TÜRK KİŞİSEL VERİLERİ KORUMA MEVZUATININ AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ İLE UYUMLAŞTIRILMASI SÜRECİNDE DOĞABİLECEK SORUNLAR VE BU SORUNLARA YÖNELİK ÇÖZÜM ÖNERİLERİ

AYCA ZANBAKLAR SEÇKİN

YEDİTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İSTANBUL, 2022

TÜRK KİŞİSEL VERİLERİ KORUMA MEVZUATININ AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ İLE UYUMLAŞTIRILMASI SÜRECİNDE DOĞABİLECEK SORUNLAR VE BU SORUNLARA YÖNELİK ÇÖZÜM ÖNERİLERİ

AYCA ZANBAKLAR SEÇKİN

DANIŞMAN
DR. ÖĞR. ÜYESİ CİHAN AVCI BRAUN

SOSYAL BİLİMLER ENSTİTÜSÜ'NE SUNULAN BU TEZ

HUKUK YÜKSEK LİSANS

DERECESİ İÇİN KISMİ YETERLİLİKLERİ KARŞILAMAKTADIR

YEDİTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İSTANBUL, 2022

İNTİHAL SAYFASI

Yüksek lisans tezi olarak sunduğum, bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu ve bu eserleri her kullanışımda alıntı yaparak yararlandığımı belirtir; bunu onurumla doğrularım.

Enstitü tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

Tarih : 15.12.2022
Ad/soyad : Ayca Zanbaklar Seçkin
İmza :

ÖZET

Özellikle 90'lı yıllardan itibaren bilgi teknolojileri alanında yaşanan hızlı gelişim, kişisel verilerin yasal olarak korunma ihtiyacını ön plana çıkarmıştır. Bu ihtiyaçtan yola çıkarak pek çok ülke kendi yasal mevzuatında düzenlemeler yapma gereği duymuştur. 95 yılında 95/46/EC sayılı Direktifin kabul edilmesiyle Avrupa Birliği hukukunda kişisel veriler ilk kez yasal bir çerçeveye oturmuştur. 14 Nisan 2016 tarihinde onaylanan Avrupa Birliği Genel Veri Koruma Tüzüğü ise 25 Mayıs 2018 tarihinde yürürlüğe girmiştir.

Türkiye'de ise 2010 yılında yapılan Anayasa değişikliğinden sonra 7 Nisan 2016 tarihinde Kişisel Verileri Koruma Kanunu (KVKK) kabul edilerek ilk çerçeve Yasa yürürlüğe girmiştir. Ne var ki Kişisel Verileri Koruma Kanunu'nun, 2 (iki) senelik uyum sürecinden sonra 25 Mayıs 2018 tarihinde yürürlüğe giren Genel Veri Koruma Tüzüğü ile mukayese edildiğinde yetersiz kaldığı görülmektedir. Bu yetersizliklerin temelinde, KVKK'nın, Avrupa Konseyi'nin 1 Ekim 1995 tarihinde kabul ettiği 95/46/EC sayılı "Kişisel Verilerin İşlenmesi ve Bu Verilerin Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi"ni referans alması yatmaktadır.

Bu açıklamalardan hareket ile ülkemizdeki kişisel verilerin korunması yönündeki ihtiyacı karşılamaya yönelik hazırlanan Kişisel Verilerin Korunması Kanunu, Türkiye'nin Avrupa Birliğine uyum sürecinde hayati önemi haizdir. Bununla birlikte Tüzüğün bölgesel kapsamı düşünüldüğünde pek çok ülke mevzuatıyla etkileşim içinde olacağı açıktır. Dolayısıyla Tüzüğün, Türk mevzuatına uyumlaştırılması sürecinin karşılaştırılmalı olarak değerlendirilmesi ve ortaya çıkabilecek sorunların çözümüne yönelik çalışmalar yapılması gerekmektedir. Bu hususta, Türkiye'de yerleşik kişi ya da tüzel kişilerin, KVKK ile uyum içerisinde olması yeterli olmamakta, aynı zamanda AB Genel Veri Koruma Tüzüğü ile de uyumluluk göstermesi gerekmektedir. Kişisel Verileri Koruma Kanunu'nda yapılacak uyumlaştırma çalışmaları, halihazırda AB Genel Veri Koruma Tüzüğü'ne dahil olan gerçek kişi ve tüzel kişiler için önem taşıyacağı gibi Kişisel Verileri Koruma Kurulu bakımından ileride uygulamada oluşabilecek boşlukların doldurulmasında da önem kazanacaktır.

Anahtar Kelimeler: Kişisel veri, Kişisel Verilerin Korunması, Genel Veri Koruma Tüzüğü, 6698 Sayılı Kişisel Veriler Korunma Kanunu.

ABSTRACT

The rapid development in the field of information technologies, especially since the nineties, highlighted the need for legal protection of personal data. Starting from this need, many countries have felt the need to make arrangements in their own legal regulations. With the adoption of Directive 95/46/EC in 1995, in the European Union law for the first-time personal data was placed in a legal framework. The General Data Protection Regulation of the European Union, which was approved on April 14, 2016, entered into force on May 25, 2018.

In Turkey, after the constitutional amendment in 2010, on April 7, 2016, Turkish Personal Data Protection Law no. 6698 entered into force and the first framework law was adopted. However, when the Personal Data Protection Law is compared with the General Data Protection Regulation, which entered into force on 25 May 2018 after a two-year harmonization process, it seems to be insufficient. The reason for these inadequacies is that Turkish Personal Data Protection Law no. 6698 takes as reference the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, European Treaty Series-No.108 and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. " adopted by the Council of Europe on October 1, 1995.

Based on these explanations, Turkish Personal Data Protection Law no. 6698 which was prepared for the need for the protection of personal data in our country, is also of vital importance in Turkey's harmonization process with the European Union. In addition, considering the regional scope of the Regulation, it is clear that it will interact with the legislation of many countries. Therefore, the Regulation should be evaluated comparatively in the process of harmonization with Turkish legislation and studies should be carried out to solve the problems that may arise. In this regard, it is not sufficient for the persons or legal entities residing in Turkey to be in compliance with the Turkish Personal Data Protection Law no. 6698, but also need to comply with the EU General Data Protection Regulation. Harmonization studies to be carried out in the Turkish Personal Data Protection Law no. 6698 will be important for real persons and legal entities included in the EU General Data Protection Regulation and will also gain importance in filling the gaps that may arise in practice in the future for the Personal Data Protection Board.

Keywords: Personal data, Personal Data Protection, General Data Protection Regulation, Turkish Personal Data Protection Law no. 6698.

ÖNSÖZ

Tez çalışmam boyunca sabrı ve özverisi ile beni destekleyen ve her koşulda yanımda olan değerli danışman hocam Dr. Öğr. Üyesi Cihan Avcı Braun'a ve maddi-manevi desteklerini hep hissettiğim, verdiğim her kararda yanımda olan değerli annem Ferhan Zanbaklar, babam Feyzi Zanbaklar, abim Arda Zanbaklar ve beni hiçbir koşulda yalnız bırakmayan değerli eşim Hakan Seçkin'e sonsuz minnet duygularımla teşekkür ederim.

Ayca Zanbaklar Seçkin

İÇİNDEKİLER

KISALTMALAR

AB	**:** Avrupa Birliği
ABAD	**:** Avrupa Birliği Adalet Divanı
ABD	**:** Amerika Birleşik Devletleri
AİHM	**:** Avrupa İnsan Hakları Mahkemesi
AİHS	**:** Avrupa İnsan Hakları Sözleşmesi
Article 29 WP	**:** 29. Madde Çalışma Grubu
AYM	**:** Anayasa Mahkemesi
bkz.	**:** Bakınız
BAM	**:** Bölge Adliye Mahkemesi
BGE	**:** İsviçre Federal Mahkemesi Kararları
C.	**:** Cilt
Direktif	**:** 95/46/EC Sayılı AB Direktif'i
DPO	**:** Data Protection Officer (Veri Koruma Görevlisi) (Kısaca "VKG")
E.	**:** Esas Numarası
ed.	**:** Editör
eds.	**:** Editörler
EDPB	**:** European Data Protection Board (Avrupa Veri Koruma Kurulu)
FSEK	**:** 5846 Sayılı Fikir ve Sanat Eserleri Kanunu
HD	**:** Hukuk Dairesi
HGK	**:** Hukuk Genel Kurulu
ICO	**:** Information Commissioner's Office
K.	**:** Karar Numarası
Kurum	**:** Kişisel Verileri Koruma Kurumu
Kurul	**:** Kişisel Verileri Koruma Kurulu
KVKK	**:** 6698 sayılı Kişisel Verilerin Korunması Kanunu

m.	**:** Madde
No	**:** Numara
OECD	**:** Ekonomik Kalkınma ve İşbirliği Örgütü (Organisation for Economic Co-operation and Development)
OECD Rehber İlkeleri	**:** Özel Hayatın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler
p.	**:** page (sayfa)
para.	**:** Paragraf
R.G.	**:** Resmî Gazete
s.	**:** Sayfa Sayısı
ss.	**:** Sayfa Sayıları Arasında
Sicil	**:** Veri Sorumluları Sicili
T.	**:** Tarih
TBB	**:** Türkiye Barolar Birliği
TBK	**:** 6098 sayılı Türk Borçlar Kanunu
TCK	**:** Türk Ceza Kanunu
TTK	**:** Türk Ticaret Kanunu
TBMM	**:** Türkiye Büyük Millet Meclisi
T.C.	**:** Türkiye Cumhuriyeti
TCK	**:** Türk Ceza Kanunu
TMK	**:** Türk Medeni Kanunu
Tüzük (GDPR)	**:** Avrupa Birliği Genel Veri Koruma Tüzüğü
V. / Vol	**:** Volume (Cilt)
vb.	**:** Ve benzeri
vd.	**:** Ve devamı
VERBİS	**:** Veri Sorumluları Sicili Bilgi Sistemi
WP	**:** Working Party (Çalışma Grubu**)**
YHGK	**:** Yargıtay Hukuk Genel Kurulu
YÜHFD	**:** Yeditepe Üniversitesi Hukuk Fakültesi Dergisi

GİRİŞ

Günümüzde hızla ilerleyen teknolojik gelişmelerin ışığında kişisel verilerin korunma ihtiyacı giderek önem kazanmış ve bu alanda yapılan çalışmalar her geçen gün hız kazanarak ülkelerin yasal mevzuatında yer almaya başlamıştır[1]. Ülkelerin teknolojik gelişmelere ayak uydurma çabası içerisinde başta insan hak ve temel özgürlüklerini korumak[2], kişilerin özel hayat sınırlarına müdahaleyi engellemek ve kişisel veri ihlallerinin önüne geçmeye yönelik atılan bu adımlar, ülkemizde de "6698 sayılı Kişisel Verilerin Korunması Kanunu"'nun yürürlüğe girmesi ile önemli bir aşama kaydetmiştir.

Bugün hayatımızın pek çok alanına hâkim olan teknolojik araçlar ile kişisel verilerimiz her an her dakika işlenmektedir. Bu işlemelere konu olan verilerin internet ortamında sınır ötesi ülkelere aktarımı ile kişisel verilerin korunması anlamındaki menfaat dengesi ise son derece hassas bir denge oluşturmaktadır. Elbette kişisel verilerin her ülke mevzuatında kanunlaşma aşamaları farklı zamanlara denk gelmektedir. Bu anlamda 4 Kasım 1950 tarihinde imzalanarak 3 Eylül 1953 yılında yürürlüğe giren "Avrupa İnsan Hakları Sözleşmesi'nin"[3] özel hayatı korumaya ilişkin 8. maddesi önem arz etmektedir. Sözleşme, her ne kadar kişisel verileri korumaya yönelik doğrudan bir ifade barındırmıyor olsa da 8. madde kapsamında kişilerin özel hayatına ve aile hayatına saygı kapsamında önemli bir hüküm barındırmaktadır.

Kişisel verilerin korunmasına yönelik daha doğrudan atılan adımların tarihi ise 1970'lı yıllara kadar uzanmaktadır[4]. Bu anlamda kişisel verileri koruması anlamında

---

[1] **TEZCAN** Durmuş, "Bilgisayar Karşısında Özel Hayatın Korunması", Anayasa Yargısı Dergisi, C. 8, Ankara, 1991, ss. 385-392, s. 385.

[2] **ŞİMŞEK** Oğuz**,** Anayasa Hukukunda Kişisel Verilerin Korunması, 2008, Beta yayınları s. 4.

[3] Convention for the Protection of Human Rights and Fundamental Freedoms, ("European Human Rights Convention"), ("Avrupa İnsan Hakları Sözleşmesi" bir diğer ifade ile "İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme", 4 Kasım 1950'de İnsan Hakları Bildirisinde yer alan hakları tümüyle güvence altına almak üzere Avrupa Konseyi üyelerinin bir araya gelerek anlaştıkları metindir.

[4] **TORTOP** Nuri, "Çağımızın Önemli Sorunu: Kişisel Bilgilerin Güvenliği Sorunu", Amme İdaresi Dergisi, Cilt: 33, Sayı: 3, 2000, ss. 1-14, s. 2; **ÜZELTÜRK TAHMAZOĞLU** Sultan, "Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği", Legal Hukuk Dergisi, Sayı 93, Eylül 2010. s. 3152; **LANG** Peter, Data Rights Law 1.0, The Theoretical Basis Key Laboratory of Big Data Strategy Edited by Lian Yuming, "Chapter 1-The Significance of Data Rights to Mankind's Common Life", 2019, s. 8; **SCHWARTZ** Paul, The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, Amerian Journal of Comparative Law, C. 37, 1989, s. 675-702, s. 688.

yapılan ilk kanuni düzenlemenin 7 Ekim 1970 tarihli Hessen Veri Koruma Kanunu[5] olduğu ifade edilebilir[6]. Bunun yanı sıra 1973 tarihinde İsveç Veri Kanunu[7], 1974 tarihinde Amerika Birleşik Devletleri'nin Gizlilik Yasası (Privacy Act), 1978 tarihinde Alman Federal Cumhuriyetinin Federal Veri Koruma Kanunu, 1978 tarihinde Fransa'da düzenlenen Veri Koruma Kanunu[8] kişisel verileri koruma anlamında yer alan kanuni düzenlemelerdir. Danimarka, Norveç, Avusturya ve Lüksemburg gibi ülkelerde kişisel verilere ilişkin kanuni düzenlemeler yapan ilk ülkeler olarak yer almaktadır[9].

Ülkelerin kendi yasal mevzuatındaki düzenlemelerden ayrı olarak 23 Eylül 1980 tarihinde, "Ekonomik İş birliği ve Kalkınma Örgütü" (OECD[10]) tarafından "Özel Hayatın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeler" yayımlanmıştır. Bu ilkeler tavsiye niteliğinde ilkeler olup, ülkelerin iç hukuk sistemlerine aktarılması anlamında bir bağlayıcılığı olmasa da uluslararası alanda atılan önemli bir adım olmuştur[11]. Tarih 28 Ocak 1981'i gösterdiğinde, Avrupa Konseyi tarafından hazırlanan ve 1 Ekim 1985'te yürürlüğe giren ilk uluslararası sözleşme niteliğinde 108 sayılı[12] "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"[13] kabul edilmiştir. 108 sayılı Sözleşme'nin yasal mevzuatımıza dahil edilmesi 30 Ocak 2016 tarih ve 6669 sayılı Kanun'la[14] kararlaştırılmış, Bakanlar Kurulu'nun 29 Şubat 2016 tarih ve 2016/8576[15] sayılı kararıyla onaylanarak 17 Mart 2016 tarihli Resmi Gazetede yayımlanmıştır.

---

[5] Hessisches Datenschutzgesetz/ German Hessen Data Protection Act, 7 October 1970. 1970 yılında, Hessen federal eyaleti, aynı zamanda dünyanın ilk veri koruma yasası olan ilk ulusal veri koruma yasasını kabul etmiştir..

[6] **DEVELİOĞLU** Murat, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul 2017, s. 5; **AKGÜL** Aydın, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta Yayınları, İstanbul 2014, s. 167.

[7] **KUNER** Christopher**,** Transborder Data Flows and Data Privacy Law, Oxford University Press, 2013, s. 26. bkz. Swedish Data Act of 1973, Article 11.

[8] Fransa Veri Koruma Yasası (Loi relative â l'informatique, aux fichiers et aux libertes).

[9] **EVANS** A.C, "Europian Data Protection Law" The American Journal of Comparative law, C. 29, 1981, ss.571-582, s. 582.

[10] OECD Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Document C (80) 58(Final), October 1, 1980.

[11] **ŞİMŞEK**, s. 13.

[12] **Kişisel Verileri Koruma Kurumu,** "Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler (Son Erişim Tarihi: 06.10.2021)

[13] 108 sayılı Sözleşme- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, European Treaty Series-No.108, 28 Ocak 1980, https://rm.coe.int/1680078b37(Son Erişim Tarihi: 03.05.2021). (Bundan böyle kısaca 108 sayılı Sözleşme olarak anılacaktır.)

[14] R.G., T. 18.02.2016, S. 29628.

1990'lı yıllardan itibaren internet kullanımının yaygınlaşması ve beraberinde getirdiği teknolojik ilerlemeler ile kişisel verilerin işlenmesi, kayıt altına alınması, paylaşılması gibi hususlar yaygınlaşmıştır. Bu ilerlemelere karşın, verilerin güvenliğinin sağlanması bakımından gerek ülkelerin iç mevzuatları gerekse uluslararası alanda atılan adımların yetersiz kaldığı görülmüştür. Netice olarak, kişisel verilerin korunmasına ilişkin atılacak adımlarda hem çağa ayak uyduracak düzenlemelerin yapılması amaçlanmış, hem de ülkeler nezdinde yeknesak bir uygulama ihtiyacı ortaya çıkmıştır. Bu ihtiyaçları karşılamaya yönelik olarak, Avrupa Birliği'nin 24 Temmuz 1995 tarihli "95/46/EC[16] sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktif"'i kabul edilmiştir. AB'ye üye devletler, Direktif'i esas alarak kendi iç hukuk sistemlerine bu yeni düzenlemeleri uyumlaştırma çabalarını başlatmıştır. Ne var ki Direktif hükümlerinin üye devletler bakımından bağlayıcılığının olmaması, 2000'li yıllardan itibaren teknolojik gelişmelerin hızla aldığı seyir karşısında, 95/46/EC sayılı Direktif'in yeterli korumayı sağlayamadığı gözlemlenmiştir[17]. Nihayetinde, tez konumuza kaynaklık eden "2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü"[18], 95/46/EC sayılı Direktif'in yürürlükten kalkması ile uygulamadaki yerini almıştır.

GVKT'nin getirdiği en önemli yenilik, tüzüğün üye devletler bakımından bağlayıcılığının olmasıdır. Zira Avrupa Birliği hukuku kaynakları arasında yer alan direktifler bütünüyle bağlayıcı değillerdir[19]. Bu anlamıyla direktiflerin temel rolü, üye devletlerin kendi iç hukuk sistemine bu düzenlemeleri uyumlaştırma aracı olmasıdır.

---

[15] R.G., T. 17.03.2016, S. 29656.

[16] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data" https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en (Son Erişim Tarihi: 03.04.2021); **Kişisel Verileri Koruma Kurumu**, "Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler", s. 6.

[17] **BAŞALP** Nilgün, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt: 21, Sayı: 1, 2015, ss.77-106, s. 82.

[18] Bundan sonra kısaca GVKT ya da Tüzük olarak anılacaktır.

[19] Bir diğer ifade ile direktifler, ilgili üye devletleri belirlenen amaçlar ile ulaşılmak istenen sonuçlar itibariyle bağlar. Direktiflere muhatap üye ülkeler belirlenen amaçlar doğrultusunda gerekli yasal düzenlemeleri yaparak kendi iç hukuklarına aktarırlar. **TAPAN** Mehmet Nuri, **"**Avrupa Birliği (AB) Hukukunun Kaynakları ve Ulusal Hukuka Etkileri Avrupa Adalet Divanı, Türkiye Barolar Birliği Dergisi, 1998/3, ss. 971-1020, s. 994; **AKINCI** Ayşe Nur, "Avrupa Birliği Genel Veri Koruma Tüzüğü' nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi", Çalışma Raporu 6, T.C. Kalkınma Bakanlığı Yayın No: 2968, 2017, s. 14.

Tüzükler yapısı itibariyle, ülkelerin iç hukuk sistemlerinde ilave bir düzenlemeye ihtiyaç duymamaktadır.

Avrupa Birliği hukukunda gidişat böyle iken, ülkemizde kişisel verilerin korunması ile ilgili atılan adımlar geriden gelmiştir. Kişisel verileri korumaya yönelik atılan adımlara özellikle 2000'li yıllardan itibaren hız kazandırılmak istenmişse de mevcut yasal düzenleme olan Kişisel Verileri Koruma Kanunu'nun yürürlüğe girmesi 2016 yılına denk düşmektedir. Bu anlamda ülkemizde kişisel verilerin korunmasına ilişkin yasal mevzuatın oluşturulması uzun yıllar almıştır[20]. 7 Mayıs 2010 tarihinde Anayasanın 20. maddesinde yapılan değişikliğe ilave olarak[21] neticede 24 Mart 2016'da kabul edilen 7 Nisan 2016 tarihli ve 29677[22] sayılı Resmi Gazetede yayımlanarak yürürlüğe giren "6698 sayılı Kişisel Verilerin Korunması Kanunu" (KVKK) mevzuatımızda yerini almıştır. Avrupa Genel Veri Koruma Tüzüğü'nün yürürlük tarihine kıyasla, KVKK önceki tarihli bir düzenlemedir. Bununla birlikte KVKK, Avrupa Konseyi'nin 1 Ekim 1995 tarihinde kabul ettiği 108 sayılı Sözleşmeyi ve "95/46/EC sayılı Direktif"'i referans alması ile çağımızın ihtiyaçlarına cevap olacak düzenlemelere sahip değildir.

KVKK'nın kabulünden kısa bir süre sonra yürürlüğe giren Tüzük ile amaçlanan, 95/46/EC sayılı Direktif'teki düzenlemelerin revize edilerek, güncel teknolojik gelişmelere ayak uyduracak yeterliliğe ulaşmasıdır. Bu anlamda Tüzük, Direktif ile karşılaştırıldığında, uygulanacak yaptırımlar, alınacak tedbirler, veri sorumlusuna yüklenecek sorumluluklar kapsamında daha geniş düzenlemelere yer vermiştir. Buna ek olarak, veri sahibine veri taşınabilirliği hakkı, unutulma hakkı gibi daha geniş haklar sunulmuştur. Bu güncellemeler ışığında, KVKK bakımından da benzer düzenlemelerin uygulamaya alınması gerekmektedir. Bu amaçların gerçekleştirilebilmesi için gerekli görülecek yasal düzenlemelerin mevzuata uygun düşecek şekilde Avrupa Veri Koruma Tüzüğüne uyumlu hale getirilmesi, halen

---

[20] **Kişisel Verileri Koruma Kurumu,** "Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı" https://kvkk.gov.tr/yayinlar/ANAYASAL%20B%C4%B0R%20HAK%20OLARAK%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASINI%20%C4%B0STEME%20HAKKI.pdf (Son Erişim Tarihi: 06.10.2021).

[21] Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun, Kanun No: 5982, Resmi Gazete Tarihi: 13.05.2010, Sayı: 27580, 2010 yılında 5982 sayılı Kanun ile gerçekleştirilen Anayasa değişikliği ile Anayasa'nın 20. maddesine kişisel veriler ile ilgili olacak şekilde ilave bir fıkra eklenmiştir; **ÜZELTÜRK TAHMAZOĞLU**
, s. 3152.

[22] R.G. T. 07.04.2016, S. 29677.

sürmekte olan Avrupa Birliği aday ülkesi ülkemiz bakımından da son derece önemlidir.

Kişisel verilerin korunmasına ilişkin uyumlaştırma kapsamında karşılaşılabilecek sorunlar ve bu sorunlara yönelik çözüm önerilerini incelediğimiz çalışmamız, iki bölümden oluşmaktadır. Birinci bölümde, bir hak olarak kişisel verileri koruma kavramı ele alınacak olup, kişisel verileri koruma ihtiyacının hukuki niteliği üzerinde durulacak; kişisel verileri korunma hakkı kapsamında "mülkiyet hakkı", "fikri mülkiyet hakkı" ve "kişilik hakkı" görüşlerine de bu bölümde yer verilerek, kişisel verilerin işlenmesine ilişkin ilkeler ve bu ilkelerin işlenme esaslarına değinilecektir. Çalışmamızın birinci bölümünde ayrıca kişisel verileri koruma hukuku kapsamında, kişisel veri, kişisel verinin unsurları, genel özel nitelikli veri gibi bazı temel kavramlara ilişkin açıklamalar yapıldıktan sonra, kişisel verilerin korunmasına ilişkin düzenlemelerin tarihsel gelişim süreci hem uluslararası hem de yasal mevzuatımız ele alınarak incelenecektir. İkinci bölümde, çalışmamızın ana konusunu oluşturan Kişisel Verileri Koruma Kanunu'nun AB Genel Veri Tüzüğüne uyumlaştırması bakımından ele alınması gereken kavramlar ve kavram farklılıkları ele alınmıştır. Bu kapsamda, veri sorumlusuna ve veri işleyene düşen ek görev ve yükümlülüklerin mevzuatımıza uyum sürecinde nasıl değerlendirileceği üzerinde durulmuştur. Veri sorumlusuna ve veri işleyene düşen ek görev ve yükümlülüklerden, özellikle Tasarım ile Gizlilik ve Varsayılan Gizlilik dahil olmak üzere alınması gereken idari ve teknik tedbirler, Veri Koruma Etki Değerlendirmesi Yapmak ve Ön İstişarede Bulunma hususları irdelenmiştir. Buna ek olarak, Kişisel Verileri Koruma Kanun'u ile farklılık gösteren AB Veri Koruma Tüzüğü İlkeleri üzerinde durulmuş, bölüm devamında Veri Koruma Görevlisi kavramı, Veri Koruma Görevlisine ihtiyaç duyulma nedenleri irdelenmiş, bu kurumun mevzuatımızda yer alması halindeki hususlar irdelenmiştir. Son olarak Veri sahibinin ek haklarından veri taşınabilirliği hakkı ve unutulma hakkı üzerinde durulmuş olup, Avrupa birliği dışına kişisel veri aktarımın hukuki boyutu incelenerek bölüm tamamlanmıştır.

BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN BİR HAK OLARAK KORUMASI VE BAZI TEMEL KAVRAMLAR

I. KİŞİSEL VERİLERİN BİR HAK OLARAK KORUNMASI

A. KİŞİSEL VERİLERİN KORUNMA İHTİYACININ HUKUKİ NİTELİĞİ

1990'lı yıllardan itibaren internet kullanımının yaygınlaşması ve beraberinde getirdiği teknolojik ilerlemeler ile kişisel verilerin işlenmesi, kayıt altına alınması, paylaşılması gibi hususlar önem kazanmıştır. Günümüzde devlet kurumları ve özel sektör anlamında çok sayıda kişiye ait veriler hızla işlenmekte ve aktarımı sağlanmaktadır[23]. Kişilere ait bu denli büyük verilerin paylaşımı, kişisel verilerin korunması ihtiyacını da gerekli kılmaktadır.

Kişisel verileri koruma hukuku Medeni Hukuk bakımından yalnızca kişilerin özel hayatlarına ilişkin verileri ele almakla kalmaz, aynı zamanda temel bir kişilik hakkı olarak uluslararası düzenlemeleri konu edinmektedir. Nitekim temel bir hak olan kişisel verilerin korunması hakkı ve bu anlamda kişilik hakkı, uluslararası anlamda pek çok sözleşme ile de korunmaktadır. Bunun yanında mevzuatımızda olduğu gibi devletler kişisel verilerin korunmasını özel hukuk alanı dışında anayasal güvencelerle kamu hukuku koruması altına almaktadır. Mevzuatımızda da Anayasa'nın 20. maddesiyle "kişisel verilerin korunmasını talep etme hakkı" yer almaktadır.

Teknolojinin hızla aldığı seyir, küresel anlamda kişisel verilerin korunması konusunda ortak bir görüş birliği sağlanmasına katkı sağlamıştır. Bu bağlamda ilk sorulacak soru, kişisel verileri niçin korunmaya ihtiyaç duyulduğudur. Bir diğer soru da kişisel verileri korumanın yasal gerekçesinin ne olduğu yönündedir. Bu sorular, kişisel verilerin hangi veri gruplarını kapsadığı, kişisel verinin öznesinin kim olduğu,

---

[23] **Kişisel Verileri Koruma Kurumu**, "KVKK Uygulama Rehberi", s. 11. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF (Son Erişim Tarihi: 17.04.2021).

kişisel verileri koruma yöntemlerinin ne olması gerektiğine kadar pek çok soruyu beraberinde getirmektedir[24].

Kişisel veriler doğal olarak insan mahremiyetinin bir parçasıdır. İçinde bulunduğumuz çağın "bilgi çağı" olarak ifade edildiği göz önüne alındığında, teknolojide yaşanan gelişmeler sonucu mahremiyet haklarının kolaylıkla ihlal edilmesi, bu hakkın korunmasına yönelik önemi ifade etmektedir[25]. Mahremiyet hakkının yasal olarak korunması özellikle Samuel Warren ve Louis Brandies'in "Gizlilik Hakkı[26]" isimli makalelerini yayınlamasıyla büyük bir önem kazanmıştır[27]. Temel bir hak olarak kişisel verilerin korunması, bireylerin mahremiyetine ilişkin olup, kişilerin gizliliklerini korumayı da hukuken gerekli kılmaktadır[28]. Ancak unutulmamalıdır ki, kişisel veri ihlaline sebep olacak unsurlar kişinin mahremiyet hakları ile sınırlandırılamayacak kadar geniş ölçüdedir.

1. Özel Hayatın Gizliliği Kapsamında Kişisel Verilerin Korunması

İnsanlar özgür varlıklar olarak, yaşam hakkını haiz kişiliğini kendi serbestisi içerisinde sürdürme arzusunu taşımaktadır. İnsan olarak kişiliğin bir yansıması kabul edilen yaşam hakkının içerisinde de özel hayatının korunması ilkesi yatmaktadır[29].

Günümüzde teknolojinin ilerlemesi sonucu bilgi ve iletişim teknolojilerinin hayatımızda her geçen gün daha fazla kullanılıyor olmasıyla, kişisel verileri işlenen kişilerin özel hayatlarının ve gizliliklerinin ihlal edilmesi sorunu daha fazla önem kazanmıştır. Bu anlamda, kişilerin özel hayatına ilişkin her türlü ihlalin önüne geçmeyi konu alan pek çok ulusal ve uluslararası düzenlemeler yapılmıştır. Nitekim "Avrupa İnsan Hakları Sözleşmesi" (AİHS), 8. madde[30] kapsamında, kişilerin özel ve aile

---

[24] **KILINÇ** Doğan, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 61, Sayı 3, 2012, ss.1089-1169, s. 1192.

[25] **KILINÇ**, s. 1191; **ÇEKİN** Mesut Serdar, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 3. Baskı, On İki Levha Yayıncılık, İstanbul 2020, s. 5.

[26] **WARREN** Samuel D. & **BRANDEIS** Louis D., "The Right to Privacy", Vol. 4, No:5, Harvard Law Review, 15 Aralık 1890, ss.193-220, s. 193

[27] **KÜZECİ** Elif, Kişisel Verilerin Korunması, On İki Levha Yayınları, 4. Baskı, İstanbul, Mayıs 2020, s. 81.

[28] **Kişisel Verileri Koruma Kurumu**, "KVKK Uygulama Rehberi", s. 12.

[29] **AKGÜL** Aydın, "Kişisel Verilerin Korunmasında Yeni Bir Hak: 'Unutulma Hakkı' Ve AB Adalet Divanı'nın 'Google Kararı'", TBB Dergisi 2016 (116), ss.11-38, s. 19; **DURAL** Mustafa/**ÖĞÜZ** Tufan, Türk Özel Hukuku, Cilt II, Kişiler Hukuku, Filiz Kitabevi, İstanbul, 2020, s. 137.

[30] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950 (Avrupa İnsan Hakları Sözleşmesi bir diğer ifade ile İnsan Hakları ve Temel Özgürlüklerin

yaşamlarında saygı görülme hakkını düzenlemiştir. Sözleşme'nin 8. maddesi, "özel hayat ve aile hayatına saygı hakkı" ile dört ana hakkı korumayı amaçlamıştır. Dört ana hak kapsamında, "özel hayata saygı", "aile yaşamına saygı", "haberleşme hakkına saygı" ve "konut hakkına saygı" hakları güvence altına alınmıştır. 8. madde de bu haklara ilişkin tanımlamalar yer almasa da Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde bu haklar yorumlanmakta ve Avrupa İnsan Hakları Mahkemesi[31] içtihatları ile de karara bağlanmaktadır[32].

Hukukumuzda da Anayasa m. 20 ile herkesin, özel ve aile hayatına saygı gösterilmesi hakkına sahip olduğu ifade edilmektedir. Bunun yanı sıra, AİHS'nin 8. maddesi ile korumaya alınan diğer haklar da Anayasa'nın ilgili maddeleri ile güvenceye kavuşmuştur. Nitekim Anayasa'nın "kişinin dokunulmazlığı ile maddi ve manevi bütünlüğü" başlıklı 17. maddesi, "konut dokunulmazlığı" başlıklı 21. maddesi, "haberleşme hürriyeti" başlıklı 22. maddesi, Sözleşmenin 8. maddesi ile de uyumlu olacak şekilde düzenlenmiştir[33].

Özel hayatın gizliliği kavramı her ne kadar mahremiyet hakları ile eşdeğer ifade edilse de kişisel verilerin ihlalini oluşturacak her unsur kişinin mahremiyet haklarını kapsamayacak kadar geniş nitelikte olabilmektedir[34]. Kişinin sosyal hayatı, iş ve meslek yaşamı, alışkanlıkları, hobileri gibi pek çok unsuru kapsayan veriler kişinin özel hayatına ilişkin olabilmektedir[35]. Nitekim Avrupa İnsan Hakları Mahkemesi'nde, Sözleşme'nin 8. maddesi ile koruma altına alınmak istenen hususlar, geniş bir

---

Korunmasına İlişkin Sözleşme (European Human Rights Convention), 4 Kasım 1950'de İnsan Hakları Bildirisinde bulunan hakları topluca güvence altına almak için Avrupa Konseyi üyelerinin üzerinde anlaştıkları metindir.*"*

[31] Kısaca AİHM.

[32] Bkz. Niemietz-Almanya kararı, p. 29 (https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57887%22]}), Axel Springer AG /Almanya kararı, p. 83 (https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-109034%22]}), Avrupa İnsan Hakları Mahkemesi, Rotaru -Romanya Davası, Başvuru Numarası: 28341/95, 4 Mayıs 2000, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]} (Son Erişim Tarihi: 02.05.2021); Benedik/Slovenya kararı, p.107-108 (https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-182455%22]}); **ÖNCÜ ARSLAN** Gülay, "Özel Yaşama ve Aile Yaşamına Saygı Hakkı", Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi – 8, Anayasa Mahkemesine Bireysel Başvuru Sisteminin Desteklenmesi Ortak Projesi, Avrupa Konseyi, 2019, s. 23.

[33] **ÖNCÜ**, s. 23.

[34] **ROAGNA** Ivana, Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması Avrupa Konseyi insan hakları el kitapları, Türkçeye Çeviren: Ayşe Gül Alkış Schäling, Avrupa Konseyi, Strazburg, 2012, s. 12.

[35] **ÖNCÜ**, s. 25.

yorumlamaya tabi olduğu gibi hukukumuzda da özel hayatın gizliliği kapsamını ele alan hükümler oldukça geniş şekilde yorumlanmaktadır[36].

Özel hayat genel kabule göre, *"Kişinin başkalarının bilgisinden korumak istediği her türlü görünümü, kendi iradeleri ile gerçekleştirdikleri faaliyetlerinden hangilerinin başkaları tarafından bilinmesini istediklerini içerir iradelerini, olayları ya da tarafları"* ifade etmektedir[37]. Bu anlamda kişinin özel hayatına ilişkin üç unsurun varlığından söz edilir. Bu unsurlar bireylerin yaşam alanlarını, "kamuya açık yaşam alanı", "özel yaşamlarını ilgilendiren alan" ve "gizlilik alanı" olarak üç gruba ayırmakta ve kişinin özel hayatına ve gizlilik hayatına yapılacak her türlü saldırıyı da kişilik hakkı ihlali olarak adlandırmaktadır[38]. Kişinin özel hayatına ya da gizliliğine ilişkin yapılacak her türlü müdahale ise kişilik haklarına bir saldırı olarak hukuka aykırı kabul edilmektedir.

Teknolojinin gelişmesi ve internet kullanımının artması ile kişisel verilerin ihlali ile mahremiyet haklarının zarar görmesi çok daha kolay hale gelmiştir. Bu bağlamda, Anayasa'nın 20. maddesine, kişisel veriler ile ilgili olacak ilave bir fıkra eklenmiştir. Söz konusu fıkrada; her bireyin kendilerini ilgilendiren kişisel verileri konusunda bu verilerin korunmasını isteyebileceği, kişisel verileri konusunda bilgilendirilmeyi, bu verilere erişmeyi ya da bunların düzeltilmesini ya da silinmesini talep edebilecekleri düzenlemiştir. Bu anlamda özel hayatın gizliliğine ilişkin iki yönlü bir koruma olduğundan söz edilebilir. İlk olarak kişilerin özel hayatlarına ya da gizliliklerine ilişkin her türlü ihlalin, kişilik haklarının korunması kapsamında özel hukuk ve ceza hukuku yönünden korunmasıdır. Özel hukuk, özel hayatın gizliliğine ilişkin doğacak zararlara karşı tazmin yolunu düzenlerken; özel hayatın gizliliğine ilişkin her türlü tecavüzde ceza hukuku hükümleri de devreye girmektedir[39]. İkinci olarak özel hayatın gizliliği, devletin herhangi bir ihlaline karşı koruma sağlamaktadır. Zira devletlerin pozitif yükümlülükleri gereği insan haklarına saygı göstermek ve bu hakları yerine getirme yükümlülükleri bulunmaktadır[40]. Bu anlamda devletlerin,

---

[36] **AKSOY** Hüseyin Can, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara 2010. s. 48 vd.; **EREN** Fikret, Borçlar Hukuku Genel Hükümler, 18. Baskı, Yetkin Yayınları, Ankara 2015, s. 803.

[37] **KILINÇ** Doğan, s. 1101.

[38] **DURAL/ÖĞÜZ**, s. 138; **ŞİMŞEK**, s. 140; **AKYÜREK** Güçlü, Özel Hayatın Gizliliğini İhlal Suçu, 2. Baskı, Seçkin Yayıncılık, 2014, s. 25-26.

[39] **BOZLAK** Ayhan, Avrupa İnsan Hakları Mahkemesi Kararları Çerçevesinde Türk Ceza Hukukunda Özel Hayatın Korunması, Adalet Yayınevi, Ankara, 2013, s. 266.

[40] **DEĞİRMENCİOĞLU** Burcu, "Klasik Egemenlik Anlayışında Bir Kırılma: "Pozitif Yükümlülük Doktrini" ve Türkiye'ye Yansıması", İnsan Hakları Yıllığı Cilt 39, 2021, ss. 55-104, s. 72.

bireylerin haklarını güvence altına almak için gerekli tedbirleri almaları gereklidir[41]. Ancak bu tedbirlerin uygulanabilir tedbirler olması gerekir. Bu yönüyle sağlanan koruma, anayasal düzenlemelerde yer alan korumayı amaçlamaktadır[42].

2. Bağımsız Temel Bir Hak Olarak Kişisel Verilerin Korunması

İnsan hakları, insan şeref ve haysiyetini, maddi ve manevi gelişimini korumayı amaçlayan temel haklar olarak isimlendirilmektedir[43]. Temel hakların, temel olarak değerlendirilmesinin nedeni, tüm diğer haklardan yararlanmak için bu hakların korunmasının zorunlu olmasından kaynaklanmaktadır. İnsanların toplum içerisinde yaşamaya başladıkları andan itibaren, insan hakları kavramı da devamlı gelişmekte olan bir konu olup, bu gelişmeler günümüz teknolojik ilerlemeleri ile halen ilerleyişini sürdürmektedir[44].

İnsan hakları, "insan" kavramı ve "hak" kavramları temelinde kurulmuş olduğundan, insan yönü ile gerçek kişileri ifade etmektedir. İnsanın, insan olarak kişiliğine sıkı sıkıya bağlı temel hakları başkalarına devredilememekte, zamanaşımına uğramamakta ve bu haklardan feragat etmek mümkün olmamaktadır. Bu temel haklar, insan olmanın bir özelliği olarak herkese karşı ileri sürülebilen haklardandır[45]. Devletler de bu temel hakları korumaya alarak, kişilerin bu haklarının ihlaline yönelik her türlü tedbiri almakla yükümlüdürler.

Kişisel verileri koruma hakkının temel bağımsız bir hak olarak ortaya çıkışı, özellikle AB Temel Haklar Şartı'nın 8. maddesi ile önem kazanmıştır. AB Temel Haklar Şartı 8. madde ile kişisel verileri koruma hakkı yeni ve bağımsız bir hak olarak değerlendirilmeye başlanmıştır. Özellikle ABAD'ın içtihatları ve AİHM içtihatları ile değerlendirildiğinde, kişisel verilerin koruma hakkının ayrı bir özerk hak statüsünde

---

[41] **AKANDJİ-KOMBE** Jean-François, Avrupa İnsan Hakları Sözleşmesi Kapsamında Pozitif Yükümlülükler, Avrupa İnsan Hakları Sözleşmesinin Uygulanmasına İlişkin Kılavuz Kitap, İnsan Hakları El Kitapları, No. 7, 1. Baskı, 2008, s. 7.

[42] **KILINÇ**, s. 1103.

[43] **TEZCAN** Durmuş/**ERDEM** Mustafa Ruhan/**SANCAKTAR** Oğuz, Avrupa İnsan Hakları Sözleşmesi Işığında Türkiye'nin İnsan Hakları Sorunu, Gözden Geçirilmiş 2. Baskı, Seçkin Yayınları, 2004, s. 43.

[44] **TEZCAN/ERDEM/SANCAKTAR**, s. 46; **KORKMAZ** Ali, "İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması", KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi 16 (Özel Sayı I): 99-103, 2014, s. 100.

[45] **TEZCAN/ERDEM/SANCAKTAR,** s. 46.

yer almaya başladığı görülmektedir[46]. ABAD'ın 13 Mayıs 2014 tarihli Google-İspanya[47] kararı temel bir hak olarak kişisel verileri koruma hakkına önemli bir örnektir. Karar ile, çoğunlukla mahremiyet hakları kapsamında özel hayatın gizliliğine ilişkin haklar kategorisinde değerlendirilen kişisel verilerin korunması hakkının yarattığı karmaşıklığın önüne geçilmeye çalışılmıştır. Her ne kadar başlıkta bahsi geçtiği üzere kişisel verileri koruma hakkı bağımsız temel bir hak olarak kabul edilse de kanaatimizce de söz konusu hakkın kişinin mahrem alanın korunması hakları ile sınırlandırılamayacak ölçüde geniş bir kişilik hakkını ele aldığını ifade edebiliriz.

B. KİŞİSEL VERİLERİN KORUNMASI HAKKININ DAYANDIĞI HUKUKİ GÖRÜŞLER

Kişisel verilerin korunması hakkının yukarıda ifade edilen diğer hak kategorileriyle olan ilişkisini daha iyi ifade edilmek adına, kişisel verileri koruma hakkının dayandığı temel görüşleri değerlendirmek gereklidir. Kişisel veri kavramının dayandığı görüşlerin bir kısmı ekonomik açıdan değerlendirilirken bir kısmı da insan hakları açısından değerlendirilmektedir. Bu amaçla kişisel verilerin korunması hakkı kapsamında temel olarak üç görüş olduğu ifade edilmektedir. Bu görüşler ekonomik bir hak olarak değerlendirilen mülkiyet hakkı ile fikri mülkiyet hakkı görüşü ve kişisel verileri temel bir insan hakkı olarak şahsi hak kapsamında değerlendiren kişilik hakkı görüşü olarak ifade edilmektedir. Aşağıda kişisel verilerin korunması hakkı kapsamında bu görüşler incelenecektir.

1. Mülkiyet Hakkı Görüşü

Mülkiyet hakkı, ulusal ve uluslararası düzenlemelerde temel bir hak olarak karşımıza çıkmaktadır[48]. Mevzuatımız açısından mülkiyet hakkı, Anayasa'nın 35. maddesi ile düzenlenerek yasal güvence altına alınmıştır. Nitekim AİHS'nin Ek

[46] Google/İspanya Kararı; **ERDOS** David, "The Emergence of Personal Data Protection as a Fundamental Right of the EU." Cambridge Law Journal, vol. 74, no. 2, July 2015, ss. 374-375, s. 374.
[47] **ERDOS**, s. 375.
[48] **OĞUZMAN** Kemal/**SELİÇİ** Özer/**ÖZDEMİR OKTAY** Saibe, Eşya Hukuku, Filiz Kitabevi, 23. Bası, İstanbul, 2021, s. 28; **AYBAY** Aydın/**HATEMİ** Hüseyin**,** Eşya Hukuku, Gözden Geçirilmiş 4. Bası, Vedat Kitapçılık, İstanbul, 2014, s. 3; **GEMALMAZ** Burak, "Mülkiyet Hakkı", Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi– 6, İstanbul, 2018, s. 1.

Protokolü'nde yer alan 1. madde ile de mülkiyet hakkının kapsamı ve sınırları ifade edilmiştir.

Medeni Hukukta ayni haklar, iki gruba ayrılmaktadır[49]. Mülkiyet hakkı, ayni bir hak olarak kişiye "kullanma", "yararlanma" ve "tasarrufta bulunma" haklarını tanıyan en geniş mutlak hak olarak ifade edilmektedir. Bu anlamıyla sınırlı ayni haklardan farklı olarak kişiye bu üç yetkiyi kullanma imkânını veren tam bir ayni haktır[50]. Geçmişte mülkiyet kavramı daha çok sosyal ve ekonomik açıdan değerlendirilmiş iken günümüzde bu anlayış yerini daha modern ve mülkiyet kavramını daha geniş yorumlayan bir anlayışa dönüşmüştür. Bu anlamda mülkiyeti yalnızca "eşya" olarak değerlendiren görüş yerini maddi olmayan nitelikteki mal varlığı değerlerini de kapsayacak şekilde gelişmiştir[51].

Tarihsel gelişimine bakıldığında mülkiyet hakkını savunan klasik görüş, bu hakkı mutlak ve dokunulmaz bir hak olarak değerlendirmektedir. Ancak zamanla gelişen modern anlayış ile mülkiyet hakkı, özel mülkiyet kavramını kabul eden ve bu hakkın kullanımını kamu yararına sınırlandıran bir anlayışa dönüşmüştür.

Özellikle ABD Hukuku'nda mülkiyet anlayışına dayalı bir yaklaşımın kabul edildiği görülmektedir. Mülkiyet yaklaşımını savunanların temel argümanı, kişisel verilerin metalaştırılmasına yönelik günümüzdeki gelişmeler karşısında bireylere, kendileriyle ilgili bilgilerde bir tür mülkiyet hakkı verilmesi gerektiği yönündedir. Bazı yazarlar veri gizliliği tartışmasını çözmenin bir yolu olarak kişilere, kişisel verileri bakımından mülkiyet haklarının tanınması gerektiğini ifade etmiştir[52]. Kişilere, kişisel verilerini korumada mülkiyet hakkı esası tanınmasında iki temel nokta olduğu ifade edilmektedir. İlki, bireylere kişisel verileri üzerinde bir eşya gibi dilediği şekilde tasarrufta bulunma yetkisi sağlamaktır[53]. Çünkü bireylerin kişisel verilerini kontrol etmede kendilerine ait açık çıkarları vardır ve bu nedenle mülkiyet kavramının

---

[49] **OĞUZMAN/SELİÇİ/ÖZDEMİR OKTAY**, Eşya Hukuku, s. 28; **AYBAY/HATEMİ,** Eşya Hukuku, s. 3; **ÖZLÜK** Betül, "Mülkiyet ve Zilyetlik Üzerine Düşünceler", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 27, S. 1, 2019, ss. 139-166, s. 141.

[50] **AYAN** Mehmet, Eşya Hukuku II, Adalet Yayınevi, 10. Baskı, Ankara, 2020, s. 28; **OĞUZMAN/SELİÇİ/ÖZDEMİR,** Eşya Hukuku s. 28; **AYBAY/HATEMİ,** s. 116; **ÖZLÜK,** s. 141

[51] **ÖZLÜK,** s. 141.

[52] **BARTOW** Ann, "Our Date, Ourselves: Privacy, Propertization, and Gender." University of San Francisco Law Review, vol. 34, no. 4, Summer 2000, p. 633-704, s. 688.

[53] **KANG** Jerry, "Information Privacy in Cyberspace Transactions." Stanford Law Review, vol. 50, no. 4, April 1998, p. 1193-1294, s. 1246; **LITMAN** Jessica. "Information Privacy/Information Property." Stanford Law Review, Vol. 52, No. 5, May 2000, p. 1283-1314, s. 1287; **JANGER** Edward J, "Privacy Property, Information Costs, and the Anticommons." Hastings Law Journal, vol. 54, no. 4, 2002-2003, p. 899-930, s. 903.

faydalarından yararlanmaları gerekir. İkincisi, kişisel verileri toplayan, kullanan, işleyen ve üçüncü kişilere bu verileri aktaran şirketlere yönelik kişisel veri sahiplerine bu veriler karşılığında bir kazanç sağlamaktır[54].

Ancak Samuelson'a göre kişisel verilerin korunmasına yönelik mülkiyet hakları modeli yine de birçok sorunu beraberinde getirmektedir[55]. Nitekim yazar, mülkiyet hakkı esasına dayalı yaklaşımın, özel hayata bir insan hakkı olarak değer veren hukuk sistemlerinde bir geleceği olmadığını ifade etmektedir. Samuelson, kişilerin kendileriyle ilgili verilere sahip olduklarını veya sahip olmaları gerektiğini son derece doğal değerlendirmesine rağmen mülkiyet hakkı görüşünün benimsenmesinin olumsuzluklarını ifade etmiştir. Kişiler, kişisel verilerine ilişkin olarak üçüncü kişilerin bu verilere erişimini kısıtlamak için menfaat dengesini aşan yasal bir hakka sahip olabileceklerdir. Keza bu veriler hastanelerin, doktorların, bankaların ya da sigorta şirketleri gibi kurumların kullanımında olsa dahi mülkiyet hakkı kapsamında kişiler bu veriler üzerinde söz sahibi olmaya devam edeceklerdir. Oysa kanun koyucular kişisel verileri, kişilerin menfaatlerini yanlış kullanma durumlarına karşı korumakla yükümlüdürler.

Kişisel verileri korumaya yönelik mülkiyet hakları yaklaşımının daha fazla kişisel veri gizliliği elde etmek için istenen etkiyi sağlama ihtimali de düşük görünmektedir. Nitekim Samuelson, Avrupa Birliği hukukunda kişisel veri gizliliğini, insanların yaşamak isteyeceği bir bilgi toplumuna ulaşmak için mimarinin temel taşı olması gereken bir değer olarak ifade etmiştir[56]. Bu yaklaşımın ABD hukuku içinde bazı önemli çıkarımları olabileceğini ifade ederek, Avrupa'da olduğu şekli ile bireylerin kişisel verilerinde birden fazla ilgi alanına sahip olunduğunu kabul etmenin de bir ilerleme olduğunu vurgulamıştır[57]. Nitekim 2016/679 sayılı GVKT'nin yürürlüğe girmesi ile kişisel verilere ilişkin mülkiyet anlayışının yaygınlaştığı kabul edilmekte ve mülkiyet haklarına bağlı kazanımların giderek daha fazla görünür kılındığı ifade edilmektedir[58].

---

[54] **SAMUELSON** Pamela, "Privacy as Intellectual Property." Stanford Law Review, vol. 52, no. 5, May 2000, p. 1125-1174, s. 1130.
[55] **SAMUELSON**, s. 1130.
[56] **SAMUELSON**, s. 1172.
[57] **SAMUELSON,** s. 1172.
[58] **HAZEL** Steven H., "Personal Data as Property." Syracuse Law Review, vol. 70, no. 4, 2020, p. 1055-1114, s. 1186.

2. Fikri Mülkiyet Hakkı Görüşü

Mülkiyet kavramının giderek önem kazanması ve kapsamının genişlemesi ile küreselleşen dünyada bilgi teknolojilerinin giderek önem kazanması, fikri mülkiyet hakkı yaklaşımına da önem kazandırmıştır. Esasında maddi malvarlığı değerleri üzerine kurulan mülkiyet hakkı görüşü, telif hakları, marka ve patentler, ticari sırlar gibi fikri mülkiyet hakları karşısında bu ilkenin benimsenmesine yol açmıştır. Zira günümüzde gelişen teknolojiler sayesinde fikri mülkiyet hakların korunması giderek önem kazanmakta, bir yandan da bu haklara ilişkin yapılan ihlaller artmaktadır[59].

Fikri mülkiyet hakları, en genel tanımıyla insan zekâsı gereği ortaya çıkan ve maddi olmayan varlıklar olarak ifade edilmektedir[60]. Fikri mülkiyet haklarının korunması, ülkelerin küreselleşen pazar ekonomisindeki menfaatleri açısından da son derece önemli görülmektedir[61]. ABD hukukundaki bazı yazarlar, kişisel verilere ilişkin hakların fikri mülkiyet hakları kapsamında korunabileceği görüşünü benimsemektedir[62]. Bu noktada kişisel veriler, gelişen teknolojik araçlar karşısında korunmaya muhtaç olan fikri mülkiyet haklarından telif hakları kapsamında değerlendirmektedir[63]. Nitekim bir eser sahibinin o eser üzerindeki hakkı ile bu eserin kamuya arz edilmesinden sonra sahip olduğu haklar değerlendirildiğinde, kişisel veriler açısından da benzer bir değerlendirme yapılabileceği düşünülmektedir. Bununla birlikte gerek fikri mülkiyet hakları açısından gerek kişisel verilerin korunması bakımından kişilerin üzerinde hak iddia edebildikleri ancak bu hakkın denetimini yitirebildikleri bir veri bulunmaktadır[64].

Ann Bartow'un yaklaşımında olduğu gibi, bilginin metalaşmasının kaçınılmaz olduğu göz önüne alındığında, kişisel verilerin korunması noktasında fikri mülkiyet yaklaşımının benimsenmesi yerinde görülmektedir[65]. Bu anlamda, fikri mülkiyetin

---

[59] **YÜKSEL** Mehmet, "Fikri Mülkiyete İlişkin Felsefi Tartışmalar", Türkiye Barolar Birliği Dergisi, 2001/1, ss.177-198, s. 177.
[60] **BOZBEL** Savaş, Fikri Mülkiyet Hukuku, On İki Levha Yayınları, 1. Baskı, İstanbul, Eylül, 2015, s.17; **TEKİNALP** Ünal, Fikri Mülkiyet Hukuku, Beta Yayınları, Güncelleştirilmiş ve Gözden Geçirilmiş Üçüncü bası, Eylül, 2014, s. 5.
[61] **SULUK** Cahit, "Fikri Mülkiyet Hakları, Uygulamada Yaşanan Sorunlar ve Çözüm Önerileri", Kazancı Hukuk İşletme ve Maliye Bilimleri Dergisi, C.I, S.7, 2005, s. 7.
[62] **PRINS** Corien "When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter." SCRIPTed: A Journal of Law, Technology and Society, Vol. 3, No. 4, December 2006, ss. 270-303, s. 274; **BARTOW,** s. 685.
[63] **KÜZECİ**, s. 71.
[64] **KÜZECİ**, s. 71.
[65] **PRINS**, s. 274; **BARTOW,** s. 685.

korunması ile mahremiyetin korunması arasında bir ilişki olduğunu savunmaktadır[66]. Bu düşüncede olan yazarların ortak arzusu, kişisel verilerin dağılımını ve kullanımını korumak ve kontrolünü sağlamaktır. Nitekim, ses kayıt ve film endüstrisinin dijital haklar sağlayan teknolojik araçlarla kontrol altında tutulma amaçları, kişisel verilerin korunmasını güçlendirmek ve geliştirmek isteyenler bakımından da bir örnek teşkil etmektedir.

Öte yandan bu görüşün olumsuzlukları da mevcuttur. Nitekim, kişisel veriler ile ilgili fikri mülkiyet yaklaşımı kabul edildiğinde gerekli tüm verileri fiilen lisanslamak maliyetli, zahmetli ve zaman alıcı olacaktır. Bu durum, şirketlerin ve kuruluşların kişisel verilerini işlemek istedikleri yüz milyonlarca kişinin her birinden izin almaları gerektiği anlamına gelecektir[67]. Üstelik bu görüşte fikri haklarda olduğu şekliyle bir fikrin ortaya konulması amaçlanmaktadır[68]. Oysa kişisel veriler söz konusu olduğunda, böyle bir ihtiyaç yoktur. Bununla birlikte kişisel veriler genellikle kişilerin kendi tercihlerine göre doğmaktadır. Bir diğer ifade ile telif haklarında olduğu gibi kişisel verilerin doğmasında kişilerin özel bir gayreti bulunmamaktadır[69]. Dolayısıyla, telif hakkını çevreleyen mülkiyet rejimleri ile kişisel veri haklarını çevreleyen olası bir mülkiyet rejimindeki farklılıklar, özel mülkiyet, fikri ürünler ve sosyal fayda arasındaki ilişkiler bakımından farklılık oluşturmaktadır.

3. Kişilik Hakkı Görüşü

Avrupa Birliği hukukunda mülkiyet hakları yönünden hatırı sayılır bir "kabul" olduğu ifade edilse de günümüz teknolojik gelişmeleri ile bu yaklaşımın kişisel verileri koruma noktasında daha yüksek bir koruma düzeyi sağlayacağına şüphe ile yaklaşılmaktadır[70].

Kişisel verilerin korunması noktasında, mülkiyet hakkı kabulünün avantajları ve dezavantajları üzerine yapılan pek çok değerlendirme, bu yaklaşımın özel hayata bir

---

[66] **PRINS,** s. 279.
[67] **PRINS,** s. 293; **KÜZECİ**, s. 71.
[68] **TAŞTAN** Furkan Güven, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, Oniki Levha, 1. Baskı, İstanbul, Temmuz 2017, s. 55.
[69] **PRINS,** s. 296; **TAŞTAN,** s. 55.

[70] **PRINS** J.E.J., "The Propertization Of Personal Data And Identities", Electronic Journal of Comparative Law, vol. 8.3, October, 2004, s. 2.

insan hakkı olarak değer veren hukuk sistemlerinde bir geleceği olmadığı yönündedir. Mülkiyet hakları aracılığı ile mahremiyet kavramının korunması daha çok ABD hukukunda destek görmektedir. AB hukukunda ise kişisel verilere yalnızca mahremiyetin korunması yönünden değil, insan hakları perspektifinden yaklaşılmasının temel nedeni, mahremiyet haklarının doğası gereği kişilere sıkı sıkıya bağlı haklardan olmasıdır. Zira bu haklardan feragat edilebilmesi ya da devredilebilmesi mümkün de değildir.

Özellikle 1950 tarihli AİHS ile bireylerin "özel hayatlarına saygı hakkı", AİHM tarafından AİHS m. 8. ile geniş bir ölçüde yorumlanmıştır. Zaman içerisinde mahremiyet kavramı yalnızca bir menfaat ya da hak olarak değil, aynı zamanda "temel bir hak" olarak değerlendirilmeye başlamıştır. Ancak mahremiyet haklarının kişinin yalnızca "gizlilik" alanına ilişkin olması, kişisel verilerin korunması noktasında yeterli görülmediğinden eleştirilmektedir[71]. Bu eleştirilerin temelinde, Alman Anayasa Mahkemesi'nin 1983 tarihli "Nüfus Sayım Kararı"[72] etkili olmuştur[73]. Alman toplumu, bu istatistiksel sayım kararının, menfaatleri aşan ve özel hayatı ihlal niteliği taşıyan bir karar olduğunu vurgulamıştır. Ancak kararda daha önemli ölçüde vurgulanan, devletin bireylerin kişisel verileri üzerindeki tasarruf yetkisinin kapsamı olmuştur. Alman Anayasa Mahkemesi, Nüfus Sayım kararının kısmen anayasaya aykırı olduğuna karar vererek ilgili kararı iptal etmiştir[74]. Verilen iptal kararı, Alman Veri Koruma tarihindeki en önemli kararlardan biri olarak görülmektedir. Zira bu karar ile Mahkeme, kişilerin kendi verileri üzerinde tasarrufta bulunma hakkının kişilere ait olduğunu vurgulayarak, *"kişisel verileri üzerinde kendi kaderini tayin etme hakkı"* kavramını tanımlamıştır[75].

Bu hakkın tanımlanmasında, özellikle Nüfus Sayım Kararı'nın yarattığı etki gerekçe oluşturduğundan, kişilerin verileri üzerinde kendi kaderini tayin etme hakkını mülkiyet hakkı kavramından ayrıştırmak gerekir. Kişisel verileri üzerinde kişinin kendi kaderini tayin etme hakkı, kişiye kendi kişisel verileri üzerinde bir tasarruf yetkisi tanımaktadır. Ancak bu tasarruf yetkisinin, kişinin kişisel verileri üzerinde tam ve

---

[71] **TAŞTAN**, s. 64.

[72] 15 Aralık 1983 tarihli Nüfus Sayım Kararı'nın İngilizce Metni için bkz. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html (Son Erişim Tarihi:08.05.2021).

[73] **TAŞTAN**, s.64; **ŞİMŞEK**, s. 115; **KÜZECİ**, s. 75-77; **HORNUNG** Gerrit /**SCHNABEL** Christoph, "Data protection in Germany I: The Population Census Decision and The Right to Informational Self-Determination", Computer Law & Security Report, Volume 25, Issue 1, 2009, ss. 84-88, s. 84.

[74] **HORNUNG/SCHNABEL,** s. 85.

[75] **HORNUNG/ SCHNABEL,** s. 85; **TAŞTAN**, s. 3.

mutlak bir kontrol mekanizmasını sağlamak niyetinden öte kişilerin bireysel özgürlüklerini sağlamayı amaçladığı ifade edilmektedir[76]. Zira bu hak, bireylerin kişisel verilerinden hangilerine ne amaçlarla ulaşılabildiği, bu bilgilerin ne amaçla saklanıp işlendiği, veri sahibi kişilerce kontrol edilemediği sürece onların menfaatlerinin zedelemesine yol açabilmektedir. Dolayısıyla asıl olarak vurgulanmak istenenin, kişisel verileri üzerinde kişilerin tam hâkimiyetinin sağlanması değil, devletin kişisel verilerin işlenmesi ile ilgili gerekli düzenlemeleri yaparak kişilerin menfaatlerinin korunmasını sağlamak olduğu ifade edilmektedir[77].

Bu noktada ifade edilmesi gereken husus, kişisel verileri üzerinde kişinin kendi kaderini tayin hakkının mahremiyet haklarından ayrı olarak ifade edilmesi noktasındadır. Alman Anayasa Mahkemesi, bu hakkı mülkiyet hakkı kavramından ayrıştırdığı gibi özel hayatın gizliliği hakkından da ayrı tutmuş ve bu hakkı insan hakları özelinde insan onuru ve bireysel özgürlük alanından yorumlamıştır[78]. Zira bireylere ait elde edilen kişisel veriler her zaman kişilerin özel hayat alanlarına ilişkin olmayabilir. Bu hak ile asıl olarak amaçlanan mahremiyet haklarına dayalı gizlilik ihlali değil, kişilerin verilerinin kendi tasarrufları dışında elde edilerek işlenmesi noktasında toplanmıştır. Özellikle Nüfus Sayım Kararının etkili olmasında, devletin kişilerin kişisel verilerini işleme tasarrufu sorgulanmıştır.

Kişisel verilerin kişilik hakkı kapsamında özellikle mahremiyet haklarından daha geniş bir perspektifte korunması ihtiyacı açıktır. Kanaatimizce de kişisel verilerin mahremiyet hakları kapsamında yalnızca özel hayatın gizliliğine ilişkin hükümler ile değil, gelişen teknoloji ile sınırlı sayıda sayma ilkesinin geçerli olmadığı kişilik haklarının bir görünümü olarak, temel bağımsız bir hak olarak değerlendirilmesi gerekmektedir[79].

---

[76] **KÜZECİ** Elif, "İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı", İnsan Hakları Yıllığı, Cilt 32, 2014, ss. 53-75, s. 57; **KÜZECİ**, s. 75; **ŞİMŞEK**, s. 119.
[77] **KÜZECİ**, "Bilgilerin Geleceğini Belirleme Hakkı", s. 57.
[78] **KÜZECİ,** "Bilgilerin Geleceğini Belirleme Hakkı", s. 57; **ŞİMŞEK**, s. 134-135.
[79] **YILMAZ** Ozan Barış, Türkiye ve Avrupa Birliği'nde Kişisel Verilerin Korunması ve Uygulanacak Hukuk, Adalet Yayınevi, Ankara 2022, s. 30.

II. KİŞİSEL VERİ İLE İLGİLİ TEMEL KAVRAMLAR

A. GENEL OLARAK

Teknolojik ilerlemeler ile internet kullanımının hız kesmeden devam etmesi karşısında, kişisel verilerin işlenmesi, depolanması ve paylaşılması konuları da önemli boyutlara ulaşmıştır. Özellikle 2016 yılında GVKT'nin yürürlüğe girmesi ile kişisel verileri koruma bakımından küresel anlamda yeni bir sayfa açılmıştır. Gelişen teknoloji ile Genel Veri Koruma Tüzüğü'nün bu ihtiyaçlara karşılık verip veremeyeceği tartışılagelen önemli konulardan biridir. Ancak daha önemli bir husus, çalışma konumuzu esas alması bakımından 95/46/EC sayılı Direktif'in, KVKK'nın mehaz düzenlemelerini barındırması noktasındadır. Direktif'in, AB ülkelerinde uzun yıllar yarattığı problemler karşısında, GVKT ile uyumlu olarak Türk hukukunda yapılacak düzenlemeler, ülkemizde de bu alanda getirilen eleştirilere çözüm olabilecek niteliktedir.

Kişisel verileri koruma hukukunda bahsedilecek temel kavramlar gerek yasal mevzuatımızda gerekse AB Genel Veri Koruma Tüzüğünde yer alan kavramlar bakımından mukayese edilerek incelenecektir.

B. KİŞİSEL VERİ KAVRAMI

Kişisel veri kavramını tanımlamaya geçmeden, bu kavramları ayrı olarak açıklamakta fayda olacaktır. Sözlük anlamı ile değerlendirildiğinde "kişisel" kavramı, kişiye ilişkin, kişiye ait olan şeklinde tanımlanmaktadır. İngilizce anlamı ile *"data", "knowledge", "information"* olarak ifade edilebilen "veri" ise, deney ve gözleme dayalı bir araştırmanın neticelerini yorumlamaya elverişli olarak gösteren bilgiler bütünüdür[80].

[80] TDK Güncel Türkçe Sözlük, https://sozluk.gov.tr/ (Son Erişim Tarihi: 03.04.2021).

1. Kişisel Verinin Unsurları

Ulusal ve uluslararası düzenlemelerde kişisel veri, ortak bir yaklaşımla belirli unsurların bir araya gelmesi ile yorumlanır. Genel kabul gören görüşe göre kişisel verinin unsurları üç temel başlıkta incelenmektedir. Ancak kimi düzenlemelerde kişisel verinin unsurlarının dört temel başlık altında incelendiği de görülmektedir. Çalışmamızda kişisel verinin unsurları, genel kabul gören görüş çerçevesinde üç temel başlık altında incelenecektir. Bu başlıklar, kişisel verinin kaynağı olan bilgi; kimliği belirli ya da belirlenebilir kılan veri sahibi ve kişisel verinin ilgili kişi olan veri sahibine ait olması halidir. Bu anlamda, bir kişiyi belirli kılan ya da kılabilen her türlü bilgiyi kişisel veri olarak değerlendirmek gerekmektedir[81].

a. Kişisel Verinin Kaynağı Olarak Bilgi

Teknolojik ilerlemelerin akıl almaz hızı, özellikle bilgi teknolojilerinde çok sayıda bilginin hızla üretimine, işlenmesine ve dağılımına imkân sağlamaktadır. Bilginin bu denli dağılımı, kişisel verileri koruma anlamında da bu kavramın iyi anlaşılmasını gerekli kılmaktadır. Ulusal ve uluslararası düzenlemelerde, kişisel verinin kabul edilen ilk unsuru bilgidir. Sözlük anlamına bakıldığında bilgi, *"insan aklının erebileceği olgu, öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü*[82]*"* olarak ifade edilir. Ancak bilginin bu geniş tanımı karşısında, çalışma konumuzu oluşturması bakımından "bilgi", "veri" ve "enformasyon" kavramlarının izah edilmesi gerekmektedir[83].

Bilgi, veri ya da enformasyon kavramları ile tam olarak ne anlatılmak istendiği gerek literatürümüzde gerek yabancı kaynaklı literatürde pek çok kez tartışmalara konu olmuş ve bu kavramlarım ayrımı yapılmaya çalışılmıştır[84]. Kavramların ayrımı net bir şekilde ortaya konamadığı gibi kimi zaman birbirlerinin yerine kullanıldıkları da gözlemlenmiştir[85]. Bu karmaşıklığın nedenlerinden biri olarak, İngilizce ifade ediliş

---

[81] **Kişisel Verileri Koruma Kurumu,** "6698 Sayılı Kanun'da Yer Alan Temel Kavramlar", s. 12.
[82] TDK Güncel Türkçe Sözlük, https://sozluk.gov.tr/ (Son Erişim Tarihi: 03.04.2021).
[83] **KÜZECİ,** s. 10 vd.; **AKSOY**, s. 11
[84] **KÜZECİ,** s. 10 vd; **ŞENOCAK** Kemal, "Kişisel Veri Kavramının Kapsamı ve Unsurları" Editör: **ŞENOCAK** Kemal, Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuku, Eskişehir Osmangazi Üniversitesi Hukuk Fakültesi Yayınları-5, Yetkin Yayınları, Ankara 2022., s. 5.
[85] **YILMAZ** Malik, "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi," Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi, 49 (1), ss.95- 118, s. 96.

şekli ile verinin "data", bilginin "knowledge", enformasyonun ise "information" olarak dilimize tek ve ortak bir anlamda çevrilmesi olduğu düşünülmektedir[86].

