi istenmiştir.

Yine Kişisel Verileri Koruma Kurulu, aldığı bir ihbar dilekçesinden hareketle, Amazon Turkey'in veri işleme faaliyetlerine yönelik resen bir inceleme yapmış ve aralarında ilgili kişinin bilgilendirilme hakkının da yer aldığı birtakım ihlaller tespit etmiştir. Bu ihlallerden konumuza ilişkin olan kısım aktarılacaktır. Yapılan incelemede; işleme faaliyetinin daha site henüz ziyaret edildiğinde başladığı ve hatta çerezler hakkında hazırlanan metinde sitenin ziyaretçilerinin tarayıcısını ve kullandığı aleti tanımak, ilgi alanları hakkında bilgi edinmek ve doğru ürünle hizmeti sağlamak gibi amaçlarla çerezlerin, piksellerin ve diğer teknolojilerin kullanıldığı görülmüştür. Kurul, sorumlusunun internet sayfasında gerekli metinlere yer verildiğine dair açıklamayı, aydınlatma yükümlülüğünün yerine getirilmesi kapsamında yetersiz bulmuştur. Zira siteye ilk defa giriş yapan bir kişinin, daha veri sorumlusu şirketle bir sözleşme akdedip akdetmeyeceği yahut verilerinin işlenmesine rızası gösterip

[264] Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğü, s. 14.
[265] Kişisel Verileri Koruma Kurulu, 02.05.2019 tarih ve 2019/122 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5461/2019/122, (E.T. 15.10.2023).

göstermeyeceğinin belli olmadığı göz önüne alındığında, yalnızca siteyi ziyaret etmekle işleme faaliyetine açık rıza verdiği sonucuna varılamayacaktır. Kararda, siteye girişle birlikte işleme yapılmaya başlanabilmesi için aydınlatma yükümlülüğünün daha giriş aşamasında yerine getirilmesi lazım geldiği vurgulanmıştır. Ancak söz konusu veri sorumlusunun site girişinde, çerezler ve pikseller gibi farklı araçlarla kişisel verilerin işlendiğine ilişkin olarak, bir pop-up mesaj gönderme vb. surette bilgilendirme sunulmamaktadır. Ayrıca yapılan işleme için izin almak amacıyla "Sitemizde gezinmeye devam etmek için çerez bildirimimize onay vermelisiniz" gibi bir istem de mevcut değildir. Bu durumun hem işleme faaliyetindeki açık rıza şartına hem aydınlatma yükümlülüğüne (ilgili kişinin bilgilendirilme hakkına) aykırılık teşkil ettiği tespit edilerek veri sorumlusuna yüz bin Türk Lirası idari para cezası uygulanmıştır[266].

Kişisel Verileri Koruma Kurulu başka bir kararında[267], çevrim içi ortamda başvuru toplayan veri sorumlusunun kişisel veri işleme süreçlerini incelemiştir. Söz konusu platformda iş başvurusunda bulunurken üyelik kaydı yapılması zorunludur. Bu esnada, ortak bir kutucuğun işaretlenmesi suretiyle, hem aydınlatma metninin okunup anlandığına hem de kişisel verilerin işlenmesine dair açık rıza verildiğine yönelik onay alınmaktadır. Bu husus, "veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi" kuralına (Yön. m. 5/1-f) aykırılık teşkil etmektedir. Kurul kararda, aydınlatma yükümlülüğünün yerine getirilmesinin ilgili kişinin onayına bağlı olmadığını vurgulayarak, kişinin işleme faaliyetiyle ilgili olarak aydınlatıldıktan sonra metinde yazılanlara açık rıza vermek zorunda olmadığını belirtmiştir. Zira platformdaki dizayna göre, kişi aynı anda ve tek hareketle, hem bilgilendirildiğine hem de açık rıza verdiğine dair onay vermeye zorlanmaktadır. Kurul bu nedenle, her iki hususa ilişkin işlemin yapılabilmesi için gereken mekanizmaların ayrıştırılması hususunda platformun talimatlandırılmasına karar vermiştir.

[266] Kişisel Verileri Koruma Kurulu, 27.02.2020 tarih ve 2020/173 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6739/2020-173, (E.T. 15.10.2023).

[267] Kişisel Verileri Koruma Kurulu, 26.07.2018 tarih ve 2018/90 sayılı kararı, https://www.kvkk.gov.tr/Icerik/5420/2018-90, (E.T. 15.10.2023).

Bilgilendirilme hakkına yönelik bir örnek de Fransa'nın veri koruma otoritesi olan Ulusal Bilişim ve Özgürlükler Komisyonu (CNIL) tarafından verilen bir kararda yer almaktadır[268]. CNIL, Google'ın veri koruma ve gizlilikle ilgili olarak düzenlediği bilgilendirme metinlerinin birden fazla çevrimiçi belgeye dağıldığını ve bunların kullanıcılar tarafından "kolayca erişilebilir" olmadığını tespit etmiştir. Bu bilgilerin dağınık düzenlemesi, veri öznelerinin haklarını ve Google'ın kişisel verilerini nasıl işlediğini anlamalarını zorlaştırmıştır. Ayrıca CNIL, Google'ın internet sitesi tasarımının da erişilebilirliği zorlaştıran unsurlardan biri olduğunu dile getirmiştir. Zira söz konusu tasarım, kullanıcıların ilgili gizlilik protokollerine erişmek için bir dizi tıklamalar gerektiren buton ve bağlantı gibi unsurlar içermekteydi. Bu bölünme de kullanıcıların aydınlatma metninde yer alan bilgilerin detaylarına kolayca erişmelerini zorlaştırmıştır. Veri sorumluları, bilgilendirme metinlerinin içeriğine dikkat ettiği kadar, bu bilgilerin nasıl sunulduğuna da dikkat etmeli ve internet sitelerinde bu husus için ayrılan kısımları kullanıcı dostu olacak şekilde dizayn edilmesine önem göstermelidir. Aksi takdirde GDPR m. 12/1'de yer alan yükümlülüklerini ihlal etmiş olacaklardır.

B. Erişim Hakkı

1. Erişim Hakkının Kapsamı ve Esasları

Erişim hakkının amacı; kişilerin, verilerinin işlenmesinin hukuka uygunluğunu ve işlenen verilerin doğruluğunu denetleme imkanına sahip olmaları için yeterli, şeffaf ve kolay erişilebilir bir şekilde bilgilendirilmesinin sağlanmasıdır.[269]. Bu nedenle erişim hakkı, ilk bakışta bilgilendirilme hakkına benzese de aslında aralarında bir fark bulunmaktadır. Bilgilendirilme hakkı, veri işleme faaliyeti başlamadan önceki aşamada daha önemli bir role sahipken; erişim hakkı, işleme faaliyetinin başlamasından itibaren tüm aşamalarda büyük bir öneme sahiptir[270]. Yani kişi, bilgilendirilme hakkı kapsamında, henüz işleme faaliyeti başlamamışken verilerinin

[268] CNIL, 21.01.2019 tarih ve SAN-2019-001 sayılı Google LLC kararı, https://www.cnil.fr/sites/cnil/files/atoms/files/san-2019-001.pdf, (E.T. 15.10.2023).
[269] European Data Protection Board, **Guidelines 01/2022 on data subject rights - Right of Access**, 2022, (Right of Access), s. 2.
[270] Vrabec, s. 104.

ne koşullar altında işleneceğini ve işlenmesine izin vermesi durumunda haklarının neler olduğu konusunda bilgi edinir. Ancak verileri işlenmeye başladıktan sonra ise bilgi edinme talepleri erişim hakkı kapsamında değerlendirilecektir. Bu yönüyle erişim hakkı, idare hukukundaki bilgi edinme hakkına benzetilebilir[271].

Erişim hakkı kapsamında veri öznesi, ilk olarak "kendisi ile ilgili kişisel verilerin işlenip işlenmediğini veri sorumlusundan teyit etme" hakkına sahiptir. İkinci olarak eğer verisi işlenmişse, bu verilere erişim talep edebilir. Üçüncü olarak işlenen verilerine ilişkin olarak; işleme amaçları, ilgili kişisel veri kategorileri, kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri, verilerin saklanma süresi veya bilinmiyorsa bu sürenin belirlenmesinde kullanılan kriterler, haklarının neler olduğu, denetim makamına şikayette bulunma hakkı, veriler kendisinden elde edilmemişse bu verilerin kaynaklarına ilişkin mevcut bilgiler, profil çıkarma da dahil olmak üzere otomatik karar verilip verilmediği, veriliyorsa otomatik karar verme sürecinin arkasındaki mantık ile bunun veri öznesi açısından önemi ve öngörülen sonuçları hususlarındaki bilgileri de talep edebilir (GDPR m. 15/1). Dördüncü olarak, "kişisel verilerin üçüncü bir ülke ya da uluslararası bir kuruluşa aktarılması durumunda, veri öznesinin verilerin uygun güvencelerle korunup korunmadığına dair bilgilendirilme hakkı bulunur" (GDPR m.15/2).

Kişi, erişim hakkını kullanma başvurusunda bulunurken herhangi bir gerekçe göstermek zorunda değildir. Veri sorumlusu, veri öznesinin talebinin, işlemenin hukuka uygunluğunu kontrol veya diğer haklarını kullanma konusunda gerçekten işe yarayıp yaramayacağına karar veremez[272]. Verilerin GDPR kapsamında korunduğu sürece[273], veri sorumlusu talebi dikkate alıp gereğini yapmalı, yani kişiye erişim sağlamalıdır. Veri sorumlusu, kendisi ile ilgili kişisel veri işlenip işlenmediğine dair bilgi edinmek isteyen herkese, sorunun yanıtı olumsuz olsa dahi, söz konusu kişiyle

---

[271] Ancak bu iki hak arasındaki fark şu şekilde ortaya konulabilir: İdare hukukunda bilgi edinme hakkı kişilere, kamu yetkililerinin karar alma süreçlerinde şeffaflığı sağlamak için tanınmıştır. Bu kapsamda herkes, idare tarafından kendisiyle ilgili tutulan bilgi ve belgelere erişim hakkına sahiptir. Bu hak, bu nedenle iyi yönetim hakkıyla da yakından bağlantılıdır. Ancak ilgili kişilere tanınan erişim hakkı, başta kişisel verilerin korunması hakkı ve özel hayatın gizliliği olmak üzere çeşitli temel hak ve özgürlüklerin korunmasına hizmet eder (ABAD, 29.06.2010 tarih ve C-28/08 numaralı European Commission v The Bavarian Lager Co. Ltd. kararı, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0028, (E.T. 15.10.2023)).

[272] European Data Protection Board, Right of Access, s. 2.

[273] Örneğin anonimleştirilmiş veriler artık kişisel veri olarak sayılmadığı için kişisel veri koruma mevzuatları tarafından korunmaz (GDPR 26 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-26/, (E.T. 15.10.2023).

ilgili bir veri işlenmediğini belirterek cevap vermek zorundadır[274]. Kişiyle ilişkili bir verinin işlenmesi halinde ise işlendiğini belirten cevabı, ister işlenen veriyle ilgili bilgilerle birlikte isterse de ayrıca verebilir[275].

Kişisel verilere erişim, yasal düzenlemelerden kaynaklanan bir engel yoksa, işlenen ve erişim talep edilen verilerin tamamının, doğru, güncel ve talebin alındığı andaki veri işleme durumuna mümkün olduğunca yakın bir şekilde veri öznesine sağlanmasıyla olur[276]. Bu bağlamda, sadece toplanan veri gruplarına dair verilen genel bilgi yeterli değildir. Örneğin, kişinin bir otomobil üreticisinin veri tabanında kişisel verilerinin bulunduğunu düşünelim. Kişi işlenen verilerinin neler olduğuna dair bir erişim talebinde bulunduğunda, firma yalnızca "kimlik, iletişim, banka hesap bilgileri ve satın alma geçmişi" gibi genel bir cevap verirse, bu durumda erişim hakkının gerekliliklerini yerine getirmemiş olacaktır. Veri sorumlusu ayrıca, verilerin türüne veya kaynağına bakmaksızın istenen erişimi sağlamakla yükümlüdür[277]. Hatta veri öznesi, söz konusu verileri en başta veri sorumlusuna sağlayan taraf olsa bile, bu verilere erişebilmelidir. Çünkü veri sorumlusunun, verileri doğru bir şekilde kaydedip kaydetmediğinin kontrolü ancak bu şekilde sağlanabilecektir[278]. Böylece eğer bir yanlışlık söz konusuysa bu verilere yönelik olarak düzeltme, silme veya itiraz haklarını kullanmasının da yolu açılmış olacaktır.

Ayrıca erişim hakkı kapsamında, yukarıda ifade edildiği üzere, veri öznesinin erişim talep ettiği verilere yönelik olarak bilgilendirilmesi de esastır. Bu bilgiler işleme faaliyeti başlamadan önce veri öznesine bilgilendirilme hakkı kapsamında genel anlamda sağlanmış olabilir. Örneğin, denetim makamına şikayet hakkı konusundaki bilgilendirme, işleme faaliyeti öncesinde ve sonrasında değişmeyecek bir bilgi içerir. Fakat her bilgi böyle genel nitelikte değildir. Mesela işleme faaliyeti başladıktan sonra, hangi verilerin hangi alıcılara açıklandığı gibi özgün detaylar, ancak erişim hakkının kullanılması sayesinde veri öznesine spesifik bir şekilde sunulabilecektir. Benzer şekilde işleme amacı da, veri öznesinin özellikle erişim talep ettiği veri bazında değerlendirilip açıklanmalıdır. Veri sorumlusunun sadece veri işlemedeki genel amaçlarının açıklanması yeterli olmaz. İşlemenin birden fazla amaç için

[274] Vrabec, s. 107.
[275] European Data Protection Board, Right of Access, s. 11.
[276] European Data Protection Board, Right of Access, s. 14.
[277] European Data Protection Board, Right of Access, s. 12.
[278] Dülger, s. 479.

gerçekleştirilmesi halinde, hangi verinin hangi amaçlar için işlendiğinin de açıklığa kavuşturulması gerekir[279].

Kural olarak veri sorumlusu kişinin kendisine ilişkin tüm verilere erişimi sağlamakla yükümlü olduğu için talebi sorgulamadan doğrudan erişim sağlaması gerekir. Ancak veri öznesine ilişkin çok fazla verinin işlendiği durumlarda, istenen erişim sağlanmadan önce veri sorumlusu, talebin tam olarak hangi işleme faaliyetine veya hangi bilgiye ilişkin olduğunu sorabilir[280]. Örneğin hasta, erişim hakkını kullanırken tüm tıbbi geçmişiyle ilgili bilgilerin kendisine verilmesini isterken aslında sadece son bir yıl içinde aldığı ilaçlarla ilgili bilgilere erişmek istemiş olabilir. Veri sorumlusu konumundaki hastanenin, kişiye özellikle öğrenmek istediği hususun ne olduğunu sorması, hem talebin kapsamını anlamalarına yardımcı olup iş yükünü azaltacak hem de veri öznesine daha hızlı ve amaca yönelik bir şekilde erişim sağlamasına katkıda bulunacaktır. Ancak veri öznesine bu hususta soru sorulması sırasında, veri işleme süreci hakkında anlamlı bilgi verilerek, talebi hakkında izahat istemenin sebebi açıklanmalıdır. Bunun erişim sağlanmasını geciktirmek veya engellemek için yapılan bir uygulama olmadığı ve her halükarda erişim talep edilen tüm bilgilerin kendisine sağlanacağı özellikle belirtilmelidir. Veri öznesi cevap olarak, miktarı çok fazla olsa da kendisine dair tüm verilere erişmek istediğini belirtiyorsa artık verilerin tamamı eksiksiz bir şekilde kendisine sağlanmalıdır.

Erişim talep edilen veriler, yanlışsa veya veri sorumlusu tarafından hukuka aykırı olarak işleniyorsa bile, veri öznesinin talebi yerine getirilmelidir[281]. Söz konusu veriler derhal silinmemeli veya düzeltilmemelidir. Veri öznesine verilerinin hukuka aykırı olarak işlendiği, bu durumdaki hakları ve veri sorumlusunun yükümlülükleri hakkında bilgi verilip bundan sonra nasıl ilerleneceği hakkındaki karar veri öznesine bırakılmalıdır[282].

Veri saklama süresinin geçmesi gibi nedenlerle silinen ve dolayısıyla artık veri sorumlusunun elinde bulunmayan verilere erişim sağlanması gerekmemektedir[283].

---

[279] European Data Protection Board, Right of Access, s. 36.

[280] GDPR 63 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-63/, (E.T. 15.10.2023).

[281] European Data Protection Board, Right of Access, s. 16.

[282] European Data Protection Board, Right of Access, s. 17.

[283] Ancak bir sonraki başlıkta örnek olarak incelenen Österreichische Post kararında ABAD, erişim hakkını geniş yorumlayarak veri öznesinin eskiden işlediği fakat şu an çeşitli nedenlerle elinde bulundurmadığı verileri de kapsadığı şeklinde bir değerlendirme yapmıştır.

Erişim talebinde bulunulan veriler, veri sorumlusunun talebine cevap verilmesi gereken yasal sürenin dolmasından önce, veri sorumlusunun gizlilik politikaları gereği silinecekse; veri öznesine söz konusu süre beklenmeksizin, yani veriler silinmeden önce erişim hakkı sağlanmalıdır[284]. Bu husus şöyle bir örnekle açıklanabilir: Diyelim ki, bir e-ticaret şirketi müşterilerinin siparişlerinin yer aldığı veri tabanını her üç yılda bir düzenli olarak temizliyor olsun. Bir müşteri de, bu üç yılın dolmasına on gün kala, geçmiş siparişlerinin verilerini incelemek ve bazılarını silmek istediği için veri sorumlusu konumunda olan şirkete erişim başvurusu yapsın. Bu durumda söz konusu veriler on gün sonra zaten silinecek olsa bile, kişiye derhal talebi doğrultusunda erişim sağlanmalı ve arzu ettiği inceleme ile işlemi yapmasına imkan sağlanmalıdır. Böylece veri öznesine verileri üzerinde daha fazla kontrol yetkisi verilmektedir.

Veri öznesinin çocuk olması durumunda erişim hakkını ileri sürecek kişi de doğal olarak çocuğun kendisi olacaktır. Ancak çocuğun algılama ve davranışlarını yönlendirme kabiliyetinin gelişmişlik durumuna göre, bu hak yasal temsilcisi tarafından da kullanılabilir. Ancak işlenen verileriyle ilgili olarak çocukla iletişim kuruluyorsa, çocuğun kolaylıkla anlayabileceği açık ve sade bir dille yapılmalıdır[285].

Veri öznesi, işleme faaliyetinden geçen kişisel verilerin bir nüshasını alma hakkına sahiptir (GDPR m. 15/3). Bu hak, erişim hakkının sağlanmasının fiziksel bir görünümüdür. Ancak bu hak, "başkalarının hakları ve özgürlüklerini olumsuz yönde" etkileyecek şekilde kullanılamaz (GDPR m. 15/4). Anlaşılacağı üzere burada erişim hakkına bir kısıtlama getirilmiştir. Şayet üçüncü kişilerin ticari sırları veya fikri mülkiyet veya mahremiyet hakları başta olmak üzere başkalarının hakları veya özgürlüklerinin olumsuz etkilenmesi söz konusuysa[286], veri sorumlusu her iki menfaat arasında makul ve adil bir denge kurmalıdır. Yani ne başkalarının sırlarını ifşa etmeli ne de veri öznesinin erişim talebini yerine getirmekten kaçınmalıdır. Bu durumda ilgili verilere erişim, üçüncü kişileri ilgilendiren kısımların; takma isim kullanma, maskeleme ve karartma gibi yöntemlerle sansürlenmesi ile sağlanabilir[287]. Veri öznesi erişim hakkından tümüyle yoksun bırakılamaz. Erişim hakkına bir başka kısıtlama da

[284] European Data Protection Board, Right of Access, s. 17.
[285] GDPR 58 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-58/, (E.T. 15.10.2023).
[286] GDPR 63 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-63/, (E.T. 15.10.2023).
[287] Yöntemler hakkında detaylı bilgi için lütfen bkz. Dipnot 77.

GDPR m. 12/5 hükmü ile getirilmiştir, ancak veri öznesinin tüm haklarının kısıtlanmasına yönelik olarak başka bir başlık altında incelenecektir.

KVVK'de ise erişim hakkı ilgili kişinin haklarını içeren 11. madde hükmü içerisinde birden fazla ve bağımsız haklar olarak düzenlenmiştir. Buna göre herkes, veri sorumlusuna başvurarak kendisiyle ilgili şunları yapabilir: "Kişisel veri işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgi talep etme, işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme". Yukarıda GDPR için yapılan açıklamalar göz önüne alındığında, ayrı ayrı düzenlenen bu hakların erişim hakkının içeriğini oluşturduğu görülecektir. Bu nedenle konuya ilişkin olarak yukarıda yapılmış açıklamalar KVKK'deki hüküm açısından da geçerlidir.

2. Erişim Usulü

Veri öznesi, işlenen kişisel verilerin bir nüshasını alma hakkına sahiptir (GDPR m. 15/3). Kural olarak erişim hakkının ne şekilde sağlanacağı konusunda takdir hakkı veri sorumlusuna ait olduğu için, veri öznesine dilerse işlenmekte olan kişisel verileri içeren orijinal belgelerin aynen çoğaltılarak verilmesini, dilerse de yalnızca kişisel verilerin neler olduğuna ilişkin bir kopyanın verilmesini sağlayabilir. İkinci durumda, kişisel verilerin değiştirilmemiş bir kopyası veri öznesine sunulmak zorundadır[288]. Bu durumu bir örnek üzerinden şu şekilde açıklayabiliriz: Bir eğitim kurumu öğrencilerin akademik kayıtlarını elektronik olarak tutuyor olsun. Kurumun öğrencilerinden birinin; ders notları, sınav sonuçları ve genel olarak öğrenci performansıyla ilgili verilere erişim talebinde bulunduğunu varsayalım. Okul, erişim talep edilen tüm bu verileri ayrı ayrı belgelerle sunmak yerine, hepsini derlediği bir raporu sunabilir. Fakat bunun tam tersinin önemli olduğu durumlar da olabilir. Örneğin bir işverenin, çalışanının işyerindeki performansını değerlendirmek için bir dizi e-posta yazışması ve performans değerlendirme raporu gibi belgeleri kullandığı durumda; işveren, çalışanının erişim talebini yerine getirirken tüm orijinal belgelerin bir nüshasını vermesi daha doğru olacaktır. Böylece hem çalışan kendi performansını bağımsız bir şekilde değerlendirebilir hem de işverenin değerlendirme sürecinin şeffaflığı sağlanır.

[288] European Data Protection Board, Right of Access, s. 46.

Ayrıca, kişinin kendi sesini içeren kayıtlar veya üzerinde ıslak imza bulunan evraklar gibi materyallerin sahici olup olmadığını doğrulama amacıyla, orijinal örnek sağlanması daha uygun olacaktır. Fakat veri öznesinin onayının olması halinde, ses kaydının sadece dökümünün verilmesiyle de yetinilebilir[289].

Kişinin ilk talebine yönelik verilen nüshalar ücretsiz sağlanır. Ancak nüshanın kaybolması veya zarar görmesi ve sair nedenlerle başka nüshalar da talep edilirse, veri sorumlusu "idari masraflar için makul bir ücret talep edebilir" (GDPR m. 15/3). Peki veri öznesinden gelen "ikinci talebin" farklı bir "ilk talep" olup olmadığı nasıl anlaşılacaktır? Eğer ikinci talep; zaman ve kapsam açısından önceki talepte erişim istenen aynı kişisel veri seti ile ilgiliyse, artık bunun ek bir kopyanın istendiği "ikinci talep" olarak yorumlanmak mümkündür. Ancak aynı veri setiyle ilgili farklı bir zaman dilimine ilişkin bir nüsha istenirse, bu yeni ve ayrı bir talep olarak kabul edilip ücretsiz karşılanmalıdır[290]. Örneğin, veri sorumlusuna işlenen tüm verilerimize erişim talep ettiğimizi bildirdik ve tarafımıza nüsha verilmesini istedik. Aradan iki ay geçtikten sonra yeniden aynı taleple başvurduğumuzda, bunun yeni bir ilk talep olarak kabul edilmesi gerekmektedir. Zira aradan geçen zamanda yeni veriler işlenmiş olabilir. Benzer şekilde, veri öznesine ilk talebi üzerine, erişim eksik sağlanmış veya hiç sağlanmamışsa da ikinci talebi aslında bir "ilk talep" olarak kabul edilip ücret alınmamalıdır. Ayrıca istenen ücret hiçbir zaman fahiş bir bedel olmamalı, sadece yapılan masrafı karşılamaya yönelik olmalıdır. Veri sorumlusu ücret talep edecekse bunu veri öznesine önceden bildirip talebini geri çekip çekmeme konusunda karar almasına olanak sağlamalıdır[291].

Veri öznesi erişim talebini elektronik yoldan yapmış ve aksini talep etmemişse, istenen bilgiler yaygın kullanılan bir elektronik yolla kendisine sağlanır (GDPR m. 15/3). Yaygın kullanılan elektronik yolun tanımı GDPR'da yapılmamış olup erişim talebinin yapıldığı zamanın koşullarına göre değerlendirilmesi gerekecektir. Ancak "yaygın kullanım" teriminden kastın, veri sorumlusunun profesyonel anlamda günlük işleyişinde kullanılan değil, genel olarak insanlar tarafından yaygın olarak kullanılan bir biçim olduğu söylenebilir. Yani kişi, sırf veriye erişim sağlamak için belirli bir

[289] European Data Protection Board, Right of Access, s. 47.
[290] European Data Protection Board, Right of Access, s. 13.
[291] European Data Protection Board, Right of Access, s. 14.

yazılımı satın almak zorunda kalmamalıdır[292]. Veri sorumlusunun erişimi sağlamayı seçtiği format ne olursa olsun, içindeki bilgiler hem anlaşılır hem de kolayca erişilebilir bir şekilde bulunmalıdır. Verilerin kağıt, CD veya USB gibi bir elektronik depolama cihazında ve sair somut ve kalıcı bir şekilde sunulması önemlidir[293]. Her ne kadar veri sorumlusu, verilerin bir kopyasının verilmesi dışında başka türden erişim sağlaması yönünde zorunlu tutulamazsa da, makul bir çözüm için başka yollar seçebilir[294]. Yani erişim sözlü, dosyaların denetimine izin verme, yerinde veya uzaktan erişim sağlama şeklinde de olabilir. Elverişli hallerde veri sorumlusu, veri öznesinin kişisel verilerine güvenli bir sisteme uzaktan ve doğrudan erişim sağlayabilmelidir[295]. Ancak bu yolun seçilmesi ve uygulanması, veri öznesinin bir nüsha alma hakkını ortadan kaldırmaz.

