KADİR HAS ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
HUKUK ANABİLİM DALI

KİŞİSEL VERİLERİN İŞLENMESİNİN HUKUKİ BOYUTU

HABİP BOZKURT

DANIŞMAN: YRD. DOÇ. DR. İPEK SEVDA SÖĞÜT

YÜKSEK LİSANS TEZİ

İSTANBUL, MAYIS, 2019

KİŞİSEL VERİLERİN İŞLENMESİNİN HUKUKİ BOYUTU

HABİP BOZKURT

DANIŞMAN: YRD. DOÇ. DR. İPEK SEVDA SÖĞÜT

YÜKSEK LİSANS

Hukuk Anabilim Dalı Özel Hukuk Programı'nda Yüksek Lisans derecesi
için gerekli kısmi şartların yerine getirilmesi amacıyla
Kadir Has Üniversitesi Lisansüstü Eğitim Enstitüsü'ne
teslim edilmiştir.

İSTANBUL, MAYIS, 2019

Ben, HABİP BOZKURT;

Hazırladığım bu Yüksek Lisans Tezinin tamamen kendi çalışmam olduğunu ve başka çalışmalardan yaptığım alıntıların kaynaklarını kurallara uygun biçimde tez içerisinde belirttiğimi onaylıyorum.

HABİP BOZKURT

27.05.2019

KABUL VE ONAY

HABİP **BOZKURT** tarafından hazırlanan **KİŞİSEL VERİLERİN İŞLENMESİNİN HUKUKİ BOYUTU** başlıklı bu çalışma **27.05.2019** tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Dr. Öğr. Üy. İpek Sevda Söğüt (Danışman)	Kadir Has Üniversitesi
Doç. Dr. Bahar Ceyda Efeçınar	Kadir Has Üniversitesi
Prof. Dr. Pervin Somer	Okan Üniversitesi

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof. Dr. Sinem AKGÜL AÇIKMEŞE
Lisansüstü Eğitim Enstitüsü Müdürü
27.05.2019

İÇİNDEKİLER

KISALTMALAR LİSTESİ

AB: Avrupa Birliği
ABD: Amerika Birleşik Devletleri
AİHM: Avrupa İnsan Hakları Mahkemesi
AİHS: Avrupa İnsan Hakları Sözleşmesi
ABAD: Avrupa Birliği Adalet Divanı
ABK: Avrupa Birliği Komisyonu
AK: Avrupa Konseyi
APEC: Asya-Pasifik Ekonomik İşbirliği
AT: Avrupa Topluluğu
AYM: Anayasa Mahkemesi
BM: Birleşmiş Milletler
CMK: Ceza Muhakemesi Kanunu
DNA: Deoksiribo Nükleik Asit
EUROPOL: Avrupa Polis Teşkilatı
FVSK: Fikir ve Sanat Eserleri Kanunu
GVKT: Genel Veri Koruma Tüzüğü
IP: İnternet Protokol Adresi
İK: İş Kanunu
İVKK: İspanyol Veri Koruma Ajansı
KVKK: Kişisel Verileri Koruma Kanunu
OECD: Ekonomik Kalkınma ve İşbirliği Örgütü
s. : Sayfa
TBK: Borçlar Kanunu
TCK: Türk Ceza Kanunu
TDK: Türk Dil Kurumu
TMK: Türk Medeni Kanunu
TÜİK: Türkiye İstatistik Kurumu

ÖZET

BOZKURT, HABİP. *KİŞİSEL VERİLERİN İŞLENMESİNİN HUKUKİ BOYUTU*, YÜKSEK LİSANS TEZİ, İstanbul, 2019.

Küreselleşen dünyada, bilgi teknolojilerindeki hızlı gelişmelere paralel olarak bireylerin kişisel verileri, hukuka uygun ya da aykırı şekilde dijital ortama aktarılarak erişime açılmış olup, bu durum veri güvenliği tartışmalarını beraberinde getirmiştir. Özellikle, II. Dünya Savaşı öncesi yükselen totaliter rejimlerin kişisel veri güvenliğinin aleyhindeki girişimlerinin varabileceği noktayı milyonlarca hayatla tecrübe etmiş Avrupa'da ilgili hak, birçok düzenleme ile koruma altına alınmıştır. Kişisel verilerin korunması hakkının Türk Hukuku'nda anayasal güvence altına alınması için 2010 yılında yapılan Anayasa değişikliği beklenmişse de, bu alanda 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) kabulüyle birlikte, ilgili hak ilk kez kanuni bir düzenlemeye sahip olmuştur. Bu bağlamda birçok eksik yönlerine vurgu yapılabilmekle birlikte KVKK ile, Türk Hukuku'nda kişisel verilerin korunması hakkına ilişkin önemli bir düzenleme çerçevesi getirildiği tespit edilmiştir.

Anahtar Sözcükler: Kişisel Veri, Kişisel Verilerin Korunması, Özel Hayatın Gizliliği, 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK).

ABSTRACT

BOZKURT, HABİP. *LEGAL DIMENSION OF PERSONAL DATA PROCESSING*, MASTER'S THESIS, İstanbul, 2019.

In the globalized world, throughout the rapid developments in information technologies, the personal data of individuals has been opened to digital media in accordance with the law or in contradiction and this situation has brought the discussions about data security. Especially, in Europe where have been experienced with millions of lives because of the totalitarian regimes' attemps to the personal data security before World War II, the right has been protected by many regulations. Although, the constitutional amendment was expected until 2010 to ensure the protection of personal data for the constitutional guarantee in Turkish Law, the right for the first time was granted with the adoption of Law No. 6698 on the Protection of Personal Data in this field. In this context, it can be emphasized that many deficiencies can be emphasized and it has been determined that a significant regulatory framework regarding the right to protection of personal data has been introduced in Turkish Law with Law No. 6698.

Keywords: Personal Data, Personal Data Protection, The Right of Privacy, Law No.6698.

GİRİŞ

Tarihin erken dönemlerinden itibaren toplumsal hayatı organize etmek ve idari süreçlerin yürütülmesi amacıyla yönetim organları bireylerin verilerini toplamakta olup, bu verilerin korunmasına yönelik erken dönem hukuki enstrümanlarının geliştirildiği görülmektedir. Ancak, özellikle II. Dünya Savaşı öncesinde dünyadaki totaliter siyasi eğilimler, kişisel verilerin toplum aleyhine sınırsız bir şekilde kullanımını beraberinde getirmiş ve bu durum büyük bir yıkıma neden olmuştur. Modern dönemde, kişisel veri tanımının genişlemesi ve modern bireyi belirli ve belirlenebilir kılan birçok unsurun eklenmesiyle, kişisel verilerin korunmasına yönelik uluslararası ve ulusal düzenlemelerin arttığı görülmektedir. Ancak, özellikle küreselleşmenin büyük bir hız kazandığı ve bilgi teknolojilerinin sınırları kaldırdığı günümüzde hem dolaşıma giren veri sayısı büyük bir hacme erişmiş hem de verilere karşı yeni risk ve tehdit formları gündeme gelmiştir. Daha önceden sınırlı sayıda kişi ya da kurum tarafından fiziksel ortamda depolanan kişisel veriler, bilgi teknolojilerindeki gelişmeler doğrultusunda hukuka uygun ya da aykırı şekilde dijital ortama aktarılarak erişime açılmışsa da, bu verilerin güvenliğini arttıran değil, riskleri çoğaltan birçok durumu beraberinde getirmiştir.

Günümüzde de devletlerin vatandaşlarının kişisel alanlarına müdahalesi çeşitli düzeylerde sürmekle birlikte, siber oluşumların bizatihi devletlerin tekelindeki verilere yönelik girişimleri ile ulusal ya da uluslararası ticari işletmelerin pazarlama amacıyla bu verilere erişme talebi birçok hukuki soruna neden olmaktadır. OECD, Birleşmiş Milletler ve Avrupa Birliği gibi uluslararası oluşumların yanı sıra, devletlerin de çoğunlukla bu kurumların oluşturduğu mevzuattan bazen ilham alarak bazense direkt ulusal hukuka aktarım yöntemiyle faydalandığı bir düzenleme iklimi söz konusuysa da, yeni sorunlar oluşmaktadır.

Kişisel verilerin korunması alanında uluslararası ortamdaki gelişmelere karşın uzun yıllar Türk hukukunda anayasal bir güvence altına alınmayan Türk Hukukunda 2010 yılında gerçekleştirilen referandumun beklendiği görülmüştür. Bu bağlamda, kişisel verilerin korunması hakkı, Anayasa'nın 20'inci maddesine eklenen bir fıkrayla Anayasal bir güvence altına alınmış; 24.3.2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) kabulüyle birlikte, bu hak özel bir kanuni düzenlemeye sahip olmuştur.

Bu doğrultuda çalışmanın amacı; doktrindeki tartışmalar, uluslararası ve ulusal düzenlemeler ile mahkeme kararları ışığında ve KVKK bağlamında kişisel verilerin korunmasının hukuki boyutunun ele alınmasıdır. Çalışmada; kişisel verilerin işlenmesi ve korunması hakkı, ceza hukuku boyutu ile alınmamıştır.

Çalışma üç bölümden oluşmaktadır. Birinci bölümde kişisel veri tanımı, kapsamı ve unsurları incelenirken; kişisel verilerin korunmasıyla ilgili temel kavramlar, doktrindeki tartışmalar ve gerek uluslararası gerekse ulusal düzeydeki yargı kararları ışığında ele alınmıştır. Çalışmanın ikinci bölümünde, kişisel verilerin korunması hakkının medeni hukuk, idare hukuku ve ceza hukuku bağlamında görüşlerle sağlanan hukuki niteliği ile uluslararası (OECD, BM, AB vb.) ve ulusal düzenlemelerdeki (T.C. Anayasası, Türk Ceza Kanunu, KVKK vb.) hukuki dayanakları belirtilmiştir. Çalışmanın son bölümü ise Türk hukukunda kişisel verilerin korunması hakkını koruyan ilk özel kanuni düzenleme niteliğindeki KVKK kapsamında kişisel verilerin işlenmesinin şartlarına odaklanmış olup; kişisel verilerin korunmasına ilişkin temel ilkeler, kişisel verilerin işlenmesinin hukuka uygunluğu, KVKK'da yer alan veri sorumlusunun yükümlülükleri ve ilgili kişinin hakları, öngörülen denetim mekanizması ve hukuka aykırı olarak kişisel veri işlemenin hukuki sonuçları incelenmiş, doktrindeki tartışmalar, uluslararası düzenlemeler ve güncel yargı kararları ışığında KVKK'nın içerdiği eksiklikler ve geliştirilmeye açık yönler tartışılmıştır.

Çalışmanın oluşturulmasında; doktrindeki tartışmalar bağlamında ulaşılabilen tüm ulusal ve uluslararası literatür (kitap, dergi ve online makaleler), güncel düzenleme ve uygulamaların taranması metodu kullanılmıştır.

BİRİNCİ BÖLÜM: KİŞİSEL VERİ TANIMI VE KAPSAMI

1.1. Kişisel Verinin Tanımı

Küreselleşen dünyada teknolojik gelişmelerin dinamizmiyle paralel olarak kişisel veri tanımı ve kapsamı hızla değişmekte olup, beraberinde önemli bir hukuki sorun alanı oluşturduğu görülmektedir.

Türk Dil Kurumu'na (TDK) göre veri kelimesine ilişkin altı tanım yer almakta olup en uygunu, "*olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi*" olarak tanımlanmakta iken, kişisel kelimesi ise "*kişiye ilişkin, kişinin kendi malı olan, şahsi ve zati*" şeklinde tanımlanmaktadır[1].

En genel anlamda kişisel veri; *"belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi"* olup, *"bir kişiyi belirlemeye yarayan akla gelebilecek her türlü bilgi, o kişinin kişisel verisidir"*[2]. Bir başka tanıma göre ise kişisel veri "*kişinin şahsi, ailevi, mesleğine ilişkin ayırt edici özelliklerini ve niteliklerini göstermeye yarayan her türlü bilgidir"*[3]. Bir diğer tanıma göre ise kişisel veri; "*bir kişinin belirlenebilir kılınması, verilerin doğrudan ya da dolaylı olarak bir gerçek kişiyle ilişkilendirilmesi suretiyle kişinin tanımlanabilmesi, yani şahsın o şahıs olduğunu ortaya çıkarılabilmesi özelliğidir"*[4].

Ayrıca, kişisel veri kavramı birçok ulusal ve uluslararası metinde benzer şekilde tanımlanmaktadır. Örneğin; 1995/46/AT sayılı Veri Koruma Direktifi'ne göre (Direktif)[5]; "*fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan*

[1] Türk Dil Kurumu, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c9894bf10f272.34340734, Erişim Tarihi (25.03.2019).
[2] Dülger, M. Volkan: Kişisel Verilerin Korunması Hukuku (Kişisel Verilerin Korunması), Hukuk Akademisi Yayınları, İstanbul 2019, s.1.
[3] Şen, Ersan: "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", İstanbul Barosu Dergisi, 83 (3), İstanbul 2009, s.1197.
[4] Başalp, Nilgün: Kişisel Verilerin Korunması ve Saklanması (Kişisel Verilerin Korunması), Yetkin Yayınları, Ankara 2004, s.16.
[5] Bundan sonra "Direktif" diye kullanılacaktır.

veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye (veri öznesi) ilişkin herhangi bir bilgiyi kast edecektir" cümlesi ile bu tanım yapılmaktadır[6]. Birçok ülkenin kendi iç hukuklarına aktardıkları bu tanım içerik itibari ile oldukça geniş olup, farklı yorumları beraberinde getirmektedir[7].

1980 tarihli "OECD Kişisel Verilerin Sınıraşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri'nin" "Genel Tanımlar" başlıklı 1. maddesinin (b) bendinde yapılan tanıma göre ise kişisel veri; *tanımlanmış/belirlenmiş veya tanımlanabilir/belirlenebilir olan bireyle ilişkili her türlü bilgidir*". Dolayısıyla, kişisel veri tanımına uygun şartların oluşması için; bir veri, bu verinin bir kişiye ilişkin olması ve kişiyi belirli ya da belirlenebilir kılma özelliğini haiz olması gerekmektedir[8].

Türkiye'de ise kişisel veri tanımı ilk olarak telekomünikasyon sektörüne ilişkin Veri Koruma Yönetmeliği'nin 3'üncü maddesinde yapılmış olup, şu şekildedir; "*Tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgi"*[9]. Diğer yandan, KVKK'da ise kişisel veri; "*kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmış olup, tüzel kişiler kapsama alınmamaktadır[10].

Kişisel verilerin hayati öneme sahip olduğu sağlık verileri alanında ise Sağlık Bakanlığı tarafından hazırlanarak yürürlüğe giren "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin" 4.maddesinin 1. fıkrasının (g)

[6] "Directive 95/46/EC", Official Journal L 281, 23.11.1995, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, (Erişim Tarihi): 01.0.2019.
[7] Ayözger, A. Çiğdem: Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması (Yayımlanmamış Doktora Tezi), İstanbul 2016, s.14.
[8] Dülger, Kişisel Verilerin Korunması, s.10.
[9] Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, R.G. 25365, 16.02.2004.
[10] 6698 sayılı Kişisel Verilerin Korunması Kanunu, R.G. 29677, 07.07.2016.

bendinde kişisel sağlık verisi, "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü sağlık bilgisi*" olarak ele alınmıştır[11].

Tüm bu tanımlardan çıkarımla kişisel veri kavramını, kimliği belirli veya belirlenebilir gerçek kişiye ait fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel verilerin tamamı olarak tanımlamaktayız.

Kişisel veri kavramı ile birlikte tartışılması gereken bir başka kavram ise "hassas veridir". Bazı kaynaklarda "duyarlı veri" bazılarında ise "özel nitelikli kişisel veri" olarak kullanılan bu veriler kamusallaştıkları takdirde bireylerin toplumdaki yerini ve diğer insanların kişiye bakış açısını değiştirme özelliğine sahiptir. Dolayısıyla, içeriğinde inanç, politik düşünce, cinsel tercih, etnik köken, kılık kıyafet gibi unsurları bulunduran bu verilerin açıklanması kişinin "ötekileştirilmesi" sonucunu doğurabileceği için "hassasiyet" taşımaktadır. Kişisel verilerin daha fazla koruma sağlandığı küçük bir grup olarak nitelenen bu veriler, iç hukukta uygun güvence sağlanmadığı sürece otomatik işleme tabi tutulamazlar[12]. Bu bağlamda, hassas verilerin kapsamı genişletilemeyeceği ve sadece KVKK'nın 6'ıncı maddesinde yer alan istisnai hallerde işlenebileceği için, bu veriler bakımından "kesin işlem yasağı" söz konusudur[13]. Bu bağlamda, Türk Ceza Kanunu'nun 135'inci maddesinde düzenlenen kişisel verilerin kaydedilmesi suçu şayet hassas kişisel verilerin kaydedilmesi suretiyle işlenmekteyse, verilecek ceza yarı oranında arttırılmaktadır[14].

Ulusal ve uluslararası hukuki metinlerde kişisel veriler ile hassas veriler arasına ayrım koyulduğu görülmektedir. Örneğin; hem Direktif'te hem de 108 sayılı Sözleşme'de ırk, politik düşünce, dini inanç, sağlık ve cinsel hayat hassas veri kategorisinde kabul edilirken, etnik unsur, felsefi düşünce, sendika ve ticari birlik üyeliği Direktif'te; diğer

[11] Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, R.G. 29863, 20.10.2016.
[12] Henkoğlu, Türkay: Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi (Yayımlanmamış Doktora Tezi), Ankara 2015, s.18.
[13] Yücedağ, Nafiye: "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 2, İstanbul 2017, s.768.
[14] Sert, Şeyma: Kişisel Verilerin 5237 Sayılı Türk Ceza Kanunu Kapsamında Korunması (Yayımlanmamış Yüksek Lisans Tezi), Erzurum 2018, s.22.

inançlar ise 108 sayılı Sözleşme'de hassas veri türleri olarak kabul edilmiştir[15]. Türk hukukunda ise hassas veri yerine özel kişisel veri tabiri kullanılmış ve bu kapsamda; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleri ile biyometrik ve genetik veriler sayılmıştır[16].