Bilginin net bir tanımının yapılmasının güç olduğu açıktır. Zira bilginin kaynağına ilişkin eleştirilerde, açıklamaya ihtiyaç duyulan diğer kavram "enformasyon" dur[87]. Bilgiye ulaşmak için yapılan gözlemlerin harf, sayı, görüntü, şekil ya da karakterle ifade edilmesi olarak işlenmemiş en küçük enformasyon "veri" olarak değerlendirilir[88]. Enformasyon ise bir ya da birden fazla verinin toplanmasıyla oluşan ve her kişi için farklı anlamlara gelebilen veri topluluğudur[89]. Bilgiyi oluşturmak için ise enformasyon kullanılır.

Her ne kadar yukarıda açıkladığımız kavramlardan veri, bilgi ve enformasyon tanımları arasında farklılıklar olsa da kişisel verilerin korunması hukuku açısından anlam karmaşası oluşturmamak adına, bu farklılıkların çalışma konumuz bakımından ayrıştırılmayacağını ifade etmek gerekir. Bu anlamda, genel olarak bilginin kaynağı veri ve veri topluluğunun oluşturduğu bilgi kavramları aynı anlamda kullanılacaktır.

b. Kişisel Verinin Unsuru Olarak Kimliği Belirli ya da Belirlenebilir Kişi

Kişisel verinin unsurlarından inceleyeceğimiz ikinci unsur, bilginin kimliği belirli ya da belirlenebilir bir kişiyi tanımlaması halidir. Modern hukuk anlayışında kişi kavramı, gerçek ve tüzel kişiler olarak iki[90] kategoriye ayrılmaktadır. Ulusal ve

---

[86] **YILMAZ**, "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi," s. 97.

[87] **YILMAZ**, "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi," s. 97.

[88] **AKGÜN**, Ali, **KESKİN**, Hüseyin, "Sosyal Bir Etkileşim Aracı Olarak Bilgi Yönetimi ve Bilgi Yönetimi Süreci", Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 1/2003, ss.175-183, s. 176.

[89] **DURNA** Ufuk, **DEMİREL** Yavuz, "Bilgi Yönetiminde Bilgiyi Anlamak Bilgi Yönetiminde Bilgiyi Anlamak", Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Sayı: 30, Ocak-Haziran 2008, ss. 129-156, s. 132.

[90] **AKİPEK** Jale/**AKINTÜRK** Turgut/**ATEŞ** Derya, Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku, Birinci Cilt, Yenilenmiş 16. bası, Beta Yayınları , İstanbul Eylül 2020, s. 242; **ÖZTAN** Bilge, Medeni Hukukun Temel Kavramları, Yetkin Yayınları, 45. Baskı, Ankara, 2020, s. 234; **DURAL**/**ÖĞÜZ**, s. 7; **HATEMİ** Hüseyin/**OĞUZTÜRK KALKAN** Burcu, Kişiler Hukuku (Gerçek Kişiler- Tüzel Kişiler), Vedat Kitapçılık, İstanbul, 2014, s. 7; ; **OĞUZMAN** Kemal/**SELİÇİ** Özer/**ÖZDEMİR OKTAY** Saibe, Kişiler Hukuku, (Gerçek ve Tüzel Kişiler), 20. Bası, Filiz Kitabevi, İstanbul, 2021, s. 2.

uluslararası düzenlemelerde kabul edilen ortak görüş, kişisel verinin süjesini oluşturan kişinin hak ehliyetine sahip olan gerçek kişi olduğu yönündedir[91].

Tüzel kişilerin ise ulusal ve uluslararası mevzuatta kişisel veri süjesi olarak korunup korunmayacağına ilişkin bir görüş birliği bulunmamaktadır[92]. Keza benzer bir durum, ölen kişilerin kişisel verilerinin ne şekilde işleneceğine ilişkin durum için de geçerlidir[93]. Kişisel veri unsuru olarak "kimliği belirli ya da belirlenebilir kişi" için ele alınan son durum ise ceninin kişisel verilerine ilişkin durumdur. Başlığımızda, genel olarak belirli ya da belirlenebilir kişi unsuru açıklandıktan sonra, tüzel kişiliğe, ölenin kişisel verilerine ve cenine ilişkin yöneltilen eleştiriler üç ayrı başlık olarak incelenecektir.

Kişiyi belirli ya da belirlenebilir kılan bilgilerin neler olduğu hususu, belirli bireye özgü ve o kişi ile ilişkili kılınacak bilgiler ile elde edilir. Örneğin, boy, saç rengi, kıyafet gibi kişinin dış görünümüne ait bilgiler ile bir isim, meslek gibi kişiyi hemen belirli kılmaya olanak tanımayan bilgiler, bir kişiyi belirli ya da belirlenebilir kılmaya yetecek nitelikte bir araya gelebilir[94]. Kişinin kimliğinin belirli olması, o kişiyi içerisinde bulunduğu toplumdan ayırt etmeye ve tanımaya yarayacak bilgiyi içerir. Kişinin kimliğinin belirlenebilir olması durumu ise kişiyi belirli kılmaya yetecek bilgilerin yetersiz kaldığı ya da o kişiyi tanımlamaya yetmediği ancak kişiyi içerisinde bulunduğu toplumdan bu ek bilgiler ile ayırt etmeye yarayacak bilgilerdir[95]. Bir diğer ifade ile belirlenebilir olma hali, kişiyi net olarak tanımlamaya yetecek bilgilerin yanında yardımcı bilgilerin de vasıtasıyla gerçekleşir[96].

---

[91] Her ne kadar OECD'nin "Rehber İlkeleri", "108 sayılı Sözleşme", "95/46/EC sayılı Direktif", GVKT ve KVKK'da kişisel veriye konu olan süje yalnızca gerçek kişi olarak kabul edilmiş olsa da 12 Temmuz 2002 tarihli ve 2020/58 sayılı "Elektronik Haberleşme Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkındaki Yönetmelik"te veri sahibi kişilere tüzel kişilerin de dahil edildiğini belirtmek gerekir.

[92] **29. Madde Çalışma Grubu,** WP 136, ss.1-26. s. 23-24.

[93] **29. Madde Çalışma Grubu**, WP 136, s. 24.

[94] **29. Madde Çalışma Grubu**, WP 136, s. 12; **ŞİMŞEK**, s. 122.

[95] **29. Madde Çalışma Grubu**, WP 136, s. 12.

[96] **29. Madde Çalışma Grubu**, WP 136, s. 12; **AKSOY,** s. 21-23**; TAŞTAN**, s. 34-35; **ŞİMŞEK**, s. 122.

aa. Tüzel Kişilere İlişkin Kişisel Verilerin Durumu

Tüzel kişi, belirli bir amaç etrafında bağımsız bir kişilik yaratmak üzere örgütlenerek toplanan insan ya da mal toplulukları olarak ifade edilmektedir[97]. Her ne kadar tüzel kişilerin kişisel verileri koruma hukuku düzenlemeleri karşısında gerekli korumadan yararlanamayacağı yönündeki görüş baskın olsa da 12 Temmuz 2002 tarihli ve 2002/58/EC sayılı Direktif (Elektronik Haberleşme Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkındaki Avrupa Birliği Direktifi) ile veri sahibi kişiler arasında tüzel kişilerin de kabul edildiğini ifade etmek gerekir[98]. Keza Avrupa Birliği'ne üyeliği bulunan Lüksemburg, İtalya, Danimarka, Avusturya, gibi ülkelerin kendi mevzuatlarında da tüzel kişilerin korunduğu görülmektedir[99]. Ancak 2002/58/EC sayılı Direktif'te tüzel kişilerin menfaatlerinin korunması yolu ile veri sahibi olarak kabul edilmelerinin sınırı çizilmiştir. Bu anlamda 2002/58/EC sayılı Direktif, sadece elektronik haberleşme sektörüne ilişkin olarak gerçek ve tüzel kişilerin veri sahibi kabul edileceğini ifade etmektedir.

2008 yılında Adalet Bakanlığı'nca hazırlanan ve TBMM Başkanlığı'na iletilen KVKK Tasarısı'nda tüzel kişilerin bilgilerinin de kanun kapsamında korunacağı ifade edilmişse de hem sonraki tasarı metinlerinde hem de yürürlüğe giren KVKK metninde tüzel kişiler kişisel verileri koruma kapsamına dahil edilmemiştir[100]. Dolayısıyla tüzel kişiliğe ait bir veri gerçek bir kişiye ait bilgi içermiyorsa, "kişisel veri" şeklinde kabul

---

[97] **OĞUZMAN/SELİÇİ/ÖZDEMİR**, Kişiler Hukuku s. 290; **SEROZAN** Rona, Medeni Hukuk, Genel Bölüm/Kişiler Hukuku, Vedat Kitapçılık, İstanbul, 2015, s. 491; **HATEMİ/OĞUZTÜRK KALKAN**, s. 79; **AKİPEK/AKINTÜRK /ATEŞ,** s. 511.

[98] Elektronik Haberleşme Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkındaki Avrupa Birliği Direktifi, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN (Son Erişim Tarihi: 04.04.2021) Direktif açıklamalarında, Elektronik haberleşme sektöründe kişisel verilerin korunması, mahremiyet ve tüzel kişilerin meşru menfaatleri ile ilgili olarak üye devletler tarafından kabul edilen yasal, düzenleyici ve teknik hükümler, elektronik iletişim sektöründe iç pazarın önündeki engellerden kaçınmak için uyumlu hale getirilmesi gerektiğinden söz edilmiştir. Bununla birlikte, Halka açık bir elektronik iletişim hizmetinin abonelerinin gerçek kişiler yanında tüzel kişilerde olabileceği ifade edilecek Direktif'in amacının gerçek kişilerin temel haklarını ve özellikle gizlilik haklarını ve tüzel kişilerin meşru menfaatlerini korumayı amaçladığı ifade edilmiştir. Keza, Direktif m. 1/f.2, "Bu Direktif hükümleri, 95/46/EC sayılı Direktif paragraf 1'de belirtilen amaçlar ve ayrıca, tüzel kişi olan abonelerin meşru menfaatlerinin korunmasını sağlarlar." demektedir.

[99] **AKSOY**, s. 19; **WALDEN** I.N., **SAVAGE** R.N; "Data Protection and Privacy law: Should Organizations Be Protected?", International and Comparative Law Quaterly, 1988, Cilt 37, Sayı:2, s. 337-347, s. 338 vd.

[100] **AKSOY**, s. 106; bu konudaki eleştiri için bkz. **ÇELİKEL** Serdar, Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, Doktora Tezi, Ankara, 2021, s. 59.

edilmemektedir[101]. Keza KVKK, verileri korunan kişilerin gerçek kişi olduğunu açıkça ifade etmiştir. Bu anlamda tüzel kişilerin kişisel verileri KVKK kapsamında yer almamaktadır[102]. Her ne kadar KVKK'da tüzel kişilerin kişisel verilerinin korunmadığı ifade edilmişse de 4 Aralık 2020'de Resmi Gazetede yayımlanarak 6 ay sonrasında yürürlüğe giren "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına ilişkin Yönetmelik"[103] gereği tüzel kişilerin kişisel verileri de koruma altına alınmıştır.

Anayasa Mahkemesi'nin 2013/84 Esas ve 2014/193 sayılı Kararı[104] dikkate alındığında, KVKK'nın henüz yürürlüğe girmediği, Kanun'un Taslak metninde her ne kadar kişisel veri sahibi kişiler arasında tüzel kişilere de yer verildiği göz önüne alınsa da yürürlük tarihi itibariyle Kanunun kapsama alanının yalnızca gerçek kişileri ele alarak tüzel kişileri veri sahibi olarak değerlendirmediği görülmektedir. Bununla birlikte, halihazırda tüzel kişilere ait bilgilerin ticari sır kapsamında[105] korunması bakımından, Türk Ticaret Kanunu[106] ve Türk Ceza Kanunu[107] hükümleri uygulanmaya devam etmektedir.

bb. Ölen Kişilere İlişkin Kişisel Verilerin Durumu

Kişisel verileri koruma hukuku bakımından tartışma konusu olan diğer bir konu, ölen kişilerin kişisel verilerinin korunup korunmayacağı noktasındadır. Ölen kişilerin verilerine ilişkin 95/46/EC sayılı Direktif doğrudan bir koruma sağlamamaktadır[108]. Keza mülga 95/46/EC sayılı Direktif'ten sonra yürürlüğe giren GVKT de vefat eden veri sahiplerinin verileri için herhangi bir koruma

---

[101] **BAŞALP** Nilgün, Kişisel Verilerin Korunması ve Saklanması, Ankara, 2009, s. 35; **AYDIN** Sedat Erdem, (AİHM İçtihatları Bağlamında) Kişisel Verilerin Kaydedilmesi Suçu, On Levha Yayınları, İstanbul, 2015, s. 8–9.

[102] Nitekim Kişisel Verileri Koruma Kurulu'nun da tüzel kişi verilerinin KVKK kapsamı dışında yer aldığına ilişkin kararları mevcuttur. Bkz. 19/11/2018 tarihli ve 2018/131 sayılı Kararı.

[103] R.G., T. 04.12.2020, S. 31324.

[104] AYM, E. 2013/84, K. 2014/183, T. 04.12.2014, R.G. Tarih-Sayı: 13.03.2015-29294 https://www.resmigazete.gov.tr/eskiler/2015/03/20150313-12.pdf (Son Erişim Tarihi: 04.04.2020).

[105] Tüzel kişiliğe ait ticari sır kapsamında kişisel verileri korumaya ilişkin mevzuatımızda özel bir düzenleme yer almadığından, TTK'nın haksız rekabete ilişkin 54. maddesi ve devamı ile TCK m. 239 hükmü uygulanacaktır. Netice itibariyle, tüzel kişilere ait verilerin KVKK ile korunamayacağı, yasal mevzuatımızda yer alan genel hükümler bakımından korunmaya devam edileceği açıktır. **ARSLAN** Çetin/**ÖZDEMİR** Didar, "Ticari Sırların Ceza Hukuku Tarafından Korunması", International Conference On Eurasian Economies, 2017, Session 4A: Hukuk, ss. 125-131.

[106] R.G., T. 14.02.2011, S. 27846.

[107] R.G., T. 12.10.2004, S. 25611.

[108] **29. Madde Çalışma Grubu**, WP 136, s. 22.

sağlamamaktadır[109]. Ancak üye devletlerin ölüm sonrası veri koruma kuralları koymasına ilişkin bir engel bulunmamaktadır. Bununla birlikte ölen kişiler kimi zaman yaşayan kişilerin de kişisel verisini teşkil edebilmektedir. Böyle bir durumun varlığında ölen kişiye ait verilerin aynı zamanda yaşayan kişilerle de ilgili olduğu kabul edileceğinden veri korumasından yararlanabilmektedirler[110].

95/46/EC sayılı Direktif'te ve Direktif'i referans alan KVKK m. 2'de kişisel verileri işlenen gerçek kişiler korumadan faydalanmaktadır. Türk Medeni Kanunu'nun 28. maddesi de kişiliğin ölümle sona erdiğini ve ölüm anıyla kişinin hak ehliyeti ile taraf ehliyetinin sona erdiğini belirtmektedir. Ancak bu durumun, ölenin korunmaya değer bir menfaatinin kalmadığı şeklinde anlaşılmayacağı ifade edilmektedir[111]. Zira kişisel verilerin korunmasına ilişkin düzenleme ve uzatılmış kişilik hakkı teorisi[112] ile kişilik ölümden sonra da korunabilmektedir[113]. Yine de belirtmek gerekir ki ölen kişilerin kişisel verilerinin korunup korunmayacağı hususunda gerek Avrupa Birliği hukukunda gerekse Amerikan hukukunda tartışmalar süregelmektedir. Nitekim bu tartışmalardan biri ölen kişilerin ölümlerinden sonra sosyal medya üzerinde yer alan kullanıcı hesapları üzerindeki kontrolün gizlilik ilkeleri gereği ne şekilde olacağı üzerinedir[114]. Keza sosyal medya üzerinde yer alan kullanıcı hesaplarının ölen kişinin

---

[109] **GVKT**, Resital 27.

[110] **ÇEKİN,** s. 41; **TAŞTAN**, s. 35; **AMIRASLANLI** Nijat, Türk ve Avrupa Birliği Hukukunda Kişisel Verilerin Aktarılması, On İki Levha Yayıncılık, Ekim 2022, s. 11; **29. Madde Çalışma Grubu**, WP 136, s. 22.

[111] **BÜYÜKSAĞIŞ** Erdem, "Digital Varlıkların Miras Yolu ile İntikalı", Yargıtay Dergisi 2/2021, ss. 337-408, s. 344.

[112] Uzatılmış kişilik hakkı teorisi ölümden sonra ölenin kişiliğinin ihlal edilmeyeceğinden yola çıkarak ölenin güvenini korumaya dayanan bir teoridir. Ölenin güvenini korumak adına da ölenin ya da üçüncü kişilerin verileri korunmadan faydalanmalıdır. **BÜYÜKSAĞIŞ**, s. 345; **ÇELİKTAŞ** İlyas, "Vefat Eden Kişinin Elektronik Posta Hesabı Mirasçılara İntikal Eder Mi?", Terazi Hukuk Dergisi, Y.2011, C.VI, S.62, ss .34-39, s. 38, https://www-jurix-com-tr.lproxy.yeditepe.edu.tr/article/1320 (Son Erişim Tarihi: 27.12.2022).

[113] **BÜYÜKSAĞIŞ**, s. 344; **GEZDER** Ümit: "Ölüm Sonrası Hatırayı Koruma Doktrini ve Ölüm Sonrası Kişiliğin Korunması Teorisi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, S.2007/1(65), s. 214, https://dergipark.org.tr/tr/download/article-file/95696 (Son Erişim Tarihi: 27.12.2022).

[114] **BÜYÜKSAĞIŞ**, s. 344; Nitekim doktrinde, TMK m. 28 uyarınca kişiliğin ölümle birlikte sona ermesinin, ölen kişinin artık korunacak bir menfaati kalmadığı yönünde anlaşılmaması gerektiği, ölüm sonrası kişiliğin ölenin yakınları aracılığıyla korunmasının mümkün olduğu ifade edilmiştir. **TURAN BAŞARA** Gamze, "Kişiliğin Korunması Kapsamında Ölümden Sonra Hatıranın Korunması Teorisi", Çankaya Üniversitesi Hukuk Fakültesi Dergisi, S.2020/1(5), ss. 341-390, s. 341 vd.), (Son Erişim Tarihi: 28.10.2022) https://www.acarindex.com/pdfs/186467; **UÇAK** Murat, "Kişisel Verilerin Ölümden Sonra Korunması", İMHFD, C. VI, S. 10, 2021, ss. 97-123, s. 108. Örneğin Facebook, bir kullanıcının şahsi hesabının kullanım koşulları ve şartlarını belirleyen politikalara yer vermekte ise de bu politikalar genellikle vefat eden kişinin gizlilik haklarını tam olarak korumamaktadır. Nitekim Facebook ve diğer benzeri hizmet sağlayıcıları, ölen kişinin gizlilik çıkarlarını görmezden gelmek yerine, ölenlerin arkadaşlarının veya ailelerinin memnuniyetine göre hareket etmeyi seçen politikalara sahiptir. Facebook, ölen kullanıcılarının profil sayfalarını "anma" şeklinde bir hizmet sunmaktadır. Her ne kadar Facebook ölen kullanıcıya ait hesap giriş bilgilerini paylaşmayacak olsa da profil sayfasının

malvarlığına dahil edilip edilemeyeceği ya da ne şekilde dahil olacağı bir diğer tartışma konusunu oluşturmaktadır[115].

Kanaatimizce, teknolojinin günlük yaşamdaki rolü büyümeye devam ederken, ölen kişinin mahremiyete ilişkin uygulanabilir bir hakka sahip olduğunun kabul edilmesi, kişilerin ölümden sonra mahremiyet hakkını korumanın en iyi yoludur. Her ne kadar bir kişinin ölümü ile kişiliği sona ermekte ise de günümüz teknolojisinde ölen

---

anılması ile ölen kişiye ait fotoğraflar, gönderiler görünür kılınmaktadır. Web sitelerinin büyük bir çoğunluğu ölen kişinin aile üyelerinin ölen kişiye ait hesabını iptal etmelerine izin vermekte ise de Facebook'ta ölen kişi ile ilişkinin niteliğine bakılmaksızın herhangi bir kişi 'profili anma' talebinde bulunabilmektedir. Bu durum, ölen kişiye ait hesap profilinin uzun süre görünür kalmasına sebebiyet vermektedir. **CHU** Natasha, "Protecting Privacy after Death", Northwestern Journal of Technology and Intellectual Property, Vol 13, No: 2, September, 2015, s. 255-264; **FACEBOOK**, How Do I Report a Deceased Person or an Account that Needs To Be Memorialized? https://www.facebook.com/help/150486848354038 (Son Erişim Tarihi: 12.04.2021).
Bu noktada bir sorun da ölen kişilerin sosyal medya hesapları da dahil dijital malvarlıklarının ne şekilde değerlendirileceği hususudur. Nitekim Afganistan'da yirmi yaşında ölen bir denizci asker örneğinde, ölen askerin ailesi, oğullarının fiziksel eşyalarının yanında Yahoo'ya ait e-posta hesabına da erişim talebinde bulunmuşlar ancak Yahoo'nun şirket politikaları gereği bu bilgilerin paylaşılması mümkün olmadığı için ailenin talebi kabul edilmemiştir. Bunun akabinde aile mahkemeye başvurarak oğullarına ait hesaba erişim taleplerini dile getirmişlerdir. Nitekim mahkeme ölen askere ilişkin hesap bilgilerini maddi mal varlığı değeri olarak kabul ederek iadesine karar vermiştir. Mahkemenin verdiği bu karar dijital varlıklar ile maddi varlıklar arasındaki ayrımın bulanıklaştığı örneklerden birini oluşturmaktadır. **HU** Jim, Yahoo Denies Family Access to Dead Marine's E-Mail, CNET, https://www.cnet.com/news/yahoo-denies-family-access-to-dead-marines-e-mail/ (Son Erişim Tarihi: 12.04.2021).

[115] Dijital varlıkların tam olarak neleri kapsadığına ilişkin net bir tanımlama yapılamasa da kişi üzerinde bir hak ya da menfaat sağlayan elektronik her türlü varlığını ifade ettiği kabul görmektedir. **SHERRY** Kristina, "What Happens to Our Facebook Accounts When We Die? Probate Versus Policy and the Fate of Social-Media Assets Postmortem", Vol. 40: 185, 2012, s. 193-204, 208–210. **ALTINDAL** Hasan/ **ARSLAN** Yusuf Enes, "Türk Hukukunda Dijital Miras: Karşılaşılan Sorunlar ve Uluslararası Uygulamalar Çerçevesinde Bazı Çözüm Önerileri", Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, Cilt XXV, 2021, Sayı 1, s. 321. Yine de kullanım amaçları ve kullanım sıklığına bağlı olarak e-posta içerikleri, sosyal medyada yer alan hesaplar, alan adları ya da internet hesapları, çevrim içi oyun karakterleri ve hesapları, kullanım-kiralama hakları, elektronik para, kripto para, dijital para ve sanal para değerleri dijital varlık olarak değerlendirilmektedir.
Ülkemizde de dijital varlıkların tespiti ve buna ilişkin uygulanacak yasal düzenlemeler sınırlı olsa da bu konuda yeni anlayışlar gelişmektedir. Nitekim Antalya Bölge Adliye Mahkemesi 6. Hukuk Dairesi'nin bu bakımdan oldukça yeni bir kararı mevcuttur. Söz konusu kararda, trafik kazası sonucu ölen murisin eşi, murise ait telefon üzerinden Apple'a başvurarak, murisin e-ticaret sitesi hesabına ait bilgi ve dokümanları ve aileye ait fotoğraf, ses kaydı video ve mesajların depolandığı iCloud hesabına erişim talebinde bulunmuştur. Apple talebi, konuya ilişkin bir mahkeme kararının olmadığı gerekçe ile reddetmiştir. Bunun üzerine muris bırakanın eşi, sulh hukuk mahkemesinde terekenin tespiti için dava açmıştır. Sulh hukuk mahkemesi, özel hayatın gizliliğini gerekçe göstererek davayı reddetmiştir. Ret kararının üzerine dosya istinafta inceleme yapılmak üzere Antalya Bölge Adliye Mahkemesinin 6. Hukuk Dairesine gönderilmiştir. Yapılan inceleme neticesinde murisin eşinin talebi yerinde görülerek neticede ilk derece mahkemesinin kararı kaldırılmıştır. Kararın gerekçesinde, mülkiyet açısından menkul ve gayrimenkul mülkiyeti ile şekillenen ayni haklar karşısında, fikri mülkiyet kavramının gelişimi ve "Fikir ve Sanat Eserleri" kavramının da mülkiyet hukuku çevresinde korumaya alındığı ifade edilmiştir. Bununla birlikte dijital mal varlığına ilişkin mülkiyet esasına dayalı yasal düzenlemelerin mevzuatımızda henüz yer almadığı ifade edilmiştir. Sonuç olarak istinaf mahkemesi, murisin ölüm tarihi itibariyle mal varlığının tespitinde tüm aktif ve pasif malvarlıklarının hesaba katılması bakımından dijital malvarlıklarının da terekeye dahil olması gerektiği yönünde kararını açıklamıştır. **Antalya Bölge Adliye Mahkemesi 6. Hukuk Dairesi**, 13.11.2020 Tarih, 2020/1149 Esas ve 2020/905 sayılı Kararı, https://okyayevren.com/wp-content/uploads/Antalya-BAM-6.-HD.-E.-20201149-K.-2020905-T.-13.11.2020.pdf (Son Erişim Tarihi:12.04.2021).

kişilere ait pek çok kişisel veri internet ortamında var olmaya devam etmekte ve bu dijital varlıklara ne olacağı sorusuna henüz net bir cevap verilememektedir. Keza kişisel verilerin korunması anlamında, e-posta hesapları, sosyal medya hesapları, bulut depolamasında yer alan dosyaları ve çevrimiçi banka hesapları gibi dijital varlıklar, kullanıcıyla ilgili birçok kişisel ve özel nitelikteki bilgileri kolayca ortaya çıkarabilmektedir.

cc. Cenine İlişkin Kişisel Verilerin Durumu

Doğum gerçekleşmeden önce çocuğun ana rahmindeki durumu "cenin" olarak ifade edilmektedir[116]. Ceninin hukuki statüsünün kabulü ve kişilik hakkı kapsamında korunmasına yönelik düzenlemeler ulusal ve uluslararası düzenlemelerde yer almaktadır. 4721 sayılı TMK m. 28'e göre gerçek kişilerin tam ve sağ doğumu ile kişilik başlamaktadır[117]. Ancak gerek mevzuat hükümlerimizde gerek uluslararası düzenlemelerde doğmamış çocuğun kişisel verilerinin ne şekilde değerlendirileceği tartışma konusu olmaktadır[118].

---

[116] **OĞUZMAN/SELİÇİ/ÖZDEMİR,** Kişiler hukuku, s. 10; **HELVACI**, s. 31.

[117] **HATEMİ/OĞUZTÜRK KALKAN**, s. 29.

[118] Başvurucu Thi-NhoVo'nun Fransa Devleti'ne karşı açtığı davada, başvurucu çocuğunun ölümünden sorumlu olan bir doktorun davranışının kasıtsız adam öldürme olarak sınıflandırılmadığı gerekçesiyle AİHS'nin 2. maddesine aykırı olduğunu iddia etmiştir. Davada başvuran, doktorun kendi üzerinde uyguladığı tıbbi prosedür gereği hamileliğini sonlandırmak zorunda kaldığını ifade etmiştir. Fransız hukukunda doğmamış çocuğun açık bir yasal tanımının veya embriyonun hukuki statüsüne ilişkin bir Avrupa mutabakatının bulunmadığına dikkat çeken Mahkeme, yaşamın ne zaman başladığına veya doğmamış çocuğun bir kişi olup olmadığına 2. madde kapsamında karar vermeyi reddetmiştir. Mahkeme bunun yerine, başvuranın çocuğunun kaybında doktor tarafından herhangi bir ihmal durumunun olup olmadığına ya da bu durumların açığa çıkarılmasında mevcut mekanizmaların yeterli olup olmadığını incelemiştir. Avrupa İnsan Hakları Mahkemesi, Vo v France Kararı, Başvuru Numarası: 53924/00, 8 Temmuz 2004, 82. Başlık, s. 26; **AİHM**, European Court of Human Rights, "Thematic Report: Healthrelated issues in the case-law of the European Court of Human Rights", June 2015, s. 1-34, https://www.echr.coe.int/Documents/Research_report_health.pdf (Son Erişim Tarihi:13.04.2021).
Bununla birlikte, 95/46/EC sayılı Direktif'in kabulünden bir süre sonra, Avrupa Konseyi Bakanlar Komitesi, 108 sayılı Sözleşme'ye atıfta bulunarak, doğmamış çocukların tıbbi verilerinin korunması hakkında görüşleri de içeren tıbbi verilerin korunması hakkında R (97) 5 Sayılı Tavsiye Kararı'nı yayınlamıştır. Kararın "doğmamış çocuklara" ilişkin 4.5 ve 4.6 numaralı başlıklarında, doğmamış çocuklarla ilgili tıbbi bilgilerin kişisel veri olarak değerlendirilmesi ve reşit olmayanların tıbbi verilerinin korunmasına benzer bir korumadan yararlanmaları gerektiği ifade edilmiştir. Bununla birlikte, üye devletlerin yasal mevzuatlarında aksi belirtilmedikçe, doğmamış çocuğun sorumluluk sahibi olarak ebeveynlerinin, doğmamış çocuk için yasal olarak hareket etme hakkına sahip kişi olarak değerlendirilebileceği ifade edilmiştir. Tavsiye kararı bağlayıcı niteliğe sahip olmadığından, ülkelerin ulusal mevzuatlarında uygulanması zorunlu değildir. Kanaatimizce Tavsiye kararında yer alan görüşler, üye devletlere bırakılan takdir yetkisinin sınırları içinde kabul edilmekte ise de bu tartışmaların tüm üye devletler bakımından soru işareti olmaktan çıkarılması için Tüzüğün bu konuda bir düzenleme yapması en sağlıklı çözüm yollarından biridir. Avrupa Konseyi Bakanlar Komitesinin Tıbbi Verilerin

Ceninin her zaman tam ve sağ olarak doğumu mümkün olmayabilir. Bununla beraber cenine ilişkin bilgiler, yaşayan kişiler ile ilgili bilgi sağlayabilmektedir. O halde doğum anı gerçekleşmeyen bir çocuğa ilişkin genetik bilgilerin kişisel veri olarak kabul edilip edilmeyeceği değerlendirmesi önem kazanmaktadır[119]. 95/46/EC sayılı Direktif'te olduğu gibi GVKT'de kişisel verileri koruma noktasında gerçek kişilere odaklanmaktadır.

Üye devletlerin ilgili kuralları belirleme serbestisi bulunmaktadır[120]. Dolayısıyla Tüzük, doğmamış çocukların kişisel verilerinin korunması açısından herhangi bir kural veya rehberlik sağlamadığından, veri koruma kurallarının doğmamış çocuklara uygulanabilirliği üye devletler tarafından yorumlanacaktır. Elbette doğmamış çocukların genetik verilerinin korunmasına yönelik daha açık ve daha güçlü yasal düzenlemelere ihtiyaç olduğu açıktır. Genetik veriler, Tüzüğün 9. maddesi gereği özel kişisel veri kategorilerinden biridir. Genetik verilerin bir özelliği de sadece bir kişi ile değil, aynı zamanda bu kişilerin yakın akrabalarıyla ilgili özel nitelikte verileri de barındırıyor olmasındandır. Keza Tüzüğün 4. maddesinin 13. fıkrası genetik verileri, gerçek kişilerin fizyolojisi ve sağlığı ile ilgili spesifik bilgiler sağlayan, gerçek kişilerden alınan biyolojik numunelerin analiz edilmesiyle elde edilen ya da bu kişilerin kalıtımsal özelliklerine dayanan veriler olarak tanımlamaktadır. Bu tanımdan da yola çıkarak Tüzük m. 9/f.4 ile üye devletler kendi yasal mevzuatlarında doğmamış çocukların genetik verilerini koruma konusunu ele alabilseler de bu takdir yetkisi sınırsız değildir. Nitekim, Resital 53 ile, madde 9 uyarınca özel nitelikteki kişisel veri kategorilerinin işlenmesi açısından kendilerine tanınan takdir yetkisinin sınırları çizilmiştir[121].

Korunmasına R (97) 5 Sayılı Tavsiye Kararı, s.106-108. https://rm.coe.int/16806af967 (Son Erişim Tarihi: 13.04.2021).

European Court of Human Rights, "Thematic Report: Healthrelated issues in the case-law of the European Court of Human Rights".

[119] Kişilere ilişkin elde edilen genetik verilerin, kişiler hakkında çok fazla bilgi içeriyor olması ve sınırsız sayıda amaç için kullanılabilecek olması bu değerlendirmelerden biridir. Genetik nitelikteki veriler, bilimsel ve ticari amaçlarla daha yaygın şekilde kullanılırken, Tüzük kapsamında özel bir veri kategorisi olarak yer alan genetik verilerin işlenme şartlarına ilişkin pek çok soru işareti var olmaya devam etmektedir. Bu noktada hassas olarak değerlendirilen bir konu da doğmamış kişilere ilişkin doğum öncesi testlerle toplanan verilerin nasıl korunacağına ilişkindir. Bu endişenin kaynaklarından biri de birçok genetik rahatsızlığın teşhisine imkân sağlayan doğum öncesi ve doğum sonrası kavramlara ilişkindir. **PORMEISTER** Kart, and **DROZDZOWSKI** Lukasz, "Protecting the Genetic Data of Unborn Children: A Critical Analysis." European Data Protection Law Review (EDPL), Vol. 4, No. 1, 2018, p. 53-64, s. 53; **ÖZER DENİZ**, s. 177-178; **ŞENOCAK**, Kişisel Verilerin Korunması Hukuku, "Kişisel Veri Kavramının Kapsamı ve Unsurları", s. 22; **29. Madde Çalışma Grubu**, WP 136, s. 23.

[120] **29. Madde Çalışma Grubu**, WP 136, s. 22.

[121] **GVKT**, Resital 53, Higher Protection Of Sensitive Data In Health And Social Sector.

Kanaatimizce AB Genel Veri Koruma Tüzüğünde, "genetik verileri" tanımlayan maddeler üzerinde değişikliğe gidilmesi bir çözüm olabilir[122]. Daha iyi bir diğer alternatif de doğmamış çocukların genetik verilerine ilişkin özel bir rejimin oluşturulması şeklinde olabilir[123]. Genetik verilerin uzun vadede mahremiyet haklarına etkileri göz önüne alındığında, doğmamış çocuğun ebeveyninin çocuğun genetik verilerini kontrol etmede sınırsız bir hakkı olmamalıdır. Ebeveynlerin, çocuğun genetik verilerinin kontrol etme açısından sınırlandırılması, tam ve sağ doğumu gerçekleşen çocuğun cenin halindeyken işlenen kişisel verileri açısından da geçerli olmalıdır. Avrupa genelinde veri koruma ile amaçlananın ortak uygulanabilir kurallar olduğu düşünülse de yorumlamaya açık birçok konuyu açıkta bıraktığı ortadadır. Doğmamış çocuğun kişisel verilerinin işlenmesine ilişkin tek kararın R (97) 5 No'lu Tavsiye Kararı olduğu göz önüne alındığında, kararın bağlayıcılığı da olmaması bakımından bu konuda yasal bir düzenlemeye ihtiyaç duyulduğu açıktır[124].

c. Kişisel Verinin İlgili Kişiye İlişkin Olması

Genel olarak bilgi, söz konusu kişi ile ilgili olduğunda, o kişi ile "ilişkili" olarak kabul edilmektedir[125]. 29. Madde Çalışma Grubu tarafından yayınlanan 4/2007

---

[122] Doğmamış çocukların genetik verilerini ele almada iki yönlü bir değerlendirme yapılmaktadır. Birincisi biyolojik ebeveynleri, doğmamış çocuktan elde edilen genetik veriler açısından veri özneleri olarak tanımlanabilir. İkincisi doğmamış çocuğun kendisi, veri konusu olarak ele alınabilir. R (97) 5 No'lu Tavsiyenin Açıklama Memorandumunda yapılan önerilerden biri, doğmamış çocuğun genetik verilerini annenin özel nitelikte verileri olarak kabul etmektir. Bu durumda biyolojik ebeveynler, doğmamış çocuğun genetik verilerine ilişkin tüm hakların sahipleri olacaklardır. Ancak doğmamış çocuğun genetik verilerini biyolojik ebeveynlerin verileri olarak düşünmek, özellikle biyolojik anlamda, doğmamış çocuğun genetik verilerinin biyolojik ebeveynlerin genetik verilerinden farklı olması gerçeğiyle çelişmektedir. Üstelik bu husus çocuğun haklarını ve çıkarlarını etkili bir şekilde korumamaktadır. Örneğin, doğmamış çocuğun genetik verilerine ilişkin veri sahibi olarak biyolojik bir ebeveyn, genetik verileri kamuya açıklarsa, işlemenin genel yasağı geçerli olmayacaktır. Veriler kamuoyuna açıklandığında, çocuk daha sonra itiraz etme ve unutulma hakkına sahip olsa da çocuk açısından bu hakları etkili bir şekilde kullanmak son derece zor olacaktır. **PORMEISTER/DROZDZOWSKI**, s. 58; **SIMIĆ**, s. 255.

[123] **PORMEISTER/DROZDZOWSKI**, s. 63.

[124] Bu konudaki görüşler için ayrıca bkz. **ŞENOCAK**, Kişisel Verilerin Korunması Hukuku, " Kişisel Veri Kavramının Kapsamı ve Unsurları", s. 22.

[125] **29. Madde Çalışma Grubu,** WP 136, s. 9-10; **KORFF** Douwe, European Commıssion Directorate-General Justıce, Freedom And Security Comparative Study On Differeny Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments, Working Paper No. 2: Data protection laws in the EU, General Justice, Freedom and Security, Londra 20 Ocak 2010, s. 42-43; **WITZLEB** Normann &**WAGNER** Julian, "When is Personal Data "About" or "Relating to" an Individual?" A Comparison of Australian, Canadian, and EU Data Protection and Privacy Laws", Canadian Journal of Comparative and Contemporary Law 4, 2018, 293-330, s. 317.

sayılı Rapor, kişisel veri kavramı üzerine bu terimin nasıl yorumlanacağına dair açıklamalar sunmaktadır.

Çoğu durumda, kişisel veri ile ilgili arasında ilişkinin kurulması kolay olabilir. Örneğin, bir işyerinde çalışan kişi hakkında personel özlük dosyasında tutulan belgeler, kişinin kişisel verileridir ve o kişi ile ilişkilidir. Bir hastanede üzerinde ismi bulunan hastaya ilişkin test sonuçları ya da raporlar da o kişi ile ilişkili olmaktadır. Bununla birlikte, söz konusu bilgiler, her zaman bir kişi ile "ilişkili" olmaya yetecek kesinlikte olmayabilir. Örneğin tamirciye getirilen bir arabanın servis kaydı ile ilgili tutulan kayıtlar, servis kontrollerinin tarihleri, teknik sorunlar ve malzeme durumu hakkında bilgi içerecektir. Bu bilgiler, servis kaydında yer alan araba ile ilgili bir plaka numarası ve bir şase numarası ile ilişkilendirilirse bunlar da bir kişiye ilişkin bilgi sağlayabilir[126].

Çalışma Grubu, bilginin ne zaman bir kişiyle "ilgili" olarak değerlendirilebileceği konusuna belirli bir yaklaşım geliştirmiştir. Buna göre, bilgi, bir kişinin kimliğine, fiziksel özelliklerine, davranışlarına atıfta bulunuyorsa veya o kişiye nasıl davranılacağı veya kişinin nasıl değerlendirileceği ile ilgili ise kişi ile ilişkili kabul edilecektir[127]. O halde bilginin içeriğinin, kişi ile ilişkili olacak bir bağlam kurmaya yeterli olup olmayacağını belirlemek için her somut olayın kendi içerisinde değerlendirilmesi gerekmektedir[128].

2. Özel Nitelikli Kişisel Veri Kavramı

Kişisel veri ile ilgili yapılan ortak tanımlardan yola çıkarak, bazı veri türlerinin özel kategoriye ayrılarak incelendiği görülmektedir. Bu veri kategorilerini genel nitelikteki kişisel verilerden ayıran unsur, verinin kişiler hakkında içerdiği bilginin hassasiyet düzeyi ile ilgilidir. Bu verilerin hassasiyet düzeyleri fazla olduğu için özel

[126] **29. Madde Çalışma Grubu**, WP 136, s. 10; **29. Madde Çalışma Grubu**, WP 105, s. 8; **AKSOY**, s. 29; **TAŞTAN**, s. 40; **AŞIKOĞLU** Şehriban İpek, "Avrupa Birliği ve Türk Hukuku'nda Kişisel Verilerin Korunması ve Büyük Veri", Yüksek Lisans Tezi, İstanbul 2018, s. 12.

[127] **29. Madde Çalışma Grubu,** WP 136, s. 9-10.

[128] **29. Madde Çalışma Grubu**, WP 136, s. 10. Bir taksi şirketi tarafından, mevcut taksilerin konumunu gerçek zamanlı olarak belirlemeyi mümkün kılan bir uydu sisteminin kullanıldığı durumda işlemenin esas amacı, müşterilerin adresine en yakın arabayı yönlendirerek kaliteli hizmet vermek ve yakıt tasarrufu sağlamaktır. Dolayısıyla burada kullanılan veriler ne yolcular ne de taksi şoförleri ile ilgilidir. Bir diğer ifade ile işlemenin asıl amacı taksi şoförlerinin performansını değerlendirmek değildir. Ancak yine de uygulanan sistem taksi şoförlerinin performansının izlenmesine, hız sınırlarına uyup uymadıklarına, uygun güzergahlar arayıp aramadıklarına ilişkin de değerlendirilebilir. Ancak böyle bir durumun varlığında işlemenin amaç unsuru değişecektir.

bir korumadan faydalanmaları gerektiği düşünülmüştür[129]. Zira bu tür verilere yönelik eylemler, kişilerin mahremiyetlerine doğrudan bir saldırı niteliğinde olup ihlal yaratma ihtimalleri de oldukça yüksektir[130]. Nitekim bu veriler gerek mülga Direktif ve Tüzük hükümlerinde gerek KVKK'da sınırlı sayıda sayılmıştır[131].

108 sayılı Sözleşme'nin özel nitelikteki kişisel verileri içeren 6. maddesi ülkelerin kendi yasal mevzuatlarında uygun güvenceler sağlanmadığı sürece, bireylerin ırksal özellikleri, dini inançları ya da siyasi düşüncelerini ortaya koyan bilgiler ile sağlıklarına ya da cinsel yaşamlarına ilişkin bilgilerin otomatik olarak işlenemeyeceğini ifade etmektedir. Bu husus ceza mahkûmiyet kararları için de geçerli kabul edilmektedir. 95/46/EC sayılı Direktif'te özel nitelikli kişisel verinin tanımı 8. madde ile düzenlenmiştir. Maddeye göre üye devletler, kişilerin dini inançlarına, felsefi inançlarına, sağlık verilerine, cinsel yaşamlarına, siyasi görüşlerine, ırksal özelliklerine ya da etnik özelliklerine ve sendika üyeliklerine ilişkin kişisel verilerin işlenmesini yasaklamakla yükümlüdür.

GVKT m. 9/f.1'de, kişilerin etnik kökenlerine ya da ırksal özelliklerine ilişkin bilgileri, dini ya da felsefi inançları ile siyasi düşüncelerine ilişkin bilgileri, sendika üyeliklerine ilişkin bilgileri, genetik ve biyometrik de dahil sağlık bilgileri ile cinsel yaşamlarına ilişkin bilgileri ve ceza mahkumiyetleri ile güvenlik tedbirlerine ilişkin verileri, özel nitelikli kişisel veriler olarak kabul edilmekte ve bu tür verilerin GVKT m. 9/f.2'de belirtilen istisnai haller dışında işlenmesi yasaklanmaktadır. Görüleceği üzere Tüzük, Direktif'ten farklı olarak genetik veriler ile biyometrik verileri de özel nitelikli veri olarak kabul etmiştir. Ayrıca belirtmek gerekir ki GVKT m. 9/f.4'te üye devletler Tüzük kapsamında ifade edilen genetik, biyometrik ya da sağlık verileri ile ilgili olarak ek koşullar belirleme serbestisine sahiptir.

Özel nitelikli kişisel veriler KVKK'nın "Özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6. maddesinde tanımlanmıştır. KVKK m. 6/f.1'de kişilerin etnik kökenleri ya da ırksal özellikleri ile dini inançları, felsefi düşünceleri, siyasi görüşleri, dernek, vakıf ve sendika üyeliklerine ilişkin verileri, genetik ve biyometrik verileri de dahil sağlık verileri ile cinsel yaşamlarına ilişkin verileri, kılık ve kıyafetlerine ilişkin

[129] **ŞENOCAK**, Kişisel Verilerin Korunması Hukuku, "Kişisel Veri Kavramının Kapsamı ve Unsurları", s. 22; **AMIRASLANLI**, s. 14; **YILMAZ**, s. 45; **BULUT** Metin, "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", 2020/3 Ankara Barosu Dergisi, ss.101-150, s. 109; TBMM Komisyon Raporu, s. 84. https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf, (Son Erişim Tarihi: 28.10.2022); **ŞİMŞEK**, s. 121; **ÇELİKEL**, s. 75.
[130] TBMM Komisyon Raporu, s. 10.
[131] **AKSOY**, s. 30; **ŞİMŞEK**, s. 121.

veriler ile ceza mahkumiyetleri ya da haklarında uygulanan güvenlik tedbirlerine ilişkin verileri özel nitelikte veriler olarak kabul edilmektedir. Tüzük hükümleri ile karşılaştırıldığında, KVKK kapsamında yer alan kişinin mezhep ya da diğer inançları ile kılık kıyafetine ilişkin düzenlemelerin ve dernek/vakıf üyeliklerine ait verilerin Tüzük kapsamındaki özel nitelikli kişisel veriler içerisinde düzenlenmediği görülmektedir[132]. Öte yandan cinsel yaşama ilişkin kişisel veriler açısından da Tüzük, kişinin cinsel eğilimine yönelik bilgileri de özel nitelikli veri grubuna dahil etmiştir. Bir diğer ifade ile cinsel eğilime ilişkin kişisel veriler KVKK kapsamında yer almamaktadır[133].

3. Genel Nitelikli Kişisel Veri Kavramı

Genel nitelikte kişisel veriler yukarıda özel nitelikli kişisel veri başlığında yaptığımız açıklamalar doğrultusunda değerlendirilmelidir. Dolayısıyla sınırlı sayıda sayılan ve verilerin hassasiyet düzeyi ile yakından ilgili olan hassas veriler dışındaki tüm kişisel veriler genel nitelikte kişisel veri kabul edilmektedir. Genel nitelikte kişisel verileri sınırlı sayıda saymak mümkün olmadığından bu veriler oldukça geniş yorumlanmaktadır.

OECD'nin 23 Eylül 1980 tarihli "Özel Hayatın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeleri"'nde kimliği belirli ya da belirlenebilir her türlü bilgi kişisel veri olarak ifade etmektedir. 108 sayılı Sözleşme m. 2/a'da kişisel veri, benzer şekilde tanımlanmıştır. 95/46/EC sayılı Direktif m. 2 ile ise kişisel veri tanımının detaylandırıldığı görülmektedir. Buna göre kişisel veri, zihinsel ya da fiziksel, ekonomik, kültürel ya da sosyal kimliğe ya da bir kimlik numarasına ilişkin, bir ya da daha fazla faktöre dayalı olarak doğrudan veya dolaylı olarak bir kişiyi belirli ya da belirlenebilir kılacak her türlü bilgiyi ifade etmektedir. Görüldüğü üzere kişisel veriler oldukça geniş bir değerlendirmeye konu olmaktadır.

KVKK m. 3/f.1-d'de kişisel veri tanımının, ülkemizde 1981 tarihinde imzalanarak 2016 yılında onaylanan 108 sayılı Sözleşme hükmü ile aynı şekilde ifade edildiği görülmektedir. Buna göre "*kimliği belirli ya da belirlenebilir ve gerçek kişiye*

---

[132] **ÖZER DENİZ** Miray, Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk, On İki Levha Yayıncılık, Eylül 2022, s. 49.
[133] **BULUT**, s. 138.

ait her türlü bilgi" kişisel veriyi ifade eder. Bu anlamda kişisel verinin, uluslararası düzenlemelerde ortak ve oldukça geniş yorumlanabilen bir tanımı bulunmaktadır.

GVKT'nin 4. maddesine bakıldığında, gerçek kişiye ait belirli ya da belirlenebilir her bilgi kişisel veri olarak açıklandıktan sonra, gerçek kişi olarak veri sahibinin kişisel verileri kategorize edilmiştir. Buna göre gerçek bir kişinin zihinsel ya da fiziksel, fizyolojik ya da genetik, ekonomik, kültürel veya sosyal kimliğine ait bir ya da birden fazla faktöre atıfla doğrudan veya dolaylı olarak tanımlanabilen veriler, belirli ya da belirlenebilir nitelikte isim, bir kimlik numarası, konum verisi, çevrimiçi tanımlayıcılar kişisel veri olarak ifade edilmektedir.

III. KİŞİSEL VERİLERİN İŞLENMESİ

KVKK m. 3/f.1-e'ye, göre kişisel verilerin işlenmesi en temel ifade ile kişisel verilerin tamamen ya da kısmen otomatik olarak ya da bir veri kayıt sisteminin parçası olarak otomatik olmayan şekilde işlenmesini ifade etmektedir. Bu anlamda KVKK m. 3/f.1-e, kişisel verilerin tamamen ya da kısmen otomatik olarak yahut bir veri kayıt sisteminin parçası olmak üzere otomatik olmayan yollarla işlenmesi, verilerin muhafaza edilerek, kayıt altına alınarak, depolanarak, yeniden yapılandırılarak ya da değiştirilerek, üçüncü taraflara yayılarak, aktarılarak, silinerek ya da tümüyle yok edilerek gerçekleştirilen çok kapsamlı işlemeleri ifade etmektedir. Örneğin bir şirket içerisinde çalışan personele ait özlük evraklarının yönetiminde bu verilerin bir flash diskte ya da bir bulut ortamında ya da fiziki bir ortamda olması fark etmeksizin veri işleme faaliyeti gerçekleşmektedir[134].

[134] What Activities Count as Processing Under the GDPR? 18 January 2021 https://www.termsfeed.com/blog/gdpr-processing-activities/ (Son Erişim Tarihi: 09.06.2021).
GVKT, "processing" olarak ifade edilen "işleme" ifadesine 630'dan fazla kez yer vermektedir. Dolayısıyla kişisel verilerin işlenmesi denildiğinde "işleme" ile ifade edilenin sınırlı sayıda olmayan çok çeşitli işlemeleri karşıladığı kabul edilmelidir. İçinde bulunduğumuz teknolojik çağa bakıldığında, kişisel verilerin işlenmediği bir ortamı hayal etmenin zorluğu açıktır. Nitekim GVKT m. 4/f.2'de de işleme faaliyeti, otomatik bir yolla gerçekleşip gerçekleşmediği fark etmeksizin her türlü işlemeyi ele alır. Görüldüğü üzere, Tüzük bakımından kişisel verilerin işlenmesine getirilen tanım son derece geniş şekilde ifade edilmiştir. Kişisel verilerin işlenmesi noktasında "toplama", GVKT'de en fazla yer alan işleme faaliyetlerinden birini oluşturmaktadır. Zira Tüzük, kişisel verilerin doğrudan veri sahibi gerçek kişiden alınması hususunda "toplama" (collect) terimini kullanır. Benzer şekilde Tüzük, kişisel verilerin üçüncü taraflardan alınmasına atıfta bulunurken ise "elde etme" (obtain) terimini kullanmaktadır.

A. KISMEN VEYA TAMAMEN OTOMATİK YOLLA İŞLEME

Gerek Direktif metninde gerek KVKK'da kişisel verilerin otomatik yolla işlenmesinin tanımına yer verilmemiştir. Bununla birlikte OECD, kişisel verilerin otomatik yolla işlenmesine ilişkin bir tanımlamaya yer vermiştir. Bu tanıma göre otomatik işleme, herhangi bir insan müdahalesi olmaksızın ya da en azından insan müdahalesine en asgari şekilde ihtiyaç duyulan, kendi içinde bağlantılı bir elektronik sistem üzerinden veri işleme faaliyetlerini gerçekleştiren işleme olarak ifade edilmiştir[135]. Nitekim 108 sayılı Sözleşme m. 2/c'de otomatik yolla işleme ifadesinden, tamamen veya kısmen otomatik yollarla işlenen verilerin kaydedilmesi, verilerin düzenlenmesi ya değiştirilmesi, silinmesi ya da imha edilmesi, geri getirilmesi ya da yayılmasının anlaşılacağı belirtilmiştir.

Öte yandan KVKK'nın gerekçe kısmında da benzer bir ifadeye yer verilerek, bu verilerin özel sektörde ve kamu sektöründe bilişim sistemleri kullanarak otomatik yollarla kullanıldığı ifade edilmiş ve otomatik yolla işlemeye ilişkin açıklamaya yer verilmiştir[136]. O halde otomatik yolla veri işleme ile ifade edilenin, bilgisayar, telefon, tablet, akıllı saat gibi bilişim teknolojilerinin kullanıldığı yazılımsal ya da donanımsal pek çok araç ile ve insan müdahalesi gerekmeksizin gerçekleştirilen işlemeler olduğunu ifade etmek mümkündür[137].

B. BİR VERİ KAYIT SİSTEMİNİN PARÇASI OLMAK KOŞULUYLA OTOMATİK OLMAYAN YOLLA İŞLEME

GVKT ile KVKK'nın lafzına bakıldığında, verilerin otomatik yollarla işlenmesinde ya da bir veri kayıt sisteminin parçası olarak otomatik olmayan şekilde işlenmesinde herhangi bir ayrıma gidilmediği görülmektedir. Elbette içinde bulunduğumuz teknolojik çağ düşünüldüğünde, kişisel verilerin işlenmesinin çok

---

[135] **Kişisel Verileri Koruma Kurumu,** 6698 Sayılı Kanun'da Yer Alan Temel Kavramlar, s.13; Glossary of Statistical Terms, Automated Data Processıng (Adp), https://stats.oecd.org/glossary/detail.asp?ID=4370 (Son Erişim Tarihi: 24.06.2021).

[136] **Kişisel Verileri Koruma Kurumu,** Kişisel Verilerin Korunması Kanunu ve Uygulaması, s.35. https://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf (Son Erişim Tarihi: 14.05.2021).

[137] **GÜRSEL** İlke, "Protection Of Personal Data In International Law And The General Aspects Of The Turkish Data Protectıon Law", D.E.Ü. Hukuk Fakültesi Dergisi, Cilt: 18, Sayı: 1, 2016, s. 33-61 (Basım Yılı: Ekim 2016), s. 46.

büyük ölçüde otomatik işlemeye konu olduğu hatta daha önceleri otomatik olmayan şekilde işlenen kişisel verilerin de elektronik ortamlara aktarılarak otomatik işlemelere konu edildiği ifade edilebilir[138]. Ancak otomatik olmayan yollarla işlenen kişisel verilerin, Kanun'un ya da GVKT'nin kapsamına girebilmesi için bu işlemelerin bir veri kayıt sisteminin parçasını oluşturması gerekmektedir. Diğer bir ifade ile otomatik olmayan şekilde işlemeye konu olan veriler bir veri kayıt sisteminin parçasını oluşturmadıkça Kanun ya da Tüzük kapsamında değerlendirilemeyecektir. Örneğin, kapı kapı gezerek ürün satışı yapan bir kişinin satış yapmak istediği kişiler ile ilgili edindiği bilgiler fiziken kayıt altına alınıp muhafaza edilmediği sürece bu kapsamda yer almaktadır.

KVKK'nın 3. maddesi veri kayıt sistemini[139], *"...Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi..."* olarak ifade etmiştir. Benzer şekilde GVKT'nin "Tanımlar" başlıklı 4. maddesinin 6. fıkrasında, veri kayıt sistemi (dosyalama sistemi), *"...Merkezi ya da merkezi olmayan yahut işlevsel ya da coğrafi olarak belirli kriterlere göre erişilebilir yapılandırılmış herhangi kayıt sistemini..."* ifade etmektedir[140]. GVKT m. 4/f.6, "herhangi" yapılandırılmış kayıt sistemi ile

---

[138] **Kişisel Verileri Koruma Kurumu,** Kişisel Verilerin Korunması Kanunu ve Uygulaması, s. 21; **AYÖZGER ÖNGÜN** Çiğdem, Kişisel Verilerin Korunması Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, İstanbul, Beta Yayınları, 2016, s. 122; **ÇELİKEL**, s. 137; **KÜZECİ**, 371.

[139] Ayrıca "Kişisel Verilerin Silinmesi Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"'in m. 4 de kayıt ortamı, "Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortam" olarak ifade edilmiştir.

[140] Bir veri kayıt sisteminin parçası olma ile ifade edileni anlayabilmek için bu konuda detaylı açıklamalara yer veren Avrupa Birliği Adalet Divanı'nın Jehovan Todistajat- Tietosuojavaltuutettu (kısaca Jehovan) ya da (Yehova'nın Şahitleri) davasına değinmek gerekmektedir. Bahse konu Avrupa Birliği Adalet Divanı'nın (Yehova'nın Şahitleri) davasında üzerinde durulan husus, veri kayıt sistemi (dosyalama sistemi) kavramının, verilerin daha sonra kullanılmak üzere alınabileceğinden bahisle dini cemaat üyeleri tarafından vaaz faaliyetleri sırasında kişilerin evlerini kapı kapı dolaşırken bu kişiler ile ilgili elde edilen isim ve adreslerin ve bu kişilerle ilgili toplanan diğer verilerin Direktif kapsamında yer alıp almadığı üzerinedir. Davada, kişisel verilerin otomatik olmayan yolla elde edilmesinde Direktif kapsamında bir dosyalama sistemini oluşturduğu ifade edilmiştir. Zira dini cemaat üyeleri tarafından vaaz faaliyetleri sırasında kapı kapı dolaşırken temasa geçilen kişilerle ilgili olarak elde edilen kişisel veriler, daha sonra aynı kişileri daha sonraki ziyaretlerinde o kişilerle ilgili bilgilerin hatırlanmasına yardımcı olmakta dolayısıyla ortak bir amaç dahilinde elde edilmektedir. Bu sebeple bu kişisel verilerin daha sonra kullanılmak üzere belirli kriterlere göre yapılandırılmış olduğu kabul edilmiştir. Ayrıca elde edilen verilerin, ziyaret edilen kişilerin isim ve adreslerini içerdiği, özellikle dini inançlar ve ailevi koşullarla ilgili konuşmaların içeriğinin bir özetinin yer aldığı bildirilmiştir. Dolayısıyla söz konusu kararda dini cemaatin, coğrafi olarak belirli kriterlere göre kişisel verilerin elde edildiği ve elde edilen bu verilerin yapılacak sonraki ziyaretlere hazırlık amacıyla, bir dosyalama sistemini oluşturduğu kabul edilmiştir. İlgili karar ile ilgili yapılan değerlendirmeler GVKT'nin yürürlüğe girmesinden önceki bir tarihe denk geldiği için bu anlamda Direktif açısından bir değerlendirme yapılmıştır. **YILMAZ** Süleyman/**ÇAVUŞOĞLU** Gökçe Filiz, Kişisel Verileri Koruma Hukuku, Yetkin Yayınları, Ankara, 2020, s. 56-57; Jehovan Todistajat Kararı, para. 55-76, https://curia.europa.eu (Son Erişim Tarihi:24.06.2021).; **Golden Data Law**, "What is a 'filing system' under EU data protection law?", Nov

oldukça geniş bir tanımlamaya yer vermiştir. Dolayısıyla Tüzük, veri kayıt sisteminin yapılandırılması ile ilgili herhangi bir kriter belirlemiş olsa dahi Tüzük resitallerine bakıldığında, veri kayıt sistemine (dosyalama sistemi) dahil olacak verilerin öncelikle *"kişiler ile ilgili olan her türlü veriyi"* ele aldığını söylemek mümkün olacaktır[141]. Veri kayıt sisteminin parçasını oluşturan veriler gerek fiziki gerek elektronik ortamda oluşturulmuş verilerden oluşabilir.

IV. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN DÜZENLEMELERİN TARİHSEL SÜRECİ

A. ULUSLARARASI ALANDA YAPILAN DÜZENLEMELER

1960'lı yıllardan itibaren kişisel verilerin otomatik olarak işlenmeye başlanması ile kamu otoriteleri, verileri işlenen kişilerin haklarını korumak adına çalışmalar yapmaya başlamıştır. Elbette bu gelişmeler başta bireylerin mahremiyet haklarını korumak ve bu hakların kamu otoritelerindeki hâkimiyetinin sınırlandırılması gerektiği üzerine pek çok tartışma yaratmıştır[142]. Nitekim bu tartışmaların temel gerekçesini Alman Anayasa Mahkemesi'nin 1983 tarihli "Nüfus Sayım Kararı" oluşturmuştur. Anılan karar ile bireylerin kişisel verileri üzerindeki devlet hâkimiyetinin sınırlanması gerektiği ve bireylerin kendi verileri üzerinde tasarrufta bulunma hakkının kişilere ait olması gerektiği ifade edilmiştir[143].

Ancak bireylerin kişisel verileri üzerindeki hâkimiyetin sınırlanması ve kişilerin mahremiyet haklarının korunmasına ilişkin yapılan ilk yasal düzenleme 1983 tarihli Nüfus Sayım Kararı'ndan on üç yıl önce Almanya Hessen Eyaleti'nde yürürlüğe giren Kişisel Verileri Koruma Kanunu[144] ile olmuştur. Hessen Eyaleti'ne ait bu kanun Avrupa hukukundaki ilk düzenleme olması bakımından son derece önemlidir. 1973 yılında İsveç, kişisel veri sahiplerine kayıtlarına erişme hakkını tanıyan ilk ulusal

---

29, 2018, https://medium.com/golden-data/what-is-a-filing-system-under-eu-data-protection-law-6e7222743f71 (Son Erişim Tarihi: 24.06.2021).

[141] **GVKT**, Resital 15.

[142] **ÇEKİN**, s. 5.

[143] **HORNUNG/ SCHNABEL,** s. 85; **TAŞTAN**, s.64; **ŞİMŞEK**, s. 115; **KÜZECİ**, s. 75-77.

[144] **Kişisel Verileri Koruma Kurumu,** "Kişisel Verilerin Korunması Kanununa Duyulan İhtiyaç", s. 1, https://www.kvkk.gov.tr/Icerik/4182/Kisisel-Verilerin-Korunmasi-Kanununa-Duyulan-Ihtiyac (Son Erişim Tarihi: 07.10.2021); **ÇEKİN**, s. 5; **KÜZECİ,** "Bilgilerin Geleceğini Belirleme Hakkı", s. 53.

gizlilik yasası olan Veri Kanunu'nu yürürlüğe koymuştur[145]. Bununla birlikte Almanya'da federal olarak düzenlenen ilk kanun 28 Ocak 1977 tarihinde yürürlüğe giren Alman Federal Veri Koruma Kanunu[146] olmuştur[147]. Benzer şekilde 1978 tarihli Fransa Veri Koruma Kanunu[148] da veri işleme faaliyetleri karşısında kişisel verileri işlenen kişilerin hukuki menfaatlerini koruma adına yürürlüğe girmiştir[149]. Avusturya'da 1978 yılında hazırlanan Federal Kişisel Verilerin Korunması Kanunu, 1980 tarihinde yürürlüğe girmiş; İsviçre Veri Koruma Kanunu ise 1992 yılında yürürlüğe girmiştir. İngiltere'de hazırlanan Veri Koruma Kanunu'nun yürürlüğe giriş tarihi ise 1998 yılına denk düşmektedir[150].

Aşağıda kişisel verilerin korunmasına ilişkin uluslararası düzeyde yapılan temel düzenlemelere çalışma konumuzla sınırlı kalacak şekilde yer verilerek, ilgili düzenlemeler kronolojik sırada incelenecektir.

1. Avrupa İnsan Hakları Sözleşmesi

Tarih boyunca insan hakları kavramı ülkeler nezdinde farklılıklar göstermesine karşın, günümüzde insan hakları kavramının evrensel nitelikte bir anlam kazandığı ifade edilebilir. Özellikle İkinci Dünya Savaşı'nı takip eden dönemlerde, insan haklarına yapılan ihlaller, uluslararası alanda düzenlemelere konu olmuştur.

İnsan hakları kavramının gerçek anlamda koruma altına alınması 20. Yüzyılın ikinci yarısına denk düşmektedir. 20. Yüzyılın ikinci yarısından itibaren insan haklarının gelişimi ile gerek bölgesel gerek uluslararası alanda hazırlanan belge ve sözleşmeler hız kazanmıştır. İnsan hakları ihlallerine yönelik atılan ilk adımların başında Birleşmiş Milletler Sözleşmeleri gelmektedir[151]. Bu anlamda Birleşmiş Milletler İnsan Hakları Evrensel Bildirgesi büyük önem arz etmektedir. Nitekim Bildirge'nin, Avrupa Konseyi'nin insan hakları bağlamında hazırladığı uluslararası

[145] **Kişisel Verileri Koruma Kurumu,** "Kişisel Verilerin Korunması Kanununa Duyulan İhtiyaç", s. 1-2; **ÇEKİN,** s. 6.
[146] Bundesdatenschutzgesetz (BDSchG) Federal Veri Koruma Yasası.
[147] **ÇEKİN,** s. 6.
[148] Loi "informatique et libertés" du 6 janvier (ocak) 1978.
[149] **ÇEKİN,** s. 6.
[150] **ÇEKİN,** s. 6.
[151] **TEZCAN/ERDEM/SANCAKTAR,** s. 29.

sözleşmelerden, Avrupa İnsan Hakları Sözleşmesi'ne[152] etkisinin büyük olduğu ifade edilebilir[153].

Sözleşmenin tam adı, "İnsan Hakları ve Temel Özgürlüklerin Korunmasına Dair Avrupa Sözleşmesi" olarak yer almaktadır. AİHS'nin en önemli özelliği, insan haklarını koruma anlamında uluslararası denetim mekanizmalarını gerekli öngören ilk sözleşme olmasıdır[154]. Sözleşme 4 Kasım 1950 yılında Roma'da kabul edilmiştir. Eylül 1953 tarihinde ise yürürlüğe girmiştir. Günümüzde tüm Avrupa Birliği üye devletleri de dahil olmak üzere Sözleşmeye taraf 47 üye devlet bulunmaktadır. Türkiye, Sözleşmeyi 18 Mayıs 1954 tarihinde yürürlüğe koymuştur[155]. Avrupa İnsan Hakları Sözleşmesi[156] ile sağlanan koruma sistemi günümüzde de en etkili uluslararası insan hakları mekanizması olarak önem görmektedir.

Özel hayatın gizliliğine ilişkin hukuki unsurlar ile kişisel verilerin korunması noktasında hem AİHS hem de ABAD güncel içtihatlarıyla konuyu yakından ele almaktadır[157]. Bu anlamda Sözleşme'nin 8. maddesi önem taşımaktadır. Sözleşme'nin m. 8/f.1 hükmü, kişilerin özel hayat, aile hayatı, konut ve haberleşmeye saygı hakkı gibi devlet tarafından güvence altına alınan belli haklarını düzenler. Ancak AİHM, içtihatlarında 8. maddeyi oldukça geniş yorumlamaktadır.

AİHM'nin kişisel verileri korumaya yönelik vermiş olduğu önemli bir kararı Klass-Almanya[158] kararıdır. Sözleşmenin 8. maddesi kapsamında bir diğer önemli karar Rotaru/Romanya kararıdır[159]. AİHM'nin kişisel verileri korumaya yönelik bir diğer önemli kararı Leander v. İsveç[160] kararıdır.

---

[152] European Convention on Human Rights, https://www.echr.coe.int/Documents/Convention_ENG.pdf (Son Erişim Tarihi: 07.10.2021).
[153] **TEZCAN/ERDEM/SANCAKTAR,** s. 30; **ŞİMŞEK**, s. 30-31; **KÜZECİ**, s. 151-153.
[154] **TEZCAN/ERDEM/SANCAKTAR,** s. 34; **ŞİMŞEK**, s. 30-31; **KÜZECİ**, s. 151-153.
[155] **GÖLCÜKLÜ** Feyyaz/**GÖZÜBÜYÜK** Şeref, Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, 11.Ek Protokole Göre Hazırlanıp Genişletilmiş, 9. Bası, Turhan Kitabevi, Ankara, 2011, s. 10;
[156] Kısaca AİHS.
[157] **KÜZECİ**, s. 156-158; Özel hayatın gizliliği ve kişisel verilerin korunması haklarının unsurlarına yönelik hazırlanan hukuki standartlar, başta Avrupa Konseyi ve Avrupa Birliği tarafından geliştirilmiştir. AİHS, AB Temel Haklar Şartı, 108 sayılı Sözleşme, GVKT bu hukuki standartları sağlamaya yönelik atılan adımlardan bazılarıdır.
[158] Avrupa İnsan Hakları Mahkemesi, Klass, Almanya'ya karşı kararı, Başvuru Numarası: 5029/71 Karar Tarihi: 6 Eylül 1978, http://hudoc.echr.coe.int/eng?i=001-57510 (Son Erişim Tarihi: 04.05.2021). Mahkeme verdiği kararla, haberleşmenin yetkili mercilerce yapılan haberleşmenin gizli olduğunu ve mahkemeye başvuran tarafın bu uygulamadan haberdar olmasının mümkün olmayacağına kanaat getirerek mevzuat hükümlerinin, 8. madde kapsamındaki haklarına müdahale olduğunu ifade etmiştir. Ayrıca bkz. **DUTERTRE** Gilles, Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler, Avrupa Konseyi Yayınları, Eylül 2007, Ankara, s. 345.
[159] Ayrıca bkz. Rotaru/Romanya davasında, AİHM ülkenin güvenliğini ilgilendiren bilgileri toplayan, kaydeden ve bu bilgileri arşivleyen Romanya mevzuatını, bu bilgilerin toplanmasına, kaydedilmesine ve

Görüldüğü üzere Sözleşme koruma altına aldığı haklar bakımından bir yenilik getirmese de oluşturduğu uluslararası koruma mekanizmalarıyla insan hakları bağlamında bir öncü olmuştur. Bu anlayış ile insan hakları, devletlerin iç hukuk sistemlerinde olmanın ötesine geçerek uluslararası bir noktaya taşınmıştır. Sözleşme, insan haklarının uluslararası alanda korunmasında AİHM'yi kurarak etkili bir koruma sistemi geliştirmiştir. Her ne kadar Sözleşme kapsamında kişisel verilerin korunmasına ilişkin ayrı bir madde yer almasa da kişisel verilerin korunması hakkının Sözleşmenin 8. maddesi kapsamında geniş ölçüde yorumlanmaktadır.

2. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Rehber İlkeleri

1970'lerin ortalarından bu yana OECD, kişisel verileri sınır ötesi aktarımında, özel hayata saygı ve bu hakkın korunması anlamında önemli bir yol oynamıştır. Bu anlamda OECD, kişisel verilerin uluslararası düzeyde korunması amacıyla, 23 Eylül 1980'de "Özel Hayatın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri"[161] yayınlamıştır. Özellikle büyük ölçekli verilerin sınır ötesine aktarımının son derece hızlı ve kolay olması, kişisel verileri işlenen veri öznelerinin gizliliklerinin korunmasını gerekli kıldığından OECD üye devletlerinin ulusal mevzuatlarını uyumlu hale getirmeye yardımcı olacak rehber ilkeler yayınlanmıştır.

---

depolanmasına ilişkin yetkilerin kullanımının sınırına ilişkin bir yasal düzenleme olmadığı gerekçesi ile Sözleşmenin 8. maddesine aykırı bulmuştur. Mevcut davada başvurucu, Romanya İstihbarat Servisi (RIS) tarafından, çoğunlukla 1946 yıllarına ait kişisel bilgiler içeren bir dosyanın tutulması ve kullanılması nedeniyle özel hayata saygı hakkına aykırı olduğunu ileri sürerek başvuruda bulunmuştur. Mahkeme Rotaru davasında, elli yıldan uzun bir süre öncesine kadar dayanan veri işleme ve muhafaza faaliyetlerine ilişkin, bu bilgilerin imha edilip edilmeyeceğini veya kapsamlı erişim ve düzeltme haklarının garanti edilip edilmeyeceğinin mahkemenin görevinde olmadığını ifade etmiş, ancak bu tür bilgilerin depolanmaya devam edilmesinin, meşru ulusal güvenlik endişesini haklı kıldığını ve devletlerin, kişilerin bilgilerini dosyalama ve arşivleme sistemine tabi tutma konusunda sınırsız takdir yetkisine sahip olmadığını ifade etmiştir. Nitekim Mahkeme, mevcut davadaki ihtilaf konusunun Sözleşmenin m. 8/f.2 anlamında meşru bir amaç taşımadığını dile getirerek ihlal kararı vermiştir.

[160] Avrupa İnsan Hakları Mahkemesi, Leander-İsveç kararı, Başvuru Numarası: 9248/81 Karar Tarihi: 26 Mart 1987. http://hudoc.echr.coe.int/eng?i=001-57519 (Son Erişim Tarihi: 04.05.2021). Davaya konu olayda, görevine son verilen başvurucunun, kendisi hakkında yapılan güvenlik soruşturmasına ilişkin olumsuz gösterilen sonucun içeriği hakkında kendisine bilgi verilmemesi yer almaktadır. Başvurucu, kendisi hakkında elde edilen kişisel verilere karşın kendisine herhangi bir bilgi verilmemesi noktasında özel hayatın gizliliği kapsamında bir ihlal gerçekleştiğini iddia etmiştir. Mahkeme her ne kadar özel hayatın gizliliğine yönelik bir müdahalenin varlığını kabul etmiş olsa da bu müdahaleyi haklı kılacak sebeplerin de var olduğunu ifade etmiştir. Mahkeme başvuran kişiye ait elde edilen kişisel veriler ile ilgili kendisine bilgi verilmemiş olmasının Sözleşmeye aykırılık teşkil etmediğini, devletlerin takdir yetkisi olduğunu ve dolayısıyla bu tarzdaki müdahalenin meşru amaçlarla orantılı bir müdahale olduğu sonucuna varmıştır.

[161] OECD Rehber İlkeleri, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Son Erişim Tarihi: 03.05.2021).

Bu ilkeler üye devletler bakımından tavsiye niteliğinde olup, herhangi bir bağlayıcılıkları yoktur. Bir diğer ifadeyle üye devletler bu rehber ilkeleri kendi iç hukuk sistemlerine alıp almama serbestisine sahiptirler. OECD Rehber İlkeleri bağlayıcılık taşımasa da devletleri geniş ölçüde etkilemiştir. Ülkemizde de KVKK'nın gerekçesinde OECD Rehber İlkelerine atıfta bulunulması bu ilkelerin öneminin bir göstergesidir[162].

3. Avrupa Konseyinin 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ve 181 Sayılı Ek Protokol

1949 yılında kurulan Avrupa Konseyi'nin insan hakları ve hukuk devletinin demokratik yapısını güçlendirme hareketleri, 1950 tarihinde AİHS'ni kabul etmesinin ardından verilerin korunması noktasında da önemli adımlarla devam etmiştir. Özellikle 1960'lı yıllarda Konsey, özel hayatın gizliliği ve kişisel verilerin korunmasına ilişkin çalışmalarını yoğunlaştırmıştır. 1968'de Bakanlar Komitesi (BK), kişisel verilerin korunması ve insan hakları bakımından ülkelerin yasal mevzuatlarının yeterliliğini değerlendirmek üzerine toplanmıştır[163]. Bilgi teknolojilerinin hızla aldığı seyir karşısında kişisel verilerin ve kişilerin özel hayat alanlarının korunmasına ilişkin çalışmalar yapılması ihtiyacı sebebiyle Bakanlar Komitesi 1973'te özel sektörde elektronik veri toplayan bankalara karşı özel yaşamı koruyan karar[164] ile 1974'te kamuda elektronik veri toplayan bankalara karşı özel yaşamı koruyan kararı [165] kabul ederek 108 sayılı Sözleşme'nin temelini atmıştır[166].

Konsey, 28 Ocak 1981'de, "108 sayılı Sözleşmeyi" imzaya sunmuştur. 1985 tarihinde yürürlüğe giren Sözleşme, kişisel verileri koruma hususunda bağlayıcılığı olan ilk uluslararası belge olması yönünden büyük bir öneme sahiptir. Sözleşme aynı zamanda Konsey üyesi bulunmayan diğer devletlerin de imzasına sunulmuştur. 108 sayılı Sözleşme, sadece otomatik yollarla işlenen kişisel verileri kapsamaktadır.

---

[162] **KÜZECİ,** s. 132; **TAŞTAN**, s. 12; **AŞIKOĞLU**, s. 35.
[163] **ATAK** Songül, "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", TBB Dergisi, Sayı 87, 2010, ss. 90-120, s. 92.
[164] Özel Sektörde Elektronik Veri Bankaları Karşısında Bireylerin Özel Hayatlarının Korunmasına İlişkin Karar, https://rm.coe.int/1680502830 (Son Erişim Tarihi: 03.05.2021).
[165] Kamu Sektöründe Elektronik Veri Bankaları Karşısında Bireylerin Özel Hayatlarının Korunmasına İlişkin Karar, https://rm.coe.int/16804d1c51 (Son Erişim Tarihi: 03.05.2021).
[166] **ATAK,** s. 92.

Türkiye, Sözleşmeyi 1981 tarihinde imzalamış ancak Sözleşme'nin 4. maddesindeki düzenleme gereği Sözleşme ancak 30 Ocak 2016'da TBMM'de kabul edilen 6669 sayılı Kanun ile 18 Şubat 2016 tarihli ve 29628[167] sayılı Resmi Gazete'de yayımlanarak onaylanmıştır. İlgili BK Kararnamesi ise 17 Mart 2016 tarih ve 29656[168] sayılı Resmi Gazete'de yayımlanmıştır.

108 sayılı Sözleşme, yürürlüğe girdiği tarihten itibaren büyük bir öneme sahip olmasına karşın, gelişen teknolojik gelişmeler neticesinde Sözleşme üzerinde revizeler yapılması gerekli görülmüştür. Bu gerekçelerle Avrupa Konseyi, 1981 tarihinde imzalanan 108 sayılı Sözleşmeye ek olarak, 2001 yılında "Kişisel Verilerin Otomatik Yöntemlerle İşlenmesi, Denetleyici Otoriteler ve Sınır Ötesi Veri Akışları Hakkında Bireylerin Korunması Sözleşmesine Ek Protokol"'ü[169] (181 sayılı Ek Protokol) kabul etmiştir. 181 sayılı Ek Protokol ile taraf devletlerin, kişisel verilerin korunması noktasında kendi yasal mevzuatlarında bağımsız, özerk bir denetleme kurumu oluşturması ve kişisel verilerin sınır ötesi aktarımlarına ilişkin belirli standartların belirlenmesi amaçlanmıştır. 181 sayılı Ek Protokol, ülkemizde 8 Kasım 2001'de imzalanmış, ancak o tarihte Türkiye'nin yasal mevzuatında Kişisel Verilerin Korunması Kanun'u yürürlüğe girmediğinden onaylanamamıştır. Dolayısıyla 181 Sayılı Protokol'ün iç hukukumuza dahil edilmesi, 5 Mayıs 2016 tarihli 29703[170] sayılı Resmi Gazete'de yayımlanması ile gerçekleşmiştir.

108 sayılı Sözleşme 18 Mayıs 2018 tarihinde Avrupa Konseyi Bakanlar komitesi tarafından yenilemiştir[171]. Sözleşme'nin yenilenmesi ile kişisel verileri koruma noktasında gelişen teknolojik unsurların hassasiyetle değerlendirildiği ve çağın gereklerine uygun olacak yeni gelişmeler sağladığı ifade edilebilir[172]. Çağdaşlaştırılan Sözleşme ile daha esnek, şeffaf ve sınır ötesi veri akışının kötüye kullanımlarına karşın daha etkili bir mekanizma sağlanmaya çalışılmış, özellikle kişisel verilerin sınır ötesine aktarımının Avrupa Birliği mevzuatı da dahil olmak üzere tüm dünyadaki normatif çerçevelerle uyumlu ve tutarlı olmasını sağlamak amaçlanmıştır.

---

[167] Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Sözleşmenin Onaylanmasının Uygun Bulunduğuna Dair Kanun, https://www.resmigazete.gov.tr/eskiler/2016/02/20160218-2.pdf (Son Erişim Tarihi: 03.05.2021).
[168] Karar Sayısı: 2016/8576.
[169] 181 sayılı Ek Protokol, 8 Kasım 2001, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626 (Son Erişim Tarihi:04.05.2021).
[170] R.G., T. 05.05.2016, S.29703.
[171] Sözleşme 108+ https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (Son Erişim Tarihi: 04.05.2021). (Bundan böyle Sözleşme 108+ olarak anılacaktır).
[172] **KÜZECİ**, Elif, Avrupa Konseyi'nin 108 sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter kararı ve Diğer Bazı Gelişmelere İlişkin Bir Değerlendirme.

4. Birleşmiş Milletlerin 45/95 Sayılı Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri

Kişisel verilerin korunması hususunda yer alan bir diğer düzenleme, Birleşmiş Milletler Genel Kurulu'nun 14 Eylül 1990 tarihinde yayımladığı "Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Yönlendirici İlkeler[173]" olmuştur. Tavsiye niteliğinde olan bu ilkelerin bağlayıcılıkları yoktur ancak devletler bu ilkeler doğrultusunda kendi yasal mevzuatlarında gerekli düzenlemeleri yapabilmektedir. Bununla birlikte İlkeler, kural olarak yalnızca bilgisayarla işlenen veri gruplarına ilişkin olarak hazırlanmıştır.

5. Avrupa Parlamentosu ve Avrupa Birliğinin 95/46/EC Sayılı Avrupa Topluluğu Veri Koruma Direktifi

108 sayılı Sözleşme'nin kabul edilmesinden sonra, Avrupa Konseyi, farklı sektörlerdeki uygulamalar üzerine Bakanlar Komitesi'nin bir dizi tavsiye kararının daha geliştirilmesinde rol oynamaya devam etmiştir[174]. Bu tavsiye kararları hem ulusal mevzuatın yolunu hazırlamış hem de diğer uluslararası anlaşmalar için faydalı kriterler sağlamıştır. Bununla birlikte, 1997'den bu yana Avrupa İnsan Hakları Mahkemesi, bir dizi davada kişisel verilerin korunmasının, özel hayata saygı hakkından yararlanmak için "temel bir öneme" sahip olduğuna karar vererek belirli ölçütler çıkarmıştır[175]. İlgili davaların sayısı halen sınırlı ve üye devletler için kişisel verilerin korunması anlamında bir yükümlülük oluşturmasa da Sözleşme kişisel verilerin korunması anlamında tamamlayıcı rol oynamaya devam etmektedir. Öte yandan her ne kadar Avrupa Konseyi, kişisel verileri koruma noktasında başarılı adımlar atmış olsa da bazı üye devletler 108 sayılı Sözleşmeyi yasal mevzuatlarına uyarlama bakımından oldukça geç kalmışlardır[176]. Söz konusu gerekçeler, Avrupa'nın temel haklara dayalı

---

[173] Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Yönlendirici İlkeler, https://www.refworld.org/pdfid/3ddcafaac.pdf (Son Erişim Tarihi: 04.05.2021).

[174] **HUSTINX** Peter, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", s.7. https://edps.europa.eu/sites/default/files/publication/14-09-15_article_eui_en.pdf (Son Erişim Tarihi: 08.05.2021).

[175] **HUSTINX,** s. 7.

[176] **HUSTINX,** s. 9; **IŞIK KAMA** Sezen, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış, Oniki Levha Yayınları,1. Baskı, Ocak 2021, İstanbul, s. 117.

yaklaşımıyla uyumlu olmayan bir duruma yol açmıştır[177]. Dolayısıyla Avrupa Komisyonu, kişisel verilerin işlenmesinde giderek artan önemin farkında olarak bu tutarsızlığı gidermek ve verilerin işlenmesi bakımından kişilerin hak ve özgürlüklerini korunmayı ve verilerin serbest dolaşımın sağlanmayı gerekli bulmuştur.

Anılan gerekçeler ile 1990'lı yıllarda kişisel verileri koruma anlamında yapılan çalışmalar sonucu, 24 Ekim 1995 tarihinde "95/46 EC sayılı Direktif" kabul edilmiştir. Direktif'in temel amacı, kişisel verileri korunmaya ilişkin kabul edilen ilk uluslararası belge olan 108 sayılı Sözleşmede yer alan farklılıkları ve çelişkileri teknolojinin gereklerine uyumlaştırarak, verilerin işlenmesi bakımından bireylerin hak ve özgürlüklerini korunmak ve verilerin serbest dolaşımını sağlamak olmuştur[178].

Direktif ile ilgili öne çıkan bir diğer husus, Direktif'in temel olarak kişisel verileri korumayı değil, "kişisel verilerin işlenmesi yönüyle kişilerin korunmasını" esas aldığı şeklindedir[179]. Bu anlamıyla Direktif, kişilerin özellikle mahremiyet haklarını korumak bakımından başta kişilerin temel hak ve özgürlüklerini korurken bir yandan da özel hayata ilişkin kişisel verilerin işlenmesi noktasında kişileri korumayı amaçlamıştır. Direktif, kişisel verilerin korunması noktasında pek çok kavramı geniş ölçüde belirlemiştir. Bununla birlikte m. 5 gereği üye devletlere, temel olarak formüle edilen bu kavram ve standartları iç hukuklarına aktarma hususunda oldukça geniş bir takdir yetkisi de vermiştir.

Bu noktada Direktif ile ilgili olarak ABAD'ın kişisel verilerin korunmasına ilişkin mevcut yasal çerçeve üzerine verdiği kararları son derece önemlidir[180].

---

[177] **IŞIK,** s. 118.

[178] **CİVELEK YÜKSEL** Dilek, Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Uzmanlık Tezi), Bilgi Toplumu Dairesi Başkanlığı, T.C Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı, Ankara, Nisan 2011, s. 72.

[179] **IŞIK,** s. 119.

[180] ABAD'ın 95/46/EC sayılı Direktif hakkında vermiş olduğu ilk kararı olan Bodil Lindqvist davasında ABAD, kendisine ait bir internet sitesi olan Bayan Lindqvist'in bir kilisede kendisi ile çalışan bazı gönüllü kişilerinde verilerini internet sitesinde yayınlamış olmasının, üçüncü bir ülkeye aktarım sayılıp sayılmayacağını incelemiştir. Mahkeme, kişisel verilerin internet sunucusundan internet kullanıcılarına otomatik olarak gönderilme amacını taşımadığını, bu nedenle sunucuya bilgileri yükleyen kişi ile sunucudan verilere erişen kişi arasında kişisel verilerin doğrudan aktarımının olmadığı ifade etmiştir. Zira bir kişi tarafından internet sitesinde yüklenen verilere erişim bu kişiler arasında değil, sayfanın bulunduğu web (hosting) sağlayıcısının ağ altyapısı aracılığı ile gerçekleşmektedir. Dolayısıyla Lindqvist 'in internet sayfasında yer alan bilgileri kasıtlı olarak bu sayfalara erişmek istemeyen kişilere otomatik olarak gönderme isteği yoktur. İnternet sitesine konulan bir verinin, internet sitesinde yayımlanmış olması sebebiyle üçüncü ülkelere veri aktarımı olarak değerlendirilmesi, bu verilerin ancak bu sayfalara özel olarak erişmek istemeyen kişilere gönderimi ya da AB üyesi olmayan bir ülkede sunucusunun yer alması halinde aktarım olarak değerlendirilmektedir. Lindqvist kararında ABAD ayrıca, Direktif'in 3. maddesi uyarınca uygulama alanı bakımından kişiyi belirli ya da belirlenebilir kılan ad-soyad, telefon numarası gibi bilgilerin internet ortamında yayımlanmasının "verilerin otomatik

6. Avrupa Birliği Temel Haklar Şartı

Avrupa Birliği Temel Haklar Şartı[181], AB ülkeleri arasında ekonomik, siyasal ve anayasal bütünlüğü sağlamak ve temel insan haklarının Birlik düzeyinde toplanması gerekliliğine ilişkin olarak 7 Aralık 2000'de Fransa Nice'de imzalanmıştır.

AB Temel Haklar Şartı'nın önceliği, AB'nin yetkilerini temel insan hakları lehine sınırlandırarak güvence altına almaktır[182]. 1 Aralık 2009 tarihli Lizbon Anlaşması'nın yürürlüğe girmesi ile AB Temel Haklar şartı bağlayıcılık kazanmıştır[183].

7. 2016/679 Sayılı AB Genel Veri Koruma Tüzüğü (GDPR)

95/45/EC sayılı Direktif'in yürürlüğe girmesinin ardından teknolojik gelişmelerin seyri karşısında Direktif'in gözden geçirilmesi ve gerekli düzenlemelerin yapılması gündeme gelmiştir. Avrupa Komisyonu teknolojik gelişmelerin gerisinde kalan ve AB ülkeleri arasında yapılacak yeni düzenlemeler ile Birlik hukukunda tam bir yeknesaklığı sağlamak üzere Ocak 2012 tarihinde AB Veri Koruma Reformu'nu gerçekleştirmiştir. Nitekim bu reform ile 2014 tarihinde Avrupa Birliği Parlamentosu tarafından Tüzük taslak olarak kabul edilmiştir[184]. Toplamda 173 paragraflık giriş bölümünden ve 99 maddeden oluşan GVKT, 27 Nisan 2016 tarihinde kabul edilerek 4

---

yolla işlenmesi" anlamına geldiğini ifade etmiştir. Söz konusu olayda Lindqvist'in verileri işlemesi, işlenen verilerin bir hayır işi amacıyla yapılması ve internet ortamında yayımlandıktan sonra bu bilgileri pek çok kişinin erişimine açık hale getirmesi Direktif m. 3/f.2'ye göre bir istisna teşkil etmektedir. Dolayısıyla işlenen bu kişisel veriler, "bireyin özel ve aile yaşamına" ilişkin veriler olarak Direktif kapsamı dışında değerlendirilmiştir. Bodil Lindqvist Kararı, https://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en (Son Erişim Tarihi: 09.05.2021); **IŞIK**, s. 130-131; **KUNER**, s. 12; **KÜZECİ**, s. 190.

[181] Council of the EU, Charter of Fundamental Rights of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (Son Erişim Tarihi: 10.05.2021).

[182] **METİN** Yüksel, "Avrupa Birliği Temel Haklar Şartı", Süleyman Demirel Üniversitesi Iktisadi ve Idari Bilimler Fakültesi, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, Cilt: 57, Sayı: 4, 2002, ss. 35 – 63, s. 46; **KÜZECİ**, s. 78; **ŞİMŞEK**, s. 69.

[183] Şart metninde yapılan yeni düzenlemeler ile klasik medeni ve siyasi haklar yanı sıra kişisel verilerin korunması hakkı da 8. madde ile düzenlenmiştir. Madde hükmüne göre, "…Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir…" Bu noktada kişisel verilerin korunması hakkının, Şart metninin 7. maddesi ile düzenlenen özel hayata gizlilik hükmünden ayrı düzenlendiği görülmektedir. **KÜZECİ**, s. 175-176.

[184] **BAŞALP**, "Tüzüğün Temel Yenilikleri", s. 83.

Mayıs 2016 tarihinde Avrupa Birliği Resmi Gazetesi'nde yayımlanmıştır[185]. GVKT'nin kabul edilme sürecinin ardından AB içerisinde uyumlaştırılması için iki yıllık süre öngörülmüş ve nihayet Tüzük bu sürenin ardından 25 Mayıs 2018 tarihinde yürürlüğe girmiştir.

95/46/EC sayılı Direktif'in yerini alan GVKT'nin yürürlüğe girmesi pek çok yeniliği de beraberinde getirmiştir. GVKT'nin getirdiği en önemli yeniliklerden biri hukuki metnin kendisi ile ilgilidir. Direktif'in, üye devletlerde doğrudan uygulanamaması, 2016/679 sayılı düzenlemenin Tüzük metni olarak hazırlanması ile "genel uygulama alanına sahip tümüyle bağlayıcı ve üye devletlerin tümünde doğrudan uygulanan bir düzenleme" halini almıştır.

Tüzüğün hazırlanmasında temel alınan politikalar, kişisel verilerin korunması noktasında tüm üye devletlerin farklı düzenlemelerini de ortak bir düzenleme ile bir araya getirirken Birliğin hukuk sistemini iyileştirmek, kişisel verilerin sınır ötesi aktarımına ilişkin bürokratik süreçlerin etkisini azaltmak, kişisel verilerin korunması anlamında Birlik hukuku içerisinde bir tutarlılık ve uyumu sağlamak ve bu kuralların etkili bir şekilde uygulanmasını sağlamıştır[186]. Üye devletler bakımından ayrı bir düzenleme gerekmeksizin doğrudan uygulanabilir olan Tüzük, kişisel verilerin korunması anlamında bir dönüm noktası yaratmıştır. Nitekim Tüzük ile amaçlanan, farklı üye devletlerde faaliyet gösteren şirketler açısından da tek bir muhatapla karşılaşmaları bakımından kazançlı olacaktır[187].

GVKT'nin coğrafi kapsamı yalnızca Avrupa Birliği ile sınırlı değildir. GVKT'nin 3. maddesi, Avrupa Birliği'nde kişisel verilere ilişkin olan hakların kapsamlı bir şekilde korunmasını sağlama açısından, sınır ötesi veri aktarımının sağlanmasında AB pazarlarında faaliyet gösteren şirketler için de dengeli bir oyun alanı oluşturma amacını taşımaktadır.

---

[185] Avrupa Birliği Genel Veri Koruma Tüzüğü, https://eur-lex.europa.eu/eli/reg/2016/679/oj (Son Erişim Tarihi: 07.10.2021).
[186] **AKINCI**, "Tüzüğün Getirdiği Yenilikler", s. 13; **KÜZECİ**, s. 224; **BAŞALP**, "Tüzüğün Temel Yenilikleri", s. 85.
[187] **KÜZECİ**, s. 224.

B. TÜRK HUKUKUNDA KİŞİSEL VERİLERİ KORUMA HUKUKUNUN GELİŞİMİ

1. Genel Olarak

Ülkemizin kişisel verilerin korunması anlamındaki çalışmalarına bakıldığında, kişisel verilerin korunmasını yasal bir temele oturtmada pek çok diğer ülkeye göre geri kaldığı gözlemlenir. Nitekim bu yasal boşluğu doldurmaya yönelik olarak atılan en önemli adım, ancak 7 Nisan 2016 tarihinde yürürlüğe giren KVKK ile mümkün olmuştur. Ülkemizde her ne kadar 1981 tarihli 181 sayılı Sözleşmeyi imzalamış ise de sözleşmenin 4. maddesindeki düzenleme gereği o tarihte KVKK'nın yürürlükte olmaması sebebiyle onaylanması ancak 2016 tarihinde gerçekleşmiştir. Elbette kişisel verilerin korunması anlamında KVKK'ya kadar hiçbir yasal düzenleme yapılmamış değildir. Nitekim Türk Medeni Kanunu, Türk Ticaret Kanunu ya da Türk Ceza Kanunu gibi temel hukuki düzenlemeler ile kişisel verilere yönelik bazı temel güvenceler sağlamıştır. Kişisel verilerin işlenmesine yönelik yapılan ilk düzenlemelerden biri 6 Şubat 2004 tarihli "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik[188]" ile gerçekleşmiştir. Ancak bu yönetmelik, 24 Temmuz 2012 tarihli "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik"'in 23. maddesi ile yürürlükten kaldırılmıştır[189]. Ancak bu yönetmelik de 4 Aralık 2020 tarihli "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunmasına İlişkin Yönetmelik"[190] ile yürürlükten kaldırılmıştır. Yönetmelik ile, elektronik haberleşme sektöründe faaliyet gösteren işletmelerin tüzel kişi abonelikleri de dahil olmak üzere uymaları gereken usul ve esaslar belirlenmiştir. Diğer bir ifadeyle, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunmasına İlişkin Yönetmelik ile tüzel kişilerin de kişisel verileri korunmaktadır. Bunun yanında 12 Eylül 2010 tarihinde yapılan değişiklik ile Anayasa'nın "Özel Hayatın Gizliliği" başlıklı 20. maddesine ilave olunan 3. fıkra ile, kişisel verileri korunmayı talep etme hakkı düzenlenmiştir. Ancak anılan bu düzenlemeler, özellikle 90'lı yıllardan itibaren teknolojik gelişmelerin aldığı seyir

[188] R.G. T. 06.02.2004, S. 25365.
[189] R.G. T. 24.07.2012, S. 28363.
[190] R.G. T. 04.12.2020, S. 31324.

karşısında ülkemizi, kişisel verilerin korunması noktasında yasal düzenlemeleri diğer dünya ülkelerine kıyasla uygulamada geri bırakmıştır.

2. Kişisel Veri Korumasının Anayasal Dayanağı

12 Eylül 2010 tarihinde yapılan değişiklik ile Anayasa'nın "20. maddesine eklenen 3. fıkra ile kişilerin verilerinin korunması talep etme hakkı anayasal güvenceye kavuşmuştur. Düzenlemenin yapılmasında özellikle AB Temel Haklar Şartı'nın etkili olduğu ifade edilmiştir[191]. Bununla birlikte, bağımsız temel bir hak olarak kişisel verilerin korunması hakkına yer verilmesinde Türkiye Barolar Birliği'nin (TBB) hazırladığı Anayasa önerisinin de etkili olduğu vurgulanmıştır[192].

3. Kişisel Verileri Koruma Kanunu

Ülkemiz 31 Temmuz 1959'da ilk kez Avrupa Birliği başvurusunu gerçekleştirmiş olmasına rağmen kişisel verilerin korunması anlamında yapılan çalışmalar ve Avrupa Birliği'nde yapılan çalışmaları takip etmek konusunda son derece geç kalmıştır[193]. Tarihsel gelişimine bakıldığında kişisel verilerin korunmasına ilişkin yapılan ilk çalışmaların Durmuş TEZCAN tarafından hazırlandığı ifade edilmektedir[194]. Nitekim 70'li yıllarda başlayan çalışmalar 2000'li yıllara gelinceye dek sonuçsuz kalmıştır.

---

[191] **KÜZECİ**, s. 321.

[192] Türkiye Barolar Birliği'nin sunmuş olduğu öneride, herkesin kendi hayatına ilişkin olan kişisel verilerinin korunmasını isteyebileceği, kendisi ile ilgili kişisel verilerinin gizli kalmasını talep edebilecekleri ve bu taleplerinin yasal olarak güvenceye kavuşturulması, özellikle teknolojik araçların gelişmesinde kişilere ait veri ihlallerinin doğurduğu endişe kapsamında kaçınılmaz bir gereksinim olduğu ifade edilmiştir. Nitekim teknolojik gelişmeler sonucu ortaya çıkan sorunları ele almada hem kişisel veri ihlallerinin hem de temel insan haklarının korunmasının sağlanması amacıyla bağımsız bir denetim mekanizmasının varlığına dikkat çekilmiştir. **KÜZECİ**, s. 321; Türkiye Barolar Birliği, Türkiye Cumhuriyeti Anayasa Önerisi Geliştirilmiş Gerekçeli Yeni Metin, Kasım 2007/ 4. Baskı, s. 78. http://tbbyayinlari.barobirlik.org.tr/TBBBooks/2007_Anayasa%20Taslagi_TBB.pdf (Son Erişim Tarihi: 07.10.2021).

[193] Türkiye-AB İlişkilerinin Tarihçesi, https://www.ab.gov.tr/turkiye-ab-iliskilerinin-tarihcesi_111.html#:~:text=Bu%20do%C4%9Frultuda%2C%20insanl%C4%B1k%20tarihinin%20en,da%20Toplulu%C4%9Fa%20ortakl%C4%B1k%20ba%C5%9Fvurusunda%20bulunmu%C5%9Ftur. (Son Erişim Tarihi: 14.05.2021); Ayrıca bkz. Türkiye Avrupa Birliği İlişkileri Kronolojisi, https://www.ab.gov.tr/files/5%20Ekim/turkiye_avrupa_birligi_iliskileri_kronolojisi.pdf (Son Erişim Tarihi: 14.05.2021).

[194] **IŞIK**, s. 227; **TEZCAN** Durmuş, "Bilgisayarın Hukukta Kullanılması ve Özellikle Adli Sicil Sisteminin Mekanik Hale Dönüştürülmesi", Adalet Dergisi, Yıl: 70, 1979, No:1-2, ss. 53-79; **ÖZTÜRK**

Türkiye'de kişisel verilerin korunmasına ilişkin olarak ilk komisyon 1989 tarihinde oluşturulmuştur[195]. Ancak komisyon, çalışmalarını tamamlayamadan dağılmış ve 2000 yılında yeni bir komisyon oluşturulmuştur. 2000 yılında kurulan Komisyon, geçen üç yılın ardından kişisel verilerin korunması anlamında bir kanun taslağı hazırlamış olmasına rağmen bu tasarı kanunlaşamamıştır[196]. Komisyon çalışmaları 2008, 2011 ve 2014 tarihlerinde devam etmiş ancak hazırlanan tasarılar, yasama döneminin sona ermesi sebebi ile kadük hale gelmiştir. Bununla birlikte 2010 tarihinde Anayasada yapılan değişiklik ile m. 20/f.3'e getirilen düzenlemeye 2010 tarihli İlerleme Raporu'nda yer verilmiş ancak kişisel verilerin korunmasına ilişkin kanunun kabul edilmesindeki gecikmenin de altı çizilmiştir[197].

Ülkemiz açısından kişisel verilerin korunması anlamında devam eden süreç, 18 Ocak 2016 tarihinde kişisel verileri korunmaya ilişkin "Kanun Tasarısının[198]" TBMM'ne ulaşması ve tasarının 24 Mart 2016 tarihinde kabulü ile tamamlanmıştır. Tasarı metninin kanunlaşması ile 7 Nisan 2016 tarihinde KVKK yürürlüğe girmiştir[199].

Bahri/**ÇALIŞKAN ALTINOK** Elif, "Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu", Fasikül Hukuk Dergisi, S.100, Mart 2018, ss. 277-336, s. 278-280.

[195] **Kişisel Verileri Koruma Kurumu,** Kişisel Verilerin Korunması Kanunu ve Uygulaması, s. 16.

[196] Nitekim, Avrupa Birliği'ne katılım sürecinde AB tarafından yayınlanan pek çok İlerleme Raporu'nda Türkiye'de kişisel verileri koruma hukuku anlamında yasal düzenlemelerin eksikliğine dikkat çekilmiştir.

[197] Türkiye 2010 Yılı İlerleme Raporu, s. 84. https://www.ab.gov.tr/files/AB_Iliskileri/AdaylikSureci/IlerlemeRaporlari/turkiye_ilerleme_rap_2010.pdf (Son Erişim Tarihi: 14.05.2021).

[198] Kişisel Verilerin Korunması Kanun'u Tasarısı ve Gerekçe Metni, https://www2.tbmm.gov.tr/d26/1/1-0541.pdf (Son Erişim Tarihi: 14.05.2021).

[199] R.G. T. 07.04.2016, S. 29677.

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİ KORUMA KANUNUNUN AB GENEL VERİ TÜZÜĞÜ'NE UYUMLAŞTIRMASI BAKIMINDAN ELE ALINMASI GEREKEN KAVRAMLAR VE İLKELER

I. AB VERİ KORUMA TÜZÜĞÜ İLE MEVZUATIMIZDAKİ KAVRAM FARKLILIKLARI

A. KİŞİSEL VERİNİN TANIMINA İLİŞKİN FARKLILIKLAR

KVKK m. 3/f.1-d'ye göre kişisel verinin tanımı, *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak kabul edilmektedir. Kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi ifadesinin, kişisel verilerin korunmasını konu alan pek çok uluslararası sözleşmede ortak bir tanımla ve benzer unsurlar dahilinde ifade edildiği görülmektedir.

Bununla birlikte 95/46/EC sayılı Direktif'in 2. maddesi ile kişisel veri tanımının genişletildiği ve kişisel verinin, *"...fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğe özel, bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak belirli ya da belirlenebilir gerçek kişiye ait her türlü bilgiyi kastedecektir…"* şeklinde tanımladığı görülmektedir. GVKT'nin yürürlüğe girmesi ile de kişisel veri tanımının detaylandırılarak kişisel verinin, gerçek kişiye ait belirli ya da belirlenebilir her türlü bilgiyi ifade ettiği belirtildikten sonra gerçek kişi olarak veri sahibinin kişisel verilerinin neler olduğu genel hatlarıyla kategorize edilmiştir. Tüzüğün 4. maddesine göre veri sahibi, "…*belirli ya da belirlenebilir nitelikte isim, kimlik numarası, konum verisi, çevrim içi tanımlayıcı ya da gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda etmene atıfla doğrudan veya dolaylı olarak tanımlanabilen kişi…"* olarak ifade edilmektedir.

Görüldüğü üzere, KVKK'ya esas teşkil eden Direktif hükümlerinde ve daha sonra yürürlüğe giren Tüzük hükümlerinde kişisel veri tanımını detaylandırılarak, nelerin kişisel veri sayılacağı örneklerle kategorize edilmiştir. Elbette kişisel verinin

tanımına ilişkin yapılan açıklamalar son derece geniş ve yoruma açık olduğundan, kişisel veri sayılacak tüm veri kategorilerinin sınırlı sayıda sayılması mümkün değildir.

Her ne kadar KVKK, 95/46/EC sayılı Direktif'i referans almışsa da KVKK ile GVKT'nin kişisel verinin tanımına ilişkin farklılıklarının yanında ortaklık taşıdığı yönlerinin de ifade edilmesi önem arz etmektedir. Bu ortak yan, kişisel verinin unsurlarına ilişkindir. Zira, "29.Madde Çalışma Grubu[200]" kişisel verinin unsurları bakımından farklı yorumlarda bulunarak dört unsurun[201] varlığını gündeme taşımıştır[202]. Oysa KVKK ile Tüzük kişisel verinin üç unsuru olduğunu kabul etmektedir. Bu unsurlar, kişisel verinin kaynağı olan "bilgi", "kimliği belirli ya da belirlenebilir kılan veri sahibi" ve "bilginin/kişisel verinin ilgili kişi olan veri sahibine ait olması" halidir. Bu anlamda, bir kişiyi belirli kılan ya da kılabilen her türlü bilgiyi kişisel veri olarak değerlendirmek gerekmektedir[203]. Kanaatimizce, kişisel verinin unsurlarını, kişisel veri niteliğini taşıyan "bilgi", bilginin sahibi olarak "belirli ya da belirlenebilir veri sahibi kişi" ve bilginin ilgili veri sahibi kişiye "ilişkin olması" şeklinde ifade etmek yerinde olacaktır.

Kişisel verilerin korunmasına ilişkin düzenlemelerde kişisel verinin, bir kişiyi belirli ya da belirlenebilir kılan "her türlü bilgi" olarak değerlendirildiği görülmektedir. Her türlü bilgi ile kanun koyucuların asıl amacının, kişisel veriye ilişkin bilgi kaynağını oldukça geniş yorumlayacak şekilde tanımladığı ifade edilebilir[204]. Bilginin tanımı gereği, kişisel veri kavramı, bir kişi bakımından "nesnel" ya da "öznel" nitelikte olabilecek her türlü veriyi içerebilir. GVKT m. 4/f.1'e göre, bir gerçek kişi ile ilgili olarak adı ve soyadı, doğum yeri ve tarihi, pasaport bilgileri; parmak izi; iletişim

[200] 29. Madde Çalışma Grubu (Article 29 Working Party) 95/46/EC sayılı Direktif'in 29 uncu maddesi uyarınca kurulmuştur. 29. Madde Çalışma Grubu, veri koruma ve gizlilik konusunda bağımsız bir Avrupa danışma organıdır. Ancak 95/46/EC sayılı Direktif'i mülga eden GVKT'nin 25 Mayıs 2018 tarihinde yürürlüğe girmesiyle 29. Madde Çalışma Grubu yerini "Avrupa Veri Koruma Kurumu" (Europian Data Protection Board)'a bırakmıştır.

[201] Bu unsurlar, "bilgi", "ilgili olma", "belirli ya da belirlenebilir olma" ve "(natural person)- gerçek kişi" olarak ifade edilmiştir. Çalışmamızda, mevcut Avrupa Birliği düzenlemeleri ve yasal mevzuatımız açısından da görüş birliği olan kişisel veri unsurları, üç ana grupta incelenmiştir. **29. Madde Çalışma Grubu,** WP 136, s. 5.

[202] Çalışma Grubu tarafından 20 Haziran 2007 tarih ve 4/2007 sayılı kişisel veri kavramı hakkında yer alan görüşlere göre kişisel verinin dört temel unsuru olduğu kabul edilmektedir. Çalışma Grubu, kişisel veri kavramının derinlemesine bir analizini yapma ihtiyacından yola çıkarak, Avrupa Birliğine üye devletlerdeki uygulamalar ile ilgili kişisel veri kavramının tanımına ve işleyişine ilişkin belirsizliklerin ve uygulamada ortaya çıkan farklılıkların da tek bir çatıda toplanması amacıyla görüşlerini paylaşmıştır. Grubun bu anlamda görüş sunma amacı, kişisel veri kavramı ile ilgili ulusal veri koruma kurallarının Avrupa çapında meydana gelen belirli kategorilerdeki durumlara uygulanması gerektiği konusunda rehberlik sağlayarak ortak bir anlayışa ulaşmaktır.

[203] **AKSOY,** s. 21-23**; TAŞTAN**, s. 34-35; **ŞİMŞEK**, s. 122; **Kişisel Verileri Koruma Kurumu,** "6698 Sayılı Kanun'da Yer Alan Temel Kavramlar", s. 12.

[204] **AŞIKOĞLU**, s. 7; **29. Madde Çalışma Grubu**, WP 136, s. 6.

numarası, mail adresi, ikametgahı gibi iletişim ve adres bilgileri; sosyal güvenlik numarası, araç plakası, mesleki deneyimini gösterir cv bilgileri ya da resim, video, ses kayıtları, kişisel tercihleri, hobileri, kişiyi belirlenebilir kılan alışkanlıkları, aile üyelerine ait bilgileri, sendika üyelikleri ile sağlık verileri kişisel veri olarak kabul edilmektedir.

Kişisel verinin her koşulda doğru ya da kanıtlanmış bir bilgi olması gerekli değildir[205]. Hiç şüphesiz ilgili gerçek kişiye ilişkin kişisel verilerin yanlış olabilme ihtimali kişisel verinin niteliğine bakılmaksızın özel nitelikteki bilgileri de kapsamaktadır[206]. Kişisel verilerin değerlendirilmesinde, kişisel veri kaynağının hangi formattan elde edildiğinin bir önemi bulunmamaktadır[207]. Bu anlamda kişisel veri gerek kağıt üzerinde yer alan fiziksel bir formattan elde edilebileceği gibi, bilgisayar ya da internet ortamında tutulan elektronik verileri de içerebilir[208]. Özellikle ses ve görüntü verileri, bir birey hakkındaki bilgileri ifade ettikleri sürece kişisel veri olarak nitelendirilir. Keza 95/46/EC sayılı Direktif'in 33. maddesi ve Tüzüğün 4. maddesinin 14. fıkrası da ses ve görüntü verilerini kişisel veri olarak kabul etmektedir[209].

Kişisel veri olarak kabul edilen veri kategorilerinde sınırlı sayı ilkesi kabul edilmediğinden kişisel veri kapsamının genişletilmesi mümkündür. Bu noktada kişisel verinin önemi, bu verilerin kişiyi belirli ya da belirlenebilir kılması halidir[210]. Nitekim, takma ad[211], lakap ya da mahlas gibi isimler, kişiyi belirlenebilir kılmaya yetiyorsa,

---

[205] **29. Madde Çalışma Grubu**, WP 136, s. 6; **ŞİMŞEK**, s. 122; **ŞENOCAK**, Kişisel Verilerin Korunması Hukuku, "Kişisel Veri Kavramının Kapsamı ve Unsurları" s. 7.
[206] **29. Madde Çalışma Grubu**, WP 136, s. 6.
[207] **29. Madde Çalışma Grubu**, WP 136**,** s. 7; **AŞIKOĞLU,** s. 8.
[208] **29. Madde Çalışma Grubu**, WP 136**,** s. 7.
[209] **29. Madde Çalışma Grubu**, WP 136, s. 6.
[210] **Kişisel Verileri Koruma Kurumu,** "Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular", s. 21, https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular (Son Erişim Tarihi: 09.10.2021).
[211] Takma ad kullanılarak isimlendirme, kimi durumlarda kimlikleri gizleme amacını taşır. Böyle bir sürecin amacı, özellikle özel nitelikte kişisel verileri işlenen hastalar gibi durumlarda karşımıza çıkmaktadır. Temel olarak amaçlanan kişinin kişisel verilerini korumaya alarak, kişi hak ve menfaatlerini korumak, bir yandan da kimliği ortaya çıkarmadan kişi ile ilgili ek verileri toplamaktır. Bu amaç, özellikle araştırma ve istatistik bağlamında önem taşır. Kimlikleri gizlemek, örneğin genel olarak anonimleştirilmiş verilerden oluşan ve tanımlamanın mümkün olmadığı bir şekilde de yapılabilir. Takma isimlendirme prosedürünün etkililiği, hangi aşamada kullanıldığı, ters izlemeye karşı ne kadar güvenli olduğu, kişinin gizlendiği nüfusun büyüklüğü gibi birtakım faktörlere de bağlıdır. Bu anlamıyla takma adlar rastgele ve tahmin edilemez olmalıdır. Geriye dönük izlemeyi mümkün kılan takma adlar, dolaylı olarak belirlenebilen kişiler hakkında bilgi olarak değerlendirilirler. Dolayısıyla, bu verilerden kişiye ilişkin bilgilere geriye dönük ulaşılabilir. Bu durumda, veri koruma kuralları geçerli olsa da bu tür dolaylı olarak belirlenebilir bilgilerin işlenmesiyle ilgili olarak kişiler için kişisel verilerin tehlike yaratacak riskleri daha düşük olacaktır. **29. Madde Çalışma Grubu**, WP 136, s. 18.

kişisel veri olarak kabul edilecektir[212]. Bununla birlikte kişiyi belirli ya da belirlenebilir kılan müşteri şikâyet raporları gibi belgeler, çalışanlar hakkında tutulan başta özlük evrakları, bordrolar, nüfus cüzdanı fotokopileri, performans değerlendirme raporları, mülakat değerlendirme raporları gibi belgeler, müşteriye ait kullanıcı işlem bilgileri, banka hesap bilgileri, banka dekontları ya da kredi kartı ekstreleri gibi belgeler de kişisel veri olarak kabul edilebilecektir[213].

Tüzüğün 4. maddesinin 1. fıkrasına göre kişi isim, kimlik numarası, konum bilgisi gibi bilgiler ile belirli kılınabilirken; fiziksel ve ruhsal özelliklerine, sosyal durumuna, kültürel durumuna ya da ekonomik durumuna, genetik özelliklerine ilişkin bilgiler ile de belirlenebilir kişi olabilmektedir. 29. Madde Çalışma Grubu'nun 4/2007 sayılı Raporu, belirli bir ana kadar kimliği belirlenmemiş olan kişinin halen kimliğinin belirlenebilir olabileceğini ifade etmiştir[214]. 4/2007 sayılı Rapor, kişiyi belirli kılmayı sağlayacak yeterlilik derecesinin, her durumun kendi nezdindeki bağlama dayalı olduğunu ifade etmiştir. Örneğin, yaygın olarak kullanılan bir aile adının, bir sınıftaki öğrencinin kimliğini belirli kılma ihtimali yüksek iken, bu aile adının, ülkenin nüfusunun tamamından birini tanımlamak ya da ayırt etmek için yeterli olmayacağı ifade edilmiştir[215]. Yine, "Beyaz takım elbiseli adam" gibi yardımcı bilgilerin, yoldan geçen sıradan bir kişiyi tanımlama ihtimalinin yüksek olması, kişinin doğru şekilde belirli kılınıp kılınmadığı ihtimalleriyle her durumun özelinde değerlendirilmelidir.

4/2007 sayılı Rapor, kişiyi belirli ya da belirlenebilir kılma durumunu, doğrudan ve dolaylı olacak şekilde iki gruba ayırmıştır. Buna göre, "doğrudan" belirli ya da belirlenebilir kişilerle ilgili olarak, kişinin adı, gerçekten de en yaygın belirleyici bilgi olarak karşımıza çıkmakta ve pratikte de o kişiye doğrudan atıf yapmaktadır. Elbette, belirleyici kabul edilecek ismin yaygın olarak kullanılması ihtimalinde, bir kişiyi belirli kılmak ve olası karışıklıkları önlemek için bazı durumlarda kişinin isminin farklı veri grupları ile bir araya getirilmesi gerekmektedir. Bu veriler, kişinin doğum tarihi, aile bireylerinin isimleri, adres bilgileri ya da kişiye ait fotoğraflar

---

[212] Örneğin "Megastar" lakabı Tarkan Tevetoğlu isimli sanatçıya, "Süperstar" lakabı Ajda Pekkan isimli sanatçıya verilmiş bir lakaptır. Yine Tarık Akan takma adını kullanan sanatçın gerçek ismi Tarık Tahsin Üregil, Seda Sayan takma adını kullanan sanatçının gerçek ismi Aysel Gülaçar'dır. https://www.hurriyet.com.tr/mahmure/galeri-iste-unlulerin-gercek-isimleri-34942507 Dünyaca ünlü Şilili yazar Pablo Neruda da mahlas kullanan yazarlardan olup yazarın gerçek ismi Ricardo Eliecer Neftalí Reyes Basoalto'dur. https://tr.wikipedia.org/wiki/Pablo_Neruda Yine ünlü çizgi romancı Stan Lee'nin gerçek ismi Stanley Martin Lieber'dır. https://tr.wikipedia.org/wiki/Stan_Lee

[213] **MANAV** Eda A., "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XIX, Y. 2015, Sa. 2, s. 99.

[214] **29. Madde Çalışma Grubu**, WP 136, s. 12 vd.

[215] **29. Madde Çalışma Grubu**, WP 136, s. 12 vd.

olabilir[216]. Örneğin, spesifik bir dükkânda bir miktar para borcu olduğu bilinen Ahmet isimli kişinin, adı ile bağlantılı olarak bir kişiyi belirlenebilir kılması pekâlâ mümkündür. Zira isim, kişinin içinde bulunduğu toplumda kendisini ayırt etmek ve ilişki kurduğu kişilerce tanınmak için kullanılan harf ve ses kombinasyonundan oluşan bilgidir[217]. Bununla birlikte isim, kişinin nerede yaşadığı ya da nerede bulunabileceği hatta soy ismi aracılığı ile aile bireyleri, eğitim bilgileri, sağlık kayıtları, banka bilgilerine ilişkin bilgi veren bir başlangıç noktası da olabilmektedir[218].

Kişiyi belirli ya da belirlenebilir kılmaya yetecek "dolaylı" bilgiler ise, bilginin önemine ya da büyüklüğüne bakılmaksızın, kişiyi belirlenebilir kılmaya yetecek "eşsiz kombinasyonlar" olgusu ile ilişkilendirilmektedir[219]. İlk bakışta mevcut bilgilerin kişiyi belirli ya da belirlenebilir kılmaya yetmediği durumlarda, bu kişi yine de diğer yardımcı bilgiler ile değerlendirilerek "belirlenebilir" kılınabilir[220]. Bu bilgiler, somut olayın özelliğine göre kimi zaman son derece benzersiz olabilmektedir. Örneğin, "İtalya'nın şu anki Başbakanı" denildiğinde, ifade edilen veriler ile kişi net olarak belirli kılınacaktır[221].

Avrupa Adalet Divanı bir kararında[222], bir web sayfasında spesifik kişilere atıfta bulunmanın ve bu kişileri isimleri, telefon numaraları, çalışma şartları, hobileri ve benzeri bilgileri kullanarak tanımlamanın, 95/46/EC sayılı Direktif'in 3. maddesinin 1. fıkrası uyarınca kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesi anlamında kişisel veri işlemeye dahil olacağını ifade etmiştir. Keza, KVKK'nın 3. maddesi kapsamında yer alan kişisel verilerin tanımına ilişkin gerekçede[223], bireylerin spesifik olarak teşhis edilmesini sağlayan isim, soy isim ya da doğum yeri ve tarihi gibi bilgilerle değil, aynı zamanda kişilerin sosyal, ekonomik, kültürel özelliklerine atıfta bulunan, fiziksel özelliklerine ya da aile yaşamlarına ilişkin alışkanlıkları ortaya koyan verilerinde kişisel veri olarak kabul edildiği ifade edilmiştir.

---

[216] **29. Madde Çalışma Grubu**, WP 136, s. 13.
[217] **29. Madde Çalışma Grubu**, WP 136, s. 13.
[218] **29. Madde Çalışma Grubu**, WP 136, s. 13.
[219] **29. Madde Çalışma Grubu**, WP 136, s. 13; **AYÖZGER ÖNGÜN**, s. 6; **ÇELİKEL**, s. 69.
[220] **29. Madde Çalışma Grubu**, WP 136, s. 13.
[221] **29. Madde Çalışma Grubu**, WP 136, s. 13.
[222] Bodil Lindqvist Kararı, para. 27
[223] **Kişisel Verileri Koruma Kurumu,** "Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) Ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü (Kısaca KVKK Terimler Sözlüğü), s. 9. https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu (Son Erişim Tarihi: 06.04.2021).

Bu noktada bahsedilmesi gereken bir diğer kişisel veri türü, anahtar kodlu verilerdir[224]. Anahtar kodlu veriler, istatistiksel amaçlar ile makul sınır çerçevesinde kullanılabilen verilerdir. İstatistiksel amaçlı işlenecek veriler belirli bir düzende kümelenerek belirli kişilerle ilgili spesifik kodlara dönüştürülür[225]. "A202 kodlu kişi, günde 2 litre su içer" şeklindeki bir ifade bu anahtar kodlamaya bir örnektir. Bu tür veriler genellikle ilaçlarla yapılan klinik çalışmalarda kullanılır. Klinik çalışmaların araştırılması ve yürütülmesine ilişkin 4 Nisan 2001 tarih ve 2001/20 sayılı Direktif[226] bu faaliyetlerin izlenmesi için yasal bir çerçeve ortaya koymaktadır[227]. Her ne kadar anahtar kodlu veriler kişiyi belirlenebilir kılmaya yetecek açıklıkta olmasa da bu verilerin 3. kişilerce ele geçirilmesi durumunda kişisel verilerin ihlali söz konusu olabilecektir. Örneğin, klinik çalışmaların yapıldığı kurumda yer alan bir çalışanın gerekli kodları bir araya getirerek açığa çıkarması durumunda çalışmaya katılan kişilerin kimlikleri ortaya çıkabilecektir.

Bir diğer ifade edeceğimiz veri türü, anonim verilerdir. Anonim veriler, kişinin veri sorumlusu veya üçüncü bir kişi tarafından, makul olarak kullanılan muhtemel tüm araçlar dikkate alınmasına rağmen belirlenemediği durumlar için söz konusu

---

[224] **29. Madde Çalışma Grubu**, WP 136, s. 18.

[225] İstatistiksel amaçla kullanılan ve işlenerek kayıt altına alınan bu veriler, örneğin tüketicilerin su içme alışkanlıklarına ilişkin ulusal bir su firmasına aktarılabilir. Tüketicilerin su içme alışkanlıklarına ilişkin su firmasına gönderimi yapılan bu listenin halen kişisel veri olarak değerlendirilip değerlendirilemeyeceği, işleme amaçlarının makul sebepleri aşıp aşmadığına bağlıdır. İlgili kişiler hakkında kullanılan anahtar kodlar benzersiz olmasına rağmen, bu kod anahtarlarına herhangi bir saldırı karşısında, ilgili kişilerin kişisel verilerinin ortaya çıkma riski olacaktır. Böyle bir durumda verileri işleyen veri sorumlusunun sorumluluğu doğacaktır. Buna rağmen, kullanılan anahtar kodlar, her ilgili kişi için benzersiz olarak yaratılmamış olabilir. Bir diğer ifade ile aynı kod numarası (örneğin, "202") farklı yıllardaki ve farklı şehirlerdeki bireyleri ifade etmek için kullanılabilir. Böyle bir durumda veri sorumlusu ya da üçüncü kişi, söz konusu verilerin hangi ilgili kişilere ait olduğunu ancak o yılları ya da o şehri bildiğinde tanımlayabilecektir. Bu kişisel verilere karşı gerçekleşecek muhtemel bir saldırıda ya da bu bilgilerin geri döndürülemeyecek şekilde yok olması durumunda, bilgilerin kimliği belirlenebilir kişilere atıfta bulunmadığı ve veri koruma kurallarına tabi olmayacağı ifade edilebilir. ICO, Anonymisation: managing data protection risk code of practice, About this code, s. 7-8. https://ico.org.uk/media/1061/anonymisation-code.pdf (Son Erişim Tarihi: 08.10.2021); Information ICO, "Guide to the General Data Protection Regulation (GDPR)", 1 Ocak 2021, s. 48. https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection regulation-gdpr-1-1.pdf (Son Erişim Tarihi: 08.10.2021).

[226] Klinik çalışmaların araştırılması ve yürütülmesine ilişkin Direktif, https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/dir_2001_20/dir_2001_20_en.pdf (Son Erişim Tarihi: 06.04.2021).

[227] Buradaki soru, klinik araştırma için kullanılan verilerin "kimliği belirlenebilir" gerçek kişilerle ilgili olarak kabul edilip edilemeyeceği ve dolayısıyla veri koruma kurallarına tabi olup olmadığıdır. Daha önce ifade edildiği gibi kişiyi belirlenebilir kılmada veri sorumlusu veya başka herhangi kişi tarafından söz konusu kişiyi belirlemek için makul olarak kullanılması muhtemel tüm araçların hesaba katılması gerekmektedir. Bu durumda, ihtiyaç halinde uygun tedaviyi uygulamak adına bireylerin belirlenmesi, anahtar kodlu verilerin makul sınırlar dahilinde işlenme amaçlarından birini oluşturur. Hastaların bu yöntemlerle verilerinin işlenmesinde anahtar kodlu verilerin, kimliği belirlenebilir gerçek kişilere ilişkin bilgiler oluşturduğu ve veri koruma mevzuatı kurallarına tabi olması gerektiği sonucuna varılabilir. **29. Madde Çalışma Grubu**, WP 136, s. 19-20.

olmaktadır[228]. Bir diğer ifade ile "anonim veriler", önceden belirlenebilir bir kişiye atıfta bulunan ancak bu kimliğin artık kişiyi belirlenebilir kılmasının mümkün olmadığı durumlarda kullanılan verilerdir[229]. Yine verilerin bir bireyin kimliğinin belirlenmesine izin verip vermediğinin ve bilginin anonim olarak kabul edilip edilemeyeceğinin değerlendirilmesi mevcut koşullara ve duruma göre analiz edilir.

Kanaatimizce, madde hükmünde yer verilen bilgilerin, bir gerçek kişiyi hangi ölçüde belirli ya da belirlenebilir kıldığı her somut olaya ve duruma göre değişebilecektir. Buna göre, kişisel verinin kişiyi belirli ya da belirlenebilir kılma hali, gerekli araştırmanın yapılması ile doğrudan ilişkilidir. Yapılacak incelemenin, makul sebepler dahilinde kullanılan tüm araçlar hesaba katılarak her somut olaya göre ayrı ayrı değerlendirilmesi gerekmektedir. Sonuç olarak gerek Türk Hukukunda gerek Tüzük'teki kişisel veri kavramının örtüştüğü ancak Tüzük'te yer alan tanımlamanın daha açıklayıcı olduğu ifade edilebilir.

B. TÜZÜĞÜN VERİ İŞLEME FAALİYETİNİ YÜRÜTENLER BAKIMINDAN FARKLILIKLARI

Kişisel verilerin işlenmesi faaliyetini sürdüren gerçek ya da tüzel kişilerin gerek KVKK gerek Tüzük hükümleri bakımından bazı farklılıklar taşıdığı açıktır. Aşağıda bu farklılıkları önce veri sorumlusu bakımından, özellikle ortak veri sorumlusu kavramına değinerek irdeleyecek; ardından veri işleyen, alıcı (recipient) ve üçüncü kişi (third party) yönünden değerlendireceğiz.

1. Veri Sorumlusu Bakımından

KVKK'nın 3. maddesine göre veri sorumlusu, *"Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak ifade edilmiştir. Dolayısıyla kişisel verilerin nasıl ve hangi amaçlar dahilinde işleneceğini belirleyen kişi, veri sorumlusu olmaktadır[230].

---

[228] **29. Madde Çalışma Grubu**, WP 136, s. 21; Ayrıca bkz. **ÇELİKEL**, s. 82; **AŞIKOĞLU**, s. 10.
[229] **29. Madde Çalışma Grubu**, WP 136, s. 21.
[230] **Kişisel Verileri Koruma Kurumu,** 100 Soruda Kişisel Verilerin Korunması Kanunu, s. 30.

Veri sorumlusu kavramı, 95/46/EC sayılı Direktif'te "data controller" olarak ifade edilmiş olup, Direktif'in "Tanımlar" başlıklı 2. maddesinin d bendinde verilerin işlenme amaçlarını tek başına ya da başkalarıyla ortak olarak belirleyen gerçek ve/veya tüzel kişi, kamu kurum ya da kuruluşları ya da diğer kuruluşlar olarak tanımlanmıştır[231]. GVKT "Tanımlar" başlıklı m. 4/f.7'de veri sorumlusu kavramının Direktif hükümleri ile benzer olacak şekilde veri işlenme amaçlarını tek başına ya da başkalarıyla ortaklaşa belirleyen gerçek ve/veya tüzel kişileri, kamu kurum/ kuruluşları ya da diğer kuruluşlar şeklinde ifade edildiği görülmektedir.

Gerek KVKK'nın 3. maddesi gerek Direktif ve Tüzük hükümleri incelendiğinde, veri sorumlusu kavramının ortak bir anlayışla ifade edildiği görülmektedir[232]. Buna göre veri sorumlusu her üç metinde de gerçek bir kişi olabileceği gibi şirket, dernek, vakıf ya da kamu kurumları gibi tüzel kişileri de kapsayabilmektedir[233]. Bununla birlikte tüzel kişiliği bulunan kurum ya da kuruluşlar bakımından veri sorumlusu, o tüzel kişiliğin kendisi olmaktadır[234]. Ayrıca veri sorumlusu bakımından kamu tüzel kişiliği ya da özel tüzel kişiler bakımından da bir ayrım gözetilmemiştir[235]. Belirtmek gerekir ki, KVKK m. 16/f.2'ye ve Veri Sorumluları Sicili Hakkında Yönetmelik m. 5/f.1-b'ye göre Türkiye sınırları içerisinde kişisel veri işleyen tüm gerçek ve tüzel kişiler, kanun hükümleri ya da kurul kararlarıyla, istisna olmadıkça kural olarak Veri Kayıt Siciline (VERBİS) kaydolmakla yükümlüdür.

Veri sorumlusu, kişisel verilerin ne amaçla ve/veya hangi yöntemlerle işlemeye konu olacağını belirlemekle yükümlüdür. Bununla birlikte kişisel verilerin işlenmesine yönelik olarak birden fazla veri sorumlusu bir araya gelerek verilerin işlenmesi

---

[231] Veri denetleyici ya da Kontrolör kavramı yerine KVKK'da yer alan Veri Sorumlusu ifadesi kullanılmaktadır.

[232] **KÜZECİ,** s. 364.

[233] **ÇEKİN,** s. 52; **KÜZECİ,** s. 365; **Kişisel Verileri Koruma Kurumu,** 100 Soruda Kişisel Verilerin Korunması Kanunu, s. 30.

[234] **Kişisel Verileri Koruma Kurumu**, Veri Sorumlusu ve Veri İşleyen, s. 1. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf (Son Erişim Tarihi: 18.05.2021).

[235] KVKK Veri Yönetimi Dairesi Başkanlığı, Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), s. 18., *"…Tüzel kişilerde veri sorumlusu, görevlendirilen bir gerçek kişi değil tüzel kişiliğin bizzat kendisidir. Buna göre şirketlerde veri sorumlusu; şirket çalışanı, yöneticisi, patronu, yönetim kurulu başkanı, yönetim kurulu üyeleri, avukatı gibi şirketi temsil eden kişiler veya dışarıdan hizmet alınan kişiler değil, şirketin kendisidir. Ancak şirket, Kanunun uygulanmasıyla ilgili iş ve işlemleri yerine getirme konusunda bu kişileri görevlendirebilir. Bu görevlendirme o kişinin veri sorumlusu olduğu anlamına gelmez…"* https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERB%C4%B0S.pdf (Son Erişim Tarihi: 11.10.2021).

hakkındaki yöntemlere ortaklaşa karar verebilir[236]. Böyle bir durumda bu veri sorumluları, "ortak veri sorumluları" olarak ilgili GVKT kurallarına uymak bakımından kendi sorumluluklarını belirleyen bir düzenleme yapmak durumundadır. Yapılan bu düzenleme, Tüzüğün 26. maddesine göre kişisel verileri işlenen kişilere de bildirilmelidir. Ayrıca GVKT'nin 24. maddesine göre veri sorumluları, verileri işlenme faaliyetleri bakımından, kişisel verileri işlenen gerçek kişilerin hak ve menfaatlerini koruma noktasında ortaya çıkabilecek her türlü riske karşı gereken uygun tedbirleri almakla yükümlüdür. Benzer bir ifade KVKK m.12/f.1'de veri sorumlusunun verilerin güvenliğini sağlamada gerekli tedbirleri alması gerektiği ve kişisel verilerin hukuk kurallarına aykırı olacak şekilde işlenmesini, erişilmesini, muhafazasını önlemekle yükümlü olduğu şeklinde yer almaktadır.

Veri sorumlusu kavramına ilişkin ortak ifadelere yer verdikten sonra Tüzük, Direktif ve Kanun metni açısından farklılık yaratan hususlara değinmek gerekir. Nitekim GVKT'de yer alan veri sorumlusu kavramı, Direktif ve Kanun hükümlerine nazaran daha ayrıntılı açıklamalar içermektedir. Ancak bu noktada önemli bir detayı açıklığa kavuşturmak gerekir. KVKK'nın 3. maddesi veri sorumlusu ile ilgili olarak "*veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* tanımlamasını yapmıştır. Söz konusu tanımlamaya göre bir gerçek ya da tüzel kişiliğin KVKK'nın 3. maddesinde yer alan her iki ön koşulu da gerçekleştirdiği sürece mi veri sorumlusu sayılacağı tartışma yaratmaktadır. Buna göre, gerçek veya tüzel bir kişinin veri sorumlusu olarak kabul edilebilmesinde ilk unsur, veri sorumlusunun kişisel verilerin nasıl ve hangi yöntemler kullanılarak işleneceğine karar verici mekanizma olmasıdır[237]. Gerçek veya tüzel bir kişinin veri sorumlusu olarak kabul edilebilmesi için kanun lafzından anlaşılan ikinci unsur, veri sorumlusunun "veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan kişiyi" ifade ettiği hususudur[238]. İşte bu noktada, Tüzük metni de birlikte değerlendirildiğinde, doktrinde kabul gören genel görüş, veri sorumlusunun veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olduğuna ilişkin ikinci unsurun zorunlu değil aksine tamamlayıcı bir unsur olduğu yönündedir[239]. Bir diğer ifade ile, bir kimsenin veri

---

[236] **DÜLGER** Murat Volkan, "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması", Yaşar Hukuk Dergisi C.1 S.2 Temmuz 2019, s. 90.

[237] **PEKMEZ** Cüneyt, "Overview of the Definitons of Data Controller and Data Processor within the Scope of The Turkish Code of Personal Data Protection (TCDP)", Annales de la Faculté de Droit d'Istanbul, Sayı 67, 2019, ss. 59-71, s. 63; **ÇEKİN**, s. 54; **ÇELİKEL**, s. 84, 87; **DEVELİOĞLU**, s. 42.

[238] **PEKMEZ, s**. 63.

[239] **PEKMEZ,** s. 63; **ÇEKİN**, s. 54-55.

sorumlusu kabul edilebilmesi için kişisel verilerin hangi amaçlar dahilinde ne için işleneceğini belirlemesi gerekli ve yeterli iken, veri kayıt sisteminin kurulup kurulmadığı ya da yönetilip yönetilmediğini belirlenmesinin gerekli olmadığı yönündedir[240].

Son olarak KVKK'nın veri sorumlusu kavramına ilişkin tanımsal bir eksikliğinden bahsetmek gerekecektir. Kanun'un veri sorumlusuna ilişkin tanımında Tüzük'te yer aldığı şekliyle *"...kamu kuruluşu, kurumu veya diğer herhangi bir organ..."* ifadesine yer verilmemiştir. Bu durum uygulamada gerçek kişi ya da adi şirket ile devlet teşkilatı içerisinde yer alan üniversite, kamu hastaneleri ve tüzel kişiliği olan diğer kamu kurum/kuruluşu dışındaki kuruluşlar bakımından sorun teşkil etmektedir[241]. Örneğin, tüzel kişiliği bulunmayan kurum ve kuruluşlardan Bakanlıkların veri sorumluluğu sıfatı tartışılabilir. Ancak böyle bir ihtimalde Bakanlığın tüzel kişiliği olmasa da veri sorumlusu olarak kabul edilmesi gerektiği ifade edilmiştir[242]. Dolayısıyla Kanun'da veri sorumlusu ile ilgili yer verilen tanıma, kanaatimizce Tüzük ile uyumluluk gösterir nitelikte *"...kamu kuruluşu, kurumu veya diğer herhangi bir organ..."* ilavesinin yapılması isabetli olacaktır. Zira üniversitelerin, kamu hastaneleri gibi kamu kurum ve kuruluşlarının da KVKK kapsamında veri sorumlusu sayılacakları tartışmasız olduğundan "organ" ifadesinin KVKK metninde yapılacak değişiklerde yer alması gerektiği kanaatindeyiz.

2. Ortak Veri Sorumlusu (Joint Controllers) Bakımından

GVKT, iki ya da daha fazla veri sorumlusunun bir araya gelerek, kişisel verilerin işlenme amaçlarına ortak bir şekilde karar vermeleri halinde bu veri sorumlularını "ortak veri sorumlusu" olarak 26. maddede tanımlamaktadır. 26. madde ek olarak, veri sahibinin 13 ve 14. maddelerde atıfta bulunulan bilgi sağlama yükümlülükleri ile ilgili Tüzük kapsamındaki yükümlülüklere uygunluğa ilişkin sorumlulukların ortak veri sorumluları arasında nasıl düzenleneceğini ifade etmektedir.

---

[240] **PEKMEZ,** s. 63.
[241] **ÇEKİN**, s. 61-62.; **KÜZECİ** Elif/**KILIÇ** Şebnem, "6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler", Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi (2019) 16 (63), s. 12.
[242] **KÜZECİ /KILIÇ,** s. 12; **ÇEKİN,** s. 62.

Ortak veri sorumluları Tüzüğün 26. maddesi gereği belirledikleri "ortak amaç" dahilinde kişisel verilerin işlenmesine birlikte karar verirler[243].

GVKT'de yer verilen bu kavrama 108 sayılı Sözleşme ile Direktif'te yer verilmemiştir. Bununla birlikte Direktif'in "Tanımlar" başlıklı 2. maddesi, veri işleme faaliyetlerini "tek başına ya da başkalarıyla" belirleyen ifadesi ile ortak veri sorumlusu kavramını kabul etmiştir[244]. Nitekim 29. Madde Çalışma Grubu da ortak veri sorumlularının sorumluluk paylaşımlarının farklı şekillerde olabileceğini ya da farklı veri sorumlularının veri işleme faaliyetlerine katılımının eşit derecede olmayabileceğini ifade etmektedir[245].

Ortak veri sorumlusu kavramından bahsedebilmek için öncelikle yer alması gereken ilk kriter, bir işleme faaliyetinin amaçlarının ve araçlarının belirlenmesine iki veya daha fazla gerçek kişi ya da tüzel kişinin ortak katılımının olmasıdır[246]. Bu ortak katılım halinde iki ya da daha fazla gerçek kişi veya tüzel kişi ortak bir şekilde karar alabileceği gibi sorumluluk paylaşımını aralarında yapacakları bir anlaşma ile farklı şekilde de yapabilmektedir[247]. Yukarıda ifade ettiğimiz üzere böyle bir durumda "ortak veri sorumluları" GVKT m. 26 bakımından kendi sorumluluklarını belirleyen bir düzenleme de yapmakla yükümlüdürler. Ayrıca yapılan bu düzenleme, kişisel verileri işlenen kişilere de bildirilmelidir. Tüzüğün 26. maddesinin 3. fıkrası gereği ortak veri sorumlularının olası bir zarardan dolayı ilgili veri sahibine karşı sorumlulukları müteselsil sorumluluk olacaktır[248]. Keza Tüzüğün "Tazminat ve Sorumluluk" başlıklı 82. maddesinin 4. fıkrası gereği her veri sorumlusunun olası zararlardan sorumlu oldukları ifade etmektedir.