3. Erişim Hakkına İlişkin Örnek Kararlar

ABAD yakın tarihli bir kararında[296], veri sorumlusu olan posta hizmeti şirketine erişim hakkı kapsamında başvuru yapılan bir olaya ilişkin hüküm kurmuştur. Kişi, veri sorumlusunun şu an kendisine ilişkin olarak hangi kişisel verileri toplamakta olduğu ve geçmişte hangi kişisel verileri uhdesinde sakladığı, ayrıca bu veriler üçüncü şahıslara ifşa edilmişse, bu üçüncü şahısların kim olduğuna yönelik hususlarda bilgilendirilmek istemiştir. Veri sorumlusu verdiği cevapta, kanunun kendisine verdiği izin çerçevesinde verileri telefon rehberi yayıncılığında kullandığını ve bu kişisel verileri pazarlama amacıyla ticari müşteriler, bilişim şirketleri, hayır kurumları, siyasi partiler gibi alıcılara sunduğunu ifade etmiş; ancak bu verilerin alıcılarının kim olduğunu isimle sayarak belirtmemiştir. ABAD yaptığı değerlendirmede öncelikle erişim hakkının sınırlarını genişleterek, geçmişte saklanan veriler hakkında da bilgilendirilme talep edilebileceğini ifade etmiştir. Buna ek olarak kişisel verilerin, geçmişte alıcılara açıklanmış olması veya halen açıklanmakta olması durumunda, veri

[292] European Data Protection Board, Right of Access, s. 45.
[293] European Data Protection Board, Right of Access, s. 46.
[294] European Data Protection Board, Right of Access, s. 41.
[295] GDPR 63 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-63/, (E.T. 15.10.2023).
[296] ABAD, 12.01.2023 tarih ve C-154/21 numaralı Österreichische Post kararı, https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-154/21, (E.T. 15.10.2023).

sorumlusunun alıcının kimliğini veri öznesine bildirmekle yükümlü olduğunu vurgulamıştır. Ancak bu yükümlülüğün, alıcıların kimliğinin belirlenmesi mümkün olmadığı veya veri öznesinden gelen bilgi ve erişim taleplerinin GDPR m. 12/5 maddesi uyarınca açıkça temelsiz veya aşırı olduğunun veri sorumlusu tarafından kanıtlandığı durumlarda, veri öznesinin yalnızca ilgili alıcı kategorileri hakkında bilgilendirilmesinde bir sakınca olmadığı ifade edilmiştir.

ABAD yakın tarihli başka bir kararında[297], üçüncü tarafların kredi notu hakkında müşterilerine bilgi sağlayan bir şirket olan veri sorumlusuna yapılan erişim talebine ilişkin olarak hüküm kurmuştur. Veri öznesi kendisine ilişkin olarak işlenen verilerin bir nüshasının verilmesini istemiş, şirket de kendisine işlenen verilerin özetlendiği bir liste temin etmiştir. Divan, yaptığı değerlendirmede öncelikle GDPR'da bir "nüsha" tanımının yer almadığına; fakat kelimenin sözlük anlamına bakıldığında "genel bir özet" değil, "orijinal materyalin aslına uygun bir şekilde çıkarılmış kopyası veya hazırlanmış dökümü" anlamına geldiğine dikkat çekmiştir. Ancak nüsha, her zaman kişisel verilerin yer aldığı orijinal belgelerin kopyası olmak zorunda değildir. İşlenen verilerin eksiksiz, aslına uygun ve anlaşılabilir bir şekilde belirtildiği herhangi bir nüsha, erişim hakkının gerekliliğinin yerine getirilmesini sağlayacaktır. Belgelerin orijinallerinin bir nüshasının verilmesi gerekliliği, şeffaflık gerektiren konularda söz konusu olabilir. Bu husus somut olayın özelliklerine bakılarak değerlendirilmelidir.

Kişisel Verileri Koruma Kurulu ise bir kararında[298], ilgili kişinin yaptığı telefon görüşmesi kayıtlarının tarafına verilmesi talebinin reddedildiği iddiasına ilişkin olarak inceleme yapmıştır. Kurul, kişinin kendisine ilişkin verilerin işlendiği hallerde, bilgilendirilme hakkının, mevzubahis veriye erişim hakkını da kapsadığını ve erişim hakkının, bilgilendirilme hakkını tamamladığını ifade etmiştir. Zira erişim hakkı, ilgili kişinin verilerinin nasıl işlendiği hususunda bilgi sahibi olmasına olanak tanımaktadır. Böylece de verileri üzerindeki haklarını kullanması kolaylaşmaktadır. Veri sorumlusu talep edilen erişimi, teknik olanakların izin verdiği ölçüde ve uygun bir şekilde sağlamalıdır. Olayda veri sorumlusu kişinin talebini "görüşmede ilgili kişiden

[297] ABAD, 04.05.2023 tarih ve C-487/21 numaralı F.F. v Österreichische Datenschutzbehörde and CRIF GmbH kararı, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021CJ0487, (E.T. 16.10.2023).

[298] Kişisel Verileri Koruma Kurulu, 14.01.2020 tarih ve 2020/13 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6698/2020-13, (E.T.17.10.2023).

başkalarının da hassas verilerinin yer alması" sebebiyle reddettiğini ifade etmişse de; Kurul, ilgili kişi ile üçüncü kişilerin menfaatleri arasında makul dengenin kurulmadığını belirtmiştir. Zira ilgili kişiye doğrudan ses kayıtlarının kayıt ortamı verilmeyip, bu kayıtların ilgili kişiyi ilgilendiren kısımlarının tam olarak anlaşılır dökümlerinin verilmesiyle de erişim hakkının gerekliliklerinin yerine getirilebileceğine işaret edilmiştir.

C. Düzeltme Hakkı

1. Düzeltme Hakkının Kapsamı ve Esasları

KVKK m. 11/1-d ile ilgili kişiye "kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme" hakkı verilmiştir. Benzer şekilde, düzeltme hakkı GDPR m. 16'da kendine yer bulmuştur. Buna göre "ilgili kişi, kendisi ile ilgili doğru olmayan kişisel verilerin düzeltilmesini" veri sorumlusundan isteyebilir. İlgili kişi, işleme amaçlarına uygun olarak eksik kişisel verilerini, gerekirse ek bir beyanla tamamlama hakkına da sahiptir.

Bu hak esasen, kişinin kendi verileri üzerindeki kontrolünün bir tezahürü olup erişim hakkının bir uzantısı olarak kullanılmaktadır[299]. Yani işlenen verilerine erişerek yanlış veya eksik olduğunu fark eden kişi, düzeltme veya tamamlama talebinde bulunabilecektir. Bu hak ayrıca, kişisel verilerin GDPR m. 5/1-d'de ve KVKK m. 4/2-b'de yer alan "doğru ve gerektiğinde güncel olma" ilkesiyle yakından ilgilidir[300]. Veri sorumlusuna ayrıca ve açıkça böyle bir yükümlülük getirilmesi, bu hakka verilen önemi göstermektedir. Yanlış veya eksik işlenen veriler, hem ilgili kişi hem de veri sorumlusu açısından olumsuz sonuçlar doğurabileceği için düzeltme taleplerinin geciktirilmeksizin yerine getirilmesi doğru olacaktır[301].

---

[299] Cécile de Terwangne, "Article 16 Right to rectification", **The EU General Data Protection Regulation (GDPR): A Commentary**, (Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler), Oxford University Press, Croydon, 2020, s. 471.

[300] Dülger, s. 486; Lloyd-Jones ve Carey, s. 139.

[301] Article 29 Data Protection Working Party, "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)", **Avrupa Komisyonu Web Sitesi**, 2017, https://ec.europa.eu/newsroom/article29/items/610178, (E.T. 16.10.2023), (EU 2016/680), s. 21.

Veri sorumlusunun işlediği verilerdeki yanlışlık birkaç şekilde gerçekleşebilir. İlgili kişi tarafından sağlanan bilgi, en başta bilerek veya bilmeyerek yanlış verilmiş olabilir. Yahut başta doğru verilmiş bilgi, sonradan durumun değişmesi ile yanlış hale gelmiş olabilir. Her halükarda veri sorumlusu tarafından verinin doğru olup olmadığının araştırılması söz konusu olamayacağı için düzeltilmesi istenen verinin yanlışlığını uygun şekilde kanıtlamak, her ne kadar haklarını kullanırken bir gerekçe göstermek zorunda olmasa da, ilgili kişiye düşmektedir[302]. Veri sorumlusu düzeltme talebini aldığında, ilgili kişi tarafından sağlanan bilgiler doğru görünüyorsa gerekli işlemi yapmalıdır.

Eksik bilgilerin tamamlanması hususunda ise, işleme amaçlarına uygun olup olmadığı değerlendirilir. Öyle ki bazı veriler, bir işleme faaliyeti için tamamken bir başkası için eksik nitelikte olabilir[303]. İşte düzeltme hakkı kapsamında yapılacak tamamlama bu noktada devreye girecektir. İlgili kişinin sağlayacağı ek beyan ile bu hakkını kullanması mümkündür. Örneğin, bir kişinin kredi çekmek için bankasına müracaat ettiğini düşünelim. Ayrıca yakın zamanda yeni bir taşınmaz da iktisap etmiş olsun. Geçmiş yıllarda yaptığı başka bir işlem kapsamında sunduğu maaş bordrosu banka kayıtlarında yer alıyorsa ve kredi başvurusunun değerlendirilmesinde kullanılacaksa, kişi malvarlığında yaşanan değişimi de belirtip kredi alma şansını yükseltmek için ek bir beyanla taşınmazın tapusunu da sunarak eksikliğin tamamlanması talebinde bulunabilir.

2. Düzeltme Usulü

Düzeltme hakkı kapsamında veri öznesi, "kendisi ile ilgili doğru olmayan kişisel verilerin **gereksiz gecikmeye mahal verilmeksizin** düzeltilmesini" talep edebilmektedir (GDPR m. 16). Düzeltme talebini alan veri sorumlusu, hemen harekete geçerek gerekli düzeltmeleri ve tamamlamaları yapmalı yahut veri öznesine bunu yapması için gerekli imkanları sağlamalıdır. Bu durumda GDPR m. 12'de yer alan kurallar da göz önünde bulundurulmalıdır. Bu hususta tüm haklar anlatıldıktan sonra, genel bir açıklama yapılacağı için bu başlık altında daha detaylı bilgi verilmeyecektir.

[302] Sanjay Sharma, **Data Privacy and GDPR Handbook**, John Wiley & Sons Inc, New Jersey, 2019, s. 203.
[303] De Terwangne, s. 473.

Bazen de düzeltme hakkının kullanılması sırasında, kişisel verilerin yanlış veya eksik olup olmadığı konusunda bazı anlaşmazlıklar yaşanabilir. Örneğin veri öznesinin, işlediği verilerin doğruluğundan ve eksiksizliğinden emin olduğu durumlarda, düzeltme talebi reddedilebilir. Böyle durumlarda veri öznelerine bu reddin gerekçesi ve redde karşı başvurabileceği hukuki yollar yazılı olarak bildirilmelidir[304]. Veri sorumlusu her ihtimale karşı, yanlış veya eksik olduğu iddia edilen verilere ek olarak, bu verilerin düzeltilmiş versiyonlarını da ayrıca ve açıkça veri öznesinin beyanı olduğunu belirterek tutabilir[305]. Ayrıca makul bir gerekçesi varsa, yanlış veri de kayıt sisteminde tutulmaya devam edilebilir. Bu durumda doğrusunun da anlaşılacak şekilde ayrıca ve açıkça belirtilmesi gerekir[306]. Örneğin, bir hastaya her ne kadar kalp hastalığı olmasa da bu yönde yanlış bir teşhis konulmuş olsun. Yıllar sonra durum fark edildiği zaman, teşhis hasta kaydından kaldırılmak yerine yanlış olduğu belirtilerek arşiv amaçlı saklanmaya devam edilebilir.

3. Düzeltme Hakkına İlişkin Örnek Kararlar

Kişisel Verileri Koruma Kurulu'na yapılan bir başvuruda[307], veri sorumlusunun daha sonraki tarihlerde ilgili kişiye sunduğu tüm hukuki belgelerde, e-posta adresinin halihazırda yazması nedeniyle bu hususdaki yanlışlığı düzeltme imkanının verilmediği iddia edilmiştir. Yapılan incelemede; mevzubahis e-posta adresinin, ilk olarak ilgili kişinin ortağı olduğu şirketin vekili tarafından bankayla paylaşıldığı, sonrasında ilgili kişinin bireysel emeklilik başvurusu sırasında kendisine sunulan formda yer alan söz konusu e-posta adresini formu imzalamak suretiyle onayladığı ve ilgili kişinin düzeltme başvurusu üzerine veri sorumlusunun hemen harekete geçerek e-posta adresinde gerekli düzeltmeyi yaptığı için veri sorumlusunun özen yükümlülüğü çerçevesinde hareket ettiği ifade edilerek bir ihlal bulunmamıştır. Fakat yanlış e-posta adresine giden bildirimlerin, olası dolandırıcılık olaylarında hesaptan para çekildiği zaman haberdar olunamamasına sebebiyet verebileceği için, veri sorumlusunun iletişim bilgilerinin belirli aralıklarla doğrulanması ve

[304] Article 29 Data Protection Working Party, EU 2016/680, s. 22.
[305] Lloyd-Jones ve Carey, s. 139.
[306] Dülger, s. 296.
[307] Kişisel Verileri Koruma Kurulu, 12.01.2023 tarih ve 2023/67 sayılı kararı, https://www.kvkk.gov.tr/Icerik/7592/2023-67, (E.T. 20.10.2023).

güncelliğinin sağlanması hususunda gerekli mekanizmaları kurması gerektiği belirtilmiştir[308].

İrlanda Veri Koruma Komisyonu da bir kararında[309], düzeltme hakkının kullanımına ilişkin detaylı bir değerlendirme yapmıştır. Veri öznesi, tedavi olduğu sağlık kuruluşuna başvurarak, adındaki İrlandacaya özgü geleneksel işaretin (síneadh fada aksanı) kullanılmadan yazıldığı için kayıtlarda adının yanlış tutulduğunu belirtmiş ve gerekli düzeltmenin yapılmasını istemiştir. Hastane ise hasta kayıt sisteminin bu yerel işareti barındırmadığı, dolayısıyla ilgili düzeltmenin yapılamayacağını bildirerek düzeltme talebini reddetmiştir. Ayrıca zaten hastalara bir numara verilerek takibinin yapıldığı ve bu nedenle de kişinin ismindeki bu yanlışlığın bir karışıklığa yol açmayacağı da veri öznesine iletilmiştir. Komisyon yaptığı incelemede, düzeltme hakkının sınırsız olmadığına ve işleme amacıyla birlikte değerlendirilmesi gerektiğine dikkat çekmiştir. Veri öznesinin adı, hastane kayıtlarında onu belirli kılan tek tanımlayıcı değildir; veri sorumlusunun belirttiği üzere, hastalara ayrıca hasta numarası verilmiştir. Bu nedenle, kişinin adındaki karakteristik işaretlerin yokluğunda da veri işleme faaliyeti amacına ulaşmış olup bu husus kişinin temel hak ve özgürlükleri üzerinde olumsuz bir etki yaratmayacaktır. Bu nedenle GDPR m. 16'ya aykırılık söz konusu değildir. Ancak Komisyon veri öznesinin hasta kaydına, kişinin adının bir parçası olan aksanın varlığını gösterecek bir not eklenmesi gerektiğini de belirtmiştir.

AİHM de bir kararında[310], etnik kökenini Roman olarak düzeltmek isteyen kişinin talebinin Moldova resmi makamları tarafından reddedilmesine ilişkin hüküm kurmuştur. Moldova toprakları, Sovyetler Birliği'nin bir parçası haline geldiğinde, Sovyet yetkilileri başvurucunun Romanya'da doğan ebeveynleri de dahil olmak üzere burada yaşayan herkesin etnik kimliğini bu şekilde kaydetmiştir. Bu nedenle de başvurucu resmi belgelerinde yer alan bu bilginin düzeltilmesi talebinde bulunmuştur. Fakat Moldova makamları kişinin talebinin yerine getirilmesini sağlayacak yeterli

[308] Bu hususta bkz. Kişisel Verileri Koruma Kurulu, 22.12.2020 tarih ve 2020/966 sayılı İlke Kararı, https://www.kvkk.gov.tr/Icerik/6858/2020-966, (E.T. 20.10.2023).

[309] Ireland Data Protection Commission, Ciarán Ó Cofaigh kararı, https://www.dataprotection.ie/index.php/en/dpc-guidance/blogs/examination-right-rectification-complaints, (E.T. 20.10.2023).

[310] AİHM, 27.04.2010 tarih ve 27138/04 başvuru numaralı Ciubotaru/Moldova kararı, https://hudoc.echr.coe.int/, (E.T. 21.10.2023).

kanıtın sunulmadığını ileri sürmüştür. AİHM kişiye bu açıdan katlanılması beklenmeyecek derecede ağır bir ispat yükü yüklendiğinden, yetkililerin ilgili kişinin etnik kökenini beyan ettiği şekilde düzeltmeyi reddetmesi nedeniyle özel yaşama saygı hakkının ihlalini saptamıştır.

D. Silme (Unutulma) Hakkı

1. Silme (Unutulma) Hakkının Kapsamı, Esasları ve Uygulanma Usulü

Kişisel verilerin neredeyse bir meta gibi kullanıldığı günümüz toplumunda, ilgili kişinin verileri üzerindeki hakimiyetini ve insan onurunu korumasını sağlayan bir diğer hak da silme (unutulma) hakkıdır. GDPR m. 17/1'e göre; "veri öznesi, kendisi ile ilgili kişisel verilerin herhangi bir gecikmeye mahal verilmeksizin silinmesini" isteme hakkına sahiptir. Buna ek olarak bazı durumların varlığı halinde veri sorumlusuna söz konusu verileri gecikmeksizin silme yükümlülüğü yüklenmiştir. Bu durumların ilki, "kişisel verilerin toplanma veya işlenme amaçlarıyla ilişkili olarak artık gerekli olmaması" halidir. Böylece kişisel bilgilerin yanlış veya güncelliğini kaybetmiş olma ihtimaline karşı silinmesine olanak sağlanmaktadır. Ayrıca veri işlemenin sınırlı ve belirli bir amaç için yapılması ilkesine de uygun davranılmaktadır[311]. Örneğin, veri öznesi iki ay önce istifa ettiği firmanın internet sitesinde, hala orada çalışıyormuş gibi görünüyor olsun. Bu durumda söz konusu bilgi, doğru ve güncel olmayacağı için firmanın bu verileri internet sitesinden gecikmeksizin kaldırma yükümlülüğü bulunmaktadır. Veri işleme amacının değiştiği durumlarda da kişiye bu hususta bilgilendirme yapılmalı, kişinin bu amaç doğrultusunda rızasının olup olmadığı araştırılmalı veya veri işlemek için yasal başka bir gerekçenin olup olmadığı araştırılmalıdır. Eğer her iki şart da gerçekleştirilemiyorsa artık verilerin silinmesi gerekmektedir[312]. İkinci olarak, veri öznesinin işleme faaliyetinin dayanağı olan rızasını geri alması ve işleme faaliyetini sürdürmeye yönelik olarak rıza dışında başka bir yasal gerekçenin bulunmaması hali de veri sorumlusuna silme yükümlülüğü yüklemektedir. Bilindiği üzere, veri işlemenin hukuki olması sağlayan koşullardan

[311] Vrabec, s. 141.
[312] Turgut, s. 212.

biri, açık rızanın varlığıdır. Kişiler, verilerinin geleceğini belirleme hakkı ve özgür iradeleri doğrultusunda, işleme faaliyeti için verdiği rızayı her zaman geri alabilir. Bu durumda, işleme faaliyetini sürdürmeye yönelik olarak rıza dışında başka bir yasal gerekçe bulunmuyorsa, söz konusu verilerin silinmesi gerekir[313]. Örneğin, bir sosyal medya platformunda hesap açarken kullanım şartlarını kabul etmiş olsun. Ancak daha sonra, kişisel verilerinin gizliliği konusundaki endişeleri nedeniyle hesabını kapatmak istesin. Eğer sosyal medya platformunun bu hesabı tutmak için başka bir yasal gerekçesi yoksa, kullanıcının verilerini silmekle yükümlüdür. Üçüncü olarak, veri öznesinin "kişisel verilerin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda" itiraz hakkını (GDPR m. 21/2) kullanması hali de veri sorumlusuna silme yükümlülüğü yüklemektedir. Örneğin kişi, bir e-ticaret sitesinin kişiselleştirilmiş öneriler ve promosyonlardan yararlanmak için site kurallarını kabul etti ve bu çerçevede kişisel verilerini paylaştı diyelim. Daha sonra itiraz hakkını kullanırsa artık veri sorumlusunun söz konusu amaçla ilgili olan her türlü veri işleme faaliyetini durdurması ve işlenen verileri de silmesi gerekmektedir. Veri öznesinin genel itiraz hakkını (GDPR m. 21/1) kullanması durumunda da, veri sorumlusunun elinde işleme faaliyetini devam ettirmeye yarayacak ağır basan meşru bir gerekçe bulunmaması halinde silme yükümlülüğü mevcuttur. Bu gerekçelerle ilgili açıklama "İtiraz Hakkı" başlığı altında daha detaylı anlatıldığı için o kısma atıf yapmakla yetinmekteyiz. Dördüncü olarak, kişisel verilerin hukuka aykırı olarak işlenmesi durumunda da silme yükümlüğü söz konusu olacaktır. Örneğin, bilgilendirme hakkının gerekleri yerine getirilmeksizin işlenen verilerin silinmesi gerekmektedir[314]. Beşinci olarak, "veri sorumlusunun tabi olduğu Birlik veya üye devlet hukukundaki bir yasal yükümlülüğe uymak amacı ile kişisel verilerin silinmesinin zorunlu olması" halinde de verilerin silinmesi gerekecektir. Bu yükümlülük doğrudan bir mevzuat hükmünden kaynaklanacağı gibi bir mahkeme kararının icrası kapsamında da doğabilir. Son olarak, kişisel verilerin çocuklara yönelik "bilgi toplumu hizmetlerinin sağlanması ile ilgili toplanmış olması"" durumu da verilerin silinmesini gerektirebilir. Şöyle ki GDPR m. 8 uyarınca, çocuğa; talebi karşılığında, çevrimiçi ortamda mesafeli olarak

[313] Turgut, s. 216.
[314] Turgut, s. 221.

ücret karşılığı bir hizmet[315] sunuluyorsa, bu esnada çocuğun en az on altı yaşında olması halinde kişisel verileri işlenebilmektedir. On altı yaşından küçük çocukların kişisel verilerinin işlenmesi için gerekli rızayı yasa temsilcisi vermelidir[316]. Eğer veri öznesi çocuk, daha sonradan söz konusu işleme faaliyetinin kendisi açısından riskli olduğunu değerlendirirse, kaç yaşında olduğuna bakılmaksızın yani hala "çocuk" sıfatını haiz olmasa bile, rızayı veren kişi kendisi olmasa bile verilerinin silinmesini isteyebilecektir[317].

Bahsedildiği üzere veri sorumlusunun silmekle yükümlü olduğu veriler ayrıca alenileştirilmişse, bu durumda silme talebi, söz konusu verileri işleyen diğer veri sorumlularına da bildirilmek zorundadır. Veriler, diğer veri sorumlularına bağlantı sağlama, nüsha iletme veya çoğaltma yöntemleriyle sağlanmış olabilir. Bu yükümlülüğün yerine getirilmesi için mevcut teknoloji ve uygulama maliyeti göz önünde bulundurularak teknik tedbirler de dahil olmak üzere makul adımlar atılmalıdır (GDPR m. 17/2).

Silme (unutulma) hakkı, mutlak bir hak değildir. İşleme faaliyetinin şu sebeplerle yapılması durumunda, verilerin silinmesi talep edilemeyecek ve veri sorumlusunun silme yükümlülüğü doğmayacaktır: İfade özgürlüğü ve bilgi edinme hakkının kullanılması, veri sorumlusunun AB veya üye devlet hukukundaki bir yasal yükümlülüğe uymak amacıyla yapılması, kamu yararına gerçekleştirilen bir görevin ifası, veri sorumlusuna verilen resmi bir yetkinin uygulanması, kamu sağlığının korunması, kamu yararına arşivleme, bilimsel veya tarihi araştırma ya da istatistiki amaçların bulunması, birtakım hukuki iddiaların ileri sürülmesi ve bunların uygulanması veya savunulması[318], silmenin veri işleme amaçlarına ulaşılmasını imkansız hale getirmesi veya ciddi şekilde zarar vermesinin muhtemel olması (GDPR

[315] Bu tip hizmetlere "bilgi toplumu hizmeti" denilmektedir. Tanım için lütfen bkz. 17.09.2015 tarihli Avrupa Birliği Resmi Gazetesi'nde yayınlanan 2015/1535 Sayılı Direktif, **Avrupa Birliği Resmi Gazetesi**, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2015:241:FULL&from=EN, (E.T. 28.12.2023).

[316] Bu hususta detaylı açıklamalar için lütfen "İlgili Kişi" başlığı altında yer alan açıklamalara bakınız.

[317] GDPR Gerekçe 65, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-65/, (E.T. 28.12.2023).

[318] Bu konuda bkz. İrlanda Veri Koruma Komisyonu, 14.09.2023 tarihli Airbnb Ireland kararı, https://www.dataprotection.ie/sites/default/files/uploads/2023-10/20231012%20Full%20decision%20Airbnb%20September%202023.pdf, (E.T. 01.01.2024). Söz konusu kararda, veri sorumlusu olan Airbnb'ye başvurarak kendisi hakkında ellerinde bulundurdukları tüm kişisel verilerin silinmesini isteyen veri öznesinin talebinin; misafir olarak kalan üçüncü bir şahsa saldırdığı ve bu hususta bir cezai soruşturma yürütüldüğü gerekçesiyle reddi GDPR'ye aykırılık teşkil etmemiştir.

m. 17/3). Bu durumlardan herhangi birinin varlığı halinde, artık söz konusu kişisel verilerin silinmesi mümkün değildir. Örneğin, kamuoyunu bilgilendirme amacı taşıyan gazetecilik amacı ile bilim ve sanatın gelişmesini sağlama amacı taşıyan "akademik, sanatsal veya edebi anlatım amaçları doğrultusunda" yapılan veri işleme faaliyetleri, ifade özgürlüğü ve bilgi edinme hakkı kapsamında olduğu kabul edildiğinden (GDPR m. 85), bu hallerde silme hakkının kullanılamayacağı kabul edilmelidir. Gazeteciliğin kapsamı da geniş yorumlanmalı; sadece sosyal medya üzerinden yayınlanan haber gönderileri, bloglar gibi diğer dijital kaynaklar da bu kapsama dahil edilmelidir. Her durumun somut koşullarına göre değerlendirilerek kişisel verilerin korunması hakkı özelinde silme hakkı ile bilgi alma hakkı arasında makul bir denge kurulması son derece önemlidir[319]. Başka bir istisna örneği olarak da arşivleme amaçlı veri işleme faaliyetleri gösterilebilir[320]. Geçmişteki totaliter devletlerdeki siyasi davranışlar, soykırım veya savaş suçları gibi insanlığa karşı suçlara ilişkin spesifik bilgiler sağlanması amacıyla arşivlemeye izin verilmekte ve bu verilerin silinmesi mümkün olmamaktadır[321].