Biz ise bu noktada, KÜZECİ'nin "hassas veri ve diğer veriler ayrımının kişisel verilerin etkin korumasının sağlanması amacından uzaklaşmadan tartışılması"[17] görüşüne katılmaktayız. Dolayısıyla; etnisite, din, felsefi görüş, ideoloji vb. tüm bu unsurları hassas kişisel veri kategorisinde kabul ederek; bunun maddi yansıması kapsamına ise tahlil sonucu, kişinin geçirdiği hastalıklar, kullandığı ilaçlar, sabıka kaydı, askerlik muafiyet raporu, sendika ve parti üyeliği gibi örnekleri almaktayız.

1.2. Kişisel Verinin Kapsamı ve Unsurları

Kişisel verilerin sınırları ve kapsamlı tartışmalı bir konu olup, bugün de tam olarak çizilememektedir[18]. Bu bağlamda, bir görüşe göre kişisel veri kapsamına; doğrudan veya dolaylı olarak bir kişi ile ilişkilendirilerek, kişinin kimliğini belirli kılan veya kılabilecek olan kimlik, etnik köken, fiziksel özellikler, sağlık, istihdam, eğitim, ikamet, emniyet, kredi kartı bilgileri, başkaları ile gerçekleştirilen haberleşmeler, kişisel inanç ve ideoloji, alışveriş alışkanlıkları da girmektedir[19].

Kişisel veri kapsamına; telefon rehberi, maaş bordrosu, vergi mükellefiyetine ilişkin bilgiler, fotoğraflar, kamera kaydı, ses veya görüntüsü, yüz, iris, gen izi, yazı, ses tanıma gibi yöntemlerle elde edilen verileri, bilgisayarların internet protokol adresleri (IP), parmak izleri, telefon mesajları ile önceki gün yediği yemek[20]; vakıf, dernek,

[15] Akgül, Aydın: Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi (Kişisel Verilerin Korunması), (Yayımlanmamış Doktora Tezi), Kocaeli 2013, s.16.
[16] Sefer, Oğuz: "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri", Bilgi ve Ekonomi Yönetimi Dergisi, 13 (2), Ankara 2018, s.127.
[17] Küzeci, Elif: Kişisel Verilerin Korunması, Turhan Kitabevi, Ankara 2018, s.237.
[18] Dülger, M. Volkan: "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması (Ceza Normu)", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 3(2), İstanbul 2016, s.102.
[19] Aksoy, H. Can: Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara 2010, s.1.
[20] Küzeci, s.9.

sendika üyelikleri, adli sicil kayıtları, ekonomik bilgileri, sosyal medya hesapları, kişisel blog sayfasında paylaştığı yazılar dahilken[21]; kişi hakkındaki önemsiz sayılan veriler ve açık kaynaklarda yayımlanmış veriler de aslında birer kişisel veri niteliğindedir ve daha az öneme sahip değildir[22]. Diğer yandan, kişisel veri alfabetik, sayısal, grafik, fotografik ya da akustik biçimlerde olabilmektedir.

DÜLGER'e göre insanın insan olarak evrendeki yerini alması ve toplumsal konumu, ona bağlı bazı değerleri kişisel veriye dönüştürmektedir. Kişinin adı, adresi, medeni durumu, hastalıkları, cinsel tercihleri kişisel verileri olarak öne çıkarken, 20. yüzyılın son çeyreğinden itibaren hızla artan teknolojik gelişmeler birçok bilgiyi daha kişisel veriye dönüştürmüştür. Bunlar; banka hesap numarası, sosyal güvenlik numarası, vatandaşlık numarası, elektronik posta adresi şifreleri ve sosyal medya hesaplarının şifreleri olarak sıralanabilmektedir[23].

Özellikle ikinci kategoride yaşanan gelişmeler baş döndürücü bir hıza sahiptir. Sosyal medya aracılığıyla her gün milyarlarca verinin paylaşıldığı günümüzde kişisel veriler ticari meta haline gelmiş olup, bu verilerle işlenen siber suçlar hızla artmakta; izleme, gözetlenme, denetlenme ile ilgili kaygılar tetiklenmekte, bu da kişisel verileri korumaya yönelik mevzuatın yetersiz kaldığı bir düzleme referans vermektedir[24]. Henüz on beş yıl önce kişisel veri olarak tanımlanmayacak birçok veri, bugün kişisel veri olarak kabul edilmekte ve koruma kapsamına alınmaktadır.

Bu nedenle, kişisel veriler iki başlık altında toplanmaktadır. İlk grupta insanın varoluşundan kaynaklanan kişilik bilgileri iken, ikinci grupta ise insanın modern teknoloji ve bilişim toplumunda yer almasından ve çeşitli hizmetlere ulaşmasında kullandığı veriler yer almaktadır. Ancak bu ayrım, iki kategorideki kişisel verilerin değerini ve korunmaya olan ihtiyaçlarını birbirinden farklı kılmamaktadır[25].

---

[21] Akgül, Aydın: Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması (Danıştay ve Avrupa), Beta Basım Yayın, İstanbul 2016, s.8-9.
[22] Bayram, M. Hanifi: Avrupa Birliği ve İnternet Hukuku, Seçkin Yayınevi, Ankara 2011, s.23.
[23] Dülger, Ceza Normu, s.102.
[24] Oğuz, Habip: "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum", Uyuşmazlık Mahkemesi Dergisi, 3, Ankara 2014, s.2-3.
[25] Dülger, Ceza Normu, s.102.

Diğer yandan, bir bilginin öznel ya da nesnel; gerçek veya uydurma; açık veya gizli olması ise, kişisel veri olarak kabul edilmesine yönelik bir engel değildir[26]. Nitekim, veri sahibine kendisiyle ilgili toplanmış olan ancak doğru olmayan kişisel verilerin düzeltilmesi veya silinmesini talep etme hakkı tanınmış olup, gerçek dışı veriler kayıtlardan kaldırılabilmektedir[27].

Öte yandan, kişinin başka kişisel bilgisini içermeyen ve sadece isminin geçtiği başkasına ait fiziksel belgeler veya e-postalar ise, kişisel veri kapsamına girmemektedir. Bu noktada "kişiyle doğrudan ya da dolaylı belirlenebilir kılmak" ifadesinden ne anlaşılması gerektiğini netleştirmek önem arz etmektedir. Bu bağlamda, bazen kişinin ismi gibi bilgiler kişiyi doğrudan ve tek başına belirlemek için yeterli olurken, "dolaylı" kavramı ise, kişinin kim olduğunu saptamakta tek başına yeterli olamayacak bilgilere referans vermektedir. Ses kaydı, fotoğraf, telefon numarası, meslek gibi bilgiler bu anlamda bağlantı kuran ve dolaylı olarak kişiyi belirleyen bilgilerdir[28].

Bu tanımlar beraberinde çeşitli sorun alanlarını doğurmaktadır. Örneğin; Avrupa İnsan Hakları Mahkemesi'nin (AİHM) vermiş olduğu *von Hannover v. Almanya Kararı*[29] başvurucunun fotoğrafları karara esas teşkil etmiştir. Buna göre bir paparazzi Monako Prensesi Caroline'i sürekli takip ederek, çocukları ile gezintisinden alışverişine kadar her anının fotoğraflarını kaydetmiş ve magazin haberlerinde kullanmıştır. Başvurucunun şikayeti sonrası durumu inceleyen Alman mahkemeleri, başvurucunun kamuya mal olmuş bir kişi olduğu için izole olmayan kamusal alanlarda çekilmiş fotoğraflarının özel yaşamın gizliliği için bir tehdit oluşturmadığı yönünde bir sonuca ulaşmıştır. Ancak başvurucu davayı AİHM'ye taşımış ve AİHM her ne kadar başvurucunun kamusal bir şahsiyet olsa bile, özel hayatına saygı duyulması gerektiği konusunda meşru bir

[26] Aksoy, s.14-15.
[27] "Unutulma hakkı" olarak ele alınan bu kavram dijital ya da yarı fiziksel hafızada yer alan bireylere ait rahatsız edici her türlü kişisel içeriğin, yine bireylerin talebi üzerine bir daha geri getirilemeyecek biçimde ortadan kaldırılması/silinmesi" olarak tanımlanmaktadır. Bkz: Gülener, Serdar: "Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak Unutulma Hakkı", Türkiye Barolar Birliği Dergisi, 102, Ankara, s.226.
[28] Aydın, S. Erdem: Kişisel Verilerin Kaydedilmesi Suçu, Oniki Levha Yayıncılık, İstanbul 2015, s.5.
[29] Von Hannover vb. Germany, Başvuru No. 59320/00, 24.06.2004.

beklentiye sahip olabileceğini belirtmiş ve eylemi Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 8'inci maddesine aykırı bularak ihlale hükmetmiştir[30].

Ancak, bugün kişisel verinin kapsamına ilişkin tartışmalar kişiyle ilgili olan ve onun tanınmasını sağlayan her türlü verinin kişisel veri olarak kabul edilmesinden kaynaklı olarak önemini yitirmiştir. Örneğin; birçok kişi kişisel veriyi yakın çevresi haricindekilerin bilmesini istemediği veri olarak tanımlarken, bazı bireyler kamunun bilmesinin önemsenmediği genel veriler konusunda hassas olabilmektedir. Dolayısıyla, kişinin kendi mantık çerçevesince saklamak istediği veriler de kişisel veriler kapsamına girmektedir. Doktrinde AKDAĞ tarafından savunulan görüş de bu kişinin subjektif konumunun bir önemi olmadığı ve kişinin başkaları tarafından bilinmesini önemli bulmadığı ve açıkladığı birçok verinin de aslında kişisel veri kapsamına girdiği yönündedir[31].

Diğer yandan, bir verinin kişisel veri olarak kabul edilebilmesi için sahip olması gereken dört temel unsur bulunmakta olup, bunlar sırasıyla incelenecektir.

1.2.1. Bir veri bulunması

Gerek AB mevzuatında gerekse de bu mevzuattan hareketle oluşturulan 6698 sayılı KVKK'da verinin kapsamı "her türlü bilgi" olarak çevrelenmiştir. Bu kapsamda veri; "*bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgidir"*. Ancak, günümüzde eş anlamlıymış gibi kullanılmaktaysa da, veri ve bilgi kavramlarının aslında aynı şey olmadıkları ile ilgili ciddi tartışmalar söz konusudur. Aslında bilgi alıcı için anlamlı bir formda işlenen tüm verileri ifade ederken, veri ise bilgi üretmek için işlenen ve rafine edilen hammadde olarak tanımlanmaktadır. Dolayısıyla, *"bilgi = veri + anlam"* olarak formüle

[30] Aydın, s.5.
[31] Akdağ, Hale: Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara 2013, s.8.

edilmektedir. Buna göre veri bilgiden daha dar kapsamlıdır ve ancak anlamlı bir hale geldiğinde bilgiye dönüşmektedir[32].

Nitekim, veriye dair geliştirilen bir başka tanım da benzer şekilde işlenmemiş olma durumuna referans vermektedir. Bu bağlamda veri; *"tek başına anlam ifade etmeyen veya kullanılamayan, bununla birlikte enformasyona ve bilgiye temel oluşturan ilişkilendirilmeye, gruplandırılmaya, yorumlanmaya, anlamlandırılmaya ve analiz edilmeye gereksinim duyulan ham bilgidir"*[33]. Burada dikkat çekici olan husus verinin işlenmeye hazır olması ve bilgiye temel oluşturmasıdır.

Bununla birlikte veri koruma hukuku bağlamında veri (data), enformasyon (informasyon) ve bilgi (knowledge) birbirlerinin yerlerine kullanılmaktadırlar[34]. Bununla birlikte her ne kadar farklı anlama sahip olsalar da, yararlandıkları hukuki koruma bakımından farklılaşmamaktadırlar[35].

Diğer yandan veriler, sadece bilgisayar verisi ya da elektronik veri olarak sınıflandırılamaz. Böyle bir tanım bilgisayarlar ya da elektronik ortam dışındaki veri güvenliğinin ihlaline ilişkin suçları kapsam dışı bırakma riski doğurmakta ve kişisel verilerin koruma alanını daraltmaktadır. Bununla birlikte, verinin *öznel ya da nesnel olması; gerçek ya da yanlış olması, nasıl ve nerede bulunduğu* da kişisel veri olma niteliğini değiştirmemektedir. Çünkü kişiyi belirlemeye yarayan bir yanlış bilgi de kişisel bir veridir[36]. Dolayısıyla "her türlü bilgi" kavramı, bireyin saklamak isteyebileceği tüm bilgilere referans vermekte olup, geniş bir kapsama sahiptir. Bir şahsın ya da tüzel kişiliğin kendisi ile ilgili paylaşılmasına izin vermediği tüm bilgileri saklama hakkı mahfuz olup, bir kişinin diğerinden ayrışmasını sağlayacak bilgiler kişisel veri kapsamındadır. Kişinin içinde bulunduğu toplumun diğer üyelerinden ayrılmasına imkan sağlayan her türlü bilgi onun kimliğinin belirlenmesine yarayan bilgi durumunda olup; ad-soyadı, bilgisayar ortamındaki dijital kimlikleri gibi birinin

[32] Dülger, Kişisel Verilerin Korunması, s.6.
[33] Doğan, Korcan ve Arslantekin, Sacit: "Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum", DTCF Dergisi, 56, Ankara 2016, s.16.
[34] Aksoy, s.11.
[35] Küzeci, s.12.
[36] Dülger, Kişisel Verilerin Korunması, s.8-9.

bulunmasına katkı sağlayan her türlü bilgi kimliği belirleyen bilgiler arasında yer almaktadır[37].

1.2.2. Gerçek kişiye ait olma

KVKK'ya göre bir bilginin kişisel olabilmesi için gerçek kişiye ait olması gerekmektedir. DÜLGER de, kişisel verilerin korunması hakkının bir insan hakkı olduğunu belirtmekte olup, bu koruma hakkının gerçek kişilere ait olması gerektiğinin altını çizmektedir. Ona göre, tüzel kişilerin kimlikleri kişisel veri niteliğinde değildir. Yine, tüzel kişilere ait olsa da, gerçek kişilerle ilişkilendirilemeyen bilgiler de yasal koruma kapsamında değildir. Tüzel kişilere ait olup gerçek kişilerle ilişkilendirme mümkünse bu veriler de KVKK'nın kapsamına girmektedir. Örneğin; 2014 tarihli Anayasa Mahkemesi (AYM) kararında kişisel bilgilerin sadece gerçek kişilere ilişkin kimlik belirleyici bilgiler olmadığının altı şu ifadelerle çizilmiştir; "*..Tüzel kişilerin reklam ve tanıtım amacıyla da olsa fiziki ve elektronik adreslerinin rızaları dışında bir başka özel hukuk tüzel kişisi ticari işletme tarafından ticari amaçlarla kullanmak üzere Kanunla yetkilendirilmesi adaletsiz ve hakkaniyete aykırı olduğundan, hukuk devleti ilkesiyle bağdaşmaz"*[38].

Buradan da anlaşılacağı üzere tüzel kişilik aslında hukuk dünyasında kabul edilen bir olgudur ve gerçek kişiden bağımsız değildir. Tüzel kişilik bünyesinde çalışan X kişisine ait bir cep telefonundaki veriler tüzel kişiye ait veriler olarak kabul edilse de, muhatap X kişisidir. Dolayısıyla, tüzel kişiye ait olduğu var sayılan bilgiler bile gerçek kişilerle ilişkilendirilebildiği takdirde kişisel veri niteliğini haiz olmaktadır. Bir diğer deyişle, kişisel verilerin korunmasını sağlayan yasal düzenlemeler, ancak bu kişisel veriler gerçek kişilere aitse uygulama alanı bulabilmektedir[39].

[37] Küzeci, s.13.
[38] AYM, E. 2013/84, K. 2014/183, KT: 4.12.2014, R.G. 29294, 13.03.2015.
[39] Dülger, Kişisel Verilerin Korunması, s.9-10.

1.2.3. İlişkin olma

Bir bilginin kişisel veri kapsamına girebilmesi için bir kişiye ilişkin olması gerekmektedir. Bu kapsamın dışında kalan, kişiye ait olmayan ya da kişiyle ilişki kurulamayan bilgilerin kişisel veri değerinde görülmesi mümkün değildir. Bu bağlamda, hangi bağlantı ve ilişkilerin belirleyici olduğu ve nasıl ayırt edilebileceği önem arz etmektedir. Nitekim kişisel veriler doğrudan kişileri gösterebileceği gibi, o kişinin kimliğini tanımlamamakla birlikte herhangi bir başka kayıtla ilişkilendirilmesi mümkündür ki, bu da onu KVKK kapsamına almaktadır.

Birçok durumda (cep telefonu, isim, fotoğraf vb.) veri ile kişi arasında doğrudan ilişki, kolayca kurulabilmektedir. Bu durumda verilerin aktardığı bilgiler, kişiyle açıkça ilgilidir. Ancak veriler bazen bireyle doğrudan ilişkili olmayıp, gerçek kişiye ait nesnelerle ilgilidir. Bu veriler doğrudan bir kişiye işaret etmese de, bireylerle veya başka nesnelerle fiziksel ya da coğrafi bir yakınlık sağlayabilmektedir ve bu da başka verilerin kullanımıyla bir kişiye belirleyebileceğinden yine de, o kişiye ait kabul edilmektedir[40].

Diğer yandan verilerin kişi ile olan bağlantısı; hukuka aykırı şekilde, olağanüstü veya beklenmedik yöntemlerle kuruluyor ya da kurulmasına imkan tanınıyorsa, bu verinin kişi ile ilişkili olduğu ve kişisel veri kavramına dahil olduğu söylenememektedir[41].