KVKK'da ise ortak veri sorumlusu kavramına değinmemiştir. KVKK m. 3/f.1-ı'ya bakıldığında, Direktif hükümlerinde olduğu gibi "*tek başına ya da diğerleriyle"* ifadesine yer verilmediği görülmektedir. Doktrin, Direktif'teki gibi "tek başına ya da diğerleriyle" ifadesine yer verilmemiş olmasını KVKK'nın ortak veri sorumlusu

---

[243] **KÜZECİ,** s. 365; **29. Madde Çalışma Grubu**, WP 136, s. 22.
[244] **29. Madde Çalışma Grubu**, WP 136, s. 22; **ÇEKİN**, s. 56.
[245] **29. Madde Çalışma Grubu**, WP 136, s. 22.
[246] Kişisel Verilerin Korunması El Kitabı 2018, https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf (Son Erişim Tarihi: 17.04.2021). s. 106; **KÜZECİ,** s. 365; **ÇELİKEL**, s. 87.
[247] **GVKT**, Resital 79.
[248] Bu konudaki açıklamalar için ayrıca bkz. Üçüncü Bölüm, Kişisel Verileri Koruma Kanununun AB Genel Veri Tüzüğü'ne Uyumlaştırması Bakımından Ele Alınması Gereken Kavramlar, IV. Uyumlaştırma Kapsamında Veri Sorumlusuna ve Veri İşleyene Düşecek Ek Görev ve Yükümlülükler, Veri Sorumlusu Ya Da Veri İşleyenin Tazminat Yükümlülüğü s. 136.

kavramını kabul etmediği anlamına çıkmayacağını, zira Kanun'da "tek başına" ifadesinin de şart koşulmadığını ifade etmektedir[249]. Dolayısıyla her ne kadar kanun metninde ortak veri sorumluları kavramına yer verilmemiş olsa da kanaatimizce birden fazla veri sorumlusu bir araya gelerek veri işleme faaliyetlerini gerçekleştirebilecektir.

Birden fazla veri sorumlusunun söz konusu yükümlülüklerini eşit olarak paylaşmaları bir zorunluluk değildir. Bu anlamda tıpkı Tüzük'te olduğu gibi veri sorumluları, veri işleme faaliyetlerine ilişkin olarak aralarında bir iş bölümü sözleşmesi imzalayabilirler. Nitekim Kişisel Verileri Koruma Kurulu'nun 23 Aralık 2021 tarihli ve 2021/1303 sayılı kararında[250] ortak veri sorumlusu kavramına değinilmiş ve veri sorumlularının işleme faaliyetlerine ilişkin bir sözleşme imzalayarak sorumluluklarını müşterek olarak belirleyebilecekleri aksi halde herkesin kusuru oranında sorumlu olacağı ifade edilmiştir. Kurul ayrıca veri sorumlularının sorumluluk ve kusur oranları belirlemede her olayın ayrı ayrı değerlendirilerek işleme faaliyetine konu olan süreçlerin incelenmesi gerektiğini ifade etmiştir. Kurul kararda veri sorumlularının sorumluluklarını müşterek olarak belirleyebileceklerini ifade etmişse de işleme faaliyetlerinden kaynaklı bir hukuka aykırılık ortaya çıktığında zararın ne şekilde tazmin edileceğini ifade etmemiştir. Birden fazla veri sorumlusu, veri güvenliğine ilişkin doğacak zararlar sebebiyle KVKK m. 12/f.2 uyarınca sorumlu olacaklardır. İlgili veri sahiplerinin TBK m. 61-62 gereği genel hükümlere göre tazminat talep hakları saklı olmakla, TBK'nın genel bir kanun olması, KVKK'nın ise özel bir kanun olması ve her iki kanun metninin yürürlüğe girdikleri tarihler düşünüldüğünde veri işleme faaliyetlerinden zarar görenlerin KVKK m. 12/f.2'ye gitmesi gerekecektir. Bununla birlikte Kanun'un 14. maddesinin 3. fıkrası, kişilik hakkı ihlal edilen veri sahiplerinin genel hükümlere göre tazminat talep etme hakkını saklı tutmuştur.

Avrupa Birliği Adalet Divanı'nın Jehovan Todistajat- Tietosuojavaltuutettu[251] davasında, aynı zamanda ortak veri sorumlularına ilişkin bir inceleme de yapılmıştır. Söz konusu olayda dini topluluk ile evlerini ziyaret ettikleri kişilerle ilgili kişisel verileri toplama yetkisine sahip topluluk mensuplarının ortak veri sorumlusu olarak

---

[249] **DÜLGER** Murat Volkan, "GDPR'da Bulunan Ancak KVKK'da Yer Verilmeyen Bir Kavram: Ortak Veri Sorumlusu Kavramı ve Güncel Kararlar Işığında Değerlendirilmesi, 2021, ss. 1-12, s. 1; **PEKMEZ**, s. 68.

[250] Kişisel Verileri Koruma Kurulu'nun 23 Aralık 2021 tarihli ve 2021/1303 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/7288/2021-1303 (Son Erişim Tarihi: 26.12.2022).

[251] Kısaca Jehovan ya da Yehova'nın Şahitleri.

değerlendirilip değerlendirilemeyeceği tartışılmıştır[252]. Nitekim ABAD, topluluk mensuplarının ziyaretlerini gerçekleştirdikleri kişilerle ilgili hangi kişisel verileri toplayıp bu verilerin nasıl ve ne şekilde işleneceği hususlarında söz sahibi olduklarını ifade ederek, bu kişilerin veri işleme faaliyetleri bakımından ortak bir amaç dahilinde hareket ettiklerini ve dolayısıyla ortak veri sorumlusu olarak kabul edilmeleri gerektiğini ifade etmiştir[253].

3.Veri İşleyen Bakımından

KVKK m. 3/f.1-ğ'de veri işleyen, veri sorumlusu adına ve ondan aldığı emir ve talimatlarla işleme faaliyetini gerçekleştiren gerçek ve/veya tüzel kişi olarak tanımlanmıştır. GVKT m. 4/f.8'e göre de veri sorumlusu adına veri işleme faaliyetlerini gerçekleştiren gerçek ve/veya tüzel kişiliğe sahip kamu kurum ya da kuruluşları ile diğer organları ifade eden kişi veri işleyen olarak ifade edilmiştir. Veri işleyen, veri sorumlusundan talimatları doğrultusunda onun adına işleme faaliyetlerini gerçekleştirirken işlemenin daha ziyade teknik kısımları ile ilgilenen gerçek kişi, tüzel kişi ya da tüzel kişiliğe bağlı organı temsil eden kişi olarak ifade edilir. Buna göre veri işleyen sıfatını haiz olmanın iki temel koşulu olduğu ifade edilebilir. Bu koşullardan ilki, kişisel verileri veri sorumlusu adına işlemesi, ikinci koşul ise veri sorumlusundan ayrı bir gerçek kişiliği, tüzel kişiliği ya da tüzel kişiliğe bağlı bir organı temsil eden kişi bulunmasıdır[254].

Gerçek bir kişi ya da tüzel kişiliğin işleme faaliyetleri bakımından hem veri sorumlusu hem de veri işleyen olarak değerlendirilmesi mümkündür. Örneğin bir reklam ajansı kendi çalışanlarına karşı tuttuğu kişisel veriler bakımından veri sorumlusu sıfatını haiz iken, müşterilerine ilişkin tuttuğu kişisel veriler bakımından veri işleyen olarak değerlendirilecektir[255]. Bununla birlikte veri sorumlusu, işleme faaliyetlerini kendi çalışanlarından seçtiği bir veri işleyenle yürütebileceği gibi, dışarıdan aldığı bir hizmet ile sözleşme ilişkisine dayalı olarak da gerçekleştirebilir[256].

---

[252] Jehovan Todistajat Kararı, para. 64-65.
[253] Jehovan Todistajat Kararı, para. 63.
[254] **29. Madde Çalışma Grubu**, WP 169, s. 24; **Kişisel Verileri Koruma Kurumu,** "KVKK Terimler Sözlüğü", s. 9.
[255] **Kişisel Verileri Koruma Kurumu**, Veri Sorumlusu ve Veri İşleyen, s. 2; **ÇEKİN**, s. 65; **KÜZECİ**, s. 366.
[256] **ÇEKİN**, s. 63-64; **BAŞARA TURAN** Gamze, "Kişisel Veri İşleme Sözleşmesi", Uyuşmazlık Mahkemesi Dergisi- Yıl 8, Sayı 16, Aralık 2020, ss. 57-90, s. 67; **TAŞTAN**, s. 69; **MEMİŞ** Tekin,

Bir diğer ifade ile veri işleyen bizzat veri sorumlusunun bir çalışanı ya da veri sorumlusu tüzel kişiliğe bağlı bir birimi temsil eden bir kişi de olabilir[257]. Örneğin bir şirketin dışarıdan aldığı hizmet ile şirket müşterilerine çağrı merkezi hizmeti vermesi durumunda çağrı hizmeti veren şirket işleme faaliyetleri bakımından veri işleyen olarak değerlendirilirken, veri sorumlusu kendi bünyesi altında çağrı hizmetleri sunmak adına ayrı bir departman da kurabilir[258]. Her ne şekilde olursa olsun veri işleyen, kendi menfaatleri doğrultusunda değil, veri sorumlusunun menfaatleri doğrultusunda ve onun emir ve talimatlarına uygun olarak hareket etmelidir[259]. Bu noktada Kurul'un veri işleyen tanımındaki farklılığa değinmek gerekir. Kişisel Verilerin Korunması Kurumu, veri işleyenin, veri sorumlusunun organizasyon sahası dışındaki gerçek ya da tüzel kişi olduğunu ifade etmiştir[260]. Ancak veri sorumlusu bünyesinde yer alan çalışanlar da veri işleyen adına işleme faaliyetlerini yürütebilmektedir. Dolayısıyla Kurum'un veri işleyen ile ilgili olarak, veri sorumlusunun organizasyon sahası dışında yer alan gerçek ya da tüzel kişi ifadesine katılmıyoruz. Zira veri sorumlularının dışarıdan hizmet almaktansa kendi tüzel kişilikleri altında uzman departmanlar kurması gerek vergilendirme gerekse maliyetler açısından da kazançlı bir yöntem olmaktadır[261]. Üstelik veri sorumlusunun organizasyon sahası dışından belirleyeceği veri işleyen seçimi her koşulda avantajlı olmayabilir. Bu ihtimalde örneğin denetleme mekanizması güçleşecek, dışarıdan hizmet satın almak suretiyle belirlenen veri işleyenin birden fazla veri sorumlusunun işleme faaliyetini yürütmesinde veri ihlalleri artabilecek, küçük çaplı şirketlerin maaliyet yükleri artacak, veri sorumlusunun işleme faaliyetleri ile ilgili kendi bünyesinde uzman yetiştirmesi ya da istihdam etmesi engel oluşturacaktır[262].

"Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 6, 2017, s. 9-23, s. 14. https://www.jurix.com.tr/article/12604 (Son Erişim Tarihi:29.10.2022).

[257] **TAŞTAN**, s. 69; **BAŞARA**, s. 77; **MEMİŞ** Tekin, "Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 6, 2017, s. 9-23, s. 14. https://www.jurix.com.tr/article/12604 (Son Erişim Tarihi:29.10.2022).

[258] **Kişisel Verileri Koruma Kurumu,** 100 Soruda Kişisel Verilerin Korunması Kanunu, s. 31 https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf (Son Erişim Tarihi: 03.04.2021).

[259] **ÇEKİN**, s. 65; **PEKMEZ**, s .65-68; **KÜZECİ**, s. 366.

[260] **Kişisel Verileri Koruma Kurumu**, Veri Sorumlusu ve Veri İşleyen, s. 1.

[261] **YILMAZ** Sabire Sinem, "KVKK Uyum Sorunsalı: "Veri Sorumlusu ve Veri İşleyen Kavramlarını İyi Anlamak", 14/05/2020, Lexpera Blog, https://blog.lexpera.com.tr/kvkk-uyum-sorunsali-veri-sorumlusu-ve-veri-isleyen-kavramlarini-iyi-anlamak/ (Son Erişim Tarihi: 26.12.2022)

[262] **YILMAZ,** "KVKK Uyum Sorunsalı: "Veri Sorumlusu ve Veri İşleyen Kavramlarını İyi Anlamak", 14/05/2020, Lexpera Blog.

Veri işleyen, kişisel verilerin işlenmesi ile ilgili daha çok işin teknik yönü ile ilgilendiğinden, veri işlemenin gizliliği ve güvenliği anlamında önemli bir rol oynamaktadır. GVKT'nin "Tazminat Hakkı ve Sorumluluk" başlıklı 82. maddesinde, veri işleyenin yükümlülüklerini ihlal etmesi halinde doğrudan sorumlu tutulabileceği düzenlenmiştir. KVKK'da veri işleyen ile ilgili açıklamalara m. 3/f.1-ğ dışında, veri sorumlusunun kişisel verilerin işlenmesinde, veri güvenliğine ilişkin tedbirlerin alınması noktasında veri işleyenle birlikte müştereken sorumluluğunu ifade ettiği m. 12/f.2 ve veri sorumluları ile veri işleyenlerin, elde ettikleri kişisel verileri KVKK'ya aykırı olarak üçüncü kişilere açıklayamayacağı ve işleme amacı dışında kullanamayacaklarını ifade eden m. 12/f.4 hükümlerinde değinilmiştir[263]. Ancak yine de KVKK bakımından veri işleyen ile ilgili açıklamaların son derece yetersiz olduğu anlaşılmaktadır. Nitekim, gerek mehaz düzenleme Direktif m. 2/f'de gerek GVKT m. 4/f.10'da üçüncü kişinin tanımına yer verilerek bu kişilerin veri işleyen ile arasındaki farklara yer verilmiştir[264]. Oysa KVKK metninde üçüncü kişi tanımına yer verilmediği gibi üçüncü kişiye ilişkin ifadeler de çok muğlak ve sınırlıdır[265]. Üstelik hem Direktif m. 17/f.2 hem de GVKT m. 28/f.1 ile özel bir düzenlemeye yer verilerek, Direktif m. 17/f.3 ve GVKT m. 28/f.3 ile veri sorumluları ile veri işleyenlerin aralarında yapılacak sözleşme[266] sorumluluğuna ilişkin açıklamalara ve sözleşmenin taşıması gereken asgari unsurlara yer verilmiştir[267].

95/46/EC sayılı Direktif'te veri işleyenin veri sorumlusu ile ortak sorumluluğuna ilişkin hükümler yer almaktadır. Bununla birlikte Direktif ile karşılaştırıldığında GVKT'nin getirdiği yeni düzenlemeler ile veri işleyenin işleme faaliyetlerindeki aktif rolünün önemi daha iyi çizilmiştir. Gerek Direktif gerek Tüzük açısından bu hükümlere ayrıntılı olarak yer verilmesinin amacının kişisel verilerin korunma seviyesini artırmak olduğu düşünüldüğünde, KVKK'da yukarıda ifade edilen kavramlardan hiçbirine değinilmemiş olması kanaatimizce önemli bir eksikliktir.

---

[263] **ÇEKİN**, s. 62; **BAŞARA TURAN**, s. 67.
[264] **ÇEKİN**, s. 63.
[265] **KVKK**, m. 10/f.1 11/f.1-ç, f, m. 16/f.2, m. 28.
[266] GVKT'de ayrıntılı olarak ele alınan ve veri sorumlusu ile veri işleyen arasında yapılan bu sözleşme "Kişisel Veri İşleme Sözleşmesi" olarak ifade edilmektedir. Her ne kadar KVKK kapsamında veri işleme sözleşmesine değinilmemiş ise de Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunmasına İlişkin Uygulama Rehberi"'nde veri işleyeni açıklarken veri işleme sözleşmesine değinmiştir. **BAŞARA,** s. 58. Veri işleme sözleşmesine ilişkin ayrıntılar için Bkz. İkinci Bölüm, Kişisel Verileri Koruma Kanununun AB Genel Veri Tüzüğü'ne Uyumlaştırması Bakımından Ele Alınması Gereken Kavramlar ve İlkeler, IV. Uyumlaştırma Kapsamında Veri Sorumlusuna ve Veri İşleyene Düşecek Ek Görev ve Yükümlülükler, D. Veri İşleme Kayıtları ile İlgili Ek Yükümlülükler, 1. Veri İşleme Sözleşmesi, s. 108.
[267] **ÇEKİN**, s. 63; **BAŞARA TURAN,** s.58; **PEKMEZ**, s. 65.

4. Alıcı (Recipient) ve Üçüncü Kişi (Third Party) Bakımından

GVKT m. 4/f.9'da alıcı, üçüncü bir kişi olup olmadığı fark etmeksizin, kişisel verilerin açıklandığı gerçek kişiler, tüzel kişiler, kamu kurum ya da kuruluşları ile bunlar dışında kalan diğer kuruluşları ifade etmektedir. "Alıcı", veri sorumlusu ya da veri işleyenin kişisel verilerini açıkladığı kişiler ile ilgili bu kişilere bilgi verme yükümlülüğünden dolayı önem arz eden bir kavramdır. O halde üçüncü şahısları kapsasın ya da kapsamasın, kişisel verilerin açıklandığı herkes alıcı olarak değerlendirilebilir[268]. Örneğin bir veri sorumlusunun kişisel verileri bir başka kuruluşa, veri işleyene ya da diğer üçüncü bir tarafa göndermesi halinde, verilerin aktarıldığı kişi alıcı olarak değerlendirilecektir.

Veri sorumlusu ya da veri işleyen, kişisel verilerini açıkladığı kişiler hakkında veri sahiplerine bilgi verme yükümlülüğüne sahip olduğundan "Alıcı", önemli bir kavramdır[269].Bununla birlikte veri sorumlusunun kişisel verilerin düzeltilmesi, silinmesi gibi konular ile ilgili ilgili kişiyi bilgilendirme yükümlülüğü çerçevesinde, işlediği kişisel verilerin olası tüm alıcılarını belirleyebilmesi gerekir[270]. Örneğin müşterilerinden gelen talepler üzerine her şey dahil paketler ile seyahat düzenleyen bir seyahat acentesi, müşterileri ile ilgili hizmetleri yerine getirebilmek adına havayollarına, otellere, tur organizasyonlarına müşterilerinin verilerini iletir. Bu kişiler arasında kural olarak bir veri sorumlusu ve veri işleyen ilişkisi olmadığı için havayolu şirketleri, oteller ve tur organizasyonları alıcı olarak kabul edilmelidir[271]. Ancak havayolu şirketleri, oteller ya da tur organizasyonu şirketleri kendi hizmetleri dahilinde ve kendi müşterilerine karşı gerçekleştirdikleri işleme faaliyetlerinde veri sorumlusu konumundadır.

GVKT m. 4/f.10'da üçüncü kişi, bir veri sorumlusu, veri işleyen ya da veri sahibinin yetkisi altında ve kişisel verileri işleme yetkisi bulunan kişiler dışındaki tüm gerçek kişileri, tüzel kişileri ve kamu kurum/kuruluş ya da organları ifade etmektedir.

---

[268] **Avrupa Veri Koruma Kurulu (EDPB),** Guidelines 07/2020 on consent under Regulation 2016/679 (Rıza Rehberi) Version 1.1, Adopted on 4 May 2020, s. 29. 93.https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (Son Erişim Tarihi: 12.10.2021); **LAMBERT** Paul, Understanding the New European Data Protection Rules, Taylor & Francis, 2017, s. 126; **ÇELİKEL**, s. 99.

[269] **29. Madde Çalışma Grubu**, WP 169**,** s. 31.

[270] **29. Madde Çalışma Grubu**, WP 169**,** s. 31.

[271] **Avrupa Veri Koruma Kurulu (EDPB),** Rıza Rehberi, s. 29.

29. Madde Çalışma Grubu'nun 169 No'lu çalışma belgesine göre üçüncü kişi, kişisel verilerin işlenmesinde herhangi bir yetkisi ya da meşru bir amacı olmayan herhangi bir kişi olarak yorumlanmaktadır[272]. Başka bir ifadeyle üçüncü kişi, başlangıçta kişisel verileri işlememesi gereken bir kişidir. Çalışma Grubuna göre örneğin, bir şirketin çalışanı olarak başkalarına ait kişisel verilere yetkisiz olarak erişim sağlayan kişi, kişisel verilerin işlenmesinin yasallığı bakımından ortaya çıkacak tüm sonuçlarla birlikte işverenine karşı "üçüncü kişi" olarak değerlendirilmelidir[273]. Bu kavram genel olarak kişisel verilerin veri sorumlularının yetkilendirdiği veri işleyenler dışında herhangi bir diğer tarafça yetkisiz olarak işlenebileceği durumları sınırlamak ve belirli yükümlülükler oluşturmak amacıyla kullanır[274].

Üçüncü kişi ile ilgili olarak yapılan değerlendirmeler Tüzük açısından da benzerdir. Avrupa Veri Koruma Kurulu'nun Temmuz 2020 tarihli Rehberinde, kişisel verileri işleme yetkisi olmayan ve işverenin talimatlarının dışında kişisel verilere erişim sağlayan kişinin üçüncü kişi olarak düşünülmesi gerektiği ifade edilmiştir[275]. Buna göre çalışan, kişisel verileri işverenin amaçladığından farklı şekilde ve kendi amaçları doğrultusunda işlediği ölçüde tıpkı veri sorumlusu gibi kabul edilerek, kişisel verileri işlemesi bakımından ortaya çıkacak tüm sonuçları ve yükümlülükleri üstelenecektir.

Üçüncü kişi her zaman, veri sorumlusunun, veri işleyenin ya da bu kişilerin herhangi bir çalışanı vasfına sahip olmayabilir. Nitekim, ofislerini temizletmek üzere bir temizlik hizmeti veren şirketle sözleşme imzalayan A şirketi varsayımında, ofisi temizleyen temizlik personelleri, etrafta dolanırken zaman zaman kişisel verilerle karşılaşsalar dahi görevlerini bu verilere erişmeden sürdürmelidir[276]. Dolayısıyla bu personellerin kişisel verilere erişmeleri ya da bu verileri işlemeleri sözleşmesel olarak yasaktır. Kaldı ki bu personeller, A şirketi tarafından istihdam edilmemişlerdir. Bu

---

[272] **29. Madde Çalışma Grubu**, WP 169**,** s. 31; **ÇELİKEL**, s. 99; **BUSSCHE/VOIGHT**, s. 208; **WAEM** Heidi/**Van ESSEN** Jacqueline/ **WELLENS** Vincent, "Can the GDPR's Main Players still fulfil their Roles Effectively in an Era Characterised by Developments such as the Blockchain and the Internet of Things?", https://www.e-nautadutilh.com/56/2412/landing-pages/part-2---gdpr.asp?sid=c5019f94-05ff-4f2c-a894- a5ba75ac9208, (Son Erişim Tarihi: 05.11.2022).

[273] **29. Madde Çalışma Grubu**, WP 136**,** s. 31.

[274] **ÇELİKEL**, s. 95; **29. Madde Çalışma Grubu**, WP 136**,** s. 31; Ayrıca bkz. **BUSSCHE/VOIGHT**, s. 69.

[275] **Avrupa Veri Koruma Kurulu (EDPB),** Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Veri Sorumlusu ve Veri İşleyen Rehberi), Version 1.0 Adopted on 02 September 2020, s. 27; **BUSSCHE/VOIGHT**, s. 80. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (Son Erişim Tarihi: 18.05.2021).

[276] **Avrupa Veri Koruma Kurulu (EDPB),** Veri Sorumlusu ve Veri İşleyen Rehberi, s. 29.

nedenle temizlik hizmeti şirketi ve çalışanları üçüncü kişi olarak değerlendirilmelidir. Bunun yanında veri sorumlusu A şirketi de KVKK'nın 12. maddesi gereği temizlik hizmeti personellerinin çalıştıkları sürece, kişisel verilere erişimlerini önlemeye yönelik gerekli güvenlik tedbirlerini aldığından emin olmalı ve şirket içinde kişisel verilerle karşılaşma durumlarına karşın gerekirse gizlilik konusunda bir anlaşma sağlamalıdır[277].

Kişisel verilerin korunması bakımından "üçüncü kişi" ile "alıcı" kavramları arasındaki temel fark, bu kişilerin veri sorumluları ile aralarındaki ilişkiden ve dolayısıyla veri sorumlusu tarafından tutulan kişisel verilere erişim yetkileri bakımından kaynaklanmaktadır[278]. Bir diğer ifade ile "üçüncü kişi" ile "alıcı arasındaki ayrım, işlenen kişisel verilerin yasal olarak açıklanması hususu ile yakından ilişkilidir[279]. Örneğin bir veri sorumlusunun çalışanları ya da veri işleyenler, kişisel verilerin işlenmesi aşamalarında yer alıyorlarsa, başkaca herhangi bir yasal gereklilik olmaksızın bu kişiler, kişisel verilerin alıcısı olarak kabul edilirler. Buna rağmen bir veri sorumlusu ya da veri işleyici tarafından yetkilendirilmeyen ya da yasal bir gerekçeye dayanmaksızın kişisel verileri elde eden bir kişi üçüncü kişi olabilmektedir. Bir diğer ifade ile veri sorumlusunun çalışanı, kişisel verileri veri sorumlusu adına ve onun talimatları ile kullandığından "üçüncü kişi" olarak değil, "alıcı" olarak değerlendirilecektir[280].

KVKK "alıcı" kavramına yer vermemiştir. Bununla birlikte KVKK m. 16/f.3-ç, "kişisel verilerin aktarılabileceği alıcı veya alıcı grupları" şeklindeki ifadeye yer vermiştir. Veri Sorumluları Sicili Hakkında Yönetmelik'in 4. maddesinin a bendinde ise alıcı grubu, veri sorumluları tarafından verilerin aktarıldığı gerçek ya da tüzel kişi kategorisi şeklinde ifade edilmektedir. Benzer şekilde Kanun'da "üçüncü kişi" tanımına yer verilmemişse de bazı madde hükümlerinde dolaylı olarak üçüncü kişi ifadesi yer almaktadır[281]. Nitekim Kanun'un "Haklar ve Yükümlülükler" başlıklı

---

[277] **Avrupa Veri Koruma Kurulu (EDPB),** Veri Sorumlusu ve Veri İşleyen Rehberi, s. 28; **ÇELİKEL,** s. 94; **DEVELİOĞLU**, s. 44-44.
[278] Kişisel Verilerin Korunması El Kitabı, s. 110.
[279]Kişisel Verilerin Korunması El Kitabı, s. 110; **WAEM** Heidi/**Van ESSEN** Jacqueline/ **WELLENS** Vincent, "Can the GDPR's Main Players still fulfil their Roles Effectively in an Era Characterised by Developments such as the Blockchain and the Internet of Things?", https://www.e-nautadutilh.com/56/2412/landing-pages/part-2---gdpr.asp?sid=c5019f94-05ff-4f2c-a894- a5ba75ac9208, (Son Erişim Tarihi: 05.11.2022).
[280] Kişisel Verilerin Korunması El Kitabı, s. 111.
[281] **ÇELİKEL,** s. 94; **ÇELİK** Işıl, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması, On

üçüncü bölümünde "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10. maddesinde "yetkilendirdiği kişi" ifadesine yer verilmiş ancak bu kişinin kim olduğu, hukuki statüsünün ne şekilde yer aldığı ya da hangi şartlar altında yetkilendirileceğine ilişkin açıklamalara yer verilmemiştir. Dolayısıyla veri sorumlusu tarafından yetkilendirilen bu kişi veya kişilerin, işlenen kişisel veriler bakımından hangi sıfatla sorumlu olacakları muallaktır. Kanaatimizce KVKK m. 10'da yer alan "yetkilendirdiği kişi" ifadesi ile alıcıya atıf yapılmaktadır. Zira kişisel verilerin elde edilmesi sırasında veri sorumlusunun yetkilendirdiği kişi yasal amaçlar dahilinde kişisel verilere ulaşma ulaşmaktadır. O halde Tüzük hükümlerinde yer alan bu kavramların hukukumuz açısından da ayrımları net olarak ortaya konarak KVKK kapsamına alınması gereklidir. Böylelikle veri sorumlusu ve veri işleyen dışında kişisel verilere ulaşan kişiler bakımından herhangi bir veri ihlalinde sorumlulukların ne şekilde doğacağına ilişkin daha net ifadeler KVKK bakımından da yerini alabilir.

C. KVKK'DA YER ALMAYAN PSEUDONYMISATION (TAKMA ADLANDIRMA) KAVRAMI

Pseudonymization kavramı, KVKK'da yer verilmeyen bir kavram olup, Kanun m. 3/f.1-b'de yer alan "anonim hale getirme" tanımı[282] ile ayrımının yapılması bakımından son derece önemlidir. Kelime anlamı olarak Pseudonymization, takma adlandırma, takma ad konulmuş veri olarak ifade edilebilmektedir. Aynı zamanda, "bulanıklaştırma" olarak da ifade edilen pseudonymization[283] kavramı, *"...Bir kişinin kimliğinin, o kişi ile ilgili veriler üzerinden izi sürülemez hale getirilmesi amacıyla, algoritmalar kullanarak kişiyi belirli kılan verilerin şifreli verilerle değiştirildiği teknik bir yöntem..."* olarak ifade edilmektedir[284].

Anonimleştirme ve takma adlandırma kavramları, GVKT'nin yürürlüğe girmesinden bu yana çokça tartışılan iki kavram olmuştur. Her ne kadar Tüzük

---

İki Levha Yayıncılık, Haziran 2022, s. 15; Ayrıca ilgili maddeler için bkz. **KVKK**, m. 10/f.1 11/f.1-ç, f, m. 16/f.2, m. 28.

[282] **KVKK**, m. 3/f.1-b bendi, "…Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini…" demektedir.

[283] Pseudonymization kavramı ile açıklamalarımızın devamında GVKT kapsamında "pseudonymization" teriminin Türkçe bir karşılığı yer almadığından bundan böyle "takma adlandırma" ifadesi kullanılacaktır.

[284] **AKINCI** Ayşe Nur, Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti (Uzmanlık Tezi). T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Ankara, 2019, s. xv.

kapsamında anonimleştirme tanımına yer verilmemiş ise de Tüzük resitallerinde takma adlandırma ile anonimleştirme arasındaki ayrımın çizildiği açıklamalar yer almaktadır. GVKT m. 4/f.5'te takma adlandırma, kişisel verilerin belirlenebilir gerçek bir kişiyle ilişkilendirilmemesini sağlamak üzere kişiye ilişkin bir takım ek bilgilerin ayrı muhafaza edilmesini ve uygun güvenlik önlemlerine tabi olma şartıyla, bu verilerin söz konusu ek bilgiler kullanılmaksızın o gerçek kişi ile ilişkilendirilemeyecek yöntemlerle işlenmesi şeklinde ifade edilmiştir. Bununla birlikte takma ad verilerek yaratılan kişisel verilerin Tüzük kapsamında kişisel veri olarak kabul edileceği 26 No'lu resitalde ifade edilmiştir[285]. GVKT 26 No'lu resital, gerçek bir kişi ile ilgisi olmayan ve onu belirlenebilir kılmaya yetmeyen ya da anonim hale gelen verilere uygulanmaması gerektiğini ifade etmiştir[286]. O halde takma adlandırmanın, bir kişiyi belirlenebilir kılan kişisel verilerinin çeşitli parçalara ayrılarak, bu parçalara belirli kodlar ya da şifreler verilmesiyle oluştuğunu ve bu parçalı verilerin bir araya getirilmeden gerçek bir kişiyi belirli ya da belirlenebilir kılmasının mümkün olmadığı işlenme olduğu ifade edebilir[287]. Örneğin, bir psikiyatri kliniğinde tedavi gören kişi ile ilgili tutulan verilerin özel bir kodlama yöntemiyle parçalara ayrılarak kaydedilmesi durumunda "takma adlandırma" yönteminin kullanıldığı ifade edilecektir. Hasta ile ilgili tutulan kişisel veriler ya da özel nitelikli kişisel veriler, hastane ya da hastanenin yetkilendirdiği kimse tarafından belirli kodlama/şifreleme yöntemleri kullanılarak sisteme kaydedilecek, bu hastanın verilerine erişilmek istenilmesi durumunda da bu kod ya da şifreler kullanılarak hastaya ait bilgiler görüntülenecektir. Dolayısıyla, kişiye ait kişisel veriler hastane tarafından tutulmakta ise de bu veriler herkesçe ulaşılabilir ve direkt olarak herhangi bir gerçek kişiyi belirli kılmaya yetecek ölçüde olmayacaktır[288].

Bu noktada takma adlandırma ile anonimleştirme kavramları arasındaki ayrımın altının biraz daha çizilmesi gerekmektedir. Zira anonimleştirme ve takma adlandırma kişisel verilerin ait olduğu gerçek kişilerin kimliklerinin gizlenmesinin iki

---

[285] **GVKT,** Resital 26.
[286] **GVKT,** Resital 26; **AKINCI**, "Tüzüğün Getirdiği Yenilikler", s. 30; **ÇELİKEL**, s. 74.
[287] **DEVELİOĞLU,** s. 36; **SAKA** Rıza/**ÇAĞLAYAN** Ramazan/**KOCA** Mahmut, Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası, Seçkin Yayıncılık, Güncellenmiş ve Genişletilmiş 2. Baskı, Ankara, 2022, s. 213.
[288] **UYSAL** Emin Hamdi," Kişisel verilerin korunmasına ilişkin mevzuatımızdaki kavram belirsizliği ve pseudonymization kavramı", Ocak, 2020, s. 9 https://www.academia.edu/41692959/Ki%C5%9Fisel_verilerin_korunmas%C4%B1na_ili%C5%9Fkin_mevzuat%C4%B1m%C4%B1zdaki_kavram_belirsizli%C4%9Fi_ve_pseudonymisation_kavram%C4%B1(Son Erişim Tarihi: 20.06.2022); Gizlilik-Koruma Depolama ve Tıbbi Erişim Takma Adlandırma ve Şifreleme ile Veriler, 7 Eylül 2011, https://www.xylem-technologies.com/2011/09/privacy-preserving-storage-and-access-of-medical-data-through-pseudonymization-and-encryption/ (Son Erişim Tarihi: 20.06.2022).

farklı yolu olup, her birinin özünde kendi amacı bulunmaktadır[289]. Kişisel verilerin takma adlandırma yöntemi ile oluşturulmasında kullanılan işlemler tersine çevrilebilir ve yetkili kullanıcıların korunan verileri daha sonra görüntülemesine ve yönetmesine izin verebilir. Bu yöntem daha çok kişilerin kimlik numaraları, sosyal güvenlik numaraları gibi verilerinin yetkisiz kullanıcılar için daha az erişilebilir hale getirilmesine yardımcı olan bir gizlilik yöntemidir[290].

Buna karşın anonimleştirme yöntemi kullanıldıktan sonra, kişisel verilerin artık gerçek bir kişiyi belirlenebilir kılması mümkün değildir[291]. Bu veriler artık herhangi bir kişiye atfedilemeyeceği gibi bir kişiyi belirli ya da belirlenebilir kılmaya yetecek ölçüde de değildir[292]. Bununla birlikte hem anonimleştirme hem de takma adlandırma, GVKT'nin kişisel veri ihlallerini en aza indirmek ve bu verilerin kötüye kullanımlarını engellemek adına kullanılacak yöntemlerdendir. Ancak belirtmek gerekir ki, takma adlandırma yöntemi ile kişisel verilerin doğru bir şekilde gizlenememesi durumunda, kişisel verileri işleyenler açısından ağır yaptırımlar ortaya çıkacaktır. Üstelik yeterli gizlilik önemlerinin alınmadığı durumlarda bu kişisel verilerin kötü aktörlerin eline geçmesi de ihtimaller dahilinde olacaktır.

Yukarıda ifade edildiği üzere Direktif'i referans alan KVKK, takma adlandırma tanımına yer vermemiştir. Tüzük'ten ayrı olarak KVKK'nın 3. maddesi ile anonim hale getirme kavramına yer verilmişse de bu husus Kanun tasarı metninde eleştiri almıştır[293]. Her ne kadar kişisel verilerin anonim hale getirildikten sonra geri

---

[289] **WILLIAMSON** Clyde, "They're Not Just Long Words: Anonymization and Pseudonymization Protect Data-driven Business", March 29, 2021, https://www.protegrity.com/protegrity-blog/theyre-not-just-long-words-anonymization-and-pseudonymization-protect-data-driven-business (Son Erişim Tarihi: 06.07.2021).

[290] **WILLIAMSON**, s. 66.

[291] **AKINCI**, "Tüzüğün Getirdiği Yenilikler", s. 30; **ÇELİKEL**, s. 73; **WES** Matt, "Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization", 25 Nisan 2017, https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and pseudonymization/ (Son Erişim Tarihi:20.06.2022).

[292] **29. Madde Çalışma Grubu,** WP 216, s. 23. Ancak 29. Madde Çalışma grubu, veri anonimleştirme yönteminin uygulanmasının gerçekte zor olduğunu, zira ilgili kişiye ait kişisel verilerin geri alınmasının artık mümkün olmadığı durumlarda dahi diğer bilgi kaynaklarının yardımıyla (kamuya açık olsun ya da olmasın) o kişi ile ilgili bilgi toplamanın mümkün olacağını ifade etmektedir. Dolayısıyla veri sorumlusunun yükümlülükleri kapsamında doğru gerçekleştirilmeyen bir anonimleştirme halinde kişisel verilerin kötü niyetli bir saldırgan tarafından ele geçirilmeleri mümkün hale gelecek, veri sahipleri de hedef konuma geleceklerdir. Bu sıkıntıların önüne geçilmesinin en temel şartının veri sorumluları ve veri işleyenlerin doğru gizlilik adımlarıyla atmaları gerektiği ifade edilmiştir.

[293] 3. maddeye konulan muhalefet şerhinde özellikle gelişen teknoloji ile kişisel verileri anonim hale getirmenin neredeyse imkansız olduğu, verilerin anonim hale getirilmesi için alınan önlemlerin artmasına rağmen bu önlemleri aşacak teknolojilerin de hızla geliştiğinden bahsedilmiştir. İlave olarak anonim hale getirmenin işlevselliğini korumak adına, anonimleştirmenin koşullarını belirleyen ilave bir madde konulması gerektiği ifade edilmiştir. TBMM Komisyon Raporu, s. 81-82.

döndürülmesi gelişen teknoloji ile imkânsız görünmemekteyse de aksi de söz konusu olabilmektedir. Bu şekilde Tüzük bakımından anonim hale gelen verilerin korumadan faydalanamayacağı açıktır. Aynı durum KVKK için de geçerlidir. Ancak KVKK'da takma adlandırma tanımına yer verilmemiş olması, takma adlandırma yöntemi ile muhafaza edilen kişisel verilerin korunmayacağı anlamına gelmemektedir. Nitekim Kişisel Verileri Koruma Kurumu'nun Rehberinde [294] bu husus ifade edilmiştir. Rehberde takma adlandırmanın, verileri anonimleştirerek kişisel veri olma niteliğini sonlandırmadığını, kişisel verilerin anonim hale gelmediği sebeple kişisel veri niteliğini haiz olarak KVKK'ya tabi olacağı ifade edilmiştir [295] . Kanaatimizce KVKK'da takma adlandırma yöntemine ilişkin bir düzenlemenin yer alarak, bu kavramın anonim hale getirmeden ayrımı ortaya konularak Kanun maddelerinde yer alması gereklidir[296].

II. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI BAKIMINDAN FARKLILIKLAR

A. BİR HUKUKA UYGUNLUK SEBEBİ OLARAK RIZA KAVRAMI

Hukuka aykırılık teşkil eden fiiller, kanun tarafından belirlenen özel durumlarda, kanunun gerektirdiği şartları sağlayarak hukuka uygun zemine oturabilirler. Kanunun, hukuka aykırı bir fiili hukuka uygun hale getiren, bir diğer ifade ile fiili hukuka aykırı olmaktan çıkaran bir unsuru da "rıza" kavramıdır[297]. İlgili kişi tarafından verisinin işlenmesi için rızanın verilmesiyle aslında "kişisel verileri üzerinde kendi kaderini tayin etme hakkı" kullanılmaktadır[298]. Elbette kişinin verdiği rızanın geçerli olabilmesinin belirli şartları vardır. Bu şartlar; rızayı verenin iradesini

[294] **Kişisel Verileri Koruma Kurumu**, 6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar-2 (KVKK hakkında Doğru Bilinen Yanlışlar), https://www.kvkk.gov.tr/Icerik/7151/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Dogru-Bilinen-Yanlislar-2 (Son Erişim Tarihi: 21.06.2022).
[295] **Kişisel Verileri Koruma Kurumu**, (KVKK hakkında Doğru Bilinen Yanlışlar), s. 29.
[296] Nitekim KVKK tasarısının "Tasarıda Yer Almayan Eksik Hususlar" başlığında GVKT Tasarısında yer alan takma adlandırma kavramına değinilmiştir. Bu yöntemde veri sorumluları kişisel verilerin tümüyle ilişkilendirilmesinin önüne geçmek adına gerekli tüm teknik ve idari önlemleri alacakları ifade edilmiş ve takma adlandırma tanımının madde 3'e alınması gerektiği belirtilmiştir.
[297] **HELVACI** Serap**,** Gerçek Kişiler, Legal Yayıncılık, 9. Bası, Eylül 2021, s. 149-150.
[298] **AVCI BRAUN** Cihan, "Kişisel Verilerin İşlenmesinde Rıza", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 15, ss. 13- 33, s. 18.

açıkça yansıtması, rızanın bilinçli ve özgür bir irade beyanına dayalı verilmiş olması ve rızanın hukuka aykırı olmaması halidir[299].

Kişisel verilerin işlenmesi kural olarak yasak olan eylemlerdendir. Ancak bu husus hukukumuzda, Anayasa'nın 20. maddesinin 3. fıkrasının 3. cümlesi ile, Kanun'da öngörülmedikçe ve kişilerin açık rıza göstermedikleri sürece kişisel verilerinin işlenemeyeceğini ifade eder[300]. Dolayısıyla kural olarak kişisel verilerin işlenmesi yasak olmakla gerek Anayasa'nın ilgili hükmü gerek KVKK'da yer verilen istisnai hükümler ile kişisel verilerin işlenmesi hukuka uygun hale gelmektedir. GVKT'nin 6. maddesi de kişisel verilerin işlenme şartlarının hukuka uygunluğu konusunda hükümler içermektedir. GVKT'nin 7. maddesi ile hukuka uygunluk şartlarından biri olan rıza kavramının hangi unsurlara sahip olması gerektiği ifade edilmiştir.

Son olarak, aşağıda alt başlıklar halinde inceleyeceğimiz rıza kavramı ile ilgili olarak, KVKK'da yer verilen açık rıza dışında Tüzük hükümlerinde hem rıza kavramına hem de açık rıza kavramına ayrı ayrı değinildiğini ifade edelim. Bu ayrım ile ilgili değerlendirmeleri ve KVKK'da sadece açık rıza kavramına yer verilmiş olmasının olumsuz yönlerine ilerleyen başlıklarda değineceğiz.

1. Tüzük Kapsamında Rıza Kavramı ve Unsurları

Bilindiği üzere 95/46/EC sayılı Direktif m. 2/h ilgili kişinin rızasını, veri öznesinin iradesini yansıtan, özgür bir şekilde verilmiş ve aydınlatılmış olarak alınan rıza olarak tanımlamaktaydı. Direktif'in 7. maddesinin a fıkrası ile de ilgili veri sahibinin rızasının açık, kesin ve net bir biçimde iradesini yansıtma şartını aramaktaydı. GVKT, rıza kavramını mülga 95/46/EC sayılı Direktifle benzer olacak şekilde tanımlamıştır. Rıza kavramı GVKT'nin 4. maddesinin 11. fıkrasında veri öznesinin özgür olarak verilmiş, bilgilendirmeye dayalı ve belirsizlik (muğlak olmayan) içermeyen şekilde kişisel verilerin işlenmesini kabul ettiğine yönelik irade açıklanması olarak tanımlanmıştır. Tüzük m. 7'de geçerli bir rızanın taşıması gereken

---

[299] **OĞUZMAN/SELİÇİ/ÖZDEMİR**, Kişiler Hukuku, s. 103; **HELVACI**, s.149-150; **AKİPEK/AKINTÜRK/ATEŞ,** s. 364.
[300] **ÇEKİN**, s. 82.

şartlar belirlenmiştir. Bununla birlikte rıza kavramına ilişkin açıklamalar genel olarak GVKT'nin 4 ile 9. maddeleri arasındadır[301].

29. Madde Çalışma Grubunun Tüzük kapsamında rızaya ilişkin hazırladığı rehberde[302], geçerli bir rızanın 4 şarta bağlandığı ifade edilmiştir. Bu şartlar; rızanın serbestçe/özgür olarak verilmiş olması, spesifik (açık ve net) olması, bilinçli olması (bilgilendirmeye dayanması) ve veri sahibinin açık bir beyanı ile kendisine ait kişisel verilerin işlenmesine onay verdiğini göstermesi şeklindedir[303].

Buna göre rıza, açık ve net bir irade beyanını göstermelidir. Örneğin internet üzerinde kişilere daha önceden işaretlenmiş (opt-out[304]) seçenekli kutucuklar sunmada kişilerin rızası geçerli değildir[305]. Zira Tüzük ilgili veri sahibi kişinin rızasının aktif bir beyanını aramaktadır[306]. Dolayısıyla internet sitelerinde yer alan bir onay kutusundaki işaretin kaldırılmaması (opt-out) şeklinde alınan rızada kişinin aktif bir irade beyanının varlığından söz etmek mümkün olmayacaktır[307]. GVKT'nin 32 No.lu resitalinde de ifade edildiği şekliyle opt-out yönteminin gerek genel nitelikli gerek özel nitelikli kişisel verilerin işlenmesinde alınan rıza bakımından geçerli olmayacağı yer almaktadır[308]. Bununla birlikte rıza kavramı bireylere gerçek bir seçim ve kontrol sağlamalı ve baskı unsuru barındırmamalıdır[309]. Bir diğer ifade rızanın tereddüde yer

---

[301] Bu konuda ayrıntılı bilgi için ayrıca; **DÜLGER**, "Tüzük Bağlamında Kişisel Verilerin Korunması", s.111 vd.

[302] **29. Madde Çalışma Grubu,** WP 259, ss.3-30.

[303] **29. Madde Çalışma Grubu,** WP 259, s. 5-7; **DÜLGER** Murat Volkan, "AB Genel Veri Koruma Tüzüğü ve KVKK'da Rıza Kavramı", ss. 1-9, s. 3. https://dulger.av.tr/wpcontent/uploads/2019/05/AB_Genel_Veri_Koruma_Tuzugu_GDPR_ve_KVKK.pdf(Son Erişim Tarihi: 11.10.2021).

[304] Kişisel verilerin korunmasında sıklıkla adı geçen "Opt-in" ve "Opt-out" terimlerini kısaca izah etmek gerekirse; "Opt-in" ifadesi internet üzerinde bireylerin kendileriyle hakkında bilgi elde edilmesine bu bilgilerin paylaşılmasına açık bir biçimde izin vermesi yöntemidir. Uygulama genel olarak Avrupa Birliği ülkelerinde geçerlidir. Daha sıklıkla Amerika'da uygulanan bir yöntem olan "Opt-out" seçeneğinde ise, ilgili siteye gire kullanıcıların kendileri ile ilgili kişisel bilgilerini paylaşmayı kabul ettiği varsayılmaktadır. Kendileri ile ilgili kişisel bilgi paylaşmak istemeyen kullanıcıların bu hususu açık bir şekilde ve net olarak belirtmeleri gerekir. **JOHNSON** Eric J./**BELLMAN** Steven/**LOHSE** Gerald L., "Defaults, Framing and Privacy: Why Opting In-Opting Out?" Received October 25, 2000; Revised and Accepted October 3, 2001, Marketing Letters, s. 13:1, 5–15, 2002.

[305] **AVCI BRAUN**, s. 28; **KÜZECİ**, s. 273; **BAŞALP**, s. 40; **ÖZER DENİZ**, s. 111; **SELEK** Ozan**,** "Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 21, Sayı: 2, 2019, ss. 911-951, s. 933.

[306] 32. paragrafta ilgili veri sahibi kişinin otomatik olarak işaretli bir butona onay vermesi bir hareketsizlik sayılacağından burada açık rızanın varlığından söz edilemeyeceği ifade edilmiştir. Verilen rızanın geçerli olması ancak ilgili veri sahibi kişinin bu işlemeye onay verdiğini gösteren bir tıklama ile (opt-in) ile mümkün olabilmektedir. Dolayısıyla Tüzük, ilgili veri sahibi kişinin hareketsiz kalmasını/susmasını açık rıza kapsamında kabul etmemektedir. **AVCI BRAUN**, s. 28; **SELEK**, s. 933.

[307] **AVCI BRAUN**, s. 28; **ÖZER DENİZ**, s. 111.

[308] **ÇEKİN**, s. 84; **BIETTI** Elettra, "Consent as a Free Pass: Platform Power and the Limits of the Informational Turn." Pace Law Review, Vol. 40, No. 1, 2019, ss. 310-398, s. 340; **SELEK,** s. 933.

[309] **29. Madde Çalışma Grubu,** WP 259, s. 6.

bırakmayacak açıklıkta olması gerekir[310]. Rızanın unsurları ile ilgili açıklamalara ilerleyen bölümlerde ayrıntılı olarak yer verilecektir.

GVKT'nin 7. maddesinin 4. fıkrası, rızanın serbestçe verilip verilmediğini değerlendirirken, veri işlemenin bir sözleşmenin ifası için gerekli olup olmadığına azami özen gösterilmesi gerektiği ifade etmiştir. Ancak önemle vurgulamak gerekir ki, alınan rıza kural olarak geçerli olsa bile, kişisel veri işlemeyi hukuka uygun kılmada yeterli olmamaktadır. Bu anlamda veri sorumlularının veri güvenliği ilkesi gereği ilave koruyucu ve önleyici tedbirler de alması gerekmektedir.

a. Tüzük Kapsamında Rızanın Unsurları

Tüzük uyarınca, alınan rızanın geçerli olabilmesi için bazı unsurların varlığı şarttır. Bu unsurlar; rızanın serbestçe/özgür olarak verilmiş olması, spesifik (açık ve net[311]) olması, bilinçli olması (bilgilendirmeye dayanması), ve veri sahibinin açık bir beyanı ile kendisine ait kişisel verilerin işlenmesine onay verdiğini göstermesi şeklinde ifade edilmektedir. Burada belirtmek gerekir ki rızanın, ilgili veri sahibinden işleme faaliyetlerinden önce alınması zorunludur. Veri işleme faaliyetlerinden sonra onay alınması şeklindeki rıza beyanları geçerli kabul edilmemektedir[312]. Ek olarak veri işlemenin ilgili veri sahibinin rızasına dayandığı durumlarda, veri sorumlusu veri sahibinin işleme faaliyetine rıza gösterdiğini ispat edebilmelidir[313]. Bir diğer ifade ile veri sahibinden geçerli bir rıza alındığını ispatlamak veri sorumlusundadır.

Rızanın serbest bir şekilde (özgür olarak) verilmesi, ilgili kişinin işleme faaliyetlerine göstereceği rıza öncesi bir baskı hissetmemesini ifade etmektedir[314]. Dolayısıyla ilgili veri öznesinin bir seçim hakkı yoksa ya da rıza vermeye kendisini mecbur hissediyor ve rıza göstermemesi durumunda bazı olumsuz sonuçlara katlanması gerekecekse bu halde verilen rızanın geçerli olmayacağı ifade edilebilir[315].

---

[310] **AVCI BRAUN**, s. 29.
[311] Tüzük bakımından alınacak rızanın hukuka uygun olarak değerlendirilebilmesi için şüpheye yer bırakmayacak nitelikte kesinlik taşıması gerekmektedir.
[312] **GVKT**, Resital 40; **AVCI BRAUN,** s. 18 vd.
[313] **GVKT**, Resital 42.
[314] **AVCI BRAUN**, s. 21.
[315] **AVCI BRAUN**, s. 21; **29. Madde Çalışma Grubu,** WP 259, s. 5; Ayrıca rızanın tanımına ilişkin **29. Madde Çalışma Grubu**, WP 187, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (Son Erişim Tarihi:10.07.2022).

Rızanın spesifik olması, ilgili veri öznesinin hem "serbest" bir şekilde rıza vermesi hem de "bilgilendirilmiş" olması ile ilişkilidir[316].

Rızanın diğer bir unsuru olan "bilgilendirmeye dayalı olma" hususu da ilgili veri öznesinin rıza vereceği konu ile ilgili bilinçli olmasını ifade eder. Diğer bir ifade ile veri sorumlusu, ilgili veri öznesinin hangi konuda rıza vereceği ile ilgili gerekli aydınlatmayı yapmalı, bu aydınlatmayı yaparken açık ve net olmalıdır[317]. Son olarak rızanın, ilgili veri öznesinin açık ve onay veren bir beyana dayanması gerekmektedir. Dolayısıyla beyan ya da onay verme işlemi muğlak bir ifade barındırmamalıdır. Daha önce söz ettiğimiz üzere kişinin, kişisel verilerinin toplanmasına ve paylaşılmasına etkin bir biçimde izin vermediği, bir diğer ifade ile "Opt-out" seçeneği ile verilen rıza geçerli olmayacaktır.

b. Tüzük Kapsamında Rıza ve Açık Rıza

AB hukuku uyarınca ister genel ister özel nitelikteki her verinin yasal olarak işlenebilmesi için ilgili veri sahibi kişinin rızası gereklidir. Genel nitelikli kişisel verilerin işlenmesinde rızanın varlığı yeterlidir. Tüzük bakımından özel nitelikli kişisel verilerin işlenmesinde ise aranan rıza açık olmak zorundadır. Zira Tüzük ciddi veri koruma risklerinin ortaya çıktığı, bu nedenle kişisel veriler üzerinde bireysel kontrolün gerekli olduğu durumlarda açık rıza alınması gerekli kılmaktadır[318]. Tüzük kapsamında açık rıza, özel nitelikli kişisel verilerin işlenmesine ilişkin 9. maddede, bir yeterlilik kararının olmadığı ve gerekli güvencelerin bulunmaması nedeniyle üçüncü ülkelere aktarımı konusunda 49. maddede ve profil oluşturma dahil otomatik karar alma mekanizmaları ile ilgili 22. madde kapsamında aranmaktadır[319].

Tüzük, rıza kavramını hem rıza (consent) hem de açık rıza (explicit consent) olarak ayrı ayrı ele alırken Kanunumuz yalnızca açık rıza kavramına yer vermiştir. Rızanın "açık rıza" olarak değerlendirilmesi, Avrupa Veri Koruma Kurulu'nun 2020 tarihli rehberinde, ilgili veri sahibinin rızayı ifade biçimi şeklinde ifade edilmiştir[320]. Rızanın açık rıza olarak değerlendirilmesinde yazılı bir beyan şeklinde olması ispat

---

[316] **KÜZECİ,** s. 265-269;
[317] **DÜLGER,** "Rıza", s. 5.
[318] **Avrupa Veri Koruma Kurulu (EDPB),** Rıza Rehberi, s.20; Ayrıca bkz. **29. Madde Çalışma Grubu,** WP 259, s. 18.
[319] **ÇEKİN**, s. 84.
[320] **Avrupa Veri Koruma Kurulu (EDPB),** Rıza Rehberi, s. 20

açısından da önem taşımaktadır[321]. Ancak rızanın GVKT'nin 7. maddesinin 2. fıkrasına göre yazılı bir beyan olarak verilmesi halinde, bu rıza beyanın açık, net bir şekilde anlaşılır ve kolay ulaşılabilir olması gerekmektedir[322]. Elbette açık rıza almanın tek yolu, yazılı olarak imzalı bir beyan değildir. Bu anlamda 32 No'lu resitalde ifade edildiği üzere rıza, yazılı olarak alınabileceği gibi elektronik ortamda ya da sözlü olarak da alınabilir[323]. Veri sorumlusunun ileride olası şüpheleri ortadan kaldırması ve açık rızanın geçerlilik koşullarının sağlandığını kanıtlaması için açık rızanın yazılı verilmesi önem arz edecektir[324]. Sözlü beyan, geçerli bir rıza elde etmede kabul görse de veri sorumluları açısından bu beyanın alındığının ispatı zor olacaktır. Zira Tüzüğün 7. maddesinin 1. fıkrasına göre rızanın varlığı veri sorumlusu tarafından ispatlanması gereken bir husustur.

2. KVKK Kapsamında Rıza Kavramı ve Unsurları

Tüzük, rıza kavramını hem rıza (consent) hem de açık rıza (explicit consent) olarak ayrı ayrı ele alırken Kanunumuz yalnızca açık rıza kavramına yer vermektedir. Tüzük hükümlerinde olduğu gibi kanunumuz bakımından da açık rızanın geçerli olabilmesi için belirli unsurları barındırması gerekmektedir. Bu unsurlar üç unsur olarak kabul görmektedir. Buna göre açık rıza, spesifik bir konuya ilişkin olmalı, rıza aydınlatmaya/bilgi vermeye dayanmalı ve rıza özgür bir irade beyanı ile açıklanmış

---

[321] **Avrupa Veri Koruma Kurulu (EDPB),** Rıza Rehberi, s.20

[322] **DÜLGER**, "Tüzük Bağlamında Kişisel Verilerin Korunması", s. 114.

[323] **GVKT**, Resital 32.

[324] Dijital bir ortamda ilgili veri sahibinin elektronik bir form doldurarak ya da veri sahibinin imzasını taşıyan bir belgeyi tarayarak çevrimiçi ortamda karşıya yüklemesi ya da elektronik imza kullanması durumunda açık rızaya örnek teşkil edebilir. Bir doktorun hastası ile ilgili ikinci bir doktorun görüşünü alması durumunda, hastanın tıbbi kayıtlarının ikinci doktor tarafından elde edileceğine ilişkin elektronik imza ile açık rızasını istemesi durumu böyledir. Açık rıza bir butona/düğmeye basarak onay verme ya da telefon görüşmesinde açık onay alınması şeklinde de gerçekleşebilir. Yine veri sorumlusunun veri sahibinin tıbbi kayıtlarının belirli bir amaç dahilinde kullanılacağını bildirdiği bir e-postaya onay istediğini bildirmesi halinde "Kabul Ediyorum" şeklinde bir e-posta alması bu şekildedir. Kabul yanıtı gönderildikten sonra ilgili veri sahibi bir doğrulama bağlantısı ve doğrulama kodu içeren bir SMS mesajı alır. Ancak rıza yalnızca tek bir fare tıklaması ya da bir butona onay verme şeklinde elektronik yollarla alındığında ilgili veri sahibi bu rızayı aynı kolaylıkla geri alabilmelidir. Ayrıca veri sahibi rızasını çekerken herhangi bir zarara uğramamalıdır. Örneğin bir müzik festivaline çevrimiçi ortamda bilet almak isteyen ilgili veri sahibi onaylama işlemini "Evet" ya da "Hayır" şeklinde verebilir. Veri sahibi müşterilere verdikleri onayı geri çekme hakkına sahip olduklarını ve çalışma günlerinde mesai saatleri içerisinde ücretsiz çağrı merkezi ile iletişime geçebileceklerini bildirir. Ancak bu örneğin Tüzüğün 7. maddesinin 3. fıkrasına uygun olmadığı ifade edilmektedir. Zira verilen rızanın geri alınması mesai saatleri içerisinde bir telefon görüşmesi yapılmasını gerektirir ve veri sahibi rızanın veriliş şeklindeki gibi tek bir tıklamadan daha külfetli hale gelir. **Avrupa Veri Koruma Kurulu (EDPB),** Rıza Rehberi, s. 20-24.

olmalıdır[325]. Ancak Direktif'i referans alan Kanunumuz bakımından rızanın 4 unsur olarak kabul görmesi gerektiği ve "tereddüde yer bırakmayacak açıklıkta" ifadesinin de son unsur olarak yer alması gerektiğine inanıyoruz. Bu konu ile ilgili açıklamalara "KVKK Kapsamında Rıza ve Açık Rıza" başlığını ele alırken yer vereceğiz.

a. KVKK Kapsamında Rızanın Unsurları

KVKK m. 3/f.1-a'da açık rıza, spesifik bir konuya ilişkin, aydınlatmaya dayalı ve özgür bir biçimde sunulan rıza olarak ifade edilmiştir. Kanunda yer alan rızanın üç unsuru bulunmaktadır. Buna göre rıza ilk olarak belirli bir konuya ilişkin olmalı (spesifik), ilgili veri sahibine yönelik olarak bilgilendirmeye dayanmalı ve nihayetinde rıza ilgili kişinin özgür iradesiyle açıklanmış olmalıdır. Bununla birlikte açık rıza mutlaka kişisel verilerin işlenmesinden önce açıklanmış olmalıdır. Bir diğer ifade ile kişisel verilerin işlenmesinden sonra alınan rızanın veri işleme faaliyetini meşru kılması mümkün değildir[326].

KVKK bakımından rızanın ilk unsuru olan belirli bir konuya ilişkin olmadır. Bu unsur, rızanın hangi konu ile ilgili ve hangi amaçla işleneceğinin belirli olması durumunu ifade eder.

Rızanın bilgilendirmeye dayanma unsuru ise ilgili veri sahibinin bilgilendirilmiş olmasını, kendisi ile ilgili işlenecek kişisel verileri hakkında aydınlatılmış olmasını ifade eder. Bu unsur KVKK'nın m. 10 ve m. 11 hükümleri dikkate alınarak değerlendirilmelidir. Buna göre veri sorumluları veri sahibi kişilere karşı ilgili madde hükümlerini de içerir şekilde aydınlatma yükümlülüklerini yerine getirmelidir. Nitekim veri sorumlusunun ilgili madde hükümlerinde yer alan bilgilere internet web sitesinde yer verdiği gerekçeyle bilgilendirme yapmış sayılacağının kabulü mümkün değildir[327]. Dolayısıyla bu noktada veri sorumlusunun veri sahibi kişiyi aydınlatma yükümlülüğünü yerine getirdiğinden söz edilemeyecektir. Keza benzer bir durum kişisel verilerin üçüncü bir kişiye aktarımında da söz konusudur.

---

[325] **Kişisel Verileri Koruma Kurumu,** Açık Rıza, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf (Son Erişim Tarihi: 08.07.2021) s. 5; **KÜZECİ**, s. 265-268; **AVCI BRAUN**, s. 18 vd.; **ERARSLAN** Sevgi, Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, On İki Levha Yayınları, Aralık, 2020, s. 143-145.

[326] **ÇEKİN**, s. 88; **YÜCEDAĞ** Nafiye, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 75 (2), 2017, ss. 765-789, s. 773; **AVCI BRAUN**, s. 18 vd.

[327] **AVCI BRAUN**, s. 25-26.

Veri sorumlusu veri sahibi kişiye ait kişisel verileri üçüncü kişiye aktarırken veri sahibini bu konuda bilgilendirmelidir[328]. Veri sahibine ait kişisel verilerin aktarılacağı üçüncü kişinin kim olduğu belirtilmeksizin verilerin aktarılacağına ilişkin yapılan aydınlatma ve alınan rıza da geçerli kabul edilmemektedir[329].

KVKK bakımından rızanın son unsuru, rızanın özgür iradeye dayalı olarak verilmesidir. Özgür bir iradenin varlığı, ilgili kişinin seçim serbestisinde olmasını ifade eder[330]. Örneğin işçi- işveren iş ilişkisi kapsamında işçinin kişisel verilerinin işlenmesinde özgür iradenin varlığından söz edebilmek için işçinin kendini herhangi bir baskı altında hissetmemesi gerekmektedir. Kişisel verilerin işlenmesine rıza göstermeme ya da verdiği rızayı geri alması işçi adına olumsuz bir sonuç yaratmadığı ölçüde özgür iradenin varlığından söz edilebilecektir[331]. Çalışma Grubunun 259 No'lu Çalışma Raporunda[332] film çekmek üzere işverenin ofislerinin bir kısmını kullanacak olan bir film ekibinin olduğu örneğinde, işveren işçilere videonun arka planında görünebileceklerini gerekçe göstererek rızalarına başvurur. Bununla birlikte filmde yüzlerinin görünmesini istemeyenler için herhangi bir yaptırım olmamakta hatta bunun yerine çekim süresi boyunca bu kişiler binanın başka yerlerinde kendilerine verilen eşdeğer masalarda çalışabilmektedirler. Bu örnekte olduğu gibi işçiler üzerinde bir baskı unsuru olmadığı, verilen rızanın da özgür iradeye dayandığına şüphe duyulmamaktadır[333].

---

[328] Kişisel Verileri Koruma Kurulu'nun 2 Ağustos 2018 tarihli karar özetinde, bir şirketler topluluğu içerisinde yer alan birden fazla veri sorumlusunun şirketler arasındaki veri aktarımının üçüncü kişiye aktarım olarak değerlendirildiği, şirketler topluluğu içinde her bir veri sorumlusunun ayrı bir tüzel kişiliği olduğundan bahisle KVKK'nın 8. maddesinin esas alınması gerektiği ifade edilmiştir. Kurul, iş başvurusunda bulunan bir adayın açık rızası olmaksızın kişisel verilerinin bir şirketler topluluğu içindeki veri sorumluları arasında aynı veri tabanını kullanarak paylaşılmasının KVKK'nın 12. maddesinin 1. fıkrasına da ayrılık teşkil ettiğinden bahisle idari para cezası uygulanmasına karar vermiştir. Kişisel Verileri Koruma Kurulu'nun 2 Ağustos 2018 Tarihli Karar Özeti, https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi (Son Erişim Tarihi: 31.12.2022).

[329] Bu konuda daha fazla açıklama için **AVCI BRAUN**, s. 25-26.

[330] **AVCI BRAUN**, s. 21.

[331] **YÜCEDAĞ**, s. 775; **AVCI BRAUN**, s. 21.

[332] **29. Madde Çalışma Grubu,** WP 259, s. 7.

[333] **ÇEKİN,** s. 94; **29. Madde Çalışma Grubu,** WP 259, s. 7.

b. KVKK Kapsamında Rıza ve Açık Rıza

Anayasa m. 20/f.3'te ilgili kişinin rızayla kişisel verilerin işlenebilecek olması istisnasında rızanın niteliği "açık rıza" şeklinde tanımlanmıştır. KVKK bakımından sadece açık rıza kavramına yer verildiğinden, hem genel nitelikli kişisel verilerin işlenmesinde hem de özel nitelikli kişisel verilerin işlenmesinde açık rıza bir hukuka uygunluk sebebi olarak kabul edilmektedir[334].

KVKK'nın açık rıza ile ilgili "*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* ifadesiyle yalnızca açık rıza tanımına yer vermiş olmasını, Tüzük bakımından değerlendiren bazı yazarlar, ilgili kişiden alınması gereken rıza şartlarının kuvvetlendirildiği yönünde yorumda bulunmuşlardır[335]. Bu anlamda Tüzük bakımından açık rıza kavramına ayrı olarak yer verilmediği ifade edilerek, aslında KVKK ile yapılan mukayesede *"bilgilendirmeye dayalı rıza"* alınması ifadesinden bu rızanın da açık rıza olduğu ifade edilmiştir[336]. Diğer yandan farklı bir görüş, KVKK'da yer verilen "açık rıza" tanımı ile aslında açık rızanın değil, mülga 95/46/EC sayılı Direktif hükümlerindeki açıklamalarıyla örtüşen "rıza" kavramının tanımının yapıldığını ifade etmiştir[337]. Zira KVKK'nın gerekçesinde açık rızanın tanımı yapılırken Direktif referans alınmıştır[338]. Referans alınan Direktif'in 7. maddesinin a bendi ise açık rızanın tanımını yaparken rızanın *"tereddüde yer bırakmayacak açıklıkta"* (unambiguously) olması gerektiğini belirtmektedir. Kanun'un gerekçesinde yer verilen *"tereddüde yer bırakmayacak açıklıkta"* ifadesi ise Kanun'un açık rıza tanımında yer almamaktadır. Dolayısıyla kanun koyucunun gerçek arzusunun açık rızanın değil rızanın tanımını yapmak istediği ifade edilmiştir[339]. Bir diğer ifade ile ingilizce olarak "unambiguously" şeklinde ifade edilen hususun aslında KVKK'nın 5. maddesindeki genel nitelikli verilerin işlenmesinde aranan açık rıza kavramını karşıladığı belirtilmektedir[340]. Kanaatimizce bu görüş oldukça isabetlidir. Kanun'un açık rızaya ilişkin madde gerekçesi, Direktif'te yer alan açık rıza tanımı ve nihayetinde gerekçeden farklı olarak KVKK'da yer alan açık rıza tanımı dikkate alındığında bu

---

[334] **Kişisel Verileri Koruma Kurumu,** Açık Rıza, s. 2; **ÇEKİN**, s. 83.
[335] **Avrupa Veri Koruma Kurulu (EDPB),** Rıza Rehberi s. 20; **DÜLGER**, "Tüzük Bağlamında Kişisel Verilerin Korunması", s. 114; **DÜLGER** Murat Volkan, Kişisel Verilerin Korunması Hukuku, 1. Bası, İstanbul, 2019, s. 67.
[336] **DÜLGER**, s. 67.
[337] **AVCI BRAUN**, s. 19.
[338] **AVCI BRAUN**, s. 19; TBMM Komisyon Raporu, s. 7.
[339] **AVCI BRAUN**, s. 19.
[340] **AVCI BRAUN**, s. 19.

görüşe katılıyoruz[341]. KVKK bakımından rıza ile açık rıza ayrımının net olarak yapılmadığı ya da Direktif'in 7. maddesinin a bendinde olduğu gibi *"tereddüde yer bırakmayacak açıklıkta"* ifadesinin yer almadığı, tüm bunların karşılığı olarak ise yalnızca "açık rıza" kavramının kullanıldığı açıktır[342]. Doktrinde savunulan bu görüş, KVKK kapsamında genel ve özel nitelikli kişisel verilerin işlenmesi bakımından aranan rıza türünde bir ayrım yapılmamış ve açık rıza olarak ifade edilmekteyse de özel nitelikli kişisel verilerin işlenmesinde yer alan açık rıza kavramının Direktif'in 8. maddesinin 2. fıkrasının a bendinde yer alan "explicit consent" terimini karşıladığını belirtmiştir[343]. Dolayısıyla Direktif'in 7. maddesinin a bendinde yer alan rızanın KVKK'nın 5. maddesinde yer alan genel nitelikli kişisel verilerin işlenmesinde aranan açık rızayı karşıladığını, Direktif'in 8. maddesinin 2. fıkrasının a bendinde yer alan açık rızanın ise KVKK bakımından da özel bir koruma gerektiren 6. maddesinde yer alan özel nitelikli kişisel veriler için aranılan açık rızayı karşıladığını ifade etmektedir[344].