KVKK'de ise m. 11/1-e ile ilgili kişilere "kişisel verilerin silinmesini veya yok edilmesini isteme" hakkı verilmiştir. Bu hak, kanunun "Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi" başlıklı 7. maddesinde öngörülen şartlar çerçevesinde kullanılabilecektir. Buna göre, "hukuka uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler

[319] Örneğin AİHM bir kararında, Monako Prensesi Caroline Von Hannover'in tahttaki babası Prens Rainier'in bir kayak tatili sırasında görüntülenmesi ve sağlık sorunlarına ilişkin bir fotoğraf hakkında, özel hayatın gizliliği hakkının ihlal edilmediğine hükmetmiştir. Zira prensin konumu nedeniyle kamuoyunun sağlığı hakkında bilgi almaya hakkı vardı. Bu nedenle kişisel verilerin korunması hakkı ile basının düşünceyi açıklama ve yayma özgürlüğü arasında özenli bir denge sağlanması gerekmiştir (AİHM, 07.02.2012 tarih ve 40660/08 ve 60641/08 başvuru numaralı Von Hannover/Almanya (2) kararı, https://hudoc.echr.coe.int/, (E.T. 28.12.2023)).

[320] Arşivleme amaçlı veri işleme faaliyetlerinin silme hakkının istisnasını oluşturduğuna ilişkin karar örneği için lütfen bkz. Avusturya Veri Koruma Otoritesi, 22.01.2021 tarih ve DSB-D124.1177/0006-DSB/2019 numaralı kararı, https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=ade5bfc2-3a92-44cc-90b6-36c9132c2332&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20210122_DSB_D124_1177_0006_DSB_2019_00, (E.T. 29.12.2023).

[321] GDPR 158 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-158/, (E.T. 28.12.2023); Tamer Soysal, "Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi", **Uyuşmazlık Mahkemesi Dergisi**, Sayı: 13, 2019, s. 405.

resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir". Dikkat edileceği üzere, düzenlemeyle hem ilgili kişiye silme başvurusunda bulunma hakkı tanınmış hem de başvuruya gerek olmaksızın veri sorumlusuna silme yükümlülüğü verilmiştir. Kişisel Verileri Koruma Kurumu'na göre veri işlemeyi gerektiren sebeplerin ortadan kalktığı haller şunlardır:

> *Kişisel verileri işlemeye esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası; taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi; kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması; kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olduğunun tespit edilmesi; kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği haller; ilgili kişinin rızasını geri alması; ilgili kişinin KVKK m. 11/1-e,f'deki hakları çerçevesinde kişisel verileri işleme faaliyetine ilişkin yaptığı başvurunun veri sorumlusu tarafından kabul edilmesi; veri sorumlusunun, ilgili kişi tarafından kişisel verilerinin silinmesi veya yok edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde Kurula şikayette bulunulması ve bu talebin Kurul tarafından uygun bulunması; kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması; KVKK'nin 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması*[322].

Yukarıda sayılan hallerin varlığında, söz konusu verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekmektedir. Bu işlemlere ilişkin usul ve esaslar "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" ile düzenlenmiştir[323]. Öncelikle, kişisel verilerin silinmesi ile kastedilenin "verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi" olduğunu belirtmek gerekmektedir (Yön. m. 8/1). Yok edilme işlemi ise "kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi" anlamına gelmektedir (Yön. m. 9/1). Anonim hale getirme ise, "kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi" ile olmaktadır (Yön. m. 10/1). Veri sorumlusu, kişisel verilerin silinmesi, yok edilmesi ve anonimleştirilmesini tanımlardaki

[322] Kişisel Verileri Koruma Kurumu, Rehber, ss. 83, 84.

[323] 28.10.2017 tarihli Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, **Resmi Gazete**, https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm, (E.T. 28.12.2023).

anlamıyla sağlamak için "gerekli her türlü teknik ve idari tedbirleri almakla yükümlü" kılınmıştır.

Veri sorumlusunun silme, yok etme veya anonimleştirme yükümlülüğünü resen yerine getirmesi gereken durumlarda, eğer saklama ve imha politikası hazırlamakla da yükümlüyse; artık "silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde" yerine getirmelidir (Yön. m. 11/1). "Periyodik imhanın gerçekleştirileceği zaman aralığı, veri sorumlusu tarafından kişisel veri saklama ve imha politikasında belirlenir. Bu süre her halde altı ayı geçemez" (Yön. m. 11/2). Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumluları ise "silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde bu yükümlülüğünü resen yerine getirmelidir" (Yön. m. 11/3).

İlgili kişinin silme veya yok etme talebinde bulunduğu durumlarda ise, işleme şartlarının tamamının ortadan kalkması halinde silme işleminin yapılması gerekmektedir. "Veri sorumlusu, verilerin ilişkin olduğu kişinin talebini en geç otuz gün içinde sonuçlandırır ve kişiye bilgi verir". Ayrıca söz konusu veriler, "üçüncü kişilere aktarılmışsa durum üçüncü kişilere bildirir ve gerekli işlemlerin yapılmasını temin eder". Ancak işleme şartlarının tamamı ortadan kalkmamışsa, silme veya yok etme talebi "gerekçesi açıklanarak reddedilebilir". Bu durumda "ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda" bildirilmelidir (Yön. m. 12).

"Kişisel verilerin silinmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır" (Yön. m. 7/3). "Veri sorumlusu, kişisel verilerin silinmesi işlemiyle ilgili uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklamakla yükümlüdür" (Yön. m. 7/4). Veri sorumlusu, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer". İlgili kişinin talebi halinde yaptığı seçimin gerekçesini açıklamalıdır (Yön. m. 7/5).

KVKK m. 7/2 uyarınca, "kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümler"in saklı tutulması öngörülmüştür. Örneğin, Polis Vazife ve Salahiyetleri Kanunu kapsamında

şüphelilerin parmak izlerinin alınması veya Adli Sicil Kanunu kapsamında kişilerin aldığı cezaları gösteren adli sicil kaydı tutulması durumlarında KVKK uygulanmayacaktır[324].

2. Silme (Unutulma) Hakkına İlişkin Örnek Kararlar

Silme (unutulma) hakkına ilişkin belki de en önemli karar, ABAD'ın hükme bağladığı Google İspanya davasıdır[325]. Başvuru sahibi avukat, bir arama motoru olan Google'da kendi adını arattığında, hakkında birtakım mali zorluklar yaşadığına dair güncelliğini yitirmiş bilgilerin çıktığını görmüş ve haberlerin arama listesi sonuçlarından silinmesini talep etmiştir. Fakat Google söz konusu bilgileri sağlayanın kendisi olmadığını, kendilerinin bu olaya bilgilerin bulunduğu orijinal sayfalara link aracılığıyla yönlendirme yapmak dışında bir dahlinin bulunmadığını, dolayısıyla da silme talebinin söz konusu haberleri yapan gazetenin kendisine yapılması gerektiğini belirterek silme talebini yerine getirmemiştir. ABAD ise Google'ın arama sonucu sağlamak için söz konusu içerikleri, kendisine ait dizine eklemesiyle veri işleme faaliyeti gerçekleştiğini ve bir veri sorumlusu haline geldiğini kabul etmiştir. Zira kişisel veri sağlayan internet arama motoru sonuçları da bir kişi hakkında detaylı bir profil sunabilmektedir. Kamuoyunun bilgi alma hakkı elbette önemlidir ancak kişisel verilerin doğru ve güncel tutulması da gerekmektedir. Bu nedenle her iki hak arasında hassas bir denge gözetilmelidir. Kişiyle ilgili yanlış, eksik, abartılı, alakasız ve güncel olmayan verilerin silinmesini istemek, kişisel verilerin korunması hakkının doğal bir sonucudur.

İtalya Veri Koruma Otoritesi (Garante per la protezione dei dati personali) önüne gelen bir başvuruda[326], Eleven Sports uygulaması aracılığıyla spor müsabakalarının televizyon yayın hizmetlerini sağlayan veri sorumlusu şirket nezdinde aylık bir abonelik başlatan veri sorumlusunun silme talebiyle ilgili bir karar

---

[324] Turgut, s. 196.

[325] ABAD, 13.05.2014 tarih ve C-131/12 numaralı Google Spain SL ve Google Inc. v Agencia Española de Protección de Datos (AEPD) ve Mario Costeja González kararı, https://curia.europa.eu/juris/liste.jsf?num=C-131/12, (E.T. 30.12.2023).

[326] İtalya Veri Koruma Otoritesi (Garante per la protezione dei dati personali), 15.09.2022 tarih ve 9819285 sayılı kararı, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9819285, (E.T. 01.01.2024).

vermiştir. Ancak verilerinin silinmesini talep ettikten ve veri sorumlusunun haber bültenini alma iznini geri çektikten sonra da çok sayıda istenmeyen e-posta almaya devam etmesi üzerine şikayette bulunmuştur. Veri sorumlusu şikayete karşı yaptığı savunmada; veri öznesinin farklı e-posta adreslerine bağlı aylık ve sezonluk iki ayrı aboneliği olduğunu ve sezonluk olanın devam ettiğini, aylık aboneliğin bitmesi üzerine hala sezonluk aboneliğe bağlı e-posta adresiyle kişisel verilerinin silinmesinin talep edildiğini, ayrıca iki hesapla da ilişkili olmayan üçüncü bir e-posta adresinden yazarak başka taleplerde bulunulduğunu ve bu taleplerin bölük pörçük halde, listelenmeden kendilerine iletildiğini, bu durumun da yapılan işlemleri yavaşlattığı ve karmaşıklaştırdığını öne sürmüştür. İtalya Veri Koruma Otoritesi, veri öznesine ilişkin verilerin, veri sorumlusunun sözleşmeden doğan yükümlülüklerini yerine getirmesi için gerekli olduğunu dikkate alarak silme talebinin yerine getirilmesinin şu anda mümkün olmadığına ve GDPR m. 17/3'e aykırılık teşkil etmediğine karar vermiştir[327].

Belçika Veri Koruma Otoritesi (Gegevensbeschermingsautoriteit) bir kararında[328], veri öznesinin işi için kullandığı arabasının kişiselleştirilmiş plakasına ilişkin olarak silme hakkının istisnasıyla ilgili bir hüküm kurmuştur. Veri öznesinin kullandığı kişiselleştirilmiş plaka, Türk futbol takımı olan Galatasaray'a gönderme yapan ibareler içeriyordu. Veri sorumlusu olan bir televizyon programı yapımcısı, dizisinin bazı sahnelerinde, kurgusal bir suç örgütünde yer alan dizi karakterine, veri öznesinin aracına model olarak çok benzeyen ve aynı kişiselleştirilmiş plakayı taşıyan bir araç kullandırmıştır. Veri öznesi, dizideki kurgusal suç örgütüyle ilişkilendirilebileceği nedeniyle kendisine ait bu plakanın diziden kaldırılmasını (silinmesini) talep etmiştir. Fakat arabanın modeli ve plakasının sanatsal bir ifade oluşturduğuna, Galatasaray'ın bilinen bir futbol kulübü olması nedeniyle tesadüfen böyle bir plakanın seçilmiş olabileceğine kanaat getirilerek GDPR'ye aykırılık olmadığına hükmedilmiştir. Yani plakanın kullanılması, sanatsal anlatım amacı

[327] Benzer şekilde İspanya Veri Koruma Kurumu da verilerin beş yıl süreyle saklanmasını öngören bir kanun hükmünün varlığı nedeniyle silme talebinin yerine getirilmesinin GDPR'yi ihlal etmediğine karar vermiştir (İspanya Veri Koruma Kurumu, 28.02.2022 tarih ve CDP/IMI/LSA/17/2022 sayılı kararı, https://edpb.europa.eu/system/files/2022-09/mt_2022-03_decisionpublic.pdf, (E.T. 01.01.2024)).

[328] Belçika Veri Koruma Otoritesi (Gegevensbeschermingsautoriteit), 21.12.2022 tarih ve DOS-2022-00944 188/2022 sayılı kararı, https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-188-2022.pdf, (E.T. 01.01.2024).

doğrultusunda yapılan bir veri işleme faaliyetleri olarak değerlendirilmiş ve ifade özgürlüğü kapsamında olduğu kabul edildiğinden (GDPR m. 85), silme hakkının kullanılamayacağı kabul edilmiştir.

Fransa'nın veri koruma otoritesi olan Ulusal Bilişim ve Özgürlükler Komisyonu (CNIL) tarafından işleme faaliyetine verilen rızanın geri çekilmesi halinde silme hakkının kullanılmasına ilişkin bir karar verilmiştir[329]. Başvuru konusu olaya göre, veri sorumlusu ve çevrimiçi reklamcılık şirketi Criteo, çerezler aracılığıyla kişisel veri toplamaktadır ve her veri öznesinin arama geçmişleriyle en alakalı reklamları belirlemek amacıyla analiz yapmaktadır. Durumu fark eden veri özneleri, veri işleme faaliyetlerine verdikleri rızalarını geri aldığında veya verilerinin silinmesini talep ettiğinde, veri sorumlusu her ne kadar kişiselleştirilmiş reklamlar göstermeyi bırakmışsa da veri öznelerine atanan tanımlayıcıyı kaldırmamış veya geçmişteki tarama etkinliklerine ilişkin bilgileri silmemiştir. Bu nedenle CNIL tarafından GDPR m. 17/1 uyarınca ihlal tespit edilmiştir.

Finlandiya Veri Koruma Komisyonu önüne gelen bir başvuruda[330], bir bankayla müşterilik ilişkisini sona erdiren veri öznesinin kendisine ilişkin verilerin silinmesine yönelik isteminin reddedilmesi değerlendirilmiştir. Öyle ki artık kişisel verileri, toplanma veya işlenme amaçlarıyla ilişkili olarak artık banka açısından gerekli değildir. Fakat banka ile veri sorumlusu müşteri arasında akdedilmiş olan yatırım hizmeti sözleşmesinin feshinin manuel olarak yapılması gerektiğinden, bu işlem insan hatası nedeniyle gerçekleştirilememiş ve bu nedenle de talep yerine getirilemediği ileri sürülmüştür. Komisyon yine de, verilerin saklanmasına artık gerek kalmadığı ölçüde silme talebinin yerine getirilmesi gerektiğinden bahisle GDPR'nin ihlal edildiğine karar vermiştir.

Anayasa Mahkemesi de önüne gelen bir bireysel başvuru dosyasında[331], hakkında ulusal bir gazetenin internet arşivinde, uzun yıllar önce uyuşturucu kullandığı için adli para cezasına çarptırıldığına ilişkin haberlerin kaldırılmasını isteyen bir kişi hakkında karar vermiştir. Söz konusu olayda; silinmesi istenen

---

329 CNIL, 15.06.2023 tarih ve SAN-2023-009 sayılı Criteo kararı, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000047707063, (E.T. 02.01.2024).

330 Finlandiya Veri Koruma Komisyonu, 20.07.2022 tarih ve 7587/163/20 sayılı kararı, https://finlex.fi/fi/viranomaiset/tsv/2022/20221524, (E.T. 02.01.2024).

331 Anayasa Mahkemesi, 03.03.2016 tarih ve 2013/5653 başvuru numaralı N.B.B. kararı, https://www.anayasa.gov.tr/tr/kararlar-bilgi-bankasi/, (E.T. 28.12.2023).

haberlerin güncelliğini yitirdiği, artık haber değerinin bulunmadığı, gündemde kalmasında bir kamu yararı kalmadığı ve bu nedenle ilgili kişinin özel hayatına yönelik incitici ve örseleyici bir mahiyet taşıdığı gerekçesiyle yerel sulh ceza mahkemesince talep haklı bulunmuştur. Ancak daha sonra söz konusu karar itiraz sonucu kaldırılmış ve haberler silinmemiştir. Anayasa Mahkemesi başvuru özelinde, şeref ve itibarın korunması hakkı ile unutulma hakkına karşı, ifade ve basın özgürlükleri ile kişilerin haber ve fikirlere ulaşma özgürlüğü arasında adil bir denge kurulması gerektiğini belirtmiştir. Başvuru tarihinde mevzubahis haberlerin yaklaşık on dört yıl öncesine ilişkindir ve güncelliğini yitirmiştir. İstatistiki ve bilimsel sebeplerle de bu bilgilerin ulaşılır olması gerekmemektedir. Ayrıca verilerin sahibi olan başvurucu, siyasi veya medyatik bir kişi de değildir. Bu nedenle söz konusu haberler başvurucunun itibarını zedelemektedir ve unutulma hakkı kapsamında değerlendirilmelidir.

Benzer şekilde Yargıtay Hukuk Genel Kurulu da unutulma hakkına ilişkin bir karar vermiştir[332]. Cinsel saldırı suçuyla ilgili yapılan bir ceza yargılamasında mağdur sıfatıyla yer alan kişinin ismi, Yargıtay kararlarının değerlendirildiği bilimsel bir eserde, baş harflerine indirgenerek kısaltılmadan veya takma isim kullanılmadan yer almıştır. Davacı, bu meselenin kişilik haklarına saldırı teşkil ettiğini ve unutulma hakkının ihlali olduğunu belirterek manevi tazminat talebinde bulunmuştur. Kararda unutulma hakkı "Üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanılan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlemesini isteme hakkıdır." şeklinde tanımlanmıştır. Yüksek mahkeme, söz konusu kitabın toplumun her kesimi tarafından yaygın yararlanılan bir eser olmadığı ve sadece ceza hukukuyla ilgilenen profesyonellerce okunduğuna yönelik savunmalara karşın; açıkça tarafların isimlerinin belirtilmesinin eser içeriğine bir fayda sağlamadığını, olayın hassasiyeti ve Türk toplumunun yapısı göz önünde alınarak bu mahiyette bir olayla davacının adının açıkça anılmasının davacının kişilik haklarını zedelediğini belirterek davanın kabulüne

[332] Yargıtay Hukuk Genel Kurulu, 17.06.2015 tarih ve E. 2014/56, K. 2015/1679 kararı, https://kararara ma.yargitay.gov.tr/, (E.T. 27.12.2023). Ayrıca benzer mahiyette kararlar için lütfen bkz. Yargıtay Ceza Genel Kurulu, 30.10.2018 tarih ve E. 2016/18-1169, K. 2018/490; Yargıtay 19. Ceza Dairesi, 05.06.2017 tarih ve E. 2016/15510, K. 2017/5325; Yargıtay 19. Ceza Dairesi, 19.10.2020 tarih ve E. 2019/28149, K. 2020/13099 kararı, https://kararara ma.yargitay.gov.tr/, (E.T. 27.12.2023).

karar vermiştir. Kararda bilim ve sanat özgürlüğü ile unutulma hakkı arasında hassas bir denge sağlanmıştır.

Kişisel Verileri Koruma Kurulu'nun unutulma hakkının kullanılmasına yönelik verdiği karardan da özellikle bahsetmek gerekmektedir. Öncelikle unutulma hakkının; Anayasa m. 20/3, KVKK m. 4, 7, 11 ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği m. 8'de yer alan hükümlerle iç hukukumuzda karşılık bulduğu ve bu nedenle ayrı bir hak olarak tanımlanmasına gerek olmadığı ifade edilmiştir. Unutulma hakkını sağlamaya yönelik olarak veri işleme faaliyetinin durdurulması, silme, yok etme veya anonim hale getirme ile indeksten (dizinden/listeden) çıkarma işleminden somut olaya göre en uygun olan araca karar verilebilecektir[333]. İlgili kişilerin adı ve soyadı ile arama motorları üzerinden yapılan aramalarda çıkan sonuçların indeksten çıkarılmasına ilişkin değerlendirmede dikkate alınacak ve her somut olay üzerinde incelenecek kriterler şunlar olarak belirlenmiştir: İlgili kişinin kamusal yaşamda önemli bir rol oynayıp oynamadığı, çocuk olup olmadığı, bilgilerin doğru ve güncel olup olmadığı, kişinin çalışma hayatı ile ilgili olup olmadığı, ilgili kişi hakkında hakaret, onur kırıcı, iftira niteliğine sahip olup olmadığı, önyargıya yol açıp açmayacağı, özel nitelikli kişisel veri niteliği taşıyıp taşımadığı, ilgili kişi için riskli olup olmadığı, verilerin sahibi tarafından mı alenileştirildiği, verilerin gazetecilik faaliyeti kapsamında mı işlendiği, verilerin yasal zorunluluk sebebiyle mi yayınlandığı, verilerin ceza gerektiren bir suçla ilgili olup olmadığı[334].

Bu bağlamda Kurul önüne gelen bir başvuruda[335], öğretim üyesi olarak çalışan ilgili kişinin çalıştığı kurumda açılan akademik kadroya bir aile yakınının alınması sebebiyle usulsüzlük yapıldığına dair haberlerin listeden kaldırılması istenmiştir. Ancak usulsüzlük iddiaları hakkında üniversite gerçekten de soruşturma açmıştır. Haberler kişinin özel değil, iş hayatıyla ilgilidir ve gazetecilik faaliyeti kapsamında kalmaktadır. Özel nitelikli bir veri söz konusu değildir. Haberler güncel olup kişi için

[333] Kişisel Verileri Koruma Kurulu, 23.06.2020 tarih ve 2020/481 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6776/2020-481, (E.T. 03.01.2024).

[334] Kişisel Verileri Koruma Kurumu, **Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi**, KVKK Yayınları No: 34, Ankara, 2021, (Unutulma Hakkı), s. 26.

[335] Kişisel Verileri Koruma Kurulu, 08.12.2020 tarih ve 2020/927 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6871/2020-927, (E.T. 03.01.2024).

bir risk doğurmamaktadır. Bilgilerin kanıtlanabilir bir önyargı oluşturma durumu yoktur. Mevzubahis kriterleri taşımadığı için kişinin talebi yerine getirilmemiştir.

Kişisel Verileri Koruma Kurulu silme hakkına ilişkin bir kararında[336], ilgili kişinin bir internet sitesinde yer alan ve daha önce kullandığı ancak şu anda kullanmadığı adres bilgilerinin silinmesini talebinin reddine yönelik bir hüküm kurmuştur. Veri sorumlusu şirketin savunmasında; fatura adreslerinin silinemeyeceği, 213 sayılı Vergi Usul Kanunu uyarınca bu bilgilerin beş yıl saklanması gerektiği, tarafların yükümlülüklerini karşılıklı olarak yerine getirdiğine yönelik bir kanıt olarak tutulması gerektiği, bu hususa ilişkin gelecekteki on yıllık zamanaşımı süresince TBK uyarınca doğabilecek anlaşmazlıkların çözümünde delil olarak kullanılabileceği gibi gerekçeler ileri sürmüştür. Kurul yaptığı incelemede, fatura belgelerinin veri sorumlusunun TBK'den kaynaklanan yükümlülükleri kapsamında on yıl saklanabileceği; ancak kişisel verilerin "doğru ve gerektiğinde güncel olma" ilkesinin yerine getirilebilmesi, bu kapsamda kişisel verilerin güncellenmesine/imha edilmesine ve güncel olmayan kişisel verilerin ilgili kişilere gösterilmemesine imkân sağlayacak kanalların oluşturulması ile imha edilen/edilmesi istenen kişisel verilerin saklama amacı dışında kullanılmamasına ilişkin gerekli tedbirlerin alınmasının lazım geldiği değerlendirmesinde bulunmuştur.

Kurul verdiği başka bir kararda ise[337], ilgili kişi ile veri sorumlusunun aralarındaki iş akdinin sonlanmasından sonra, veri sorumlusunun sosyal medya hesabından ilgili kişiye ait herkese açık şekilde paylaştığı fotoğraflarının silinmesi talebiyle ilgili değerlendirme yapmıştır. Anlaşılacağı üzere ilgili kişi, fotoğraflarının yayınlanması konusundaki açık rızasını geri almıştır. Bu nedenle veri işleme faaliyetinin yasal bir dayanağı kalmamış olup KVKK m. 12/1 kapsamında gerekli teknik ve idari tedbirleri almadığı kanaatine varılması nedeniyle, veri sorumlusu hakkında hem idari para cezası uygulanmış hem de Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümleri uyarınca fotoğrafların uygun usulle silinmesi/yok edilmesi hususunda veri sorumlusu talimatlandırılmıştır.

---

[336] Kişisel Verileri Koruma Kurulu, 26.08.2021 tarih ve 2021/847 sayılı kararı, https://www.kvkk.gov.tr/Icerik/7140/2021-847, (E.T. 03.01.2024).

[337] Kişisel Verileri Koruma Kurulu, 27.04.2021 tarih ve 2021/422 sayılı kararı, https://www.kvkk.gov.tr/Icerik/7110/2021-422, (E.T. 03.01.2024).

E. İşleme Faaliyetini Kısıtlama Hakkı

İşleme faaliyetini kısıtlama hakkı; veri öznesinin düzeltme, silme ve itiraz haklarıyla yakından ilgili bir hak olup GDPR m. 18'de düzenlenmiştir. Veri sorumlusunun işleme faaliyetine devam etmekten kaynaklanan menfaatleri ile veri öznesinin silme hakkını kullanmasıyla elde edeceği menfaatleri arasında bir denge kurulmasını sağlar[338]. Ayrıca belirtilen haklara ilişkin taleplerin yerine getirilmesi sırasında, hukuka aykırı olabilecek işlemlerin önüne geçilmesine yarar[339]. Veri öznesi, belirli durumlarda veri sorumlusuna başvurarak verilerinin işlenmesinin kısıtlanmasını talep edebilir.

Bu durumlardan ilki; veri öznesinin, verilerinin doğruluğuna itiraz etmesi ve veri sorumlusuna kişisel verilerinin doğruluğunu teyit etmesi için vereceği süre boyunca kısıtlamadır (GDPR m. 18/1-a). Örneğin, bir kişinin eskiden olduğu bir tedavinin kayıtlarına erişme talebinde bulunduğunu ve kendisine sağlanan kayıtları incelediğinde hasta dosyasında yer alan bir bilginin yanlış olduğunu düşündüğünü varsayalım. Bu nedenle hastaneye itirazda bulunur ve düzeltilmesini ister. Hastane, bu talebi değerlendirip ve verilerin doğru olup olmadığını teyit ederken, veri öznesi de bu süreçte hasta kaydına ilişkin işleme faaliyeti yapılmamasını isteyebilir. İtiraz edilen verilerin doğruluğu teyit edilir edilmez, öncesinde veri öznesine bilgi verilerek kısıtlama kaldırılmalıdır (GDPR m.18/3).

İkinci durum; işleme faaliyetinin hukuka aykırı olmasına rağmen, veri öznesinin silme hakkı yerine işleme faaliyetini kısıtlamayı tercih etmesidir (GDPR m. 18/1-b). Örneğin, bir e-ticaret sitesine olan üye kaydını silen kişinin, hala bu siteden e-posta yoluyla indirim haberlerini içeren iletiler almaya devam ettiğini fark etmiş olsun. Böylece kişisel verisi olan e-posta adresinin hukuka aykırı şekilde hala işlendiğini görecektir. Veri öznesi bu durumda söz konusu verinin silinmesi yerine kullanılmasının kısıtlanmasını isteyebilecektir.

Üçüncü durum; her ne kadar veri sorumlusunun bu verileri işlemeye ihtiyacı olmasa da, veri öznesinin birtakım hukuki iddialarını ileri sürmek, uygulamak ya da

---

[338] Sharma, s. 214.