1.2.4. Belirli ya da belirlenebilir olma

Kişisel veri kavramının bir diğer önemli unsuru ise kişinin kimliğinin hangi hallerde belirli ya da belirlenebilir olduğunun tespit edilmesidir. Bu bağlamda bir kişinin kimliğinin belirli olması o kişinin bir grup insan arasında ayırt edilebilmesi durumu iken, belirlenebilir olması ise henüz grup içerisinde ayırt edilememiş birisinin diğerlerinden ayırt edilmesinin mümkün olduğu durumlara referans vermektedir. Bu bağlamda, bir verinin bir gerçek kişiyi belirlenebilir kılması doğrudan ya da dolaylı olarak gerçekleşebilir. Örneğin; kişinin kimliğinin belirlenmesinde ismi bir doğrudan

[40] Aksoy, s.19.
[41] Korkmaz, İbrahim: Kişisel Verilerin Ceza Hukuku Kapsamında Korunması (Kişisel Veriler ve Ceza), Seçkin Yayınevi, Ankara 2017, s.42.

belirleme unsuru iken, telefon, ruhsat, sosyal güvenlik, pasaport numaraları ile yaş, meslek, ikametgah gibi birden çok ölçütün birleşmesi de kişinin kimliğinin belirlenmesine dolaylı olarak katkı sağlamaktadır[42]. Bu unsurların sayısını çoğaltmak elbette mümkündür.

Hangi şartlarda verinin ilgili kişinin kimliğini belirlenebilir kılacak olduğunun tespiti tartışma konusudur. Buna göre bir verinin bir kişiyi belirlenebilir kılıp kılmadığının araştırılması ciddi bir süreç olup, eldeki verinin ayrıntılı ve yoğun bir çaba harcanarak ilgili kişinin kimliğini belirlenebilir kılacak niteliği haizse kişisel veri olarak kabul edilebileceği yönünde bir görüş söz konusudur. Bir diğer deyişle araştırmacının makul olmayan maddi yükümlülük altına girmemesi gerekmektedir[43]. Diğer yandan, ulusal veri koruma mevzuatı ise araştırma çok fazla zaman veya çaba gerektirmeden kişiyi belirlemeye yarayan verileri kişisel veri olarak kabul etmektedir[44].

Bu noktada uygulanması gereken yöntem, her somut olaydan hareketle sübjektif veri oluşturmak olup, amaç; verinin kimliği belirli ya da belirlenebilir bir gerçek kişiyi tanımlamaya yetip yetmediğinin tespit edilmesidir. Dolayısıyla sorulması gereken sorular; *"elimizdeki herhangi bir veri gerçek kişiyle ilişkilendirilebiliyor mu? Bu veri herhangi bir gerçek kişiyi tanımlayabiliyor mu?"* olmalıdır. Örneğin bir evin ekonomik değeri bir nesneye ilişkin gözükse de, bir kişinin mal varlığını belirlemeye yardımcı olacağından o kişiye ait bir kişisel veridir. Benzer şekilde, bir kişiyi tanımlamaya yetmeyen dolayısıyla kişisel veri olmadığı düşünülen takma isimler başka verilerle bir araya getirilerek kişiyi tanımlamaya yardımcı oluyorsa, kişisel veri kapsamına girmektedir[45]. Çalışan performans değerlendirme raporları, mülakat sonuçları, müşteri şikayet notları da bu kapsamda kişisel veriye dönüşmektedir[46].

[42] Aksoy, s.22.
[43] Korkmaz, Kişisel Verilerin Korunması, s.41.
[44] Sarıusta, Kader: Kişisel Verilerin Ceza Hukuku Yoluyla Korunması (Yayımlanmamış Yüksek Lisans Tezi), Gaziantep 2018, s.12.
[45] Atasoy, Kemal: "Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 3, İstanbul 2016, s.295.
[46] KVKK: 100 Soruda Kişisel Verilerin Korunması Kanunu, KVKK Yayınları, Ankara 2018, s.19.

1.3. Kişisel Verilerin Korunmasına İlişkin Temel Kavramlar

Kişisel verinin daha değerli ve aynı zamanda tehditlere açık olduğu günümüzde kişisel verilerin korunmasına yönelik düzenlemeler artmaktadır. Bu doğrultuda kişisel verilerin korunmasına ilişkin temel kavramların doğru bir şekilde tanımlanması, artan risklere yönelik hukuki düzenlemelerin gerçekleştirilmesi açısından önem arz etmektedir.

1.3.1. Veri kayıt sistemi

Avrupa Birliği Genel Veri Koruma Tüzüğü'nde (GVKT) kişisel verilerin işlenmesi; "*otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme ya da imha gibi herhangi bir işlem veya işlem dizisi"* olarak tanımlanmakta olup, tüm bu işlemlerin gerçekleştirildiği platform için bir veri kayıt sistemi gerekmektedir[47].

Bu bağlamda, GVKT'ya göre veri kayıt sistemi ya da dosyalama sistemi; kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği/dosyalandığı kayıt sistemleridir. Bu sistemler fiziksel ya da elektronik ortamda oluşturulabilmektedir. Bu sistemler kapsamında kimlik bilgilerinin yanı sıra, trafik cezalarından vergi ve banka borçlarına kadar geniş bir amaçlar yelpazesi söz konusu olabilmektedir. Bu bağlamda, önemli olan gelişi güzel bir kayıt değil; Kanun kapsamında ve belirli bir kritere göre kayıt tutmaktır. Örneklendirmek gerekirse; A şehrinde oturanlar B hastanesinin hastaları C firmasından telekomünikasyon hizmeti alanlar gibi sınıflandırma belirli kriterlere göre yapıldığından ve otomatik ya da yarı-otomatik bir ortamda tutulduğundan Kanun kapsamına girmektedir. Nitekim, KVKK'nın 3. maddesinde kişisel verilerin işlenmesi kavramı için *".. kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla*" ifadelerine yer verilmektedir. Bu bakımdan GVKT ile KVKK arasında ciddi bir paralellik söz konusudur[48]. Diğer yandan, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'le,

[47] General Data Protection Regulation (GDPR), Official Journal of the European Union, 2016.
[48] Aysun, M. Köse: Kişisel Verilerin Kaydedilmesi Suçu, Seçkin Yayınevi, Ankara 2018, s.82.

veri kayıt sistemi tanımı; kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi olarak değiştirilmiştir[49].

Bu bağlamda, otomatik olmayan yollarla yani insan müdahalesiyle tutulan kayıtlar kişisel özelliği haiz olsa da, bu kapsama girmemektedir. Ancak bu veriler kişisel veri niteliğini haiz olmayı sürdüreceği için bu verilere ilişkin hukuka aykırı eylemler Türk Ceza Kanunu (TCK) kapsamında suç teşkil etmeyi sürdürecektir[50].

Diğer yandan, kişisel verilerin muhafaza edileceği veri kayıt sisteminde verilerin saklanma süresi ve verilerin boyutları ile ilgili sorunlar oluşabilmekte olup kişisel verilerin saklanması açısından verilerin boyutlarının ekonomik ölçeklere çekilmesi ya da büyük veri kapsamındaki çalışmalarla daha güvenli saklanması sağlanabilmektedir[51].

1.3.2. İlgili kişi/veri kişisi

Bu kavram, Direktif'in 2. maddesinde ve 108 sayılı Avrupa Konseyi (AK) Sözleşmesi'nin 2. maddesinde "veri öznesi" olarak nitelendirilmekte olup, referans verilen husus "*belirli veya belirlenebilir kıldığı gerçek kişidir"*. KVKK'da bu kavram yerine "ilgili kişi" kavramı tercih edilmekte olup, 3'üncü maddede, "*kişisel verisi işlenen gerçek kişi"* tanımına yer verilmektedir. Bir diğer görüşe göre ise veri öznesi, kendisini belirli veya belirlenebilir kılan verilerin ilişkili olduğu, verileri işleme konusu yapılan ve korunması gereken "ilgili kişidir"[52].

İlgili kişi kavramının kapsamı bir tartışma konusudur. Örneğin, tüzel kişi bu kapsama girmemektedir ancak gerçek kişileri ilgilendiren tüzel kişilere ait veriler bu kapsamda sayılmaktadır. Ancak, herhangi bir şirket olmadan tacir olarak ticari faaliyet yürüten kişilerin verilerinin kişisel veri olarak kabul edilip edilmeyeceği tartışmalı olup,

[49] Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğde Değişiklik Yapıldığına Dair Tebliğ, R.G. 30758, 20.04.2019.
[50] Gündüz, Ünsal: "KVKK ve GDPR Kapsamında Veri Kayıt Sistemi", https://unsalgunduz.av.tr/tr/kvkk-ve-gdpr-kapsaminda-veri-kayit-sistemi, (Erişim Tarihi): 26.03.2019.
[51] Erdinç, G. Hazar: Bilgi Güvenliği, Kişisel Verilerin Korunması ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler (Yayımlanmamış Yüksek Lisans Tezi), İstanbul 2017, s.105.
[52] Küzeci, s.17.

Türkiye'de bu konudaki yaklaşım henüz belirsizdir[53]. Diğer yandan, vefat etmiş kişilerin "ilgili kişi" olması İtalya'da bazı durumlarda kabul görürken, Türkiye'de ise bu söz konusu değildir. Çocukların "ilgili kişi" olması hususunda ise İspanya gibi bazı AB ülkelerinde özel düzenlemeler bulunurken, Türkiye'de ise özel düzenleme bulunmamaktadır[54].

1.3.3. Veri sorumlusu

Kişisel verilerin dolaşım hızının artmasıyla birlikte verinin sorumluluğu önemli bir konu olmuştur. Tarihte ilk veri sorumlusu devletler olup, kamunun güvenliğini sağlamak ve hizmet sunmak için insan kaynağını bilmeye ihtiyaç duyarlar. Devlet dışındaki özel sektör kuruluşlarının veri sorumlusu statüsüne sahip olmaları ise tüketim ekonomisiyle birlikte kişilerin belirli mal ve hizmetlerin müşterisine dönüşmesiyle mümkün olmuştur[55].

OECD Rehber İlkeleri'nde veri sorumlusu; "*bizzat sorumlu veya yetkili kıldığı temsilcisi tarafından toplanmış, yayılmış, depolanmış veya işlenmiş olup olmadığına bakılmaksızın kişisel verilerin, ulusal hukukta kullanılması ve kullanım içeriğinin belirlenmesi konusunda karar vermeye yetkili kişi*" olarak tanımlanırken[56], 108 Sayılı Sözleşmede "*otomatik veri dosyasının amacının ne olacağı, hangi kişisel veri kategorilerinin kaydedilmesi gerektiği ve bunlara hangi işlemlerin uygulanacağı hakkında karar verebilecek olan gerçek veya tüzel kişiler, kamu kurumu, birimi veya ulusal kanunlara göre yetkili olan diğer kuruluşlar*" şeklinde tanımlanan "dosya yöneticisi" burada veri sorumlusuna karşılık gelmektedir. GVKT veri sorumlusunu, "*kişisel verilerin işlenme amaçlarını ve araçlarını belirleyen gerçek veya tüzel kişi*" olarak tanımlarken, GVKT ile uyumlu KVKK'nın "Tanımlar" başlıklı 3'üncü maddesinin 1'inci fıkrasının (ı) bendinde ise veri sorumlusu; "*kişisel verilerin işleme*

[53] Uzun, F. Burak: Türk Hukukunda Kişisel Verilerin Korunmasına Genel Bakış (Yayımlanmamış Yüksek Lisans Tezi), İstanbul 2016, s.9-10.
[54] Uzun, s.10.
[55] Oğuz, s.122.
[56] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, (Erişim Tarihi):26.03.2019.

amaçlarını ve araçlarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak ifade edilmektedir.

Veri sorumlusu kavramının yanı sıra veri denetçisi (data controller) ve veri kütüğü sahibi terimlerinin de kullanıldığını belirten KÜZECİ ise, daha kapsamlı bir şekilde veri sorumlusunu, "*verilerin işlenmesindeki amaç ve araçlara karar veren kişi ya da örgüt*" olarak tanımlamaktadır[57].

KVKK'ya göre tüzel kişiler, kişisel verileri işleme noktasında gerçekleştirdikleri faaliyetler itibariyle bizatihi "veri sorumlusu" olurken, bunların eylemlerinden doğacak hukuki sorumluluk tüzel kişiliğin şahsındadır. Bu bağlamda, şirketler bünyesinde yer alan birimler tüzel kişiliğe sahip olmadığından, veri sorumlusu olarak kabul edilememektedir. Ancak bir şirketler topluluğunda, her bir şirket tüzel kişiliğe sahip olduğundan, bu şirketlerin her birinin ayrı veri sorumlusu olması söz konusudur[58].

KVKK'ya göre veri sorumlusu kişisel verilerin işlenme amacını ve yöntemini belirlemektedir. Veri sorumlusunun tespiti için, kişisel verilerin toplanması ve toplama yöntemi, toplanacak kişisel veri türleri, toplanan verilerin hangi amaçlarla kullanılacağı, hangi bireylerin kişisel verilerinin toplanacağı, toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı ve saklanma süresi konularında kimin karar verdiği önem arz etmektedir[59].

Diğer yandan, veri sorumlusundan KVKK'dan doğan bütün yükümlülükleri[60] yerine getirmesi beklenmemektedir. Bu yükümlülüklerin yerine getirmesinden sorumlu tutulacak olanlar; yetkili organlar ve tüzel kişilik çevresinde bulunan gerçek kişilerdir. Bu bağlamda, yükümlülüklerin gerektiği gibi yerine getirilmemesinden doğacak hukuki sorumluluk tüzel kişiliğin kendisine yani veri sorumlusuna ait olacaktır[61].

---

[57] Küzeci, s.15.
[58] KVKK, s.30.
[59] KVKK, s.30.
[60] Veri sorumluluklarının yükümlülükleri kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek ile bu verilerin muhafazasını sağlamak olup, ayrıntılı bilgi için Bkz. 3. Bölüm.
[61] Dülger, Kişisel Verilerin Korunması, s.19.

1.3.4. Veri işleyen

KVKK'ya göre veri işleyen, "*veri sorumlusunun verdiği yetkiye dayanarak ve veri sorumlusu adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek, bağımsız veya tüzel kişilerdir*". Veri işleyenler veri sorumlusuna bağlı olmak zorunda değildir. Veri işleyenler kendilerine verilen talimata dayanarak verileri işlerken, veri sorumlusu ile veri işleyen arasında kişisel veri sözleşmesi yapılmaktadır. Bu veri sözleşmesi kapsamında; kişisel verilerin toplanması ve saklanması için hangi bilgi teknolojileri sistemlerinin veya diğer metotlarının kullanılacağı, veri koruma için alınacak güvenlik önlemlerinin detayları, veri aktarımının yöntemleri, veri saklama sürelerinin uygulanmasında kullanılacak yöntem ile kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi yöntemleri karar verme yetkisi veri sorumlusu tarafından veri işleyene bırakılabilmektedir. Bu durumların birer örnek olduğu belirtilmiş olup sayıları çoğaltılabilecektir. Ancak, veri sorumlusunun yetkisini veri işleyene devretmesi onu sorumluluktan kurtarmayacak olup esas muhatap veri sorumlusunun kendisidir. Bununla birlikte ilgili kişinin kişisel verileri üzerindeki hakları için başvurması gereken kişi de yine veri sorumlusu olarak öne çıkmaktadır. Veri sorumlusu aynı zamanda aydınlatma yükümlülüğü, ilgili kişilerin hakları ve veri güvenliği ile ilgili yükümlülüklere dair her türlü teknik ve idari önlemin alınmasında da sorumludur[62].

KVKK'dan hareketle veri sorumlusuyla veri işleyen arasındaki müşterek bazı noktaların belirtilmesi gerekmekte olup, veri sorumlusunun bir şirket içerisinde veri işleme faaliyetinden sorumlu kişi olmadığı bilinmelidir. Bu anlamda veri sorumlusu KVKK'nın kendisine tanıdığı statüye göre tüzel kişilik olarak kabul edilmektedir. Bir diğer deyişle evrak teslim alan ya da kaydeden kişi "veri sorumlusu" sıfatına sahip değildir.

Bir diğer önemli husus ise her iki kavramın da hem tüzel hem gerçek kişiler için geçerli olduğudur. Örneğin; serbest bir mali müşavir de, mali müşavirlik firması da veri sorumlusu ve veri işleyen pozisyonunda olabilir. Yine, bir tüzel ya da gerçek kişi aynı anda hem veri sorumlusu hem de veri işleyen olabilmektedir. Örneğin bir

[62] Aysun, s.83.

telekomünikasyon şirketi kendi çalışanlarının verileri açısından "veri sorumlusu" pozisyonunda iken, hizmet sunduğu müşteriler açısından "veri işleyen" sıfatına sahip olabilmektedir[63].

1.3.5. Veri sorumluları sicili

Veri sorumluları sicili sorumlularının kayıt olmak zorunda oldukları ve veri işleme faaliyetleri ile ilgili bilgileri beyan ettikleri bir kayıt sistemidir. Direktif'in 21'inci maddesinde üye devletlere bir sicil tutma zorunluluğu getirilmiştir. KVKK'nın 16. maddesi uyarınca ise; "*Kurulun gözetiminde Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulmaktadır"* ifadeleri ile Kişisel Verileri Koruma Kurulu'nun gözetiminde, kamuya açık olarak Veri Sorumluları Sicili tutulacağına ilişkin bir düzenleme yapılmıştır[64]. Bu hususstaki düzenlemelerin ayrıntıları ise "Veri Sorumluları Sicili Hakkında Yönetmelik" ile belirlenmiştir[65].

Veri koruma sicilinin düzenlenmesinin amacı "ilgili kişilerin bilgilendirilmesi" olup, bu ilke bireyin kişisel haklarını etkin bir şekilde kullanabilmesi ve idarenin şeffaflığının sağlanabilmesi için önem arz etmektedir[66].

KVKK, veri sorumlularının veri sorumluları siciline kaydolmalarını zorunlu kılmakta olup, bu uygulamanın amacı veri sorumlularının kimler olduğunun kamuya açıklanması ve bu sayede kişisel verilerin korunmasının daha etkin şekilde kullanılmasıdır. Bu bağlamda, ilgili sicilin kanun kapsamında, kamuya açık olarak tutulması gerekmektedir. Bu şekilde ilgili kişiler istedikleri her an sicili görebilecek ve inceleyebilecektir. Böylece, hak ihlallerine karşı daha etkili şekilde mücadele etmesine imkan tanınacaktır. Dolayısıyla, tüm veri sorumlularının Veri Sorumluları Siciline kaydolmaları ve bu kayıt işleminin veri işleme sürecinin başlamadan tamamlanması gerekmektedir[67].