Ancak her halükârda KVKK bakımından benimsenen açık rıza kavramın Tüzük ile uyumlu olmadığı ve aslında büyük bir kavram karmaşasına yol açtığı ifade edilebilir. Zira hukukumuzda yer alan açık rıza kavramı ne Direktif hükümlerine yer alan rıza kavramını ne de Tüzük hükümlerinde yer alan rıza kavramını tam karşılar nitelikte değildir[345]. Üstelik bu kavram karmaşası yalnızca rıza ya da rızanın unsurları ile de sınırlı değildir. KVKK'nın var olan kavramlara yeni anlamlar yükleyerek bir kavram karmaşası oluştuğu doktrinde eleştirilmektedir[346]. Nitekim kanundaki boşlukların yalnızca mevzuat hükümlerimizle değil AB Hukukuna ait bilimsel görüş ve içtihatlarla doldurulması gerektiğinin altı çizilmiştir[347]. Bizim de katıldığımız görüşe göre, KVKK kapsamında her türlü kişisel verilerin işlenme faaliyetlerine açık rızanın uygulanması uygulamada sorunlara sebebiyet verdiği gibi "rıza" kavramı ile kıyaslandığında pratik de değildir[348]. Diğer bir ifade ile kişisel verilerin işlenmesi noktasında AB hukukunda kabul edilen şekline uyumlu olarak, genel nitelikli kişisel verilerin işlenmesi bakımından zımni verilen rızaların kabulü gereklidir.

---

[341] TBMM Komisyon Raporu, s. 8-9.
[342] **ÇEKİN**, s. 84; **AVCI BRAUN**, s. 26-27.
[343] **AVCI BRAUN**, s. 26-27.
[344] **AVCI BRAUN**, s. 30-31.
[345] **DÜLGER** "Rıza", s. 2.
[346] **AVCI BRAUN**, s. 19.
[347] **AVCI BRAUN**, s. 19.
[348] **AVCI BRAUN**, s. 31; **ÇEKİN**, s. 84.

3. Rızanın Geri Alınması

GVKT'nin 7. maddesinin 3. fıkrası, kişisel verileri işlenen ilgili kişilerin rızalarını her an geri alabileceklerini ve rızalarını geri almalarının da rızanın verilmesi kadar basit nitelikte olması gerektiğini ifade etmektedir. Ayrıca ilgili kişi kişisel verilerinin işlenme faaliyetleri ile ilgili olarak vereceği rıza beyanını geri alabileceği ile ilgili rıza beyanını sunmadan önce veri sorumlusu tarafından bilgilendirilecektir. GVKT'nin 7. maddesinin 3. fıkrası devamında, rızanın geri alınmasından önce rızaya dayalı olarak yapılan kişisel verilerin işlenme faaliyetlerinin hukuka uygunluğunun etkilenmeyeceğini de ifade etmiştir. KVKK'ya bakıldığında ise verilen rızanın geri alınması hususunda bir madde hükmü tesis edilmediği görülmektedir. Bununla birlikte "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik Taslağı"'nın[349] m. 5/f.2-d bendinde, veri işleme faaliyetlerinin yalnızca açık rıza şartına istinaden gerçekleştiği durumlarda, veri sahibinin rızasını geri çekmesinin kişisel veri işleme şartlarını ortadan kaldırdığı kabul edilmektedir. Ancak 28 Ekim 2017 tarih ve 30224 sayılı Resmi Gazete'de yayımlanarak 1 Ocak 2018'de yürürlüğe giren ve 15 maddeden oluşan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"'te taslak metninde yer verilen hükme açıkça yer verilmemiştir. Her ne kadar KVKK'da ve Yönetmelik'te açık rızanın geri alınabileceği hükmü yer almasa da veri sahibinin rızasını geri alma imkânı elbette mevcut olacaktır[350]. Zira rıza kavramı kişiye sıkı sıkıya bağlı bir hak olarak, ilgili kişinin kişisel verileri üzerinde kendi kaderini tayin etme hakkını ilgilendirdiğinden, verilen rıza her zaman geri alınabilecektir[351]. KVKK çerçevesinde verilen rızanın geri alınması, açık rıza beyanının veriliş şekline uygun düşecek ölçüde ve kolaylıkta olmalıdır[352].

---

[349] https://kisiselveri.com/kisisel-verilerin-silinmesi-yok-edilmesi-veya-anonim-hale-getirilmesi-hakkinda-yonetmelik-taslagi (Son Erişim Tarihi: 22.11.2022).

[350] **AVCI BRAUN**, s. 16; **ÇELİKEL** Serdar, "Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR'la Karşılaştırmalı Olarak İncelenmesi", Uyuşmazlık Mahkemesi Dergisi- Yıl 9, Sayı 17, Haziran 2021- ss. 161-190, s. 176-177.

[351] **AVCI BRAUN**, s. 17; **ŞİMŞEK**, s. 107; **SEROZAN**, s. 470; **HELVACI**, s. 153.

[352] **ÇEKİN**, s. 98; **POLATER** Salih, "Kişisel verilerin reklam amaçlı işlenmesinde hukuka uygunluk sebepleri", Kişisel Verileri Koruma Dergisi. 1(1), 1-20, s. 7.

4. Özel Nitelikli Kişisel Verilerin İşlenmesinde Rıza

GVKT m. 9/f.1'de kişilerin etnik kökenler, ırksal özellikleri, dini inançları, felsefi görüşleri, siyasi düşünceleri, sendika üyeliklerine ilişkin bilgileri, genetik ve biyometrik verileri ve sağlık verileri ile cinsel yaşamlarına ilişkin veriler özel nitelikli veriler olarak kabul edilmekte ve kural olarak bu verilerin işlenmesi yasak kabul edilmektedir. Bununla birlikte aynı maddenin 2. fıkrası ile istisnai olarak ilgili kişinin rıza göstermesi halinde belirtilen özel nitelikli kişisel verilerin işlenebileceği ifade edilmektedir. Bu anlamda özel nitelikli kişisel verilerin işlenmesi bakımından da sunulacak açık rıza beyanı, veri işlenme faaliyetlerini hukuka uygun kılar.

KVKK'ya bakıldığında, daha önce ifade ettiğimiz üzere rızanın türüne göre bir ayrım yapılmadığı dolayısıyla hem özel hem de genel nitelikli kişisel verilerin işlenmesinde açık rıza kavramına yer verildiği görülmektedir[353]. Özel nitelikli kişisel veriler KVKK'nın 6. maddesinde tanımlanmıştır. Buna göre m. 6/f.1'de kişilerin etnik kökenleri ya da ırksal özellikleri ile dini inançları, felsefi düşünceleri, siyasi görüşleri, sendika üyeliklerine ilişkin verileri, genetik ve biyometrik verileri de dahil sağlık verileri ile cinsel yaşamlarına ilişkin verileri, kılık ve kıyafetlerine ilişkin veriler ile ceza mahkumiyetleri ya da haklarında uygulanan güvenlik tedbirlerine ilişkin verileri özel nitelikte veriler olarak kabul edilmektedir. Görüleceği üzere özel nitelikli kişisel veriler sınırlı sayıda sayılmıştır[354]. Her ne kadar genel özel nitelikli kişisel veriler bakımından da açık rızanın şart olduğu ifade edilmişse de özel nitelikli kişisel verilerin daha sıkı bir korumaya ihtiyaç duyduklarının altı çizilmektedir[355]. Nitekim KVKK'nın gerekçesinde belirtildiği üzere özel nitelikte sayılan kişisel veriler üçüncü kişiler tarafından öğrenildiklerinde ilgili veri sahibinin ayrımcılığa uğramasına, mağdur olmasına sebep oldukları için hassas veri kabul edilirler[356]. Dolayısıyla KVKK m. 6/f.3'e göre, ilgili kişinin cinsel yaşamına ve sağlığına ilişkin verileri dışındaki kişisel verilerinin ancak kanunlarda öngörülen hallerde; teşhis, tedavi ve bakım gibi hizmetlerin yürütülmesi gibi sebeplerle, belirli kişiler veya yetkili kurum ve kuruluşlar

---

[353] **ERARSLAN**, s. 152.
[354] **KAYA** Cemil, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 69, Sayı 1-2, 2011, ss. 317-334, s. 319; **AVCI BRAUN**, s. 31.
[355] **AVCI BRAUN**, s. 29.
[356] **AVCI BRAUN**, s. 30.

aracılığı ile işlenebilmesinin mümkün olduğu ifade edilmiştir[357]. Ancak tekrardan altını çizmekte fayda vardır ki özel nitelikli kişisel verilerin hangi kategoriye ait olduğu fark etmeksizin bu tür verilerin ancak yeterli ve gerekli tedbirler alınmak suretiyle işlenebileceğini ifade edelim. Doktrinde ifade edilen görüşe katılarak, genel ve özel nitelikli kişisel verilerin bakımından herhangi bir ayrım öngörmeyen Kanunu'nun, her türlü kişisel verilerin işlenmesinde "açık rıza" aranmasını şart koşan hükümlerinin ve Kişisel Verileri Koruma Kurumu'nun açıklamalarının[358] tek başına yeterli olmadığına ve her olay nezdinde değerlendirilme yapılması gerektiğini ve bu konudaki uyuşmazlığa bakmaya yetkili merciin mahkemeler olduğu görüşüne katılıyoruz[359]. Bu konuda ihtisas mahkemelerinin kurulması ve bu tür davalara uzmanlaşmış mahkemelerin bakmasının yararlı olacağı kanaatindeyiz.

5. Çocukların Kişisel Verilerinin İşlenmesinde Rıza

Çocukların kişisel verilerinin korunması ilk kez mülga 95/46/EC sayılı Direktif'in yerini alan Tüzük'te yer bulmuştur[360]. Diğer bir ifade ile 95/46/EC sayılı Direktif çocukların kişisel verilerinin işlenmesine ilişkin herhangi bir hükme yer vermemiştir. Buna karşın o tarihte ABD hukukunda "Çocukların Çevrimiçi Platformlarda Mahremiyetinin Korunmasına İlişkin Kanun" olan 1998 tarihli (Children's Online Privacy Protection Act) (COPPA) yürürlükte bulunmaktaydı. "Çocukların Çevrimiçi Platformlarda Mahremiyetinin Korunmasına İlişkin Kanun" ile temel olarak amaçlanan, çocukların kişisel verilerinin elde edilmesi, bu verilerin kullanımı ya da aktarımına ilişkin çocukların menfaatlerine zarar verecek her türlü eylemi yasaklamaktı[361]. Bu anlamda GVKT'nin yürürlüğe girmesi ile çocuğun kişisel

---

[357] TBMM Komisyon Raporu, s. 10; **Kişisel Verileri Koruma Kurumu,** Özel Nitelikli Kişisel Verilerin İşlenme Şartları, s. 3. https://www.kvkk.gov.tr/Icerik/5238/Ozel-Nitelikli-Kisisel-Verilerin-Islenme-Sartlari (Son Erişim Tarihi: 11.10.2021).

[358] **Kişisel Verileri Koruma Kurumu,** Açık Rıza, s. 4.

[359] **AVCI BRAUN**, s. 30.

[360] **MACENAITE** Milda/**KOSTA** Eleni, "Consent for Processing Children's Persona Data in the EU: Flowing in the US Footsteps?", Information and Communication Technology Law, Cilt.26, Sayı.2, 2017, ss. 146-147; Avrupa Komisyonu, "Towards a Safer Use of Internet for Children in the European Union – A Parents' Perspective", Analytical Report, Flash Eurobarometer Series, The Gallup Organization, 2008, https://op.europa.eu/en/publication-detail/-/publication/4c7ece29-058c-44fe-9aa0-27d67cfc3029/language-en (Son Erişim Tarihi: 24.07.2021).

[361] **UÇAK** Murat, "Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası", Kişisel Verileri Koruma Dergisi. 3(1), 2020, ss. 41-60, s. 47.

verilerinin korunmasına ilişkin yer verdiği hükümlerinde bu sözleşmeden yararlandığı söylenebilir[362].

GVKT'nin 8. maddesine göre, Tüzük m. 6/f.1-a'nın uygulandığı hallerde çocuğun rızası 16 yaşından büyük olması halinde kişisel verilerin işlenmesini meşru kılmaktadır. Ancak 16 yaşından küçük çocuklar için veri işlemenin hukuka uygun hale gelmesinde çocuğun velayet hakkı bulunan kişilerin rıza göstermesi ya da onay vermesi gerekmektedir. GVKT m. 6/f.1-f, çocuğun kişisel verilerinin korunmasına ilişkin menfaatlerinin ağır basması hali dışında, işlemenin bu menfaatler doğrultusunda gerçekleşmesi gerektiğini ifade eder[363]. Bir diğer ifade ile çocuğun temel hak ve özgürlükleri de dahil kişisel verilerini korumaya yönelik denge gözetilmelidir. GVKT m. 6/1-f *"...özellikle veri sahibinin çocuk olması halinde veri sahibinin kişisel verilerin korunmasını gerektiren menfaatler ile temel hak ve özgürlüklerinin bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması…"* şeklinde hüküm kurmuştur. O halde çocuğun kişisel verilerinin korunmasına ilişkin menfaatlerinin ağır basması veri işleme faaliyetlerini hukuka uygun kabul edilecektir[364].

Bununla birlikte GVKT m. 8/f.1'de üye devletlerin kendi yasal mevzuatları bakımından 13 yaşından aşağı olmayacak şekilde bir yaş sınırı belirlemeleri de mümkün kılınmıştır. Dolayısıyla Tüzük bakımından çocuğun kişisel verilerinin işlenmesinde 16 yaşında olma şartı aranmakta, ancak çocuğun 16 yaşını doldurmadığı haller içinde çocuk üzerinde velayet hakkı bulunan kişilerin bu rızayı verebilecekleri ya da rızanın çocuk tarafından verilmesi halinde bu işlemi onaylayabilecekleri kabul edilmektedir[365]. Elbette bu noktada çocuğun rızasının alınması ve alınan rızanın yeterliliği önem taşımaktadır [366]. Keza doktrinde kabul edilen bir görüşe göre, çocuklar

---

[362] **UÇAK,** s. 47.

[363] **ERDOĞAN** Canan, "Çocukların Kişisel Verilerinin Korunması (Sosyal Medya Örneği Kapsamında)", D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019, ss. 2445-2467, s. 2458; Daha üstün nitelikte özel yarar ile ilgili açıklamalar için ayrıca bkz. **HELVACI**, s. 151; **DURAL/ÖĞÜZ**, s. 139.

[364] **ERDOĞAN**, s. 2458.

[365] **DÜLGER** Murat Volkan/**KAHRAMAN** Cansu Ceren/**YALÇIN** Simay, "GDPR ve KVKK Bakımından Çocukların Kişisel Verilerinin Korunması ve Konuya İlişkin Kurul Kararının Değerlendirilmesi" (Protecting Personal Data Of Children From Point Of GDPR and Personal Data Protection Law and Review Of Assize), ss. 1-12.

[366] **DÜLGER/KAHRAMAN/YALÇIN**, s. 3.

kişisel verilerinin işlenmesi noktasında doğabilecek her riski öngöremeyebilirler[367]. Örneğin, 12 yaşında bir çocuğun bir sosyal medya sitesine kaydolmasında dini inanına ilişkin kişisel verilerini paylaşmadan evvel ebeveynlerinin onayına ihtiyaç duyacağı açıktır[368]. Ebeveynler, çocuğun dini bilgilerinin paylaşılmasını sakıncalı bulmadıkları takdirde işleme faaliyetine onay verebilir. Veri sorumluları için özellikle internet teknolojilerinin kullanıldığı ortamlarda, çocuğun ebeveynlerinin rızaya onay verdiğini tespit etmek ise güç olacaktır. GVKT m. 8/f.2 veri sorumlularının, mevcut teknolojiyi dikkate alarak rızanın çocuğun ebeveynleri tarafından verildiğini ya da onaylandığını doğrulamak adına gerekli çabayı sarfetmekle yükümlü olduklarını ifade etmiştir. O halde veri sorumluları, çocuğun verilerini işlemeye yönelik olarak ebeveynlerden alınan rıza ya da onayı ispat edebilmek adına gerekli teknik altyapıyı sağlamalıdır. 17 yaşında bir çocuğun giyim kuşamı ile ilgili tüketim alışkanlıklarına ilişkin çevrimiçi bir ankete katılması ve internet web sitesinin paylaşılacak kişisel veriler ile ilgili onay istemesi halinde ise, çocuğun 16 yaşından büyük olması sebebiyle ebeveynlerinin rızasına ihtiyaç duymaksızın onay verebileceği söylenebilecektir[369].

Tüzüğün 8. madde lafzından da anlaşıldığı üzere, çocuğun kişisel verilerinin korunmasına ilişkin yer alan düzenlemelerde öncelikle çocuk ebeveynleri dışında üçüncü kişilere karşı koruma altına alınmak istenmiştir[370]. Bir diğer ifade ile ebeveynlerin kasti olarak çocuğun zararına bir davranış sergileme potansiyeli düşük olduğundan öncelikle üçüncü kişilere karşı koruma sağlanmak istenmiştir[371]. Ancak her halükârda dikkat edilmesi gereken durum, çocuğun kişisel verilerinin kendi ebeveynleri tarafından paylaşılması halinde çocuğun rızasına ihtiyaç duyulup duyulmayacağı hususudur[372]. Bu noktada BM Çocuk Hakları Sözleşmesi'nin çocuğun özel hayatına ilişkin 16. maddesine değinmek gerekir. Sözleşmenin 16. maddesinin 1. fıkrası, çocuk hakkında velayet hakkı bulunan kişiler de dahil, kişisel verilerin

---

[367] **KRALJIC** Suzan, Children Have The Right To Privacy- Also Against The Parents, IV. Türkiye-Slovenya Karşılaştırmalı Hukuk Sempozyumu Kişilik Hakları, Ankara 2016, ss. 185-197; **GVKT**, Resital 38, Resital 58. Ayrıca bkz. Avrupa Komisyonu, Can personal data about children be collected? https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en (Son Erişim Tarihi: 21.07.2021).

[368] Avrupa Komisyonu, Can personal data about children be collected? **ERDOĞAN**, s. 2457; İskoçya'da 12 yaşın üzerinde olan çocukların aksi ispatlanmadığı sürece kişisel verilerini koruma amaçları dahilinde alınan rızası kabul edilmektedir. **DÜLGER/KAHRAMAN/YALÇIN,** s. 4.

[369] Avrupa Komisyonu, Can personal data about children be collected?

[370] **SERTSÜTÇÜ** Selin, Çocukların Kişisel Verilerinin Korunması, Editörler: **ÖZCAN** Hüseyin/**BAŞAR** Mehmet/**ORMANOĞLU** H. Derya/**KAYIŞ** Ferhat, Kişisel Verilerin Korunması Alanında Yeni Gelişmeler Sempozyumu, Adalet Yayınevi, 5 Aralık 2019, s. 197; **KÜZECİ**, s. 274.

[371] **ERDOĞAN**, s. 2457.

[372] **ERDOĞAN**, s. 2458.

işlenmesi bakımından çocuğun özel hayatına keyfi bir müdahalede bulunamayacağı gibi böyle bir müdahalede bu fillerden sorumluluk doğacağını ifade eder[373]. Örneğin çocuğun rızası dışında kişisel veri niteliğinde fotoğraf ya da videolarının ebeveynleri tarafından paylaşılması, çocuğun kişisel verilerin korunması hakkına müdahale niteliği taşıyacaktır. Bir diğer ifade ile çocuğun kişisel verilerini onun izni dahilinde olmadan paylaşan ebeveyn dahi çocuğun kişisel verilerin korunması hakkını ihlal etmekten ötürü sorumlu olabilecektir[374]. Bu nedenle çocuğun ebeveynleri de olsa, çocuğun kişisel verilerin korunması hakkına müdahalede haksız bir tasarrufta bulunamayacakları söylenebilir[375]. Elbette Kanun'un 28. maddesinin 1. fıkrasının a bendi gereği, üçüncü kişilerle paylaşılmamak ve kişisel veri güvenliğine gerekliliklere uyularak tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili işlemeler kapsamında çocuğun kişisel verileri de işlenebilecektir. Zira her zaman çocuktan rıza alınması mümkün olmayabilir. Rıza alınamayacak küçüklükte olan çocuğun kişisel verilerinin işlenmesi açısından önemli olan husus, menfaat dengesinin gözetilmesi olacaktır[376].

Ülkemizde çocukların kişisel verilerinin korunması ile ilgili düzenlemelere bakıldığında KVKK'da açık bir madde hükmüne yer verilmediği görülmektedir. Ancak KVKK m. 2'de ifade edilen "gerçek kişiler" tanımlamasına çocukların da dahil olduğu görülmektedir. Bu açıdan KVKK bakımından her ne kadar çocukların kişisel verilerine ilişkin bir madde hükmüne yer verilmemiş ise de çocukların da KVKK kapsamında korumadan faydalandığı söylenebilecektir. Bununla birlikte 23 Nisan 2020 tarihinde Kurumun internet sitesinde yayımlanan broşürler önem arz etmektedir[377]. Nitekim bu broşürlerde çocukların, yetişkinlerin ve çocuklara ürün ve

---

[373] **ERDOĞAN**, s. 2454.

[374] **SPOOKY**, 16-Year-Old Takes Mother to Court for Posting Photos of Him on Facebook, January 15th, 2018, https://www.odditycentral.com/news/16-year-old-takes-mother-to-court-for-postingphotos-of-him-on-facebook.html (Son Erişim Tarihi: 22.07.2021).

[375] **AKKURT** Sinan Sami, "Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", Kişisel Verileri Koruma Dergisi, 2(1), 2020, ss. 20-32, s. 26; **AKDİ** Murat, "Ana-Babanın Çocuğun Fotoğraf ve Görüntülerinin Sosyal Medyada Yayınlamasından Doğan Sorumluluğu" Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 2016, ss. 123-144, s. 131.

[376] **AKDİ,** s. 143; **UÇAK**, s. 52; **ERDOĞAN**, s. 2454.

[377] Kişisel Verileri Koruma Kurumu, çocukların kişisel verilerinin korunmasına yönelik farkındalığı arttırmak adına yayımladığı broşürler ile çocukların kişisel verilerinin korunması anlamında kendi farkındalıklarını arttırmaları adına ailelerin bu konuda çocuklarını doğru yönlendirmeleri gerektiğine, ürün ve hizmet geliştirenler açısından ise KVKK'ya uyum konusunda ekstra özen göstermeleri gerektiğine vurgu yaptı. Bunun yanında çocuklara yönelik yayımlanan broşürlerde, özellikle çocukların internet ortamında karşılaşacakları riskler üzerine açıklamalara ve aydınlatma metinlerinin öneminden

hizmet sağlayanların dikkat etmesi gereken bilgilere yer verilmiştir. Benzer şekilde Kişisel Verileri Koruma Kurul'unun 11 Ağustos 2020 tarih ve 2020/622 sayılı Kararı'nın değerlendirilmesi önemlidir. Kararda, bir çocuğa ilişkin sağlık raporunun gerçeğe aykırı olacak şekilde düzenlendiği ve sonrasında imha edildiğine yönelik çocuğun ebeveyni baba tarafından yapılan şikâyete yer verilmiştir. Kurul, TMK m.16/f.1'de, ayırt etme gücüne sahip küçüklerin, yasal temsilcilerinin rızası olmaksızın borç altına giremeyeceğini düzenlenmiş ancak kişiye sıkı sıkıya bağlı hakları kullanırken yasal temsilcinin rızasının alınmasının gerekli olmadığını ifade etmiştir. Ancak bazı kişiye sıkı sıkıya bağlı hakların[378] yasal temsilci tarafından kullanılabileceği, dolayısıyla çocuğun üstün yararı gözetilerek somut olaya göre karar verilmesi gerektiği belirtilmiştir[379]. Doktrin, Kurul kararında da yer verildiği üzere çocuğun kişisel verilerin korunmasında hakkın niteliğinin mutlak değil, nispi kişiye sıkı sıkıya bağlı bir hak olarak kabulünün Kanun hükümlerine uygun olduğunu zira bu hakların kullanılması bakımından ayırt etme gücüne sahip olunup olunmamasının önem taşıdığı, yaş küçüklüğü bakımından ise doktrindeki hâkim görüşe göre her olay nezdinde ayırt etme gücünün değerlendirilmesi gerektiğini ifade etmiştir[380]. Ancak kişisel verilerin korunması anlamında her veri işleme faaliyetinde çocuğun ayırt etme gücüne sahip olup olmadığını değerlendirmenin zahmetli olması neticesinde, KVKK'da yer alacak bir düzenleme ile standart bir yaş sınırının belirlenmesinin yerinde olacağı ifade edilmiştir[381]. Kanaatimizce de bu konuda Tüzük hükümleri dikkate alınarak bir düzenleme yapılması yerinde olacaktır.

Kurul ek olarak "Kişisel Sağlık Verileri Hakkında Yönetmelik" m. 5/f.6'da veri sorumlusuna başvurarak KVKK'nın 11. maddesinde yer alan haklarını kullanabileceğini; aynı Yönetmelik'in 8. maddesi uyarınca da çocuk tarafından aksi

---

bahseden açıklamalara yer verilirken yetişkinlere yönelik yayımlanan broşürlerde yukarıda ifade edildiği üzere çocukların farkındalıklarını arttıracak önerilere yer veriliyor.

[378] Kişisel Verileri Koruma Kurulu'nun 11 Ağustos 2020 tarihli ve 2020/622 sayılı Kararı Özeti, https://www.kvkk.gov.tr/Icerik/6816/2020-622 (Son Erişim Tarihi: 22.07.2022) *"…Ayırt etme gücüne sahip küçüklerin kişiye sıkı sıkıya bağlı hakları kullanmalarında yasal temsilcilerinin rızasının gerekli olmadığına ilişkin kuralın çocuk için bir yetki kuralı olduğu, ancak veli için bir yasak kuralı olmadığı; velinin nispi kişiye sıkı biçimde bağlı hakları küçük adına ve hesabına kullanabildiği ifade edilmiştir. (SEROZAN, Rona; Çocuk Hukuku, Vedat Kitapçılık, İstanbul 2017, s. 282; BAYGIN: s. 315.) …"*

[379] **ERDOĞAN**, s. 2461; **AKINTÜRK** Turgut/**ATEŞ KARAMAN** Derya, Türk Medeni Hukuku, Aile Hukuku, C.II, 14.B., İstanbul 2012, s. 406; **DURAL** Mustafa/**ÖĞÜZ** Tufan/**GÜMÜŞ** Mustafa Alper, Türk Özel Hukuku, Aile Hukuku, C.III, 10.B., İstanbul 2015, s. 351; **DÜLGER/KAHRAMAN/YALÇIN,** ss. 1-12; Kişisel Verileri Koruma Kurulunun 11 Ağustos 2020 tarihli ve 2020/622 sayılı Kararı Özeti, https://www.kvkk.gov.tr/Icerik/6816/2020-622 (Son Erişim Tarihi: 22.07.2021.

[380] **DÜLGER/KAHRAMAN/YALÇIN,** s. 5-8.

[381] **DÜLGER/KAHRAMAN/YALÇIN,** s. 7.

talep edilmediği sürece, çocuklarının sağlık verileri ile ilgili olarak ebeveynlerin herhangi bir onay gerekmeksizin e-Nabız aracılığı ile, sağlık verilerine erişim hususunda yetkili kılınabileceği ifade edilmiştir. Dolayısıyla somut olay değerlendirildiğinde ilgili kişi çocuk ve babanın şikâyet hakkını kullanmada yetkili olduğuna ve KVKK'nın 15. maddesinin 1. fıkrası gereği inceleme başlatılmasına karar verilmiştir.

B. DİĞER HUKUKA UYGUNLUK SEBEPLERİ

Kişisel verilerin işlenebilmesi için Kanun'da öngörülen tek hukuka uygunluk sebebi rıza değildir. Bir diğer ifade ile ilgili kişinin rızası olmasa dahi Kanun'da yer verilen diğer hukuka uygunluk sebeplerinin varlığında da kişisel veriler işlenebilmektedir. Dolayısıyla rıza gerektirmeyen ancak Kanun çerçevesinde kişisel verilerin işlenmesine imkân tanıyan bu durumlar işleme faaliyetlerini hukuka uygun hale getirmektedir[382]. Daha önce ifade edildiği üzere KVKK'nın 5. maddesinde genel nitelikli kişisel veri işleme şartları, 6. maddesinde ise özel nitelikli kişisel veri işleme şartları açıklanmıştır. Dolayısıyla rıza dışında yer alan hukuka uygunluk sebepleri de sınırlı sayıda olup, bu sebepler dışında gerçekleşecek veri işleme faaliyetlerinin hukuka uygun hale gelmesi söz konusu değildir.

1. KVKK ile Uyum Gösteren Hukuka Uygunluk Sebepleri

KVKK'da genel nitelikli kişisel verilerin işlenmesi bakımından rıza dışında yer alan hukuka uygunluk sebepleri, m. 5/f.2'de yer almaktadır. Kanun'un 5. maddesi kapsamında açık rıza dışındaki hukuka uygunluk sebeplerini yedi şart altında toplamak mümkündür. Bu şartlar; veri işleme faaliyetlerinin kanunlarda açıkça öngörülmüş olması; fiili imkânsızlık sebebiyle rıza beyanını açıklayamayacak kişinin kendisi ya da başkasının hayat veya beden bütünlüğünün korunması için işlemeyi zorunlu kılması; bir sözleşmenin kurulması/ifası ile ilgili olmak kaydıyla kişisel verilerin işlenmesinin sözleşmenin tarafları için gerekli olması; veri sorumlusunun hukuki gereklilikleri yerine getirmesi bakımından işleme faaliyetlerinin zorunlu olması; kişisel verilerin veri sahibi kişi tarafından alenileştirilmiş olması; işlemenin bir hakkın

[382] **ÇEKİN**, s. 100.

tesisi/kullanımı/korunması için gerekli olması ve son olarak veri sahibinin temel hak ve özgürlüklerine zarar vermemek şartıyla veri sorumlusunun yasal menfaatleri adına işlemenin zorunlu olması halleridir.

GVKT'nin veri işleme şartları başlıklı 6. maddesine bakıldığında ise, veri işleme şartlarının, 6 şart olarak belirlendiği ancak bu şartlardan bazılarının KVKK'dan farklılık taşıdığı görülmektedir. Bu farklılıklar bir sonraki başlıkta irdelenecek olup, öncelikle Tüzük ile Kanun bakımından benzerlik taşıyan veri işleme şartlarından bahsedilecektir.

GVKT'nin 6. maddesine göre veri sahibinin rızasının olması; bir sözleşmenin ifası ya da ifadan önce sözleşmenin kurulmasında gerekli olması; veri sahibinin taraf olduğu bir sözleşmenin uygulanması ya da sözleşme yapılmadan önce veri sahibinin talebiyle adım atılabilmesi için veri işlemenin gerekli olması; yasal yükümlülükleri uygulayabilmek adına veri sorumlusunun işleme faaliyetini gerçekleştirmesinin gerekli olması; veri sahibinin ya da başkalarının yaşam menfaatlerinin korunması için işlemenin gerekli olması; kamu yararı sebebiyle bir görevin ifası ve resmi bir yetkinin uygulanmasında işlemenin gerekli olması ve ilgili kişinin çocuk olması durumunda çocuğun temel hak ve özgürlükleri ile menfaatlerinin veri sorumlusu ve üçüncü kişilerce yasal menfaatlere ağır basması dışında, söz konusu menfaatler için işlemenin gerekli olmasıdır.

Bu anlamda kişisel veri işlemenin bir sözleşmenin kurulması ve ifasında zorunlu olması durumu GVKT m. 6/f.1-b bakımından KVKK ile benzerdir. Yine KVKK'da yer alan hükümler ile mukayese edildiğinde, GVKT m. 6/f.1-c'de yer alan yasal yükümlülük ile KVKK m. 5/f.2-ç'de gereği hukuki yükümlülük hükmünün; GVKT m. 6/f.1-d'de yer alan gerçek kişinin yaşam menfaatlerini korumak için işlemenin gerekli olması ile KVKK m. 5/f.2-b gereği fiili imkânsızlık halinin; GVKT m. 6/f.1-f'de yer alan meşru menfaat ile KVKK m. 5/f.2-f'de yer alan meşru menfaat hükümlerinin benzer oldukları görülmektedir.

2. KVKK ile Tüzüğün Hukuka Uygunluk Sebepleri Bakımından Farklılıkları

GVKT'nin "İşleme faaliyetinin hukuka uygunluğu" başlıklı 6. maddesinde veri işleme faaliyetlerini rıza dışında hukuka uygun hale getiren sebepler, bir sözleşmenin ifası ya da ifadan önce sözleşmenin kurulmasında gerekli olması; yasal yükümlülükleri uygulayabilmek adına veri sorumlusunun işleme faaliyetini gerçekleştirmek durumda olması; veri sahibinin ya da başkalarının yaşam menfaatlerinin korunması için işlemenin gerekli olması; kamu yararı sebebiyle bir görevin ifası ve resmi bir yetkinin uygulanmasında işlemenin gerekli olması ve ilgili kişinin çocuk olması durumunda çocuğun temel hak ve özgürlükleri ile menfaatlerinin veri sorumlusu ve üçüncü kişilerce yasal menfaatlere ağır basması dışında, söz konusu menfaatler için işlemenin gerekli olması olarak 5 kaleme ayrılmaktadır. Bu anlamda KVKK ile GVKT'nin hukuka uygunluk sebepleri bakımından farklılıklarından bahsetmek gereklidir. Söz konusu ilk farklılık, GVKT m. 6/f.1-e'de kamu yararı sebebiyle bir görevin ifası ve resmi bir yetkinin uygulanmasında işlemenin gerekli olması haline KVKK'nın 5. maddesinde yer verilmemiş olmasıdır. İlgili düzenlemeye Kanun'un "İstisnalar" başlıklı m. 28/f.1-c/d'de yer verilmiştir. Bunun yanında daha önce ifade ettiğimiz üzere KVKK m. 5/f.2-d uyarınca kişisel verilerin veri sahibince alenileştirilmiş olması hali de GVKT'nin veri işleme şartlarının hukuka uygunluğunu ifade eden 6. maddesinde düzenlenmemiştir. Kişisel verilerin veri sahibi kişi tarafından alenileştirilmiş olması Tüzük m. 9/f.2-e'de yer almaktadır. Özel nitelikli kişisel verilerin işlenmesi başlıklı Tüzük m. 9/f.2-e, veri işleme faaliyetlerinin ilgili veri sahibi tarafından açık bir şekilde kamuya açıklanması halinde işleme yasağının ortadan kalktığını ifade etmektedir. Dolayısıyla kişisel verilerin veri sahibi tarafından alenileştirilmiş olması Tüzük'ün işleme şartlarının hukuka uygunluğunu gösteren 6. maddesinde düzenlenmemişken KVKK'nın 5. maddesinde verilerin işlenme şartlarından biri olarak düzenlenmiştir.

Öte yandan özel nitelikli veri işleme bakımından yer alan uygunluk sebeplerinin irdelenmesi gerekir. KVKK'nın 6. Maddesinin 2. fıkrasına göre, sınırlı olarak belirtilen özel nitelikteki verilerin veri sahibinin açık rızası bulunmadan işlenmeye konu olması yasaktır. Aynı hükmün devamında ise Kanun, özel nitelikli kişisel verilerin açık rıza şartına istisna getirmiştir. Bu istisnayı getirirken de özel nitelikli kişisel veriler arasında bir ayrıma giderek sağlık ve cinsel yaşama ilişkin

verileri ayrı bir değerlendirmeye tabi tutmuştur[383]. KVKK'nın m. 6/f.3 hükmüne göre, sağlık ve cinsel yaşama ilişkin kişisel veriler dışında kalan "kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi ya da diğer inançları, kılık kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirlerine ilişkin kişisel verileri" kanunda öngörülen hallerde ve açık rıza aranmaksızın işlenebilmektedir. Bir diğer ifade ile kanunlarda öngörülen hallerde kişisel verilerin işlenebilmesi bakımından KVKK m. 5/f.2-a'daki gibi bir uygunluk sebebi oluşmaktadır[384]. Cinsel yaşam ile sağlık verilerine ilişkin özel nitelikli veriler bakımından ise m. 6/f.3'ün açık rıza şartının istisnasını teşkil edip etmeyeceği tartışmalıdır[385]. Bu tartışmada ilk olarak ifade edilen, genel nitelikteki veriler bakımından kanunlarda "açıkça" öngörülme şartının özel nitelikli veri grubundaki hassas verilerde ele alınmamış olmasıdır[386]. Zira Kanun'un m. 6/f.3 hükmü, sağlık ve cinsel yaşam dışındaki kişisel verilerin istisnasını "kanunda öngörülen hallerde" işlenebilir şeklinde ifade etmiş KVKK m. 5/f.2-a'daki gibi "kanunlarda açıkça öngörülmesi" şeklinde bir düzenlemeye yer vermemiştir. Özel nitelikli kişisel verilerin daha yüksek bir koruma düzeyi gerektirdiği gerekçesiyle bu düzenleme eleştirilmektedir[387].

Eleştiriye konu olan ikinci önemli husus, sağlık ve cinsel yaşamı ilgilendiren veriler ile ilgili olarak m. 6/f.3'ün verileri işlemeye yetkili kişileri sınırlı olarak belirtmesine karşın, "kanunda öngörülme" halini bu istisna kapsamına almamış olmasıdır[388]. Esasında açık rızanın istisnasını oluşturan "kanunda öngörülme" halinin ayrım yapılmaksızın tüm özel nitelikli veri grupları için geçerli olması gerekir. Keza doktrin, sağlık ve cinsel yaşama ilişkin verilerin işlenme şartlarına ilişkin istisnaya yer verilirken kanunda öngörülme halinin madde hükmü içerisinde yer almayışının, yetkilendirilen kişilerin ve işleme amaçlarının geniş ölçüde yorumlanabilecek olması ile bu veri türleri üzerindeki korumayı azalttığını ifade etmektedir[389]. Dolayısıyla açık rızaya getirilen istisnanın, genel nitelikli kişisel verilerde olduğu gibi özel nitelikli kişisel veriler içinde geçerli olduğunu, bir diğer ifade ile m. 6/f.3'te yer alan istisnanın

[383] **KÜZECİ**, s. 405.
[384] **TAŞTAN**, s. 169.
[385] **KÜZECİ**, s. 405.
[386] **KÜZECİ**, s. 405; **TAŞTAN**, s. 221.
[387] **KÜZECİ**, s. 406.
[388] **KÜZECİ**, s. 405; **TAŞTAN**, s. 170; **DÜLGER**, s. 221.
[389] **KÜZECİ**, s. 406.

hukuka uygun hale gelmesi için KVKK m. 5/f.2'deki rıza dışındaki uygunluk sebeplerinden birinin varlığının gerekli görüldüğünü ifade eder[390].

Son olarak KVKK bakımından genel nitelikli ya da özel nitelikli kişisel veriler arasında ayrım yapılmaksızın 28. maddenin koşullarının oluşması durumunda Kanun hükümlerinin uygulanmayacağını ve kişisel verilerin işlenebileceğini belirtmek gerekir. KVKK'nın 28. maddesine dayanılan hallerde veri işleme faaliyetlerinin hukuka aykırılığından söz edilemeyecek olup, işleme faaliyetleri açık rızası olmaksızın gerçekleşebilecektir[391].

Ülkemizin de içinde bulunduğu pandemi koşullarında KVKK m. 28/f.1-ç'de ifade edilen istisna hallerinden kamu ve ekonomiye ilişkin güvenlik ve düzeni sağlamak için yetkilendirilmiş kamu kurum ve kuruluşlarınca yürütülen faaliyetler kapsamında veri işleme açık rıza olmaksızın işlenebilmektedir[392]. Nitekim tüm dünyada etkisi olan COVID-19'un hayatımızı önemli ölçüde etkileyen varlığı karşısında, kişisel verilerin kamu sağlığının korunması anlamında işlenmesi gerekmektedir. Bu husus ile ilgili olarak Kurulun *"COVID-19 ile Mücadelede Konum Verisinin İşlenmesi ve Kişilerin Hareketliliklerinin İzlenmesi Hakkında Bilinmesi Gerekenler"* başlıklı kamuoyu duyurusunda toplum sağlığının korunması ve bu vesileyle kamu güvenliğinin ve düzeninin sağlanması amacıyla yetkililer tarafından veri işlemenin yasal olarak mümkün olduğu, bununla beraber kişisel verilerin güvenliğinin gözetilmesinin de gerekli olduğu ifade edilmiştir[393].

---

[390] **YÜCEDAĞ**, "Medeni Hukuk Açısından Kişisel Verilerin Korunması", s. 773; **29. Madde Çalışma Grubu,** WP 217, s. 14-16.

[391] **TAŞTAN**, s. 171.

[392] **AKKURT** Sinan Sami, "Kişisel Sağlık Verilerinin İşlenmesine ve Covıd19 Pandemisi Sürecinde Mobil Uygulamalarla Paylaşılmasına Hukukî Bir Bakış", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi Covid-19 Hukuk Özel Sayısı Yıl:19 Sayı:38 Yaz 2020/2 (Covid-19 Özel Ek) ss. 142-160; s. 151.

[393] **Kişisel Verileri Koruma Kurumu**, 9 Nisan 2020 Tarihli Kamuoyu Duyurusu, https://www.kvkk.gov.tr/Icerik/6726/COVID-19-ILE-MUCADELEDE-KONUM-VERISININ-ISLENMESI-VE-KISILERIN-HAREKETLILIKLERININ-IZLENMESI-HAKKINDA-BILINMESI-GEREKENLER-2- (Son Erişim Tarihi:23.07.2021).

III. KİŞİSEL VERİLERİ KORUMA KANUNU İLE FARKLILIK GÖSTEREN AB VERİ KORUMA TÜZÜĞÜ İLKELERİ

A. GENEL OLARAK

Kişisel verilerin korunması hukukunda, gelişen teknoloji ile her geçen gün veri işleme yöntemleri de artmaktadır. Dolayısıyla gerek rıza kavramı gerek rıza kavramı dışında yer alan diğer hukuka uygunluk sebeplerinde veri işleme faaliyetlerinin dürüstlük ve iyi niyet başta olmak üzere hukuk kurallarına ve ahlaka uygun işlenebilmesi için belirli ilkeler tesis edilmiştir. Kişisel verilerin işlenmesi bakımından rıza ya da rıza dışında yer alan diğer hukuka uygunluk halleri var olsa bile, bu ilkelere uyulmadığı ya da bu ilkelere aykırı davranıldığı müddetçe işleme faaliyetleri hukuka uygun olmamaktadır[394].

Kişisel verilerin işlenmesine ilişkin düzenlenen temel ilkeler hemen hemen tüm hukuk sistemlerinde ortak bir yaklaşıma sahiptir. Nitekim GVKT'nin 5. maddesinde genel ilkeler, "*hukuka uygunluk, adillik ve şeffaflık*", "*amacın sınırlandırılması*", "*veri minimizasyonu*", "*doğruluk (bilgilerin isabetli olması)*", "*saklama süresinin sınırlandırılması*", "*bütünlük ve gizlilik*", ve "*hesap verilebilirlik*" şeklinde sıralanmıştır. KVKK'nın 4. maddesinde bu ilkeler, "*hukuka ve dürüstlük kurallarına uygun olma*", "*doğru ve gerektiğinde güncel olma*", "*belirli, açık ve meşru amaçlar için işlenme*", "*amaçla bağlantılı, sınırlı ve ölçülü olma*", "*işlendikleri amaç ile gerekli olan süre kadar muhafaza edilme*" şeklinde sıralanmıştır.

B. HUKUKA UYGUNLUK, ADİLLİK, ŞEFFAFLIK

Kişisel verilerin işlenmesine ilişkin olarak hemen hemen bütün uluslararası metinlerde ortak olan ilk ilke, hukuka ve dürüstlük kuralarına uygun veri işlemenin gerçekleştirilmesidir. Ancak belirtmek gerekir ki kişisel verilerin işlenmesine ilişkin olarak getirilen tüm ilkeler birbiri ile yakından bağlantılı, kimi zaman birbirleri ile iç içe geçen ve birbirlerine kaynaklık eden nitelikte ilkelerdir[395]. Bu nedenle kişisel verilerin işlenmesine ilişkin bu ilkenin bu konuya ilişkin ortaya çıkan ilk ilke olduğu

[394] **DEVELİOĞLU,** s. 44.
[395] **KÜZECİ**, s. 228; **KORKMAZ** İbrahim, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", Türkiye Barolar Birliği Dergisi, 2016, S.124, s. 100; **AKGÜL**, "Kişisel Verilerin Korunması", s. 125.

ifade edilmektedir[396]. Aşağıda bu ilkenin unsurları, KVKK ile mukayeseli olarak irdelenecektir.

1. Hukuka Uygunluk

GVKT'nin "İlkeler" başlıklı 5. maddesinin 1. fıkrasının a bendi kişisel verilerin, hukuka uygun, adilane ve şeffaf bir işlenmeye konu olması gerektiğini ifade etmiştir. Ancak m. 5/f.1-a'da hukuka uygunluk ile ifade edilmek istenen hususun ne olduğu açıklanmamıştır[397].

GVKT m. 6'da işleme faaliyetini hukuka uygun kılan unsurlar sıralanmıştır. Benzer şekilde GVKT'nin 40 No'lu resitalinde, kişisel veriler bakımından gerçekleşecek işleme faaliyetlerinin hukuka uygun olması için ilgili veri sahibi kişilerin rızasının alınması gerekliliği ya da Birlik veya üye devletlerin mevzuatlarında işleme faaliyetlerinin, Tüzük ile uyumlu ve meşru hale getirilmiş olması gerektiği ifade edilmiştir[398].

KVKK m. 4/f.2-a'ya göre de kişisel verilerin, Tüzük ile paralel olacak şekilde hukuk kurallarına ve dürüstlük kurallarına uygun olarak işleneceği belirtilmiştir. İlke, veri işleme bakımından ikili bir ayrımla değerlendirilerek, hukuka uygun işleme ve dürüstlük kurallarına uygun işleme olarak da ifade edilmektedir. KVKK m. 4/f.2-a'nın yorumlanması bakımından da hukuka uygunluk ile ifade edilen hususun diğer tüm kanun ve hukuki düzenlemelere uygun olarak işlenmesi gerektiği ifade edilmektedir[399]. Dolayısıyla burada ifade edilen esas husus gerek KVKK gerek Tüzük bakımından değerlendirildiğinde, kişisel verilerin genel ilkelere uygun ve veri işlenme faaliyetlerinin rıza ya da diğer hukuka uygunluk hallerden herhangi birine aykırılık taşımaması gerektiği şeklinde ifade edilebilir[400].

---

[396] **AKGÜL**, "Kişisel Verilerin Korunması", s. 126; **KÜZECİ**, s. 228.
[397] **YÜCEDAĞ** Nafiye, "Kişisel verilerin korunması kanunu kapsamında genel ilkeler", Kişisel Verileri Koruma Dergisi, 2019, 1(1), ss. 47-63, s. 48.
[398] **YÜCEDAĞ**, "Genel ilkeler", s. 48; **GVKT**, Resital 40.
[399] **KÜZECİ**, s. 229; **AYÖZGER ÖNGÜN**, s.124; **KORKMAZ**, s. 100; **AKGÜL**, "Kişisel Verilerin Korunması", s. 126; **ÇEKİN**, s. 69.
[400] **YÜCEDAĞ**, "Genel ilkeler", s.49; **ÇEKİN,** s. 70.

2. Adillik

GVKT m. 5/f.1-a'da yer verilen adillik ile anlatılmak istenenin dürüstlük kurallarına uygun olma hususunu ifade ettiği dile getirilebilir[401]. KVKK m. 4/f.2-a'ya göre dürüstlük kurallarına uygun olarak işleme faaliyetleri gerçekleşmelidir. Kişisel verilerin dürüstlük kurallarına göre işlenmesi ile veri işleme faaliyetlerini gerçekleştiren veri sorumlusunun ilgili veri sahibi kişilerin beklenti ve çıkarlarını gözeterek amacı dışında ve aşırılıklardan uzak adilane bir işleme faaliyeti gerçekleştirmesi ifade edilebilir[402]. Direktif'in 38 No'lu giriş paragrafında ifade edildiği şekliyle, ilgili veri sahibi, işleme faaliyetlerinden haberdar olmalı ve veri sorumlusu, ilgili veri sahibine doğru ve güncel bilgileri aktarmış olmalıdır. Veri sorumlusu tarafından ilgili veri sahibine doğru ve güncel bilgilerin sunulması şeffaflık ilkesi ile de değerlendirilmektedir[403]. Doktrin, dürüstlük kurallarına uygun olma halinin başka bir deyişle adillik unsurunun TMK m. 2/f.2 anlamında dürüstlük kuralına eş değer olmadığını ifade eder[404]. Aksi görüşte olanlar ise, dürüstlük kurallarına göre işlemenin TMK m. 2/f.2'deki dürüstlük kuralının bir görünümü olduğunu ifade etmektedirler[405]. Ancak belirtmek gerekir ki, ister dürüstlük kurallarına uygunluk olarak ifade edilsin, ister adil olma şeklinde ifade edilsin, söz konusu temel ilke veri sorumlularınca ilgili kişinin makul çıkar ve beklentilerini dikkate almalıdır[406].

---

[401] Almanca metninde "Treu und Glauben" şeklinde ifade edilen dürüstlük kurallarına uygun olma hususu, Tüzük'ün İngilizce metninde "fair" adil olma, İtalyanca metninde de "corretto" doğru, adil olma şeklide kullanılmıştır. **YÜCEDAĞ**, "Genel ilkeler", s. 49.

[402] **KÜZECİ**, s. 229; **ÖZER DENİZ**, s. 74.

[403] **KÜZECİ**, s. 230; **AKGÜL**, "Kişisel Verilerin Korunması", s. 126; **DEVELİOĞLU**, s. 45.

[404] **YÜCEDAĞ**, "Genel ilkeler", s.49, Naklen; **BRAUN** F. (2019). Bundesdatenschutzgesetz (13. Bası). Gola, P. ve Heckmann, D. (ed.). München: C. H. Beck; **ÇEKİN**, s. 70. Medeni Kanun'daki dürüstlük kuralı dürüst ve namuslu bir kişiden beklenen makul davranışları gösteren kurallar bütünüdür. **OĞUZMAN** Kemal/**BARLAS** Nami, Medeni Hukuk (Giriş, Kaynaklar, Temel Kavramlar), Onikilevha Yayınları, 28 Bası, İstanbul, 2022, s. 245-247.

[405] **TAŞTAN**, s. 46; **ÖZDEMİR** Hayrunnisa, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara, Seçkin Yayınları, 2009, s. 138; **DÜLGER**, s. 111.

[406] **ÇEKİN**, s. 70; **KÜZECİ**, s. 230; **AKGÜL**, "Kişisel Verilerin Korunması", s.126; **YÜCEDAĞ**, "Genel ilkeler", s. 50. Nitekim Kişisel Verileri Koruma Kurulunun 31 Mayıs 2019 Tarih ve 2019/159 Sayılı Kararında, bir kişinin cep telefonuna farklı tarihlerde aynı tarzda mesajlar göndermenin veri sorumlusunun kötüye kullanımı olarak değerlendirilmesi gerektiği ve bu durumun hukuk kurallarıyla ve dürüstlük kurallarıyla bağdaşmayacağı ifade edilmiştir. Benzer şekilde Kurulun 8 Temmuz 2019 Tarih ve 2019/206 sayılı Kararında, veri sahiplerinin kişisel verilerini işleyen bir web sitesinde, işleme faaliyetlerinin açık rızaya mı ya da veri sorumlusunun yasal yükümlülükleri çerçevesinde işlendiğinin tespit olunamadığı, ayrıca web sitesinde yer alan aydınlatma metninden bu hususun anlaşılamadığı dolayısıyla açık rıza dışında yasal bir zorunluluk sebebiyle işleme faaliyetleri mümkün olmasına rağmen işlemenin açık rıza şartına dayandırılmasının veri sorumlusunun sahip olduğu hakları kötüye kullanmak olarak anlaşılacağı ifade edilmiştir. Çünkü veri sorumlusundan açık rızanın geri çekilmesi halinde veri işlemenin bu kez yasal zorunluluklara dayandırılacak olması hukuk kuralları ve dürüstlük kuralları ile örtüşmeyecektir. *Ulaşım hizmeti sunan bir mobil uygulama kapsamında işlenen kişisel veriler*

3. Şeffaflık

KVKK bakımından şeffaflık ilkesi ayrı bir şekilde düzenlenmemiş olsa da[407] GVKT m. 5/f.1-a'da şeffaflık ilkesine ayrıca değinilmiş ancak şeffaflık kavramının tanımı yapılmamıştır[408]. Doktrin, şeffaflık ilkesini ilgili veri sahibi kişinin, kişisel verilerinin kim tarafından ve hangi amaçlarla işlendiğini kolay bir şekilde öğrenebilmesi olarak ifade etmiştir[409]. Bir diğer ifade ile şeffaflık ilkesi, ilgili kişinin kişisel verileri üzerindeki hâkimiyetini sürdürmesi olarak da değerlendirilmiştir[410]. Nitekim GVKT'nin ilgili madde gerekçesinde, veri sorumlularının, ilgili veri sahibi kişilere karşı kendileriyle ilgili kişisel verilerin hangi amaçlarla ve ne ölçüde toplandığı, kullanıldığı, ne şekilde işlendiği veya işleneceği hususlarında şeffaf olmaları gerektiği ifade edilmiştir. Ek olarak şeffaflık ilkesi ile kişisel verilerin işlenmesine ilişkin her türlü bilgiye kolayca erişilebilmeli ve kolay anlaşılır olmalı ve kullanılacak dilin açık ve sade olması gerektiği ifade edilmiştir[411].

C. AMACIN SINIRLANDIRILMASI

GVKT m. 5/f.1-b'ye göre "amacın sınırlandırılması" şeklinde ifade edilen ilke gereğince, kişisel verilerin açık olacak şekilde belirli ve yasal amaçlara göre elde edileceği aksi şekilde işlenemeye konu olamayacakları ifade edilmiştir[412]. Nitekim KVKK m. 4/f.2-c'de de aynı ifadeler yer almaktadır. Dolayısıyla bu ilkeye göre kişisel veriler, işlemeyi hukuka uygun kılan sınırlı amaçlar dahilinde işlenmelidir[413]. Böylelikle ilgili kişi de kendisiyle ilgili kişisel verilerin hangi amaçlar dahilinde

---

hakkında" Kişisel Verileri Koruma Kurulunun 27 Ocak 2020 tarih ve 2020/65 sayılı Kararında, veri sorumlunca veri sahibi müşterilerini puanlayarak işleme faaliyetini gerçekleştirmede işleme faaliyetlerinin gerçek amacının açıklanmadığı söz konusu durumun açık ve yasal amaçlar dahilinde işlemeye uygun düşmeyeceği ifade edilmiştir.

[407] Doktrinde, kişisel verilerin işlenmesi aşamalarında veri sorumlularının şeffaf olmalarına ilişkin ifadeler, hukuka ve dürüstlük kurallarına uygunluk kapsamında değerlendirilmektedir. **KÜZECİ**, s. 230; **DEVELİOĞLU**, s. 45; **KORKMAZ,** s. 100.

[408] **29. Madde Çalışma Grubu**, WP 260, s. 9

[409] **DEVELİOĞLU**, s. 44.

[410] **ÇEKİN**, s. 79.

[411] **GVKT**, Resital 39, "Principles of Data Processing", Ayrıca bkz. ICO, What is transparency?, s. 21-22. https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf (Son Erişim Tarihi:25.07.2021).

[412] **KÜZECİ**, s. 230-235.

[413] **ŞİMŞEK**, s. 83; **AKGÜL,** "Kişisel Verilerin Korunması", s. 127.

işlendiğini bilebilecek ve verileri üzerinde hâkimiyetini korumaya devam edebilecektir. Kişisel verilerin açık olacak şekilde belirli ve yasal amaçlara göre işlenmesi ilkesinin verilerin korunması anlamında yer verilen diğer ilkeler açısından da son derece önemli olduğu, zira veri işleme faaliyetlerinin diğer ilkelere de uygunluk bakımından gerçekleşip gerçekleşmediğinin tespitinin bu vesileyle değerlendirilebileceği ifade edilmektedir[414].

Kişisel verilerin belirli amaçlar dahilinde işlenmesine yönelik gerek Direktif gerek Tüzük gerekse KVKK bakımından bir tanımlamaya yer verilmemiştir. Bununla birlikte 29. Madde Çalışma Grubu kişisel verilerin korunması için oluşturulan yasal çerçevenin temelinde kişisel verilerin işlenme amaçlarının belirlenmesinin yattığını ifade etmektedir[415]. Dolayısıyla kişisel veri işlemenin hukuka uygunluğunu belirlemek ya da hangi veri koruma tedbirlerinin uygulanması gerektiğini tespit edebilmek için kişisel verilerin toplanmasının gerekli olduğu spesifik amaçlar belirli olmalıdır[416]. O halde kişisel verilerin işlenme amaçlarının hangi amacı gösterdiği belli olmayan muğlak ifadeler barındırmaması gerektiği söylenebilir[417]. Nitekim 29. Madde Çalışma Grubu da *'kullanıcıların deneyimini geliştirmek', 'pazarlama faaliyetleri', 'gelecekteki araştırmalar'* gibi ayrıntıya girmeyen belirsiz nitelikteki amaçların bu ilkenin "belirli amaç" kriterini karşılamayacağını ifade etmiştir[418]. Elbette bir amacın belirli sayılabilmesi için, toplanan kişisel verilere ve bu verilerin işlenme amaçlarına bakmak gerekir. Dolayısıyla kimi durumda basit bir açıklama yeterli iken kimi durumda daha fazla ayrıntıya yer verilmesi gerekecektir. Netice olarak her somut veri toplama faaliyetine göre ayrı ayrı değerlendirilmesi gerektiği ifade edilebilir. Kişisel veri işleme amaçlarının "ileride gerekli olabilir" düşüncesi ile toplanarak işlenmesi, amaca uygunluk ilkesine aykırı kabul edilmekte, bu nedenle işleme amacının işleme faaliyetinden önce belirli olması[419] ve ilgili kişinin bu anlamda aydınlatılmış olması gerekmektedir[420].

---

[414] **YÜCEDAĞ**, "Genel ilkeler", s. 52.
[415] **29. Madde Çalışma Grubu**, WP 203, s. 15.
[416] **29. Madde Çalışma Grubu**, WP 203**,** s. 15.
[417] **KÜZECİ**, s. 231; **AKGÜL**, "Kişisel Verilerin Korunması", s. 127; **29. Madde Çalışma Grubu,** WP 203, s. 16.
[418] **29. Madde Çalışma Grubu,** WP 203**,** s. 16; **YÜCEDAĞ**, "Genel ilkeler", s. 53; **ÇEKİN**, s. 73.
[419] Kişisel verileri işleme amacının veri işleme faaliyetlerinden önce belirlenmiş olması gereği, en geç kişisel verilerin toplaması anında gerçekleşmiş olmalıdır. **GVKT**, 39 No'lu resital; **ÇEKİN**, s. 73.
[420] **AKGÜL**, "Kişisel Verilerin Korunması", s. 127; **KÜZECİ**, s. 231.

Kişisel verilerin amacının "açık" olması, işleme amaçlarının anlaşılır bir biçimde ifade edilmesini, açıkça ortaya konması gerektiğini ifade etmektedir[421]. Bu gerekliliğin amacı da kişisel verileri işlenecek ilgili kişiye karşı işleme amaçları konusunda bir belirsizlik yaratmanın önüne geçmektir[422]. Bir diğer ifade ile kişisel verilerin işlenme amaçlarının anlaşılmasında hiçbir şüphe yer almamalıdır.[423] O halde amaçların "açıkça" belirtilmesi gerekliliği şeffaflık ilkesi ile yakından ilişkili kabul edilebilir[424].

Kişisel verilerin meşru amaçlar dahilinde işlenmesi, işlemenin tüm aşamalarında hukuka uygunluk sebeplerinden birine dayanması gerekliliğini ifade etmektedir[425]. Bir diğer ifade ile kişisel verilerin işlenmesi hukuki bir temele dayanmalı, bütün hukuki gereksinimleri karşılamalı ve kişisel verilerin işlenmesinden elde edilen menfaatler arasında bir denge sağlamalıdır[426]. Nitekim KVKK Terimler Sözlüğü 'nde[427] Kanun'un 4. madde gerekçesinden kişisel verileri işleme amacının meşruluğu veri sorumlusunun sunduğu hizmetle ilgili ve bu hizmetler için gerekli olması ile ilişkilidir. Ayrıca kişisel verilerin toplanma amaçları ile işleme faaliyetlerindeki amaçların bir paralel olması gerekmektedir[428].

D. VERİ MİNİMİZASYONU

GVKT m. 5/f.1-c'ye göre veriler, işlendikleri amaçlarla ilgili yeterli (ölçülü), yerinde ve gerek olduğu kadar (sınırlı olacak şekilde) işlenmelidir. Tüzük bakımından bu ilke verilerin minimizasyonu olarak ifade edilmiştir. KVKK m. 4/f.2-ç'de de veri minimizasyonu ile verilerin işlendikleri amaçla ölçülü, bağlantılı ve sınırlı olması gerektiği belirtilmiştir. Kanun'un 4. madde gerekçesinde[429] kişisel verilerin işlenmesinde, işleme amaçlarıyla bağlantılı olmayan ya da veri işleme kapsamında ihtiyaç duyulmayan kişisel verilerin işlenmemesi gerektiği ifade edilmiştir. Benzer

[421] **29. Madde Çalışma Grubu,** WP 203, s. 17.
[422] **29. Madde Çalışma Grubu,** WP 203, s. 17.
[423] **29. Madde Çalışma Grubu,** WP 203, s. 17.
[424] **YÜCEDAĞ**, "Genel ilkeler", s. 52.
[425] **29. Madde Çalışma Grubu,** WP 203, s. 20; **YÜCEDAĞ**, "Genel ilkeler", s. 53; **KÜZECİ**, s. 232.
[426] **KÜZECİ**, s. 232.
[427] **Kişisel Verileri Koruma Kurumu,** "KVKK Terimler Sözlüğü", s. 15.
[428] TBMM Komisyon Raporu, s. 8; **Kişisel Verileri Koruma Kurumu,** "KVKK Terimler Sözlüğü", s. 16.
[429] TBMM Komisyon Raporu, s.8; **Kişisel Verileri Koruma Kurumu,** ""KVKK Terimler Sözlüğü", s. 16.

şekilde kişisel verilerin amacın gerçekleştirilmesi için gerekli ölçüde sınırlı tutulması gerektiği ifade edilmiştir[430]. Bu anlamda kişisel verilerin yeterli, ilgili ve gerekli olanla sınırlı olarak işlendiğinin belirlenmesinde kişisel verilerin belirli, açık ve meşru amaçlarla işlenip işlenmediği hususu da dikkate alınacaktır[431].

Görüleceği üzere veri minimizasyonu ilkesinde kişisel verilerin işlenmesi için üç ana unsurun gerekliliği ifade edilmiştir. Kişisel verilerin yeterli olması ile verilerin ölçülü[432] bir şekilde işlenmesi gerekliliği ifade edilmektedir. Ancak belirtmek gerekir ki yeterlilik ile ifade edilmek istenen üzerine ortak bir fikir birliği bulunmamaktadır. Bu anlamda yeterlilik kimi yazarlar tarafından "verileri asgari seviyede işleme" olarak da değerlendirilebilmektedir[433]. Kişisel verilerin ölçülü bir şekilde işlenmesi ile verileri işlenen kişilerin temel hak ve özgürlüklerine ne ölçüde müdahale edildiği, bu müdahalenin orantılı olup olmadığı, kişisel verilerin elde edilme yöntemlerinin tümü dikkate alınmaktadır[434]. Kişisel verilerin işleme amaçları dışında başka amaçlar için işlenmesi, veri işlemenin ilgili (bağlantılı) ve sınırlı olması unsurlarına aykırılık teşkil edecektir. Dolayısıyla ilgili kişiden elde edilecek verilerin asgari seviyede olması gerekmektedir[435]. Bir diğer ifade ile teknik imkânlar kullanılarak gerçekleştirilecek işleme faaliyetlerinde elde edilen veriler minimize edilmelidir[436]. Veri sahiplerinin el ve avuçlarını otomatik olarak okutarak kendileri ile ilgili biyometrik veri elden eden ve bu bilgileri spor salonu işletirken üyelerinin giriş çıkış zamanlarda toplayan veri sorumlusu ile ilgili olarak Kurulun vermiş olduğu bir karar mevcuttur[437]. Kararda spor salonu üyelerinden elde edilen biyometrik verilerin üyelere ilişkin özel nitelikte verileri de içerecek şekilde fotoğraf, giriş çıkış saati gibi bilgilerin herkesin görebileceği bir ekranda yansıtılarak işlendiği dolayısıyla bu verilerin güvenli bir şekilde muhafaza edilip edilmediğinin tespiti üzerine bir değerlendirme yapılmıştır.

---

[430] TBMM Komisyon Raporu, s. 8.
[431] **YÜCEDAĞ**, "Genel ilkeler", s. 59.
[432] Ölçülülük ilkesinden veri işleme faaliyetlerinde gerçekleşmesi beklenen amaç ile işleme faaliyetleri arasında makul bir dengenin kurulması anlaşılmaktadır. **Kişisel Verileri Koruma Kurumu,** "KVKK Terimler Sözlüğü", s. 16.
[433] **AKGÜL**, "Kişisel Verilerin Korunması", s. 127; **KÜZECİ**, s. 237; **ÖZER DENİZ**, s. 85.
[434] **ŞİMŞEK**, s. 99.
[435] TBMM Komisyon Raporu, s. 8.
[436] **AKGÜL**, "Kişisel Verilerin Korunması", s. 133.
[437] Kişisel Verileri Koruma Kurulu'nun 25 Mart 2019 Tarih ve 2019/81 Sayılı Kararı ve 31 Mayıs 2019 Tarihli ve 2019/165 sayılı Karar Özeti https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 (Son Erişim Tarihi: 12.10.2021). Daha yakın tarihli benzer bir karar için bkz. Kişisel Verileri Koruma Kurulu'nun 3 Eylül 2021 Tarih ve 2021/889 Sayılı Kararı, Editör: **İÇÖZ KOYUNCUOĞLU** Ömrüncegül, Hazırlayanlar: **ULUSEL** Melis/**BOZKURT** Tuğçe/**DEMİREL** İdil, Kişisel Verileri Koruma Kurulu Kararları, On İki Levha Yayıncılık, 2. Baskı, İstanbul, Mayıs 2022, s. 260.

Nitekim Kişisel Verileri Koruma Kurumu, AİHM'nin Marper/Birleşik Krallık kararında[438], veri sahiplerinin parmak izi, DNA profilleri gibi özel nitelikteki verilerin saklanmasının ölçülülük ilkesini aşan, aşırı ve orantısız bir müdahale olduğunu bu sebeple AİHS'nin 8. maddesine aykırı düştüğünü ifade etmiştir. Dolayısıyla üyelere sunulan üyelik sözleşmesinde avuç izi alınmasına rıza gösterilmesinin sözleşmenin kurulması için zorunlu bir şart olarak sunulduğu, spor salonu üyelerinin avuç içi bilgilerinin alınmasına açık rıza göstermedikleri takdirde spor salonu hizmetlerinden faydalanamayacakları birlikte değerlendirilmiş netice olarak üyeler tarafından alınan açık rıza beyanlarının da iradeye dayalı ve özgür biçimde verilmiş rıza beyanları olamayacağının altı çizilmiştir.

E. DOĞRULUK (BİLGİLERİN İSABETLİ OLMASI)

GVKT m. 5/f.1-d'ye göre veriler doğru ve güncel olmalıdır. Bunun yanında, işleme amaçları dikkate alınarak doğruluğu olmayan verilerin gecikme olmaksızın düzeltilmesi ya da silinmesi için gerekli tüm tedbirler alınmalıdır. KVKK m. 4/f.2-b'de verilerin doğru ve güncel olması gerektiği ifade edilmiştir. İşlenen verilerin doğruluğu ve güncelliği, söz konusu veri sahibinin sosyal ortamını da etkilediği gibi bilgilerin doğru olması aynı zamanda veri sorumlusu açısından da bir gerekliliktir[439]. Zira veri sorumlusu elde ettiği kişisel verileri belirli bir amaç dahilinde işlemekte, dolayısıyla işlenen verilerin bu amaçlar dahilinde doğru ve güncel veriler olması gerekmektedir[440].

Bunun yanında ilgili kişiye ilişkin bilgilerin yanlış olması kişilerin haklarına, özgürlüklerine ya da ekonomik anlamda menfaatlerine zarar verici nitelikte olabilir[441]. Bu anlamda AİHM'nin Rotaru/Romanya kararında olduğu gibi avukat olan bir kişinin öğrencilik yıllarında kaleme aldığı mektupların üzerinden elli yıl geçmesi dolayısıyla bilgilerin gereğinden uzun süre tutulması ve bilgilerin doğru olmayışı sebebiyle AİHS'nin 8. maddesine aykırı olduğu kararı verilmiştir[442].

---

[438] Marper/Birleşik Krallık Kararı, (Başvuru Numarası 30562/04 ve 30566/04), STRASBOURG, 4 December 2008, https://rm.coe.int/168067d216 (Son Erişim Tarihi: 10.10.2021).
[439] **KÜZECİ**, s. 243.
[440] **KÜZECİ**, s. 243; **DEVELİOĞLU**, s. 48; **KORKMAZ**, s. 101.
[441] **KÜZECİ**, s. 243; **AKGÜL**, "Kişisel Verilerin Korunması", s. 131-132; **DEVELİOĞLU**, s. 48; **KORKMAZ**, s. 101.
[442] Rotaru/Romanya Kararı; **AKGÜL**, "Kişisel Verilerin Korunması", s. 132.

Doğruluk ilkesinin ilgili veri sahibinin erişim hakkı ile de yakından ilgili olduğu, ilgili kişinin kendisiyle ilgili bu verilere erişemediği durumlarda bilgilerin doğruluğundan ya da güncelliğinden söz edilemeyeceği ifade edilmektedir[443]. Nitekim kendisi ile ilgili işlenen kişisel verileri doğru olmayan veri sahibinin GVKT'nin 16. maddesi doğrultusunda gecikmeksizin düzeltilmesini talep hakkı olduğu ifade edilmiştir. Benzer şekilde KVKK m. 11/f.1-d'de veri sahibi, verilerin eksik ya da doğru olmayan şekilde işlenmiş olması durumunda bu bilgilerin düzeltilmesini talep edebilir. Ancak KVKK m. 4/f.2-b'den farklı olarak GVKT m. 5/f.1-d'ye göre ilgili veri sahibi, kişisel verileri üzerinde düzeltme hakkını kullanmasa dahi veri sorumlusu gerekli tüm makul tedbirleri almakla yükümlüdür. Elbette veri sorumlusunun ilgili kişi hakkındaki kişisel verileri doğru ve güncel şekilde tutmasının, ilgili kişinin durumunu sürekli araştırması anlamı taşıdığı düşünülmemelidir[444]. Bizim de katıldığımız görüşe göre, veri sorumlularının kişisel verileri periyodik olarak güncellenmesi ağır bir yükümlülük olarak değerlendirilemeyecekse de somut olaya göre yapılacak bir inceleme ile veri sorumlularının gerektiğinde ekstra özen göstermeleri gerekebilecektir[445]. Nitekim GVKT m. 5/f.1-d'de ifade edilen veri sorumlularının makul tedbirleri alma yükümlülüklerinin KVKK bakımından da geçerli olması gereklidir.