[339] Gloria González Fuster, "Article 18. Right to restriction of processing", **The EU General Data Protection Regulation (GDPR): A Commentary**, (Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler), Oxford University Press, Croydon, 2020, (Article 18), s. 486.

savunmak amacıyla bu verilere ihtiyaç duyması halinde kısıtlamadır. Bu durum daha iyi anlaşılabilmesi için şöyle bir örnekle açıklanabilir: Kişinin kullandığı telefon operatörü, gizlilik politikaları kapsamında yaptığı bir değişiklikle artık arama kayıtlarını üç aydan uzun süre saklamayacağını bildirmiş olsun. Bu sırada veri öznesi de telefonda birine dört ay önce hakaret ettiği gerekçesiyle yargılanıyor olsun. Artık bu durumda veri öznesi, kendisine isnat edilen suçu işlemediğini kanıtlamak için dört ay öncesinin arama kayıtlarının saklanmasını fakat bunun başka bir amaçla işlenmemesini talep edebilir. Veri öznesinin artık bu verilerin saklanmasına ihtiyacının kalmadığını belirtmesi üzerine, veri sorumlusu kısıtlamayı kaldırmalıdır. Ancak öncesinde veri öznesine bu hususta bilgi vermesi gerekmektedir (GDPR m.18/3).

Dördüncü durum ise; profilleme de dahil verilerin otomatik olarak işlendiği hallerde, veri sorumlusunun mu yoksa sahibinin mi meşru gerekçelerinin ağır bastığına karar verilene kadar uygulanacak kısıtlamadır. Örneğin, otuz yaşında bir kadının kullandığı sosyal medya platformunda sürekli bebek ürünleri veya hamilelik kıyafetlerinin reklamını gördüğünü düşünelim. Üstelik kişi, bu ürünlerle ilgili hiçbir arama yapmamış olsun. Veri öznesi bu durumda, sırf belirli yaşta bir kadın olduğu için algoritma tarafından bu reklamların gösterildiğini iddia ederek itirazda bulunabilir. Platform bu iddiaların aslı olup olmadığını araştırırken kişinin verilerinin işlenmesi kısıtlanabilir. Eğer iddia doğruysa, bu durumda veri öznesi cinsiyetçi bir uygulamaya maruz kaldığı için meşru gerekçesi ağır basacaktır. Ancak veri sorumlusunun meşru gerekçesinin ağır basması durumunda, öncesinde veri öznesine bilgi verilmek şartıyla söz konusu kısıtlama kaldırılmalıdır (GDPR m.18/3).

Kural olarak kısıtlama uygulandıktan sonra, veri öznesine ilişkin olarak veri işlenmez. Ancak bu durumun istisnaları mevcuttur: Veri öznesinin rıza göstermesi, veri öznesinin hukuki iddialarını ileri sürmek, uygulamak ya da savunmak amacıyla bu verilere ihtiyaç duyması, başka bir kişinin temel hak ve özgürlüklerinin korunması, AB veya bir üye devletin önemli kamu yararı (GDPR m.18/2).

İşlemenin kısıtlanmasında; söz konusu verilerin geçici olarak başka bir veri işleme sistemine aktarılması, kullanıcılar tarafından erişilemez hale getirilmesini veya bir internet sitesinde yayınlanmışsa ilgili sayfadan geçici olarak kaldırılması gibi yöntemler izlenebilir. Eğer veri, bir otomatik kayıt sistemi içerisinde işleniyorsa, kısıtlama teknik araçlarla sağlanmalıdır. İşlemesinin kısıtlandığı, sistemde açıkça

görülebilir ve anlaşılabilir bir şekilde belirtilmelidir[340]. Veri sorumlusu ayrıca kısıtlama işlemini GDPR m. 19/2 gereğince alıcılara bildirmek zorundadır.

KVKK'de ise bu hak açıkça düzenlenmemiştir. Ancak kanunun bazı maddelerinden ve hukukun genel ilkelerinden yola çıkılarak, ilgili kişinin işleme faaliyetinin kısıtlanmasını isteyebileceği sonucuna varılabilir[341]. Örneğin, kişisel verilerin açık rıza olmaksızın işlenemeyeceği göz önüne alındığında, veri sorumlusu tarafından söz konusu rıza olmaksızın hukuka aykırı bir işleme faaliyeti yapılıyorsa ve ilgili kişinin bu duruma itiraz etmesi sonucu rızanın varlığının araştırılıyorsa; bu esnada, işlemenin dürüstlük kuralına uygun olması ilkesi (KVKK m. 4/2-a) gereği, söz konusu verilerin işlenmesinin kısıtlanması gerektiği kanaatindeyiz. Ancak elbette bu hakka sadece yorumla ulaşılmaması gerektiğini, bunun kanunilik ilkesine aykırı olacağını ve en kısa sürede GDPR'dekine benzer bir hükmün KVKK'ye eklenmesi gerektiğini de belirtmek gerekmektedir.

F. İşlemlerin Üçüncü Kişilere Bildirilmesini İsteme Hakkı

KVKK m. 11/1-f'ye göre, ilgili kişi kendisine ilişkin verilerin düzeltilmesini, silinmesini veya yok edilmesini sağladıktan sonra, "bu işlemlerin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme" hakkına da sahiptir. GDPR'de bu hak ayrıca düzenlenmemiş olup veri sorumlusuna bir yükümlülük olarak verilmekle yetinilmiştir. Düzenleme uyarınca veri sorumlusu, gerçekleştirdiği her türlü düzeltme, silme veya işleme faaliyetini kısıtlama işlemini kişisel verilerin açıklandığı alıcılara bildirir. Veri öznesinin bu yönde bir talebinin bulunması halinde, veri öznesini bu alıcılar hakkında bilgilendirir. Fakat bunun "imkansız olmaması veya ölçüsüz bir çabayı gerektirmemesi" gerekmektedir[342]. Aksi takdirde bu yükümlülük yerine getirilmeyebilir (GDPR m. 19). Her iki veri koruma düzenlemesinde böyle bir hükmün

---

[340] GDPR 67 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-67/, (E.T. 21.10.2023).

[341] Nitekim Kişisel Verileri Koruma Kurulu'nun verdiği bir kararda veri işleme faaliyetinin durdurulmasına karar verilebileceği ifade edilmiştir (Kişisel Verileri Koruma Kurulu, 23.06.2020 tarih ve 2020/481 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6776/2020-481, (E.T. 03.01.2024)).

[342] ABAD, 19.10.2016 tarih ve C-582/14 numaralı Patrick Breyer v Bundesrepublik Deutschland kararı, https://curia.europa.eu/juris/liste.jsf?num=C-582/14, (E.T. 21.10.2023). ABAD söz konusu kararında, ölçüsüz çabayı; işin çok fazla zaman, masraf ve insan gücü gerektirmesi olarak değerlendirmiştir.

öngörülmesinin amacı, hatalı veya eksik olan bilginin yayılmasını engellemektir[343]. Böylece kişiye verisi üzerinde kontrol yetkisi de sağlanmış olacaktır.

KVKK uyarınca ilgili kişi, düzeltme veya silme talebinden sonra bu durumun kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteyebileceği gibi; düzeltme veya silme talebi yerine getirildikten sonra uygulanmak üzere, bu yöndeki talepleri ile birlikte de bildirimde bulunulmasını isteyebilir[344]. GDPR'a göre ise, söz konusu bildirim doğrudan yükümlülük olarak düzenlendiği için; veri öznesinin düzeltme, silme veya işleme faaliyetini kısıtlama talebine yönelik yapılan işlemlere ilişkin bildirimde bulunulmasını istemesine gerek yoktur. Hatta veri sorumlusu kişisel verilerin açıklandığı alıcılara bu yönde bildirimde bulunduğuna ilişkin veri öznesine bilgi verebilir. Fakat bunu veri öznesinin talep etmesi gerekmektedir.

Veri sorumlusu tarafından bu bildirimin yapılması, söz konusu alıcıların da işledikleri veriler üzerinde aynı düzeltme veya silme işlemini yaptığı anlamına gelmez. Veri öznesi bu alıcılarla da temasa geçerek verilerine erişim, düzeltme, silme gibi taleplerde bulunarak kontrol sağlamalıdır[345].

G. Veri Taşınabilirliği Hakkı

Veri taşınabilirliği hakkı, veri koruma hukukunda ilk defa GDPR ile tanınmıştır[346]. KVVK'de ise yer almamaktadır. Kısaca ifade etmek gerekirse; kişisel verilerin işlenmesinin otomatik araçlarla gerçekleştirildiği durumlarda, "veri öznesinin kendisi ile ilgili olarak bir veri sorumlusuna sağladığı kişisel verileri; yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek" uyumlu bir formatta alabilmesine ve bir engelle karşılaşmaksızın başka bir veri sorumlusuna iletebilmesine yönelik bir haktır[347]. Böylece veri öznesine, kendi verilerini birbiriyle uyumlu

---

[343] De Terwangne, s. 471.
[344] Dülger, s. 506.
[345] Gloria González Fuster, "Article 19. Notification obligation regarding rectification or erasure of personal data or restriction of processing", **The EU General Data Protection Regulation (GDPR): A Commentary**, (Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler), Oxford University Press, Croydon, 2020, s. 496.
[346] 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, s. 194.
[347] GDPR 68 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-68/, (E.T. 22.10.2023).

uygulamalarda herhangi bir kayba uğramadan yeniden kullanmasına olanak sağlayarak verileri üzerindeki kontrolünü daha fazla güçlendirmesine yarar[348]. Söz konusu verilerin otomatik araçlarla işlenmesi, ya veri öznesinin rızasına ya da veri sorumlusuyla yapılmış olan bir sözleşmeye dayanmalıdır (GDPR m. 20/1-a, b). Aksi takdirde veri taşınabilirliği hakkını kullanmak mümkün değildir.

Veri sorumlularının bu hakkın yerine getirilmesini sağlamak için uyumlu formatlar geliştirmesi gerekmektedir. Bir formatın uyumlu sayılabilmesi için bilgi sistemlerine veri alışverişi yapma ve bilgi paylaşımı sağlama imkanı vermesi gerekmektedir[349]. Verilerin "yapılandırılmış" olabilmesi için de belirli bir yapıya sahip olması lazımdır. Böylece hem veri setlerinin taşınmasında hem de birleştirilmesinde çeşitlilik sağlayarak veri analitiği yapılmasına yardımcı olacaktır. Veriler örneğin; bir veri tabanında, XML, JSON veya CSV dosyaları gibi belirli dosyalarda saklanabilir[350]. "Yaygın olarak kullanılan" format ise işlenen verinin niteliğine ve veri sorumlusunun ait olduğu sektöre göre uyumlu olma açısından değişiklik gösterebilmektedir. Bu nedenle her somut olayı kendi özelliklerine göre ele almak gerekir. Ayrıca her sektörün yaygın olarak kullanacağı formatları bir düzenlemeyle standart hale getirebileceği gibi yukarıda belirtilen türden açık formatlar kullanarak da bu hakkın yerine getirilmesinde rol oynayabilir[351]. Son olarak, belirli verilerin yazılım uygulamaları tarafından kolayca tanımlanabilir, tanınabilir ve ayrıştırılabilir olması ise "makine tarafından okunabilen" formatı ifade etmektedir[352].

Veri taşınabilirliğini sağlamak için veri sorumlusunun, veri öznesine kişisel verilerini başka bir veri sorumlusuna iletirken herhangi bir engel çıkarmaması gerekmektedir. Bu engeller; verilerin uyumlu formatta sunulmaması olabileceği gibi bu işlem için ücret talep edilmesi, teslimde gecikme veya veri kümelerinin gizlenmesi gibi hukuki, teknik veya mali engeller olabilir[353].

---

[348] Vrabec, s. 159.
[349] Fundamental Rights Agency, s. 228.
[350] Article 29 Data Protection Working Party, "Guidelines on the right to data portability", **Avrupa Komisyonu Web Sitesi**, 2017, https://ec.europa.eu/newsroom/article29/items/611233, (E.T. 22.10.2023), (Data Portability), s. 18.
[351] Article 29 Data Protection Working Party, Data Portability, s. 18.
[352] 2013/37/EU Direktifi – Gerekçe 21, https://www.ulapland.fi/loader.aspx?id=91486ead-c3aa-4819-8de7-514251af8a83, (E.T. 22.10.2023).
[353] Article 29 Data Protection Working Party, Data Portability, s. 15.

Veri öznesi, teknik açıdan mümkünse, kişisel verilerin doğrudan bir veri sorumlusundan diğerine iletilmesini isteyebilir (GDPR m. 20/2). Örneğin, veri sorumlusu bu yükümlülüğünü, doğrudan veri aktarımının en etkili ve ucuz yöntemi olan API[354] kullanarak yerine getirebilir. Fakat bu yükümlülük veri sorumlularına teknik olarak uyumlu işleme sistemlerini benimseme veya sürdürme zorunluluğu yüklememelidir[355]. Ayrıca veri öznesine bu seçeneğin sağlanmaması durumunda, teknik imkanların yetmediğini kanıtlama yükü veri sorumlusuna düşmektedir[356].

Veri taşınabilirliği hakkının bir istisnasını, "kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması için gereken işleme faaliyetleri" oluşturmaktadır (GDPR m. 20/3). Vergi işlemleri, suç ihbarı, kamu sağlığı, sosyal hizmet ve seçim kampanyaları gibi hususlar buna örnek verilebilir. Diğer bir istisna ise, başkalarının temel hak ve özgürlüklerine olumsuz bir etki yaratacağı hallerdir (GDPR m. 20/4).

Veri taşınabilirliğinin her ne kadar erişim ve silme haklarının bazı yönlerine benzer olduğu düşünülse de durum böyle değildir. Gerçekten de veriye erişim sağlamasına ek olarak yararlı amaçlarla yeniden kullanılabilmesi için başka bir veri sorumlusuna transfer edilmesine olanak sağlaması yönüyle erişim hakkından, verilerin sahibine uygun formatta teslim edilmesine rağmen kopyasının hal veri sorumlusunda kalmaya devam etmesi yönüyle de silme hakkından farklılık göstermektedir[357]. Bununla beraber veri taşınabilirliği, erişim, silme ve işleme faaliyetlerini kısıtlama hakları birbirlerinin kullanılmasına halel getiremez[358].

Veri taşınabilirliği hakkı, henüz 2018 yılında yürürlüğe giren GDPR ile veri öznelerine tanındığı için bu konuda verilen karar sayısı oldukça kısıtlıdır. Hakkın kullanımına ilişkin örnek vermek gerekirse, Amsterdam Bölge Mahkemesi'nin Ola's Driver App kararından bahsedilebilir[359]. Mahkeme önüne gelen uyuşmazlıkta, şoför

---

[354] "API" ya da açılımının Türkçe anlamıyla "Uygulama Programlama Arayüzü" veri sorumlusu tarafından sağlanan uygulama veya web hizmetlerinin, diğer sistemlerin veya uygulamaların kendi sistemlerine sorunsuzca bağlanabilmesi ve etkileşimde bulunabilmesi için sunulan arayüzlerini temsil etmektedir (Article 29 Data Protection Working Party, Data Portability, s. 15).

[355] Article 29 Data Protection Working Party, Data Portability, s. 16.

[356] Vrabec, s. 166.

[357] De Hert, Papakonstantinou, Malgieri, Beslay ve Sanchez, ss. 201, 202.

[358] GDPR 68 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-68/, (E.T. 22.10.2023).

[359] InstantieRechtbank Amsterdam, 11.03.2021 tarih ve C/13/689705 numaralı Ola's Driver App kararı, https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBAMS:2021:1019, (E.T. 22.10.2023).

olan davacıların çalıştığı taksi uygulamasından veri taşınabilirliği hakları kapsamındaki taleplerinin yerine getirilmediği iddiasını değerlendirmiştir. Davaya konu olaya göre; davacılar, işçilerin çalışma sırasında kendileri hakkında toplanan kişisel verilerine erişmesini sağlamayı amaçlayan ve kar amacı gütmeyen bir kuruluş olan WIE'ye verilerin aktarılabilmesi için, veri taşınabilirliği hakkı kapsamına giren kişisel verilerinin CSV dosyası olarak veya bir API yahut TTP aracılığıyla verilmesi yönünde talepte bulunmuşlardır. Davalı istenen verilerin yalnızca bir kısmını CSV formatında davacılara vermiştir. Mahkeme öncelikle, GDPR m. 20'nin söz konusu kişisel verilerin, bir CSV dosyasında veya bir API aracılığıyla (her ne kadar önerilen uygun format tipi olsa da) sağlanması yönünde otomatik olarak bir yükümlülük yüklemediğini; makine tarafından okunabilir başka uygun formatlarla da verinin sağlanabileceğini vurgulamıştır. Daha sonra veri öznelerinin kendilerine dair tam olarak hangi verileri istediklerini taleplerinde belirtmediklerini ifade etmiştir. Davalının ise, taksi uygulamasını kullanan yolcuların da birtakım kişisel verilerini içerdiğinden; başkalarının temel hak ve özgürlükleri üzerinde olumsuz bir etki yaratacağı sebebiyle şoförlerin verilerin tamamını sağlamamasının GDPR'ye bir aykırılık oluşturmadığını belirtmiştir.

H. İtiraz Hakkı

1. İtiraz Hakkının Kapsamı, Esasları ve Uygulanma Usulü

GDPR m. 21'de düzenlenen türden bir itiraz hakkı, KVKK'de açıkça yer almamaktadır. Ancak tıpkı işleme faaliyetini kısıtlama hakkında olduğu gibi, kanunun bazı maddelerinden ve kanunun kendisi ile hukuka esas olan genel ilkelerden yola çıkılarak, veri öznesinin itiraz hakkını kullanabileceği sonucuna varılabileceği kanaatindeyiz. Ancak elbette, bu hakka sadece yorumla ulaşılmaması gerektiğini, bunun kanunilik ilkesine aykırı olacağını ve en kısa sürede GDPR'dekine benzer bir hükmün KVKK'ye eklenmesi gerektiğini de belirtmek gerekmektedir.

İtiraz hakkının tanınmasındaki amaç, her ne kadar veriler hukuka uygun olarak işlense de işleme faaliyetinin veri öznesinin beklentileriyle uyuşmaması halinde

sonlandırılmasına imkan tanımaktır[360]. GDPR'nin ilgili maddesinde veri öznesine esasen iki tür itiraz hakkı tanınmıştır. Bunlar, kişisel verilerin işlenmesine genel itiraz ve doğrudan pazarlama amacıyla işlenmesine itiraz olarak gruplandırılabilir.

"Kişisel verilerin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda, veri öznesinin doğrudan pazarlama ile alakalı olduğu ölçüde" herhangi bir zamanda itiraz etme hakkı bulunmaktadır (GDPR m. 21/2). Buna, doğrudan pazarlama için yapılan profil çıkarma (profilleme) işleminin[361] yanı sıra istenmeyen pazarlama mesajlarının gönderilmesinin engellenmesi de dahildir. Bu mesajlar fiziki posta, e-posta, faks, kısa mesaj, telefon gibi araçlarla gönderiliyor olabilir[362]. Anlaşılacağı üzere "doğrudan pazarlama" kavramı ile belirli alıcılara yönelik yapılan tüm reklam ve pazarlama faaliyetleri kastedilmektedir. Bu açıdan sadece işletme, ürün ve hizmetlerin tanıtımıyla sınırlı olmayıp siyasi partilerin seçmenlere yönelik kampanyalarını ve hayır kuruluşlarının olası bağışçılarla olan iletişimlerini de kapsamaktadır[363]. Dikkat edilmelidir ki itiraz yapıldığında, söz konusu amaçla ilgili olan her türlü veri işleme faaliyeti durur (GDPR m. 21/3). Yani artık kişiyle ilgili olarak veri toplanmaz, saklanmaz, analiz edilmez, tasnif edilmez, profil çıkarılmaz ve kişiye ileti gönderilmez. Ancak doğrudan pazarlama haricindeki amaçlarla yapılan işleme faaliyetleri devam edebilir. Veri öznesine tanınan bu hak mutlaktır, bir başka deyişle istisnası yoktur. Böylece veri özneleri, veri sorumlularının menfaatleri doğrultusunda hedef haline gelmekten ve veri objesi olarak kullanılmaktan korunur. İtiraz hakkının ileri sürülmesine yönelik talep alındıktan sonra, veri öznesine ilişkin veriler, ileride doğrudan pazarlama amacıyla kullanılmamasını sağlayacak şekilde işaretlenmelidir[364]. GDPR m. 17/1-c hükmü uyarınca veri sorumlusuna kişisel verileri herhangi bir gecikmeye mahal vermeksizin silme yükümlülüğü verildiği için artık veri öznesinin talebine gerek olmaksızın bu veriler silinmelidir. Fakat dilerse veri öznesi bunu ayrıca da talep edebilir.

Öte yandan genel itiraz hakkı, veri öznelerine kendi özel durumlarına yönelik gerekçelerle işlemeye itiraz edilmesine olanak sağlar. Fakat bu hak mutlak değildir, zira veri sorumlusu birtakım zorlayıcı meşru gerekçelerin varlığını sebep göstererek

[360] Sharma, s. 221.
[361] Profil çıkarma veya profilleme hakkındaki açıklamalar için lütfen bkz. Dipnot 109.
[362] Lloyd-Jones ve Carey, s. 140.
[363] Lloyd-Jones ve Carey, s. 141.
[364] Lloyd-Jones ve Carey, s. 142.

itiraz talebini yerine getirmekten kaçınabilir. Bu gerekçeler; veri öznesinin menfaatleri, hakları ve özgürlüklerinden ağır basan bir işleme faaliyetinin varlığına, birtakım hukuki iddiaların ileri sürülmesi ve bunların uygulanması veya savunulmasına yönelik olmalıdır (GDPR m. 21/1). Veri sorumlusu, itiraz talebini reddedip işlemeye devam edecekse, bu istisnalardan birinin veya birkaçının varlığını kanıtlamalıdır[365]. Ayrıca veri öznesine reddin sebebini gerekçeleriyle birlikte açıklamalıdır[366].

İtiraz talebini alan veri sorumlusu, talebin yerine getirilip getirilmeyeceğine bakmaksızın, GDPR m. 18/1-d gereğince işleme faaliyetini derhal kısıtlamalıdır. İtiraz talebi uyarınca, veri sorumlusu ile veri öznesinin meşru gerekçelerinden hangisinin birbirine ağır bastığı değerlendirilene kadar bu kısıtlama devam edecektir. Bu süreçte işleme faaliyeti, sadece GDPR m. 18/2 kapsamındaki durumların mevcut olması halinde ve saklama haricinde devam edebilecektir[367]. Eğer veri sorumlusu itiraz talebini yerinde bulursa, artık veri öznesine ilişkin veri işleyemez. Ayrıca bu durumda, GDPR m. 17/1-c hükmü uyarınca veri sorumlusuna kişisel verileri herhangi bir gecikmeye mahal vermeksizin silme yükümlülüğü verildiği için artık veri öznesinin talebine gerek olmaksızın bu veriler silinmelidir[368]. Veri öznesi bunu kendi de talep edebilir.

Genel itiraz hakkının bir başka istisnasını da kişisel verilerin bilimsel, tarihi ve istatistiki araştırma amaçları doğrultusunda işlenmesi oluşturur. Bu durumda işleme faaliyeti, kamu yararı kapsamında yürütülen bir görevin ifası için gerekliyse artık veri öznesi itiraz hakkını haiz olmayacaktır (GDPR m. 21/6). Madde metninde, veri sorumlusunun itiraz talebini reddetmek için zorlayıcı meşru gerekçelerin var olması gerektiğine dair bir ibare yer almadığı için bu durumda reddin daha esnek koşullara bağlandığı kanaatindeyiz.

Düzenlemede yer alan özel bir şeffaflık kuralı gereği, itiraz hakkının diğerlerinden ayrıca ve açıkça veri öznesinin bilgisine sunulması gerekmektedir. Bu

---

[365] GDPR 69 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-69/, (E.T. 25.10.2023).

[366] Gabriela Zanfir-Fortuna, "Article 21. Right to object", **The EU General Data Protection Regulation (GDPR): A Commentary**, (Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler), Oxford University Press, Croydon, 2020, (Right to object), s. 517.

[367] Bu konuda detaylı bilgi için lütfen "İşleme Faaliyetini Kısıtlama Hakkı" başlığı altındaki açıklamalara bakınız.

[368] Zanfir-Fortuna, Right to object, s. 518.

bilgilendirme, en geç veri öznesiyle ilk kez iletişime geçildiğinde yapılmalıdır (GDPR m. 21/4). Bu sayede, özellikle de doğrudan pazarlama amacıyla veri işlendiği durumlarda, daha ilk temasta veri öznesine çekilme fırsatı tanınmış olur[369]. Örneğin, kişiye çevrim içi dil kursu veren bir platformdan "ay sonuna kadar kayıt yaptırılması halinde, bir sonraki kur için yüzde elli indirim uygulanacağına" dair doğrudan pazarlama amaçlı bir e-posta gelmiş olsun. E-postanın altında "Bizden bu tür iletiler almak istemiyorsanız, buraya tıklayın" şeklinde belirgin bir bağlantı yer alsın. Veri öznesi bunun üzerine tıklayarak söz konusu platformun e-posta listesinden çıkabilir. Böylece "teknik açıklamaları kullanmak suretiyle otomatik yollarla itiraz hakkını" da kullanmış olacaktır (GDPR m. 21/5).

2. İtiraz Hakkına İlişkin Örnek Kararlar

CNIL bir kararında[370], ısı pompası ve kapı gibi ekipmanların montajı işiyle uğraşan bir şirketin, doğrudan pazarlama amacıyla yaptığı veri işleme faaliyetleri kapsamında veri öznelerinin itiraz hakkına ilişkin hüküm kurmuştur. Komisyona yapılan ihbarda; şirketin çok sayıda kişiyi sürekli olarak hizmetlerinin reklamını yapmak için aradığı ve hem telefonda şifahi olarak hem de şirkete gönderilen e-postalar yoluyla bu aramalara itiraz edilmesine rağmen aramaların durmadığı bildirilmiştir. Veri sorumlusu şirket de çok sayıda çağrı merkezi aracılığıyla bu işlemlerin yürütüldüğü bilgisini vermiştir. CNIL bunun üzerine bir denetim yapmış ve itiraz hakkı kapsamında yapılan taleplerin gereğinin yerine getirilmesinde eksiklikler olduğunu tespit ederek bunların giderilmesi için süre tanımıştır. Süre sonunda yapılan kontrolde; veri sorumlusu şirket ile veri işleyen çağrı merkezleri arasında, itiraz edenleri diğerlerinden ayırt etmeye, veri tabanından çıkarmaya veya ileride herhangi bir pazarlama faaliyeti kapsamında iletişime geçilmesini engelleyecek türden bir işaretlemeye yarayan bilgi paylaşımı için etkili bir mekanizma kurulmadığı ve çağrı merkezlerinden çok azının GDPR m. 21/2 uyarınca yapılan itirazların ardından veri öznelerini hedef almayı bıraktığı tespit edilmiştir. Dolayısıyla söz konusu veri

[369] Zanfir-Fortuna, Right to object, s. 519.

[370] CNIL, 21.11.2019 tarih ve SAN-2019-010 sayılı X Şirketi kararı, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000039419459/, (E.T. 25.10.2023).

öznelerinin kişisel verilerinin doğrudan pazarlama amacıyla işlenmesine itiraz hakları ihlal edilmiştir.