---

[63] KVKK, Veri Sorumlusu ve Veri İşleyen, https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen, (Erişim Tarihi): 31.03.2019.
[64] Sert, s.67.
[65] Veri Sorumluları Sicili Hakkında Yönetmelik, R.G. 30286, 30.12.2017.
[66] Küzeci, s.212.
[67] Oğuz, s.132.

KVKK'nın 28'inci maddesinin 2. fıkrasında sayılan hallerde kayıt yükümlülüğünü düzenleyen 16'ıncı madde hükümleri uygulanmayacak olup, Kurul tarafından kayıt zorunluluğuna istisna getirme yetkisi verilmiştir. Bu yetkiye istinaden belirlenen kriterler ise; kişisel verinin niteliği, sayısı, işlenme amacı, işlendiği faaliyet alanı, üçüncü kişilere aktarılma durumu, saklanma süresi, veri konusu kişi grubu veya kategorileri ile veri işleme faaliyetinin kanunlardan kaynaklanması olarak sıralanmaktadır[68].

Veri Kurulu Sicilinin oluşturulması, GVKT ile kaldırılmış olup, hâli hazırda kaldırılmış olan böyle bir organın, Türkiye'de yürürlüğe konması çeşitli tartışmaları beraberinde getirmiştir. DÜLGER ise AB'de yirmi yıldan fazla süre uygulanmış ve konuya ilişkin önemli bir farkındalık ve güven ortamı oluşturmuş olan bu organın kişisel verilerin korunması mevzuatına yeni adapte olan bir ülkede var olması gerektiğini belirtmektedir[69].

1.3.6. İlgili kişinin açık rızası

Kapsamı oldukça geniş olan kişisel verilerin işlenmesi faaliyeti belirli şartlar bir araya geldiğinde hukuki dayanak kazanmakta olup, bunların başında ilgili kişinin rızası yer almaktadır[70]. Bu bağlamda, ilgili kişinin rızası en önemli meşruiyet şartı olarak kabul edilmektedir[71]. Rıza kavramı sayesinde veri öznesi yani ilgili kişi, verilerinin geleceğini belirlemeye yönelik irade sahibi olurken, veri işleme prosedüründe basit bir obje konumunda kalmaktan kurtulmaktadır[72]. BAŞALP'e göre ise kişisel verilerin işlenmesi yasağının uygulama alanını daraltan en kapsamlı unsur, ilgili kişinin verilerinin işlenmesine karşı rızasıdır[73]. Doktrindeki tüm bu görüşlerden de anlaşılacağı üzere kişisel verilerin işlenmesinde hukuki meşruiyet sağlanması için ilgili kişinin rızası en önemli unsurdur.

---

[68] KVKK, s.70.
[69] Dülger, Kişisel Verilerin Korunması, s.19.
[70] Develioğlu, s.51.
[71] Küzeci, s.240.
[72] Şimşek, Oğuz: Anayasa Hukukunda Kişisel Verilerin Korunması, Beta Yayınevi, Ankara 2008, s.128.
[73] Başalp, Kişisel Verilerin Korunması, s.39.

Ancak, verilerin işlenmesine yönelik rızanın muteber kabul edilebilmesi için çeşitli niteliklerle donanmış olması gerekmektedir. Bu bağlamda, rızanın serbestçe verilmesi, spesifik olması, kişinin aydınlatılmasına/bilgilendirilmesine dayanması ve tereddütsüz kabul göstermesi onu açık rıza (expilicit consent) statüsüne dönüştürmektedir. Bu unsurun yerine getirilmesi aynı zamanda kişisel verilerin "amaçla bağlılık" ilkesine uygun işlenmesine de zemin sağlamaktır[74].

Açık rıza kavramı, hem özel nitelikli (hassas) hem de adi nitelikteki kişisel verilerin işlenmesi için şart niteliğinde temel kuraldır[75]. Ancak, kişisel verilerin işlenmesinde "tereddüde yer vermeyecek bir rıza beyanı" aranırken, hassas verilerin işlenmesinde "açık rıza" beyanı gerekmektedir[76].

Bu bağlamda, KVKK'nın oluşmasında önemli rolü olan Direktif'e göre açık rıza; "*ilgili kişilerin özgürce, o konuya ilişkin yeterli bilgi sahibi olarak ve belirsizliğe mahal vermeyecek şekilde irade beyanını dile getirmesi veyahut kendisine ilişkin kişisel verinin işlenmesini kabul ettiğine ilişkin açık olumlu hareket"* olarak tanımlanırken, KVKK 3. maddesinde açık rıza; "*belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*" şeklinde tanımlanmaktadır.

Bu kural uyarınca ilgili kişiler, kişisel verilerinin işlenmesi hususunda veri işleyene açık rıza vermelidirler. Nitekim, KVKK'nın 5. maddesinde "*kişisel veriler ilgili kişinin açık rızası olmadan işlenemez"* ifadesine yer verilirken, ayrıca kişisel verilerin yurt içinde aktarılması (KVKK, md. 8) ve yurtdışına aktarılması (KVKK, md. 9) noktalarında da ilgili kişinin açık rızası şart koşulmaktadır. Ayrıca, Anayasanın özel hayatın gizliliği ve korunmasına ilişkin 20'inci maddesinde de kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği belirtilmiştir[77].

[74] Akdağ, s.34.
[75] Oğuz,s.131.
[76] Başalp, Kişisel Verilerin Korunması, s.44.
[77] Erdinç, s.18.

Açık rızanın oluşması ile ilgili KVKK'da üç husus aranmaktadır. Bunlar;

- *Belirli bir konuya ilişkin olmak:* Buna göre ilgili kişi neye rıza verdiğini, hangi amaca yönelik ve hangi kapsamda kişisel verisini paylaşacağını bilmeli ve kişisel verisini buna göre paylaşmaya rıza göstermelidir. Buna göre açık rıza şartlarının oluşabilmesi için veri ilgilisi tarafından veri sorumlusuna yöneltilecek *"Kişisel verilerimin işlenmesini onaylıyorum/kabul ediyorum*" ya da *"Bütün kişisel verilerimin her türlü konuya ilişkin işlenmesine rıza gösteriyorum"* gibi genel ifadeler Kanun'un aradığı niteliği haiz değildir. Veri ilgilisinin veri sorumlusuna olumlu cevap vermesi de geçerli bir rıza talebi olmayacaktır. Bu nedenle hangi bilgilerin hangi konu için işlenebileceği rızada açıkça belirtilmelidir[78]. Rıza, özgür iradeyle ve hiçbir tereddüde mahal bırakmayacak şekilde açık olacak şekilde sözlü, yazılı veya elektronik ortamda alınmalıdır[79]. Ayrıca, kişinin rıza göstermesini müteakip, kişisel verinin üçüncü bir kişi ile paylaşılması ya da yurtdışına aktarılması söz konusuysa bu hususlarda da ilgili kişinin rızasının alınması gerekmektedir[80].

- *Bilgilendirme:* Açık rıza şartının oluşması için bir diğer önemli unsur bilgilendirme olup, KVKK'nın 10'uncu maddesi bu doğrultuda bir düzenleme içermektedir. Buna göre veri sorumluları, kişisel veri paylaşımının kapsamı ve sonuçlarından ilgili kişileri bilgilendirmekle/aydınlatmakla yükümlüdür. Bu bilgilendirme ise kişi açık rızasını vermeden önce "doğru bir şekilde" yapılması ve kişinin vereceği açık rıza da bunun sonucunda gerçekleşmelidir. Ayrıca, başka bir konuda kişisel verilerin işlenmesi gerekiyorsa, bu konuda da ilaveten rıza alınması gerekliliği söz konusudur[81]. Diğer yandan, bilgilendirme metninde yer alması gereken bilgiler; veri sorumlusunun kimliği, verinin hangi amaçla ne kadar süre işleneceği, kimlere hangi amaçla aktarılabileceği, kişisel verileri toplama yöntemi ve hukuki sebebi gibi hususlar olarak sıralanmaktadır. Ancak,

[78] Uncular, s.144.
[79] Oğuz, s.131.
[80] Erdinç, s.21.
[81] KVKK, s.26.

somut olayın özelliği doğrultusunda bilgilendirmede yer alması gereken hususlar bunlarla sınırlı olmayabilir[82].

- *Özgür iradeyle açıklama:* Son olarak açık rıza tanımının tam anlamıyla gerçekleşmesi için bir diğer önemli unsur ise "özgür iradedir". Buna göre ilgili kişiler belirli bir konu hakkında bilgilendirildikten sonra kişisel veri paylaşmaya rıza gösterirken hiçbir etki altında kalmadan ve bilinçli bir şekilde karar vermelidir[83]. Tehdit, korkutma, aldatma, yalan vb. durumlarda özgür iradenin varlığı risk altında olup, rızayı sakatlayan durum ve rızayı etkileme derecesi belirlenmelidir. Örneğin; işçi-işveren ilişkilerinde işçiler iş kaybı korkusuyla kendilerinden istenen rızayı sunmak zorunda hissedebilmektedir. Bu nedenle işverenler tüm işçilerine eşit ve açık bir biçimde rıza gösterme hakkı tanımalı ve rıza göstermedikleri takdirde olumsuz sonuçlarla karşılaşmayacakları konusunda garanti vermelidir. Ancak işverenin Kanun'dan doğan işleme hakkı söz konusuysa işçinin açık rızasına ihtiyaç duymayabileceği bilinmelidir. İşçi buna rağmen açık rıza vermiyorsa işçinin haklı olduğu söylenemeyeceği gibi, işçi-işveren ilişkisinin sürmesi de beklenemeyecektir[84].

Diğer yandan, kişinin sessiz kalmasının kişisel verisinin işlenmesine onay verdiği anlamına gelmediği unutulmamalı ve açık rıza gerektiren bir durumda ilgili kişinin susması kabul değil ret olarak yorumlanmalıdır[85]. Diğer yandan, kişinin sorulan sorular karşısında hareketsiz kalmasının bir rıza göstergesi olmadığı belirtilmektedir[86]. Nitekim, Kanuna göre kişi kendine ait verinin işlenmesine kendi isteği ya da karşı tarafa onay vererek açık irade beyan etmelidir. Bu açık irade beyanı ise verinin sınırları, kapsamı, gerçekleştirilme şekli ve süresini kapsamalıdır. Bu irade beyanı yazılı olmak zorunda olmayıp, elektronik ortamda, yani tüm dijital mecralarda gerçekleştirilebilmektedir[87].

[82] Yücedağ, s.774.
[83] Develioğlu, s.51; Erdinç, s.22.
[84] KVKK, s.27.
[85] Küzeci, s.221.
[86] Uncular, Selin: İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Seçkin Yayınevi, Ankara 2018, s.144.
[87] Erdinç, s.22.

Bu bağlamda bir diğer sorun alanı ise, açık rızanın geri alınıp alınamayacağıdır. Kişinin kendi verileri üzerinde hakimiyet kurabilme ve verilerinin geleceğini belirleyebilme hakkı ışığında verilerinin işlenmesini durdurma talebinin yerine getirilmesi en temel hakları arasındadır. Ancak, bu haklar ileriye doğru işleyebilmektedir. İlgili kişi böyle bir talep geliştirdiğinde daha önceden kaydedilen verilerden hareketle oluşacak sonuçlar engellenemez. Çünkü ilgili kayıtlar gerçekleştirilirken bu rıza alınmıştır. Bu nedenle veri sorumlusu rızanın geri alınması yönündeki beyan kendisine ulaştığı andan itibaren veri işleme faaliyetlerini durdurmak zorundadır[88].

Kişisel veriler bakımından açık rızanın aranmadığı haller

Kişisel verilerin işlenmesinde açık rızanın aranmadığı istisna durumlar söz konusu olup, bunlar; kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması olarak sıralanmaktadır[89].

Özel nitelikli kişisel veriler bakımından açık rızanın aranmadığı haller

Özel nitelikli kişisel verilerin işlenmesinde de açık rızanın aranmadığı istisna halleri olabilmektedir. Bunlar; sağlık ve cinsel hayata ilişkin özel nitelikli kişisel verilerin ve bunların dışındaki özel nitelikli kişisel verilerin işlenmesinde açık rıza aranmayan durumlar olarak farklı düzenlenmiştir. Buna göre sağlık ve cinsel hayat dışındaki özel nitelikli veriler ancak kanunlarda öngörülen hallerde işlenebilmektedir. Sağlık ve cinsel

[88] KVKK, s.29; Aysun, s.89.
[89] Sert, s.19.

hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacı dahilinde ve sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebilmektedir[90].

1.3.7. Verilerin işlenmesi

Kişisel verilerin işlenmesi KVKK'nın 2'inci maddesine göre; kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla ilk defa elde edilmesiyle başlayan bir süreç ve devamındaki her türlü işleme, veri işleme faaliyetidir. Bu bağlamda, kişisel verilerin hukuka uygun şekilde toplandıktan sonra silinmesi, yok edilmesi ya da anonim hale getirilmesine sürecine kadar olan her türlü faaliyet kişisel verilerin işlenmesi kapsamındadır.

Kişisel verilerin işlenmesinde çeşitli yöntemler kullanılmakta olup, bunlar; kişisel verilerin ilk kez elde edildikleri an itibari ile işleme fiiline başlamayı ifade eden elde etme veya kaydetme; fiziksel ya da dijital ortamda kişisel verilerin saklanması, tutulması ya da depolanması işlemin yani depolama/muhafaza etme; kişisel verilerin çeşitli yöntemlerle değiştirilmesi ya da düzenlenmesi olan değiştirme/yeniden düzenleme; çeşitli yöntemlerle kişisel verilerin iletilmesi olan aktarım/devralmadır[91].

Diğer yandan verilerin işlenmesi otomatik ya da bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla yapılabilmektedir. Otomatik işleme mecraları; bir algoritma çerçevesinde, yazılım veya donanım özellikleri sayesinde bilgisayar, telefon, saat vb. işlemci sahibi cihazlardır[92].

[90] KVKK, Özel Nitelikli Kişisel Verilerin İşlenme Şartları, s.3.
[91] KVKK, 6698 Sayılı Kanun'da Yer Alan Temel Kavramlar, s.11-12.
[92] KVKK, 6698 Sayılı Kanun'da Yer Alan Temel Kavramlar, s.13-14.

1.3.8. Anonimleştirme

Kişisel verilerin korunmasına dair bir diğer önemli kavram ise anonimleştirmedir. Verilerin ilişkin olduğu kişinin maskelenmesi[93] olarak da nitelendirilen anonimleştirme; "verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek" hale getirilmesi olarak ifade edilmektedir. Anonimleştirmede önemli kriter, veri ile veri sahibinin ilişkisinin kesilmesidir. Dolayısıyla, anonimleştirme faaliyeti yapıldıktan sonra hala verinin kime ait olduğu anlaşılmaktaysa, verinin anonim hale gelmesi söz konusu değildir.

Ancak, anonimleştirilmiş ve anonim veri farkına dikkat etmek gerekmektedir. Buna göre anonim veri başından itibaren kişiyle ilişkilendirilme imkanı olmayan veri iken, anonimleştirilmiş veri ise daha öncesinde bir kişiyle ilişkilendirilmiş ancak sonradan bağlantısı kesilmiş olan veridir[94].

Diğer yandan, anonimleştirmenin tam bir koruma sağlayıp sağlamadığı tartışma konusudur. Örneğin; bilimsel araştırmalar için elde edilen verilerin daha uzun süre depolanabilmesi için anonimleştirme mahremiyet hakkının korunmasına hizmet edebilirken, sağlık verilerinin anonimleştirilmesinde veri kişisinin verdiği onamı geri alma ya da vazgeçme hakkını kullanamamasına neden olmaktadır[95].

1.4. Kişisel Verilerin Korunmasına İlişkin Temel Kavramlara Dair Değerlendirme

Kişisel verilerin korunmasına ilişkin kavramlara dair gerek doktrinde gerekse de ulusal ve uluslararası mahkeme kararlarında yorum farkları söz konusudur. Bunlardan ilki kişi kavramının içeriğidir. Bu doğrultuda doktrin ve mevzuatta bir görüş birliği söz konusu olmayıp TEZCAN; veri koruma yasalarının sadece gerçek kişilere ait verileri kapsadığını söylemekte ve tüzel kişilerin koruma kapsamına alınmasına karşı

[93] Küzeci, s.224.
[94] KVKK, 6698 Sayılı Kanun'da Yer Alan Temel Kavramlar, s.18.
[95] Büken N. Örnek ve Ünsal, Ç. Zeybek: "Kişisel Verilerin Korunması Kanunun Biyomedikal Alana Yansımaları Açısından Değerlendirilmesi, Hacettepe Hukuk Fakültesi Dergisi 7, Ankara 2017, s.36.

çıkmakta[96], buna karşılık ŞEN tarafından dile getirilen görüş ise tüzel kişilerin de kişisel veri niteliğine sahip olabileceğini belirtmektedir[97]. Diğer yandan, KORFF ise tüzel kişilerin kişisel verilerinin de korunması gerektiğini savunmakta, özellikle dini, siyasi ve sendikal örgüt niteliğini haiz tüzel kişilerin verilerinin diğer tüzel kişilere göre daha sıkı bir koruma çerçevesi çizilmesi gerekliliğine vurgu yapmaktadır[98].

Bir diğer önemli husus ise kişisel veri ile hassas kişisel veri arasındaki ayrıma ilişkin olup, doktrinde bağlamsal ve amaçsal olmak üzere iki farklı görüş söz konusudur. Bağlamsal görüşün savunucularına göre, verilerin sınıflandırılarak bir kısmının hassas veri şeklinde sayılması kabul edilemeyecektir. Çünkü herhangi bir veri, bağlamı gereği hassas kişisel veriye dönüşebilecektir. Dolayısıyla, hassasiyet düzeyine karar verilmeden önce bir değerlendirme gerçekleştirilmelidir[99].