F. SAKLAMA SÜRESİNİN SINIRLANDIRILMASI

GVKT m. 5/f.1-e'ye göre kişisel veriler, veri işleme amaçlarının gerektirdiği süre ile sınırlı olarak tutulmalıdır. Bununla birlikte Tüzük m. 89/f.1 gereği verilerin tarihsel, bilimsel ya da istatistiki amaçlarla işlenmesinde, kamu yararı gözetilerek işlenmesinde, ilgili kişinin hak ve özgürlüklerinin güvence altına alınmasına ilişkin gerekli teknik ve idari tedbirleri almasıyla saklama süreleri daha uzun olabilmektedir. KVKK m. 4/f.2-d'de de kişisel verilerin Kanunda öngörülen süre ile sınırlı olacak şekilde yahut veri işleme amaçları için gerekli olan süre ile sınırlı olacak şekilde muhafaza edilmeleri gerektiğini ifade etmektedir. Dolayısıyla kişisel verilerin

[443] **KÜZECİ**, s. 243.
[444] **KÜZECİ**, s. 244; **AŞIKOĞLU**, s. 166; **UNCULAR** Selen, İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Ankara, Seçkin Yayıncılık, 2014, s. 63.
[445] **YÜCEDAĞ**, "Genel ilkeler", s. 51.

muhafaza edilmesi ile istenilen amaç gerçekleşinceye kadar bu verilerin muhafazası hukuka uygun kabul edilecektir[446].

Kişisel verilerin saklama süresinin sınırlandırılması, yukarıda ifade edilen veri minimizasyonu ilkesi de dahil diğer tüm ilkeler ile de yakından ilişkilidir. Zira gerçek kişilerin verilerinin bir amaç doğrultusunda hukuka uygun olarak işlenmesi durumunda dahi gereğinden uzun bir süre tutulması bir risk taşımaktadır[447]. Bunun yanında bu ilkenin bir başka öneminden de söz edilmektedir[448]: kişisel verilerin muhafaza edilmesine ilişkin kanuni bir saklama süresinin belirlenmemesi, kişisel verileri elde eden veri sorumluları bakımından bu verilerin "ileride kullanılmak üzere" muhafaza edilebileceği düşüncesini ortaya çıkarabilmektedir[449]. Böyle bir düşüncenin, kişisel verileri elde edilen gerçek kişilerin hak ve özgürlüklerine zarar vereceği düşüncesi kaçınılmazdır[450]. Dolayısıyla veri işleme faaliyetlerinin ileride kullanılmak üzere muhtemel ihtiyaçları karşılamak üzere işlenmesi hususunun hukuka aykırılığına KVKK kapsamında yer verilmelidir[451].

Kişisel verilerin işlenmesi, işleme amaçları doğrultusunda artık gerekli değil ise ilgili kişi verilerinin silinmesini talep edebilecektir[452]. Kişisel verilerin işleme amaçları doğrultusunda gereksiz hale gelmesi ya da bu veriler ile ilgili işleme amaçlarının ortadan kalktığı haller, kişisel veri işleme amacının veri sorumlusunca artık gerekmediği ya da kişisel verinin işlenmesi için gereken amaca ulaşılması halinde ortaya çıkabilir[453]. Her ihtimalde, veri sorumlusunun kural olarak saklama süresinin sınırlandırılması ilkesine uygun hareket etmesi gerekmektedir. Nitekim GVKT m. 13/f.2-a ile m. 14/f.2-a'ya göre veri sorumlusu verilerin saklanma sürelerini

---

[446] **AKGÜL**, "Kişisel Verilerin Korunması", s. 132.
[447] **KÜZECİ**, s. 245.
[448] **YÜCEDAĞ**, "Kişisel verilerin işlenmesinde genel ilkeler", İstanbul Üniversitesi Yayınları, İstanbul, ss. 1042-1055, 2020, s. 1054.
[449] **KÜZECİ,** Kişisel Verilerin Korunması, s. 245; **YÜCEDAĞ**, "Kişisel verilerin işlenmesinde genel ilkeler", s. 1054.
[450] **KÜZECİ**, s. 245.
[451] **YÜCEDAĞ**, "Kişisel verilerin işlenmesinde genel ilkeler", s. 1054.
[452] Nitekim GVKT m. 17/f.1, ilgili veri sahibinin kendisi ile ilgili tutulan verileri hakkında veri sorumlusuna başvurarak bu verilerin silinmesini talep etme hakkı olduğunu ifade etmektedir. Buna ek olarak veri sorumlusu da m. 17/f.1'de yazılı sebeplerden birinin varlığı halinde herhangi bir gecikmeye mahal vermeksizin kişisel verileri silmekle yükümlü olmaktadır. Benzer şekilde KVKK m. 7/f.1'de ilgili kanun hükümlerine göre işlenmiş verilerin, işleme amaçlarının kalmaması üzerine resen ya da veri sahibinin talebiyle veri sorumlusunca silinmesini, yok edilmesini ya da anonim hale getirilmesi gerektiğini ifade etmektedir. Görüldüğü üzere gerek KVKK gerek Tüzük bakımından, işleme amaçlarının ortadan kalmaması halinde verilerin silinmesi veri sorumlusunu yükümlü kılmaktadır. Tüzüğün 17. maddesinin 1. fıkrasının a bendi gereği veri sahibinin kendisi ile ilgili tutulan kişisel verilerin silinmesini isteme, KVKK m. 11/f.1-e 'de yer alır.
[453] **KÜZECİ**, s. 245.

belirlemeli, bu süreyi belirlemesinin mümkün olmadığı hallerde sürenin belirlenmesi ile ilgili gerekli kriterlere yer vermelidir. Görüleceği üzere Tüzük kapsamında veri sorumlusunun saklama sürelerine ilişkin ilgili veri sahibini bilgilendirme yükümlülüğü bulunmaktadır. Oysa KVKK bakımından saklama süreleri ile ilgili bilgilendirme yükümlülüğü veri sorumlusunun bir yükümlülüğü olarak düzenlenmemiştir. Ancak Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in veri saklama ve imha politikası başlıklı m. 6/f.1-g hükmü, verilerin muhafaza ve imha sürelerini gösterir tabloya yer verilmesi gerektiğini ifade etmektedir. Kanaatimizce, Tüzük hükümlerine uyumlaştırma bakımından değerlendirildiğinde veri sorumlusunun saklama sürelerine ilişkin ilgili veri sahibini bilgilendirme yükümlülüğü, Yasada yer almayan hükümlerin Yönetmelik ile düzenlenmesi yerine KVKK kapsamında yer almalıdır.

G. BÜTÜNLÜK VE GİZLİLİK

GVKT m. 5/f.1-f'ye göre, kişisel verilerin yetkisiz erişimlere, kanuna uygun olmayan işleme faaliyetlerine, kazara kayıp olma ihtimallerine, tahribe ya da imhaya karşı gerekli teknik ve idari tedbirlerin alınması gereklidir. Bu anlamda "bütünlük ve gizlilik" ilkesi ile ifade edilen, kişisel verilerin güvende olması anlamını taşır[454]. Dolayısıyla veri sorumluları kişisel verilerin bütünlüğünün ve gizliliğinin bozulmaması için gerekli tedbirleri almakla ve veri sahibinin talebi halinde bu gerekli tedbirleri aldıklarını belgelendirmekle yükümlüdürler.

KVKK'nın "genel ilkeler" başlıklı 4. maddesine bakıldığında "bütünlük ve gizlilik" ilkesinin bu ilkeler kapsamında yer almadığı görülmektedir. Bununla birlikte "bütünlük ve gizlilik" kavramı, KVKK m. 12'de ayrı olarak düzenlenmiştir.

Veri sorumlusu, kendi namına ya da bir gerçek ya da tüzel kişiye verileri işletirse yukarıda ifade edilen m. 12/f.2'ye göre veri işleyenlerle birlikte müştereken sorumluluğu doğmaktadır. Veri sorumlusu, KVKK'nın uygulanmasını sağlamak adına m. 12/f.3 gereği gerekli denetimleri de yaptırmakla yükümlüdür. Veri sorumlusu m. 12/f.4 gereği bütünlük ve gizlilik ilkesinin bir gereği olarak kişisel verileri işlenen gerçek kişiler hakkında öğrendiklerini KVKK'ya aykırı olarak başkalarına açıklayamadığı gibi bu verileri işleme amaçları dışında da kullanamaz. Kanun'un 2.

[454] **YÜCEDAĞ**, "Kişisel verilerin işlenmesinde genel ilkeler", s. 1048.

maddesinin son fıkrasına göre, işlenen verilerin hukuka aykırı şekilde üçüncü kişilerce elde edilmesi durumunda veri sorumlunun iş bu hususu derhal veri sahibine ve Kurula bildirme yükümlülüğü bulunmaktadır. Her ne kadar yukarıda ifade edildiği üzere KVKK m. 12'de veri güvenliğine ile ilgili veri sorumlusunun yükümlülükleri belirtilmişse de kanaatimizce Tüzük ile uyumlu olacak şekilde genel ilkelerden olan bütünlük ve gizlilik ilkesine veri güvenliğinin önemi bakımından KVKK kapsamında yer verilmesi gereklidir[455].

H. HESAP VERİLEBİLİRLİK

Hesap verilebilirlik (accountability) ilkesi ilk kez GVKT m. 5/f.2'de düzenlenmiştir[456]. Madde hükmüne göre veri sorumluları, kişisel verilerin işlenmesine ilişkin olarak Tüzük m. 5/f.1'de ifade edilen ilkelere uygun davrandığını ispatla yükümlüdürler. Dolayısıyla veri sorumlularının verilerin işlenme amaçlarına göre hareket etme ve talep edildiğinde bu yönde işlemler yaptığını belgelendirme yükümlülüğü bulunmaktadır. KVKK'nın "genel ilkeler" başlıklı 4. maddesine bakıldığında "hesap verilebilirlik" ilkesinin genel ilkeler kapsamında yer almadığı görülmektedir. Ancak "bütünlük ve gizlilik" ilkesi ile ilgili ifade ettiklerimiz burada da geçerli olup, hesap verilebilirlik ilkesi de KVKK m. 12'deki veri güvenliği ile doğrudan bağlantılıdır.

Hesap verilebilirlik ilkesi, ilgili kişilerin işlenen verilerine karşı bir güvence ve saydamlık sağlayan, diğer bir ifade ile veri sorumlusunun yükümlülüklerini ağırlaştırmaya ve güven sağlamaya yönelik bir ilkedir[457]. Veri sorumlusu, kişisel verilerini işlediği gerçek kişilere, kişisel verilerin korunması anlamında her türlü teknik ve idari tedbiri aldığını, genel ilkelere uygun hareket ettiğini belgelendirmekle yükümlü tutulmuştur[458]. Nitekim GVKT'nin 24. maddesi de veri sorumlusunun temel yükümlülüklerine değinmektedir. Maddeye göre veri sorumluları, veri işleme faaliyetlerinin kapsam ve amaçlarının dışında veri sahiplerinin hakları açısından olası riskleri hesaba katmak, işleme faaliyetlerini Tüzük kapsamında gerçekleştirmek, bu

[455] **YÜCEDAĞ**, "Kişisel verilerin işlenmesinde genel ilkeler", s. 1055.
[456] Bu konuda daha fazla bilgi için bkz.: **KAYA** Mehmet Bedii, "Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi", 78(4) İstanbul Hukuk Mecmuası, 2020, ss. 1859-1897, s. 1878-1881.
[457] **ÇEKİN**, s.14; **ŞİMŞEK**, s. 16; **KILINÇ**, s. 1111.
[458] **ÇEKİN**, s. 14; **YÜCEDAĞ**, "Kişisel verilerin işlenmesinde genel ilkeler", s. 1055.

kapsamda gerekli tedbirleri almak ve yeri geldiğinde bu tedbirleri gözden geçirmekle yükümlüdür.

Avrupa Birliği hukukunda hesap verilebilirlik ilkesi ile süregelen tartışmalardan biri, söz konusu bu ilkenin başlı başına bir ilke olarak mı değerlendirilmesi gerektiği yoksa GVKT'nin 5. maddesi kapsamında diğer ilkelere uyulmasını temin anlamında bir ilke olarak mı değerlendirilmesi gerektiği yönündedir[459]. Zira bu ilkenin ne yönde değerlendirileceği, ilkeye uyulmaması anlamında ortaya çıkacak yaptırımları da belirleyecektir. Bir diğer ifade ile bu ilkenin başlı başına ayrı bir ilke olarak değerlendirilmesi durumunda uygulanacak yaptırım, diğer ilkelere uygunluk sağlanmış olsa dahi işlenen verilerin hukuka aykırı olması anlamına gelecektir[460]. Oysa söz konusu ilkenin genel ilkeleri tamamlayıcı niteliğinde kabul edilmesi halinde tek başına bir yaptırım söz konusu olmayacaktır[461]. Doktrin bu yönde tartışmaları sürdürmekte ise de bizim de katıldığımız görüşe göre, kişisel verilerin korunması anlamında ortaya çıkacak ihlal ve zararları minimize etmek adına hesap verilebilirlik ilkesinin başlı başına bağımsız bir ilke olarak kabul edilmesi gereklidir[462]. Böylece kişisel verilerin işlenmesi anlamında veri sorumlularının yükümlülükleri dahilinde kişisel verilerin koruma mekanizması artırılmış olacaktır. Ancak hesap verilebilirlik ilkesinin genel bir ilke olarak hukukumuzda kabulü halinde, bu ilkeye ilişkin gerekli düzenlemelerin KVKK'ya eklenmesi ya da veri koruma etki değerlendirilmesi, veri sahibine ve denetleme makamlarına bildirim gibi var olan düzenlemelerin revize edilmesi gerektiği ifade edilmiştir[463].

[459] **KAYA**, s. 1883.
[460] **KAYA**, s. 1883.
[461] **KAYA**, s. 1883.
[462] **KAYA**, s. 1883.
[463] **YÜCEDAĞ**, "Kişisel verilerin işlenmesinde genel ilkeler", s. 1055.

IV. UYUMLAŞTIRMA KAPSAMINDA VERİ SORUMLUSUNA VE VERİ İŞLEYENE DÜŞECEK EK GÖREV VE YÜKÜMLÜLÜKLER

A. VERİ KORUMA TEMSİLCİSİ (DPR) ATAMA YÜKÜMLÜLÜĞÜ

GVKT'nin "Tanımlar" başlıklı 4. maddesine göre temsilci (representative), Birlik içerisinde kurulu bulunan ve Tüzük m. 27'ye göre veri sorumluları ve/veya veri işleyenlerce yazılı olarak belirlenen ve Tüzük kapsamındaki yükümlükleri ile ilgili olarak veri sorumlusu ya da veri işleyenleri temsil eden gerçek kişi ya da tüzel kişi şeklinde ifade edilmiştir. Temsilci, işleme faaliyetlerinin tümünde Tüzük hükümlerine uygunluğun gerçekleştirilmesi için, denetim makamları, veri sorumluları ve veri işleyenler tarafından yetkilendirilmektedir.

GVKT'nin 27. maddesinin 1. fıkrasına göre, veri sorumluları ya da veri işleyenlerin Avrupa Birliği sınırları içerisinde bir kuruluşu bulunmadığı hallerde veri sorumluları ya da veri işleyenler Birlik içerisinde bir temsilci belirlemekle yükümlüdürler. Avrupa Veri Koruma Kurulu'nun coğrafi kapsam üzerine yayımladığı rehberin[464] 27. Maddesinde ise veri koruma temsilcilerinin nasıl atanacağı, temsilcilerin sorumlulukları ve yükümlülükleri belirtilmiştir[465].

KVKK bakımından, veri koruma temsilcisi kavramına yer verilmediği görülmektedir. Bununla birlikte ikamet etmeyen veri sorumluları ve veri işleyenler bakımından temsilcisi atama yükümlülüğü, "Veri Sorumluları Sicili Hakkında Yönetmelik" ile düzenlenmiştir. Yönetmeliğe göre temsilci, Türkiye'de ikamet etmeyen veri sorumlularını temsil edecek, Türkiye'de ikamet eden yetkili gerçek bir kişiyi ya da tüzel kişiyi ifade etmektedir.

Veri Sorumluları Sicili Hakkında Yönetmeliği m. 5/f.1-b'ye göre Türkiye'de ikamet etmeyen veri sorumluları, işleme faaliyetlerine başlamadan temsilci aracılığıyla Sicile kaydolmalıdır. O halde Türkiye dışında yerleşik olmakla, Türk vatandaşlarının ve/veya Türkiye'de mukim yabancıların kişisel verilerini toplayan veri sorumluları bakımından atanacak veri koruma temsilcisinin Türkiye'de ikamet eden bir Türk vatandaşı ya da bir tüzel kişiliğe sahip olması gerekmektedir[466]. Zira her ne kadar

---

[464] **Avrupa Veri Koruma Kurulu (EDPB),** GVKT'nin Bölgesel Kapsamı, s. 19. vd.
[465] **Avrupa Veri Koruma Kurulu (EDPB),** GVKT'nin Bölgesel Kapsamı, s. 19 vd.
[466] Bu konuda bkz. Kişisel Verileri Koruma Kurulu'nun 23 Temmuz 2019 Tarih ve 2019/225 Sayılı Kararı, **ULUSEL /BOZKURT /DEMİREL**, Kişisel Verileri Koruma Kurulu Kararları, s.62.

KVKK kapsamında veri koruma temsilcisi atanmasına ilişkin bir hüküm yer almasa da mütekabiliyet esasına dayalı olarak yasal mevzuatımız açısından da Türk vatandaşları ve/veya Türkiye'de mukim yabancı kişilerin verilerini toplayan Türkiye'de yerleşik olmayan veri sorumlularının kişisel veri işleme faaliyetleri bakımından da uygulanacağı Kişisel Verileri Koruma Kurumu ("Kurum") tarafından kabul edilmektedir[467]. Doktrin veri sorumlusu temsilcisine yapılan atıfların AB düzenlemelerinde yer alan ifadelerle benzerlik gösterdiğini ifade etmektedir[468]. Kanaatimizce KVKK'da temsilcinin kim ya da kimler olabileceği ya da hangi şartlarda temsilci atanacağına ilişkin şartların düzenlenerek AB düzenlemelerine uygun bir hüküm eklemek gereklidir[469].

B. ORTAK VERİ SORUMLULARININ İŞ BÖLÜMÜ ANLAŞMASI YAPMA YÜKÜMLÜLÜĞÜ

Kişisel verilerin işlenme faaliyetlerinde birden fazla veri sorumlusunun bir araya gelerek aralarında belirleyecekleri bir sözleşme ile yetki ve sorumluluklarını paylaşmaları durumunda "ortak veri sorumlusu" kavramının ortaya çıktığını ifade etmiştik[470]. Ortak veri sorumluları, Tüzük kapsamında doğan yükümlülükleri bakımından işbirliği içinde hareket etmekle yükümlüdür.

Ortak veri sorumluları bir araya gelerek kendi aralarında belirledikleri "ortak amaç" dahilinde kişisel verilerin işlenmesine müştereken karar verirler[471]. Ortak veri sorumluları, sorumluluk paylaşımını, yapacakları iş bölümü anlaşması ile ortaklaşa belirleyebilecekleri gibi farklı şekilde de belirleyebilmektedirler[472]. Ancak belirtmek gerekir ki, GVKT m. 26 gereği ortak veri sorumlularının aralarında yapacakları bu

---

[467] **Kişisel Verileri Koruma Kurumu,** 6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar, s. 16. https://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20Y%C3%96NEL%C4%B0K%20SORU%20VE%20CEVAPLAR.pdf (Son Erişim Tarihi: 13.10.2021.

[468] **KÜZECİ,** s. 367.

[469] **KÜZECİ,** s. 367.

[470] İkinci Bölüm, Kişisel Verileri Koruma Kanununun AB Genel Veri Tüzüğü'ne Uyumlaştırması Bakımından Ele Alınması Gereken Kavramlar, I. AB Veri Koruma Tüzüğü ile Mevzuatımızdaki Kavram Farklılıkları, B. Tüzüğün Veri İşleme Faaliyetini Yürütenler Bakımından Farklılıkları, 2. Ortak Veri Sorumlusu (Joint Controllers) Bakımından, s. 57.

[471] **KÜZECİ,** s. 365; **29. Madde Çalışma Grubu**, WP 136, s. 22; **ÇELİKEL**, s. 87; **GVKT**, m. 4/7, m. 26; **DÜLGER**, "Ortak Veri Sorumlusu", s. 1.

[472] **GVKT**, Resital 79.

sözleşmeden kişisel verileri işlenen ilgili kişilerin bilgilendirilmeleri gerekmektedir. GVKT'nin 26. maddesinde ortak veri sorumlularına ilişkin getirilmiş bu bilgilendirme yükümlülüğü ile ilgili veri sahibi kişilerin bilgilendirilme hakkının sağlanmasında açık ve şeffaf olmaları gerektiği de ifade edilmiştir[473]. Görüldüğü üzere Tüzük, ortak veri sorumlularının aralarında yapacakları iş bölümü anlaşmasına büyük bir önem atfetmekte ve ortak veri sorumlularının veri işleme faaliyetleri kapsamında ilgili veri sahiplerini açık ve şeffaf bir biçimde bilgilendirmeleri gerektiğinin altını çizmektedir.

KVKK kapsamında ise "ortak veri sorumlusu" kavramına yer verilmediğini ancak doktrinde, KVKK'nın ortak veri sorumlusu kavramına yer vermemiş olmasının bu kavramı kabul etmemiş şeklinde anlaşılmayacağı, zira Kanun'da "tek başına" ifadesinin de şart koşulmadığı ifade edilmiştir[474]. Kanaatimizce de Kanunumuz açısından da birden fazla veri sorumlusu bir araya gelerek ortak amaçları dahilinde veri işleme faaliyetlerine ilişkin iş bölümü sözleşmesi yapabilmelidir.

C. VERİ İŞLEYENLERİN SEÇİMİ İLE İLGİLİ YÜKÜMLÜLÜKLER

Veri sorumlularının kişisel verileri işlemeleri adına görevlendirecekleri veri işleyenler ile ilgili olarak, gerçek kişilerin kişisel verilerini korumak adına göz önünde bulundurması gereken bazı hususlar söz konusudur[475]. GVKT'nin 28. maddesi, veri sorumlularının veri işleyenlerin görevlendirmelerini gerçekleştirirken işleme faaliyetlerinin Tüzüğe uygunluğunu sağlamak, veri sahiplerinin haklarını korumak ve bu kapsamda gerekli tedbirleri almakla yükümlü olduklarını ifade etmiştir. Dolayısıyla veri sorumlularının veri işleme faaliyetleri ile ilgili kendi adlarına veri işleyen belirlemeleri durumunda Tüzük gerekliliklerine uygun, kişisel verileri işlenen kişilerin hak ve özgürlüklerini koruyan ve bu konuda gerekli teknik ve idari güvenceler sağlayan veri işleyenler belirlemeleri gerekir. Veri sorumluları ve veri işleyenler, işleme faaliyetleri kapsamındaki sorumlulukları ile yükümlülüklerini Tüzüğün m. 28/f.3'e göre bir sözleşme kapsamında belirlemelidirler[476].

Veri sorumlusu tarafından görevlendirilen veri işleyen, aldığı talimatlar doğrultusunda verileri işleyen ve bu işleme faaliyetleri aşamasında işlemenin daha

[473] **DÜLGER**, "Ortak Veri Sorumlusu", s. 2.
[474] **DÜLGER**, "Ortak Veri Sorumlusu", s. 1; Ayrıca bu konudaki eleştiriler için bkz. **ÇELİKEL**, s. 164.
[475] **DÜLGER**, s. 141-142.
[476] **DÜLGER**, s. 142.

ziyade teknik kısımları ile ilgilenen kişi olarak görev yapmaktadır. Bu noktada veri sorumluları, veri işleyenin işlenecek kişisel verileri koruma, verilen talimatlar doğrultusunda işleme gerçekleştirme ve gerekli teknik ve idari tedbirleri alabilme yeteneklerini dikkate almalı ve veri işleyenin seçiminde özenli davranmalıdır[477]. Ancak veri sorumlusunun iş bu hususlara dikkat ederken veri işleyen ile ilgili hangi denetim ve kontrolleri sağlaması gerektiği gerek Tüzük gerek KVKK kapsamında belirtilmemiştir.

Veri işleme faaliyetlerinin daha çok teknik yönü ile ilgilenen veri işleyenin kişisel verilerin işlenmesi ile ilgili veri işlemenin gizliliği ve güvenliği anlamında uyması gereken yükümlülükler bulunmaktadır. Nitekim GVKT'nin "Tazminat Hakkı ve Sorumluluk" başlıklı 82. maddesinde, veri işleyenin yükümlülüklerini ihlal etmesi halinde doğrudan sorumlu tutulabileceği düzenlenmiştir. Görüleceği üzere GVKT'nin yürürlüğe girmesi ile veri işleyenin rolü son derece önem kazanmış ve veri işleyenin yükümlülükleri veri sorumlusu kadar önemli bir hale gelmiştir[478]. Bu noktada gerekli niteliklere sahip veri işleyenlerin seçimi ile ilgili veri sorumlusuna yüklenen sorumluluğun tek başına yeterli olmamakta, veri işleyenin bu niteliklerini veri işleme faaliyetlerinin sonuna kadar sürdürmesi gerekmektedir[479]. Ancak Tüzük bu niteliklerin devamlılığını kontrol açısından, veri sorumlusunun veri işleyeni ne aralıklarla ve ne şekilde denetleneceğine ilişkin bir hüküm barındırmamaktadır. Doktrin, veri sorumlularının keyfi denetlemelerinin önüne geçebilmek ve kontrollerinin amacını aşmamaları adına veri işleyenle aralarında yapılan sözleşme ile tüm bu hususların açık bir şekilde belirtilmesi gerektiği ifade edilmektedir[480].

D. VERİ İŞLEME KAYITLARI İLE İLGİLİ EK YÜKÜMLÜLÜKLER

GVKT'nin 30. maddesine göre veri sorumluları ve varsa yasal temsilcileri, kendi sorumluluğu altındaki veri işleme faaliyetlerinin kayıtlarını tutmakla yükümlüdür. GVKT m. 30/f.2'ye bakıldığında ise veri sorumlusu namına veri işleyen

[477] **DÜLGER**, s. 143.
[478] **RODWAY** Suzanne/**CAREY** Peter, "Outsourcing Personel Data Processing", Data Protectıon: A Practical Guide to UK and EU Law, Ed: Peter CAREY, 5. Baskı, Oxford University Press, 2018, Oxford, ss. 177-179; **DÜLGER**, s. 142.
[479] **DÜLGER**, s. 144.
[480] **DÜLGER**, s. 144; **ÇEKİN**, s. 127.

ve varsa temsilcilerinin işleme faaliyetleri için kayıt tutma yükümlülükleri ifade edilmiştir.

Veri işleme faaliyetleri ile ilgili tutulacak kayıtların elektronik ortamlar da dahil olmak üzere yazılı olarak tutulması gerektiği, veri sorumlusunun ve veri işleyenin ya da temsilcilerinin talep edilmesi halinde iş bu kayıtları denetim makamlarına sunmakla yükümlü oldukları GVKT m. 30/f.3'de ifade edilmiştir. Maddenin son fıkrası, veri işleme faaliyetlerine ilişkin kayıt tutma yükümlülüğünün istisnalarını ifade etmiştir.

KVKK kapsamında bir mukayese yapıldığında, veri kayıt sistemi ile ilgili bazı değerlendirmelerin yapılması önem taşımaktadır. Kanun açısından veri işleme faaliyetlerinin kaydının tutulması açısından yükümlülük sadece veri sorumlularına yöneltilmiştir. Bu açıdan önemli bir farklılık GVKT'nin işleme faaliyetlerinin kaydının tutulmasını veri işleyenler için ayrı olarak düzenleyen m. 30/f.2'nin KVKK kapsamında yer almamış olmasıdır. Buna karşın KVKK m. 3/f.1-h veri kayıt sisteminin ne olduğu tanımlanmıştır. Böyle bir tanımlamanın yer almasının nedeni şüphesiz KVKK bakımından veri sorumlularının, Veri Sorumluları Siciline kaydolma zorunluluklarının bulunmasıdır.

Bununla birlikte KVKK m. 16/f.2'de, işleme faaliyetlerinin kanundan kaynaklanması, üçüncü kişilere aktarım ya da Kurulun belirlediği kriterler dikkate alınarak sicile kayıt zorunluluğuna istisna olan durumlar ifade edilmiştir. Dolayısıyla Tüzük hükümlerinden farklı olarak KVKK kapsamında yer alan veri sorumlarının verileri spesifik kriterlere göre yapılandırılarak işlediği veri kayıt sistemi ile VERBİS adı verilen ortak bir sicile kaydolma zorunlulukları şeklinde ek bir yükümlülükleri olduğunu ifade etmek gerekir.

1. Veri İşleme Sözleşmesi

GVKT'nin 28. madde kapsamında veri sorumluları ile veri işleyenlerin görevlendirilmeleri ve yetkilendirmeleri hususlarında, veri işleme faaliyetlerine ilişkin aralarında bir sözleşme akdetmeleri gerektiğine de işaret edilmiştir[481].

[481] **DÜLGER**, s. 142; **Kişisel Verileri Koruma Kurumu,** Veri Sorumlusu ve Veri İşleyen, s. 2; **YILMAZ**, "KVKK Uyum Sorunsalı: "Veri Sorumlusu ve Veri İşleyen Kavramlarını İyi Anlamak", 14/05/2020, Lexpera Blog.

GVKT m. 28/f.3'te ayrıntılı olarak düzenlenen veri işleme sözleşmesi, veri işleyenlerin, veri sorumlularından aldıkları emir ve talimatlar doğrultusunda veri işleme faaliyetlerini gerçekleştireceklerini taahhüt ettikleri, veri sorumlularının da veri işleyenlerin bu iş görme edimleri karşılığında bir ücret ödemeyi taahhüt altına aldıkları sözleşme olarak tarif edilmektedir[482]. Bu anlamda veri işleyenler ile veri sorumluları arasında akdedilecek veri işleme sözleşmesine kavram olarak KVKK'da yer verilmemiştir. Ancak Kurumun Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi'nde (Kısaca KVKK Uygulama Rehberi) veri işleyenlerin kendilerine verilen görev ve talimatlar kapsamında veri sorumlulukları ile bir veri işleme sözleşmesi yapmak üzere yetkilendirilen kişiler olarak tanımlanmıştır[483].

KVKK kapsamında veri işleme sözleşmesi ile ilgili olarak şekil şartı öngörülmemiş olmakla birlikte sözleşmenin uygulamada yazılı olarak düzenlendiği görülmektedir[484]. Ayrıca Kanun m. 9/f.2-b gereği yeterli korumanın bulunmaması halinde yabancı ülkelere kişisel veri aktarımının söz konusu olduğu hallerde gerek Türkiye'de gerek ilgili yabancı ülkede yer alan veri sorumlularının gerekli korumayı sağlanacaklarını yazılı olarak gerçekleştirmesi ve Kurulun bu konuda izninin gerekli olduğu ifade edilmiştir. Kısaca, kişisel verilerin yurtdışına aktarımının söz konusu olduğu hallerde kişisel veri işleme sözleşmelerinin yazılı olarak yapılması gerektiği sonucuna ulaşılmaktadır[485].

GVKT m. 28/f.3'te, veri sorumlusu ile işleyenler arasında yapılacak veri işleme sözleşmesinde işleme faaliyetleri, işlemeye konu olan veri öznesi grupları ile veri kategorileri, veri sorumlusunun yükümlülükleri gibi hususları içermesi gerektiği detaylı olarak ele alınmıştır[486]. GVKT m. 28/f.3'e ek olarak veri sorumlusu ile veri işleyen arasında yapılacak sözleşmede ayrıca Tüzük kapsamında uyulması gereken yükümlülüklere ilişkin alınacak tedbirlere, veri işleyenlerin ilgili veri öznesinin hak ve sorumluluklarının yerine getirilmesi noktasında veri sorumlusu ile aralarında yapılacak işbirliğine, kişisel verilerin veri sorumlusunun talimatları doğrultusunda işleneceğine ilişkin taahhütlere, işleme faaliyetlerindeki gizlilik yükümlülüklerine, alt işleyicinin

---

[482] **BAŞARA**, s. 58; **ÇELİKEL**, s. 167;
TAŞTAN Furkan Güven, "Bir Modern Sözleşme Tipi Olarak Kişisel Veri İşleme Sözleşmesi ve Kanun'a Uyum Sürecindeki Rolü", Lexpera Blog, 2018, https://blog.lexpera.com.tr/kisisel-veri-isleme-sozlesmesi/ (Son Erişim Tarihi: 06.11.2022).
[483] **Kişisel Verileri Koruma Kurumu,** "KVKK Uygulama Rehberi", s. 56.
[484] **ÇELİK**, s. 12; Veri işleme sözleşmesinin hukuki niteliği ve Türk Borçlar Hukukundaki yerine ilişkin ayrıntılı bilgi için ayrıca bkz. **TAŞTAN**, s. 112 vd.
[485] **BAŞARA**, s. 69.
[486] **DÜLGER**, s. 145.

varlığı durumunda bu hususta veri sorumlusundan alınması gereken onaya, kişisel verilerin işlenme amaçlarının gerçeklemesi ile verilerin silinmesine ilişkin açıklamalara, veri sorumlusu ile yukarıda ifade edilen hükümlere uyulup uyulmadığına ilişkin gerekli denetimlerin yapılacağına yer verilmesi gerektiği ifade edilmiştir[487].

2. Veri İhlali Açıklaması ve Bildirimi

GVKT'nin "Tanımlar" başlıklı 4. maddesinin 12. fıkrasına göre veri ihlali kavramı, aktarımı gerçekleşen, muhafaza edilen veya başka yollarla işleme faaliyetine konu olan verilerin kazara ya da hukuk kurallarına aykırı olacak şekilde silinmesi, yok edilmesi, kaybolması, değiştirilmesi, ifşa edilmesi ya da hukuka aykırı bir biçimde ele geçirilmesine sebebiyet veren güvenlik ihlali olarak ifade edilmektedir.

GVKT'nin 33. maddesinin 1. fıkrasına göre, kişisel verilerin ihlali söz konusu olduğunda ve veri ihlalinin ilgili kişinin haklarına risk teşkil etmesi durumunda veri sorumlularının gecikmeye mahal vermeksizin ve mümkün ise veri ihlalini öğrenir öğrenmez en geç 72 saat içinde söz konusu ihlali GVKT m. 55. uyarınca denetim makamlarına bildirmesi gerektiği ifade edilmiştir[488]. GVKT m. 33/f.1 devamında söz konusu veri ihlali bildiriminin 72 saat içerisinde yapılamadığı hallerde bu gecikmenin sebeplerinin de bildirilmesi gerektiği ifade edilmiştir. Ayrıca m. 33/f.2'de veri işleyenler de kişisel veri ihlalini öğrendikten itibaren herhangi bir gecikmeye mahal vermeksizin bu durumu veri sorumlularına bildirmekle yükümlü tutulmuşlardır.

GVKT'nin "Veri ihlalinin ilgili veri sahibi kişiye iletilmesi" başlıklı 34. maddesinde, söz konusu veri ihlalinin veri sahibi kişiye bildirilmesi gerektiği ifade etmektedir. İlgili veri sahibi kişiye yapılacak bu bilgilendirme açık ve anlaşır bir dil kullanılarak yapılmalıdır.

GVKT'nin "Veri ihlalinin ilgili kişiye bildirilmesi" başlıklı 34. maddesinin 3. fıkrasına göre de veri sorumlusunun, gerekli tedbirleri alarak söz konusu verilerin kişisel verilere erişim yetkisi bulunmayan kişilere karşı korunması amacıyla, herkesçe okunamaz hale gelecek şifreleme yöntemlerini uygulamış olması; ilgili kişilerin haklarına yüksek risk oluşturmasına engel olacak ilave tedbirler alması gerekmektedir.

---

[487] **RODWAY/CAREY**, s. 180.
[488] **DEVELİOĞLU**, s. 108.

Veri sorumlusu tarafından yapılacak bildirimin aşırı bir çabayı gerektirecek olması durumunda bildirim yükümlülüğü ortadan kalkmaktadır.

KVKK'ya bakıldığında ise m. 12/f.5 ile kişisel verilerin ihlalinin söz konusu olduğu durumlarda Kurul'a ve ilgililere yapılacak bildirim ile veri sorumlularının yükümlülüğü düzenlemiştir. Madde hükmünde, işlemeye konu olan verilerin hukuka uygun olmayacak yöntemlerle üçüncü kişilere geçmesi halinde, veri sorumlusu bu ihlali öğrenir öğrenmez en kısa sürede ilgili veri sahibi kişiye ve Kurula bildirmelidir. Söz konusu veri ihlaline ilişkin durumu gerekli gördüğü durumda Kurul kendi internet sitesi üzerinden farklı bir yöntemle duyurabilir. Bu noktada belirtilmesi gereken husus Tüzük hükümlerinden farklı olarak Kanun'un 12. maddesinin 5. fıkrası, veri ihlalinin öğrenilmesinden itibaren ilgili veri sahibine ve Kurul'a bildirimde bulunma süresinin ne kadar olduğuna yer vermemiş olduğudur. Ancak Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulu'nun 24 Ocak 2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyurunda[489], KVKK m. 12/f.5'teki "en kısa sürede" ifadesinin, GVKT'nin 33. maddesi ile uyumlu olması amacıyla 72 saat olarak yorumlanması veri sorumlularının söz konusu ihlali öğrenir öğrenmez ve hiç geciktirmeden 72 saat içinde Kurul'a bildirimde bulunması gerektiği ifade edilmiştir. Ayrıca verilerin ihlali sonucu hakları ya da menfaatleri zedelenen kişilerin belirlenmesiyle, bu kişilere de gerekli bilgilendirmenin yapılmasını, veri ihlali ile ilgili veri sahibi kişilere ulaşılamaması durumunda veri sorumlusunun kendi internet sitesi aracılığı ile bunu duyurması gerektiğine yer verilmiştir. Buna ek olarak Tüzük hükümlerine uyumlu olacak şekilde ve veri sorumlusu bu bildirimi ilgili süre içerisinde yapamazsa, yapılacak ayrı bir bildirimle gecikmenin nedenlerinin Kurul'a açıklanması gerektiği ifade edilmiştir. Kurul'a yapılacak bildirim formunda yer alması gereken bilgilerin tamamının temininin sağlanamadığı durumlarda da Tüzük m. 33/f.4'te yer aldığı gibi bilgilerin aşamalı olarak iletilmesinin mümkün olduğu ifade edilmiştir. Kurul kararında veri işleyenler yönünden de Tüzük m. 33/f.2'ye uyumlu olarak veri ihlalinin gerçekleştiğinin öğrenilmesinden itibaren en kısa sürede veri sorumlusuna gerekli bildirimlerim yapılması gerektiği belirtilmiştir. Elbette Kurul'un 2019/10 Sayılı Kararında yer alan bu hususların KVKK kapsamında düzenlenmesi gerektiği açıktır[490].

---

[489] Kişisel Verileri Koruma Kurulu'nun 24 Ocak 2019 Tarih ve 2019/10 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (Son Erişim Tarihi:02.08.2021).
[490] **ÇELİKEL**, s. 117; **ÇEKİN**, s. 207.

E. TASARIM VE GİZLİLİK İLE VARSAYILAN GİZLİLİK DAHİL OLMAK ÜZERE TEKNİK TEDBİRLER ALMA YÜKÜMLÜLÜĞÜ

Teknolojinin ilerlemesi ile bilginin değeri her geçen gün artmakta, bununla birlikte bilgiyi doğru bir şekilde yönetme ihtiyacı da aynı doğrultuda önem kazanmaktadır. Bilginin sağladığı fayda ve kolaylıklardan yararlanırken özellikle dijital ortamlarda ifade şeklimizi ortaya koyan seçimlerimiz de önem kazanmaktadır. Giderek dijitalleşen dünyada, kişisel verilerin korunması anlamında mahremiyetin korunmasının daha da gerekli olduğunu savunan görüşler de artmaktadır[491]. Bu anlamda veri sorumlularının da kişisel verilerin korunması ve mahremiyet için gereken sorumluluğu ciddiye almaları son derece önem kazanmaktadır.

Veri korumanın ve mahremiyetin korunmasına yönelik bu görüşler ile ifade edilen iki önemli veri koruma ilkesi bulunmaktadır. Uygulamada "mahremiyeti teşvik eden teknolojiler"[492] olarak ifade edilen ve kişisel verilerin korunması anlamında iki önemli ilkeyi barındıran yaklaşım Tüzük m. 25 kapsamında yer almaktadır. Tasarım ile Gizlilik (Privacy by Design) olarak ifade edilen ilk ilke ile Varsayılan Gizlilik (Privacy by Default) şeklinde ifade edilen ikinci ilke, kişisel veriler üzerine herhangi bir ihlal gerçekleşmeden ya da böyle bir ihlalin gerçekleşmesini beklemeden, kişisel veri koruma hukukunun esaslarının dikkate alınmasını sağlamayı amaçlar[493]. Bir diğer ifade ile burada önemli olan kişisel verilerin ihlalinin oluşumunu baştan itibaren engellemek ve bireylerin rızasına önem vermektir[494]. Nitekim ileride ayrıntılı olarak ele alınacağımız üzere GVKT m. 25 ile getirilen temel yükümlülük de veri koruma ilkelerinin ve ilgili veri sahibi gerçek kişilerin hak ve özgürlüklerinin tasarım ve varsayılan gizlilik ilkeleri kapsamında etkin bir şekilde uygulanması iken, bu konuda gerekli teknik ve idari tedbirlerin alınmasını da sağlamaktır[495]. Tasarım ile gizlilik ve

---

[491] **ÇEKİN**, s. 12.
[492] **ÇEKİN**, s. 12.
[493] **ÇEKİN**, s. 13.
[494] **ÇEKİN**, s. 13.
[495] **29. Madde Çalışma Grubu,** WP 248, s.6; **GVKT**, Resital 78'de de ifade edildiği üzere veri sorumluları, özellikle tasarım ile gizlilik ve varsayılan gizlilik ilkelerini karşılayan iç politikalar benimsemeli ve tedbirler almalıdır. Bu tür tedbirler, diğerlerinin yanı sıra, kişisel verilerin işlenmesini en aza indirmek, kişisel verilerin mümkün olan en kısa sürede takma adlı hale getirilmesi, kişisel verilerin işlevleri ve işlenmesi ile ilgili şeffaflık, veri sahibinin veri işlemeyi izlemesine olanak sağlamak gibi tedbirler içermelidir. Veri işleme faaliyetlerine dayanan ya da kişisel verileri işleyen uygulama, hizmet ve ürünleri geliştirirken, tasarlarken, seçerken ve kullanırken, ürün, hizmet ve uygulama geliştiricilerin veri koruma politikalarını dikkate almaları teşvik edilmelidir.

varsayılan gizlilik ilkelerine KVKK'da yer verilmemiştir. Ancak bu konu ile ilgili değerlendirmelerimize aşağıda yer vereceğiz.

1. Tasarım ile Gizlilik (Privacy by Design)

GVKT m. 25/f.1 veri sorumlularının, veri işleme faaliyetlerinin uygulama amaçlarına ek olarak; veri sahiplerinin hakları açısından çeşitli riskleri dikkate alarak işleme faaliyetlerini gerçekleştirildiğini göstermekle yükümlü olduklarını ifade etmektedir.

Tasarım ile gizlilik ilkesi Tüzük tarafından öngörülen veri koruma ilkelerine daha sonradan değil, tasarım aşamasından itibaren uyulması gerektiğini ifade eder[496]. Nitekim tasarım ile gizlilik ilkesi, Ekim 2010 tarihinde veri koruma yetkilileri tarafından yıllık yapılan konferansta oybirliği ile onaylanarak kişisel verilerin korunması anlamında temel gizlilik korumasının esaslı bir unsuru olarak kabul edilmiştir[497]. O tarihten bu yana tasarım ile gizlilik ilkeleri 25 dile çevrilmiş ve dünyanın pek çok yerinde yasal ve düzenleyici bir gereklilik olarak ifade edilmeye başlanmıştır[498].

Veri sorumluları bakımından alınacak bu tedbirler gerek veri işleme faaliyetleri esnasında gerek işleme faaliyetlerinin yöntemlerinin belirlenmesi aşamasında dikkate alınmak durumundadır. Dolayısıyla veri sorumluları bu gerekli teknik ve idari tedbirlerin alınması aşamasında en son ve en güncel teknolojik ilerlemeleri, uygulama, amaçları ile veri sahiplerinin hakları üzerinde doğabilecek riskleri hesaba katmakla yükümlüdür. 29. Madde Çalışma Grubu'nun, 248 No'lu Çalışma Raporunda "risk", bir olayı ve o olaya bağlı sonuçların taşıdığı ciddiyet oranı olarak ifade edilirken "risk yönetimi" ise bir işletmenin taşıdığı risk faaliyetlerinin kontrol edilmesi ve yönlendirilebilmesini sağlayan koordineli faaliyetler olarak tanımlanmıştır. O halde tasarım ile gizlilik ilkesi, Tüzük 25. madde doğrultusunda hem kişisel verileri işleme araçlarını belirlemede hem de veri işleme esnasında veri koruma amaçları ile tutarlı olarak veri minimizasyonu, takma adlandırma kullanması, veri uyumu gibi uygun

[496] **KOOPS** Bert-Jaap/**LEENES** Ronald, "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law", 28 International Review of Law, Computers & Technology (2), Y: 2014, ss. 159-171, s. 159.
[497] **HERT** Paul de/**LEENES** Ronald/**GUTWIRTH** Serge/**POULLET** Yves, European Data Protection: Coming of Age, Chapter 8 Privacy by Design: Leadership, Methods, and Results, **Ann Cavoukian,** Springer, 2013, s. 175.
[498] **HERT/LEENES/POULLET,** s. 175.

teknik ve idari tedbirlerin en baştan itibaren etkili bir biçimde uygulanmasını gerektirmektedir[499].

2. Varsayılan Gizlilik (Privacy by Default)

Varsayılan gizlilik, veri sorumlularının kişisel verilerin işlenmesi noktasında yalnızca belirledikleri amaçlara ulaşmalarına gerekli olan verileri işlenmesi olarak ifade etmektedir[500]. Nitekim GVKT m. 25/f.2, veri sorumlularının kişisel verileri yalnızca belirli işleme amaçları dahilinde işlemesini sağlamaya yönelik gerekli teknik ve idari tedbirler uygulamakla yükümlü olduğunu belirtmektedir. Söz konusu yükümlülük, işleme faaliyetleri kapsamında elde edilen kişisel veri miktarına, bu verilerin işlenme derecesine, bu verilerin saklanma sürelerine ve verilere erişilebilme sürelerine de uygulanmaktadır. Bu anlamda varsayılan gizlilik ilkesinin Tüzük kapsamında yer alan veri minimizasyonu ve amacın sınırlaması ilkeleri ile de bağlantılı olduğu ifade edilebilir[501]. Madde hükmü ayrıca söz konusu alınacak teknik ve idari tedbirlerin ilgili veri sorumlusu gerçek kişilerin müdahalesi olmaksızın, belirsiz sayıda gerçek kişinin erişimine açık olmamasını sağlamak durumundadır.

Veri sorumluları GVKT m. 25/f.2'de yer alan hususları gerçekleştirebilmek için kullanıcılara herhangi bir varsayılan ayar özelliği ile "önce gizlilik" yaklaşımını benimsemeli; işlenen kişisel veriler ile ilgili olarak kişileri yanıltıcı bir seçenek sunulmadığından emin olmalı; gerekmedikçe ve kişilerin onayı olmadıkça ek veri işlememeli; kişiler ayarları bu yönde değiştirmedikçe verilerin otomatik olarak

---

[499] Uygulamada tasarım ile gizlilik kavramının, Ann Cavoukian ile başladığı kabul edilmektedir. Bu anlamda tasarım ile gizlilik ilkesinin uygulanabilmesinde yedi temel ilke olduğu öngörülmüştür. Tasarım ile Gizlilik ilkeleri, cezalandırıcı değil önleyici olma; maksimum veri koruma yaklaşımını gözetecek biçimde varsayılan veri koruma; tasarımı başlangıçtan itibaren bütüncül olarak korumayı ele alan tasarım; kişisel verilerin korunması ve güvenliğini veri işleme faaliyetlerinin bütünü için ele alan tam işlevsellik; uçtan uca güvenlik, görünürlük ve şeffaflık; kullanıcının kişisel verilerine saygı ilkesi şeklindedir. Görüleceği üzere söz konusu ilkeler temel veri koruma ilkelerini vurgulayan ilkeler olarak ifade edilmiştir. **CAREY** Peter, A Practical Guide to UK and EU Law, 5. Baskı, Oxford University Press, İngiltere 2018, s. 26. **LAMBERT,** s. 329; **CAVOUKIAN** Ann, Privacy by Design The 7 Foundational Principles, https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/ (Son Erişim Tarihi: 06.08.2021); **ROST** Martin/**BOCK** Kirsten, "Privacy by Design and the New Protection Goals," İngilizce çevirisinden yararlanılmıştır, "Privacy by Design und die Neuen Schutzziele", Datenschutz und Datensicherheit, Cilt 35, Sayı 1, 2011, s. 31-32- İngilizce çevirisinde s. 2.
[499] von dem **BUSSCHE**, Axel Freiherr/**VOIGT** Paul, The EU General Data Protection Regulation, A Practical Guide, Springer, 2017, s. 63.
[500] **BUSSCHE/VOIGHT**, s. 63.
[501] Madde hükmünde ifade edilen "belirlenen amaç" ifadesi ile amacın sınırlandırılması ilkesi vurgulanırken, elde edilen kişisel veri miktarını, bu verilerin işlenme derecesini, bu verilerin saklanma sürelerine ve verilere erişilebilme süreleri ile de veri minimizasyonu ilkesinin altı çizilmiştir.

başkalarının erişimine açık hale getirilmemesini sağlamalı; ve kişilere haklarını kullanmaları için yeterli kontrol ve seçenekler sunmalıdır[502]. Gizlilik dostu varsayılan ayarlar genellikle, kullanıcıların kendilerini korumak için ilk kullanımda veya sonrasında, aldıkları bir hizmet ya da ürünün ayarlarını değiştirmelerine gerek kalmayacak şekilde maksimum düzeyde gizlilik sağlar. Bir diğer ifade ile kişisel verilerinin daha fazla kullanılmasına veya daha fazla tarafla paylaşılmasına izin vermek için kullanıcılar bu ayarları değiştirmek isterlerse, bu varsayılan ayarları kendileri seçmeli ve değiştirmelidirler[503]. Varsayılan gizlilik ile ayrıca teknik bilgiye sahip olmayan kullanıcıların, özellikle çevrimiçi hizmetlerin ve veri kullanımının çeşitliliği ve karmaşıklığı karşısında da korunmaları hedeflenmektedir[504].

Görüldüğü üzere gerek tasarım ile gizlilik gerek varsayılan gizlilik ilkeleri ile kişisel verilerin herhangi bir veri ihlaline sebep olmadan, en baştan itibaren korunması amaçlanmış, bu anlamda veri sorumlularının kişisel verileri koruma anlamında alması gereken teknik ve idari yükümlülükleri belirtilmiştir. Dolayısıyla, her ne kadar KVKK kapsamında GVKT'nin 25. maddesinde ifade edilen bu iki ilkeye yer verilmemişse de[505] bu ilkelerin KVKK kapsamında da yer alması gerektiği açıktır. Zira söz konusu ilkelerin benimsenmesi ile Türk hukukunda da kişisel veri ihlallerinin ve hak kayıplarının önüne geçilmede daha ileri adımlar atılabilecektir.

F. VERİ KORUMA ETKİ DEĞERLENDİRMESİ YAPMA VE ÖN İSTİŞAREDE BULUNMA YÜKÜMLÜLÜĞÜ

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün kişisel verilerin korunması anlamında veri sorumlularına çok çeşitli sorumluluklar yüklediği görülmektedir. Söz konusu sorumluluklar özellikle teknolojinin ilerlemesi ile hak ve veri kayıplarının her geçen gün artarak daha riskli hale gelmesi neticesinde önem kazanmaktadır. Dolayısıyla veri sorumluları GVKT'nin 35. maddesi kapsamında yeni teknolojilerin

---

[502] ICO, Guide to the General Data Protection Regulation (GDPR), Data Protection By Design And Default, s. 174.
[503] **BUSSCHE/VOIGHT**, s. 63.
[504] **BUSSCHE/VOIGT**, s. 63.
[505] KVKK kapsamında tasarım ile gizlilik gerek varsayılan gizlilik ilkelerine yer verilmemiş olsa da veri sorumluları ile veri işleyenlerin veri koruma anlamında alması gereken teknik ve idari yükümlülüklerine ilişkin Kurum Veri güvenliğine ilişkin bir rehber yayımlamıştır. **Kişisel Verileri Koruma Kurumu, "**Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)", https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf (Son Erişim Tarihi: 02.11.2022).

kullanıldığı veri işleme faaliyetlerinde, bu faaliyetlerin mahiyeti, kapsamı, bağlamı ve amaçlarını dikkate almalıdır.

Tüzük, veri sorumluları bakımından veri koruma etki değerlendirmesi yapma yükümlülüğünü yeni bir yasal gereklilik olarak getirmiştir. Ancak veri koruma etki değerlendirmesi ya da benzer kavramlar, ICO (Information Commissioner's Office) ve diğer Avrupa denetim makamları tarafından kuruluşların temel veri koruma yükümlülüklerine uyum sağlamalarına yararlı ve yardımcı olmak adına uzun yıllardır teşvik edilmiştir[506].

1. Veri Koruma Etki Değerlendirmesi Yapmak

GVKT m. 35/f.1'e göre güncel ve yeni teknolojik sistemlerin kullanıldığı veri işleme faaliyetlerinin ilgili veri sahiplerinin haklarına yüksek risk oluşturmasının muhtemel olması halinde, veri sorumluları işleme faaliyetlerinden önce öngörülen etkilere ilişkin temel bir değerlendirme yapmalıdır. Bu noktada Tüzük, veri koruma etki değerlendirmesinin ilgili veri sahiplerinin haklarına "yüksek risk oluşturması" ifadesiyle, Direktif'teki işleme faaliyetlerinin denetim makamlarına bildirimine yönelik genel hükümden farklı bir düzenleme getirmiştir. Direktif m. 18'de işleme faaliyetlerinin denetim makamlarına bildirilmesine ilişkin genel bir bildirim yükümlülüğü yer almaktadır[507]. Bu genel bildirim yükümlülüğünde, Tüzük kapsamında yer aldığı gibi yüksek riskli işleme faaliyetine konu olan kişisel veriler gibi bir ayrım yapılmadığı görülmektedir.

95/46/EC sayılı Direktif hükümlerini temel alarak hazırlanan KVKK'ya bakıldığında, GVKT'nin 35. maddesi ile 36. maddesinde ifade edilen veri koruma etki değerlendirmesi yapma ve ön istişarede bulunma yükümlülüğünün yer almadığı görülmektedir[508]. Doktrin, KVKK bakımından da Direktif hükümlerini temel alan genel bildirim yükümlülüğü yerine veri koruma etki değerlendirmesi (VKED) yapılmasının gerekliliğini, zira bu değerlendirmenin veri sorumluları bakımından yüksek risk içeren işleme faaliyetlerine ilişkin oluşacak risklerin kapsamlarını önceden

[506] **CAREY**, s. 205.
[507] **AKINCI**, s. 171-172.
[508] **ÇELİKEL**, s. 129.

değerlendirme imkânı tanıdığına işaret etmiştir[509]. Nitekim veri koruma etki değerlendirmesi yapmanın, özellikle hesap verilebilirlik şartına ek olarak temel veri koruma ilkelerine uygunluk anlamında yardımcı olacağı, ilave olarak Tüzük m. 25'te ifade edilen tasarım ile gizlilik ve varsayılan gizlilik koruması kapsamında da gerekli olduğu ifade edilmiştir[510].

Elbette KVKK'da veri koruma etki değerlendirmesine yer verilmemiş olması veri sorumlularının bu yükümlülüklerini ortadan kaldırmamaktadır. Keza Kişisel Verileri Koruma Kurumu da kişisel veri işleme temelli yapay zekâ çalışmalarında, kişisel verilerin korunması açısından yüksek riskin ortaya çıktığı durumlarda veri koruma etki değerlendirilmesi yapılmasını tavsiye etmiştir[511]. Kurum ayrıca Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman'da "Hesap Verebilirlik ve Diğer Esaslar/Araçlar" başlığında yüksek risk oluşturabilecek işleme faaliyetleri için bir risk analizi gerektiğini ve analize göre, veri sorumlusunun gerekli tedbirleri almamış olduğu ya da işlemenin yüksek bir risk ortaya çıkarması durumunda, işleme faaliyetlerine başlamadan Kuruma danışılması gerektiğini ifade etmiştir. Kurum her ne kadar veri koruma etki değerlendirmesine ilişkin atıflarda bulunmuşsa da bu yeterli değildir. Zira veri koruma etki değerlendirmesinin ne olduğu, hangi yöntemler dahilinde yapılması gerektiğine ilişkin yasal düzenlemelerin yer alması gerektiği açıktır. Kanaatimiz, kuruluşlar gerek KVKK gerek Tüzük hükümlerine uyum sürecinde ve özellikle işleme faaliyetlerinin ilgili veri sahibi kişilerin haklarına ilişkin yüksek bir risk taşıdığı durumlarda, yalnızca Kurum'un hazırlayacağı rehberlerle değil KVKK'nın lafzında yer alan hususlara da dikkat etmelidir. Zira veri koruma etki değerlendirmesinin hukukumuzda etkinliğinin kazandırılması için veri sorumlularının da bilinçlendirilmesi gereklidir. Veri sorumlularının bu değerlendirmeye ilişkin oluşturacakları raporlarda hangi hususların yer alacağı kişisel verilerin korunması anlamında da son derece önemli olacaktır.

GVKT m. 35/f.2, veri sorumlularının veri koruma etki değerlendirmesini gerçekleştirirken, özellikle, profillemeyi de içeren otomatik işlemeleri ve ilgili veri

---

[509] **AKINCI**, s. 155; **ÇEKİN**, s. 121-122; **BUSSCHE/VOIGHT**, s. 47-48.
[510] **CAREY**, s. 205-206.
[511] **Kişisel Verileri Koruma Kurumu,** Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler, s. 11. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf (Son Erişim Tarihi: 05.07.2022).

sahipleri hakkında hukuken sonuç doğuran ve bu kişileri etkileyen kararlara[512] dikkat çekmiştir[513]. 29. Madde Çalışma Grubu'nun Raporunda[514], hastalarının genetik verilerini ve sağlık verilerini işleyen bir hastanenin, otoyollarda sürücü davranışlarını izlemek üzerine otomatik plaka tanıma sistemi içerir uygulamaların, çalışanlarının internet etkinliği gibi çeşitli faaliyetlerini sistematik olarak izleyen bir işverenin, profil oluşturmak için herkese açık sosyal medya verilerinin toplanmasının, ulusal düzeyde kredi notu oluşturan kurumların kişisel verilerin arşivlenmesi amacıyla takma adlandırma yöntemleri kullanarak çeşitli araştırma projeleri ya da klinik deneylerden elde edilen özel nitelikteki veri depolamasının, veri koruma etki değerlendirmesi yapılacağı durumlara örnek olacağı ifade edilmiştir[515].

Tüzük'te veri koruma etki değerlendirmesinin yöntemi belirtilmemiştir. Ancak veri koruma etki değerlendirme sürecinin tek bir yöntemi olmamakla birlikte ICO'nun uygulama kuralları ile tutarlı olacak şekilde GVKT m. 34/f.7'de belirli aşamaları içermesi gerektiği ifade edilmektedir[516].

2. Ön İstişarede Bulunmak

GVKT m. 36, yapılacak etki değerlendirmesi sonucunda, gerekli tedbirleri almayan ve veri işleme faaliyetlerinin ilgili veri sahibi kişilerin haklarına yönelik

[512] Madde 35(3)'ün (a) bendinde, profil oluşturma da dahil olmak üzere, bireyleri önemli ölçüde etkileyen kararlarla sonuçlanan veri analitiği ele alınmaktadır. ICO, profil oluşturma ve otomatik karar vermeye giren veri işleme faaliyetlerine ilişkin bazı örnekler paylaşmıştır. Buna göre, riskleri hesaplamak için profilleme ve puan tespiti (örneğin, kredi için, sigorta primi belirlemek için, kara para aklamanın tespiti); konum takibi yapan mobil uygulamalardan gelen bildirimler; davranışsal reklamcılık, akıllı cihazlar aracılığıyla sağlık, fitness ve sağlık verilerinin izlenmesi bu kapsamda değerlendirilmektedir. ICO, Feedback request– profiling and automated decision-making, s. 22. https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf (Son Erişim Tarihi:07.08.2021).

[513] **LAMBERT**, s. 284-285; **BUSSCHE/VOIGHT**, s. 48; **ÇEKİN**, s. 212.

[514] Nisan 2017'de, 29. Madde Çalışma Grubu, VKED kapsamında işleme faaliyetlerinin yüksek risk oluşturup oluşturmadığını belirlemeye ilişkin Çalışma Raporunu yayınladı. Raporun Gözden geçirilmiş hali Ekim 2017 tarihinde yayınlandı. bkz. **29. Madde Çalışma Grubu,** WP 248.

[515] **29. Madde Çalışma Grubu,** WP 248, s.11; **ÇELİKEL** s. 129; **ÇEKİN**, s. 211-212.

[516] Buna göre veri koruma etki değerlendirme süreci, veri işleme faaliyetlerini ve işleme amaçlarını açıklamak; amaçlarla ilgili olarak veri işleme faaliyetlerinin gerekliliğini ve orantılılığını değerlendirmek; veri koruma risklerini değerlendirmek, kişisel verilerin korunmasını ve Tüzük ile uyumluluğu sağlamaya yönelik tedbirler de dahil olmak üzere muhtemel riskleri ele alacak tedbirler belirlemeyi içermelidir. Bunun yanında veri koruma etki değerlendirmesinin diğer önemli unsurları, gerektiğinde Veri Koruma Görevlisinin tavsiyesini almak ; gerektiğinde amaçlanan veri işleme faaliyetleri hakkında veri sahiplerinin veya temsilcilerinin görüşlerini almak ; işleme faaliyetlerinin yüksek bir riskle sonuçlanacağının anlaşıldığı durumlarda ilgili denetim makamına bildirimde bulunmak ; ilgili risklerde bir değişiklik olması durumunda, kişisel verilerin işlenmesinin veri koruma etki değerlendirmesine uygun olarak gerçekleştirilip gerçekleştirilmediğine ilişkin inceleme yapmak şeklinde ifade edilmektedir.

yüksek risk taşıdığı hallerde, işleme faaliyetlerinden önce denetim makamlarının görüşüne başvurmasının zorunlu olduğu belirtilmiştir. Veri işleme faaliyetleri kapsamında muhtemel riskler üzerine yapılacak değerlendirmeler neticesinde denetim makamına başvurulması yükümlülüğüne KVKK'da yer verilmemiştir.

Denetim makamları, özellikle risk değerlendirmesinin yetersiz kaldığı durumlarda, veri işleme faaliyetlerinin Tüzük hükümlerine uygun olmayacağını varsaydığı veya kabul ettiği durumlarda ilgili veri sorumlusuna tavsiye vermelidir[517]. Bununla birlikte veri sorumlusuna verilecek tavsiye makul bir süre içerisinde sunulmalıdır[518]. Zira yapılacak ön istişarenin veri işleme faaliyetlerinin başlamasından önce tamamlanması gerektiğinden ve veri işleme ile alınacak tavsiyelere göre uygulamaya konulacak yeni yöntemlerin zaman alabileceği ihtimali olduğundan, bu sürenin iyi belirlenmesi gereklidir[519]. GVKT m. 36/f.2'ye göre tavsiyenin genellikle sekiz hafta içinde verilmesi gerektiği öngörülmüştür. Ancak verilecek tavsiye öncesinde yapılacak değerlendirmenin karmaşıklığına göre bu süre altı hafta kadar daha uzayabilecektir[520]. Denetim makamının olası bir gecikme halinde, istişare talebi alınmasıyla bir ay içinde, veri sorumlusu ve gerektiğinde veri işleyeni süre uzatımı yönünden bilgilendirmesi gerekir. Süreler denetim makamının istişare amacıyla talep ettiği bilgi ve belgelere erişim sağlanıncaya dek askıya alınabilir[521].

Tavsiye kararının alınmasının ardından GVKT m. 35/f.11 gereği veri sorumluları, kişisel verilerin korunması ve veri işleme faaliyeti kapsamında ortaya çıkacak risklerinin veri koruma etki değerlendirmesine uygun şekilde ele alındığından ve ele alınmaya devam edileceğinden emin olmak için düzenli inceleme ve denetlemeler gerçekleştirmelidir.

Görüleceği üzere veri sorumluları bakımından gerek GVKT'nin 35. maddesinde ifade edilen veri koruma etki değerlendirmesi, gerek GVKT'nin 36. maddesinde ifade edilen ön istişare yapma yükümlülüğünün, KVKK kapsamında yer alan veri güvenliğine ilişkin politikaların belirlenmesinde de uygulanması gereklidir. Özellikle ilgili veri sahibi gerçek kişilerin hak ve özgürlüklerinin korunmasına ve bu

---

[517] **CAREY**, s. 220; **BUSSCHE/VOIGHT,** s. 52; **LAMBERT**, s. 326.
[518] **CAREY**, s. 220.
[519] **CAREY**, s. 222.
[520] **CAREY**, s. 222; **BUSSCHE/VOIGHT,** s. 52; **LAMBERT**, s. 326.
[521] Tavsiye alacak ilgili kuruluşların, veri sorumluları ve veri işleyenlerin, işleme amaç ve araçları, Tüzük kapsamında ilgili veri sahibi kişilerin hak ve özgürlüklerini korumaya yönelik aldığı tedbirler, gerektiğinde veri koruma görevlisinin iletişim bilgileri gibi bilgileri denetim makamlarına sağlaması gerekmektedir.

kişilerin verileri ile ilgili veri ihlallerinin önüne geçilmesinde uygulanacak veri koruma prosedürleri son derece önemlidir. Bu veri koruma politikalarının Tüzük kapsamında yer alan hükümlere uygun hale getirilmesi neticesinde, KVKK bakımından da telafisi güç olan veri kayıplarının önüne geçilmesinin yolu açılacaktır[522].

G. VERİ KORUMA GÖREVLİSİ ATAMA YÜKÜMLÜLÜĞÜ

GVKT'nin yürürlüğe girmesi ile gündeme gelen bir kavram da KVKK'dan farklı olarak veri koruma görevlisi[523] (VKG)[524] kavramıdır. Esasında VKG yeni bir kavram değildir. Zira Direktif'te herhangi bir kuruluşun VKG atama zorunluluğuna ilişkin bir düzenleme yer almasa da veri koruma görevlisi atama üye devletler arasında uzun yıllardır süregelen bir uygulamaya dönüşmüştür[525]. Bu durumun nedeni 95/46/EC sayılı Direktif'in 18 ile 21. maddelerindeki bildirimde bulunmaya ilişkin hükümlerin, Direktif ile ilgili eksikliklerin müzakere edildiği süreçlerde üye devletlerdeki farklı uygulamaları ortaya koymasıdır. Bu farklı uygulamalar sonucu Direktif hükümlerinin üye devletlerin bildirimde bulunma yükümlülüklerini azaltan uygulamalar koymada önüne geçilmek istenmiştir[526]. Bunun yanında üye devletler açısından yeknesak bir uygulamaya geçilmesi hedeflenmiştir[527]. Ancak belirtmek gerekir ki üye devletlerin bildirim mekanizmalarındaki farklılıklar, Direktif'in kabulünden çok önce de özellikle Fransa, Almanya ve İsveç gibi bazı ülkelerde 70'lerden ve 80'lerden bu yana var olmuştur[528]. Bu ülkeler veri koruma görevlilerinin önemli rolüne o tarihlerden itibaren dikkat çekmiştir[529]. Bu öneme dikkat çeken 29. Madde Çalışma Grubu da veri koruma

---

[522] **Kişisel Verileri Koruma Kurumu**, Kişisel Verilerin Korunması Kanunu ve Uygulaması, s. 20.
[523] Data Protection Officer.
[524] Kısaca DPO.
[525] **29. Madde Çalışma Grubu,** WP 106, s. 4-5;
[526] **29. Madde Çalışma Grubu,** WP 106, s. 4-5; **BUSSCHE/VOIGHT,** s. 53; **LAMBERT**, s. 457.
[527] **29. Madde Çalışma Grubu,** WP 106, s. 4-5.
[528] **29. Madde Çalışma Grubu,** WP 106, s. 6.
[529] **29. Madde Çalışma Grubu,** WP 106, s. 6; Tüzük yürürlüğe girene kadar bir veri koruma görevlisi atama zorunluluğu çoğu AB üye devletlerinde yaygın olarak uygulanmıyordu. Ancak, VKG atama zorunluluğu Alman Veri Koruma Yasasında uzun yıllardır uygulanmış ve bir veri koruma görevlisi belirlemenin son derece başarılı bir yöntem olduğu kanıtlanmıştır. Almanya'da, otomatik veri işleme faaliyetleri ile uğraşan ve dörtten fazla kişiye sahip her özel kuruluşun, bir veri koruma görevlisi atamak zorunluğu bulunmaktaydı. Veri koruma görevlileri, çalıştıkları kurumların sorunlarına aşinaydı ve tavsiye vermek ve herhangi bir veri koruma sorununu çözme konusunda oldukça yardımcı oluyorlardı. İsveç'te kural olarak bir veri koruma görevlisi (İsveç terminolojisinde kişisel veri temsilcisi) atama zorunluluğu yoktu ve veri koruma görevlisi atama hususu tercihe bağlı bir düzenlemeydi. Ancak tercihe bağlı olarak atanan bir veri koruma görevlisi, veri sorumlusunun, kişisel verileri hukuka uygun ve doğru bir şekilde işlemesine yardımcı olurdu. Eğer veri işleme faaliyetleri ile ilgili veri koruma görevlisinin, veri sorumlusunun bir hukuka aykırılıktan şüphelenmek için nedenleri varsa ve bu aykırılık en kısa

görevlisinin aslında hesap verilebilirliğin temel yapı taşı olduğunu ve bir veri koruma görevlisi atamanın veri koruma hukuku kapsamında üye devletler arasındaki uyumu kolaylaştırabileceğini ifade etmiştir[530].

Netice olarak GVKT'nin yürürlüğe girmesi ile veri sorumluları bakımından veri koruma görevlisi atama yükümlülüğü getirilmiştir. GVKT'nin 37. maddesine göre veri sorumluları ve veri işleyenlerin işleme faaliyetlerinde bir veri koruma görevlisi belirlemesi zorunludur. GVKT'nin 38. maddesi ise, veri koruma görevlisinin görevlerini yerine getirirken hukuki statüsüne ilişkin hükümleri içerir.