Lahey Bölge Mahkemesi de bir kararında[371], kredi kuruluşu olan veri sorumlusuna yapılan genel itiraz talebi kapsamında bir değerlendirme yapmıştır. Arkadaşına iş kurma konusunda yardımcı olmak isteyen veri öznesi, veri sorumlusu şirketten bir miktar kredi çekmiştir. Fakat geri ödeme konusunda birçok kez gecikme yaşadığı ve periyodik olarak ödeme yapamadığı için kredi notu düşürülmüştür. Veri öznesi en nihayetinde borcunu tamamen ödese de, borcun kapanmasını müteakip beş yıllık sürede kredi notuna ilişkin kayıtların saklanacağını öğrenmiştir. Bu husus, mali durumunu düzelten ve partnerinin ailesinin evinden ayrılarak kendisine ait bir eve taşınmak isteyen veri öznesini olumsuz yönde etkilemektedir. Bu nedenle veri sorumlusuna başvurarak itirazda bulunmuştur. Talebinin reddedilmesi üzerine ise mahkemeye başvurmuştur. Verdiği kararda mahkeme; veri öznesinin ailesiyle kendilerine ait bir evde yaşama arzusunun anlaşılabilir olduğunu fakat söz konusu kredi notunun neden bunu zora soktuğunu kanıtlayacak yeterli delil sunmadığını, yakın geçmişte ödeme yükümlülüklerini defalarca yerine getirmediği de göz önüne alındığında söz konusu kredi notunun sistemden silinmesinin hakkaniyetli olmayacağını belirterek veri sorumlusunun menfaatinin veri öznesinin menfaatine ağır bastığına değinmiştir.

İ. Otomatik Karara Tabi Olmama Hakkı

1. Otomatik Karara Tabi Olmama Hakkının Kapsamı, Esasları ve Uygulanma Usulü

GDPR m. 22/1 ile veri öznesine, profil çıkarma (profilleme)[372] de dahil "yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı" tanınmıştır. Bunun için söz konusu kararın, kişinin kendisiyle alakalı hukuki sonuçlar doğurması veya benzer biçimde kayda değer bir şekilde etkilemesi gerekmektedir. İlk olarak

[371] Rechtbank Den Haag, 18.11.2021 tarih ve C-09-608582 numaralı Defam kararı, https://www.navigator.nl/document/id5df2b3f48385406cbc80c8cbdd36e99b/rb-den-haag-18-11-2021-nr-c-09-608582-ha-rk-21-101, (E.T. 25.10.2023).

[372] Profil çıkarma veya profilleme hakkındaki açıklama için lütfen bkz. Dipnot 109.

belirtmek gerekir ki, alınacak "kararın" illa ki devlet makamlarının alacağı türden, hukuki açıdan bağlayıcı resmi bir karar olmasına gerek yoktur. Söz konusu ifade geniş yorumlanmaktadır. Herhangi bir muhatabın, veri öznesine karşı belirli bir tutumu benimsemesi ve buna göre hareket etmesi veya etmeyi planlaması da tanınan hak kapsamında bir "karar" sayılır[373]. İkinci olarak, "sadece otomatik işleme faaliyetine dayalı olmak" ile ifade edilmek istenen, karar alma sürecine herhangi bir insan müdahalesi ve dahlinin olmamasıdır[374]. Örneğin, bir bankanın kredi başvurusu yapan kişinin finansal geçmişini ve kredi notunu otomatik olarak analiz eden bir sistem kullanabilir. Bu sistem, bünyesinde yer alan algoritma sayesinde belirli bir kredi limitini otomatik olarak kabul etme veya reddetme kararı alabilir. Böylece değerlendirme sürecine insan müdahalesi olmaz. Fakat veri sorumluları bu hakkın getirdiği yükümlülüklerden kaçınmak için insan müdahalesini varmış gibi gösterebilir. Mesela yukarıda verilen banka örneğini ele alalım. Bir banka çalışanı, kredi vermede kullanılan sistemin aldığı kararları denetlemekle görevlendirilmiş olsun. Söz konusu çalışanın görevi, sadece sistem tarafından verilen otomatik kararların algoritmaya uygun alınıp alınmadığını kontrol etmekse, bu durumda artık gerçek anlamda bir insan müdahalesinden bahsedilemeyecektir. Yani alınan karara ilişkin yapılan her türlü gözetim ve denetimin göstermelik değil; fiili ve anlamlı bir etkisinin olması gerekmektedir[375]. Örneğin, kişinin iyi bir kredi notu olmasa da başarı vaat eden bir iş planıyla bankaya kendi limitinin üzerinde bir meblağda kredi almak için başvurduğunu düşünelim. Bankanın kullandığı sistemin tek başına otomatik olarak reddedeceği başvuruyu, çalışanın iş planından etkilenerek onaylaması karar alma sürecine gerçek anlamda bir insan dahlinin var olduğunu gösterecektir. Ayrıca karar alma sürecindeki insan dahli kriterini sağlayan kişinin, kararı değiştirme yetki ve ehliyetini haiz olma gerekliliği de unutulmamalıdır[376].

---

[373] Lee A. Bygrave, "Article 22. Automated individual decision-making, including profiling", **The EU General Data Protection Regulation (GDPR): A Commentary**, (Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler), Oxford University Press, Croydon, 2020, s. 532.

[374] Article 29 Data Protection Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", **Avrupa Komisyonu Web Sitesi**, 2017, https://ec.europa.eu/newsroom/article29/items/612053/en, (E.T. 16.11.2023), (Automated individual decision-making), s. 20.

[375] Gianclaudio Malgieri, "Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations", **Computer Law & Security Review**, Cilt: 35, Sayı: 5, 2019, (Automated decision-making), s. 3.

[376] Article 29 Data Protection Working Party, Automated individual decision-making, s. 21.

Üçüncü olarak, bu hakkın kullanılabilmesi için otomatik kararın, veri öznesinin kendisiyle alakalı hukuki sonuçlar doğurması veya benzer biçimde kayda değer bir şekilde etkilemesi gerektiği ifade edilmiştir. GDPR'da "hukuki sonucun" veya "kayda değer etkinin" tanımı yapılmamıştır. O halde kelimelerin genel anlamından yola çıkarak, "hukuki sonucun" bir kişinin yasal haklarını etkileyen bir durum olduğundan bahsetmek mümkündür. Etkilenen kişinin temel hak ve özgürlükleri, hukuki durumu veya bir sözleşme kapsamındaki hak ve menfaatleri olabilir. Örneğin, kanunla verilen bir sosyal yardıma (çocuk, yiyecek, yakacak, barınma vb.) hak kazanma ya da bu yardımın kesilmesi, kişinin eski hükümlü olduğunun açığa çıkması nedeniyle iş sözleşmesinin feshedilmesi, bir ülkeye yapılan iltica talebinin reddi gibi durumlar bu kapsamda değerlendirilebilir. Otomatik karar kişiyle ilgili hukuki bir sonuç doğurmasa bile, onu benzer derecede ve "önemli bir ölçüde etkiliyorsa" yine kişinin bu karara tabi olmama hakkı bulunmaktadır. Yukarıda verilen kredi başvurusu örneği ve çevrim içi bir platforma öz geçmiş yükleyerek yapılan iş başvurularının insan müdahalesi olmaksızın değerlendirilmesi ve mülakata alınacak adayların belirlenmesi buna örnek olarak verilebilir. Yani otomatik işleme faaliyetine dayalı kararın; verinin ilişkin olduğu kişinin tabi olduğu koşulları, davranış biçimini veya seçimlerini önemli ölçüde etkilemesi, üzerinde uzun sürecek veya kalıcı olacak bir etki yaratması yahut kişinin dışlanmasına yahut ayrımcılığa uğramasına neden olması gerekmektedir[377]. Örneğin, HIV pozitif olan birinin bu sebeple işe alınmaması veya sosyal çevrelerden dışlanması durumlarının kişinin yaşamını önemli ölçüde etkileyeceğinden bahsetmek mümkündür. Yine veri öznesinin çocuk olduğu durumlarda, önemli ölçüde etkileme kriterinin sağlandığı kabul edilir[378].

Bazı durumlarda veri özneleri hakkında otomatik yollarla karar verilmesine olanak sağlayan istisnalar öngörülmüştür (GDPR m. 22/2). Bunların ilki, AB veya üye devlet hukukunun otomatik karar alınmasına izin vermesidir. Örneğin, dolandırıcılık veya vergi kaçakçılığı gibi suçları önleme amacıyla kanunlar otomatik karar almaya izin verebilir[379]. Ancak bu durumda da söz konusu kanun, veri öznelerinin temel hak ve özgürlükleri ile meşru menfaatlerini korumaya yönelik uygun tedbirleri içermelidir.

[377] Article 29 Data Protection Working Party, Automated individual decision-making, s. 21.
[378] GDPR 38 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-38/, (E.T. 25.11.2023).
[379] GDPR 71 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-71/, (E.T. 25.11.2023).

İkinci istisna, veri öznesinin açık rızasının varlığıdır. Üçüncü istisna ise, söz konusu otomatik karar alma faaliyetinin veri öznesi ile sorumlusunun arasında bir sözleşme akdedilmesi veya bu sözleşmenin ifa edilmesi için gerekli olmasıdır. Veri sorumlusu tarafından çok fazla miktarda veri işleniyorsa, karar alma sürecinde insan müdahalesinin sağlanması zor veya imkansız olabilir[380]. Bu durumda istisnanın uygulanması gerekli sayılabilecektir. Fakat veri sorumlusu, bu istisnadan yararlanabilmek için veri öznelerinin haklarına daha az müdahaleci bir yöntemin olmadığını yani müdahalenin gerekli olduğunu kanıtlamalıdır[381]. Örneğin bir şirketin öğrencilere burs verdiğini ve bu nedenle her sene yüksek sayıda başvuru aldığını düşünelim. Öğrenciler, şirket tarafından sağlanan sistemde yer alan başvuru formunu doldurup gerekli belgeleri yükleyerek burs başvurusunda bulunuyor olsun. Çok sayıda başvurunun kısa sürede incelenip burs almaya hak kazananların açıklanabilmesi için otomatik karar almaya yarayan algoritmadan yararlanabilir. Böylece belirli bir not ortalamasının altında olanlar doğrudan elenebilecek ve sadece kısa bir liste değerlendirme kurulunun önüne gelecektir.

Veri öznesinin açık rızasının varlığı ve veri sorumlusuyla aralarında sözleşme akdetme veya ifa etme için otomatik karar almanın gerekli olması durumlarında, öncelikle insan müdahalesini sağlamak zorundadır. Ayrıca "veri öznesinin kendi görüşünü ifade etme ve karara karşı çıkma yönündeki hakları, özgürlükleri ve meşru menfaatlerini" güvence altına alacak uygun tedbirler uygulamalıdır (GDPR m. 22/3). Buna veri koruma etki değerlendirmesi yaptırılması da dahildir[382]. Değerlendirmenin; işleme faaliyetleri ve işleme amaçlarına ilişkin sistematik bir açıklamayı, faaliyetlerinin amaçlarla ilişkili olarak gerekliliği ve orantılılığına yönelik bir değerlendirmeyi, veri öznelerinin hakları ve özgürlüklerine yönelik risklere ilişkin bir değerlendirmeyi, kişisel verilerin korunmasının sağlanmasına ilişkin yasal düzenlemelere uygun hareket edildiğinin gösterilmesiyle ilgili tedbirlerin neler olduğuna dair bir açıklamayı içermesi gerekmektedir (GDPR m. 35/7). Alınacak başka bir tedbir, veri sorumlusunun alınan kararlarda herhangi bir önyargı olup olmadığını rutin olarak kontrol ettirmek olabilir. Özellikle de hassas verilerin konu olduğu hataları

[380] Hüseyin Can Aksoy, "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", **Kişisel Verileri Koruma Dergisi**, Cilt: 4, Sayı: 2, Ankara, 2022, (Algoritmik Karar Verme), s. 78.
[381] Article 29 Data Protection Working Party, Automated individual decision-making, s. 23.
[382] GDPR m. 35/3-a hükmüne göre, profilleme dahil otomatik karar almanın mevcut olması halinde veri koruma etki analizi yapılmasına özellikle ihtiyaç duyulmaktadır.

ve ayrımcılığı engellemek adına özel tedbirler uygulanmasını sağlayabilir[383]. GDPR m. 22/3'te sayılan haklar ve güvenceler tahdidi nitelikte olmadığı için verilen örneklerin çoğaltılması mümkündür. Yine benzer şekilde, veri öznesine otomatik işleme faaliyetine dayanılarak alınan kararın açıklaması da yapılabilir[384]. Açıklama hakkı kapsamında, fikri mülkiyet ve ticari sır niteliğindeki bilgilerin açıklanmasının beklenemeyeceği unutulmamalıdır[385]. Ancak mevzubahis sırların gizliliği sağlanarak veri öznesine menfaatlerini koruyup gözetebilmesi için ihtiyacının olduğu bilgiler verilebilmelidir[386]. Veri sorumlularının işletme sırlarını ileri sürerek veri öznelerinin bu hakkını kullanmasını engellemesi söz konusu olamaz[387]. Her iki tarafın da menfaatleri arasında adil bir denge kurmaya özen göstermelidir.

Son olarak, GDPR m. 22/4'te hassas nitelikli kişisel verileri içeren otomatik karar almanın hangi koşullarda mümkün olabileceği düzenlenmiştir. Buna göre, öncelikle GDPR m. 22/2'de sayılan türden bir istisna var olmalıdır. Bu şarta ek olarak, ya veri öznesinin açık rızası olmalı (GDPR m. 9/2-a) ya da kayda değer ölçüde kamu yararı sağlayan sebeplerle işleme faaliyetinin zorunlu olması gerekmektedir (GDPR m. 9/2-g). Kamu yararı sağlanabilmesi için işleme faaliyeti; işleme amacıyla orantılı, kişisel verilerin korunması hakkının özüne saygılı, veri öznesinin temel haklarının korunması için uygun ve belirli tedbirleri ihtiva eden AB veya üye devlet hukukuna dayalı olarak yapılmalıdır (GDPR m. 9/2-g). Aksi takdirde hassas verileri içeren bir otomatik karar alma faaliyetinin yapılması söz konusu olamayacaktır.

Otomatik karara tabi olmama hakkı, KVKK'de ilgili kişinin haklarını düzenleyen maddede kendine yer bulmuştur. Hükme göre, herkes işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin "kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkı"na sahip kılınmıştır (KVKK m. 11/1-g). Madde lafzı incelendiğinde GDPR'dekine paralel bir düzenleme yapıldığı görülmektedir. Verilerin "münhasıran otomatik sistemler vasıtasıyla" işlenmesinden kastın "sadece otomatik işleme faaliyetine dayalı olmak" yani karar alma sürecinin

[383] Aksoy, Algoritmik Karar Verme, s. 79.
[384] GDPR 71 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-71/, (E.T. 25.11.2023).
[385] Aksoy, Algoritmik Karar Verme, s. 81.
[386] Aksoy, Algoritmik Karar Verme, s. 82.
[387] Margot E. Kaminski, "The Right to Explanation, Explained", **Berkeley Technology Law Journal**, Cilt: 34, Sayı: 1, 2019, s. 203.

herhangi bir insan müdahalesi ve dahli olmaksızın gerçekleşmesi olduğu açıktır. Bu açıdan yukarıda bu hususla ilgili yapılan diğer açıklamalar geçerlidir. Yine benzer şekilde "kişinin kendisi aleyhine bir sonucun ortaya çıkması" ifadesinin, otomatik işlemenin ilgili kişiyle ilgili hukuki sonuç doğurması veya benzer biçimde kayda değer bir şekilde etki uyandırmasına karşılık geldiği söylenebilir. Fakat GDPR'den farklı olarak, KVKK ilgili kişiye otomatik karara tabi olmaya itiraz hakkı vermiştir. Gerçekten de GDPR'deki hak, otomatik işleme faaliyetine dayanan kararlar almama suretiyle eyleme geçme yükünü veri sorumlusuna yüklemişken[388]; KVKK'deki haliyle, bu şekilde karar alınmasına itiraz edip ilgili kişiyi bilfiil olarak bu hakkı ileri sürmeye yöneltmektedir[389]. İki düzenleme arasındaki başka bir farklılık da GDPR'deki hakkın kapsamının daha geniş olmasıdır. Otomatik karar alınmasına itiraz etmenin yanı sıra, ilgili kişinin kendi görüşünü ifade etme, alınan kararlara itiraz edip sonucu değiştirme, özgürlüklerini ve meşru menfaatlerini korunmasını sağlayacak tedbirlerin uygulanmasını isteme hakları mevcuttur. Ayrıca ilgili kişiler kendilerine ilişkin olarak alınan kararların nedenini ve arkasında yatan mantığın ne olduğunu "açıklama hakkı" kapsamında sorgulayabilmektedir. Kanaatimizce bu hak açıkça düzenlenmemiş olsa da veri koruma hukukuna hakim "adil ve şeffaf işleme ile hesap verebilirlik ilkeleri" gereğince bu yöndeki taleplerin karşılanması gerekmektedir. Bir başka husus olarak, KVKK'de öngörülen itiraz hakkının neyi kapsadığı açıklanmadığı gibi veri sorumlusunun itiraz sonrası nasıl davranması gerektiği de düzenlenmemiştir. Ancak kişisel verilerin münhasıran otomatik yöntemlerle işlenmesiyle ortaya çıkan sonucun, sürece insan dahlinin de sağlanmasıyla işlenmesi nihayetinde ortaya çıkacak sonuca göre aleyhe olması halinde, veri sorumlusunun bu kararı düzeltmesi uygun olacaktır. Yani veri sorumlusunun itiraz üzerine, anlamlı bir insan müdahalesiyle alınan kararı gözden geçirme ve gerekli değişiklikleri yapma yükümlülüğü bulunmaktadır. Aksi takdirde tanınan itiraz hakkının bir hükmü kalmayacaktır.

[388] Article 29 Data Protection Working Party, Automated individual decision-making, s. 20.
[389] Aksoy, Algoritmik Karar Verme, s. 82.

2. Otomatik Karara Tabi Olmama Hakkına İlişkin Örnek Kararlar

Finlandiya Veri Koruma Komisyonu'na tavsiye amaçlı yapılan bir başvuruda[390], bir sağlık hizmeti sağlayıcısı olan veri sorumlusu, tarama ve önleme amacıyla hasta verilerini işleyecek sisteminin GDPR ile uyumlu olup olmayacağının değerlendirmesini talep etmiştir. Sistemin yapacağı değerlendirmeye göre sağlık açısından riskli bulunan hastalarla irtibata geçilerek olumsuz durum tespit edilecek ve gerekli tedavinin sağlanması için yönlendirilecektir. Risk altındaki hastalar ise halihazırda sağlık kurumunun bünyesinde bulunan tıbbi kayıtlara bakılarak doğrudan algoritma tarafından tespit edilecektir. Bu sitemin geliştirilip kullanılmak istenmesindeki ana hedefin erken teşhis ile hayat kurtarma ve kişilerin bireysel refah seviyesini arttırma olduğu ifade edilmiştir. Komisyon, bilgisayar sistemi tarafından yapılacak veri işleme faaliyetinin otomatik karar alma kapsamına girip girmeyeceği hususunda yaptığı değerlendirmede, öznelerini "sağlık durumu riskli bulunup irtibata geçilen hastalar" ve "sağlık riski bulunmayıp irtibata geçilmeyen hastalar" olmak üzere iki kategoriye ayırmıştır. Buna göre, ilk gruptaki hastalar için oluşturulan profil, karar verme sürecinin ilk aşamasını oluşturacaktır. Zira daha sonra veri öznesi hastalar, durum hakkında karar almaya ehil doktorlar tarafından muayene edilerek gerekli tetkikler yapılacak ve kişinin gerçekten hasta olup olmadığı hakkında nihai karar verilecektir. Dolayısıyla karar alma sürecine anlamlı bir insan müdahalesi sağlandığı için gerçekleştirilen işleme faaliyeti otomatik karar alma kapsamına girmeyecektir. Ancak ikinci gruptaki hastalar için durum farklıdır. Bu gruba mensup veri öznesi hastalarla herhangi bir sağlık görevlisi irtibata geçmeyecek ve tetkik yapılmayacaktır. Yani karar alma sürecinde herhangi bir insan dahli bulunmamaktadır. Algoritmaların da yanılabileceği göz önüne alındığında, sistem tarafından alınan kararların, tıbbi tedavi uygulanması gerekli olduğu halde uygun görülmeyen bireylerin sağlığı üzerinde sonu ölüme varabilecek kayda değer olumsuz etkiler yaratması muhtemeldir. Bu nedenle sistem, ikinci grup hastalar açısından GDPR m. 22/1 hükmüyle veri öznelerine tanınan otomatik karara tabi olmama hakkını ihlal eder niteliktedir.

[390] Finlandiya Veri Koruma Komisyonu, 23.06.2022 tarih ve 3895/83/22 numaralı tavsiye kararı, https://finlex.fi/fi/viranomaiset/tsv/2022/20221545, (E.T. 25.11.2023).

Avusturya Veri Koruma Otoritesi'ne yapılan bir başvuruda da[391], veri sorumlusunun "Dominanten Geo Milieus" adlı pazarlama puanlarının hesaplanmasıyla ilgili şikayette bulunulmuştur. Veri sorumlusunun kurduğu sisteme göre, veri özneleri "muhafazakarlar", "gelenekselciler", "orta sınıf", "hazcılar" veya "dijital bireyciler" gibi gruplara ayırarak bu grupların niteliklerine uygunluğunu yüzdelik oranlarla gösteriliyordu. İşbu şikayeti yapan kişi, öncesinde veri sorumlusuna başvurarak GDPR m. 15 kapsamında erişim talebinde bulunmuştur. Talep ettiği veriler arasında pazarlama puanlarının nasıl hesaplandığına ilişkin bilgiler de bulunmaktadır. Veri sorumlusu söz konusu verilerin ticari sır olarak nitelendirilmesi nedeniyle erişim sağlanmayacağını belirterek yanıtlamıştır. Avusturya Veri Koruma Otoritesi bu pazarlama puanlarının oluşturulmasını sağlayan işleme faaliyetlerinin profilleme işlemi olduğuna kanaat getirmiştir. Otomatik karar alınmasına tabi olmama hakkı, profil çıkarma işlemini de kapsamaktadır. Her ne kadar pazarlama puanlarının hangi mantıkla hesaplandığı yerel mevzuata göre ticari sır olsa da; veri öznesinin pazarlama puanı hesaplanırken kullanılan algoritma, kaynak kodu veya derleyici kodu paylaşılmadan da veri öznesine talep ettiği verilerin sağlanması mümkündür. Bunun yerine, veri öznesinin puan hesaplamasıyla bağlantılı olarak; parametreler veya giriş değişkenlerinin neler olduğu, nasıl ortaya çıktığı ve puan üzerindeki etkisi, veri öznesinin sistemdeki gruba aidiyetinin nitelendirilmesinin sebepleri, olası profil kategorilerinin listesi veya veri öznesinin düzeltme ve silme haklarını kullanmasına olanak sağlayacak diğer benzer türdeki veriler gibi bilgiler kendisine sağlanmalıdır.

J. Şikayet Hakkı

GDPR kapsamında şikayet hakkı esasen veri öznelerine tanınan üç hakkın birleşiminden meydana gelmektedir: Bir denetim makamına şikayette bulunma hakkı, bir denetim makamına karşı etkili bir kanun yoluna başvurma hakkı ve bir veri sorumlusu veya işleyene karşı etkili bir kanun yoluna başvurma hakkı. Bu haklar, veri

[391] Avusturya Veri Koruma Otoritesi, 08.09.2020 tarih ve 2020-0.436.002 numaralı kararı, https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=f2a9b55f-02bc-446d-a8fa-4fd931cb1b57&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20200908_2020_0_436_002_00,(E.T. 25.11.2023).

öznelerinin kişisel verilerinin ihlal edilmesi halinde, üye devletlerin ulusal hukuklarında yer alması gereken asgari başvuru yollarını sağlamak amacıyla öngörülmüştür[392]. Üye devletler bunların haricinde başka çözüm yolları yaratmakta elbette özgürdür.

Her veri öznesi, GDPR hükümleri bağlamında kişisel verilerinin korunması hakkının ihlal edildiği durumlarda, bağımsız bir denetim makamına şikayette bulunma hakkına sahiptir. Veri öznesinin kendisine sağlanan diğer idari veya adli yollara başvurma hakkı saklıdır (GDPR m. 77/1). Bu denetim makamının tazminata hükmetme ve veri koruma hükümlerinin yargı tarafından ihlal edildiği iddialarını değerlendirmeye yetkisi olmamalıdır[393]. Ayrıca diğer görev ve yetkileri GDPR'nin 57. ve 58. maddelerinde sayılanlarla sınırlı kalmalıdır. Denetim makamı, şikayetin seyri ve sonucu ile etkili bir kanun yoluna başvuru olanağı hakkında şikayet sahibini bilgilendirmelidir (GDPR m. 77/2). Şikayet hakkının kullanılmasının kolaylaştırılması için bir elektronik matbu şikayet başvuru formu hazırlanarak veri öznelerinin kullanımına sunulabilir[394]. Bunun yapılması, diğer iletişim araçlarının hariç tutulabileceği anlamına gelmez.

Fakat her ne kadar bağımsız denetim makamları, veri öznelerinin şikayetleri hakkında karar vermede büyük bir öneme sahip olsa da nihayetinde yargı organı değil, idari bir makamdır. Vereceği kararlar yanlış olabilir. Her idari makam gibi yargısal denetime tabi olmalıdır. Bu nedenle GDPR'nin 78. maddesiyle "her gerçek veya tüzel kişiye, bir denetim makamının kendileriyle ilgili yasal bağlayıcılığı olan bir kararına karşı etkili bir kanun yoluna başvurma hakkı" tanınmıştır. Bu başvuru hakkı, diğer idari veya adli yollara başvurma hakkına halel getirmez. Yargı organına yapılacak başvuru; denetim makamı tarafından verilen "şikayet hakkında işlem yapılmaması" veya "şikayetin reddi" kararlarına karşı olabileceği gibi, "soruşturma yetkisini kullanması" veya "idari yaptırım" kararlarına karşı da olabilir[395]. Denetim makamı,

[392] Waltraut Kotschy, "Article 77. Right to lodge a complaint with a supervisory authority", **The EU General Data Protection Regulation (GDPR): A Commentary**, (Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler), Oxford University Press, Croydon, 2020, (Article 77), s. 1119.

[393] Kotschy, Article 77, s. 1119.

[394] GDPR 141 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-141/, (E.T. 27.11.2023).

[395] GDPR 143 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-143/, (E.T. 27.11.2023).

hukuki açıdan bağlayıcı nitelikteki kararlarına karşı yargısal denetime başvuracak kişilere kolaylık sağlamak adına; kararlarını gerekçelendirmeli, açık ve net ifadeler kullanmalı, uygulanacak tedbirin tarihini belirtmeli, yetkililerin imzasını ve kimlik bilgilerini taşımalı ve karara karşı başvurulacak hukuki yolu içermelidir[396]. Denetim makamının "üç ay içerisinde şikayeti ele almaz" yahut "şikayetin seyri veya sonucu hakkında" veri öznesini bilgilendirmezse, yargı yoluna başvurulması mümkündür (GDPR m. 78/2).