Amaçsal yaklaşım görüşünün sahiplerine göre ise, bir verinin hassas veri olup olmadığının tespitinde verinin işlenme amacı dikkate alınmalıdır[100]. Nitekim bu görüşe göre, işleme amacı dikkate alınmadan bir değerlendirme yapılmaması durumunda bir kimsenin soyadı bile etnik kökenini ortaya koyacağı için hassas veri sayılabilecektir. Bu nedenle, bir kimsenin ceza mahkumiyetine dair bilgileri hassas veri, özlük dosyasının tutulması için alınan nüfus cüzdanı fotokopisi üzerindeki veriler ise normal veri niteliğinde kabul edilmelidir[101]. Ancak, bu görüş "hassasiyet düzeyine karar verecek merciinin kimliğini gündeme getirmesi nedeniyle" eleştirilmektedir. Diğer yandan doktrinde; ülkemizde dernek ve vakıf üyeliği ile kılık kıyafet tercihlerinin bir ayrımcılık sebebi olarak algılandığı ve bu nedenle bunların özel nitelikte kişisel veri olarak sayılması gerektiği yönünde bir görüş bulunmaktadır. TAŞTAN ise vakıf ve dernek üyeliğinin bu niteliği haiz olduğunu ve gizli kalması gerektiğini ancak kılık kıyafet

[96] Tezcan, Durmuş: "Bilgisayar Karşısında Özel Hayatın Korunması", Anayasa Dergisi, Ankara 1991, s. 389.
[97] Şen, s.1202.
[98] Korkmaz, Kişisel Verilerin Korunması, s.89'den naklen Korff'un görüşü alınmıştır.
[99] Akgül, Kişisel Verilerin Korunması, s.15.
[100] Aksoy, s.34.
[101] Yücedağ, s.770.

tercihlerinin kişi tarafından alenileştirilmesi nedeniyle KVKK'nın 5'inci maddesiyle çelişeceğini belirtmektedir[102].

Bu noktada AİHM'nin verdiği S. ve Marper v. B. Krallık kararı veri kategorilerinin niteliğinin değişkenliğine dair önemli bir gösterge niteliğindedir. S. ve Marper tarafından B. Krallık aleyhine yapılan başvuru sonucunda AİHM; hücre örnekleri, DNA profili ve parmak izi kayıtlarının belirli ya da belirlenebilir bir kişi ile ilişkilendirilmesi halinde kişisel veri olduğunu ancak nitelik farkı nedeniyle bunların ayrı ayrı değerlendirilmesi gerektiğini belirtmiş ve kişisel veriler arasında bir ayrım yapılabileceğine hükmetmiştir[103]. Dolayısıyla bu noktada, KÜZECİ'nin görüşü olan verilerin niteliği ile ilgili tartışmalarda etkin koruma perspektifinin unutulmaması gerektiği fikrine[104] katılmaktayız.

Doktrinde bir başka görüş ise veri işleme faaliyetine ilişkin olup, hangi işlemlerin kişisel veri işleme faaliyeti kapsamında değerlendirileceğine kesin ve net bir cevap verilemeyeceği, ayrıca işleme faaliyetlerinin sınırlı olarak sayılmadığı savunulmaktadır. DÜLGER, veriler üzerinde herhangi bir işlem ya da değişiklik yapmadan sadece bir dijital ortamda saklanmasının bile işleme faaliyeti olduğunu belirtmektedir[105]. Bununla birlikte, kişisel verilerin elde edilmesi aşamasından başlayarak, silinme, değiştirme, yok edilme, işaretlenme, sınıflanma ve anonim hale getirilmesinin işleme faaliyeti olarak kabul edilmesi gerektiği savunulmakta[106], buna ilaveten kişisel verilerin aktarılması işlemi de hukuki mahiyeti itibari ile işleme faaliyeti olarak kabul edilmektedir[107].

Doktrinde bir başka görüş farklılığı ise veri kayıt sisteminin hukukiliğine ilişkindir. KORKMAZ tarafından öne sürülen bir görüş, kişisel verilerin tamamen ya da kısmen otomatik olan yollarla ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla kaydedilmesi gerektiğini, aksi takdirde suç oluşacağı

[102] Taştan, F. Güven: Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, Oniki Levha Yayıncılık, İstanbul 2017, s.42.
[103] S and Marper v UK, https://justice.org.uk/s-marper-v-uk-2008, (Erişim Tarihi): 03.04.2019
[104] Küzeci, s.237.
[105] Dülger, Kişisel Verilerin Korunması, s.16.
[106] Oğuz, s.128.
[107] Arslan, Çetin: "Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması", BAÜHF Kazancı Hakemli Hukuk Dergisi, Mart-Nisan, İstanbul 2011, s.41.

yönündedir[108]. Ancak, TCK 135'inci maddeye göre kişisel verilerin kaydedildiği yerin, bir veri kayıt sisteminin parçası olmak zorunda olduğunda dair herhangi bir düzenleme söz konusu olmayıp, bir bilgisayarda bulunan kişisel verilerin hiçbir veri kayıt sisteminin parçası olmayan kağıda yazılması da kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunu oluşturmaktadır[109].

Açık rızada örtülü beyanın yeterliliği, doktrinde en çok tartışılan hususlardan biridir. KÜZECİ, şüpheye yer bırakmayacak şekilde veri sahibinin iradesini ortaya koyan örtülü beyanın rıza olarak kabul edilebileceğini belirtirken[110], TAŞTAN ise örtülü beyan ile açık rızanın kabul edilmeyeceğini belirtmektedir[111]. Bu bağlamda, kişinin neye açık rıza gösterdiğini bilmesi ve göstermesi gerekmektedir. Bunun tek istisnası, doğası gereği kişisel verilerin açıklanmadan ya da bir taşıyıcıya teslim edilmeden verilmesi mümkün olmayan hizmetlerdir.

Bu bağlamda, açık rızanın amacı ile bağlılığı doğrultusunda her konu için ayrı ayrı alınması ile ilgili bir karar burada önem kazanmaktadır. Buna göre, 2012 tarihli Hamburg Veri Koruma Komisyonu'nun Facebook aleyhine idari kararıdır. Buna göre yüz tanıma yoluyla arkadaş bulma sistemi geliştiren platform, yeni kullanıcıların onaylaması gereken kullanım şart ve koşullarında bu duruma rıza gösterilmesine de yer vermiştir. Ancak, Hamburg Veri Koruma Komisyonu, standart şartlar ve koşullarda yapılan atfın, açık bir bilgilendirme kapsamına girmeyeceğine karar vermiş ve facebook'un biyometrik profil veri tabanını silmesi gerektiğine karar vermiştir. Dolayısıyla, açık rızanın geçerli olabilmesi için tüm hususların ayırt edilebilir şekilde ilgiliye sunulması gerekmektedir[112].

Açık rızaya ilişkin doktrindeki bir başka tartışma ise sınırlı ehliyetsizlerin tek başına rıza gösterip göstermeyecekleri konusudur. AKSOY'a göre kişisel verilerin işlenmesine rıza gösterilmesi nisbi anlamda kişiye sıkı sıkı bağlı hak olmasından ötürü sınırlı

[108] Korkmaz, Kişisel Verilerin Korunması, s.332.
[109] Sert, s.79.
[110] Küzeci, s.222.
[111] Taştan, s.156.
[112] Ayözger, s.121.

ehliyetsiz ile birlikte yasal temsilcinin açık rızası ile verilebilirken[113], TAŞTAN'a göre ise, mümeyyiz küçük ve kısıtlıların kişisel verileri Türk Medeni Kanunu (TMK) 16'ıncı madde doğrultusunda kişiye sıkı sıkıya bağlı haklar olduğundan tek başlarına rıza göstermelerini gerektirir[114].

[113] Oğuz, s.131.
[114] Taştan, s.163.

İKİNCİ BÖLÜM: KİŞİSEL VERİLERİN KORUNMASI HAKKI VE HUKUKİ DAYANAKLARI

2.1. Kişisel Verin Korunması Hakkı ve Hukuki Dayanakları

Kişisel veriler kişinin kendisi ve hayatıyla ilgili bilgiler olduğundan özel hayat kavramının sınırları içerisindedir. Dolayısıyla, bunların kişinin isteği dışında elde edilmesi, toplanması, kaydedilmesi noktasında haksız müdahaleler ve bu bilgilerin yayılması o kişinin özel yaşamının ihlalidir. Ancak, son yıllarda kişisel verilerin korunmasına "özel hayat kavramından hareketle yaklaşan perspektifin terk edilmeye başlandığı görülmektedir. 2000 tarihli AB Temel Haklar Şartı'nın 8. maddesi ile kişisel verilerin korunması bağımsız bir hak olarak kabul edilirken, GVKT'nın 1. maddesi ile kişisel verilerin korunması ana amacının kişilerin korunması olduğu vurgulanmıştır[115].

Bu bağlamda, kişisel verilerin korunmasını özel düzenlemelerinin konusu olmasının en temel sebebi; veri sahibinin kişilik haklarının korunması ile, bilginin serbest dolaşımı arasındaki dengenin doğru şekilde tesis edilmesidir. Bu bağlamda, demokratik toplumlarda kişilerin bilgi edinme ve haber alma hakları bulunmaktadır. Ancak, bireylerin haber alma hakları, kişisel verilerin kullanılmasını da kapsamakta olup, kişisel verilerin korunmasına yönelik düzenlemelerin, bu hakkı sınırladığına ilişkin tartışmalar gündeme gelmiştir. Özellikle, "bilginin güç olduğu" perspektifinden hareketle, kamu kurumları kamu hizmeti sunmak, suçlarla mücadele etmek ve vergi toplamak özel sektör ise tüketicilere erişmek amacıyla kişisel verileri toplamaktadır. Kamu kurumları açısından, 1960'lı yıllardan itibaren bu gelişmeler "fişleme" tartışmalarını beraberinde getirirken, bu bilgiler aynı zamanda üçüncü taraflarla paylaşılarak, ticari kazanç vesilesine de dönüşmektedir[116].

Özellikle teknolojideki hızlı gelişmeler, birbirinden bağımsız ve tek başına anlamsız duran verilerin "veri simsarları" tarafından toplanarak arşivlenmesini, mukayese edilmesini ve kazanç elde edilecek şekilde satılmasını mümkün kılacaktır. Bir adım

[115] Aysun, s.95.
[116] Aksoy, s.75.

ötesinde ise, çeşitli ilişkilendirme ve analiz yöntemleriyle, toplanan veri ile çok zararlı sonuçlar oluşabilecektir[117]. Örneğin; 2016 yılında Londra merkezli Cambridge Analytica isimli şirket, 50 milyon Facebook kullanıcısın hesaplarından izinsiz olarak topladığı kişisel verileri, Kasım 2016'daki ABD başkanlık seçimleri ile Haziran 2016'da Britanya'da gerçekleşen Brexit Referandumu'nun sonuçlarını etkilemek amacıyla kullanması ihtimaliyle büyük bir soruşturmaya uğramıştır[118].

Bu bilgiler ışığında kişisel verilerin korunması meselesinin bilgi alma hakkı ile toplanan bilgilerin zararlı kullanımı arasında bir "özgürlük mü güvenlik mi?" çatışması yaratabileceği söylenebilir. Nitekim, bu gelişmeler özel hayatın mahremiyeti, müdahale edilmezlik, yalnız kalma hakkı veya kamusal olmayan konularda kişinin ifşadan uzak tutulması ile ilgili tartışmaları gündeme getirmiş ve bireyin kendiyle ilgili veriler üzerinde tasarruf hakkı olduğunu belirten "kontrol merkezli" tanımları beraberinde getirmiştir. Bu tanımlardan biri, "bilgilerin geleceğini belirleme hakkıdır". Alman Anayasa Mahkemesi'nin 15 Aralık 1983 tarihinde verdiği Nüfus Sayımı (Census) Kararı buna önemli bir örnektir[119]. Buna göre nüfus sayısı sırasında vatandaşlardan kimlik bilgisi harici verilerin (gelir, eğitim durumu, çalışma saati vb.) toplanması ve yerel yönetimlere aktarılması, Nüfus Sayımı Kanunu'nda kişi hak ve özgürlükleri yeterince korunmamaktadır. Bu nedenle, kişiler kendilerinden elde edilen bilgilerin kim tarafından ne kadar süreyle ve hangi amaçlarla toplandığı konusunda bilgi sahibi olmalı ve bu bilgiler sınırsız şekilde işlenmekten korunmalıdır. Mahkeme kararına göre kişisel bilgilerin geleceğini belirleme hakkı, Anayasa ile güvence altındaki insan onuru ve kişiliği serbestçe geliştirme hakkının kapsamındadır[120].

Öte yandan ABD'de gerçekleştirilen bir araştırmada elde edilen sonuca göre, kişisel verilerin korunması bilgi edinme hakkına zarar vermemekte, aksine bu hakkı garanti altına almaktadır. Bunun nedeni, kişisel verilerin korunmasının serbest bilgi dolaşımının sınırını belirlemesi ve bu sınır çerçevesinde veri sahiplerinin kişisel verilerinin işlenmesine rıza göstermek zorunda olmalarıdır. Bu bağlamda, kişisel verilerin

[117] Küzeci, s.68-69.
[118] Sefer, s.123.
[119] "BVerfGE 65, 1 (44)", https://www.datenschutzbeauftragter-online.de/das-bundesdatenschutzgesetz-bdsg/urteile-des-bverfg-zur-informationellen-selbstbestimmung, (Erişim Tarihi): 28.03.2019.
[120] Akgül, Danıştay ve Avrupa, s.75.

korunması ile ilgili yasalar, bireyin mahremiyet hakkını korumayı amaçladığı gibi bilginin serbest dolaşımını da sağlamaktadır. Çünkü, kişisel verilerinin güvenliğine ilişkin daha az endişe taşıyan bireyler, bu verileri daha çok paylaşma eğilimine sahip olmakta ve bu sayede daha çok sayıda ve çeşitli bilgi paylaşıma açılmaktadır[121].

İşte tüm bu bilgiler ışığında devletin yükümlülüğü, vatandaşlarına ait verilerin hangi şartlarla işlenebileceğini düzenlemektir. Bu doğrultuda, hem ulusal hem de uluslararası mevzuatta kişisel verilerin korunması ile düzenlemeler yapılmaktadır.

Aşağıda sırasıyla medeni hukuk, idare hukuku ve ceza hukuku açısından, kişisel verilerin işlenmesine yönelik yaklaşım biçimleri ele alınacaktır.

2.1.1. Medeni hukuk bağlamında hukuki niteliği

Kişisel verilerin korunması hakkının hukuki niteliğine ilişkin birçok görüş bulunmakta olup, bu alanda tartışmalar güncel bir şekilde yürürlüktedir. Bu bağlamda, bu başlık altında kişisel verilerin korunması hakkının hukuki niteliğine ilişkin üç ana görüş olan kişilik hakkı, mülkiyet hakkı ve fikri mülkiyet hakkı görüşleri medeni hukuk bağlamında incelenecektir.

Kişilik hakkı görüşü

Türkçeye "kişi" olarak geçen "person" kavramının kökeni Latince "persona" kelimesi olup, Romalı aktörlerinin sahnede kullandıkları "maskelere" referans vermektedir. Kişilik hakkı ya da insan hakları kavramları, insanların doğuştan sahip oldukları bir takım hak ve özgürlüklere sahip olduğu fikrinden hareketle Magna Carta (1215), Virginia Haklar Bildirgesi (1776) ve Fransız İnsan ve Vatandaş Hakları Bildirgesi (1789) gibi metinlerde yer alarak modern hukuk sistemlerine girmiştir[122]. Bu bağlamda, kişilik hakkı görüşü "insan hakları yaklaşımı" başlığı altında ele alınmaktadır ve özel yaşamın gizliliği temelde bir insan hakkı olarak kabul edilmektedir. Bu yaklaşım,

[121] Culnan, Mary J., "How Did They Get My Name?": An Exploratory Investigation of Consumer Attidudes toward Secondary Information Use", MIS Quarterly3, 1993, s.360.
[122] Akkurt, S. Sami. "Kişilik Hakkının Sosyal Medya Kullanıcıları Tarafından İhlâli Halinde Ortaya Çıkacak Cezai Sorumluluğa Medeni Hukuk Bağlamında Bir Bakış", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 25 (2), Konya 2017, s.343-344.

özellikle Avrupa'da yaygın olup, bazı Amerikan yargı kararlarında da bu görüşün baskın olduğu ifade edilmektedir[123].

Özellikle Nazi Almanya'sı ve Mussolini İtalya'sı gibi bireysel özgürlüklerin kamu kurumlarının elinde büyük felaketlerle karşılaştığı ve bu nedenle bireysel özgürlükler çevresinde önemli hassasiyet oluşmuş olan Kıta Avrupa'sında hakim olan kişilik hakkı görüşünün savunucularına göre, kişisel veriler kişilik hakkının bir parçası olup, kişisel verilerin korunması ile amaçlanan kişilik hakkının görünümleri olan mahremiyet ve özel hayatının korunmasıdır. Bu görüşe göre, mahremiyet bireyin kişiliğine bağlı, devredilemez ve vazgeçilemez bir insan hakları değeri niteliğindedir. Bu değer kapsamında en önemli hususlardan biri de, bilgi mahremiyetidir. Bilgi mahremiyeti kavramı ışığında kişiler, kendilerine ait bilgilerin toplanması, kullanılması ve açıklanması üzerinde denetim hakkına sahiptir[124]. Dolayısıyla, yurttaş olmanın temelinde bireylerin kişisel verilerinin korunması çok büyük bir öneme sahip olup, kişinin insan onuru ve kişilik hakkı aynı zamanda yurttaşlığının da bir gereğidir[125]. Diğer yandan, kişilik hakkı kavramına bilimsel, teknolojik gelişmelerin yarattığı yeni ilişkilerin ortaya çıkartabileceği tehlikelere karşı koyabilmek için de gerek olduğu belirtilmektedir. Yani bu hak sayesinde kişiler, gözetlenmeden yalnız kalabileceği, kendi özel güven duyduğu kişilerle iletişim kurabileceği ve kendisini geliştirebileceği özel bir alanın varlığı konusunda garanti altına alınmaktadır[126].