1. Kavram Olarak Veri Koruma Görevlisi

Veri koruma görevlisi, en genel ifade şekliyle belirli görevleri yerine getirmek üzere veri sorumluları ya da veri işleyenler tarafından atanan, kişisel verilerin korunması kurallarına uygunluk konusunda tavsiyelerde bulunan, kişisel verilerin korunması anlamında hesap verilebilirliğin önemli yapı taşlarından olan, alanında uzman bağımsız bir kişiyi ifade etmektedir[531]. Bu kişiler aynı zamanda veri sorumluları ya da veri işleyenler ve bu kişilerin yer aldığı kuruluşlar ile denetim makamları arasında bir köprü görevi görürler[532]. Bu anlamda veri sorumluları ya da veri işleyenler tarafından hedeflenen güvenlik seviyesini arttırmaya yönelik alınacak tedbirler arasında veri koruma görevlisi atama da bulunmaktadır.

GVKT m. 37/f.1, veri sorumlusu ve ondan aldığı talimatlarla veri işleyenin; işleme faaliyetlerinin kendi yargı çevresi dışında kalan mahkemeler haricindeki kamu kurum/kuruluşlarınca[533] gerçekleştirilmesinde; işleme faaliyetlerinin[534] amaçları

---

sürede giderilmediyse, veri koruma görevlisi bu durumu denetim makamına bildirirdi. **29. Madde Çalışma Grubu,** WP 106, s. 15-19.

[530] **29. Madde Çalışma Grubu**, WP 243, s. 4.

[531] **ÇEKİN**, s. 209; **BUSSCHE/VOIGHT,** s. 53; **LAMBERT**, s. 457; GVKT'nin 37. maddesi veri koruma görevlilerinin atanmasında hem veri sorumluları hem veri işleyenler bakımından geçerlidir. Bu noktada zorunlu atama kriterini kimin yerine getirdiğine bağlı olarak kimi durumlarda sadece veri sorumluları kimi durumlarda sadece veri işleyenin, diğer durumlarda ise hem veri sorumlusunun hem veri işleyenin ortak hareket etmesi gerekmektedir. **29. Madde Çalışma Grubu**, WP 243, s. 9; Kişisel Verilerin Korunması El Kitabı, s. 175.

[532] Kişisel Verilerin Korunması El Kitabı, 2018, s. 175.

[533] Tüzük neyin bir "kamu kurum ve kuruluşu" oluşturduğunu tanımlamaz. 29. Madde Çalışma Grubu, böyle bir kavramın üye devletlerin ulusal mevzuatları kapsamında belirlenmesi gerektiğini ifade etmektedir.

[534] GVKT m. 37/1-b ve m. 37/1-c'de "veri sorumlusu ya da veri işleyenlerin temel veri işleme faaliyetlerine" atıfta bulunurken bu temel faaliyetler ile veri sorumlusu ya da veri işleyenin amaçlarına uluşmak için gerekli olan temel işlemeleri konu edindiğini ifade etmektedir. Örneğin, bir hastanenin

doğrultusunda ilgili kişilerin sistemli ve düzenli olarak büyük çapta izlenmesini gerekli kılan işleme faaliyetlerini doğurması durumunda[535]; veri sorumlusunun ya da veri işleyenin temel faaliyetlerinin özel nitelikte veri kategorilerinden ya da cezai yaptırımı olan suçlara ilişkin işlemelerden oluşması durumunda veri koruma görevlisi ataması gerekmektedir. Bu anılan hükümler dışında veri koruma görevlisi atama zorunluluğu bulunmamaktadır. Ancak GVKT m. 37/f.4 kapsamında veri sorumluları, veri işleyenler, bunları temsil eden kuruluşlar gerekli görülen durumlarda veri koruma görevlisi atayabileceklerdir. Görüleceği üzere Avrupa Birliği hukukunda veri koruma görevlisi atama zorunluluğu her zaman veri sorumluları ya da veri işleyenlerin takdirine bırakılmamış olup, belirli koşulların varlığında veri koruma görevlisi atama zorunluluğu getirilmiştir. İş bu hususlar az önce yukarıda ifade ettiğimiz üzere Tüzük m. 37/f.1'e göre üç önemli zorunluluk halinden oluşmaktadır.

GVKT m. 37/f.2'ye göre birden fazla kuruluş, "her kuruluştan kolayca erişilebilir" olması şartıyla tek bir VKG belirleyebilir. VKG'nin, veri sorumlusunu bilgilendirme ve tavsiyede bulunma görevi göz önüne alındığında kolayca erişilebilir olması önemlidir. GVKT m. 37/f.3'e göre de büyüklükleri dikkate alınarak birkaç kamu kurum/kuruluşu için tek bir veri koruma görevlisi atanabileceği ifade edilmiştir. GVKT m. 37/f.7'ye göre veri sorumluları ile veri sorumlularının görevlendirdikleri ve yetkilendirdikleri veri işleyenler, VKG'nin iletişim bilgilerini yayınlamak ve bu bilgileri ilgili denetim makamlarına iletmekle yükümlüdür. Bu gerekliliğin amacı ilgili veri sahiplerinin ve denetim makamlarının, kuruluşun başka bir bölümü ile iletişim kurmak zorunda kalmadan kolay bir şekilde veri koruma görevlisine ulaşımını sağlamaktır[536]. İletişim bilgileri, veri koruma görevlisine kolay bir şekilde ulaşılmasına

---

temel faaliyeti sağlık hizmeti sunmaktır. Dolayısıyla bu hastane, hastaların sağlık kayıtları gibi özel nitelikte sağlık verilerini işlemeden bir sağlık hizmeti sunamaz. Hastanenin bu sağlık verilerini işlemesi onun temel faaliyetlerinden olup bir veri koruma görevlisi atanması gerekecektir. **29. Madde Çalışma Grubu**, WP 243, s. 7.

[535] Veri öznelerinin düzenli ve sistematik olarak izlenmesi kavramı Tüzük kapsamında tanımlanmamıştır. Ancak, ifade etmek gerekir ki izleme kavramı çevrimiçi ortamlarla sınırlı değildir ve çevrimiçi izleme, veri öznelerinin davranışlarını izlemenin tek bir örneği olarak düşünülmelidir. **29. Madde Çalışma Grubu**, WP 243, s. 8. Örneğin, sosyal medya şirketleri ve arama motorları, veri işleme faaliyetlerinde kişisel veri konularının büyük ölçekte, sistemli olarak ve düzenli bir şekilde izlenmesini gerektiren veri sorumluları olarak değerlendirilebilir. Bu tür şirketlerin veri işleme faaliyetleri çok büyük miktarda kişisel verinin işlenmesine dayanmaktadır. Bu şirketler belirli reklam hizmetleri sunmayı hedefler ve önemli ölçüde reklam gelirleri ederler. Bu reklam faaliyetleri özellikle tüketicilerin çevrimiçi satın alma geçmişlerine göre reklam sunma imkanı tanır. Bu nedenle, ilgili veri sahibi kişilerin sistemli ve düzenli bir şekilde çevrimiçi alışkanlıklarının ve davranışlarının izlenmesi gerekir. Kişisel Verilerin Korunması El Kitabı, s. 176.

[536] **ÇEKİN**, s. 209; **BUSSCHE/VOIGHT,** s. 55; **LAMBERT**, s. 461; **29. Madde Çalışma Grubu**, WP 243, s. 11.

imkân veren (posta adresi, özel telefon numarası ve/veya özel e-posta adresi) bilgileri içermelidir[537].

2. Veri Koruma Görevlisinin Özellikleri

Tüzük, veri koruma görevlisi atama yükümlülüğü ile ilgili getirdiği yeniliklerde veri koruma görevlisinin görev ve sorumluklarına ilişkin pek çok detaylı açıklamalarda da bulunmuştur. Nitekim veri koruma görevlisi, Tüzük'ün 39. maddesine göre öncelikle kişisel verilerin işlenme faaliyetleri ile ilgili yol gösteren, veri işleme politikaları ile ilgili ve veri koruma etki değerlendirmesi kapsamında gerekli tavsiyelerde bulunan, raporlamalar yapan ve denetim makamları ile işbirliğini sağlayan bağımsız ve uzman kişidir.

Veri sorumlusu ya da veri işleyenlerce atanacak VKG, alanında uzman bir kişi olmalıdır[538]. Tüzük kapsamında veri koruma görevlisinin uzmanlık seviyesi kesin olarak tanımlanmamıştır. Ancak veri koruma görevlisi, bir kuruluşun işlediği kişisel verilerin hassasiyeti ve karmaşıklığı konusuna hâkim olmalıdır[539]. Bu husus özellikle kişisel verilerin AB ülkesi dışına aktarılıp aktarılmamasına göre farklılık arz etmektedir. Ayrıca veri koruma görevlisi, kuruluşun gerçekleştirdiği işleme faaliyetlerinin bir kamu kurum ve kuruluşuna ait olması durumunda, bu kuruluşun idari işleyişine de hâkim olmalıdır[540]. Bu nedenle veri sorumlusu ya da veri işleyenlerce atanacak VKG seçiminde dikkatli davranılması gerekmektedir[541]. Bu anlamda denetim makamlarının da veri koruma görevlileri için yeterli ve düzenli eğitimi teşvik etmesi önemlidir.

Veri koruma görevlisinin bağımsız olması, veri sorumlusu ya da veri işleyenden talimat almayacağını, almaması gerektiğini de ifade etmektedir[542]. Veri koruma görevlisi GVKT m. 37/f.6 kapsamında başka görevleri ve vazifeleri de yerine getirebilir. Veri koruma görevlisinin m. 37/f.6 kapsamında yer aldığı kuruluşun

---

[537] **29. Madde Çalışma Grubu**, WP 243, s. 12.
[538] **ÇEKİN**, s. 209-210; **LAMBERT**, s. 462; **29. Madde Çalışma Grubu**, WP 243, s. 11.
[539] **ÇEKİN**, s. 209-210; **BUSSCHE/VOIGHT,** s. 56-57; **LAMBERT**, s. 461; **29. Madde Çalışma Grubu**, WP 243, s. 11.
[540] **ÇEKİN**, s. 209-210; **BUSSCHE/VOIGHT,** s. 56-57; **LAMBERT**, s. 461; **29. Madde Çalışma Grubu**, WP 243, s. 11.
[541] **29. Madde Çalışma Grubu**, WP 243, s. 11.
[542] Nitekim Resital 97, veri koruma görevlilerinin, veri sorumlusunun bir çalışanı olup olmadığına bakılmaksızın, görevlerini ifa ederken bağımsız olmaları gerektiğini ifade etmektedir. **GVKT**, Resital 97; **29. Madde Çalışma Grubu**, WP 243, s. 15.

içerisinden belirlenebileceği gibi bir hizmet akdi ile dışarıdan görevlendirilmesi de mümkündür.

Veri koruma görevlisinin görev ve sorumluklarını yerine getirmede sadece uzmanlığa sahip olması yetmez. Bunun yanında mesleki etik kurallarına uygun davranan dürüst bir kişi olması gerekir. Zira veri koruma görevlisinin öncelikli hedefi, atandığı kuruluşun veri işleme faaliyetlerinin Tüzük hükümlerine uyumunu değerlendirmektir. Elbette veri koruma görevlisinin sunduğu tavsiyelere uyulmaması durumunda veri koruma görevlisi kişisel olarak sorumlu olmamaktadır[543]. Nitekim Tüzük m. 24/f.1, veri işleme faaliyetlerinin Tüzük uyarınca gerçekleştirildiğini gösterebilmek için gerekli tedbirlerin alındığı göstermesi gereken kişinin veri sorumluları ve veri işleyenler olduğunu ifade etmektedir.

3. Veri Koruma Görevlisinin Görev ve Sorumlulukları

GVKT'nin 39. maddesi, veri koruma görevlisinin görev ve sorumluluklarına ilişkin açıklamalara yer vermektedir. Buna göre veri koruma görevlisi diğer görevlerinin yanı sıra veri işleme faaliyetlerinin Tüzük kapsamına uyumunu değerlendirmelidir. Veri koruma görevlileri, uyumluluğu izlemeye yönelik olarak özellikle veri işleme faaliyetleri ile ilgili bilgi toplamak, bu bilgilerin doğruluğunu kontrol etmek, işleme faaliyetlerinin uygunluğuna ilişkin veri sorumlusu ve/veya veri işleyenlere bilgi ve tavsiye vermekle yükümlüdür[544]. Veri koruma görevlisinin atandığı kuruluş, kendisine sunulan tavsiyeleri görmezden gelebilir ancak doğacak sorumluluklardan ötürü veri koruma görevlilerinin görevine son verilemez ve cezalandırılamaz[545].

Veri koruma etki değerlendirmesi sürecinde, bu süreci yürütmek her ne kadar veri sorumlusunun yükümlülüğünde olsa da veri koruma görevlisi de veri sorumlusuna yardımcı olmalıdır. Tasarım ile gizlilik ilkesine uygun olarak veri koruma görevlisi, özellikle veri koruma etki değerlendirme sürecinde gerekli tavsiyeleri sunmalıdır[546].

---

[543] **29. Madde Çalışma Grubu**, WP 243, s. 17

[544] **ÇEKİN**, s. 209-210; **BUSSCHE/VOIGHT,** s. 56-57; **LAMBERT**, s. 459; **29. Madde Çalışma Grubu**, WP 243, s. 17.

[545] **ÇEKİN**, s. 209-210; **BUSSCHE/VOIGHT,** s. 56-57; **LAMBERT**, s. 459; **29. Madde Çalışma Grubu**, WP 243, s. 15.

[546] Nitekim 29. Madde Çalışma Grubu, veri koruma etki değerlendirmesinin yürütülüp yürütülmeyeceği, veri koruma etki değerlendirmesi gerçekleştirilirken izlenecek metodoloji, ilgili veri sahibi gerçek

Veri koruma görevlileri ayrıca, GVKT m. 38/f.5'te ifade edildiği üzere görevlerinin ifasıyla ilgili olarak sır saklama ve gizlilik ilkelerine de uymakla yükümlüdür. Ancak ifade etmek gerekir ki sır saklama ve gizlilik yükümlülüğü, veri koruma görevlilerinin, denetim makamlarıyla iletişime geçmesini ya da onlardan tavsiye almasını engellememektedir. Zira m. 39/f.1-e bendinde göre veri koruma görevlileri gerekli gördükleri hallerde herhangi bir konu ile ilgili olarak denetim makamlarına danışabilmektedir[547].

GVKT m. 39/f.2, veri koruma görevlisinin veri işleme faaliyetlerinin kapsamı, bağlamı ve amaçlarını göz önünde tutarak, işleme faaliyetleri ile ilgili doğabilecek muhtemel riskleri doğru şekilde ele alması gerektiğini ifade eder. Bir diğer ifade ile veri koruma görevlileri, veri işleme faaliyetlerinden riskli olanlarına öncelik vermelidir. Elbette bu öncelik daha düşük riskli veri işleme faaliyetlerinin ihmal edileceği anlamına gelmemektedir[548].

4. Veri Koruma Görevlisinin Tüzük Kapsamında Hakları

Veri koruma görevlilerinin görev ve sorumluluklarının yanında bazı hakları da mevcuttur. Bir veri koruma görevlisi atandığında veri sorumluları, kişisel verilerin korunmasına ilişkin tüm konularda veri koruma görevlisinin tüm süreçlere dahil olmasını sağlamakla yükümlüdür. Bununla birlikte veri sorumluları ve veri işleyenler, veri koruma görevlilerinin görev ve sorumluluklarını yerine getirebilmeleri adına gerekli olan tüm mali kaynakları, altyapı ve ekipmanları sağlamalıdır[549]. Buna ek olarak veri koruma görevlilerinin görev sorumluluklarını yerine getirmede yeterli süre kendilerine sağlanmalıdır. Tüzük, veri koruma görevlilerinin bağımsız bir şekilde hareket etmelerini sağlamak adına veri sorumluları ve veri işleyenlerden talimat almaması gerektiğinin altını çizer.

---

kişilerin haklarının korunmasına yönelik hangi tedbirlerin alınacağı, değerlendirmenin doğru bir şekilde yapılıp yapılmadığı gibi hususlarda VKG'ye başvurulmasını tavsiye etmektedir. **29. Madde Çalışma Grubu**, WP 243, s. 17.

[547] **29. Madde Çalışma Grubu**, WP 243, s. 18.

[548] Burada belirtmek gerekir ki veri işleme faaliyetleri kapsamında işleme faaliyetlerinin kaydının tutulmasına ilişkin getirilen yükümlülük veri koruma görevlisine ait değildir. GVKT m. 30/f.1 ve m. 30/f.2 uyarınca işleme faaliyetlerinin kayıtlarının tutulması veri sorumlularına ya da veri işleyenlere aittir. Dolayısıyla veri koruma görevlileri, görevlerini ifa ettikleri süre boyunca kişisel verilerin işlenmesine ilişkin verilere dayalı olarak bir envanter oluşturup işleme faaliyetlerinin kayıtlarını tutsalar bile bu husus veri sorumluları ya da veri işleyenlerin kayıt tutma yükümlülüklerini bertaraf etmemektedir. **29. Madde Çalışma Grubu**, WP 243, s. 18.

[549] **ÇEKİN**, s. 209-210; **LAMBERT**, s. 459; Kişisel Verilerin Korunması El Kitabı, s. 177.

KVKK kapsamında veri koruma görevlisi kavramına yer verilmediği görülmektedir. Buna karşın Veri Sorumluları Sicili Hakkındaki Yönetmelik m. 4/f.1-ç'de irtibat kişisi tanımı yapılmıştır[550]. Ancak irtibat kişisinin görevi, kuruluşlar ya da ilgili veri sahibi gerçek kişiler ile veri sorumluları arasında iletişimi sağlamakla sınırlıdır. Dolayısıyla bu kavramın veri koruma görevlisi ile bağdaşmadığı açıktır. Her halükârda veri koruma görevlisi kavramına yer verilmemiş olması kural olarak veri sorumlularının veri koruma görevlisi atamalarına engel teşkil etmemektedir. Dolayısıyla veri sorumlularının gerekli gördükleri hallerde veri koruma görevlisi atayabilecektir. Ancak bu kavramın KVKK kapsamında yer alması gerektiği kanaatindeyiz.

H. DENETİM MAKAMLARIYLA İŞBİRLİĞİ YAPMA YÜKÜMLÜLÜĞÜ

GVKT'nin 31. maddesi, veri sorumlularının, veri işleyenlerin ve varsa bu kişilerin temsilcilerinin, denetim makamlarının bu yönde bir taleplerinin olması halinde işbirliği yapma yükümlülüğünü düzenler[551]. Denetim makamlarının gerekli gördüğü haller dışında veri sorumlularının işbirliği yapma yükümlülüğü, bir ihlal meydana geldiğinde veri sorumlusunun denetim makamlarına bildirimde bulunma yükümlülüğü olarak ifade edilir. Zira olası bir veri ihlali durumunda, ilgili veri sahibi kişiler söz konusu kişisel verileri üzerindeki hâkimiyeti kaybetmektedir. Böyle bir durumda veri sorumlularının denetim makamlarıyla işbirliği yapma yükümlülüğü de önem kazanmaktadır. Nitekim daha önce ifade ettiğimiz gibi, veri sorumlusu tarafından atanan veri koruma görevlisinin, kuruluşun veri işleme faaliyetlerinin Tüzük hükümlerine uyumunu değerlendirmesi noktasında, gerektiğinde denetim makamlarına danışması halinde veri sorumlusunun bu kişilerle işbirliği içinde yer alması da bu yükümlülük içerindedir. Benzer şekilde GVKT'nin 36. maddesine göre 35. madde kapsamında yapılacak veri koruma etki değerlendirme sonucunda, veri sorumlusunun gerekli tedbirleri almaması durumunda veri işleme faaliyetlerinin ilgili veri sahibi kişilerin haklarına yönelik yüksek risk taşıdığı hallerde, işleme faaliyetlerinden önce

[550] Madde hükmüne göre irtibat kişisi, "Türkiye'de yerleşik olan tüzel kişiler ile Türkiye'de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile kurulacak iletişim için veri sorumlusu tarafından Sicile kayıt esnasında bildirilen gerçek kişiyi…" ifade etmektedir.
[551] **CAREY**, s. 100; **BUSSCHE/VOIGHT,** s. 37; **LAMBERT**, s. 163.

veri sorumlularının denetim makamlarının görüşüne başvurması zorunluluğu ve bu kapsamda alınacak tavsiye kararlarına uyum da yine veri sorumlusunun denetim makamlarıyla işbirliği yükümlülüğüne bir örnektir. Söz konusu veri ihlallerine ilişkin veri sorumlusunun denetim makamlarına bildirimde bulunma yükümlülüğü bu sebeple işbirliği yapma yükümlülüğünü de içermektedir.

1. Veri Sorumlusunun Bildirim Yükümlülüğü

Kişisel verilerin ihlaline ilişkin herhangi bir durum söz konusu olduğunda veri sorumlularının GVKT'nin 33. ve 34. maddesi gereği bildirimde bulunma yükümlülüğü doğmaktadır. Bu anlamda veri sorumlularının bildirim yükümlülüğü Tüzük'te ayrı maddeler halinde düzenlenmiş olup, GVKT'nin 33. maddesi denetim makamlarına bildirim yükümlülüğünü, GVKT'nin 34. maddesi ise ilgili veri sahibi kişiye bildirim yükümlülüğünü düzenlemektedir. Veri sorumlusunun bildirimde bulunmasına ilişkin bu yükümlülüğü, veri ihlallerinin yol açtığı zararların azaltılmasına katkı sağlayacak ve ilgili veri sahibi kişiler bakımından da hesap verilebilirliğe imkân sağlayacak bir yükümlülüktür.

a. İlgili Veri Sahibi Kişiye Bildirim Yükümlülüğü

GVKT'nin "Veri ihlalinin ilgili veri sahibi kişiye iletilmesi" başlıklı 34. maddesi veri ihlalinin, ilgili kişinin haklarına yüksek risk oluşturmasının mümkün olduğu durumlarda, gecikmeye mahal verilmeksizin bildirilmesi gerektiğini ifade etmektedir[552]. Burada bahsedilmesi gereken önemli bir husus da GVKT'nin 34. maddesinde yer alan ihlal düzeyinin 33. maddesinde yer alan ihlal seviyesine göre daha yüksek olması gerektiğidir. Ancak KVKK, m. 12/f.5 incelendiğinde, veri ihlallerinin taşıdığı risk bakımından bir ayrım yapılmadığı, aksine veri ihlalinin söz konusu olduğu durumlarda, Kurul'a ve ilgili veri sahibi kişiye bildirim yükümlülüğünün aynı çatı altında toplandığı gözlemlenmektedir.

KVKK bakımından yer alan bir diğer farklılık ise bir ihlal söz konusu olduğunda veri sorumlularına getirilen bildirim yükümlülüğünün, veri işleyenler bakımından hüküm altına alınmamış olmasıdır. Elbette bu konuda bir açıklık

[552] **LAMBERT**, s. 283; **BUSSCHE/VOIGHT,** s. 69; **CAREY**, s. 100.

olmaması, veri işleyenlerin böyle bir ihlal durumunda, veri sorumlularını bilgilendirmesi gerekemediği anlamına gelmemelidir. Aksine KVKK bakımından veri işleyenlerin pozisyonu irdelendiğinde, söz konusu veri ihlal bildirimi yükümlülüğünün veri işleyenler bakımından da geçerli olması gerektiği görüşündeyiz. Nitekim doktrin, Kanun lafzına bakıldığında her ne kadar veri ihlal bildiriminin veri sorumlusu tarafından yapılacağını ifade etmekte ise de veri işleyenin veri sorumlusuna karşı bildirimde bulunmamasından ya da geç bildirimde bulunmasından dolayı ortaya çıkacak zararlardan sorumlu tutulabileceğini, ancak bu hususun veri sorumlusu ile veri işleyenin iç ilişkisinde gerçekleşeceğini ifade ederek veri sorumlusunun, müşterek sorumluluk gereği veri işleyene rücu edebileceğini ifade etmektedir[553].

b. Denetim Makamlarına Bildirim Yükümlülüğü

GVKT'nin 33. maddesinin 1. fıkrası, verilerin ihlali söz konusu olduğunda kişisel veri ihlalinin ilgili kişinin haklarına yüksek risk oluşturmasının mümkün olduğu durumlarda, veri sorumlularının bu ihlali öğrenir öğrenmez en geç 72 saat içinde Tüzük m. 55 uyarınca denetim makamlarına bildirmesi gerektiğini belirtmektedir. Söz konusu bildirimde bulunma yükümlülüğü, yalnızca veri sorumluları bakımından değil Tüzük m. 33/f.2'ne göre veri işleyenler bakımından da geçerlidir. Ancak veri işleyenin bildirimde bulunma yükümlülüğü veri sorumlularına karşıdır.

Yukarıda bahsettiğimiz üzere KVKK, m. 12/f.5 ile kişisel verilerin ihlalinin söz konusu olduğu durumlarda Kurul'a ve ilgili veri sahibi kişiye bildirim yükümlülüğü aynı madde altında düzenlemiştir[554]. KVKK'da veri ihlalinin öğrenilmesinden itibaren ilgili veri sahibine ve Kurul'a bildirimde bulunma süresinin ne kadar olduğu açıkça ifade edilmemiş olsa da Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24 Ocak 2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyurusunda[555], KVKK m. 12/f.5'teki "en kısa süre" ifadesinin 72 saat olarak yorumlandığı ve söz konusu veri ihlalini öğrendiği tarihten itibaren veri sorumlularının

[553] **ÇEKİN**, s. 207.
[554] Bkz. İkinci Bölüm, Kişisel Verileri Koruma Kanununun AB Genel Veri Tüzüğü'ne Uyumlaştırması Bakımından Ele Alınması Gereken Kavramlar ve İlkeler, IV. Uyumlaştırma Kapsamında Veri Sorumlusuna ve Veri İşleyene Düşecek Ek Görev ve Yükümlülükler, D. Veri İşleme Kayıtları ile İlgili Ek Yükümlülükler, 2. Veri İhlali Açıklaması ve Bildirimi, s. 110.
[555] Kişisel Verileri Koruma Kurulu'nun 24 Ocak 2019 Tarih ve 2019/10 Sayılı Kararı.

gecikmeye mahal vermeksizin 72 saat içinde Kurul'a bildirimde bulunması gerektiği belirtilmiştir.

I. VERİ SORUMLUSU YA DA VERİ İŞLEYENİN TAZMİNAT YÜKÜMLÜLÜĞÜ

GVKT'nin "Tazminat Hakkı ve Sorumluluk" başlıklı 82. maddesinde veri işleyenler de Tüzük hükümlerine ilişkin ortaya çıkan herhangi bir ihlal karşısında sorumlu tutulabilir hale gelmişlerdir. Böylece ilk kez kişisel verilerini işledikleri kişiler karşısında veri işleme faaliyetini gerçekleştiren veri işleyenlerin de sorumlu tutulabileceği öngörülmüştür.

GVKT m. 82'ye göre, Tüzük hükümlerinin ihlali sonucunda zarara uğrayan bir kişi, bu zararın giderimi için veri sorumlusu ile veri işleyenden tazminat talep etme hakkına sahip olacaktır. Görüleceği üzere tazminat talep etme hakkı, zarar gören "herhangi bir kişi" için mümkündür[556]. GVKT m. 82/f.2'ye bakıldığında ise işleme faaliyetleri sonucu ortaya çıkan herhangi bir zarardan veri sorumlularının doğrudan sorumlu olacakları ifade edilirken, veri işleyenler bakımından ise bir ayrım yapıldığı gözlemlenmektedir. Buna göre veri işleyenler ancak, kendilerine yüklenen yükümlülüklere uymadıkları takdirde ya da veri sorumlularının görevlendirmeleri ve talimatlandırılmaları dışında hareket ettikleri durumlarda meydana gelen zararlardan sorumlu tutulmaktadırlar. Dolayısıyla Tüzük kapsamında hem veri sorumluları hem veri işleyenler tazminat taleplerinden sorumlu tutulabilseler de bu tazminat talepleri karşısındaki sorumlulukları farklı olmaktadır[557].

Hem veri sorumluları hem de veri işleyenler söz konusu tazminat talebine karşı, zarara yol açan işleme faaliyetlerinden sorumlu olmadıklarını kanıtladıkları ölçüde GVKT m. 82/f.3 gereği bu yükümlülükten kurtulurlar. Bununla birlikte, zarara uğrayan ilgili veri sahibi kişilerin etkili bir tazminat alabilmelerini sağlamak için Tüzük, işleme faaliyetlerini birlikte yürüten veri sorumluları ve veri işleyenlerin, bu işlemelerden kaynaklanan zararlardan müteselsil sorumlu tutulmasını sağlar[558]. Bu nedenle, ilgili veri sahibi kişiler, kusurdan bağımsız olarak, Tüzük hükümlerini ihlal ederek zarara

[556] **BUSSCHE/VOIGHT,** s. 206; **CAREY**, s. 152.
[557] **CAREY**, s. 151-152; **LAMBERT**, s. 421; **SAKA/ÇAĞLAYAN/KOCA**, s. 216.
[558] Ayrıca **GVKT**, Resital 146. İlgili veri sahipleri, meydana gelen zararları için tam ve etkin bir tazminat almalıdır.

yol açan işleme faaliyetlerine dahil olan veri sorumlusu ya da veri işleyenden birine ya da tamamına karşı tazminat talebinde bulunabilecektir[559].

Birden çok veri sorumlusu veya işleyenin işleme faaliyetini yürütmelerinde ortaya çıkan zarardan ne şekilde sorumlu tutulacakları Tüzük m. 82/f.4'te düzenlenmiştir. Buna göre tüm veri işleyenler ve veri sorumluları kural olarak tüm zarardan müteselsil sorumludur. Bu hüküm, kişisel veriler için ortaya çıkan zarara ilişkin taleplerin uygulanmasını basitleştirir, zira veri sahibi ilgili kişi bu zarardan sorumlu taraflardan yalnızca birine dava açmayı seçebilecektir[560]. Ancak bu şekilde sorumlu tutulan bir veri sorumlusu ya da veri işleyenin, Tüzük m. 82/f.5 gereği ilgili veri sahibi kişiye ödedikleri tazminatı, diğer veri sorumluları ya da veri işleyenlerden zarara karşılık gelen kısım kadarını rücu etme imkânları doğmaktadır. Tazminat için başvurulacak mahkeme, GVKT m. 79/f.2'ye göre belirlenecektir[561].

Benzer şekilde KVKK m. 11/f.1-ğ, veri sahiplerinin verilerinin KVKK'ya aykırı işlenmesi nedeniyle zarar görmeleri durumunda bu zararın giderilmesini isteyebileceklerini düzenlemiştir[562]. Dolayısıyla KVKK kapsamında da kişisel verileri Kanun'a aykırı olarak işlenen kişilerin söz konusu zararlarını tazmin ettirme imkânı vardır. Ancak KVKK bakımından vurgulanması gereken husus, Kanun'un tazminat talep etme hakkı için verilerin hukuk kurallarına aykırı işlenmesini aramaktadır[563]. Böyle bir ihtimalde haksız fiil sorumluluğunun doğacağı ifade edilmektedir[564]. Oysa GVKT'nin 82. maddesine bakıldığında, KVKK'da yer aldığı gibi kişisel verilerin kanuna aykırı işlenmesinin şart koşulmadığı, genel olarak bir ihlalin meydana gelmiş olmasının yeterli görüldüğü anlaşılmaktadır[565]

Bunun yanında KVKK bakımından bir diğer farklılık ise, kanuna aykırı olarak işlenme faaliyetlerinden zarar doğması ve bu zararın giderilmesini talep hakkının, veri

[559] Bu noktada ifade etmek gerekir ki, tazminat talebinde bulunacak olan Davacı veri sahibi kişi, veri sorumlusu ya da veri işleyenin sorumluluğuna ilişkin ispat yükümlülüğü altındadır. Ancak ilgili veri sahibinin veri sorumlusu ya da veri işleyeninin sorumluluk paylaşımı hakkında tam olarak bilgi sahibi olması da beklenemez. Dolayısıyla veri sorumlularının ya da veri işleyenlerin sorumluluklarının doğru bir şekilde belirlenebilmesinde gerçeklerin makul bir şekilde mahkeme önüne sunulması veri sahibi Davacı bakımından gerekli ispat yükümlülüğünü karşılamaya yetmelidir. Sorumluluğa ilişkin koşulların aksini ispat etmek ise bu noktadan sonra veri sorumlu ya da veri işleyene ait olacaktır. **BUSSCHE/VOIGT**, s. 207; **CAREY**, s. 151.
[560] **BUSSCHE /VOIGT**, s. 207; **CAREY**, s. 152.
[561] Ayrıca **GVKT**, Resital 145.
[562] Bu konudaki eleştiriler için bkz. **ÇELİKEL**, s. 188.
[563] **ÇELİKEL**, s. 227-228.
[564] **ÇEKİN**, s. 172; Ayrıca bkz. **GÜRPINAR** Damla, "Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk", D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı-2017, ss. 679-694, s. 690.
[565] **GVKT**, m. 82.

işleyenlere yöneltilip yöneltilemeyeceğine ilişkindir. Tüzük hükümlerine bakıldığında bu hususun detaylı olarak ele alındığı ve veri işleyenlerin, kendilerine yüklenen yükümlülüklere uymadıkları takdirde ya da veri sorumlularının talimatlarına aykırı hareket ettikleri durumlarda meydana gelen zararlardan sorumlu tutulacakları ifade edilmişti. Türk hukuku bakımından yapılan değerlendirme de ise, tazminata ilişkin sorumluluğunun, sözleşmesel sorumluluk ve sözleşme dışı sorumluluk olarak ayrıldığı, bu sebeple veri sorumlusu ile veri işleyen arasında bir sözleşme ilişkisi kurulup kurulmadığına göre sorumluluğun değişebileceği ifade edilmektedir[566]. Elbette her iki durumda da zarar gören ilgili kişi veri sorumlusuna gidebilecektir. KVKK'nın 12. maddesi göz önüne alındığında veri sorumlusu, verilerin kendi namına üçüncü kişilerce işlenmesi hâlinde bu kişilerle birlikte müştereken sorumlu olmaktadır. Dolayısıyla KVKK bakımından veri işleyenlerin sorumluluğu oldukça geniş yorumlanabilecektir. Oysa veri işleyenin, veri sorumlusundan aldığı emir ve talimatlarla işleme faaliyetlerine katıldığı düşünüldüğünde KVKK'nın 12. maddesine göre oldukça geniş yorumlanabilecek bir sorumluluk atfedilmesinin hakkaniyet sınırlarını aştığı kanaatindeyiz. Nitekim bu konuda Tüzük hükümlerinin çok daha tutarlı bir sorumluluk mekanizması öngördüğünü ve veri işleyenlerin ancak, kendilerine yüklenen yükümlülüklere uymadıkları takdirde ya da veri sorumlularının talimatlarına aykırı davrandıkları durumlarda meydana gelen zararlardan sorumlu tutulmalarının, Tüzük'teki hükümlere uygun olarak yapılacak bir değişiklik ile yerinde olacağını düşünüyoruz[567].

V. MEVZUAT HÜKÜMLERİNİN TÜZÜĞE UYUMLAŞTIRILMASINDA VERİ SAHİBİNİN EK HAKLARI

A. VERİ SAHİBİNİN UNUTULMA HAKKI

İlgili veri sahibi kişinin unutulma hakkı, GVKT'nin 17. maddesinde düzenlenmiş, ilgili kişinin en önemli haklarından biridir. Unutulma hakkı, Tüzük kapsamında "Silme Hakkı" (Right to Erasure) ya da "Unutulma hakkı" (Right to be forgotten) şeklinde ifade edilmektedir. Unutulma hakkı, ilgili kişinin kendiyle ilgili verilerinin işlenmesini artık istememesi ve kendisi ile ilgili elde edilen kişisel verilerin

[566] **MEMİŞ**, s. 15.
[567] **MEMİŞ**, s.17.

muhafaza edilmesinin artık bir amacı kalmadığını, dolayısıyla hukuka uygunluk koşullarının bulunmadığından bahisle kişisel verilerin silinmesi hakkı olarak ifade edilebilir[568]. Bir diğer ifade ile unutulma hakkı, *"...dijital hafızada kişiye ait fotoğraf, kimlik bilgisi, adres ve diğer kişisel içeriklerin, ilgili kişinin talebi ile bir daha geri döndürülemeyecek şekilde ortadan kaldırılması..."* şeklinde ifade edilmektedir[569].

1. Unutulma Hakkının Doğumu ve Unutulma Hakkına Duyulan İhtiyaç

Unutulma hakkının "temel bir hak" olarak değerlendirilmesinde ve günümüzde yer alan yasal tanımlamasında Avrupa Komisyonu'nun sunmuş olduğu önerilerin etkili olduğu iddia edilmektedir[570]. Bununla birlikte Kıta Avrupası Hukuku bakımından İsviçre Federal Mahkemesi'nin içtihatlarının da bu hakkın gelişimine katkı sağladığı ifade edilmektedir[571]. Ancak bu hak her ne kadar Tüzük hükümleri ile yasal bir zemine oturtulmuş olsa da bu hakkın çıkışı dijital çağdan çok daha eski zamanlara dayanmaktadır[572]. Bu hakkın hukuki olarak tartışmalara konu edilmesinin ilk olarak Fransa'da ortaya çıktığı belirtilmektedir[573]. Bu anlamda Fransa 2010 tarihinde çevrimiçi bir hak olarak "unutulma hakkı" üzerine ilk kanun çalışmasını gerçekleştirmiştir[574].

İnternet kullanımının artması ve içinde bulunduğumuz dijital çağda kişisel verileri korumaya yönelik artan ihtiyaç karşısında unutulma hakkının temel bir hak olarak kabulü gerek ABD'de gerek Avrupa'da tartışıla gelmiş olup farklı kararlara konu olmuştur. Nitekim bu anlamda bilinen kararlardan biri de Stacy SNYDER davasıdır[575]. Söz konusu kararda Millersville Üniversitesi'nde son sınıf öğrencisi olan

---

[568] **BAŞALP**, " Tüzüğün Temel Yenilikleri", s. 93.
[569] **GÜLENER,** Serdar, Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı", TBB Dergisi, Y: 2012, S: 102, ss. 219-240, s. 226.
[570] **GÜLENER,** s. 226.
[571] **WERRO** Franz, "The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash", George Town University, The Center of Transnational Legal Studies, Colloquim Research Paper No. 2, May 2009, s. 286; **BAŞALP**, " Tüzüğün Temel Yenilikleri", s.93.
[572] **SAKA/ÇAĞLAYAN /KOCA**, s. 223.
[573] **WEBER** Rolf H., ''The Right To Be Forgotten: More Than a Pandora's Box'', Journal of Intellectual Property, Information Technology and Electronic Commerce Law, C.2, S.2, 2011, s. 120; **BERNAL** Paul A., ''A Right to Delete?'', European Journal of Law and Technology, C. 2, S.2,2011, s. 2.
[574] **WEBER,** s. 120; **BOZKURT YÜKSEL** Armağan Ebru, "İnternet ve Unutulma Hakkı", 4.Uluslararası Bilişim Hukuku Kurultayı 2016 Bildiriler Kitabı, İzmir, s. 28.
[575] **MAYER-SCHÖNBERGER** Viktor, Delete: The Virtue of Forgetting in the Digital Age, Princeton 2009, s. 2; **KREBS** Brian, "Court Rules Against Teacher in MySpace 'Drunken Pirate' Case", The Washington Post, 03.12.2008,

stajyer öğretmen Stacy SNYDER mezun olacağı günü beklerken katılmış olduğu bir kostüm partisinde çekilmiş olduğu bir fotoğrafı "Sarhoş Korsan" ismiyle Myspace hesabında paylaşır. Ancak fotoğrafın paylaşılmasının ardından Millersville Üniversite yönetimi söz konusu fotoğrafı değerlendirerek SNYDER'ın öğretmenliğe uygun olmadığını ve gençleri alkol tüketimine özendirdiğini ifade etmiştir. SNYDER her ne kadar kendi hesabında paylaşmış olduğu bu fotoğrafın okul çalışma saatleri dışında çekildiğini belirtmişse de suçlamalardan kurtulamamış ve dolayısıyla olay yargıya taşınmıştır. Ancak SNYDER yapılan yargılama sonucunda da istediği sonucu alamamış ve üniversiteden öğretmen olarak değil yalnızca İngilizce mezunu biri olarak mezun olabilmiştir[576]. Bu karar bir ilk olmadığı gibi her geçen gün artan internet kullanımında, son da olmayacaktır. Dolayısıyla bireylerin kişisel verileri üzerinde bir denetim hakkına sahip olabilmesi ve geçmişte yaşadıkları olayların üzerine yeni bir başlangıç yapabilmeleri bu hakkın doğumuna temel sebep olarak gösterilmiştir[577].

Unutulma hakkı, Avrupa hukuku içerisinde özellikle İsviçre Federal Mahkemesi'nin içtihatlarının yaklaşımını benimserken daha ziyade kişinin şeref ve haysiyeti ile özel hayatının gizliliğini korumaya yönelik bir yaklaşıma sahip olmuştur[578]. ABD hukukunda ise bu yaklaşım daha ziyade basın-ifade özgürlüğü şeklinde kabul edilmektedir[579]. Ancak şüphesiz bu hakkın günümüz dünyasında en çok ses getiren kararlarından birini ABAD'ın 13 Mayıs 2014 tarihli Google- İspanya[580] oluşturmaktadır. Aşağıda bu karar ayrıntılı olarak ele alınacaktır.

2. Unutulma Hakkının Unsurları

Unutulma hakkının temel itibariyle iki unsuru olduğu kabul edilmektedir. Bu unsurlar bilgi unsuru ve zaman unsuru olarak adlandırılmaktadır[581]. Bilgi unsuru

---

http://voices.washingtonpost.com/securityfix/2008/12/court_rules_against_teacher_in.html (Son Erişim Tarihi: 25.09.2021).

[576] **YAVUZ** Can, Unutulma Hakkı, Güncellenmiş ve Genişletilmiş 3. Baskı, Seçkin Yayıncılık, Ankara 2020, s. 29-30; **LAÇİN** İrem, Unutulma Hakkı, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Doç. Dr. Melike Batur Yamaner'in Anısına Armağan, C: 1, Y: 2014, ss. 391-418, s. 394.

[577] **AKGÜL**, "Unutulma Hakkı", s. 35.

[578] **WEBER**, s. 121; **GÜLENER,** s. 227.

[579] **WEBER**, s. 122; **WERRO**, s. 299-300.

[580] Google/İspanya Kararı, 13 Mayıs 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (Son Erişim Tarihi: 12.10.2021).

[581] **SÖZÜER** Eren, Unutulma Hakkı- İnsan Hakları Hukuku Perspektifinden Bir İnceleme, On İki Levha Yayınları, İstanbul, Ekin 2017, s. 42.

unutulma hakkına kaynaklık ederken iki temel özelliği bünyesinde barındırır[582]. Bu özellikler bilginin başlangıçtaki hukuki durumu ve niteliğine ilişkindir[583]. Unutulma hakkının zaman unsuru ise bilginin ortaya çıkmasından itibaren geçen zamanı ifade ederken temel aldığı nokta aradan geçen zamanın uzunluğu değil, bu zaman dilimindeki unutulma hakkına konu olan kişinin durumunda meydana getirdiği değişikliktir[584].

a. Unutulma Hakkının Konusu

Unutulma hakkının konusunu oluşturan bilgi unsurunun özelliklerinden ilki, başlangıçta hukuka uygun olarak yayılan bir bilginin varlığıdır[585]. İkinci özellik ise unutulma hakkına konu olan bilginin doğru nitelikte bir bilgiyi ifade etmesidir[586].

Zaman unsuru bakımından ele alındığında ise bilgi, ortaya çıktığı zamanda güncel ve doğru bilgi niteliğini taşımakta ise de zaman içerisinde hem güncelliğini hem de toplumsal önemini yitirmiş bilgi olmalıdır[587]. Bu konuda İsviçre Federal Mahkemesinin 1983 tarihli Paul IRNIGER kararı örnek olarak gösterilebilir. Söz konusu olayda İsviçre'nin Zug kentinde 70'lerin sonuna doğru bir radyo kanalının, 1939 tarihinde idama mahkum edilen Paul IRNIGER'ın yaşamını anlatan bir piyes yayınlayacağını duyurmasının ardından idama mahkum olan IRNIGER'in oğlu mahkemeye başvurmuş ve piyesin yayınlanmasını önlemiştir[588]. Paul IRNIGER'ın oğlu yapmış olduğu başvurusunda kırk yıl önce idam cezasına çarptırılmış olan babasının söz konusu piyes ile kişilik haklarının ihlal edileceğini ve zarar göreceğini iddia etmiştir. Mahkeme kararda aradan geçen zamana rağmen tam bir unutulmanın mümkün olmadığını ancak böyle bir yayın ile olayın tekrardan hafızalarda yer etmesinin toplumda uygun olmayacağını ifade ederek unutulma hakkının doğduğuna karar vermiştir. Bu anlamda özellikle söz konusu olayın üzerinden geçen zamana dikkat çekerek haberin güncelliğini yitirdiğinin altı çizilmiştir.

---

[582] **SÖZÜER**, s. 42.
[583] **SÖZÜER**, s. 42.
[584] **SÖZÜER**, s. 42.
[585] **SÖZÜER**, s. 43.
[586] **SÖZÜER**, s. 42.
[587] **KAHRAMAN** Zafer, Unutulma Hakkı, Vedat Kitapçılık, İstanbul 2022, s. 29-30.
[588] **BAŞALP**, " Tüzüğün Temel Yenilikleri", s. 95.

b. Unutulma Hakkının Öznesi

Günümüzde genel kabul gören görüşe göre unutulma hakkının öznesini, yalnızca gerçek kişiler oluşturmaktadır[589]. Nitekim gerek ABAD'ın unutulma hakkına ilişkin kararı gerek AB hukukunun bu hakka yaklaşımı, hakkın öznesinin kişisel veri sahibi gerçek kişileri oluşturduğu yönündedir. Genel yaklaşım bu olmakla birlikte tüm AB üyesi ülkeler bakımından aynı yaklaşımın korunduğu söylenemez. Nitekim İtalya ve Avusturya bakımından unutulma hakkının öznesini gerçek kişilerin yanında tüzel kişilerinde oluşturduğu kabul edilmektedir[590]. Ancak her ne kadar gerek bazı mahkeme kararlarında gerek doktrinde tüzel kişilerinde unutulma hakkı kapsamında başvuru yapabileceğine ilişkin görüşler paylaşılsa da genel kabulün bu yönde olmadığının altı çizilmelidir[591].

c. Unutulma Hakkının Yükümlüsü

Kural olarak unutulma hakkını talep eden veri öznesinin bu hakkının yerine getirilmesinde görevli olan kimse, unutulma hakkının yükümlüsü olarak ifade edilmektedir[592]. Ancak unutulma hakkını talep eden veri öznesinin taleplerini kime yönelteceğine ilişkin en net ayrım ABAD'ın 13 Mayıs 2014 tarihli "Google- İspanya" kararında yer bulmuştur[593]. Karara göre unutulma hakkının öncelikli olarak yükümlüleri, arama motorları olacaktır[594]. Buna göre unutulma hakkını kullanmak isteyen kişisel veri sahibi gerçek kişiler, öncelikli olarak arama motorlarına başvuruda bulunacaktır. ABAD'ın kararıyla Google da unutulma hakkına başvurmak isteyenlerin talepleri için bir sistem kurmuş, buraya başvuruda bulunanların taleplerinin değerlendirilmesinde, kişilerin gizlilikleri ile kamunun bilgi alma ve bilgiyi dağıtma

---

[589] **YAVUZ**, s. 51-52; **KAHRAMAN**, s. 23.
[590] **SÖZÜER**, s. 54.
[591] **YAVUZ**, s. 53-57; Giriş, Birinci Bölüm, Kişisel Verilerin Bir Hak Olarak Koruması ve Bazı Temel Kavramlar, II Kişisel Veri ile İlgili Temel Kavramlar, B. Kişisel Veri Kavramı, 1. Kişisel Verinin Unsurlar, b. Kişisel Verinin Unsuru Olarak Kimliği Belirli Ya Da Belirlenebilir Kişi, aa. Tüzel Kişilere İlişkin Kişisel Verilerin Durumu, s. 22.
[592] **KAHRAMAN**, s. 118; **YILDIZ** Tuba, Kişilik Hakları Açısından Unutulma Hakkı, Yayınlanmamış Yüksek Lisans Tezi (Yönetici: Doç. Dr. Emel Batur), Ankara, 2019, s. 103.
[593] **YILDIZ**, s. 103; **KAYA** Mehmet Bedii, "Avrupa Birliği Adalet Divanı'nın 13 Mayıs 2014 Tarihli Google Unutulma Hakkı Kararı", Küresel Bakış, Yıl: 5, Sayı: 17, Nisan 2015, ss. 27-52, s. 32.
[594] **KAYA**, "Google Kararı", s. 32.

hakkı noktasında hassas davranacağını ifade etmiştir[595]. ABAD'ın kararını uygulamaya koyarken ayrıca Google bir danışma kurulu da oluşturmuştur[596].

3. Unutulma Hakkı Kapsamında Google İspanya Kararı

Unutulma hakkı denildiğinde örnek verilebilecek en önemli karar şüphesiz ABAD'ın 13 Mayıs 2014 tarihli Google- İspanya kararıdır. Kararda[597] İspanya'da ikamet eden Mario Costeja GONZALEZ, İspanya'nın özellikle Katalonya bölgesinde günlük tirajı yüksek olan La Vanguardia isimli gazetede kendisiyle ilgili ilanların halen yer aldığını tespit etmiştir. 10 Ocak ve 9 Mart 1998 tarihli sosyal güvenlik borçlarına ilişkin hakkında uygulanan haciz işlemleriyle bağlantılı olarak yapılan gayrimenkul açık artırma ilanları halen daha internetten yaptığı aramalarda karşısına çıkmaktadır. Neticede Bay Costeja GONZALEZ bu durumu yargıya taşınmıştır[598]. Mahkemede arama motoru Google aracılığı ile öğrendiği haberlerde, yıllar öncesine dayanan bu haberin güncelliğini yitirdiği gerekçesiyle gazetede yer alan haberlerin kaldırılması için İspanyol Veri Koruma Otoritesine başvuruda bulunmuştur. Ancak La Vanguardia isimli gazetenin, haber kaynaklarında yer alan bilgilerin İspanyol hukukuna göre açık artırmada aleniyeti sağlanmak adına paylaşılmasının hukuka uygun olduğu gerekçesiyle talebi reddetmiştir. Mario Costeja GONZALEZ ayrıca kendisi hakkında olan kişisel verileri gizlemesine ya da kaldırmasına dolayısıyla arama motorlarında çıkmasının önüne geçilmesine ve La Vanguardia'ya yapılan bağlantı linklerinin bu vesileyle görünür olmaktan çıkmasına karar verilmesi adına Google Spain şirketi ile Google Inc. şirketine de şikâyette bulunmuştur. Şikâyeti gazete bakımından reddeden İspanyol Veri Koruma Otoritesi, Bay Gonzalez'in şikayetini Google Spain ve Google Inc. bakımından kabul etmiştir.

İspanyol Veri Koruma otoritesi arama motoru işletenlerin, veri korumaya ilişkin mevzuat hükümlerine tabi olduklarını zira işleme faaliyeti gerçekleştirdiklerini ve bu faaliyetlerden veri sorumlusu sıfatıyla sorumlu olduklarını ifade etmiştir. Ancak bu kez Google İspanya ve Google Inc, İspanya Ulusal Yüksek Mahkemesinde karara

---

[595] **ŞEREFOĞLU HENKOĞLU** Halise, "Unutulma Hakkı: Dijitalleşme Sürecinde Bilgiye Erişim Özgürlüğünü Tehdit Eder mi? Bilgi Sistemleri ve Bilişim Yönetimi: Beklentiler ve Yeni Yaklaşımlar", 2017, ss. 191-212, s. 205.
[596] **ŞEREFOĞLU HENKOĞLU**, s. 205.
[597] Google- İspanya Kararı.
[598] Google/İspanya Kararı; **KAYA**, "Google Kararı", s. 32.

karşı çıkarak dava açmıştır. Açılan ayrı davaların birleşmesinin ardından mahkeme, kararı ABAD'na taşımıştır. ABAD, Direktif'i göz önünde tutarak kararını vermiştir. Kararda, arama motorlarının gerçekleştirdikleri veri işleme faaliyetlerinin, üçüncü taraf internet sitelerinin gerçekleştirdikleri veri işleme faaliyetlerinden ayrıldığını, dolayısıyla arama motorlarının da 95/46 EC sayılı Direktif'ten doğan yükümlülüklere uyması gerektiği ifade edilmiştir. ABAD ayrıca arama motorları aracılığı ile kamunun bilgilere erişiminde üstün bir menfaatini gösteren bir durumun olmaması halinde kişilerin özel hayat gizliliklerinin ön planda olduğunu, dolayısıyla kişisel verilerin artık güncel olmayan, geçersiz ya da amacı aşan şekilde tutulduklarını ifade edilerek arama sonuçlarında yer alan bu bağlantıların silinmesi gerektiği sonucuna varmıştır[599].

4. Türk Hukukunda Unutulma Hakkı

KVKK bakımından unutulma hakkına yer verilmemiş olsa da bu hak hem yargı kararlarına konu olmuş hem de doktrinde oldukça tartışılagelmiştir. Bununla birlikte bu hakka yasal dayanak olacak kanun maddeleri bulunmaktadır. Nitekim KVKK'nın 7. maddesi, kanuna uygun işlenme faaliyetine konu olan verilerin işleme amaçlarının kalmaması halinde re'sen ya da veri sahibinin talebiyle veri sorumlusunca tarafından silineceği, yok edileceği ya da anonimleştirileceğini ifade etmektedir. Kanun m. 11/f.1-e'de kişisel veri sahiplerinin veri sorumlusuna yapacakları bir başvuru ile ilgili verilerin silinmesini ya da yok edilmesini talep hakkı olduğunu ifade etmektedir. Kanun'un 7. maddesine aykırı hareket edenlerin ise m. 17 kapsamında TCK m. 138'e göre cezalandırılacağı ifade edilmiştir.

Hukukumuzda unutulma hakkı kapsamındaki yargı kararlarından biri YHGK'nun 2015 tarihli kararıdır[600]. Karar, kamu görevini kötüye kullanarak, cinsel saldırı mağduru bireyin açmış olduğu manevi tazminat istemine ilişkindir. Davacı, Nisan 2010'da yayımlanan bir kitapta rızası dışında isminin alenen yer aldığını ve bu durumun kişilik haklarının ihlaline sebebiyet verdiğini ifade etmiştir. Yargıtay Hukuk

---

[599] **NALBANTOĞLU** Seray, "Bir Temel Hak Olarak Unutulma hakkı (Right to be Forgotten As a Fundamental Right)", TAAD, Yıl:9, Sayı:35 (Temmuz 2018), ss. 583-605, s. 591.

[600] **YHGK**, E. 2014/4-56, K. 2015/1679, T. 17.06.2015 https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=hgk-2014-4-56.htm&kw=`2014/4-56,`+K.+`2015/1679,`+&cr=yargitay#fm (Son Erişim Tarihi: 25.09.2021); **YAVUZ**, s. 131; **AKKURT** Sinan Sami, "17.06.2015 Tarih, E. 2014/4-56, K. 2015/1679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı ve Mukayeseli Hukuk Çerçevesinde "Unutulma Hakkı"", Ankara Üniversitesi Hukuk Fakültesi Dergisi, 65 (4) 2016: 2605-2635.

Genel Kurulu başvurucunun rızası dışında kitapta yer verilen ismin kişisel veri niteliğinde olduğunu, unutulma hakkı gözetilerek, sadece dijital platformlardaki verilerin değil, insanların kolay şekilde ulaşabileceği bu tarz kişisel verilere yönelik de kabulünü gerekli bulmuştur. Netice olarak davacının isminin alenen kitapta bulunması özel hayatın gizliliği ve unutulma hakkı bakımından ihlal olarak nitelendirilmiş başvurucu lehine manevi tazminata hükmedilmiştir.

Unutulma hakkına konu olan bir diğer önemli karar, Anayasa Mahkemesine bireysel başvuru yapan N.B.B kararıdır[601]. Söz konusu başvuruda N.B.B, bir gazetenin internette yer alan arşiv sayfalarında uyuşturucu kullandığı iddiasıyla açılan davada verilen adli para cezasına ilişkin 1998 ve 1999 tarihli haberlerin kaldırılması adına başvuruda bulunmuştur. Mahkeme başvuruyu Anayasa m. 17 ve m. 20 çerçevesinde değerlendirerek artık haber değeri taşımayan ya da kamu yararı içermeyen haber içeriklerinin, özel hayatın gizliliği hakkından ve veri sahibinin verilerinin silinmesini talep hakkından üstün olmadığını ifade etmiştir. Bu kararlar KVKK'nın yürürlüğe girmesinden önceki dönemleri içermesine rağmen unutulma hakkının KVKK kapsamında yasal çerçeveye oturtulmamış olması büyük bir eksiklik olarak görülmektedir[602].

Son olarak daha yakın tarihli Kişisel Verileri Koruma Kurulu'nun kararları unutulma hakkına örnek teşkil etmektedir[603]. Tüm bu örnek kararlar eşliğinde gerek Kişisel Verileri Koruma Kurulu'na konu olan kararlarda gerek mahkeme kararlarında

---

[601] AYM, Başvuru No.: 2013/5653 Karar Tarihi: 3.3.2016 R.G. Tarihi: 24.8.2016 R.G. No: 29811 https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/5653 (Son Erişim Tarihi: 12.10.2021); **ÇELİKEL**, s. 218; **YAVUZ**, s. 141 vd.

[602] **GÜLENER**, s. 235; Farklı bir görüş için **ÇELİKEL**, s. 198.

[603] Kişisel Verileri Koruma Kurulu'nun 23 Haziran 2020 Tarihli ve 2020/481 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6776/2020-481 (Son Erişim Tarihi: 03.11.2022). Kararda, veri sahiplerinin internet üzerinde yer alan haber sitelerinde yer alan isimlerinin silinmesini talep ettikleri, öte yandan yine başka başvuruculaın Google gibi arama motorlarında kendileri ile ilgili bazı bilgilerin indekslenmelerini istemedikleri sebeple başvuruda bulundukları ifade edilmiştir. Kurum bu kararında, veri sahiplerinin bu taleplerinin ilgili veri sorumluları tarafından reddedilmesi halinde ya da bu taleplerine cevap alamamaları halinde Kurul'a doğrudan başvurabilecekleri gibi mahkemeye de başvurabileceklerini ifade etmiştir. Kurumun verdiği diğer bir karar Kişisel Verileri Koruma Kurulu'nun 08 Aralık 2020 tarihli ve 2020/927 sayılı kararıdır. https://www.kvkk.gov.tr/Icerik/6871/2020-927 (Son Erişim Tarihi: 03.11.2022). Kararda üniversitede görev yaparken bir aile yakının üniversite içinde açılan kadroya başvurduğunu ancak sonrasında bu konu ile ilgili belirli haber sitelerinde asılsız haberler yapıldığını dolayısıyla bu asılsız haberlerin kaldırılması için başvuruda bulunulduğu yer almaktadır. Her ne kadar bu haberlerden sonra üniversite kendi içerisinde bir soruşturma başlatmışsa da üniversitenin bir usulsüzlük tespit etmediği ancak başvurucunun haber sitelerindeki URL'lerin kaldırılması talebinin veri sorumlularınca reddedildiği ifade edilmiştir. Kurum, haberlerin 2020 yılına ait olduğunu ifade ederek güncel olduğunu, keza haberde yer alan bilgilerin söz konusu kişinin iş yaşamına ilişkin olduğu ve özel hayatına ilişkin olmadığına karar vererek karara konu olan şikayet bakımından KVKK nezdinde yapılacak bir işlem olmadığını ifade etmiştir.

unutulma hakkının varlığı kabul edilse de bu hakkın yasal çerçevesinin yapılacak uyumlaştırma neticesinde kanun sistematiğinde yerini alması gerektiği kanaatindeyiz.

B. VERİ SAHİBİNİN VERİ TAŞINABİLİRLİĞİ HAKKI

Veri taşınabilirliği hakkı ("right to data portability") Genel Veri Koruma Tüzüğü'nde öngörülen yeni haklardan biri olup 95/46/EC sayılı Direktif'te düzenlenmemiştir. Veri taşınabilirliği hakkı GVKT'nin 20. maddesinde hüküm altına alınmış olup, işleme faaliyetleri rızaya ya da sözleşmeye dayanan ve işleme faaliyetlerinin otomatik araçlarla gerçekleştirildiği, ilgili veri sahibi kişinin kendiyle ilgili veri sorumlusuna sağlamış olduğu kişisel verileri, geniş ölçüde kullanım alanına sahip, yapılandırılmış ve elektronik sistemler aracılığıyla elde edilen verileri başka veri sorumlusuna aktarma hakkı olarak ifade edilmiştir.

GVKT'nin 20. maddesi kapsamında[604] veri taşınabilirliği hakkı, kişisel verilerin korunması kapsamında veri sahibinin kişisel verilere erişim hakkıyla ilişkilendirilmiştir[605]. Hatta bu hakkın GVKT'nin 15. maddesindeki erişim hakkıyla birleştirilmesi gerektiği önerilmiştir[606]. Ancak Avrupa Birliği Konseyi bu iki hakkın birleştirilmesi yönündeki görüşe karşı direnmiştir[607]. Doktrinde bu hakkı, erişim hakkının bir uzantısı olarak gören yazarlar da mevcuttur[608]. Ancak, veri taşınabilirliği

[604] Tüzüğün 20. maddesinin 1. fıkrası, ilgili veri sahiplerine kişisel verileri bir veri sorumlusundan başka bir veri sorumlusuna herhangi bir "engel olmadan" aktarma hakkı verir. Kişisel veriler, Tüzüğün 20. maddesinin 2. fıkrası gereği veri sahibinin talebi üzerine direkt olarak bir veri sorumlusundan başka bir veri sorumlusuna aktarılabilmektedir. Nitekim Resital 68, veri sorumlularının veri taşınabilirliğini mümkün kılan, teknik olarak uyumlu sistemler kullanmasını ve veri taşınabilirliği konusunda kolaylıklar sağlamalarını tavsiye etmektedir. GVKT m. 20/f.3'e bakıldığında ise veri taşınabilirliği hakkının hangi hallerde uygulanmayacağı ifade edilmiştir. Buna göre veri taşınabilirliği hakkı, kişisel verilerin işlenmesinin rızaya veya sözleşmeye dayanmadığı durumlarda uygulama alanı bulmayacaktır. Bununla birlikte bu hakkın kullanılabilmesi GVKT m. 20/f.1-b gereği işleme faaliyetlerinin otomatik yolla gerçekleştirilmesi halinde mümkün olmaktadır. Bir diğer ifade ile veri taşınabilirliği hakkının otomatik olmayan yollarla işlenmesi durumunda söz konusu olamayacağı ifade edilebilir. Nitekim Resital 68'de de veri taşınabilirliği hakkının, veri işlemenin kamu menfaatleri gözetilerek gerçekleşen bir görevin ifası veya veri sorumlusunca resmi bir yetkinin kullanıldığı durumda, veri sorumlusunun kamu görevlerini yerine getirmesi veya yasal bir yükümlülüğe uyması için gerekli olduğu durumlarda geçerli olmadığı belirtilmiştir. Dolayısıyla bu gibi durumlarda veri sorumlularının veri taşınabilirliği hakkını sağlama yükümlülükleri bulunmamaktadır.

[605] **VANBERG** Aysem Diker/ **ÜNVER** Mehmet Bilal, "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?", European Journal of Law and Technology Vol 8, No 1, 2017, s. 2.

[606] **KUNER** Christopher/**BYGRAVE** Lee A./ **DOCKSEY** Christopher, The EU General Data Protection Regulation (GDPR) A Commentary, Assistant Editor LAURA **DRECHSLER,** Oxford University Press 2020, First Edition published in 2020, s. 500.

[607] **KUNER/BYGRAVE/DOCKSEY**, s. 500.

[608] **VANBERG/ÜNVER**, s. 2.

hakkının kapsamının, erişim hakkından daha dar olduğu ifade edilmektedir[609]. Nitekim, veri taşınabilirliği hakkı erişim hakkından ayrı olarak, ilgili veri sahiplerine yalnızca elde etme ve yeniden kullanma değil, aynı zamanda sağladıkları verileri başka veri sorumlularına iletme imkânı tanır[610].

29. Madde Çalışma Grubu, veri taşınabilirliğine ilişkin yayımladığı ilk rehberinde veri taşınabilirliğinin ilk amacının, bir hizmet sağlayıcıdan diğerine veri aktarımını kolaylaştırmak, böylece hizmetler arasındaki rekabeti arttırmak ve bu bağlamda yeni hizmetlerin yaratılmasını mümkün kılmak olduğunu ifade etmiştir[611]. Ancak rehberin güncellenmesiyle veri taşınabilirliği hakkının amacının, ilgili veri sahibi kişilerin kendi kişisel verileri üzerine hâkimiyeti arttırarak onları yetkilendirmeyi amaçladığını ifade edilmiştir[612]. Dolayısıyla bu yeni hakkın amacı, ilgili veri sahibi kişiyi yetkilendirmek ve kendisine ilişkin kişisel verileri üzerinde daha fazla kontrol sahibi olmasını sağlamaktır[613]. Bu hak aynı zamanda kişisel verilerin bir veri sorumlusundan diğerine doğrudan aktarılmasına imkân verdiği için AB'de kişisel verilerin serbest dolaşımını destekleyecek ve veri sorumluları arasındaki rekabeti teşvik edecek önemli bir araç olarak değerlendirilmektedir[614]. Aynı zamanda dijital tek pazar stratejisi bağlamında yeni hizmetlerin geliştirilmesini teşvik edeceği ileri sürülmüştür[615].

Veri taşınabilirliği, kişisel verileri alma ve veri sahibinin isteklerine göre işleme hakkını garanti eder. Bununla birlikte GVKT m. 20 çerçevesinde veri taşınabilirliği taleplerine cevap veren veri sorumluları, ilgili kişi veya kişisel verileri alan başka bir veri sorumlusu tarafından gerçekleştirilen işlemlerden sorumlu değildir[616]. Ancak veri sorumluları, veri sahibinin bir hak kaybı yaşamaması adına hareket etmeli ve bu amaçla belirli güvenlik tedbirlerini almalıdır[617]. Örneğin, iletilecek kişisel veri türünün gerçekten de veri sahibinin iletmek istediği veri olup olmadığını belirlemek için belirli

---

[609] **KUNER/BYGRAVE/DOCKSEY**, s. 500.
[610] **BUSSCHE/VOIGHT,** s. 168-170; **LAMBERT,** 229-231; **29. Madde Çalışma Grubu**, WP 242, s. 3.
[611] **KUNER/BYGRAVE/DOCKSEY**, s. 500.
[612] **29. Madde Çalışma Grubu**, WP 242, s. 3.
[613] **29. Madde Çalışma Grubu**, WP 242, s. 3.
[614] **29. Madde Çalışma Grubu,** WP 242, s. 3.
[615] **29. Madde Çalışma Grubu,** WP 242, s. 3.
[616] **29. Madde Çalışma Grubu,** WP 242, s. 6.
[617] **CAREY**, s. 139; **HERT** Paul De/**PAPAKONSTANTINOU** Vagelis/**MALGIERI** Gianclaudio/ **BESLAY** Laurent/**SANCHEZ** Ignacio, "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", Computer Law & Security Review, 2018, ss. 193–203, s. 196-199.

prosedürler oluşturulması bu tedbirlere bir örnektir[618]. Veri taşınabilirliği talebini yanıtlayan veri sorumlularının, verileri aktarmadan önce verilerin kalitesini kontrol etme ve doğrulama şeklinde özel bir yükümlülüğü yoktur[619]. Ancak bu verilerin zaten GVKT m. 5/f.1'de ifade edilen ilkelere göre doğru ve güncel olması gerekir. Benzer şekilde kişisel verilerin aktarıldığı yeni veri sorumlusu da GVKT m. 5'te belirtilen ilkelere uymalıdır.

Veri sahibi, veri taşınabilirliği işleminden sonra bile veri sorumlusunun hizmetini kullanmaya devam edebilir[620]. Bir diğer ifade ile veri taşınabilirliği, kişisel verilerin veri sorumlusunun sistemlerinden otomatik olarak silinmesini sağlamaz ya da aktarılan kişisel verilere uygulanan saklama süresini etkilemez[621]. Dolayısıyla veri sorumlusu kişisel verileri işlemeye devam ettiği sürece, ilgili kişi haklarını kullanabilir. Benzer şekilde veri sahibi GVKT kapsamında unutulma hakkını kullanmak isterse, veri sorumlusu bu tür bir silme işlemini veri taşınabilirliğini ileri sürerek erteleme ya da reddetmeyi seçemez[622].

Veri taşınabilirliği hakkına dahil olan veriler, veri sahibinin kendisi ile ilgili kişisel verilerini kapsar[623]. Bir diğer ifade ile anonim ya da veri sahibini ilgilendirmeyen herhangi bir veri kapsam dahilinde olmayacaktır. Bununla birlikte, bir veri sahibiyle açık bir şekilde ilişkilendirilebilen takma adlı veriler, veri taşınabilirliği hakkına dahil kişisel veri olacaklarıdır[624]. Elbette bu hakkın kullanımı GVKT m. 20/f.4 gereği başkalarının hak ve özgürlüklerini olumsuz etkilememelidir. Görüleceği üzere KVKK kapsamında yer almayan bu hakkın ilgili kişisel veri sahibi kişilerin haklarını korumada önemi büyüktür. Dolayısıyla kanaatimiz bu hakkın da KVKK kapsamında düzenlenmesi gerektiğidir.

---

[618] **29. Madde Çalışma Grubu,** WP 242, s. 6.
[619] **29. Madde Çalışma Grubu,** WP 242, s. 6.
[620] **29. Madde Çalışma Grubu,** WP 242, s.7.
[621] **29. Madde Çalışma Grubu,** WP 242, s. 7; **BUSSCHE/VOIGHT**, s. 175.
[622] **29. Madde Çalışma Grubu,** WP 242, s. 7.
[623] Bir kişinin çevrimiçi müzik hizmeti sunan bir uygulama aracılığıyla dinlediği şarkılar, kişisel verilere dayalı olarak işlendiğinden genellikle veri taşınabilirliği kapsamında olan kişisel verilere örnektir.
[624] **29. Madde Çalışma Grubu,** WP 242, s. 9.