Son olarak GDPR kapsamındaki hakları ihlal edilen kişilere, veri sorumlularına ve/veya veri işleyenlere karşı etkili bir kanun yoluna başvuru hakkı tanınmıştır (GDPR m. 79). Bu hak, 78. maddede öngörülen hakka ek niteliktedir. Şöyle ki, normal şartlar altında veri öznesinin herhangi bir hakkı ihlal edildiğinde, denetim makamına başvurarak ihlalin ortadan kaldırılmasına yönelik uygun tedbirler alınması istenmektedir. Denetim makamı da verdiği bağlayıcı kararla uyuşmazlığı çözüme kavuşturmaktadır. Ancak GDPR m. 79 ile tanınan hak, denetim makamına başvuru hakkına ve bu yolun işleyişine halel getirmeksizin, kişilik haklarını korumak adına doğrudan veri sorumlusuna veya işleyene dava açabilme olanağı da sağlamaktadır[397].

KVKK açısından da şikayet hakkı 14. maddede düzenlenmiş olup veri sorumlusuna yapılan "başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi" hallerinde ileri sürülebilecektir. KVKK kapsamındaki şikayet hakkına ilişkin usul ve esaslar detaylı olarak "Hakların Kullanılması" başlığı altında açıklanacağı için, şimdilik söz konusu kısma atıf yapmakla yetinilecektir.

---

[396] GDPR 129 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-129/, (E.T. 27.11.2023).

[397] Waltraut Kotschy, "Article 79. Right to an effective judicial remedy against a controller or processor", **The EU General Data Protection Regulation (GDPR): A Commentary**, (Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler), Oxford University Press, Croydon, 2020, (Article 79), s. 1139.

K. Tazminat Hakkı

1. Tazminat Hakkının Kapsamı, Esasları ve Uygulanma Usulü

Tazminat hakkı, kişisel verileri ihlal edilen kişiye; itiraz, silme ve diğer haklarının kullanımıyla giderilemeyecek zararlarının karşılanması konusunda bir güvence sağlamaktadır. Böylece veri öznesine tanınan hakların ve açık rızayı geri alma olanağının ötesine uzanan bir bireysel kontrol mekanizması da verilmiş bulunmaktadır[398]. Her ne kadar genel hükümlere göre hakları ihlal edilen veri öznesinin maddi veya manevi tazminat isteme hakkı olsa da, veri koruma kurallarını etkili kılmak için ilgili kişiye GDPR ve KVKK ile de özel olarak ve doğrudan zararlarının giderilmesini isteme hakkı tanınmıştır. Tazminat sorumluluğu sayesinde, veri sorumluları; yasal düzenlemelere uymaya, güvenlik önlemlerini artırmaya ve kişilerin haklarına saygı göstermeye teşvik edilmektedir.

GDPR açısından özel olarak ve doğrudan tazminat hakkı tanınmasının önemi daha büyüktür. Zira ulusal hukuka aktarılması gerekmeden doğrudan uygulanabilen ve bağlayıcı nitelikteki bir tüzük hükmüyle bu hakkın öngörülmesi, Birlik ülkeleri arasında yeknesak uygulamalar gelişmesini sağlayacaktır. Ayrıca düzenlemeyle, veri sorumlusu ve veri işleyene açıkça sözleşme dışı sorumluluk yüklenmiş, detaylı bir şekilde tazminat hakkının esasları ortaya konulmuştur. Öncelikle GDPR'nin herhangi bir hükmünün ihlali üzerine, maddi veya manevi zarara uğrayan herhangi birinin, yaşanan zarara ilişkin olarak tazminat talep edebileceği belirtilmiştir (GDPR m. 82/1). Madde hükmünden anlaşılacağı üzere, sadece veri özneleri değil; zarar gören herkesin bu talepte bulunabileceği ifade edilmiştir. Hem ihlalin niteliği açısından hem de ihlalden etkilenen kişinin kimliği açısından oldukça geniş bir çerçeve çizilmiştir. Ayrıca hüküm, ihlal ile zarar arasındaki illiyet bağını da sağlamıştır[399].

GDPR uyarınca tazminat sorumluluğundan bahsedildiğinde kusur şartı aranmadığı görülmektedir. Gerçekten de işleme faaliyetine dahli olan herhangi bir veri sorumlusu, söz konusu faaliyetin neden olduğu zarardan sorumlu kılınmıştır (GDPR

[398] 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), Oxford University Press, Croydon, 2020, (Right to Compensation), s. 1164.

[399] Zanfir-Fortuna, Right to Compensation, s. 1175.

m. 82/2, c.1). Yani tazminat sorumluluğunun doğması için GDPR'nin herhangi bir hükmünün ihlal edilmesi ve söz konusu ihlal nedeniyle bir zararın meydana gelmesi yeterlidir. Bu durum ayrıca GDPR m. 5/2'de öngörülmüş "hesap verebilirlik" ilkesini de tamamlar niteliktedir. Zira veri sorumlusu kişisel verilerin işlenmesine ilişkin ilkelere kast, ihmal veya hatadan bağımsız olarak uygun davranmakla yükümlüdür[400]. Veri işleyenler içinse durum veri sorumlularından biraz daha farklıdır. Veri işleyenler sadece; GDPR'nin "kendilerine yönelik yükümlülüklere uyum göstermediği ve veri sorumlusunun hukuka uygun talimatlarının dışında veya bu talimatlara aykırı hareket ettiği hallerde", işleme faaliyetinin sebep olduğu zarardan sorumludur (GDPR m. 82/2).

GDPR tazminat hakkı kapsamında çizdiği geniş çerçeveye rağmen veri sorumluları ve veri işleyenlerin sorumluluktan kurtulmaya yönelik bir imkan sağlamamış değildir. Gerçekten de zarara sebep olan olaydan hiçbir şekilde sorumlu olmadığına dair kurtuluş kanıtı getirilmesi halinde tazminat sorumluluğu kalkacaktır (GDPR m. 82/3). Örneğin veri işleyen tabi olduğu veri sorumlusunun talimatlarına göre hareket ettiğini kanıtlarsa, sorumluluktan kurtulacaktır. Örneği somutlaştırmak gerekirse, bir bulut bilişim hizmet sağlayıcısı (veri işleyen), müşterisi olan bir e-ticaret şirketinin (veri sorumlusu) müşteri verilerini işliyor diyelim. Veri işleyen verilerin tutulduğu sistemin güvenliğinin sağlanması için veri sorumlusuna iki seçenek sunmuş olsun. Birincisinin endüstri standartlarına uygun güçlü şifreleme yöntemleri ve güvenlik duvarları ile korunacak pahalı bir sistem, ikincisinin ise verilerin temel güvenlik önlemleriyle korunacağı daha az maliyetli bir sistem olduğunu varsayalım. Şirket de yaşadığı bütçe kısıtlamaları nedeniyle daha ekonomik olan seçeneği tercih etmiş olsun ve bulut bilişim hizmet sağlayıcısına bu yönde talimat versin. Düşük güvenlik seviyesi nedeniyle bir güvenlik ihlali meydana geldiğinde, veri işleyen tamamen veri sorumlusunun talimatlarına göre hareket ettiğini ve güvenlik sistemi seçimi kapsamında vuku bulabilecek risklere karşı bütün tedbirleri alıp gerekli uyarıları yaptığını kanıtlarsa artık meydana gelen zarardan sorumlu olmayacaktır. Benzer şekilde veri sorumlusu da zarara yol açan ihlalin kendisinden değil de operasyonel anlamda birlikte hareket etmediği başka bir veri sorumlusunun hareketlerinden kaynaklandığını kanıtlayabilirse tazminat ödemek zorunda

[400] Zanfir-Fortuna, Right to Compensation, s. 1176.

kalmayacaktır[401]. Örneğin, X Şirketi ve Y Şirketi, müşterilerinin verilerini kendilerine ait veri tabanlarında tutan, birbirinden bağımsız iki şirket olsun ve birer hafta arayla veri sızıntısı yaşansın. A kişisinin kişisel bilgileri de hem X Şirketi'nin hem de Y Şirketi'nin müşteri listelerinde bulunsun. Verileri kullanılarak dolandırılan A, uğradığı zararın nedeninin X Şirketi bünyesinde meydana gelen sızıntı olduğunu düşünüp tazminat talep etmiş olsun. Fakat esasen verileri Y Şirketi'ndeki güvenlik ihlali esnasında sızmış olsun. Bu durumda X Şirketi verileri sızan müşterilerin arasında, A kişisinin olmadığını kanıtlayarak tazminat sorumluluğundan kurtulma imkanına sahip olacaktır.

Veri sorumluları ve veri işleyenler, zarara yol açan işleme faaliyetinden sorumlu oldukları ölçüde, müştereken ve müteselsilen sorumlu tutulmuşlardır. Zarardan sorumlu olan, ayrı ayrı birden fazla veri sorumlusu veya veri işleyen olabileceği gibi; veri sorumlusu ve veri işleyen sıfatlarının birleştiği kişi de olabilir. Bu hükmün amacı, kişinin zararının tam ve etkili bir şekilde karşılanmasıdır (GDPR m. 82/4). Tazminat, zararın tam ve etkili karşılanması şartıyla, her bir veri sorumlusu ve/veya işleyenin söz konusu faaliyetten kaynaklanan zarara katkı payı ölçüsünde bölüştürülebilir[402]. Eğer veri sorumlusu veya veri işleyenlerden biri, meydana gelen zararı eksiksiz bir şekilde tazmin etmişse, aynı işleme faaliyetine müdahil olan diğer sorumlu veya işleyenlere rücu edebilir. Rücu hakkı sadece diğerlerinin zarardaki payı ölçüsünde kullanılabilir (GDPR m. 82/5).

KVKK de verilerinin hukuka aykırı şekilde işlenmesi halinde zarar gören kişilerin tazminat hakkına ilişkin bir düzenleme içermektedir (m. 11/1-ğ). Ayrıca söz konusu tazminatın genel hükümlere göre ileri sürüleceği de hüküm altına alınmıştır (m. 14/3). Kanunda belirtilen ve veri işleme sürecine hakim olması gereken ilkelere aykırı olarak yapılan işleme faaliyetleri, kişilerin zarara uğraması mümkündür. Örneğin, kişinin açık rızasının yokluğunda yapılan işlemeler, ilgililerin kişilik haklarını ihlal edebilir. Kişinin açık rızasına gerek olmaksızın kişisel verilerinin işlenmesinin imkanlı olduğu haller bunun bir istisnasını teşkil edecektir (m. 5/2). Ancak hem açık rızanın hem de bu durumlardan birinin olmaması halinde, söz konusu işleme faaliyeti yine hukuka aykırı olacaktır. Hassas veriler yalnızca açık rızaya dayalı

[401] Zanfir-Fortuna, Right to Compensation, s. 1176.
[402] GDPR 146 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-146/, (E.T. 27.11.2023).

olarak veya kanunlarda öngörülen belirli hallerin varlığında işlenmezse, nitelikleri gereği etkisi büyük zararlara yol açabilir (m. 6). Yine, uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde verilerin silinmemesi, yok edilmemesi veya anonimleştirilmemesi durumunda, hukuka aykırı işleme mevcut olacaktır (m. 8). Kanunda öngörülmüş kurallara aykırı hareket edilmesi suretiyle yasal olmayan işleme örneklerini çoğaltmak mümkündür.

Ortaya çıkan zarar maddi veya manevi olabilir. Bu zarara ilişkin tazminat talepleri, hukuka aykırılığın dayanabileceği; kişilik hakkını koruyan TMK (m. 25), haksız fiilden (m. 49 vd.) veya sözleşmeye aykırılıktan (m. 112 vd.) kaynaklanan tazminat sorumluluğu gibi TBK hükümlerine dayanılarak yapılabilir[403]. Burada GDPR'den farklı olarak kusur şartının varlığı aranmaktadır. Veri sorumlusu gerçek kişi veya özel hukuk tüzel kişisiyse, adli yargıda; kamu hukuku tüzel kişisiyse de idari yargıda tam yargı davası yoluyla tazminat talepleri ileri sürülebilir (TBK m. 55/2). Yine GDPR'den farklı olarak veri işleyen, veri sorumlusu gibi açıkça tazminat taleplerinden sorumlu tutulmamıştır. Fakat KVKK m. 12/2 uyarınca veri güvenliğine ilişkin tedbirlerin alınması hususunda, veri sorumlusuyla birlikte sorumlu tutulduğu için tazminat sorumluluğu olduğu ileri sürülebilecektir[404].

Tazminat talebinde bulunacak ilgili kişinin, öncelikle veri sorumlusuna veya Kişisel Verileri Koruma Kurulu'na başvurması zorunlu değildir[405]. Nitekim Kurul da bir kararında[406], verilerinin hukuka aykırı olarak işlendiği iddiasıyla banka olan veri sorumlusundan tazminat talebinde bulunan fakat talebine olumlu yanıt alınmayan ilgili kişinin başvurusu kapsamında yapılacak bir işlem bulunmadığına karar vermiştir. Zira tazminat talebinin KVKK m. 14/3 hükmü uyarınca genel mahkemeler huzurunda ileri sürülmesi gerekmektedir. Tazminat talepleri konusunda yapılan başvurular Kişisel Verileri Koruma Kurulu'nun görev alanına girmemektedir.

---

[403] Emel Badur ve Nesibe Kurt Konca, "Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini ve Görevli Mahkeme", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Sayı: Cilt: 13, Sayı: 2, 2022, s. 482.

[404] Badur ve Kurt Konca, s. 484.

[405] Badur ve Kurt Konca, s. 483; Dülger, s. 509.

[406] Kişisel Verileri Koruma Kurulu, 16.01.2020 tarihli ve 2020/41 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6714/2020-41, (E.T. 27.11.2023).

2. Tazminat Hakkına İlişkin Örnek Kararlar

ABAD yakın tarihli bir kararında[407], kişisel verilerin hukuka aykırı olarak işlenmesinden kaynaklı olarak tazminat talebiyle ilgili bir hüküm kurmuştur. Veri sorumlusu olan posta hizmeti şirketi, Avusturya vatandaşlarının siyasi eğilimlerini tahmin etmek için çeşitli sosyal ve demografik kriterleri analiz eden bir algoritma kullanmakta ve bu analizlerden yola çıkarak "hedef grup adresleri" oluşturup bunları üçüncü kişilere satarak, bu üçüncü kişilerin vatandaşları hedef alan siyasi reklamlar yapmasına olanak sağlamaktadır. Karara ilişkin olayda ise, veri sorumlusunun algoritması başvurucunun belirli bir Avusturya siyasi partisine yüksek düzeyde yakınlığı olduğunu tahmin etmiştir. Veri öznesi kişisel verilerinin bu amaçla işlenmesine izin vermediğini, üçüncü kişilerle paylaşılmamış olsa bile veri sorumlusunun veri tabanında bu bilginin muhafaza edilmesinin kendisinde ağır bir üzüntüye neden olduğunu ve yaşadığı teşhir duygusunun kendisini duygusal olarak sarstığını belirtmiştir. Kararda tazminat talebin karşılanabilmesi için üç tane şartın varlığı aranmıştır: Veri sorumlusunu etkileyen bir zararın meydana gelmesi, GDPR'nin bir hükmünün ihlal edilmesi ve söz konusu ihlalle zarar arasında illiyet bağının olması. Anlaşılacağı üzere, zarar olmadığı sürece bir ihlalin meydana gelmesi tazminata hükmedilmesine yeterli olmayacaktır. Bu durumda idari para cezası uygulanmakla yetinilebilir. Benzer şekilde, GDPR'ye göre manevi tazminat talep edilebilmesi için meydana gelen zararın belirli bir eşiği aşmasına da gerek yoktur. Etkisinin büyüklüğü fark etmeksizin her zarar için hakkaniyete uygun miktarda tazminata hükmedilmesi mümkündür.

Yargıtay'ın da önüne kişisel verilerin hukuka aykırı olarak işlenmesine yönelik bir dosya gelmiştir[408]. Dava konusu olayda, ilgili kişi davacının kimlik ve fatura bilgileri izni ve haberi olmaksızın kullanılarak bir iletişim şirketinden ilgili kişi adına hat çıkarılmıştır. Söz konusu telefon hattına ait faturalarının ödenmemesi dolayısıyla ilgili kişiye yönelik icra takibi başlatılmıştır. İlgili kişi olayla ilgili hukuki süreci takip etmesi için bir avukat yardımından yararlanmıştır. Bu nedenle davalı olan iletişim

[407] ABAD, 04.05.2023 tarih ve C-300/21 numaralı Österreichische Post kararı, https://curia.europa.eu/juris/liste.jsf?lgrec=fr&td=%3BALL&language=en&num=C-300/21&jur=C, (E.T. 27.11.2023).

[408] Yargıtay 4. Hukuk Dairesi, 17.06.2021 tarih ve E. 2021/724, K. 202/3272 kararı, https://kararara ma.yargitay.gov.tr/, (E.T. 27.11.2023).

şirketi ve bayisinden; ödediği avukatlık ücreti nedeniyle maddi, yaşadığı sıkıntılar nedeniyle de manevi tazminat talebinde bulunmuştur. Yüksek mahkeme, iletişim şirketini haksız fiili gerçekleştiren bayinin eylemlerinden sorumlu tutmuş ve bayi seçimi ve denetimi konusunda özenli davranmadığı için kusurlu bulmuştur. Kişinin rızası olmaksızın kişisel verilerini ele geçirip kullanarak hat açan bayi zaten kusurludur. Bu nedenle her iki davalı, müteselsil olarak hem maddi hem manevi tazminattan sorumlu tutulmuştur.

III. HAKLARIN KULLANILMASI VE KISITLANMASI

A. Hakların Kullanılması

GDPR m. 12'de veri öznelerinin haklarının kullanılması sürecine hakim olacak prosedürler düzenlenmiştir. Söz konusu düzenlemeyle, hem hakların etkili bir şekilde ileri sürülmesi sağlanmakta hem de veri sorumlularının efektif bir şekilde çalışmasına olanak sağlanmaktadır. Veri öznelerinin, kişisel verilerinin geleceğini belirlemesinde yakalayacağı başarı, doğrudan kendilerine bunu nasıl sağlanabileceğine ilişkin bilgilerin sunulma ve iletilme biçimine bağlıdır[409].

Veri öznesine, özellikle de veri öznesi bir çocuksa; bilginin "öz, şeffaf, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanılarak" verilmesi gerekmektedir (GDPR m. 12/1). İlk olarak bilgilendirmenin içeriği, öz yani kısa ve kapsamlı olmalıdır. Dolayısıyla veri öznesine sağlanan bilgiler, gereksiz kelimeler olmadan ve uygun düzeyde ayrıntıyla, veri öznesinin kafasının karışmasına mahal vermeyecek şekilde kaleme alınmalıdır. Bu sayede bilgilendirme metni, daha açık ve dikkat dağılmadan okunabilir hale gelir. İkinci olarak, bilgilendirme metninin anlaşılır olması gerekmektedir. Yani karmaşık cümle ve dil yapılarından, soyut ve muğlak ifadelerden kaçınılmalıdır. Örneğin, "Kişisel verilerinizi yeni hizmetler geliştirmek için kullanabiliriz" ifadesi, söz konusu hizmetlerin ne olduğu ve geliştirmekte nasıl yardımcı olacağına dair herhangi bir bilgi içermediği için anlaşılır değildir. Fakat

[409] Radim Polčák, "Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject", **The EU General Data Protection Regulation (GDPR): A Commentary**, (Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler), Oxford University Press, Croydon, 2020, s. 402.

"İlginizi çekeceğini düşündüğümüz diğer ürünler için size önerilerde bulunmak amacıyla alışveriş geçmişinizi saklayacağız ve daha önce satın aldığınız ürünlerin ayrıntılarını kullanacağız" ifadesi muğlak bir ifade içermez.[410] Bu durumda veri öznesinin yetişkin mi yoksa çocuk mu olduğu da özellikle önemlidir. Zira yaş itibarıyla hareketinin sonuçlarını anlama yeteneği çocuklarda daha düşük olduğundan, çocuklara yapılan bilgilendirmelerde bir yetişkine göre teknik terimlerden arındırılmış ve basit ifadeler kullanılması gerektiği tartışılmaz bir gerçektir. Fakat yetişkinler için de anlaşılırlık kriteri yüksek tutulmamalıdır. Zira kişisel verilerin korunması konusu, normal bireyler için de son derece karmaşık ve teknik bir konu olabilir. Her halükarda veri öznesine sağlanan bilgiler aşırı derecede hukuki, teknik veya uzmanlık gerektiren bir dil veya jargon içermemelidir[411]. Ayrıca bilgilerin başka dillere çevrilmesi halinde, veri sorumlusu bütün tercümelerin doğru olmasını ve yerelleştirilmesini sağlamalıdır. Üçüncü husus olarak, bilgilendirmenin içeriğinin kolayca erişilebilir olması da gerekmektedir. Bu nedenle, GDPR m. 12/1'de bilgilerin "yazılı olarak veya uygun olduğu hallerde, elektronik yollar da dahil olmak üzere diğer yollarla" sağlanması hüküm altına alınmıştır. Gerçekten de "Söz uçar, yazı kalır." mantığından hareketle, yazılı bilgilerin daha kalıcı ve ihtiyaç halinde bu bilgilere ulaşmanın kolay olacağını söylemek mümkündür. Özellikle de gelişen teknoloji sebebiyle kişi, dünyanın diğer ucunda olsa da kendisine gönderilen bir elektronik iletiyi yahut veri işleme faaliyetini yürüten kişinin internet sitesindeki gizlilik politikasını içeren gönderiyi istediği zaman ve sayıda okuma şansına sahiptir. Yahut kişinin verileri bir mobil uygulama (app) üzerinden işleniyorsa, gerekli bilgilendirmeler uygun zamanlarda bildirim şeklinde de gönderilebilir[412]. Ayrıca bilgilendirmenin yazılı bir şekilde yapılması, veri sorumlusunun bilgilendirme yükümlülüğünü yerine getirdiğine dair kanıt teşkil edecektir. Ancak bu husus, bilgilendirmenin sözlü olarak yapılamayacağı anlamına

[410] Article 29 Data Protection Working Party, "Guidelines on transparency under Regulation 2016/679", **Avrupa Komisyonu Web Sitesi**, 2018, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/transparency_en, (E.T. 08.12.2023), (Transparency), s. 9.

[411] Article 29 Data Protection Working Party, Transparency, s. 10.

[412] Future of Privacy Forum and the Center for Democracy & Technology, Best Practices for Mobile Application Developers, **Future of Privacy Forum Web Sitesi**, 2018, https://cdt.org/wp-content/uploads/pdfs/Best-Practices-Mobile-App-Developers.pdf, (E.T. 08.12.2023), s. 3; Mobil uygulamalarda bilgilendirme yükümlülüğünün nasıl yerine getirebileceğine ilişkin detaylı bilgi için ayrıca bkz. Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", **Avrupa Komisyonu Web Sitesi**, 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf, (E.T. 08.12.2023), (Opinion 02/2013), s. 23.

gelmez. Nitekim veri öznesi talep ederse, bilgiler sözlü olarak da sağlanabilir. Ancak bu durumda veri öznesinin kimliğinin başka şekillerle doğrulanması gerekmektedir (GDPR m. 12/1). Son olarak bilgilendirmenin içeriği şeffaf olmalıdır. Veri işleme sürecine hakim olan yaklaşımlardan biri olan bu ilke, aslında yukarıda açıklanan hususların tamamını kapsar; yani kişisel verilerin işlenmesine ilişkin olarak sağlanacak tüm bilgilerin ve kurulacak diyalogların kolayca erişilebilir ve anlaşılır olmasını gerektirmekle beraber, bu süreçte açık ve anlaşılır bir dil kullanılmasını şart koşar[413].

Bilgilendirme yükümlülüğünün yazılı, elektronik veya koşulları oluşmuşsa sözlü olarak yerine getirilebilmesinin yanı sıra, "standartlaştırılmış görsel semboller" olarak adlandırılan sembollerle de yerine getirilebileceği belirtilmiştir. Böylece anlatılmak istenen işlem, bir çırpıda ve bilgilendirme yükümlülüğünün yerine getirilmesinde uyulması gereken usullere uyularak anlatılabilecektir (GDPR m. 12/7). Örneğin, bir e-ticaret sitesi, müşterilerine kişisel verilerin korunmasıyla ilgili bilgi vermek için web sitesinde "kilit" sembolü kullanabilir. Bu sembol, verilerin güvende olduğunu göstereceğinden, kullanıcılar verilmek istenen mesajı açıkça anlayabilir[414]. "Simgelerin elektronik olarak sunulduğu hallerde, simgeler makine tarafından okunabilecek şekilde" sağlanmalıdır (GDPR m. 12/7).

Veri sorumlusu, veri öznesinin haklarını kullanmasına kolaylık sağlamakla yükümlü kılınmıştır (GDPR m. 12/2). Dolayısıyla veri öznelerinin talepleri değerlendirilirken amaç, her zaman hakkın en geniş ve etkili şekilde kullanılmasına izin verecek uygulamalarda bulunmak olmalıdır[415]. Bir başka deyişle hakların kullanılmasını kısıtlayacak ya da engelleyecek davranışlardan kaçınılmalıdır[416]. Her ne kadar veri sorumlusunun, talepte[417] bulunan muhtemel veri öznesinin kimliğini teşhis edemediği durumlarda, söz konusu talebi yerine getirmekle yükümlü olmasa da; teşhis edemediğini ortaya koyamadığı sürece "hakların kullanılması yönündeki talebini işleme koymayı reddedemez" (GDPR m. 12/2). Veri öznesinin söz konusu haklarını kullanmak amacıyla kimliğinin belirlenmesini mümkün kılan ek bilgiler

---

413 GDPR 39 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-39/, (E.T. 13.12.2023).

414 Kişisel Verileri Koruma Kurumu'nun aydınlatma için kullanılacak sembol, işaret ve ikonları için lütfen bkz. Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğü, s. 21.

415 European Data Protection Board, Right of Access, s. 17.

416 Polčák, s. 410.

417 Söz konusu taleplerin GDPR'nin 15-20. maddeleri kapsamında yapılması gerekmektedir (GDPR m. 11/2).

sunarak veri sorumlusunun yükümlülüğünü yerine getirmesini sağlayabilir (GDPR m. 11/2). Veri sorumlusu, veri öznesinin bu yolu seçmesi durumunda teşhis için istenen ek bilgilerin ne olduğunu veri öznesine bildirmelidir[418]. Bunu yaparken gereksiz veya aşırı taleplerde bulunmaması gerekmektedir. Aksi takdirde veri öznesinin haklarını kullanmasına kolaylık sağlama yükümlülüğü ihlal edilmiş olur. Veri sorumlusunun "talepte bulunan gerçek kişinin kimliği ile ilgili makul şüphelerinin bulunduğu hallerde" ise, veri öznesinin hüviyetinin doğrulanması için ek bilgi isteminde bulunabilir (GDPR m. 12/6). Ancak bu durum kişi ile verileri arasındaki bağı kurmak için alakasız veya gereksiz olan kişisel verilerin toplanmasına sebep olmamalıdır.