Kişilik hakların sınıflandırılmasında ise, doktrinde bir görüş birliği bulunmamakta olup, en temel anlamda ise, iki ana yaklaşım söz konusudur. Bunlar şöyle sıralanmaktadır[127];

- *Egger'in Yaklaşımı:* Buna göre kişisel varlıklar iç ve dış kişisel varlıklar olarak ayrılmaktadır. İç kişisel varlıklar; doğuştan kaynaklanan haklardır. Vücut, yaşam, sağlık gibi varlıklar (bedensel); ruhsal tamlık üzerindeki haklar, faaliyet özgürlüğü ve kişisel işgücü üzerindeki irade gibi varlıklar (ruhsal) bu kapsamda yer alırken dış kişisel varlıklar kapsamında ise sosyal ilişkiye girme hakkıdır. Bu

[123] Küzeci, s.69.
[124] Aksoy, s.55.
[125] Akgül, Kişisel Verilerin Korunması, s.26.
[126] Sert, s.54.
[127] Aksoy, s.45.

kavram kapsamında; isim, meslek unvanları, armalar, şeref ve haysiyet, ticari markalar vb. yer almaktadır.

- *Bucher'in Yaklaşımı*: Bu yaklaşıma göre, kişisel varlıklar; psişik alan (utanma duygusu, ölülere saygı vb. kişinin duygusal durumuna ilişkin), fiziksel alan (bedensel dokunulmazlık) ve sosyal alan (isim, resim, marka, meslek durumu, ekonomik durum, şeref ve haysiyet ile özel yaşam) olarak üçe ayrılmaktadır.

Türk hukuk doktrininde en geniş şekilde kabul gören sınıflandırma, kişilik hakkı türlerinin esas alındığı sınıflandırmadır. Bu bağlamda, Türk hukuk sisteminde kişi "hak edinebilen varlık" şeklinde tanımlanmış olup, kişiler herhangi bir özel sebep aranmaksızın tam ve sağ doğmak koşuluyla kişilik kazanmaktadır. Ancak kişilik sadece doğuştan bazı haklara ehil olmakla sınırlandırılamaz. Bu bağlamda, en geniş tanımıyla kişilik hakkı, "para ile ölçülemeyen, manevi (tinsel) bir değere sahip ve kişilerin manevi kişisel değerleri üzerinde (onur ve saygınlık, özgürlük, giz, ehliyet vb.) geçerli olan haklardır". Bu haklar kapsamında; maddi (bedensel) haklar, manevi haklar ve mesleki ve ekonomik haklar girmektedir[128]. Dolayısıyla, kişilik hakkının korunması, insana manevi ve sosyal bir değer verilmesini ve saygı gösterilmesini sağlamaktadır[129].

Kişilik hakkı kavramı ve sınırlarına ilişkin 19. yüzyıl sonu ve 20. yüzyıl başında iki temel görüş yer almaktadır. Bunlardan ilkinin sahibi olan Romanist hukukçulara göre, kişiye ait varlıklar hem kamu hukuku hem de özel hukuk tarafından korunduğundan "kişilik hakkı" adı altında, bağımsız bir kavramın kabulüne gerek bulunmamaktadır. Onlara göre, hak kişisinin kendi kişiliğini oluşturan manevi ve maddi varlıkları ile olan ilişkisi hak niteliğinde olmayan hukuki menfaatlerden ibarettir. Bu yaklaşıma göre kişiliği saldırıya uğrayan birinin özel hukuk kaynaklı tazminat isteme hakkı için saldırganın kusurlu olması ve saldırının haksız bir fiil teşkil etmesi gerekmektedir. Bu yaklaşımın egemen olduğu Alman Medeni Kanunu'nun 823'üncü maddesinin 1. fıkrasında "diğer haklar" ifadesine yer verilmekteyse de, bunlar daha ziyade mülkiyete

[128] Doğan, P. Bahar: "Çatışan İki Değer: Haber Verme Hakkı ve Kişilik Hakkı", Ankara Barosu Dergisi, 4, Ankara 2014, s.480.
[129] Sancakdar, Oğuz: "Kamu Hukukunda Kişiliğin Korunması", İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi, 16, İstanbul 2017, s.40.

ilişkin olan marka, buluş, firma adı gibi haklara referans vermektedir. Aynı tarihlerde öne çıkan ikinci görüş ise, Cermen hukukçularına ait olup, onlar kişilik hakkı adı altında bağımsız bir hakkın varlığını kabul etmektedirler. Onlara göre, her kişi kendi kişilik alanını oluşturan varlıklar üzerinde kendine egemenlik sağlayan bir hakka sahiptir ve bu nedenle kişisel varlıklarına yönelebilecek tehditleri ve müdahaleleri önleme hakkına sahiptirler. Bu nedenle, kişilik hakkının ihlal edildiği durumlarda zararın tazmin edilmesi gerekmektedir[130].

Bağımsız bir kişilik hakkının benimsendiği ilk Kanun olan İsviçre Medeni Kanunu olup, 28/1 fıkrasında *"Şahsi menfaatleri tecavüze uğrayan kimse, hakimden tecavüzün men'ini talep edebilir"* hükmünü içermektedir. Nitekim, bu kanunun Türk hukukuna iktibas edilmesiyle, ilgili hak Türk hukukuna da girmiş olup, TMK m.24 ve Türk Borçlar Kanunu (TBK) m.49 çerçevesiyle beraber özel kişilik hakkına ilişkin daha birçok düzenleme getirilmiştir. Bunlardan bazıları; TMK m.25-26 ad üzerindeki hak; Fikir ve Sanat Eserleri Kanunu'nda (FVSK) mali ve manevi haklara tecavüze yönelik m.66.; TBK m.47'deki cismani zarar veya ölüm halinde ödenecek manevi tazminata yönelik düzenlemeler bunun en önemli örnekleridir[131]. Diğer yandan, tek bir genel kişilik hakkı vardır ve özel olarak düzenlenmiş kişisel hak türleri birden çok kişilik hakkının var olduğu anlamına gelmemektedir[132].

Bu bağlamda, Türk Hukukunda kişilik hakkı "parçalanamayan bir bütün" olarak kabul edilmektedir[133]. Kişilik hakkının özelliklerini maddeler halinde sıralamak gerekirse;

- *Mutlak bir haktır* ve hak sahibine en geniş yetkiyi sağlarlar. Hak sahibi bu sayede bu değerlere saygı gösterilmesini üçüncü şahıslardan ister ve yapılan müdahaleleri önleme yetkisine sahiptir.
- *Şahıs varlığı haklarındadır* ve bu nedenle kişilik değerlerini koruma kapsamına alırlar. Bu değerlere yapılan saldırı sonucunda maddi tazminat hakkının oluşması bunların manevi boyutunu göz ardı etme sonucu doğurmaz.

[130] Aksoy, s.39-40.
[131] Aksoy, s.41.
[132] Serozan, Rona: "Kişilik Hakkının Korunmasıyla İlgili Bazı Düşünceler", Mukayeseli Hukuk Araştırmaları Dergisi 14, 1977, s.96, http://dergipark.gov.tr/download/article-file/14235, (Erişim Tarihi): 31.03.2019.
[133] Uncular, s.41.

- *Şahsa sıkı sıkıya bağlıdır.* Buna göre kişilik hakkı mutlak bir hak olduğundan, herkese karşı ileri sürülebilmekte, kişiye sıkı sıkıya bağlı olduğundan devredilmesi, vazgeçilmesi ya da zaman aşımına uğraması mümkün olmamaktadır. Bu bağlamda, kişilik hakkı hak sahibine esas olarak savunma sağladığından, bu savunma hakkı da bir başkasına devredilemez. Diğer bir deyişle, bir kimse kişilik hakkına dayanarak bir başkasından hukuki işlem yapmasını isteyemez. Diğer yandan tüzel kişiliklerde ise kişilik hakları kuruluş ile birlikte herhangi bir işleme gerek duyulmaksızın kendiliğinden başlamaktadır.
- *Ölümle sona erer.* Kişilik haklarının ihlalinden doğan bazı maddi tazminat hakları belli şartlar altında (TMK md. 25) mirasçılara geçebilmekle birlikte, kişilik hakkı kişiliğin ortadan kalkması ile birlikte sona erer.
- *İcra takibine konu olmaz ve zaman aşımına uğramaz.* Bu haklar icra takibinin konusu olamaz, haczedilemez, iflas masasına girmez. Diğer yandan, kişilik hakkı zaman aşımına da uğramaz. Ancak, bu saldırıdan doğan tazminat hakkı zaman aşımına uğramaktadır[134].

İsviçre ve Türk hukuklarında kişilik hakkı türleri mutlak bir biçimde belirlenmesi kanun koruyucunun görevi olmayıp, her somut olay çerçevesinde mahkeme içtihatları ve hakimin takdirine göre şekillenmektedir. Bu doğrultuda her somut vakada hakim bir kez daha başta Anayasa olmak üzere hem özel hukuk kurallarını hem de kamu hukuku kurallarını inceleyerek iddiaya konu olan kişisel varlığın hukuk düzeni tarafından korunup korunmadığını tespit etmektedir[135]. Diğer yandan, kişisel verilerin korunması hakkı hem Kıta Avrupa'sı hem de Türk hukukunda kanun koyucu tarafından bir kişilik hakkı olarak görülmüş ve menfaat dengesi kişisel veri sahibi olan bireyler lehine kurulmuştur[136].

[134] Akgül, Kişisel Verilerin Korunması, s.44-46.
[135] Aksoy, s.42.
[136] Çekin, M. Serdar: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, Oniki Levha Yayıncılık, İstanbul 2018, s.13.

Mülkiyet hakkı görüşü

Kişisel verilerin hukuki niteliğine ilişkin "ekonomik yaklaşım" kapsamında sayılan ikinci görüş özellikle Amerikan hukukunda ağırlık kazanan "mülkiyet hakkı" görüşüdür. Bu görüşe göre kişisel veriler sadece kişiliğin bir uzantısı değil aynı zamanda kişiliğin ürünü niteliğindedir. Bu bakış açısından hareketle tüm bireyler kendi kişisel verilerinin sahibi olup, mülkiyetindeki bu verilerin hangi şartlar altında kullanılabileceğini kontrol edebilmelidir. Mülkiyet hakkı, sahibine en geniş yetkileri tanımakta olup, bu yetkiler kullanma, yararlanma ve tasarruf yetkileridir[137].

Bu görüşün Kıta Avrupa'daki yaklaşımdan en temel farkı, ABD'de bilgi toplumundan ziyade bilgi ekonomisi yaklaşımının benimsenmesi olup, merkezinde "ekonomik değer" kavramı yer almaktadır. Nitekim bugün kişisel verilerin ticarileştirilmesi ile ilgili en hızlı mesafe kat etmiş ülke ABD'dir. Özellikle yapay zeka ve benzeri teknolojilerinin kullanımıyla kişisel veriler en üst düzeyde ticari kazanç sağlamak için hayati öneme sahiptir ve sadece veriye erişen değil, veriyi paylaşan açısından da önemli ve aynı zamanda riskler içeren bir ticari hacim söz konusudur. Bugün veri sahipleri, üçüncü tarafların verilerine erişmesinde kaynaklı birçok olumsuz sonuçla karşı karşıya kalmaktadır ve veri pazarında kişisel veri sahiplerinin oynadıkları rol çok azdır[138].

Dolayısıyla, bu görüşe göre kendi verileri üzerinde mülkiyet hakkına sahip olan kişiler, bu bilgilerin hangilerinin hangi işletmelerle paylaşılacağına karar verebilecek ve bunun karşılığında elde edebileceği bedelle ilgili pazarlık yapabilecektir. Bununla birlikte, bu görüşün kabul edilmesi uygulama açısından da kolaylıklar sunacak, böylece kişisel verilerin korunması için ilave bir sistem kurulmasına gerek kalmayacaktır. Oysa ki, Kıta Avrupa'sında her ülke bünyesinde kurulması öngörülen denetleme mekanizmaları daha bürokratik ve daha yüksek maliyetli çözümlere işaret etmektedir. Bu görüşü savunanlar, kişisel verileri üzerinde mülkiyet hakkına sahip olan bireylerin bu verileri devretmesi tasarrufuna sahip olmasının aslında gerçek anlamda insan haklarını garanti alan bir mekanizma oluşturduğunu belirtmektedir. Onlara göre bu mekanizma, aynı zamanda veri güvenliği ile veriye erişim hakkı arasındaki dengeyi de doğru bir biçimde

[137] Aydın, s.15.
[138] Küzeci, s.63.

sağlayacaktır. Çünkü herkesin kendi verileri üzerinde hak ve bedel talebiyle birlikte veri satın almak ve bunları üçüncü kişilerle paylaşmak isteyen taraflar daha az veri toplama eğilimine gireceklerdir. Bu da veri kalitesini yükseltecek ve veri elde etmeye yönelik yatırımların karşılığının daha optimum şekilde alınabileceği bir çerçeveyi beraberinde getirecektir. Dolayısıyla pazar daha iyi işlerken, daha az hak ihlali gerçekleşecektir[139].

Bu görüşe karşı çıkanlar ise veri sahiplerine kişisel verileri üzerinde mülkiyet hakkı tanınmasının bireyin kişilik haklarının ihlaline neden olacağını öne sürmektedir. Çünkü, malike verilen tasarruf yetkisi sonucunda verileri satın alan taraflar, bu verileri istediği gibi üçüncü taraflarla paylaşabilecek ve veri sahibinin verilerinden soyutlanması sonucunu doğuracaktır[140] ve ister bir bedel karşılığı isterse karşılıksız olsun, kişisel verilerin mülkiyet hakkının bir ticari şirkete devrini birçok açıdan sakıncalı olacaktır. Her ne kadar, fikri savunanlar mülkiyet hakkının devri karşılığında "adil ve makul" bir bedel fikrini önerseler de, özellikle hassas verilerin devri ile oluşabilecek bireyin kendi hayatını özgürce yönlendirebilme hakkının ihlâli hiçbir "adil ve makul" ölçüte karşı daha az önemli olmayacaktır[141]. Bir başka görüşe göre ise, mülkiyet hakkı doğadaki sınırlı kaynakların dağılımını sağlamayı amaçlasa da, kişisel veriler söz konusu olduğunda bir "kıtlık" ihtimalinden bahsedilemez. Bu da mülkiyet hakkı görüşünün bu alana uyarlanamayacağını göstermektedir[142].

Fikri mülkiyet hakkı görüşü

Kişisel verilerin hukuki niteliğine ilişkin bir başka görüş ise, fikri mülkiyet hakkından hareketle oluşturulan yaklaşımdır. Bu görüş sahiplerine göre fikri mülkiyet hakkının tanınması ile kişisel verilerin korunması arasında "bilginin korunması ve dağıtımının denetlenmesi" bağlamında amaçsal benzerlik söz konusudur. Bu doğrultuda, fikri mülkiyet hukukundaki eser sahibinin manevi hakları aslında eser sahibinin kişi olma vasfından ileri gelen haklardır. Bu bağlamda manevi haklar eser sahibinin esere verdiği özelliklerin değiştirilmesinin önlenmesi, eserin kamuya tanıtılması ve hangi şartlar altında sunulacağı ile ilgili haklar olup tıpkı kişilik hakları gibi hak sahibine ekonomik

[139] Aksoy, s.59-60.
[140] Ayözger, s.15.
[141] Aydın, s.16.
[142] Küzeci, s.63.

yarar getiren sözleşme ve tasarruflara ve rehin, cebri icra veya hapis hakkına konu olmazlar ve eser sahibinin ölümü durumunda mirasçılara geçmezler[143].

Bu görüşe yönelik bazı eleştiriler söz konusudur. İlk olarak her iki kavramın amacı da verinin bilgi ekonomisine katılması olmasına rağmen iki kavramın aslında farklar içermesidir. Buna göre fikri mülkiyet hakkının konusu olan değerler eser sahibinin bilinçli çabasının sonucu iken, kişisel veriler kendi bireysel yaşamından kaynaklanır[144]. Diğer yandan fikri eserler bir amaca (sanat, bilim, endüstri vb.) hizmet ederken, kişisel veriler kendiliğinden böyle bir amaca hizmet etmemektedir. Bundan dolayı da kişisel verilerin dağılımı için mülkiyet hakkı tanınmasına gerek bulunmamaktadır. Son olarak fikri mülkiyet hakkının korunmaması durumunda doğabilecek zararlar öngörülebilirken, kişisel verilerin korunmaması durumunda oluşabilecek zararlar çok daha büyük çaplı ve öngörülemez boyuttadır[145]. Bununla birlikte, kişisel verilerin korunmasında önemli olanın kişisel veri sahibinin izni kadar, bu verilerin kimin tarafından hangi koşullarda işlendiği ve kullanım amacı olduğuna vurgu yapılmakta ve fikri mülkiyet hakkının kişisel verilerin korunmasına zemin sağlayamayacağı belirtilmektedir[146].

Kişisel verilerin kişilik hakkının bir parçası olduğunun kabul edilmesi, onu Medeni Kanun'un konusu kılmaktadır. Bu bağlamda, TMK'nın kişiliği koruyan hükümleri olan m.23, m.24 ve m.25 devreye girecektir. Ancak bu maddelerin amaçsal farkları tartışma konusu olmuştur. Bir görüşe göre TMK m.23 kişilik hakkını bizzat kişinin kendisine karşı koruyarak, bir iç korumayı düzenlemekteyken, bir başka görüşe göre ise bu madde kişilik hakkını kişinin kendi rızası ile dışarıdan yapılan saldırılara karşı korumaktadır[147].

Öte yandan, hem m.23 hem de m.24 kişiliği dıştan gelen saldırılara karşı korurken, m. 23 kişinin, dışarıdan yapılan saldırılara karşı (kişiler arası eşitsizlik, kendi düşüncesizliği, zayıf karakterli olması, hafifliği ve gözü karalığından vb. kaynaklı); m.24 ise yine dışarıdan ancak rıza dışı yapılan saldırılara karşı korumaktadır. Bununla birlikte m.25 ise kişilik hakkının rıza dışı ihlaline yönelik bir maddedir. Diğer yandan

[143] Aksoy, s.60-61.
[144] Aydın, s.17.
[145] Uncular, s.40-41.
[146] Küzeci, s.67-68.
[147] Aysun, s.80.