C. İŞLEME FAALİYETLERİNİN KISITLANMASINI İSTEME HAKKI

İşleme faaliyetlerinin kısıtlanmasını isteme hakkı, GVKT'nin 18. maddesinde düzenlenmiştir. GVKT m. 18/f.1-a'ya göre, veri sahibinin işlenen kişisel verilerinin doğruluğuna ilişkin bir itirazının bulunması halinde, veri sorumlusunun bu verilerin doğruluğunu teyit edinceye kadar geçen sürede veri sahibi işleme faaliyetinin kısıtlanmasını talep edebilecektir. GVKT m. 18/f.1-b'ye göre de işleme faaliyetlerinin hukuka aykırılığı ve ilgili kişinin verilerinin silinmesine itiraz yerine verilerinin kullanımını kısıtlanmayı talebi halinde de bu hakkın varlığından söz edilmektedir. Bu hakkın kullanılması durumunda veri sorumluları, kısıtlama hakkına konu olan verileri saklayabilir, ancak veri sahibinin rızası olmadıkça bu verileri kullanamazlar[625].

Kısıtlama hakkının geçerli olduğu durumlarda, GVKT'nin 19. maddesi uyarınca, veri sorumlularının, kısıtlama hakkına ilişkin gerekli bilgilendirmeyi kişisel verilerin açıklandığı her alıcıya bildirmesi gerekmektedir. Ancak veri sorumlularının bu bildirim yükümlülüğü imkânsız olmamalı ya da ölçüsüz bir çabaya girişmelerine mahal vermemelidir[626]. Bununla birlikte veri sorumlularının kısıtlama talebini kabulü durumunda, şartları oluştuğu takdirde bu kısıtlamanın kaldırılmasına ilişkin GVKT m. 12 çerçevesinde ilgili veri sahibi kişileri de bilgilendirmesi gerekmektedir[627]. KVKK'ya bakıldığında ise işlemenin kısıtlanmasını talep etme hakkının düzenlenmediği görülmektedir. Oysa KVKK kapsamında da veri sahiplerinin işlemenin kısıtlanmasını talep etme hakları mevcut olmalıdır. Nasıl ki KVKK m.11./f.1-d'de, veri sahibinin verileri üzerinde düzeltme hakkı mevcutsa, ya da aynı fıkranın e bendi gereği verilerinin silinmesini isteme hakkı mevcutsa, Tüzüğün 18. maddesinde şartları oluştuğu takdirde işlemenin kısıtlanmasını talep edebilmelidir.

---

[625] **CAREY**, s. 147.
[626] **CAREY** Peter, A Practical Guide to UK and EU Law, s. 148; **WOLTERS** P.T.J., "The Control by and Rights of the Data Subject Under the GDPR", Journal of Internet Law, Cilt 22, Sayı 1, 2018, ss. 7-18, s. 10.
[627] **CAREY**, s.148; **WOLTERS**, s. 10.

D. OTOMATİK KARAR ALINMASINI KISITLAMA HAKKI

Kişisel verileri üzerinde ilgili veri sahiplerinin kontrol mekanizmasını güçlendirecek haklardan biri de kişisel verileri otomatik sistemler aracılığı ile elde edilen veri sonuçlarına itiraz etme hakkıdır. Dolayısıyla kişisel verilerin otomatik sistemler aracılığı ile analiz edildiği veriler üzerine ilgili kişinin itiraz hakkı bulunmaktadır. Esasında bu hakkın bir yasaklama hakkı olduğu ifade edilmektedir[628]. Otomatik karar alınmasını kısıtlama hakkı, GVKT'nin 22. maddesinde, veri sahibinin, profillemeyi de içeren otomatik işlemeleri ve ilgili veri sahipleri hakkında hukuken sonuç doğuran ve bu kişileri etkileyen kararlara konu olmama hakkı olarak ifade edilmiştir. Tüzük, veri sahibinin kendisini önemli ölçüde etkileyen ifadesi ile tam olarak ne ifade edildiğini açıklamamaktadır[629]. Ancak Resital 71'de bazı örneklere yer verilmiştir. Örneğin, çevrimiçi yapılan bir kredi ya da elektronik iş başvurusunda veri sahibinin bu hakkı kullanabileceği kabul edilmektedir. Zira bu tür veri işlemelerde veri sahibi çalışma performansı, sağlık durumu, satın alma alışkanlıkları, sosyal ve ekonomik durumu, konumu gibi bilgiler yer almakta olup bu veriler kendisini önemli ölçüde etkileyebilecek nitelikte verilerdir[630].

Bununla birlikte GVKT'nin 22. maddesinin 2. fıkrası gereği ilgili veri sahibinin bu hakkı kullanmasının üç istisnası bulunmaktadır. Buna göre, veri sahibinin açık rızasının bulunması; veri sorumlusu ile arasında bunu gerektirecek bir sözleşme akdedilmiş olması ya da veri sorumlusunun, ilgili veri sahibi kişinin hak ve menfaatlerini güvenceye alarak Birlik ya da üye devlet mevzuatının izni dahilinde işleme faaliyetini gerçekleştirmesi halinde veri sahibi bu hakkını kullanamamaktadır[631].

KVKK kapsamında veri sahibinin işleme faaliyetlerini kısıtlama hakkı ile ilgili ifade ettiklerimiz burada da geçerlidir. Zira veri sahibinin otomatik karar alınmasını kısıtlama hakkı KVKK kapsamında ilgili veri sahibine tanınmış haklardan biri değildir. Ancak KVKK m.11/f.1-g, ilgili veri sahibinin sadece otomatik sistemler kullanılarak işleme faaliyetine konu olan verilerinin analiziyle aleyhine çıkan sonuçlara itiraz etme hakkı olduğunu ifade etmektedir. Elbette bu itiraz hakkının bir

---

[628] **WOLTERS**, s. 12.
[629] **CAREY**, s. 149.
[630] **WOLTERS**, s. 12.
[631] **KÜZECİ,** s. 263.

kısıtlama ya da yasaklama şeklinde değerlendirilmesi mümkündür. Ancak her halükârda Tüzük hükümlerinde olduğu şekliyle veri sahibinin hangi hallerde bu hakkını kullanamayacağı belirsizdir. Kanaatimizce, otomatik yollarla işleme faaliyetlerine konu olan ve kendisi hakkında hukuken sonuç doğuran ve bu kişileri etkileyen kararlara konu olmama hakkı GVKT m. 22 referans alınarak mevzuat hükümlerinde düzenlenmelidir.

VI. UYUMLAŞTIRMA KAPSAMINDA UYGULANACAK İDARİ PARA CEZALARI

GVKT'nin yürürlüğe girmesi ile kişisel veri ihlallerinin önüne geçilebilmesi adına yapılan düzenlemelerin caydırıcı olması da hedeflenmiştir. Bu doğrultuda Tüzük hükümlerinin etkin bir şekilde uygulanabilmesi adına yapılan düzenlemelerin yanında uygulanacak idari para cezaları da bu amaç doğrultusunda belirlenmiştir. GVKT m. 83, idari para cezası kesilmesine ilişkin genel şartları ifade etmektedir. GVKT m. 83/f.1'de ifade edildiği üzere, kişisel veri ihlallerinde uygulanacak idari para cezaları her somut olaya göre ayrı olarak değerlendirilecektir.

İdari para cezalarının miktarının belirlenmesinde Tüzük kapsamında ikili bir ayrıma gidildiği görülmektedir[632]. Buna göre, veri sorumlusunun ve/veya işleme faaliyetini gerçekleştiren işleyenlerin yükümlülüklerinin ihlali söz konusu olduğunda 10 milyon Euro'ya kadar ya da bir şirket söz konusu ise, bir önceki mali yılın dünya çapındaki cirosunun %2 sine kadar idari para cezasına hükmedilebileceği GVKT m. 83/f.4'te ifade edilmiştir.

GVKT m. 83/f.5'e bakıldığında ise, işleme faaliyetlerini temel alan ilkeler; ilgili veri sahibi kişinin hakları; Tüzüğün 44 ile 49. maddeler kapsamında üçüncü ülkedeki bir alıcıya ya da uluslararası bir kuruluşa yönelik gerçekleştirdiği veri aktarımları; üye devletlerce kabul edilen yükümlülükler ve denetim makamlarının bir yaptırımı neticesinde ortaya çıkan veri ihlallerinde uygulanacak idari para cezası 20 milyon Euro'ya kadar, bir şirket söz konusu ise, bir önceki mali yılın dünya çapında yıllık cirosunun %4 üne kadar idari para cezasına hükmedilebileceği ifade edilmiştir. Bununla birlikte Tüzük uyarınca uygulanacak idari para cezaları hususunda etkinliği

[632] **SAKA/ÇAĞLAYAN /KOCA**, s. 217.

ve caydırıcılığı sağlamak adına her denetim makamının idari para cezası verme yetkisine sahip olması gerektiği ifade edilmiştir[633].

Görüldüğü üzere Tüzük kapsamında uygulanacak idari para cezalarının öncelikle etkin olmasına özellikle dikkat edilmiştir. Bununla birlikte denetim makamına da söz konusu para cezalarının miktarını belirlemede oldukça geniş bir yetki verildiği gözlemlenmektedir. Bu anlamda Tüzük, söz konusu denetim makamlarının belirleyeceği idari para cezalarındaki farklılıklardan dolayı 83. maddeyi son derece ayrıntılı düzenlemiştir. Üstelik Tüzük kapsamında idari para cezalarının belirlenme yöntemi de miktar ile sınırlı kalmamıştır. Daha önce yukarıda ifade edildiği üzere idari para cezaları söz konusu ihlale sebebiyet veren şirketlerin dünya çapındaki yıllık cirosuna göre belirli bir miktar dahilinde belirlenmiştir.

KVKK'ya bakıldığında ise idari para cezalarının 18. maddede düzenlendiği görülmektedir. Kanun'un "Kabahatler" başlıklı 18. madde hükmüne bakıldığında, Kanun'un 10. maddesi uyarınca aydınlatma yükümlülüğünü gerçekleştirmeyen veri sorumluları; 12. maddesi uyarınca veri güvenliğine ilişkin yükümlülükleri karşılamayan veri sorumluları ve veri işleyenler; 15. maddesi uyarınca Kurul tarafından kararlarına aykırı hareket eden ve 16. maddesi uyarınca VERBİS'e kayıt ve bildirim yükümlülüğüne uymayan veri sorumluları hakkında idari para cezası verileceği ifade edilmiştir. KVKK m. 18/f.2'de, hakkında idari para cezası uygulanacak kişiler, gerçek kişi olan veri sorumluları ile özel hukuk tüzel kişisi olan veri sorumlularıdır.

Görüldüğü üzere Tüzük hükümlerinin aksine Kanun'un 18. maddesi uyarınca idari para cezalarının miktarı belirlenirken her ne kadar bir alt sınır ve üst sınır belirtilmiş olsa da bu sınırların hangi hallerde geçerli olacağına ya da bu sınırların ne şekilde belirleneceğine ilişkin bir düzenlemeye yer verilmemiştir. Üstelik KVKK m. 18/f.1'e göre verilecek idari para cezaları sınırlı olarak sayılmıştır. Bir diğer ifade ile KVKK'da idari para cezasına hükmedilecek haller aydınlatma yükümlülüğüne aykırılık, veri güvenliğine ilişkin aykırılık, Kurul kararlarına aykırılık, Sicile kayıt ve bildirim yükümlülüğüne aykırılık olarak 4 ana başlık altında sayılmıştır. Buna karşın GVKT'nin 83. maddesi, idari para cezası verilmesine ilişkin veri ihlallerini çok daha kapsamlı olarak ele almıştır. Üstelik Tüzük, idari para cezalarının yalnızca alt ve üst sınır olarak değil aynı zamanda söz konusu ihlale sebebiyet veren şirketlerin yıllık

[633] **GVKT**, Resital 150.

toplam cirosuna göre oransal bir miktarda belirlenmesini öngörmüştür. Kanaatimizce KVKK kapsamında yapılacak uyumlaştırmaların idari para cezalarının gerek alt ve üst sınır bakımından gerekse Tüzük hükümlerinde olduğu şekli ile kuruluşların yıllık ciro miktarları dikkate alınarak revize edilmesi gereklidir. Zira her şirketin yıllık ciro miktarları farklı olup, cezalarında bu oranlar dahilinde belirlenmesi daha adilane olacaktır.

SONUÇ

Teknolojik gelişmelerin aldığı hız ve bilgi teknolojilerinde yaşanan gelişmeler karşısında veri üretimi oldukça yaygın hale gelmiştir. Kişisel verilerin korunması anlamında Avrupa'da 1970'li yıllardan itibaren hız kazanan gelişmeler bugün tüm dünyanın üzerine en çok eğildiği konulardan birini oluşturmaktadır. Zira bilgi toplumu olarak içinde bulunduğumuz çağda geçirdiğimiz değişim, yalnızca bireylerin mahremiyet alanlarına ilişkin olmayıp, verilerin bütünlüğü, gizliliği ve güvenli bir ortamda muhafazasını da içermektedir. Kişisel verilerin güvenliği tek başına bireyleri değil aynı zamanda küçük ve orta çaplı şirketler ile ülkeleri de ilgilendiren bir güvenlik konusudur. Bu anlamda uluslararası alanda yer alan ilk düzenleme, OECD tarafından hazırlanan Rehber İlkeler olarak yer alır. Bu düzenlemeden sonra, öncelikli amacı kişi hak ve özgürlüklerini otomatik işleme faaliyetleri kapsamında korumak olan 108 sayılı Sözleşme yürürlüğe girmiştir. İlk kez bu düzenlemeyle kişisel veriler bağımsız bir hak olarak korunmaya başlanmıştır. 108 sayılı Sözleşme uluslararası düzeyde kişisel verileri korumayan ilk bağlayıcı düzenleme olup AB üyesi olmayan ülkelerin sözleşmeye taraf olmaları mümkündür. Bu gelişmelere ek olarak ülkeler kendi yasal mevzuatlarını oluşturmuş, Avrupa Konseyi, Birleşmiş Milletler, OECD ile AB kapsamında yapılan çalışmalar hız kazanmıştır. 95/46/EC sayılı Direktif ile kişisel veri işleme faaliyetlerine ilişkin çizilen tablodan sonra özellikle GVKT'nin yürürlüğe girmesiyle birlikte etki alanı genişletilmiş ve çağın gereksinimlerine uygun bir yol izlenmeye başlanmıştır.

Avrupa'da durum böyleyken ülkemizde ise 2010 tarihli Anayasa değişikliği ile ilk kez kişisel veri koruması yasal bir zemine oturtulmuştur. 95/46/EC sayılı Direktif hükümlerini referans alan KVKK ise 2016 tarihinde yürürlüğe girmiştir. Avrupa'da yaklaşık 40 senedir yasal bir zemine oturan kişisel verilerin korunması konusu, ülkemizdeki taze geçmişine bakıldığında gerekli güncelliği henüz sağlayamamıştır. Özellikle KVKK'nın mülga 95/46/EC sayılı Direktif hükümlerini referans almış olması, içinde bulunduğumuz yılda büyük bir eksiklik olarak görülmektedir. Elbette KVKK yürürlüğe girdiği tarihten bu yana Kişisel Verileri Koruma Kurulu gerek ulusal mevzuatımız açısından eksiklikleri gerekse uluslararası alanda yapılan çalışmaları yakından takip etmiş ve bu alanda düzenli olarak çalışmalarını sürdürmüştür. Bu anlamda ayrıca Kanun hükümlerini esas alan pek çok yönetmelik, tebliğ ve kararnameler de çıkarılmış ve Kanun bakımından eksik kalan hususlar giderilmeye

çalışılmıştır. Ayrıca Kişisel Verileri Koruma Kurulu, yaptığı konferans, seminer, sempozyum, panel gibi etkinliklerle toplumda her yaştan bireyin kişisel verilerin korunması anlamında farkındalığa ulaşması için çaba harcamakta, düzenli olarak yayımladığı rehber ve broşürler ile kamuoyunda farkındalık yaratma çabalarını sürdürmektedir.

Ancak Türkiye'nin kişisel verileri koruma anlamında Avrupa ülkelerinde olduğu seviyeyi yakaladığını söylemek oldukça güçtür. Öncelikle KVKK'nın hak ve yükümlülüklere ilişkin getirdiği düzenlemeler oldukça genel bir anlatıma sahip olduğundan, Kişisel Verileri Koruma Kurulu'na ve yargı mercilerine oldukça geniş bir inisiyatif bırakılmaktadır. Mevzuatımız açısından veri sorumlusunun yükümlülükleri, ilgili veri sahibi kişinin hakları, kişisel veri ihlallerine uygulanacak idari yaptırım gibi hususlarda da Kanun'da yapılacak düzenlemelere ihtiyaç duyulmaktadır. Örneğin, veri sorumlularının veri ihlallerine karşı gerekli ve yeterli önlemleri almalarında caydırıcı olmak adına idari para cezalarının miktarı artırılmalıdır. İdari para cezalarının miktarı belirlenirken Tüzük hükümlerinde olduğu gibi alt ve üst sınır çizilmeli, şirketlerin yıllık ciro miktarları dikkate alınarak adilane bir uygulama sağlanmalıdır. İlgili veri sahibinin veri taşınabilirliği hakkı, unutulma hakkı gibi hakları KVKK kapsamında düzenlenmeli, bu hakların hangi durumlarda kullanılacaklarına ilişkin gerekli açıklamalar Kanunda yer almalıdır. Kişisel veri ihlali söz konusu olduğunda, veri sorumlusunun bildirim yükümlülüğüne ilişkin Kişisel Verileri Koruma Kurulu'nun 24 Ocak 2019 Tarih ve 2019/10 Sayılı Kararına İlişkin Duyurusunda yer alan KVKK m. 12/f.5 'deki "en kısa süre" ifadesinin 72 saat olarak yorumlandığı husus KVKK'da düzenlenmelidir. Kişisel verilerin korunması anlamında etkin bir rolü olan Veri Koruma Görevlisi kavramına da KVKK kapsamında yer verilmelidir. Benzer şekilde GVKT'de yer alan ve kişisel verilerin herhangi bir veri ihlaline sebep olmadan, en baştan itibaren korunmasını amaçlayan tasarım ile gizlilik ve varsayılan gizlilik ilkelerinin KVKK kapsamında da yer alması gerektiği açıktır. Zira söz konusu ilkelerin benimsenmesi ile Türk hukukunda da kişisel veri ihlallerinin ve hak kayıplarının önüne geçilmede daha ileri adımlar atılabilecektir. Kanunumuz açısından birden fazla veri sorumlusunun bir araya gelerek ortak amaçları dahilinde veri işleme faaliyetlerine ilişkin iş bölümü sözleşmesi yapabilmeleri mümkündür. Ancak ortak veri sorumlusu kavramına ilişkin düzenleme KVKK'da yer almalıdır. Kişisel veri işleme faaliyetlerinde yer alan "alıcı" ve "üçüncü kişi" kavramları da KVKK'nın tamımlar başlıklı 3. maddesine ilave edilmelidir.

Bilindiği üzere 2019 yılında T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı 2019-2023 yıllarını kapsayan On Birinci Kalkınma Planını TBMM'ye sunmuştur. On Birinci Kalkınma Planında gerek KVKK gerek GVKT bakımından önemli açıklamalara yer verilmektedir. Dolayısıyla bu plan ile kişisel verilerin korunması ve mevzuat çalışmalarının revize edilmesi ve kişilerin mahremiyet haklarını sağlamayı güçlendirici politikalar uygulanması amaçlanmaktadır. Görüldüğü üzere, ülkemizde kişisel verilerin korunmasına duyulan ihtiyaç karşısında yasal mevzuatımızın Tüzük hükümlerine göre güncellenmesi, yapılacak düzenlemelerin uluslararası alanda kabul gören yaklaşımlar ile uyumlu hale getirilmesi, verilerin depolanması ve yurt dışına aktarımına ilişkin gerekli güncellemelerin yapılması hedeflenmektedir. Bu açıdan bakıldığında, özellikle her geçen gün artan siber tehditlerin sayısı, siber güvenliğin dolayısıyla da veri güvenliğinin korunması anlamındaki önemi de ortaya koymaktadır. Bu noktada yapılacak düzenlemeler ile ülkemizde kişisel verilerin korunması anlamında güncel, çağa uygun yaklaşımların benimseneceği kanaatindeyiz.

Kanunda çalışmalar yapılırken Tüzük maddelerinde yer alan düzenlemeler gerek ülkemizdeki doktrin görüşleri gerek ülkemiz dışında yer alan ortak tartışma konuları dikkate alınarak değerlendirilmeli ve buna göre revize edilmelidir. Örneğin tüzel kişilerin ya da ölen kişilerin kişisel verilerine ilişkin durumların neler olacağına ilişkin daha spesifik yaklaşımlar benimsenmelidir. KVKK'nın Tüzük hükümlerine uyumlaştırılmasında, Avrupa Birliği'nde olduğu gibi bölgesel kapsam konusunda düzenlemeler yapılmalı, Kanunda yer almakla birlikte genetik verinin tanımı, sağlık verilerinin neleri kapsadığı, biyometrik verinin tanımı ayrıntılı olarak ele alınmalı, bu kavramların işlenme faaliyetlerine ilişkin hususlarda gerekli düzenlemeler hüküm altına alınmalı; Kurul kararı ile veri ihlallerine ilişkin olarak yapılacak 72 saatlik bildirim süresinin Kanun'un m. 12/f.5'e eklemesi yapılmalı; hukuka uygun işleme faaliyetleri bakımından çelişki yaratan açık rıza ve rızanın geri çekilmesi hususlarında gerekli düzeltme ve düzenlemeler yapılmalı, tebliğ ile düzenlenen veri sorumlusunun aydınlatma yükümlülüğüne ilişkin hükümlerin KVKK kapsamına alınması sağlanmalı, Kurul'un yerinde inceleme yetkisine ilişkin hususların hangi usul ve esaslara göre ve kim tarafından yapılacağının düzenlenmesi gereklidir. Ayrıca yapılacak düzenlemeler ile çocukların kişisel verileri, veri koruma görevlisi atanması, veri taşınabilirliği hakkı, unutulma hakkı, veri koruma etki değerlendirmesi gibi hususlara ve idari para cezalarının miktarları gibi hususların da düzenlenmesi gerekmektedir. Elbette Tüzük hükümlerinde yer alan ve KVKK'ya eklenmesi gereken hususlar titizlikle ele alınmalı

ve çağın gereksinimlerini karşılayacak bir yaklaşımla düzenlenmelidir. Zira her ne kadar kişisel verilerin korunması anlamında uluslararası alanda yararlanılan en güncel kaynak Tüzük olsa da Tüzüğün de bilgi teknolojilerinde her gün çıkan her yeniliğe cevap verebildiğini söylemek güçtür. Bu anlamda On Birinci Kalkınma Planı çerçevesinde Kanun metninde yapılacak düzenlemelerin yalnızca 2018 tarihinde yürürlüğe giren Tüzük hükümlerine göre değil, gelecekte gündemimizi meşgul edecek çok yönlü bir yaklaşıma sahip olması gerekmektedir.

KAYNAKÇA

Kitap, Makale ve Basılı Eserler

AKANDJİ-KOMBE Jean-François, Avrupa İnsan Hakları Sözleşmesi Kapsamında Pozitif Yükümlülükler, Avrupa İnsan Hakları Sözleşmesinin Uygulanmasına İlişkin Kılavuz Kitap, İnsan Hakları El Kitapları, No. 7, 1. Baskı, 2008.

AKDİ Murat, "Ana-Babanın Çocuğun Fotoğraf ve Görüntülerinin Sosyal Medyada Yayınlamasından Doğan Sorumluluğu" Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 2016, ss.123-144.

AKINTÜRK Turgut/**ATEŞ KARAMAN** Derya, Türk Medeni Hukuku, Aile Hukuku, C.II, 14.B., İstanbul 2012.

AKİPEK Jale/**AKINTÜRK** Turgut/**ATEŞ** Derya, Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku, Birinci Cilt, Yenilenmiş 16.bası, Beta Yayınları, İstanbul Eylül 2020.

AKGÜL Aydın, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta Yayınları, İstanbul 2014.

AKGÜL Aydın, "Kişisel Verilerin Korunmasında Yeni Bir Hak: 'Unutulma Hakkı' Ve AB Adalet Divanı'nın 'Google Kararı'", TBB Dergisi, 2016 (116), ss.11-38.

AKGÜN, Ali, **KESKİN**, Hüseyin, "Sosyal Bir Etkileşim Aracı Olarak Bilgi Yönetimi ve Bilgi Yönetimi Süreci", Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 1/2003, ss.175-183.

AKINCI Ayşe Nur, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi", Çalışma Raporu 6, T.C. Kalkınma Bakanlığı Yayın No: 2968, 2017.

AKINCI Ayşe Nur, Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti (Uzmanlık Tezi). T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Ankara, 2019.

AKKURT Sinan Sami, "Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış", Kişisel Verileri Koruma Dergisi, 2(1), 2020, ss.20-32.

AKKURT Sinan Sami, "17.06.2015 Tarih, E. 2014/4-56, K. 2015/1679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı ve Mukayeseli Hukuk Çerçevesinde "Unutulma Hakkı"", Ankara Üniversitesi Hukuk Fakültesi Dergisi, 65 (4) 2016: 2605-2635.

AKKURT Sinan Sami, "Kişisel Sağlık Verilerinin İşlenmesine ve Covıd19 Pandemisi Sürecinde Mobil Uygulamalarla Paylaşılmasına Hukukî Bir Bakış", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi Covid-19 Hukuk Özel Sayısı Yıl:19 Sayı:38 Yaz 2020/2 (Covid-19 Özel Ek) s.142-160.

AKSOY Hüseyin Can, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara 2010.

ALTINDAL Hasan/**ARSLAN** Yusuf Enes, "Türk Hukukunda Dijital Miras: Karşılaşılan Sorunlar ve Uluslararası Uygulamalar Çerçevesinde Bazı Çözüm Önerileri", Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, Cilt XXV, 2021, Sayı 1.

AMIRASLANLI Nijat, Türk ve Avrupa Birliği Hukukunda Kişisel Verilerin Aktarılması, On İki Levha Yayıncılık, Ekim 2022.

ARSLAN Hüseyin, "John Locke'un Siyaset Felsefesinin Temelleri Üzerine Bir Deneme", Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı:17, 2013/1.

ARSLAN Çetin/**ÖZDEMİR** Didar, "Ticari Sırların Ceza Hukuku Tarafından Korunması", International Conference On Eurasian Economies, 2017, Session 4A: Hukuk, ss.125-131.

AŞIKOĞLU Şehriban İpek, Avrupa Birliği ve Türk Hukuku'nda Kişisel Verilerin Korunması ve Büyük Veri, Yüksek Lisans Tezi, İstanbul 2018.

ATAK Songül, "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", TBB Dergisi, Sayı 87, 2010, ss.90-120.

AKYÜREK Güçlü, Özel Hayatın Gizliliğini İhlal Suçu, 2. Baskı, Seçkin Yayıncılık, 2014.

AVCI BRAUN Cihan, "Kişisel Verilerin İşlenmesinde Rıza", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 15, ss. 13- 33.

AYAN Mehmet, Eşya Hukuku II, Adalet Yayınları, 10. Baskı, Ankara, 2020.

AYBAY Aydın/**HATEMİ** Hüseyin**,** Eşya Hukuku, Gözden Geçirilmiş 4. Bası, Vedat Kitapçılık, İstanbul, 2014.

AYDIN Sedat Erdem, (AİHM İçtihatları Bağlamında) Kişisel Verilerin Kaydedilmesi Suçu, On Levha Yayınları, İstanbul, 2015.

AYÖZGER ÖNGÜN Çiğdem, Kişisel Verilerin Korunması Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, İstanbul, Beta Yayınları, 2016.

BARTOW Ann, "Our Date, Ourselves: Privacy, Propertization, and Gender." University of San Francisco Law Review, vol. 34, no. 4, Summer 2000, p. 633-704.

BAŞALP Nilgün, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt: 21, Sayı: 1, 2015, ss.77-106.

BAŞALP Nilgün, Kişisel Verilerin Korunması ve Saklanması, Ankara, 2009.

BAŞARA TURAN Gamze, "Kişisel Veri İşleme Sözleşmesi", Uyuşmazlık Mahkemesi Dergisi- Yıl 8, Sayı 16, Aralık 2020, ss. 57-90.

BERNAL Paul A., ''A Right to Delete?'', European Journal of Law and Technology, C. 2, S.2,2011.

BIETTI Elettra, "Consent as a Free Pass: Platform Power and the Limits of the Informational Turn." Pace Law Review, Vol. 40, No. 1, 2019, ss. 310-398.

BOZKURT YÜKSEL Armağan Ebru, "İnternet ve Unutulma Hakkı", 4.Uluslararası Bilişim Hukuku Kurultayı 2016 Bildiriler Kitabı, İzmir.

BOZBEL Savaş, Fikri Mülkiyet Hukuku, On İki Levha Yayınları, 1. Baskı, İstanbul, Eylül, 2015.

BOZLAK Ayhan, Avrupa İnsan Hakları Mahkemesi Kararları Çerçevesinde Türk Ceza Hukukunda Özel Hayatın Korunması, Adalet Yayınevi, Ankara, 2013.

BULUT Metin, "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", 2020/3 Ankara Barosu Dergisi, ss.101-150.

BÜYÜKSAĞIŞ Erdem, "Digital Varlıkların Miras Yolu ile İntikalı", Yargıtay Dergisi 2/2021, ss. 337-408.

CAREY Peter, Data Proctection A Practical Guide to UK And EU Law, 5. Baskı, Oxford University Press, İngiltere 2018.

CAVOUKIAN Ann, Privacy by Design The 7 Foundational Principles, https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/ (Son Erişim Tarihi: 06.08.2021).

CHU Natasha, "Protecting Privacy after Death", Northwestern Journal of Technology and Intellectual Property, Vol 13, No:2, September, 2015.

ÇEKİN Mesut Serdar, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 3. Baskı, On İki Levha Yayıncılık, İstanbul 2020.

ÇELİK Işıl, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması, On İki Levha Yayıncılık, Haziran 2022.

ÇELİKEL Serdar, Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, Doktora Tezi, Ankara, 2021.

ÇELİKTAŞ İlyas, "Vefat Eden Kişinin Elektronik Posta Hesabı Mirasçılara İntikal Eder Mi?", Terazi Hukuk Dergisi, Y.2011, C.VI, S.62, ss. 34-39 https://www-jurix-com-tr.lproxy.yeditepe.edu.tr/article/1320 (Son Erişim Tarihi: 27.12.2022).

DEĞİRMENCİOĞLU Burcu, "Klasik Egemenlik Anlayışında Bir Kırılma: "Pozitif Yükümlülük Doktrini" ve Türkiye'ye Yansıması", İnsan Hakları Yıllığı Cilt 39, 2021, ss. 55-104.

ÖZER DENİZ Miray, Özel Nitelikli Kişisel Verilerin İşlenmesi ve Bundan Doğan Sorumluluk, On İki Levha Yayıncılık, Eylül 2022.

DEVELİOĞLU Murat, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul 2017.

DURAL Mustafa/**ÖĞÜZ** Tufan, Türk Özel Hukuku, Cilt II, Kişiler Hukuku, Filiz Kitabevi, İstanbul, 2020.

DURAL Mustafa/**ÖĞÜZ** Tufan/**GÜMÜŞ** Mustafa Alper, Türk Özel Hukuku, Aile Hukuku, C.III, 10.B., İstanbul 2015.

DURNA Ufuk, Demirel Yavuz, "Bilgi Yönetiminde Bilgiyi Anlamak Bilgi Yönetiminde Bilgiyi Anlamak", Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Sayı: 30, Ocak-Haziran 2008, ss.129-156.

DUTERTRE Gilles, Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler, Avrupa Konseyi Yayınları, Eylül 2007, Ankara.

DÜLGER Murat Volkan, Kişisel Verilerin Korunması Hukuku, 1. Bası, İstanbul, 2019.

DÜLGER Murat Volkan, "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması", Yaşar Hukuk Dergisi C.1 S.2 Temmuz 2019.

DÜLGER Murat Volkan, "AB Genel Veri Koruma Tüzüğü ve KVKK'da Rıza Kavramı", ss. 1-9.

DÜLGER Murat Volkan, "GDPR'da Bulunan Ancak KVKK'da Yer Verilmeyen Bir Kavram: Ortak Veri Sorumlusu Kavramı ve Güncel Kararlar Işığında Değerlendirilmesi (A Concept In GDPR But Not Included In KVKK: The Concept of Common Data Responsible and Its Evaluation in the Light of Current Decisions)", February 24, 2021, ss.1-12.

DÜLGER Murat Volkan/**KAHRAMAN** Cansu Ceren/**YALÇIN** Simay, "GDPR ve KVKK Bakımından Çocukların Kişisel Verilerinin Korunması ve Konuya İlişkin Kurul Kararının Değerlendirilmesi" (Protecting Personal Data Of Children From Point Of GDPR and Personal Data Protection Law and Review Of Assize), ss.1-12.

Editör **İÇÖZ KOYUNCUOĞLU** Ömrüncegül, Hazırlayanlar: **ULUSEL** Melis/**BOZKURT** Tuğçe/**DEMİREL** İdil, Kişisel Verileri Koruma Kurulu Kararları, On İki Levha Yayıncılık, 2. Baskı, İstanbul, Mayıs 2022.

ERARSLAN Sevgi, Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller, On İki Levha Yayınları, Aralık, 2020.

ERDOS David, "The Emergence of Personal Data Protection as a Fundamental Right of the EU." Cambridge Law Journal, vol. 74, no. 2, July 2015, ss. 374-375.

ERDOĞAN Canan, "Çocukların Kişisel Verilerinin Korunması (Sosyal Medya Örneği Kapsamında)", D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019, ss. 2445-2467.

EREN Fikret, Borçlar Hukuku Genel Hükümler, 18. Baskı, Yetkin Yayınları, Ankara 2015.

EVANS A.C, "Europian Data Protection Law" The American Journal of Comparative law, Cilk 29, 1981, ss.571-582.

GEMALMAZ Burak, "Mülkiyet Hakkı", Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi – 6, İstanbul, 2018.

GEZDER Ümit: "Ölüm Sonrası Hatırayı Koruma Doktrini ve Ölüm Sonrası Kişiliğin Korunması Teorisi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, S.2007/1(65), https://dergipark.org.tr/tr/download/article-file/95696 (Son Erişim Tarihi: 27.12.2022).

GÖLCÜKLÜ Feyyaz/**GÖZÜBÜYÜK** Şeref, Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, 11.Ek Protokole Göre Hazırlanıp Genişletilmiş, 9. Bası, Turhan Kitabevi, Ankara, 2011.

GÜLENER, Serdar, Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı", TBB Dergisi, Y: 2012, S: 102, ss.219-240.

GÜRPINAR Damla, "Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk", D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı-2017, ss. 679-694.

HATEMİ Hüseyin/**OĞUZTÜRK KALKAN** Burcu, Kişiler Hukuku (Gerçek Kişiler-Tüzel Kişiler), Vedat Kitapçılık, İstanbul, 2014.

HAZEL Steven H., "Personal Data as Property." Syracuse Law Review, vol. 70, no. 4, 2020, p. 1055-1114.

HELVACI Serap, Gerçek Kişiler, Legal Yayıncılık, 9. Bası, Eylül 2021.

HERT Paul de/**LEENES** Ronald/**GUTWIRTH** Serge/**POULLET** Yves, European Data Protection: Coming of Age, Chapter 8 Privacy by Design: Leadership, Methods, and Results, **Ann Cavoukian,** Springer, 2013.

HERT Paul De/**PAPAKONSTANTINOU** Vagelis/**MALGIERI** Gianclaudio/ **BESLAY** Laurent/**SANCHEZ** Ignacio, "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", Computer Law & Security Review, 2018, ss. 193–203.

HORNUNG Gerrit & **SCHNABEL** Christoph, "Data protection in Germany I: The Population Census Decision and The Right to Informational Self-Determination", Computer Law & Security Report, Volume 25, Issue 1, 2009, s. 84-88.

HU Jim, Yahoo Denies Family Access to Dead Marine's E-Mail, CNET, https://www.cnet.com/news/yahoo-denies-family-access-to-dead-marines-e-mail/ (Son Erişim Tarihi: 12.04.2021).

HUSTINX Peter, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", 2015.

IŞIK KAMA Sezen, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış, Oniki Levha Yayınları,1. Baskı, Ocak 2021, İstanbul.

JANGER Edward J, "Privacy Property, Information Costs, and the Anticommons." Hastings Law Journal, vol. 54, no. 4, 2002-2003, p. 899-930.

JOHNSON Eric J./**BELLMAN** Steven/**LOHSE** Gerald L., "Defaults, Framing and Privacy: Why Opting In-Opting Out?" Received October 25, 2000; Revised and Accepted October 3, 2001, Marketing Letters, s 13:1, 5–15, 2002.

KAHRAMAN Zafer, Unutulma Hakkı, Vedat Kitapçılık, İstanbul 2022.

KANG Jerry, "Information Privacy in Cyberspace Transactions." Stanford Law Review, vol. 50, no. 4, April 1998, p. 1193-1294.

KAYA Cemil, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 69, Sayı 1-2, 2011, ss.317-334.

KAYA Mehmet Bedii, "Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi", 78(4) İstanbul Hukuk Mecmuası, 2020, ss.1859-1897.

KAYA Mehmet Bedii, "Avrupa Birliği Adalet Divanı'nın 13 Mayıs 2014 Tarihli Google Unutulma Hakkı Kararı", Küresel Bakış, Yıl: 5, Sayı: 17, Nisan 2015, ss.23-57.

KILINÇ Doğan, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt 61, Sayı 3, 2012, ss.1089-1169.

KORKMAZ Ali, "İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması", KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi 16 (Özel Sayı I): 99-103, 2014.

KORKMAZ İbrahim, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", Türkiye Barolar Birliği Dergisi, 2016, S.124.

KORFF Douwe, European Commıssion Directorate-General Justıce, Freedom And Security Comparative Study On Differeny Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments, Working Paper No. 2: Data protection laws in the EU, General Justice, Freedom and Security, Londra 20 Ocak 2010.

KOOPS Bert-Jaap/**LEENES** Ronald, "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law", 28 International Review of Law, Computers & Technology (2), Y: 2014, ss. 159-171.

KRALJIC Suzana, Children Have The Right To Privacy- Also Against The Parents, IV. Türkiye-Slovenya Karşılaştırmalı Hukuk Sempozyumu Kişilik Hakları, Ankara 2016, ss. 185-197.

KREBS Brian, "Court Rules Against Teacher in MySpace 'Drunken Pirate' Case", The Washington Post, 03.12.2008, http://voices.washingtonpost.com/securityfix/2008/12/court_rules_against_teacher_in.html (Son Erişim Tarihi: 25.09.2021).

KUNER Christopher, Transborder Data Flows and Data Privacy Law, Oxford University Press, 2013.

KUNER Christopher/**BYGRAVE** Lee A./**DOCKSEY** Christopher, The EU General Data Protection Regulation (GDPR) A Commentary, Assistant Editor LAURA **DRECHSLER,** Oxford University Press 2020, First Edition published in 2020.

KÜZECİ Elif, Kişisel Verilerin Korunması, On İki Levha Yayınları, 4. Baskı, İstanbul, Mayıs 2020.

KÜZECİ Elif, "İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı", İnsan Hakları Yıllığı, Cilt 32, 2014, ss. 53-75.

KÜZECİ Elif, Avrupa Konseyi'nin 108 sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter kararı ve Diğer Bazı Gelişmelere İlişkin Bir Değerlendirme.

KÜZECİ Elif/**KILIÇ** Şebnem, "6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler", Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi (2019) 16 (63), s. 12.

LAÇİN İrem, Unutulma Hakkı, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Doç. Dr. Melike Batur Yamaner'in Anısına Armağan, C: 1, Y: 2014, ss. 391-418.

LAMBERT Paul, Understanding the New European Data Protection Rules, Taylor & Francis, 2017.

LANG Peter, Data Rights Law 1.0, The Theoretical Basis, Key Laboratory of Big Data Strategy, Edited by Lian Yuming, "Chapter 1-The Significance of Data Rights to Mankind's Common Life", 2019.

LITMAN Jessica, "Information Privacy/Information Property." Stanford Law Review, Vol. 52, No. 5, May 2000, p. 1283-1314.

MACENAITE Milda/**KOSTA** Eleni, "Consent for Processing Children's Persona Data in the EU: Flowing in the US Footsteps?", Information and Communication Technology Law, Cilt.26, Sayı.2, 2017, ss. 146-147.

MANAV Eda A., "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XIX, Y. 2015, Sa. 2.

MAYER-SCHÖNBERGER, Viktor, Delete: The Virtue of Forgetting in the Digital Age, Princeton 2009.

MEMİŞ Tekin, "Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni", Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 6, 2017, s. 9-23.

METİN Yüksel, "Avrupa Birliği Temel Haklar Şartı", Süleyman Demirel Üniversitesi Iktisadi ve Idari Bilimler Fakültesi, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, Cilt: 57, Sayı: 4, 2002, ss. 35 – 63.

NALBANTOĞLU Seray, "Bir Temel Hak Olarak Unutulma hakkı (Right to be Forgotten As a Fundamental Right)", TAAD, Yıl:9, Sayı:35 (Temmuz 2018), ss.583-605.

OĞUZMAN Kemal/**SELİÇİ** Özer/**ÖZDEMİR OKTAY** Saibe, Kişiler Hukuku, (Gerçek ve Tüzel Kişiler), 20. Bası, Filiz Kitabevi, İstanbul, 2021.

OĞUZMAN Kemal/**SELİÇİ** Özer/**ÖZDEMİR OKTAY** Saibe, Eşya Hukuku, Filiz Kitabevi, 23. Bası, İstanbul, 2021.

OĞUZMAN Kemal/**BARLAS** Nami, Medeni Hukuk (Giriş, Kaynaklar, Temel Kavramlar), Onikilevha Yayınları, 28 Bası, İstanbul, 2022.

ÖNCÜ Gülay Arslan, "Özel Yaşama ve Aile Yaşamına Saygı Hakkı", Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi – 8, Anayasa Mahkemesine Bireysel Başvuru Sisteminin Desteklenmesi Ortak Projesi, Avrupa Konseyi, 2019.

ÖRNEK BÜKEN Nüket/**ZEYBEK ÜNSAL** Çağrı, "Kişisel Verilerin Korunması Kanununun Biyomedikal Alana Yansımaları Açısından Değerlendirilmesi", Hacettepe Hukuk Fakültesi Dergisi, C. 7, S. 2, 2017.

ÖZDEMİR Hayrunnisa, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara, Seçkin Yayınları, 2009.

ÖZLÜK Betül, "Mülkiyet ve Zilyetlik Üzerine Düşünceler", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 27, S. 1, 2019, s.139-166.

ÖZTAN Bilge, Medeni Hukukun Temel Kavramları, Yetkin Yayınları, 45. Baskı, Ankara, 2020.

ÖZTÜRK Bahri/**ALTINOK ÇALIŞKAN** Elif, "Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu", Fasikül Hukuk Dergisi, S.100, Mart 2018, ss.277-336.

PEKMEZ Cüneyt, "Overview of the Definitons of Data Controller and Data Processor within the Scope of The Turkish Code of Personal Data Protection (TCDP)", Annales de la Faculté de Droit d'Istanbul, Sayı 67, 2019, ss.59-71.

PRINS Corien, "When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter." SCRIPTed: A Journal of Law, Technology and Society, Vol. 3, No. 4, December 2006, ss. 270-303.

POLATER Salih, "Kişisel verilerin reklam amaçlı işlenmesinde hukuka uygunluk sebepleri", Kişisel Verileri Koruma Dergisi. 1(1), 1-20.

PORMEISTER Kart, and **DROZDZOWSKI** Lukasz, "Protecting the Genetic Data of Unborn Children: A Critical Analysis." European Data Protection Law Review (EDPL), Vol. 4, No. 1, 2018, p. 53-64.

PRINS J.E.J., "The Propertization Of Personal Data And Identities", Electronic Journal of Comparative Law, vol. 8.3, October, 2004.

ROAGNA Ivana, Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması Avrupa Konseyi insan hakları el kitapları, Türkçeye Çeviren: Ayşe Gül Alkış Schäling, Avrupa Konseyi, Strazburg, 2012.

RODWAY Suzanne/**CAREY** Peter, "Outsourcing Personel Data Processing", Data Protectıon: A Practical Guide to UK and EU Law, Ed: Peter CAREY, 5. Baskı, Oxford University Press, 2018, Oxford.

ROST Martin/**BOCK** Kirsten, "Privacy by Design and the New Protection Goals," İngilizce çevirisinden yararlanılmıştır, "Privacy by Design und die Neuen Schutzziele", Datenschutz und Datensicherheit, Cilt 35, Sayı 1, 2011.

SAKA Rıza/**ÇAĞLAYAN** Ramazan/**KOCA** Mahmut, Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası, Seçkin Yayıncılık, Güncellenmiş ve Genişletilmiş 2. Baskı, Ankara, 2022.

SAMUELSON Pamela, "Privacy as Intellectual Property." Stanford Law Review, vol. 52, no. 5, May 2000, p. 1125-1174.

SCHWARTZ Paul, The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, Amerian Journal of Comparative Law, Cilt: 37, 1989, ss. 675-702.

SEROZAN Rona, Medeni Hukuk, Genel Bölüm/Kişiler Hukuku, Vedat Kitapçılık, İstanbul, 2015.

SERTSÜTÇÜ Selin, Çocukların Kişisel Verilerinin Korunması, Editörler: **ÖZCAN** Hüseyin/ **BAŞAR** Mehmet/ **ORMANOĞLU** H. Derya/ **KAYIŞ** Ferhat, Kişisel Verilerin Korunması Alanında Yeni Gelişmeler Sempozyumu, Adalet Yayınevi, 5 Aralık 2019.

SHERRY Kristina, "What Happens to Our Facebook Accounts When We Die?: Probate Versus Policy and the Fate of Social-Media Assets Postmortem", Vol. 40: 185, 2012.

SIMIĆ Jelena, "The Protection Of Nasciturus within The Civil Law", w. Union University Law School Review (Pravni zapisi), 9(2), 255-270.

SÖZÜER Eren, Unutulma Hakkı- İnsan Hakları Hukuku Perspektifinden Bir İnceleme, On İki Levha Yayınları, İstanbul, Ekin 2017.

SPOOKY, 16-Year-Old Takes Mother to Court for Posting Photos of Him on Facebook, January 15th, 2018, https://www.odditycentral.com/news/16-year-old-takes-mother-to-court-for-postingphotos-of-him-on-facebook.html (Son Erişim Tarihi: 22.07.2021).

SULUK Cahit, "Fikri Mülkiyet Hakları, Uygulamada Yaşanan Sorunlar ve Çözüm Önerileri", Kazancı Hukuk İşletme ve Maliye Bilimleri Dergisi, C.I, S.7, 2005.

ŞENOCAK Kemal, "Kişisel Veri Kavramının Kapsamı ve Unsurları" Editör: **ŞENOCAK** Kemal, Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuku, Eskişehir Osmangazi Üniversitesi Hukuk Fakültesi Yayınları-5, Yetkin Yayınları, Ankara 2022.

ŞEREFOĞLU HENKOĞLU Halise, "Unutulma Hakkı: Dijitalleşme Sürecinde Bilgiye Erişim Özgürlüğünü Tehdit Eder mi? Bilgi Sistemleri ve Bilişim Yönetimi: Beklentiler ve Yeni Yaklaşımlar", 2017, ss.191-212.

ŞİMŞEK Oğuz**,** Anayasa Hukukunda Kişisel Verilerin Korunması, 2008, Beta yayınları.

TAŞTAN Furkan Güven, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, Oniki Levha, 1. Baskı, İstanbul, Temmuz 2017.

TAŞTAN Furkan Güven, "Bir Modern Sözleşme Tipi Olarak Kişisel Veri İşleme Sözleşmesi ve Kanun'a Uyum Sürecindeki Rolü", Lexpera Blog, 2018, https://blog.lexpera.com.tr/kisisel-veri-isleme-sozlesmesi/ (Son Erişim Tarihi: 06.11.2022).

TEKİNALP Ünal, Fikri Mülkiyet Hukuku, Beta Yayınları, Güncelleştirilmiş ve Gözden Geçirilmiş Üçüncü bası, Eylül, 2014.

TEZCAN Durmuş, "Bilgisayar Karşısında Özel Hayatın Korunması", Anayasa Yargısı Dergisi, C. 8, Ankara, 1991, s. 385-392.

TEZCAN Durmuş, "Bilgisayarın Hukukta Kullanılması ve Özellikle Adli Sicil Sisteminin Mekanik Hale Dönüştürülmesi", Adalet Dergisi, Yıl: 70, 1979, No:1-2, ss.53-79.

TEZCAN Durmuş/**ERDEM** Mustafa Ruhan/**SANCAKTAR** Oğuz, Avrupa İnsan Hakları Sözleşmesi Işığında Türkiye'nin İnsan Hakları Sorunu, Gözden Geçirilmiş 2. Baskı, Seçkin Yayınları, 2004.

TORTOP Nuri, "Çağımızın Önemli Sorunu: Kişisel Bilgilerin Güvenliği Sorunu", Amme İdaresi Dergisi, Cilt: 33, Sayı: 3, 2000, ss. 1-14.

UÇAK Murat, "Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası", Kişisel Verileri Koruma Dergisi. 3(1), 2020, ss.41-60.

UÇAK Murat, "Kişisel Verilerin Ölümden Sonra Korunması," İMHFD, C. VI, S. 10, 2021, ss. 97-123.

UNCULAR Selen, İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Ankara, Seçkin Yayıncılık, 2014.

ÜZELTÜRK TAHMAZOĞLU Sultan, "Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği", Legal Hukuk Dergisi, Sayı 93, Eylül 2010.

von dem **BUSSCHE**, Axel Freiherr/**VOIGT** Paul, The EU General Data Protection Regulation (GDPR), A Practical Guide, Springer, 2017.

WALDEN I.N., **SAVAGE** R.N; "Data Protection and Privacy law: Should Organizations Be Protected?", International and Comparative Law Quaterly, 1988, Cilt 37, Sayı :2, s. 337-347.

WARREN Samuel D. & **BRANDEIS** Louis D., "The Right to Privacy", Vol. 4, No:5, Harvard Law Review, 15 Aralık 1890, 193-220.

WEBER Rolf H., ''The Right To Be Forgotten: More Than a Pandora's Box'', Journal of Intellectual Property, Information Technology and Electronic Commerce Law, C.2, S.2, 2011.

WERRO Franz, "The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash", George Town University, The Center of Transnational Legal Studies, Colloquim Research Paper No. 2, May 2009.

WES Matt, "Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization", 25 Nisan 2017, https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/ (Son Erişim Tarihi:06.07.2021).

WILLIAMSON Clyde, "They're Not Just Long Words: Anonymization and Pseudonymization Protect Data-driven Business", March 29, 2021, https://www.protegrity.com/protegrity-blog/theyre-not-just-long-words-anonymization-and-pseudonymization-protect-data-driven-business (Son Erişim Tarihi: 06.07.2021).

WITZLEB Normann &**WAGNER** Julian, "When is Personal Data "About" or "Relating to" an Individual?" A Comparison of Australian, Canadian, and EU Data Protection and Privacy Laws", Canadian Journal of Comparative and Contemporary Law 4, 2018, 293-330.

WOLTERS P.T.J., "The Control by and Rights of the Data Subject Under the GDPR", Journal of Internet Law, Cilt 22, Sayı 1, 2018, ss. 7-18.

YAVUZ Can, Unutulma Hakkı, Güncellenmiş ve Genişletilmiş 3. Baskı, Seçkin Yayıncılık, Ankara 2020.

YILMAZ Malik, "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi," Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi, 49 (1), ss.95- 118.

YILMAZ Ozan Barış, Türkiye ve Avrupa Birliği'nde Kişisel Verilerin Korunması ve Uygulanacak Hukuk, Adalet Yayınevi, Ankara 2022.

YILMAZ Sabire Sinem, "KVKK Uyum Sorunsalı: "Veri Sorumlusu ve Veri İşleyen Kavramlarını İyi Anlamak", 14/05/2020, Lexpera Blog, https://blog.lexpera.com.tr/kvkk-uyum-sorunsali-veri-sorumlusu-ve-veri-isleyen-kavramlarini-iyi-anlamak/ (Son Erişim Tarihi: 02.11.2022)

YILMAZ Süleyman/**ÇAVUŞOĞLU** Gökçe Filiz, Kişisel Verileri Koruma Hukuku, Yetkin Yayınları, Ankara, 2020.

YÜCEDAĞ Nafiye, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 75 (2), 2017, ss.765-789.

YÜCEDAĞ Nafiye, "Kişisel verilerin korunması kanunu kapsamında genel ilkeler", Kişisel Verileri Koruma Dergisi, 2019, 1(1), ss.47-63.

YÜKSEL Mehmet, "Fikri Mülkiyete İlişkin Felsefi Tartışmalar", Türkiye Barolar Birliği Dergisi, 2001/1, ss.177-198.

YÜKSEL CİVELEK Dilek, Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Uzmanlık Tezi), Bilgi Toplumu Dairesi Başkanlığı, T.C Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı, Ankara, Nisan 2011.

ONLİNE KAYNAKLAR

Antlaşma, Görüş, Rehber ve Raporlar

European Court of Human Rights, "Thematic Report: Healthrelated issues in the case-law of the European Court of Human Rights", June 2015, https://www.echr.coe.int/Documents/Research_report_health.pdf (Son Erişim Tarihi:13.04.2021).

Antalya Bölge Adliye Mahkemesi 6. Hukuk Dairesi, 13.11.2020 Tarih, 2020/1149 Esas ve 2020/905 sayılı Kararı, https://okyayevren.com/wp-content/uploads/Antalya-BAM-6.-HD.-E.-20201149-K.-2020905-T.-13.11.2020.pdf (Son Erişim Tarihi:12.04.2021).

Avrupa Birliği Antlaşması ve Avrupa Birliği'nin İşleyişi Hakkında Antlaşma, https://www.ab.gov.tr/files/pub/antlasmalar.pdf (Son Erişim Tarihi: 10.05.2021).

Avrupa Birliği Genel Veri Koruma Tüzüğü- Regulation (Eu) 2016/679 Of The European Parliament And Of The Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj (Son Erişim Tarihi: 07.10.2021).

Avrupa Birliği Temel Haklar Şartı-Council of the EU, Charter of Fundamental Rights of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (Son Erişim Tarihi: 10.05.2021).

Avrupa İnsan Hakları Sözleşmesi- European Convention on Human Rights, https://treaties.un.org/doc/Publication/UNTS/Volume%20213/volume213-I-2889-English.pdf Sözleşmenin Türkçe metni için bkz. Avrupa İnsan Hakları Sözleşmesi https://www.echr.coe.int/Documents/Convention_TUR.pdf (Son Erişim Tarihi: 03.05.2021).

Avrupa Veri Koruma Kurulu (EDPB), Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Veri Sorumlusu ve Veri İşleyen Rehberi), Version 1.0 Adopted on 02 September 2020 https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (Son Erişim Tarihi: 18.05.2021).

Avrupa Veri Koruma Kurulu (EDPB), Guidelines 05/2020 on consent under Regulation 2016/679 (Rıza Rehberi), Version 1.1, Adopted on 4 May 2020, kn.

93.https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (Son Erişim Tarihi: 12.10.2021).

Avrupa Veri Koruma Kurulu (EDPB), Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)- Version for public consultation (GVKT'nin Bölgesel Kapsamı), Adopted on 16 November 2018, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf (Son Erişim Tarihi: 13.05.2021).

Avrupa İnsan Hakları Mahkemesi, Klass, Almanya'ya karşı kararı, Başvuru Numarası: 5029/71 Karar Tarihi: 6 Eylül 1978, http://hudoc.echr.coe.int/eng?i=001-57510 (Son Erişim Tarihi: 04.05.2021).

Avrupa İnsan Hakları Mahkemesi, Vo v France Kararı, Başvuru Numarası: 53924/00 8 Temmuz 2004, 80. Başlık, s.26. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-4246%22]} (Son Erişim Tarihi: 11.10.2021).

Avrupa İnsan Hakları Mahkemesi, Rotaru -Romanya Kararı, Başvuru Numarası: 28341/95, 4 Mayıs 2000, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]} (Son Erişim Tarihi: 02.05.2021).

Avrupa İnsan Hakları Mahkemesi, Leander-İsveç Kararı, Başvuru Numarası: 9248/81 Karar Tarihi: 26 Mart 1987. http://hudoc.echr.coe.int/eng?i=001-57519 (Son Erişim Tarihi: 04.05.2021).

AYM, E. 2013/84, K. 2014/183, T. 04.12.2014, R.G. Tarih-Sayı: 13.03.2015-29294 https://www.resmigazete.gov.tr/eskiler/2015/03/20150313-12.pdf. (Son Erişim Tarihi: 04.04.2020).

AYM, Başvuru No.: 2013/5653 Karar Tarihi: 3.3.2016 R.G. Tarihi: 24.8.2016 R.G. No.: 29811 https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/5653 (Son Erişim Tarihi: 12.10.2021).

Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Yönlendirici İlkeler-Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990, https://www.refworld.org/pdfid/3ddcafaac.pdf (Son Erişim Tarihi: 04.05.2021).

Bodil Lindqvist Kararı, https://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en (Son Erişim Tarihi: 09.05.2021).

Jehovan Todistajat Kararı, https://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130da1c73d7feec4e4cf98a3aa5c0dfc6cca3.e34KaxiLc3eQc40LaxqMbN4Pb3qKe0?text=&docid=203822&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=599058 (Son Erişim Tarihi:24.06.2021).

Google/İspanya Kararı, 13 Mayıs 2014. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (Son Erişim Tarihi: 12.10.2021).

Marper/Birleşik Krallık Kararı, (Başvuru numarası: 30562/04 ve 30566/04), STRASBOURG, 4 December 2008, https://rm.coe.int/168067d216 (Son Erişim Tarihi: 10.10.2021).

Council Of Europe Committee Of Ministers Recommendation No. R (97) 5 Of The Committee Of Ministers To Member States On The Protection Of Medical Data (Avrupa Konseyi Bakanlar Komitesinin Tıbbi Verilerin Korunmasına R (97) 5 Sayılı Tavsiye Kararı) (Adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies), https://rm.coe.int/16806af967 (Son Erişim Tarihi: 13.04.2021).

European Commission (Avrupa Komisyonu), "Towards a Safer Use of Internet for Children in the European Union – A Parents' Perspective", Analytical Report, Flash Eurobarometer Series248, The Gallup Organization, 2008, https://op.europa.eu/en/publication-detail/-/publication/4c7ece29-058c-44fe-9aa0-27d67cfc3029/language-en (Son Erişim Tarihi: 24.07.2021).

European Commission (Avrupa Komisyonu), Can personal data about children be collected? https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en (Son Erişim Tarihi: 21.07.2021).

Elektronik Haberleşme Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkındaki Avrupa Birliği Direktifi- Directive 2002/58/EC concerning processing of personal data and the protection of privacy in the electronic communications sector), e-Privacy Directive, https://eur-lex.europa.eu/legal content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN (Son Erişim Tarihi: 04.04.2021).

Glossary of Statistical Terms, Automated Data Processıng (Adp) https://stats.oecd.org/glossary/detail.asp?ID=4370 (Son Erişim Tarihi: 24.06.2021).

Golden Data Law, "What is a 'filing system' under EU data protection law?", Nov 29, 2018, https://medium.com/golden-data/what-is-a-filing-system-under-eu-data-protection-law-6e7222743f71 (Son Erişim Tarihi: 24.06.2021).

ICO, Anonymisation: managing data protection risk code of practice, About this code, https://ico.org.uk/media/1061/anonymisation-code.pdf (Son Erişim Tarihi: 08.10.2021).

ICO, What is transparency?, https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf (Son Erişim Tarihi:25.07.2021).

ICO, Guide to the General Data Protection Regulation (GDPR), Data Protection By Design And Default, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (Son Erişim Tarihi:12.10.2021).

ICO, Feedback request – profiling and automated decision-making, https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf (Son Erişim Tarihi:07.08.2021).

ICO, "Guide to the General Data Protection Regulation (GDPR)", 1 Ocak 2021, https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf (Son Erişim Tarihi: 08.10.2021).

Kamu Sektöründe Elektronik Veri Bankaları Karşısında Bireylerin Özel Hayatlarının Korunmasına İlişkin Karar- Council Of Europe, Committee Of Ministers, Resolution (74) 29 On The Protection Of The Privacy Of Individuals Vis-A-Vis Electronıc Data Banks In The Public Sector (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies), https://rm.coe.int/16804d1c51 (Son Erişim Tarihi: 03.05.2021).

Klinik çalışmaların araştırılması ve yürütülmesine ilişkin Direktif- Directive 2001/20/EC Of The European Parliament And Of The Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use, (OJ L 121, 1.5.2001, p. 34), https://ec.europa.eu/health/sites/health/files/files/eudralex/vol1/dir_2001_20/dir_2001_20_en.pdf (Son Erişim Tarihi: 06.04.2021).

Kişisel Verilerin Korunması El Kitabı-Handbook on European Data Protection Law, 2018, https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf (Son Erişim Tarihi: 17.04.2021).

Kişisel Verileri Koruma Kurulu'nun 02 Nisan 2018 tarih ve 2018/32 sayılı Kararı, https://www.resmigazete.gov.tr/eskiler/2018/05/20180515-16.pdf (Son Erişim Tarihi: 01.07.2021).

Kişisel Verileri Koruma Kurulu'nun 31 Ocak 2018 Tarihli ve 2018/10 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/4110/2018-10 (Son Erişim Tarihi: 13.08.2021).

Kişisel Verileri Koruma Kurulu'nun 08 Aralık 2020 tarihli ve 2020/927 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6871/2020-927 (Son Erişim Tarihi: 25.09.2021).

Kişisel Verileri Koruma Kurulu'nun 23 Haziran 2020 Tarihli ve 2020/481 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6776/2020-481 (Son Erişim Tarihi: 25.09.2021).

Kişisel Verileri Koruma Kurulu'nun 11 Ağustos 2020 tarihli ve 2020/622 sayılı Kararı Özeti, https://www.kvkk.gov.tr/Icerik/6816/2020-622 (Son Erişim Tarihi: 22.07.2021)

Kişisel Verileri Koruma Kurulu'nun 31 Mayıs 2019 Tarihli ve 2019/159 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/5494/2019-159 (Son Erişim Tarihi: 12.10.2021).

Kişisel Verileri Koruma Kurulu'nun 25 Mart 2019 Tarihli ve 2019/81 Sayılı Karar ve 31 Mayıs 2019 Tarihli ve 2019/165 sayılı Karar Özeti https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 (Son Erişim Tarihi: 12.10.2021).

Kişisel Verileri Koruma Kurulu'nun 24 Ocak 2019 Tarih ve 2019/10 Sayılı Kararı, https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (Son Erişim Tarihi:02.08.2021).

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Sözleşmenin Onaylanmasının Uygun Bulunduğuna Dair Kanun, https://www.resmigazete.gov.tr/eskiler/2016/02/20160218-2.pdf (Son Erişim Tarihi: 03.05.2021).

Kişisel Verileri Koruma Kurumu, 9 Nisan 2020 Tarihli Kamuoyu Duyurusu, 26 Ekim 2020, https://www.kvkk.gov.tr/Icerik/6726/COVID-19-ILE-MUCADELEDE-KONUM-VERISININ-ISLENMESI-VE-KISILERIN-HAREKETLILIKLERININ-IZLENMESI-HAKKINDA-BILINMESI-GEREKENLER-2- (Son Erişim Tarihi:23.07.2021).

Kişisel Verilerin Korunması Kanun'u Tasarısı ve Gerekçe Metni, https://www2.tbmm.gov.tr/d26/1/1-0541.pdf (Son Erişim Tarihi: 14.05.2021).

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa Duyulan İhtiyaç, https://www.kvkk.gov.tr/Icerik/4182/Kisisel-Verilerin-Korunmasi-Kanununa-Duyulan-Ihtiyac (Son Erişim Tarihi:07.10.2021).

Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler (Son Erişim Tarihi: 06.10.2021)

Kişisel Verileri Koruma Kurumu, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı", https://kvkk.gov.tr/yayinlar/ANAYASAL%20B%C4%B0R%20HAK%20OLARAK%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASINI%20%C4%B0STEME%20HAKKI.pdf (Son Erişim Tarihi: 06.10.2021).

Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi (KVKK Uygulama Rehberi)", https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF (Son Erişim Tarihi: 17.04.2021).

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu ve Uygulaması, https://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf (Son Erişim Tarihi: 14.05.2021).

Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar.https://www.kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20Y%C3%96NEL%C4%B0K%20SORU%20VE%20CEVAPLAR.pdf (Son Erişim Tarihi: 13.10.2021).

Kişisel Verileri Koruma Kurumu, "6698 Sayılı Kanun'da Yer Alan Temel Kavramlar", https://kvkk.gov.tr/yayinlar/6698%20SAYILI%20KANUN%E2%80%99DA%20YER%20ALAN%20TEMEL%20KAVRAMLAR.pdf (Son Erişim Tarihi: 03.04.2021).

Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular", https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular (Son Erişim Tarihi: 09.10.2021).

Kişisel Verileri Koruma Kurumu, "100 Soruda Kişisel Verilerin Korunması Kanunu", https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf (Son Erişim Tarihi: 03.04.2021).

Kişisel Verileri Koruma Kurumu, "Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) Ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü (Kısaca KVKK Terimler Sözlüğü), https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu (Son Erişim Tarihi: 06.04.2021).

Kişisel Verileri Koruma Kurumu, Veri Sorumlusu ve Veri İşleyen, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf (Son Erişim Tarihi: 18.05.2021).

Kişisel Verileri Koruma Kurumu, Açık Rıza, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf (Son Erişim Tarihi: 08.07.2021).

Kişisel Verileri Koruma Kurumu, Özel Nitelikli Kişisel Verilerin İşlenme Şartları, s.3. https://www.kvkk.gov.tr/Icerik/5238/Ozel-Nitelikli-Kisisel-Verilerin-Islenme-Sartlari (Son Erişim Tarihi: 11.10.2021).

KVKK Veri Yönetimi Dairesi Başkanlığı, Sorularla Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERB%C4%B0S.pdf (Son Erişim Tarihi: 11.10.2021).

15 Aralık 1983 tarihli Nüfus Sayım Kararı'nın İngilizce Metni https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html (Son Erişim Tarihi:08.05.2021).

108 Sayılı Sözleşme- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, European Treaty Series-No.108, 28 Ocak 1980, https://rm.coe.int/1680078b37 (Son Erişim Tarihi: 03.05.2021).

181 sayılı Ek Protokol- Council Of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, European Treaty Series-No. 181, 8 Kasım 2001, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626 (Son Erişim Tarihi:04.05.2021).

Sözleşme 108+ /Convention 108+, Convention for the protection of individuals with regard to the processing of personal data, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (Son Erişim Tarihi: 04.05.2021).

29. Madde Çalışma Grubu, WP 136, Article 29 Data Protection Working Party, Opinion 4/2007, On The Concept of Personal Data (Kişisel Veri), 20 Haziran 2007, ss.1-26.

29. Madde Çalışma Grubu, WP 105, Working document on data protection issues related to RFID technology, 19 Ocak 2005.

29. Madde Çalışma Grubu, WP 259, "Guidelines on consent under Regulation 2016/679" (Rıza Rehberi), 28 Kasım 2017, Gözden Geçirilmiş Son Hali 10 Nisan 2018, s.5-7.

29. Madde Çalışma Grubu, WP 169, Opinion 1/2010 on the concepts of "controller" and "processor" (Veri Sorumlusu ve Veri İşleyen) , 16 Şubat 2010.

29. Madde Çalışma Grubu, WP 187, "Opinion 15/2011 on the definition of consent", 13 Temmuz 2011.

29. Madde Çalışma Grubu, WP 217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 Nisan 2014.

29. Madde Çalışma Grubu, WP 260, Guidelines on transparency under Regulation 2016/679.

29. Madde Çalışma Grubu, WP 203**,** Opinion 03/2013 on purpose limitation, 2 Nisan 2013**.**

29. Madde Çalışma Grubu, WP 248, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 4 Nisan 2017, Gözden Geçirilmiş son Hali 4 Ekim 2017.

29. Madde Çalışma Grubu, WP 106, "Report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union", 18 Ocak 2005.

29. Madde Çalışma Grubu, WP 243, Guidelines on Data Protection Officers ('DPOs'), 13 Aralık 2016, Gözden Geçirilmiş Son Hali 5 Nisan 2017.

29. Madde Çalışma Grubu, WP 242, Guidelines on the right to data portability, 13 Aralık 2016, Gözden Geçirilmiş Son Hali 5 Nisan 2017.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Son Erişim Tarihi: 03.05.2021).

Özel Sektörde Elektronik Veri Bankaları Karşısında Bireylerin Özel Hayatlarının Korunmasına İlişkin Karar- Council Of Europe, Committee Of Ministers, Resolution (73) 22 On The Protectıon Of The Privacy Of Individuals Vis-A-Vis Electronic Data Banks In The Private Sector (Adopted by the Committee of Ministers on 26 September 1973, at the 224th meeting of the Ministers' Deputies), https://rm.coe.int/1680502830 (Son Erişim Tarihi: 03.05.2021).

TBMM, 117 sayılı Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu ("TBMM Komisyon Raporu" olarak anılacaktır, (Çevrimiçi), https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (Son Erişim Tarihi:20.07.2021).

Türkiye Barolar Birliği, Türkiye Cumhuriyeti Anayasa Önerisi Geliştirilmiş Gerekçeli Yeni Metin, Kasım 2007/ 4. Baskı. http://tbbyayinlari.barobirlik.org.tr/TBBBooks/2007_Anayasa%20Taslagi_TBB.pdf (Son Erişim Tarihi: 07.10.2021).

Türkiye-AB İlişkilerinin Tarihçesi, https://www.ab.gov.tr/turkiye-ab-iliskilerinin-tarihcesi_111.html#:~:text=Bu%20do%C4%9Frultuda%2C%20insanl%C4%B1k%20tarihinin%20en,da%20Toplulu%C4%9Fa%20ortakl%C4%B1k%20ba%C5%9Fvurusunda%20bulunmu%C5%9Ftur. (Son Erişim Tarihi: 14.05.2021)

Türkiye Avrupa Birliği İlişkileri Kronolojisi, https://www.ab.gov.tr/files/5%20Ekim/turkiye_avrupa_birligi_iliskileri_kronolojisi.pdf (Son Erişim Tarihi: 14.05.2021).

Türk Dil Kurumu Güncel Türkçe Sözlük, https://sozluk.gov.tr/ (Son Erişim Tarihi: 03.04.2021).

What Activities Count as Processing Under the GDPR? 18 January 2021 https://www.termsfeed.com/blog/gdpr-processing-activities/ (Son Erişim Tarihi: 09.06.2021).

YHGK, E. 2014/4-56, K. 2015/1679, T. 17.06.2015, https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=hgk-2014-4-56.htm&kw=`2014/4-56,`+K.+`2015/1679,`+&cr=yargitay#fm (Son Erişim Tarihi: 25.09.2021).