GDPR m. 15-22'de düzenlenen hakların kullanılmasına ilişkin bir taleple ilgili olarak gerçekleştirilen işleme ilişkin bilgiler, "herhangi bir gecikmeye mahal vermeksizin ve her halükarda talebin alınmasından itibaren bir ay içerisinde" veri öznesine sağlanır. Eğer veri sorumlusunun normal şartlar altında daha kısa bir süre (örneğin bir gün veya bir hafta) içinde harekete geçmesi mümkünse, bir ay boyunca beklememelidir. Süre talebin alınmasıyla yani veri sorumlusunun dikkatine sunulmasıyla başlar. Bu bir aylık süre, "gerekmesi halinde, taleplerin karmaşıklığı ve sayısı dikkate alınarak iki ay daha uzatılabilir". Örneğin, geniş çaplı bir veri sızıntısının yaşandığı durumlarda, başvuru sayısı çok olacağı için bu hüküm uygulanabilir. Fakat bunun söz konusu olduğu durumlarda, veri sorumlusu "talebin alınmasından itibaren bir ay içerisinde söz konusu süre uzatımıyla birlikte gecikme sebeplerini" veri öznesine bildirmelidir. "Veri öznesinin talebi elektronik yollarla yapması halinde bilgiler, veri öznesi tarafından aksi talep edilmedikçe, mümkünse elektronik yollarla sağlanır" (GDPR m. 12/3). Yani elektronik ortamda yanıt verilmesi veri sorumlusu açısından mutlak bir yükümlülük değildir. Örneğin, veri öznesi hakkını e-posta ile ileri sürse bile yanıtın kendisine fiziksel olarak posta yoluyla gönderilmesini isteyebilir.

Veri sorumlusu, veri öznesinin talebi ile ilgili işlem yapmazsa "herhangi bir gecikmeye mahal vermeden ve talebin alınmasından itibaren en geç bir ay içerisinde" veri öznesine bilgi vermelidir. Bu bilgilendirme; işlem yapmama sebepleri, bir denetim makamına şikayette bulunma ve bir kanun yoluna başvurma olanaklarını içermelidir (GDPR m. 12/4). Örneğin, veri öznesi olduğunu düşünen kişinin, veri

[418] Veri sorumlusu, veri öznesini ek bilgi sağlamaya zorlayamaz. Ek bilgi sağlayıp sağlamama kararı tamamen veri öznesine aittir. (GDPR 57 No'lu Gerekçe, **Avrupa Birliği GDPR Resmi Web Sitesi**, https://gdpr-info.eu/recitals/no-57/, (E.T. 13.12.2023)).

sorumlusu tarafından hiçbir verisi işlenmediği halde erişim başvurusu yapmışsa, bu durumda erişilecek kişisel veri bulunmadığı için talep hakkında işlem yapılmayabilir. Yahut üçüncü kişilerin temel hak ve özgürlüklerini etkileyen bir durum varsa, talebin gereği yerine getirilmeyebilir.

GDPR m. 13-22'de düzenlenen haklarla ilgili olarak veri sorumlusunca yapılan "her türlü bildirim ve gerçekleştirilen her türlü işlem" ücretsiz olmalıdır (GDPR m. 12/5). Bunun tek istisnası, veri öznesinin taleplerinin asılsız veya ölçüsüz olduğunun açıkça anlaşıldığı hallerdir. Örneğin, taleplerin cevaplanması beklenmeden sürekli tekrarlanması bu kapsama girer. Bu durumda veri sorumlusu iki şekilde davranabilir: Ya talep edilen bilgilerin sağlanması veya işlemin gerçekleştirilmesine ilişkin idari masrafları dikkate alarak cüzi bir ücret talep edebilir ya da taleple ilgili işlem yapmayı reddedebilir. Bu hükmün kötüye kullanılmasını engellemek için veri sorumlusuna söz konusu talebin açık bir şekilde asılsız veya ölçüsüz olduğunu kanıtlama yükümlülüğü getirilmiştir (GDPR m. 12/5). Talebin aşırı olup olmadığının değerlendirilmesinde; verilerin ne sıklıkla değiştiği (iki talep arasında yeni veriler işlenip işlenmediği) veya müteakip taleplerin öncekiyle aynı içerikte mi olduğu (hep aynı veriler için mi talepte bulunulduğu) gibi ölçütler kullanılabilir[419]. Veri sorumlusunun talebi yerine getirmesinin çok fazla zaman ve çaba gerektirmesi, bir talebi tek başına aşırı kılmaya yetmez. Benzer şekilde veri öznesinin talebi yaparken uygunsuz veya saygısız bir dil kullanması, veri öznesinin talepte bulunurken herhangi bir gerekçe göstermemesi veya veri sorumlusunun yapılan talebin anlamsız olduğunu düşünmesi de bu kapsama dahildir[420]. Dikkat edilmelidir ki veri sorumlusu tarafından ücret, ancak talebin asılsız veya ölçüsüz olduğu hallerde istenebilir. Aksi takdirde veri öznesinin haklarını ileri sürmek amacıyla yaptığı talepler ücretsiz olarak yerine getirilecektir. Bu kuralın aksine yönelik olarak yapılmış sözleşme hükümleri geçerli değildir. Ölçüsüz veya aşırıya kaçan taleplerle ilgili olarak makul bir ücret isteneceği, talep yerine getirilmeden önce veri öznesine bildirilmelidir. Böylece talebi geri alma hakkı sağlanacaktır[421].

Hukukumuz açısından ise ilgili kişinin haklarını kullanmak üzere veri sorumlusuna başvuru, yazılı olarak veya Kişisel Verileri Koruma Kurulu'nun belirleyeceği diğer yöntemlerle iletilmesiyle yapılmaktadır (KVKK m. 13/1). Bu

[419] European Data Protection Board, Right of Access, s. 57.
[420] European Data Protection Board, Right of Access, s. 58.
[421] European Data Protection Board, Right of Access, s. 59.

konuda çıkarılan Tebliğ[422] uyarınca, kişisel verisi işlenen gerçek kişiler, veri sorumlusuna başvuru hakkına sahiptir. Bu haktan yararlanmak için başvuruların Türkçe yapılması zorunlu tutulmuştur (Tebliğ m. 4). İlgili kişi kanunda belirtilen hakları kapsamında taleplerini; "yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla" veri sorumlusuna iletmelidir (Tebliğ m. 5/1). Kişisel Verileri Koruma Kurulu bir kararında[423], veri sorumlusu olan şirkete yapılan başvurunun kabul edilmeyip hüviyetin doğrulanabilmesi için yalnızca noter aracılığıyla ya da elektronik imza ile başvuru yapılabileceğinin iletilmesini, "mevzuatta öngörülmeyen maddi bir külfet getirilmesi ve ilgili kişinin bu şekilde yanlış yönlendirilmesi" olarak yorumlayıp başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırma yükümlülüğünün ihlali olduğuna karar vermiştir.

İlgili kişi tarafından başvuruda bulunması zorunlu olan unsurlar şunlardır: "Ad, soyad ve başvuru yazılı ise imza, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirime esas elektronik posta adresi, telefon ve faks numarası, talep konusu" (Tebliğ m. 5/2). "Konuya ilişkin bilgi ve belgeler de başvuruya eklenir" (Tebliğ m. 5/3). Veri sorumlusu başvuranın gerçekten ilgili kişi olup olmadığını teyit edebilmek için birtakım ek bilgiler talep edebilir. Ancak bu durumda ölçülü davranmalı, gereğinden fazla sayıda ve hassas nitelikte olabilecek veriler talep etmemeye özen göstermelidir. Kurulun bir kararında da bu hususa vurgu yapılmış; ilgili kişinin, din ve kan grubu gibi özel nitelikli kişisel verilerini de ihtiva eden arkalı önlü kimlik fotokopisinin talep edilmesi, KVKK m. 4/1-ç'de yer alan ilkeye aykırılık olarak değerlendirilmiştir[424]. "Yazılı başvurularda, veri sorumlusuna veya temsilcisine evrakın tebliğ edildiği tarih, başvuru tarihidir" (Tebliğ

[422] 10.03.2018 tarihli Resmi Gazete'de yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, **Resmi Gazete**, https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm, (E.T. 14.12.2023).

[423] Kişisel Verileri Koruma Kurulu, 01.10.2019 tarihli ve 2019/294 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6556/2019-294, (E.T. 15.12.2023).

[424] Kişisel Verileri Koruma Kurulu, 01.10.2019 tarihli ve 2019/296 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6557/2019-296, (E.T. 15.12.2023).

m. 5/4). "Diğer yöntemlerle yapılan başvurularda; başvurunun veri sorumlusuna ulaştığı tarih, başvuru tarihi olarak kabul edilir" (Tebliğ m. 5/5).

"Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır" (KVKK m. 13/2). GDPR'nin aksine veri sorumlusunun cevap süresinin uzatılabileceğine ilişkin bir hüküm mevzuatta yer almamaktadır. Bu nedenle, başvuru sayısının fazlalığı vb. hangi sebeple olursa olsun, veri sorumlusunun bu süreye sadık kalması gerektiği sonucuna varmak gerekmektedir. Başvurunun süresinde cevaplanmamasının direkt sonucu idari para cezası uygulanması değildir. Kişisel Verileri Koruma Kurulu önüne gelen bir şikayette, veri sorumlusunun söz konusu kurala uygun olarak hareket etmesi yönünde uyarıda bulunulmasına ve ilgili kişiye cevap verilerek bu hususta kendilerine bilgi verilmesine karar vermiştir[425]. Ancak bu kararın gereğinin yerine getirilmemesi sonucunda, veri sorumlusu hakkında KVVK m. 18/1-c hükmünce idari para cezası uygulanabilmektedir.

İşlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifedeki ücret alınabilir (KVKK m. 13/2). İlgili Tebliğ'e göre; ilgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir (Tebliğ m. 7/1)."Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez (Tebliğ m. 7/2). Ancak başvuru veri sorumlusunun kusurundan kaynaklanıyorsa alınan ücret ilgiliye iade edilir (Tebliğ m. 6/5).

Veri sorumlusu yapılan başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbiri almakla yükümlüdür (Tebliğ m. 6/1). Veri sorumlusu, başvuruyu kabul eder veya gerekçesini

[425] Kişisel Verileri Koruma Kurulu, 06.07.2021 tarihli ve 2021/666 sayılı kararı, https://www.kvkk.gov.tr/Icerik/7133/2021-666, (E.T. 15.12.2023). Bu duruma benzer başka bir karar da Fransa'nın veri koruma otoritesi olan Ulusal Bilişim ve Özgürlükler Komisyonu (CNIL) tarafından verilmiştir. Karara ilişkin olayda, ilgili kişi kendisine ait ve veri sorumlusu nezdinde kayıtlı olan iki müşteri hesabının silinmesi için başvuruda bulunmuştur. Ancak veri sorumlusu kimlik belgesini sunmadan başvuranın talebini yerine getirmeyi reddetmiştir. Fakat Komisyon kimlik belgesi ibraz edilmeksizin de başvurucunun kimliğini doğrulamanın mümkün olduğunu belirtmiştir. Zira kişinin müşteri hesaplarına yönlendirilecek bir bağlantı veya bildirimle kimliğinin doğrulanması sağlanabilecektir. Bu nedenle veri sorumluları, ilgili kişinin talebini değerlendirirken mümkün olan her türlü kolaylığı sağlamaya özen göstermelidir. (CNIL, 26.07.2020 tarihli redakte edilmiş kararı, https://edpb.europa.eu/system/files/2023-01/fr_2022-07_decisionpublic_redacted_2.pdf, (E.T. 29.12.2023)).

açıklayarak reddeder (Tebliğ m. 6/2). Ancak başvurunun hiç cevaplanmaması halinde, bu sessizliğin zımni ret olarak değerlendirilerek Kişisel Verileri Koruma Kurulu'na başvurmak mümkündür. Veri sorumlusu, cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir (Tebliğ m. 6/3). Kişisel Verileri Koruma Kurulu bir kararında[426] yapılan bildirimin şekli ile ilgili bir hüküm kurmuş ve veri ilgili kişinin, veri sorumlusu olan banka tarafından telefonla aranmak suretiyle bilgilendirilmesinin, KVKK m. 13 kapsamında usulüne uygun bir bildirim niteliğini haiz olmadığını belirterek kanun ve tebliğ hükümlerine uymada özenli davranması konusunda veri sorumlusuna talimat vermiştir. Kurul önüne gelen başka bir olayda ise bildirimin yapıldığı kişinin kimliği ile ilgili karar vermiştir. İlgili kişi eskiden çalıştığı veri sorumlusu üniversitenin akademik bölümüne verdiği dilekçesinin akıbeti hakkında 4982 Sayılı Kanun kapsamında bilgi almak istemiştir. Ancak üniversite, cevabı doğrudan ve sadece muhatabına vermek yerine, ilgili kişinin şu anda çalıştığı başka bir akademik bölümdeki herkese açık ve personele iletilen sıradan bir resmi yazı şeklinde iletmiştir. Kurul bu durumu, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirlerin alınmaması olarak yorumlamış ve başvurunun etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırma yükümlülüğüne aykırılık olarak nitelendirmiştir[427].

İlgili kişiye verilecek cevabın içermesi gereken zorunlar unsurlar şunlardır: Veri sorumlusu veya temsilcisine ait bilgiler, başvuru sahibinin adı ve soyadı, T.C. kimlik numarası, uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirime esas elektronik posta adresi, telefon ve faks numarası, talep konusu, veri sorumlusunun başvuruya ilişkin açıklamaları (Tebliğ m. 6/4). İlgili kişinin talebinin kabul edilmesi hâlinde, veri sorumlusunca talebin gereği en kısa sürede yerine getirilir ve ilgili kişiye bilgi verilir (Tebliğ m. 6/6). Zira kişisel veri işleme süreçlerine müdahale niteliği taşıyan silme ve düzeltme

[426] Kişisel Verileri Koruma Kurulu, 30.01.2020 tarihli ve 2020/78 sayılı kararı, https://kvkk.gov.tr/Icerik/6922/2020-78, (E.T. 15.12.2023).

[427] Kişisel Verileri Koruma Kurulu, 05.05.2020 tarihli ve 2020/336 sayılı kararı, https://www.kvkk.gov.tr/Icerik/6910/2020-336, (E.T. 15.12.2023).

talepleri bakımından hem talebin yerine getirilmesi hem de bilgi verilmesi hususu önemlidir[428].

Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her halde başvuru tarihinden itibaren altmış gün içinde Kurula şikayette bulunabilir (KVKK m. 14/1). Kurula başvurmak zorunlu bir başvuru yolu değildir; yani ihtiyari bir yoldur. Fakat Kurula başvurmak için öncesinde veri sorumlusuna başvurmuş olmak bir ön koşuldur (KVKK m. 14/2). KVKK m. 14/3 uyarınca, Kurula başvuru yapmak aynı zamanda genel hükümlere göre tazminat hakkının ileri sürülmesini engellemeyeceği gibi; Kurula karşı şikayet yoluna gidilmeksizin, sadece genel hükümlere göre tazminat yoluna başvurulması veya veri sorumlusunun idare olması halinde başvuruya verilen yanıta karşı idari yargıda iptal davası açılması da mümkündür[429]. Kişisel Verileri Koruma Kurumu bir idari kurum, bu kurumun karar organı olan Kişisel Verileri Koruma Kurulu'na yapılan başvurular da bir idari başvuru olduğu için Kurulun kararlarına karşı iptal ya da tam yargı davası açılabilir[430].

Kurula başvuruda, 3071 Sayılı Kanun[431] m. 6 dikkate alınmalıdır. Aksi takdirde veri sorumlunun yapacağı ihbar ve şikayetler, usulsüz başvuru olarak kabul edilip incelemeye alınmayacaktır (KVKK m. 15/2). Başvuru evrakında; dilekçe sahibinin adı-soyadı, imzası, iş veya ikametgah adresi, kendini vekille temsil ettiriyorsa vekaletnamenin kopyası, başvuruya ilişkin belgeler, şikayet konusu ve talebin açıkça izahının bulunması gerekir. Şikayet üzerine Kurul, "talebi inceleyerek ilgililere bir cevap verir. Şikayet tarihinden itibaren altmış gün içinde cevap verilmezse talep zımnen reddedilmiş sayılır" (KVKK m. 15/4). Yapılan inceleme sonucunda, ihlalin varlığının anlaşılması halinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu

---

[428] Şehriban İpek Aşıkoğlu, "İlgili Kişiler Tarafından Yapılan Başvuruların Cevaplanması Yükümlülüğü", **Kişisel Verilerin Korunmasına Akademik Bakış**, (Ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy), Arkadaş Basımevi, Ankara, 2023, s. 208.

[429] Eser Us Doğan, "Başvuru ve Şikâyet Usulleri ile Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü", **Kişisel Verilerin Korunmasına Akademik Bakış**, (Ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy), Arkadaş Basımevi, Ankara, 2023, s. 230.

[430] Us Doğan, s. 231.

[431] 10.11.1984 tarihli Resmi Gazete'de yayımlanan 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun, **Resmi Gazete**, https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=3071&MevzuatTur=1&MevzuatTertip=5, (E.T. 16.12.2023).

tarafından giderilmesine karar vererek ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilmelidir (KVKK m. 15/5). Eğer ihlal yaygın görülüyorsa, bu durumda mevzubahis konuda ilke kararı alıp yayınlar (KVKK m. 15/6). Telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması halinde, veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verilebilir (KVKK m. 15/7).

B. Hakların Kısıtlanması

Çoğu temel hak gibi, kişisel verilerin korunması hakkı da mutlak değildir. Belirli durumlarda, demokratik bir toplumdaki diğer meşru menfaatler gereği kısıtlanabilir. Fakat kısıtlamaların temel hak ve özgürlüklerin özüne saygı göstermesi, gerekli ve orantılı olması gereklidir. Bu, bir temel hakkın temel içeriğini ortadan kaldıracak kadar kapsamlı ve müdahaleci sınırlamaların haklı gösterilemeyeceği anlamına gelir. "Temel hak ve özgürlüklerin özüne saygı gösterilmesi" ile ifade edilmek istenen hakkın kullanılmasını son derece zorlaştırılmaması veya kullanılamaz hale getirilmemesidir. Her hakkın kişiye dokunulmaz, asgari bir alan güvencesi sunması gerekmektedir[432]. Hakkın amacına ulaşamayacak hale getirilmesi halinde sınırlamanın kamu yararına hizmet edip etmediğinin, gereklilik ve orantılılık kriterlerini karşılayıp karşılamadığının ayrıca değerlendirilmesine gerek olmaksızın, sınırlamanın hukuka aykırı olduğu değerlendirilmelidir[433]. "Gereklilik" ulaşılmak istenen amaç bakımından kısıtlamanın zorunluluğunu ifade etmektedir. Bir başka deyişle, söz konusu amaca daha hafif bir müdahale ile ulaşılamamalıdır[434]. "Orantılılık" ise, kısıtlama ile ulaşılmak istenen amaç arasında uygun bir dengenin kurulması gerekliliği anlamına gelir[435].

GDPR m. 23/1'de veri öznesinin haklarının şu durumlarla kısıtlanabileceği ifade edilmiştir:

> *Milli güvenlik, savunma, kamu güvenliği, kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dahil olmak üzere*

[432] Zühtü Arslan, "Temel Hak ve Özgürlüklerin Sınırlandırılması: Anayasa'nın 13. Maddesi Üzerine Bazı Düşünceler", **Anayasa Yargısı**, Cilt: 18, Sayı: 1, 2002, s. 144.
[433] Fundamental Rights Agency, s. 44.
[434] Kemal Gözler, **Türk Anayasa Hukuku Dersleri**, 24. Baskı, Ekin Kitabevi Yayınları, Bursa, 2019, s. 132.
[435] Gözler, s. 133.

suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesi, Birlik veya üye devletin önemli bir ekonomik veya mali çıkarına olmak üzere parasal hususlar ile bütçe ve vergilendirmeye ilişkin hususlar, halk sağlığı ve sosyal güvenlik de dahil genel kamu yararına yönelik diğer önemli hedefler, yargı bağımsızlığının ve adli süreçlerin korunması, düzenlenmiş mesleklere ilişkin etik kurallarının ihlalinin önlenmesi, soruşturulması, tespiti ve kovuşturulması, resmi yetkinin kullanımı ile bağlantılı bir izleme, denetleme veya düzenleme işlevi, veri öznesinin veya başkalarının haklarının ve özgürlüklerinin korunması, medeni hukuktan kaynaklanan taleplere ilişkin kararların icrası.

ABAD bir kararında[436], şirketi uzun süre önce iflas eden başvurucunun, iflasa ilişkin kaydın kamuya açık tutulan ticaret sicilinden silinmesi talebine ilişkin bir hüküm kurmuştur. Zira sicile başvuracak potansiyel müşterileri söz konusu kaydı görmesi halinde kendisiyle çalışmaktan vazgeçebilecek, bu da ekonomik durumunu zedeleyecektir. Fakat Divan başvurucunun eski şirketinin iflasına ilişkin bilgilerin kaldırılmasındaki ticari menfaati ile bu bilgilere erişimdeki kamu menfaati arasında bir denge gözetilmesi gerektiğini belirtmiştir. Anonim ve limited şirketler, üçüncü şahıslara karşı sadece şirketin malvarlığıyla sorumlu olduğu için kişilerin yatırım yapmadan önce bilinçli tercihler yapabilmesi daha önemlidir. Sicilin gözettiği meşru amacın önemi göz önüne alındığında, üçüncü kişilerin menfaatlerinin korunması ihtiyacı nedeniyle başvurucunun kişisel verisinin silinmesini talep etme hakkına sahip olmadığına karar verilmiştir.

Fakat GDPR m. 23/2 uyarınca veri öznelerine tanınan hakların kısıtlanmasına ilişkin yapılan yasa düzenlemelerde şu hususların öngörülmesi gerekmektedir:

İşlemenin veya işleme kategorilerinin amaçları, kişisel veri kategorileri, getirilen kısıtlamaların kapsamı, kötüye kullanım veya yasa dışı yollarla erişim veya aktarımın engellenmesine yönelik güvenceler, veri sorumlusu veya veri sorumlusu kategorilerinin belirlenmesi, işleme veya işleme kategorilerinin mahiyeti, kapsamı ve amaçları dikkate alınarak saklama süreleri ve uygulanabilir güvenceler, veri öznelerinin hakları ve özgürlüklerine yönelik riskler, kısıtlama amacına halel getirmemesi durumunda, veri öznelerinin kısıtlamayla ilgili bilgi sahibi olma hakkı.

Böylece veri öznelerine tanınan hakların kullanılmasının özüne dokunulmamış, varlığı anlamsızlaşmamış olacaktır. Ayrıca kısıtlamaların varlığı halinde de asgari birtakım güvenceler sağlanmış olacaktır.

[436] ABAD, 09.03.2017 tarih ve C-398/15 numaralı Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni kararı, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1512479438140&uri=CELEX:62015CJ0398, (E.T. 28.11.2023).

KVKK açısından ise ilgili kişilere sağlanan haklar ve güvencelere şu durumlarda istisnaların getirildiği görülmektedir:

> *Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi; resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi; millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi; millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi; soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi (KVKK m. 28/1).*

Ayrıca bilgilendirilme ve tazminat hakları haricindeki tüm haklar şu hallerde uygulanmayacaktır:

> *Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması, ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi, kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması, kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması (KVKK m. 28/2).*

KVKK'deki kısıtlamaların GDPR'deki düzenlemeyle çoğunlukla paralel olduğu görülmektedir. Bu nedenle mahiyetine uygun düştüğü ölçüde yapılan açıklamalar KVKK açısından da geçerlidir.

SONUÇ

Gelişen teknolojiye bağlı olarak artan bilgisayar ve internet kullanımı, kişisel verilerin de dijital ortama aktarılmasında ve dolayısıyla verilerin toplanması, saklanması ve analiz edilmesinde (kısaca işlenmesinde) büyük bir artışı meydana getirmiştir. Gerçekten de günümüzde mal ve hizmetlerin alım satımı, kamu hizmeti, sosyal hizmetler, finans, sağlık, güvenlik ve eğitim gibi pek çok alandaki işlemler, kişisel verilerin işlenmesiyle olmaktadır. Kişiler sosyalleşmek, kendisi ve çevresiyle ilgili haberleri paylaşmak için sosyal medyayı yoğun bir şekilde kullanmaktadır. Yakın bir zamanda yaşanan pandemi nedeniyle uzaktan çalışma ve öğretim modelleri de hayatımıza girmiştir.

Kişisel verilerin kullanılmasının; bireylere özelleştirilmiş ürün ve hizmetler sunulması, hastalıkların teşhis ve tedavisinin kolaylaştırılması, yeni ürünlerin ve hizmetlerin geliştirilmesi, suçun önlemesi, eğitim-öğretimin aksamasının önlenmesi gibi olumlu sonuçları olsa da, aynı zamanda kişilerin karar alma mekanizmalarının etkilenerek davranışlarının yönlendirilmesi ve bunun sonucunda demokrasinin zarar görmesi, kişilerin mahremiyetlerinin kaybı, dolandırıcılık ve özel hayatın gizliliğinin ihlaline benzer birçok suçun işlenmesi gibi olumsuz sonuçları da olmuştur. Bu nedenle tıpkı diğer temel hak ve özgürlükler gibi, kişisel verilerin korunması hakkının da bu kapsamda güvence altına alınma zarureti doğmuştur.

Kişisel verilerin korunması kısa zamanda modern hukuk sistemlerinin önemli bir odak noktası haline gelmiştir. Bu alanda ilk olarak 1980 yılında yayınlanan OECD Rehber İlkeleri'nden bahsetmek gerekmektedir. Bu ilkeler esasen veri korumaya ilişkin tavsiyeler niteliğinde temel kuralları içerse de, zaman içerisinde amacına ulaşmış ve hem ulusal hem de uluslararası çapta birçok düzenlemenin öncüsü olmuştur. Bu gelişmenin ardından Birleşmiş Milletler Teşkilatı'nın düzenlemelerinden olan İnsan Hakları Evrensel Bildirgesi ve Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme ile bir Avrupa Konseyi düzenlemesi olan Avrupa İnsan Hakları Sözleşmesi'ndeki temel hak ve özgürlüklerin yorumu, kişisel verilerin korunması hakkını da kapsar şekilde genişletilmiştir. Fakat bu geniş yorum, elbette bir noktada yetersiz kalmış ve kişilerin verilerinin otomatik işleme tabi tutulmasının insan haklarına saygılı bir şekilde gerçekleştirilmesini sağlamak ve veri koruma

standartlarını belirlemek amacıyla özel düzenlemeler de yapma ihtiyacı hasıl olmuştur. Böylece 1981 yılında, bu konuda bağlayıcı olan ilk uluslararası sözleşme olan 108 Sayılı Sözleşme hazırlanmıştır. Bunu Avrupa Birliği bünyesinde hazırlanan çeşitli direktifler ve protokoller takip etmiştir. Bunların içinde en önemlisi 95/46/EC Sayılı Direktif'tir. Fakat söz konusu Direktif, Avrupa Birliği çapında yeknesak bir kurallar bütünü oluşmasını sağlayamayınca GDPR kabul edilmiştir. Ülkemiz açısından ise Anayasa'nın 20. maddesine, 2010 yılında yapılan anayasa değişikliği referandumu ile kişisel verilerin korunmasını isteme hakkı eklenmiş olup, diğer haklardan bağımsız bir hak statüsüne kavuşturularak bu hakkın temel, vazgeçilmez ve devredilemez bir hak olduğu kabul edilmiştir. Ayrıca 2016 yılında KVKK kabul edilerek yürürlüğe girmiştir.