24'üncü maddeye göre kişisel verilerin kişilik hakkının bir parçası olması nedeniyle bunları ihlal eden kişilerin sorumluluğu söz konusudur. Bu sorumluluk durumu ise kişinin kişilik hakkından vazgeçtiğine dair bir beyanı ile ortadan kalkmaktadır. Ancak bu beyan kişinin bu haklardan vazgeçtiği durumda oluşabilecek sonuçları öngörebilmesine imkan tanıyacak şekilde bilinçli ve özgür iradesine dayanmalı ve ahlaka aykırı olmamalıdır. Benzer şekilde kamu yararı ya da ihlalin kanunun kişiye tanıdığı bir yetkiye dayanması durumlarından da ihlalden kaynaklı bir sorumluluktan söz etmek mümkün olmayacaktır[148]. Bir görüş ise, md. 24 ile getirilen korumanın kural olarak kişinin gizli ve özel hayatını korumaya yönelik olduğunu, bu alanların belirli kişilere açık olmasının, kamuya açık hale gelmesi sonucunu doğurmayacağını kabul etmektedir. Dolayısıyla, kişinin gizli ve özel hayatına yapılan her türlü hukuka aykırı girişim, kişilik hakkına saldırı mahiyetindedir[149].

TMK'nın 25'inci maddesi kişisel verilere bir saldırı sonucunda kişilik hakkı ihlal edilen kişilere yönelik bu saldırının sona erdirilmesini, sona erdirilse dahi etkileri sürüyorsa saldırının hukuka aykırılığının tespitini ve saldırı tehlikesinin önlenmesini talep ve daha hakkı tanımaktadır. Bu madde aynı zamanda, kişiye doğacak saldırılardan oluşan maddi ve manevi tazminat hakkı ile elde edilen kazancın vekaletsiz iş görme hükümleri uyarınca kendisine verilmesi hakkı da tanımaktadır[150]. Ancak, doktrinde bir görüşe göre, m.24 ve m.25'te yer verilen hükümlere dayanarak kişisel verilerin korunmasını talep etmek hem pratik hem de hukuk tekniği açısından makul bir çözüm yöntemi olarak kabul edilmemektedir[151].

Bir görüşe göre, KVKK'da hukuka uygunluk sebepleri özel olarak düzenlendiğinden TMK m.24 (2)'deki hükümde yer alan hukuka uygunluk sebeplerinin işlemenin hukuka uygunluğunun tayininde dikkate alınmayacağı belirtilmektedir. Bu bağlamda, KVKK md. 5 ve md.6'daki hükümlerin dikkate alınması gerekmektedir[152]. Nitekim TMK'nın kişisel verilerin korunmasını belirli bir oranda sağladığı ancak KVKK yürürlüğe girene

[148] Aksoy, s.80.
[149] Akgül, Kişisel Verilerin Korunması, s.56.
[150] Gürpınar, Damla: "Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk", D.E.Ü. Hukuk Fakültesi Dergisi, Özel Sayı, İzmir 2017, 689-690.
[151] Başalp, Kişisel Verilerin Korunması, s.293.
[152] Yücedağ, s.771.

kadar temel ilkeleri belirleyen bir yasanın eksikliğinin hissedilmesine engel olamadığı belirtilmektedir[153]. Bir diğer görüş ise medeni kanunun kendine özgü niteliğinden ötürü, genel hükümlerle kişisel verileri etkin şekilde korumanın her zaman mümkün olmadığını belirtmektedir[154].

2.1.2. İdare hukuku bağlamında hukuki niteliği

Kişisel verilerin korunması ile ilgili en önemli mercilerin başında idareler gelmektedir. İdareler; kamu hizmetinin vatandaşlara ulaştırılması, güvenliğin sağlanması, planlama vb. gerekçelerle bireylerin kişisel verilerine ihtiyaç duymaktadır. Kimlik, pasaport, ehliyet başvurusu, vergi beyanı, evlilik, nüfus sayımı gibi işlemler kapsamında beyan edilen kişisel veriler bunların en önemli örneği olup, idarenin bunları hukuka uygun olarak toplaması, işlemesi, kullanması ve aktarması konusunda bir ayrıcalığı bulunmamaktadır. İdare hukuku bağlamında, yetkili kamu idareleri, bireyin özel yaşamı hakkındaki bilgiyi sadece yasal nedenler ve toplumun menfaati nedeniyle talep edebilmektedir. Ancak, bunu talep ederken, kamu menfaati ile diğer bireylerin hakları arasında bir denge kurma görevine sahiptir[155]. Bu bağlamda, kişisel verilerin toplanması ve tutulmasının yasal bir dayanağı olması, hukuki düzenlemelerde öngörülen gerekliliklere uygun olması ve verilerin işlenmesi ile hedeflenen amacın dengeli olmasına atıfta bulunulurken, idarenin rolüne dikkat çekilmektedir[156].

Buna göre, kişisel verilerin idare tarafından hukuka aykırı olarak işlenmesi, bu işleme faaliyetinin ise, birey aleyhine maddi veya manevi zarar oluşturması ve idarenin işlem veya eylemleriyle bireyin zararı arasında illiyet bağı bulunması durumunda idarenin hukuki sorumluluğu kapsamında tazmin yükümlülüğü söz konusu olacaktır. Bu aynı zamanda "idarenin hukuka bağlı olması" ve "hukuk devleti" ilkelerinin de bir gereğidir[157].

[153] Küzeci, s.382.
[154] Ayözger, s.98.
[155] Akgül, Kişisel Verilerin Korunması, s.263.
[156] Küzeci, s.199.
[157] Akgül, Kişisel Verilerin Korunması, s.264.

Tazminat cezası dışında, idare hukuku açısından KVKK'da öne çıkan bir diğer husus ise idari yaptırımdır. KVKK'nın 18'inci maddesinde yer alan bazı yükümlülüklerin gerçek kişi ya da özel hukuk tüzel kişisi olan veri sorumlusu tarafından yerine getirilmemesi durumunda idari yaptırım; kamu kurum ve kuruluşları ile bu nitelikteki meslek kuruluşları bünyesinde böyle bir ihlal işlenmesi halinde ise disiplin sorumluluğu gündeme gelmektedir. Bu bağlamda, veri sorumlusu aydınlatma, veri güvenliği, kurul tarafından verilen kararları yerine getirmeme ve veri sorumluları siciline kayıt ve bildirim yükümlülüklerini yerine getirmediği takdirde 5,000 ila 1,000,000 Türk Lirası arasında değişen cezalarla karşılaşmaktadır[158].

Ancak, idarenin hukuka bağlı olduğu bir hukuk devleti olmakla birlikte uzun süredir AB üyeliği için girişimlerini sürdüren Türkiye'de 108 sayılı sözleşmenin imzalanmasını müteakiben geçen kırk yıla yakın süreçte mesafe kat edilmemiş olduğu yönünde çok sayıda eleştiri bulunmaktadır. 2016 yılında yürürlüğe giren KVKK ile birlikte kişisel verilerin korunmasına dair bireylere temel bir koruma düzeyi getirildiği görülse de, idareye tanınan istisnai çerçevenin kapsamının çok geniş tutulması nedeniyle aslında AB standartları ile uyumlu olmadığı belirtilmekte ve bu durum AB güvenlik teşkilatlarından Europol ve Eurojust ile operasyonel işbirliği yapılmasına engel olmaktadır[159].

Bu bağlamda, AB Komisyonu'nun (ABK) 2016 tarihli Türkiye raporunda şu ifadelere yer verilmektedir; *"..Bu konuya ilişkin hiçbir mevzuatın bulunmadığı önceki durumla kıyaslandığında bu kanun, bir ilerleme olduğuna işaret etmektedir. Ancak, bu kanun, özellikle kişisel verilerin kullanılmasını denetlemekten sorumlu makamın oluşumu ve işleyişine ilişkin hükümlerin bu kurumun tamamen bağımsız hareket etmesine yönelik güvenceler sağlamaması ve infaz mercileri ile yargı makamlarının faaliyetlerini, kişisel verilerinin korunması kurallarına riayet edilmesi yükümlülüğü çerçevesinde kapsama tam olarak dahil edilmemesi nedeniyle hâli hazırdaki AB müktesebatı ile uyumlu değildir. Kişisel Verileri Koruma Kurumunun bağımsız bir şekilde hareket edebilmesini*

[158] Aysun, s.104.
[159] Küzeci, s.313.

ve infaz mercilerinin faaliyetlerinin kanun kapsamına alınmasını sağlamak için Türkiye, kişisel verilerin korunması mevzuatını AB müktesebatı ile uyumlu hale getirmelidir" [160].

ABK'nin ilgili kanunu, AB müktesebatına uygun bulmamasına neden olan faktörlerden biri; KVKK hazırlanırken örnek alınan Direktif'tekine nazaran çok daha geniş bir istisnalar listesi düzenlenmesi ve böylece Kanun'un uygulama alanının daraltılmasıdır. KÜZECİ'ye göre bu istisnalar son derece belirsiz, geniş kapsamlı, soyut ve ucu açık kavramlarla dolu olup, bu durum kişisel verilerin korunmasına dair keyfi uygulamalara ve hak ihlallerine kapı aralamaktadır[161].

Özellikle, KVKK 28'inci maddenin a, c ve ç bentleri, bu ihlallere en çok kapı aralayabilecek maddelerdir. Örneğin;
"a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi" maddesinde görüldüğü üzere yukarıdaki madde Direktif'in m.2/2 (c)'sine tekabül etmekte ancak ona göre çok daha kısıtlı bir kapsam sunmaktadır. Buna göre Tüzük'te "tamamen kişisel veya ev içi faaliyet esnasında bir gerçek kişi tarafından gerçekleştirilen" işlemler kapsam dışındayken, KVKK'da "tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili işleme faaliyetleri" kapsam dışı tutulmuş ve kişinin kendisiyle veya TMK'ya göre aile ferdi konumundaki kişilerle ilgili olmayan tüm işleme faaliyetleri KVKK kapsamında alınmıştır. KVKK'nın gerekçesinde, bu konuyla ilgili herhangi bir açıklama bulunmamaktadır. Dolayısıyla, bu durum kişinin kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili olmayan veriler içeren örnekler ya da aile ferdi olmayan ama ev arkadaşı ya da sevgili gibi birlikte yaşayanların çevrimiçi etkinlikleri açısından yaşanabilecek sorunları beraberinde getirmektedir. Bu nedenle, "üçünü kişilere verilmemek" şartı ile, ticari çıkar içeren

[160] Avrupa Komisyonu'nun 09.11.2016 tarihli, SWD (2016), 366 nihai sayılı AB Genişleme Politikasına İlişkin 2016 Türkiye Raporu, https://www.ab.gov.tr/files/ceb/Progress_Reports/2016_ilerleme_raporu_tr.pdf, (Erişim Tarihi): 29.03.2018.
[161] Küzeci, s.331-340.

belirsizlikler de göz önünde bulundurulduğunda, KVKK'nın bu maddesinin, Direktif'in m.2/2 (c) doğrultusundan yorumlanmasının daha uygun olacağı belirtilmektedir[162].

Diğer yandan, (c) ve (ç) maddelerine ilişkin tartışmalar ise şu şekildedir;
c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi. İlgili maddeye göre veri işlemenin hangi durumlarda suç içereceği farklı yorumlara açık olup, her somut durum beraberinde kişisel verilerin korunması hakkı ile ilgili menfaat arasında adil bir denge sağlanması gerekliliği söz konusudur. Diğer yandan, (ç) maddesinde; "*Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi"* ifadelerinde görüldüğü üzere, kapsam bu şekilde soyut, belirsiz ve geniş tutulduğunda keyfi uygulamalara hatta fişlemeye kapı aralama tehlikesi söz konusudur. Bununla birlikte, bu bentte istisna ya da yetki sınırının olmaması, yetki aşımı ve kötüye kullanımlara karşı etkin koruma yollarının belirlenmemesi ve bireyin devlet otoritesi karşısında korumasız bırakması nedeniyle verilerin korunması hakkı ile ilgili menfaatler arasındaki denge, kişisel verilerin korunması hakkının aleyhine yorumlanabilecektir. Bu nedenle her somut olayda, insan hakları, veri koruma hukukunun temel ilkeleri, hakkaniyet esas alınarak dar yorumlanması ve titizlikle değerlendirilmesi tavsiye edilmektedir[163].

2.1.3. Ceza hukuku bağlamında hukuki niteliği

Kişisel verilerin kaydedilmesi, ele geçirilmesi, üçüncü şahıslarla paylaşılması ve yok edilmemesi gibi eylemler suç olarak kabul edilmekte olup, ceza hukuku açısından çeşitli sonuçları bulunmaktadır. Dünyada kişisel verilerin korunmasına ilişkin suçlara yönelik düzenlemelere dair iki yaklaşım söz konusu olup, İtalya ve Almanya gibi ülkelerde bu suçlar konuya ilişkin özel düzenlemeler kapsamında yer almaktadır. Ancak, Fransa gibi ülkelerde ise ceza kanunları kapsamında düzenlemeler söz konusudur. Nitekim

[162] Uncular, s.100.
[163] Uncular, s.100-101.

Türkiye'de Fransa'da benimsenen yöntem izlenmiş olup, ceza hukuku açısından başta TCK ve 5271 sayılı Ceza Muhakemesi Kanunu (CMK) kapsamında kişisel verilerin korunmasına ilişkin ihlallere yönelik birçok düzenleme söz konusudur[164]. TCK'da md.135, md.136 ve md.138 kişisel verilerin hukuka aykırı olarak kaydedilmesini, verilmesini, yayılmasını, ele geçirilmesini ve yok edilmemesini suç olarak düzenlemektedir[165]. Bu düzenlemeler ile, *"toplumsal düzenin devamı için bir ceza normuyla korunması gereken soyut, manevi ve ideal değerlerden olan özel hayatın gizliliği ve kişisel verilerin korunması"* sağlanmaktadır[166]. Ancak doktrinde ifade edilen bir görüşe göre, bu maddelerin verilerin işlenmesi kapsamında ele alınan fiilleri tam olarak kapsamadığı işaret edilmektedir[167].

Bu bağlamda, TCK'nın 135'inci maddesi bireylerin kişisel verilerinin amaca aykırı bir biçimde kullanılması ve kaydedilmesinin önlenmesi amacıyla düzenlenmiş olup, kişisel verilerin hukuka aykırı olarak kaydedilmesinin fiili suç olduğuna hükmetmektedir. Buna göre hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilirken, "hassas kişisel verilerin" kaydedilmesi durumunda verilecek ceza yarı oranında artırılmaktadır. Maddenin gerekçesinde bu suçun düzenlenmesine neden olan fiillerin bazı kurum ve kuruluşların kişilerle ilgili kayıtları bilgisayar ortamına geçirerek saklamaları olduğu belirtilmiş olup, örnek olarak hastaneler, sigorta şirketleri, bankalar ve kredi kartı ile alışveriş yapılan mağazalarda tutulan ve amaç dışı kullanılarak üçüncü şahıslara aktarılan veriler verilmiştir[168].

Diğer yandan, TCK'nın 136'ıncı maddesinde kişisel verilerin başkasına verilmesi ve yayılması yani korunmasına yönelik ihlaller suç olarak düzenlenmiştir. İlgili maddede suç tipi; kişisel verilerin verilmesi, yayılması ve ele geçirilmesi seçimlik hareketli suçlar olarak tarif edilmektedir ve bu hareketlerin gerçekleştirilmesi ile suçun tamamlandığı kabul edilmektedir. Bir diğer deyişle suç, soyut tehlike suçu olarak tanımlanmaktadır[169].

[164] Küzeci, s.401.
[165] Sarıusta, s.111.
[166] Sert, s.76.
[167] Akdağ, s.35.
[168] Sert, s.75-76.
[169] Dülger, Ceza Normu, s.132.

Ancak, bu iki maddeye dayanarak açılan davaların sayısının artmasının asıl nedeni 2016 yılında yürürlüğe giren 6698 sayılı KVKK'dır. Çünkü o tarihe kadar 5237 sayılı Kanun'un kişisel verileri korumaya ilişkin temel ilke ve kavramlarını düzenleyen ulusal bir mevzuat ya da iç hukuka dahil edilmiş uluslararası bir sözleşme bulunmamaktadır. Ancak KVKK henüz tasarı aşamasındayken bile kamuoyuna yansıyan tartışmalar ve ilgili suç tiplerinin ihlaline ilişkin davaların sayısında ciddi bir artış gözlemlenmiştir. Teknolojik gelişmelerin hızına paralel olarak bu maddeye dayanan davaların bundan sonra da hızla artması öngörülmektedir[170].

TCK'da kişisel verilerin korunmasının ihlali suçunu tanımlayan fiil olan "kişisel verilerin başkasına verilmesi" ile referans verilen başkası "gerçek ya da tüzel kişi" olabilmektedir. Vermek eylemi ise, elden ya da elektronik mecralar yoluyla gerçekleştirilebilmektedir. Bununla birlikte, Yüksek Mahkeme kararına göre, kişisel veri gerektiğinde hukuka uygun olarak o veriyi gereksinen makama verilebilmektedir. Yaymak eylemi ise, birçok kimseye duyurmak olarak ifade edilmektedir ve e-posta, telefon, yazılı ve görsel medya mecralarında gerçekleştirilebilmektedir. Gerek verme gerekse yayma eylemleri, yaygın görüşe göre iki ayrı suç değil, tek bir suçtur. Ancak, yayma eyleminin gerçekleşebilmesi için kulaktan kulağa değil, bir araçla hayata geçirilmiş olmasına referans verilmektedir[171].

Vermek ve yaymaktan sonra üçüncü önemli fiil olan "aktarmaya" yönelik düzenlemeler ise KVKK'nın 8 ve 9'uncu maddelerinde kendisine yer bulmaktadır. Veri kişisinin "açık rızasının bulunmadığı" durumlarda ya da verinin aktarılacağı yabancı ülkede koruyucu mevzuat ve kurumlar yoksa bu suçlar TCK 136'ıncı maddede düzenlenen "kişisel verileri hukuka aykırı olarak verme ve yayma suçu" kapsamına girmekte olup cezalandırılacaktır. Bu bağlamda, bir diğer kavram ise "ele geçirmedir". Buna göre fail olağan koşullarda ele geçirmesine imkan olmayan kişisel verileri seçimlik hareket olarak elde etmektedir. Bu durum kişisel verilerin korunması ile ilgili bir ihlal ve ihmali gündeme getirmektedir[172].