Kişisel verilerin korunması hakkın korunabilmesi için öncelikle kişisel verinin ne anlama gelip neleri kapsadığını tespit etmek önem arz etmektedir. Bu bağlamda çeşitli ulusal ve uluslararası hukuki metinde "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilginin" kişisel veri olduğu tespit edilmiştir. Buna göre, kişisel veriden söz etmek için bir verinin var olması, bu verinin bir gerçek kişiyi belirli veya belirlenebilir kılması ve o gerçek kişiye ilişkin olması gerekmektedir. Irk veya etnik köken, siyasi görüş, dini veya felsefi inanç, genetik ve biyometrik veriler, sağlıkla ilgili olan veriler gibi bazı veriler; doğaları gereği diğerlerine göre daha çok korumaya muhtaçtır. Bunlar hassas veya özel nitelikli kişisel veriler olarak nitelendirilmiş ve işlenmesi daha sıkı kurallara tabi tutulmuştur.

Daha üst ve genel bir konsept olan kişisel verilerin korunması hakkı, kişilerin verilerinin gizliliğinin ve güvenliğinin sağlanması hakkını içerirken; ilgili kişilere tanınan haklar da bu amacı güvence altına alan, veri işleme faaliyeti üzerindeki denetimi sağlayan ve ilgili kişilere verileri üzerinde daha fazla farkındalık ve seçenek sunan somut haklar olarak karşımıza çıkmaktadır. Yani kişilerin verileri üzerinde daha fazla bilgi ve kontrol sahibi olmalarını sağlayarak kişisel verilerin korunmasını desteklediği ifade edilebilir.

Bilgilendirilme hakkı, ilgili kişilere kişisel verilerinin nasıl işlendiği ve hakları hakkında şeffaf ve kolayca anlaşılır bilgilerin sağlanmasını kapsamaktadır. GDPR'de veri öznesine bir hak olarak verilmişken, KVKK'de veri sorumlusuna aydınlatma

yükümlülüğü olarak yüklenmiştir. Bu hak sayesinde kişi, verilerinin işlenmesine izin verip vermeyeceğine karar verecek, diğer haklarını öğrenecek ve ileri sürebilecektir.

Erişim hakkıyla kişilerin, verilerinin işlenmesinin hukuka uygunluğunu ve işlenen verilerin doğruluğunu denetleme imkanına sahip olmaları için yeterli, şeffaf ve kolay erişilebilir bir şekilde bilgilendirilmesi sağlanmaya çalışılmıştır. Bilgilendirme hakkı verilerin işlenmeye başlanmasından önceki sürece ilişkinken, erişim hakkı, işleme faaliyetinin başlamasından itibaren olan sürece ilişkindir. Bu bağlamda kişi; kendisi ile ilgili kişisel verilerin işlenip işlenmediğini ve işleme amaçlarını veri sorumlusundan öğrenebilir, bu verilere erişim talep edebilir ve işleme faaliyetinden geçen kişisel verilerin bir kopyasını alabilir.

Düzeltme hakkıyla ilgili kişiye, eksik veya yanlış işlenmiş kişisel verilerinin düzeltilmesini isteme hakkı verilmiştir. Bu hakkın, kişinin kendi verileri üzerindeki kontrolünün bir tezahürü olup erişim hakkının bir uzantısı olarak kullanıldığı ifade edilebilir. Ayrıca bu sayede kişisel verilerin işlenmesi sürecine hakim olan doğru ve gerektiğinde güncel olma ilkesinin gereği de yerine getirilmiş olacaktır.

İlgili kişi, kendisiyle ilgili kişisel verilerin herhangi bir gecikmeye mahal verilmeksizin silinmesini isteme hakkına sahip kılınmıştır. Buna ek olarak bazı durumların varlığı halinde veri sorumlusuna söz konusu verileri silme yükümlülüğü yüklenmiştir. Hukukumuzda silme hakkına ilişkin usul ve esaslar bir yönetmelik ile detaylı olarak düzenlenmiştir.

Veri sorumlusunun işleme faaliyetine devam etmekten kaynaklanan menfaatleri ile ilgili kişinin silme hakkını kullanmasıyla elde edeceği menfaatleri arasında bir denge kurulmasını sağlayan işleme faaliyetini kısıtlama hakkı; veri öznesinin düzeltme, silme ve itiraz haklarıyla yakından ilgili bir hak olup GDPR düzenlenmiştir. KVKK'de bu hak açıkça düzenlenmese de, kanunun bazı maddelerinden ve hukukun genel ilkelerinden yola çıkılarak, ilgili kişinin işleme faaliyetinin kısıtlanmasını isteyebileceği sonucuna varmaktayız.

KVKK uyarınca, ilgili kişi kendisine ilişkin verilerin düzeltilmesini veya işlenmesini gerektiren silinmesini sağladıktan sonra, bunların verilerin aktarıldığı diğer kişilere bildirilmesini isteme hakkına da sahiptir. GDPR'de bu hak ayrıca düzenlenmemiş olup veri sorumlusuna bir yükümlülük olarak verilmekle yetinilmiştir.

Veri taşınabilirliği hakkı, veri koruma hukukunda ilk defa GDPR ile düzenlenmiş olup KVVK'de yer almamaktadır. Kısaca ifade etmek gerekirse, kişisel verilerin işlenmesinin otomatik araçlarla gerçekleştirildiği durumlarda, veri öznesinin bilgilerini belirli bir formatta almasını ve bir engelle karşılaşmaksızın başka bir veri sorumlusuna iletebilmesini sağlamaktadır.

Veriler hukuka uygun olarak işlense de işleme faaliyetinin veri öznesinin beklentileriyle uyuşmaması halinde sonlandırılmasına imkan tanıyan itiraz hakkı, GDPR'de düzenlenmiş olup KVKK'de yer almamaktadır. Ancak kanunun bazı maddelerinden ve hukukun genel ilkelerinden yola çıkılarak, ilgili kişinin itiraz hakkını sonucuna varmaktayız. Bu hakka sadece yorumla ulaşılmaması gerektiği, bunun kanunilik ilkesine aykırı olacağı ve en kısa sürede gerekli düzenlemenin iç hukukumuza kazandırılması gerektiği kanaatindeyiz.

Otomatik karara tabi olmama hakkı, hem GDPR'de hem de KVKK'de yer alan ortak haklardan biri olup, karar alma sürecine herhangi bir insan müdahalesinin sağlanmasını amaçlamaktadır. Böylece kişinin kendisiyle alakalı alınacak önemli kararların geleceğine olumsuz bir etkide bulunmasının önüne geçilmeye çalışılmaktadır.

Şikayette bulunma hakkı ise kişilerin veri sorumlusunun yükümlülüklerini yerine getirmediği durumlarda hem idari hem de yargısal yoldan denetlenerek haklarını etkili kullanmalarını sağlamaktadır. Buna ek olarak tazminat hakkıyla da kişisel verileri ihlal edilenlere; itiraz, silme ve diğer haklarının kullanımıyla giderilemeyecek zararlarının karşılanması konusunda bir güvence sağlanmıştır.

Çalışmada ilgili kişilerin kendilerine ilişkin verilerle ilgili olarak ileri sürebileceği hakların içerikleri, esasları ve uygulanma usulleri; KVKK ve GDPR'deki düzenlemelerle birlikte karşılaştırmalı olarak ortaya konulmaya çalışılmıştır. Varılan sonuçlar; arasında Kişisel Verileri Koruma Kurulu, Yargıtay, Avrupa İnsan Hakları Mahkemesi, Avrupa Birliği Adalet Divanı, çeşitli Avrupa ülkelerinin veri koruma otoriteleri ve yerel mahkemeleri gibi birçok kurul, kuruluş ve yargı organlarının verdiği kararlarla da desteklenmiştir. Ayrıca ilgili kişilerin haklarını kullanmasına yönelik genel esaslar ile hakların genel kısıtlanma sebepleri de incelenmiştir.

KAYNAKÇA

Akgül, Aydın. **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, 2. Baskı, Beta Basım Yayın, İstanbul, 2016.

Akıncı, Ayşe Nur. **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, T.C. Kalkınma Bakanlığı Yayınları, Ankara, 2017.

Akıntürk, Turgut, Jale Akipek ve Derya Ateş Karaman. **Medeni Hukuk**, Beta Yayıncılık, İstanbul, 2022.

Aksoy, Hüseyin Can. **Kişisel Verilerin Korunması**, Çakmak Yayınevi, Ankara, 2010.

Aksoy, Hüseyin Can. "The Right To Personality And Its Different Manifestations As The Core Of Personal Data", **Ankara Law Review**, Cilt: 5, Sayı: 2, Ankara, 2008, (Personal Data), ss. 235-249.

Aksoy, Hüseyin Can. "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", **Kişisel Verileri Koruma Dergisi**, Cilt: 4, Sayı: 2, Ankara, 2022, (Algoritmik Karar Verme), ss. 69-87.

American Social Security Administration, "Report to Congress on Options for Enhancing the Social Security Card Chapter 3: The Expansion of the SSN as an Identifier", **Social Security Administration Web Sitesi**, https://www.ssa.gov/history/reports/ssnreportc2.html, (E.T. 01.03.2022).

Arat, Ayşe. "Gerçek Kişilerde Kişiliğin Sona Ermesi", **Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi**, Cilt: 9, Sayı: 1-2, 2006, ss. 257-276.

Arslan, Zühtü. "Temel Hak ve Özgürlüklerin Sınırlandırılması: Anayasa'nın 13. Maddesi Üzerine Bazı Düşünceler", **Anayasa Yargısı**, Cilt: 18, Sayı: 1, 2002, ss. 139-154.

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, **Avrupa Komisyonu Web Sitesi**, 2007, (Opinion 4/2007).

Article 29 Data Protection Working Party, "Advice paper on special categories of data ("sensitive data")", **Avrupa Komisyonu Web Sitesi**, 2011, (Sensitive Data).

Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", **Avrupa Komisyonu Web Sitesi**, 2013, (Opinion 02/2013).

Article 29 Data Protection Working Party, "Opinion 15/2011 on the definition of consent", **Avrupa Komisyonu Web Sitesi**, 2011, (Opinion 15/2011).

Article 29 Data Protection Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", **Avrupa Komisyonu Web Sitesi**, 2017, (Automated individual decision-making).

Article 29 Data Protection Working Party, "Guidelines on transparency under Regulation 2016/679", **Avrupa Komisyonu Web Sitesi**, 2018, (Transparency).

Aşıkoğlu, Şehriban İpek. "İlgili Kişiler Tarafından Yapılan Başvuruların Cevaplanması Yükümlülüğü", **Kişisel Verilerin Korunmasına Akademik Bakış**, Ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy, Arkadaş Basımevi, Ankara, 2023, ss. 195-210.

Ayözger Öngün, A. Çiğdem. **Kişisel Verilerin Korunması Hukuku**, 2. Baskı, Beta Yayınevi, İstanbul, 2019.

Badur, Emel. **Çocuğun Kişisel Verilerinin Korunması Kvkk, Gvkt ve Aihm Kararları Çerçevesinde Bir İnceleme**, Seçkin Yayıncılık, Ankara, 2023.

Badur, Emel ve Nesibe Kurt Konca. "Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini ve Görevli Mahkeme", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 13, Sayı: 2, 2022, ss. 476-490.

Başalp, Nilgün. **Kişisel Verilerin Korunması ve Saklanması**, Yetkin Yayınları, Ankara, 2004.

Bird & Bird Law Firm. **Guide to the General Data Protection Regulation**, 2020.

Bozkurt, Habip. **Kişisel Verilerin İşlenmesinin Hukuki Boyutu**, Yetkin Yayınları, Ankara, 2021.

BPB Online, "Yahoo Data Breach: What Actually Happened?", **BPB Online Web Sitesi**, 23.11.2020, https://bpbonline.medium.com/yahoo-data-breach-what-actually-happened-54cf8f3f7c93, (E.T. 30.09.2023).

Brkan, Maja. "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning", **German Law Journal**, Cilt: 20, Özel Sayı 6: Interrogating the Essence of EU Fundamental Rights, 2019, ss. 864–883.

Bulut, Metin. "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", **Ankara Barosu Dergisi**, Cilt: 78, Sayı: 3, Ankara, 2020, ss. 99-150.

Bük, Alaattin. **Bilişim Alanında Kişisel Verilerin Korunması**, Yetkin Yayınları, Ankara, 2021.

Bygrave, Lee A. "Article 22. Automated individual decision-making, including profiling", **The EU General Data Protection Regulation (GDPR): A Commentary**, Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler, Oxford University Press, Croydon, 2020, ss. 522-542.

Çavuşoğlu, Gökçe Filiz. **Kişisel Verilerin Yapay Zekayla İşlenmesinden Doğan Özel Hukuk Sorunları**, Yetkin Yayınları, Ankara, 2021.

Dağ, Güray. **Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması**, (Yayınlanmamış Doktora Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2011.

Deniz, İlknur. **Çocuklara Ait Kişisel Verilerin Türk Medeni Kanunu ve Kişisel Verilerin Korunması Kanunu Kapsamında Korunması**, Seçkin Yayıncılık, Ankara, 2021.

Dülger, Murat Volkan. **Kişisel Verilerin Korunması Hukuku**, Hukuk Akademisi Yayınları, 3. Baskı, İstanbul, 2020.

Dülger, Murat Volkan. **Bilişim Suçları ve İnternet İletişim Hukuku**, Seçkin Yayınevi, 4. Bası, Ankara, 2014, (Bilişim Suçları).

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, (Ceza Normları), ss. 101-168.

Dülger, Murat Volkan. "Anayasa Mahkemesi'nin Kişisel Verilerin Korunması Kanunu'nun Konu Edildiği İptal Davası Kararına İlişkin Bir Değerlendirme", **SSRN Papers Web Sitesi**, 2021, (KVKK İptal Davası).

Dülger, Murat Volkan. "Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 1, Sayı: 2, 2014, (Hasta Mahremiyeti), ss. 43-80.

Ersoy Kekevi, Çiçek. “Genel Kavramlar”, **Kişisel Verilerin Korunmasına Akademik Bakış**, Ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy, Arkadaş Basımevi, Ankara, 2023, ss. 103-134.

Erzurumlu, Nurbanu. “Türk Hukukunda Fikri Mülkiyete Konu Malların Cebrî İcrası”, **Yıldırım Beyazıt Hukuk Dergisi**, Sayı: 3, 2017, ss. 167-191.

Finck, Michèle ve Frank Pallas. “They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR”, **International Data Privacy Law**, Cilt: 10, Sayı: 1, 2020, ss. 11-36.

Fulford, Nicola ve Peter Carey. “Special Categories of Data”, **Data Protection: A Practical Guide to UK and EU Law**, 5. Baskı, Ed. Peter Carey, Oxford University Press, Croydon, 2018, ss. 66-87.

Fundamental Rights Agency. **Handbook on European Data Protection Law**, 2018.

Future of Privacy Forum and the Center for Democracy & Technology, “Best Practices for Mobile Application Developers”, **Future of Privacy Forum Web Sitesi**, 2018, https://cdt.org/wp-content/uploads/pdfs/Best-Practices-Mobile-App-Developers.pdf, (E.T. 13.10.2023)

Gözler, Kemal. “Anayasa Değişikliğinin Temel Hak ve Hürriyetlerin Sınırlandırılması Bakımından Getirdikleri ve Götürdükleri: Anayasanın 13'üncü Maddesinin Yeni Şekli Hakkında Bir İnceleme”, **Ankara Barosu Dergisi**, Sayı: 59 Cilt: 4, Ankara, 2001, (Anayasa M. 13), ss. 53-67.

Gözler, Kemal. **Türk Anayasa Hukuku Dersleri**, 24. Baskı, Ekin Kitabevi Yayınları, Bursa, 2019.

Gürsel, İlke. **İşçinin Kişisel Verilerinin Korunması Hakkı**, Adalet Yayınevi, Ankara, 2016.

Hazel, Steven H. “Personal Data as Property”, **Syracuse Law Review**, Cilt: 70, Sayı: 1055, 2020, ss. 1056-1112.

İçişleri Bakanlığı, “2022 Yılında Türkiye'de En Çok Tercih Edilen İsimler Belli Oldu”, **İçişleri Bakanlığı Web Sitesi**, 01.01.2023, https://www.icisleri.gov.tr/2022-yilinda-turkiyede-en-cok-tercih-edilen-isimler-belli-oldu#:~:text=Kız%20bebeklere%20en%20çok%20verilen,bebeğe%20ise%20Asel%20ismi%20konuldu, (E.T. 30.09.2023).

Kaminski, Margot E. “The Right to Explanation, Explained”, **Berkeley Technology Law Journal**, Cilt: 34, Sayı: 1, 2019, ss. 189-218.

Karayiğit, Mustafa T. **Avrupa Birliği Anayasa Hukuku**, Seçkin Yayıncılık, Ankara, 2018.

Kaşak, Fahri Erdem. “Tüzel Kişilik Kavramı ve Tüzel Kişilik Perdesinin Kaldırılması”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt: 26, Sayı: 2, 2020, ss. 1242-1263.

Kaya, Semih Batur. “İnsan Haklarında Devletin Pozitif Yükümlülüğü: Avrupa İnsan Hakları Mahkemesi ve Anayasa Mahkemesi Üzerine Bir Analiz”, **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 9, Sayı: 1, İstanbul, 2022, ss. 51-72.

Kayıhan, Şaban. **Medeni Hukuk Bilgisi**, 5. Baskı, Seçkin Yayıncılık, Ankara, 2022.

Keyder, Virginia. “Introductory Note To The European Court Of Justice: Scarlet Extended SA v. Société Belge Des Auteurs, Compositeurs, Et Editeurs SCRL (SABAM)”, **International Legal Materials**, Cilt: 51, Sayı: 2, 2012, ss. 382-392.

Kişisel Verileri Koruma Kurumu. **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi**, KVKK Yayınları, Ankara, 2018.

Kişisel Verileri Koruma Kurumu. **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, KVKK Yayınları, Ankara, 2019, (Rehber).

Kişisel Verileri Koruma Kurumu. **100 Soruda Kişisel Verilerin Korunması Kanunu**, Ankara, 2019, (100 Soru).

Kişisel Verileri Koruma Kurumu. **Çerez Uygulamaları Hakkında Rehber**, KVKK Yayınları, Ankara, 2022, (Çerez).

Kişisel Verileri Koruma Kurumu. **Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi**, Ankara, 2019, (Aydınlatma Yükümlülüğü).

Kişisel Verileri Koruma Kurumu. **Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi**, KVKK Yayınları No: 34, Ankara, 2021, (Unutulma Hakkı).

Koç, Fatma. **İş İlişkisinde Kişisel Sağlık Verilerinin İşlenmesi**, On İki Levha Yayınları, İstanbul, 2022.

Korkmaz, İbrahim. **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayınları, Ankara, 2017.

Kotschy, Waltraut. "Article 77. Right to lodge a complaint with a supervisory authority", **The EU General Data Protection Regulation (GDPR): A Commentary**, Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler, Oxford University Press, Croydon, 2020, (Article 77), ss. 1117-1124.

Kotschy, Waltraut. "Article 79. Right to an effective judicial remedy against a controller or processor", **The EU General Data Protection Regulation (GDPR): A Commentary**, Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler, Oxford University Press, Croydon, 2020, (Article 79), ss. 1133-1141.

Kovalenko, Yuliia. “The Right To Privacy And Protection Of Personal Data: Emerging Trends And Implications For Development In Jurisprudence Of European Court Of Human Rights”, **Masaryk University Journal of Law and Technology**, Cilt: 16, Sayı: 1, 2022, ss. 37-57.

Küzeci, Elif. **Kişisel Verilerin Korunması**, Turhan Kitabevi, Ankara, 2010.

Lloyd-Jones, Heledd ve Peter Carey. “The Rights of Individuals”, **Data Protection: A Practical Guide to UK and EU Law**, 5. Edition, Ed. Peter Carey, Oxford University Press, Croydon, 2018, ss. 122-154.

Malgieri, Gianclaudio. **Vulnerability and Data Protection Law**, Oxford University Press, Oxford, 2023.

Malgieri, Gianclaudio. “Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations”, **Computer Law & Security Review**, Cilt: 35, Sayı: 5, 2019, (Automated decision-making).

Maraşlı, Fatih ve Musa Çıbuk. “RFID Teknolojisi ve Kullanım Alanları”, **Bitlis Eren Üniversitesi Fen Bilimleri Dergisi**, Cilt: 4, Sayı: 2, 2015, ss. 249-275.

Mourby, Miranda, Elaine Mackey, Mark Elliot, Heather Gowans, Susan E. Wallace, Jessica Bell, Hannah Smith, Stergios Aidinlis ve Jane Kaye. “Are ‘pseudonymised’ data always personal data? Implications of the GDPR for administrative data research in the UK”, **Computer Law & Security Review**, Cilt: 34, Sayı: 2, 2018, ss. 222-233.

Orhan, Uğur. “Kişisel Verilerin Korunmasına İlişkin Türk Ceza Hukuku Düzenlemeleri Üzerine Değerlendirmeler”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 70, Sayı: 4, Ankara, 2021, ss. 1359-1384.

Özcan Büyüktanır, Burcu G. "Ceninin Bedensel Bütünlüğünün İhlalinde Maddi Zararının Tazmini", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 9, Sayı: 1, 2018, ss. 275-302.

Polčák, Radim. "Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject", **The EU General Data Protection Regulation (GDPR): A Commentary**, Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler, Oxford University Press, Croydon, 2020, ss. 398-412.

Poullet, Yves. "EU data protection policy. The Directive 95/46/EC: Ten years after", **Computer Law & Security Review**, Cilt: 22, Sayı: 3, 2006, ss. 206-2017.

Purtova, Nadezhda. "The law of everything. Broad concept of personal data and future of EU data protection law", **Law, Innovation and Technology**, Cilt: 10, Sayı: 1, 2018, ss. 40-81.

Quinn, Paul ve Gianclaudio Malgieri. "The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework", **German Law Journal**, Cilt: 22, Sayı: 8, 2021, ss. 1583-1612.

Sajfert, Juraj ve Teresa Quintel. "Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities", **SSRN Papers Web Sitesi**, 2017.

Seven, Hande. **Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (TCK M.136)**, Yetkin Yayınları, Ankara, 2021.

Sharkey, Jennifer ve D. Scott Brandt. "Integrating Technology Literacy and Information Literacy", **Technology Literacy Applications in Learning Environments**, (Ed. David D. Carbonara), 2005.

Sırabaşı, Volkan. **İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz**, Adalet Yayınevi, 2. Bası, Ankara, 2007.

Soysal, Tamer. "Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi", **Uyuşmazlık Mahkemesi Dergisi**, Sayı: 13, 2019, ss. 339-422.

Stalla-Bourdillon, Sophie ve Alison Knight. "Anonymous Data v. Personal Data – A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data", **Wisconsin International Law Journal**, Cilt: 34, 2016, ss. 285-322.

Şen, Ersan. "Kişisel Verilerin Korunması Kanunu Tasarısının Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", **İstanbul Barosu Dergisi**, Cilt: 83, Sayı: 3, 2009, (KVKK Tasarısı), ss. 1197-1214.

Şen, Ersan, Mert Maviş, Alperen Gözükan, M. Enes Efe ve Fırat Çetintaş. **Savunma Hakkının Kişisel Veriler Karşısında Korunması**, Seçkin Yayıncılık, Ankara, 2022, (Savunma Hakkı).

Şimşek, Oğuz. **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Basım Yayın, İstanbul, 2008.

Tanju, Erhan. **AİHM Kararları Işığında İfade ve Basın Özgürlüğü**, Seçkin Yayıncılık, Ankara, 2012.

Türkiye Büyük Millet Meclisi, "117 Sayılı Kanun Tasarısı ve Rapor", https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf, (E.T. 25.08.2022)

Trakman, Leon, Robert Walters ve Bruno Zeller, "Is Privacy and Personal Data Set to Become the New Intellectual Property?", **International Review of Intellectual Property and Competition Law**, Cilt: 50, Sayı: 8, 2019, ss. 937-970.

Toprak, Bilal. **KVKK ve GVKT Açısından İşçinin Kişisel Verilerinin Korunması**, Yetkin Yayınları, Ankara, 2021.

Turan Başara, Gamze. "Medeni Hukuk İlişkilerinde Kişisel Verilerin Korunması", **Kişisel Verilerin Korunmasına Akademik Bakış**, Ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy, Arkadaş Basımevi, Ankara, 2023, ss. 439-466.

Turgut, Cemile. **Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı**, On İki Levha Yayınları, İstanbul, 2021.

Turhan, Aydın. "İnsan Hakkı Kuşakları Arasındaki Tamamlayıcılık İlişkisi", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Sayı: 2, Cilt: 4, 2013, ss. 357-378.

Uçak, Murat. "Kişisel Verilerin Ölümden Sonra Korunması", **İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi**, Sayı: 10, Cilt: 6, İstanbul, 2021, ss. 97-123.

UN Human Rights Committee (HRC), "CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation", **United Nations High Commissioner for Refugees Web Sitesi**, 08.04.1988, https://www.refworld.org/docid/453883f922.html, (E.T. 10.08.2022).

Uncular, Selen. **İş İlişkisinde İşçinin Kişisel Verilerinin Korunması**, 2. Baskı, Seçkin Yayıncılık, Ankara, 2018.

Us Doğan, Eser. "Başvuru ve Şikâyet Usulleri ile Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü", **Kişisel Verilerin Korunmasına Akademik Bakış**, Ed. Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy, Arkadaş Basımevi, Ankara, 2023, ss. 211-252.

Uyar, Lema. **Birleşmiş Milletler'de İnsan Hakları Yorumları İnsan Hakları Komitesi ve Ekonomik, Sosyal ve Kültürel Haklar Komitesi, 1981-2006,** İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2016.

Voss, W. Gregory ve Kimberly A. Houser. "Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies", **American Business Law Journal**, Cilt: 56, Sayı: 2, 2019, ss. 287-344.

Vrabec, Helena U. **Data Subject Rights under the GDPR: With a Commentary through the Lens of the Data-driven Economy**, Oxford University Press, Croydon, London, 2021.

Walden, Ian. "The Application of Directive 95/46/EC", **The EDI Law Review**, Cilt: 3, Sayı: 2, 1996, ss. 85-98.

Wikipedia, "2017 Equifax data breach", **Wikipedia Web Sitesi**, https://en.wikipedia.org/wiki/2017_Equifax_data_breach, (E.T. 30.09.2023).

Zanfir-Fortuna, Gabriela. "Article 21. Right to object", **The EU General Data Protection Regulation (GDPR): A Commentary**, Ed. Christopher Kuner, Lee A Bygrave, Christopher Docksey, Laura Drechsler, Oxford University Press, Croydon, 2020, (Right to object), ss. 508-521.

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, Oxford University Press, Croydon, 2020, (Right to compensation), ss. 1160-1179.

Zeytin, Zafer ve Ömer Ergün. **Türk Medeni Hukuku**, 6. Baskı, Seçkin Yayıncılık, Ankara, 2022.

Zins, Chaim. “Conceptual approaches for defining data, information, and knowledge”, **Journal of the American Society for Information Science and Technology**, Cilt: 58, Sayı: 4, 2007, ss. 479-493.