[170] Sarıusta, s.113.
[171] Aysun, s.108.
[172] Uncular, s.94..

Son önemli suç ise, kişisel verilerin belirlenen süreler içerisinde "yok edilmemesi" olup, TCK 138'inci madde bu suça yönelik bir düzenlemedir. Bu düzenlemeye göre; *"kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir".* Burada ihlal edilen yok etme eylemi, verinin tümü ile erişilemez, tekrar kullanılamaz, veri kişisi ile bağlantısı kopartılmış ve veriden hareketle veri kişisinin belirlenmesinin imkansızlaştırılmış olmasını gerektirmektedir. Ancak, öngörülen süre içerisinde kişisel veriler yok edilmediğinde suç tamamlanmakta ve herhangi bir zarar doğması şart olmadığından bu da bir soyut tehlike suçu olmaktadır[173].

Bu bağlamda, bazı hukukçular "hükümde cezalandırma için fıkra ayrımı yapılmaksızın 138'inci maddenin uygulanacağının ifade edilmesi ve suçun nitelikli halinin de cezalandırmaya ilişkin bir hüküm olması nedeniyle teorik olarak KVKK'nın 17. maddesinin 2'inci fıkrasında yer alan suç açısından 138'inci maddenin 2'inci fıkrasının uygulanabileceğini" düşünmekteyken, DÜLGER, uygulamada soruşturma makamı olan savcılık ve onun yardımcısı olan kolluk güçleri ile kovuşturma makamı olan mahkemeler ve hakimlikler kişisel veri kaydetme vb. işlemleri özellikle CMK ve diğer yasalardan aldıkları yetki doğrultusunda gerçekleştirmesi nedeniyle TCK'nın 138/2. maddesinde belirtilen kişisel verilerin 6698 sayılı Yasanın istisnasını oluşturduğunu belirtmekte olup, hukuka uygun olarak soruşturma veya kovuşturma için kişisel veri kaydeden ya da işleyen makamların bunların yok edilmesi için öngörülen süre geçmesine rağmen bunu yapmamaları halinde 6698 sayılı Yasanın 17. maddesinin 2. fıkrasından hareketle TCK'nın 138'inci maddesinin 1'inci fıkrasını ihlal ettiğinden bunun nitelikli hali olan 138'inci maddenin 2'inci fıkrasının doğrudan uygulanması gerektiğini belirtmektedir[174].

Buna ilaveten, CMK'nın 135'inci maddesine göre ise yapılan iletişimin tespiti ile dinlenmesi sürecinde kayda alınan bilgiler kişisel veriler nitelikte olup, şüpheli hakkında kovuşturmaya yer olmadığında dair karar verilmesi ya da 135/1'e göre gerekli

[173] Sert, s.127.
[174] Dülger, Ceza Normu, s.139.

olan hakim onayının alınmaması halinde yapılan tespit ve dinleme kayıtlarının yok edilmesi zorunludur[175].

2.1.4. Borçlar hukuku bağlamında hukuki niteliği

Kişisel verilerin korunmasını düzenleyen bir diğer hukuki alan ise Borçlar Hukuku olup, KVKK'nın 11'inci maddesinde belirtilen işçinin tazminat talep etme hakkından söz edilmiş ve bu hükmün kişilik haklarının korunması açısından TMK'nın başta 25'inci madde olmak üzere ilgili hükümlerine atıfta bulunduğu belirtilmiştir. Bu yorum kabul edildiğinde, tazminat hususunda genel hüküm niteliğindeki TBK hükümleri uygulama alanı bulmaktadır[176]. Bu bağlamda TBK'nın 58'inci maddesinde kişisel verilerinin hukuka aykırı şekilde işlenmesiyle kişilik hakkı ihlal edilen işçinin manevi tazminat talebinde bulunması mümkün olup, *"Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilmektedir"*.

TBK 471'inci maddesi ise "*kanuna ve sözleşmeye aykırı davranışı nedeniyle işçinin ölümü, vücut bütünlüğünün zedelenmesi veya kişilik haklarının ihlaline bağlı zararların tazmini, sözleşmeye aykırılıktan doğan sorumluluk hükümlerine tabidir"* ifadeleriyle, işverenin hizmet sözleşmesinden kaynaklanan kişilik hakları ihlâlinden doğan zararın tazmininin sözleşmeye aykırılıktan doğan sorumluluk hükümlerine tabi olduğu hüküm altına alınmıştır[177]. Diğer yandan, işverenin talimatı ile bir işçiye yönelik bir başka işçi tarafından kişisel veri ihlâli gerçekleştiğinde, işverene dönük olarak TBK'nın 116'ıncı maddesinde yer verilen ifa yardımcısının eyleminden doğan sorumluluk hükümlerine göre sorumluluk yüklenmesi mümkün olacaktır[178].

[175] Aysun, s.115.
[176] Belge, A. Merve: "Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlâli ve Korunması Yolları", D.E.Ü. Hukuk Fakültesi Dergisi, Özel Sayı, İzmir 2017, 1045-1046.
[177] Belge, s.1046.
[178] Uncular, s.111.

2.2. Kişisel Verilerin Korunmasının Hukuki Dayanakları

Kişisel verilerin korunmasının hukuki dayanağı gerek uluslararası gerekse de ulusal düzenlemelerle hayata geçirilmiş olup, bu başlık altında bu düzenlemelere yer verilecektir.

2.2.1. Uluslararası düzenlemeler

Kişisel veriler birçok uluslararası düzenleme ile koruma altına alınmış olup, bu düzenlemeler ve ilgili kavrama dair çizdikleri çerçeveye aşağıda yer verilecektir.

Ekonomik İşbirliği ve Kalkınma Örgütü (OECD)

Kişisel verilerin korunmasına dair girişimde bulunan ilk uluslararası örgüt OECD'dir. Bu bağlamda, kurum tarafından 23 Eylül 1980 tarihinde yayınlanan *"Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Yönlendirici İlkeler"* başlıklı metin bir ilk niteliğindedir[179]. Bu metnin OECD üyesi ülkeler açısından bir bağlayıcılığı olmasa da, ulusal düzeydeki kişisel verilerin korunmasına ilişkin yasaların uyumlaştırılmasına yöneliktir. OECD üyesi olan ülkelerde serbest piyasa ekonomisini geliştirmeyi amaçladığından bu metindeki perspektif, normalde çatışan eğilimler olan veri korunması ile serbest dolaşımı arasında bir denge kurmak iken, ana amaç ise insan haklarının, serbest piyasa ekonomisinin ve çoğulcu demokrasinin sağlıklı işleyişinin sağlanmasıdır[180].

OECD tarafından yayınlanan ve sekiz maddeden oluşan "Rehber İlkeler" sadece OECD üyesi ülkeler için tavsiye niteliğinde olmayıp, bütün ülkeler tarafından takip edilebilir niteliktedir. Bu doğrultuda OECD üye ülkelerde kişisel verilerin korunması ve bireysel özgürlüklerle ilgili hukuki düzenlemelerin bu ilkeler gözetilerek yapılmasını tavsiye ederken, beraberinde sınır aşırı veri trafiğinin haksız yere engellenmemesini, mevcut engellerin kaldırılmasını ve bu ilkelerin hayata geçirilmesinde işbirliğini öne çıkartmaktadır[181].

[179] Dülger, Kişisel Verilerin Korunması, s.50.
[180] Develioğlu, H. Murat: Avrupa Birliği Genel Veri Tüzüğü, Oniki Levha Yayıncılık, İstanbul 2017, s.6.
[181] Aydın, s.28-29; Akgül, Kişisel Verilerin Korunması, s.113.

Bu bağlamda, OECD ilkelerinin ülkelere iç hukuklarındaki düzenlemelere yönelik getirdiği yükümlülükler; üye devletlerin uygun iç hukuk düzenlemelerini yapmak, vatandaşların haklarını kullanacakları uygun araçları sağlamak, ilkelere uyulmadığı zaman başvurulabilecek hukuki yöntemleri ve yaptırımları öngörmek ve ilgili kişilerin haksız şekilde ayrımcılığa tabi olmasını engellemek olarak sıralanmaktadır[182].

Rehber İlkeler'de öne çıkan asgari veri koruma ilkeleri şu şekilde sıralanmaktadır;

- *Veri Toplamanın Sınırlı Olması:* Bu ilke kişisel verilerin toplanmasını hukuka uygunluk, dürüst araçlar,veri öznesinin rızası veya bilgisi ile sınırlandırmaktadır.
- *Veri Kalitesi:* Buna göre kişisel veriler amacına uygun ve bu amaca yönelik gerekli ölçüde, eksiksiz ve güncel olmalıdır.
- *Amacın Belirli Olması:* Kişisel verilerin toplanma amacı verilerin toplanma anında belirlenmiş olmalı ve bu amaç dışında kullanılmamalıdır.
- *Kullanmanın Sınırlı Olması:* Kişisel veriler veri öznesinin rızası veya kanun tarafından öngörülen durumlar hariç olmak üzere açıklanamaz.
- *Veri Güvenliği:* Kişisel veriler kaybolma, yetkisi olmayanlar tarafından erişim, tahrip edilme, kullanılma, değiştirilme ya da ifşa edilme gibi risklere karşı uygun güvenlik önlemleri aracılığıyla güvenlik altına alınmalıdır.
- *Açıklık:* Kişisel verilere ilişkin işlem ve önlemler "açıklık politikası" çerçevesinde hayata geçirilmelidir.
- *Bireyin Katılımı:* Bireyler katılım hakkı çerçevesinde esas veri sorumlusu ya da başka bir usulle verilerin üzerinde değiştirme, silme, eksiklikleri tamamlama ya da onay hakkına sahiptir. Bu talebi gerçekleşmiyorsa, bunu nedeni kendisine bildirilmelidir. Birey tüm bu durumlarda hukuki yollara başvurabilme hakkına sahip olmalıdır.
- *Hesap Verilebilirlik:* Veri sorumlusu tüm bu ilkelerin hayata geçirilmesi ve gerekli önlemlere uyulması için hesap verebilir durumda olmalıdır[183].

[182] Küzeci, s.119.
[183] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, (Erişim Tarihi): 26.04.2019.

OECD tarafından ilgili metin 2013 yılında revize edilerek yeniden yayınlanmıştır[184]. Bugün 34 OECD üyesi ülkeden 33'ü kişisel verileri koruma yasasına sahip olup, son olarak Türkiye'de KVKK'nın yürürlüğe girmesi sonucu bu konuda yasaya sahip olmayan tek ülke ABD olarak kalmıştır[185]. Bu metnin OECD üyesi ülkeler açısından bir bağlayıcılığı olmasa da, en önemli özelliği uluslararası düzeyde ilgili ilkeler konusunda uzlaşmaya varılabileceğini göstermesidir[186].

OECD tarafından hazırlanan diğer metinler ise, 1985 yılında yayınlanan "Sınırötesi Veri Transferi Hakkında Bildirge" ve 1998 tarihli "Global Ağ Gizliliğinin Korunması Hakkında Bakanlık Bildirgesi" olarak sıralanmaktadır[187].

Birleşmiş Milletler (BM)

Kişisel verilerin korunmasına ilişkin düzenleme geliştiren bir diğer uluslararası organizasyon ise BM'dir. BM'nin ana ilgi alanı iletişim teknolojileri ile insan hakları ilişkisi olup, bu doğrultuda BM Genel Kurulu 14 Aralık 1990 tarihinde *"Bilgisayarlarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler"* başlıklı bir metni kabul etmiştir. Bu karar ile hedeflenen husus, üye devletlerin asgari kişisel veri koruma standartları üzerinde uzlaşmasıdır[188]. Metnin en önemli ve ayırıcı özelliği, "kişisel verilerin korunması için yetkili ve bağımsız organların kurulmasını öngören ilk uluslararası hukuk belgesi" olmasıdır[189].

BM tarafından yayınlanan ve hem kamu hem de özel sektöre yönelik düzenlemeler içeren bu metin de tıpkı OECD Rehber İlkeleri'nde olduğu gibi tavsiye niteliğindedir ve üye devletler açısından hukuki bağlayıcılığı söz konusu değildir[190]. Bu bağlamda BM Rehber İlkeleri; OECD İlkeleri ve 108 sayılı AK Sözleşmesi'nin hukuki alanda önemli bir mesafe kat etmesiyle, sınırlı bir etkiye sahip olabilmiştir[191].

---

[184] Develioğlu, s.6.
[185] Aysun, s.42.
[186] Kılınç, Doğan: "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", Ankara Üniversitesi Hukuk Fakültesi Dergisi 61 (3), Ankara 2012, s.1111; Küzeci, s.120.
[187] Kılınç, s.1111.
[188] Başalp, Kişisel Verilerin Korunması, s.24-25.
[189] Aydın, s.29.
[190] Aysun, s.43.
[191] Develioğlu, s.10.

BM tarafından belirlenmiş olan ilkeler şu şekilde sıralanmaktadır;

- *Yasallık ve dürüstlük:* Kişisel veriler kanunun öngördüğünün dışında ve dürüst olmayan yöntemlerle toplanmamalı ve toplanma amacı ile temel hak ve özgürlüklerle ilgili ilkelere aykırı olarak kullanılmamalıdır.
- *Doğruluk:* Toplanan verilerin doğru, eksiksiz ve güncel olarak saklandığı kontrol edilmelidir.
- *Amacın belirli ve haklı olması:* Kişisel verilerin toplanma amacı haklı ve kesin olarak belirlenmeli ve ilgililere açıkça bildirilmelidir.
- *İlgili kişilerin erişim hakkı:* İlgili kişi kimliğini kanıtladığı takdirde kendisi hakkında toplanan bilgilerin nasıl bir işleme tabi tutulduğunu öğrenebilmeli ve bunların anlaşılır bir örneğini aşırı bir maliyetle karşılaşmadan ve zaman kaybı yaşamaksızın elde edebilmelidir.
- *Ayrımcılıktan kaçınma:* İlgili kişinin etnik kökeni, ırkı, dini, ideolojisi, felsefi inançları ve cinsel kimliği gibi duyarlı konulardaki bilgiler ancak yasanın izin verdiği haklı ve gerekli durumlarda toplanmalıdır.
- *İstisna koyma:* Kişisel veriler söz konusu olduğundan görevli mercilere milli güvenlik, kamu düzeni, halk sağlığı, genel ahlakın korunması ve diğer kişilerin hak ve özgürlüklerine zarar vermemek amacıyla yasallık, dürüstlük, doğruluk, amacın belli ve haklı olması durumunda kişisel verilere erişim yetkisi tanınabilmektedir. Ayrımcılıktan kaçınma ilkesine getirilecek istisnasının temel hak ve özgürlüklere aykırı olmaması gerekmektedir.
- *Güvenlik:* Kişisel verilerin toplanması, işlenmesi ve korunması ile ilgili tüm kurumlar bu verilerin kaza, doğal afet, insan hatası, kusur ve suç tehlikelerine karşın korunmasına yönelik her türlü önlemi almakla yükümlüdür.
- *Denetim ve yaptırım:* Kişisel verilerin korunmasına yönelik öngörülen ilke ve kuralların hayata geçirilmesi, önlem alınması ve gerekli denetimlerin yapılması ile ilgili sorumluluk tarafsız, yetkin ve adil bir makam tarafından yürütülmelidir.
- *Sınır ötesi veri transferi:* Kişisel verilerin saklandığı ülkeden bir diğer ülkeye aktarılması için iki ülkenin de mevzuatlarının buna uyumlu olması gerekirken,

alıcı ülkenin sağladığı korumanın gönderici ülkedeki korumadan daha aşağı seviyede olmaması gerekmektedir[192].

Avrupa Konseyi (AK)

II. Dünya Savaşı'nın getirdiği yıkım sonrası Avrupa'da barışın sağlanması, demokratik rejimlerin yeniden tesisi, insan hakları ve hukuk devletinin ilkelerinin sürekliliği amacıyla 1949 yılında kurulmuş uluslararası bir örgüt olan AK, bugüne kadar kişisel verilerin korunmasına dair birçok düzenlemenin altına imza atmıştır[193]. 1973 tarihli *"Özel Sektörde Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar"* ve 1974 tarihinde yürürlüğe giren *"Kamu Sektöründe Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar"* bunların en erken tarihlileri olup, bu kararlarla elektronik veri bankalarında tutulan kişisel bilgilerin korunmasına yönelik asgari standartlar ortaya koyulmuştur. Bu kararlar aynı zamanda 1981 tarihinde kabul edilen 108 sayılı Sözleşme'nin hazırlayıcısı niteliğindedir[194]. Bu bağlamda, kurum tarafından gerçekleştirilen diğer önemli düzenlemelere aşağıda sırayla yer verilecektir.

Avrupa İnsan Hakları Sözleşmesi (AİHS)

AK kuruluş ilkeleri doğrultusunda 4 Kasım 1950 tarihinde AİHS'yi kabul etmiş olup, bu metin insan haklarının ve özgürlüklerinin korunması bakımından en temel uluslararası hukuk düzenlemelerinin başına gelmektedir[195]. AİHS'nin esası; bireyin özel hakları ile kamu menfaati veya diğer bireylerin hakları arasında bir denge görevi görmesidir[196].

Sözleşmenin 8. maddesi;
"1. Herkes özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

[192] Aydın, s.30-31; Dülger, Kişisel Verilerin Korunması, s.53; Kılınç, s.1111-1112; Akgül, Kişisel Verilerin Korunması, s.116-117; Develioğlu, s.10.
[193] Aysun, s.45.
[194] Atak, Songül: "Avrupa Konseyi'nin Kişisel Verileri Açısından Sağladığı Temel Güvenceler", TBB Dergisi 87, Ankara 2010, s.100.
[195] Küzeci, s.135.
[196] Akgül, Kişisel Verilerin Korunması, s.120.

2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için demokratik bir toplumda gerekli olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir" [197] içerdiği ifadeleri ile bireyin özel yaşamı, aile yaşamı ve evi ve haberleşmesinin temel bir insan hakkı olduğu ve bu nedenle kişisel verilerin korunmasının 8. madde kapsamında değerlendirileceğine referans verirken[198], ŞİMŞEK'e göre bu verilerin hukuka aykırı olarak toplanması, kaydedilmesi, tekrar kullanılması ve devredilmesine karşın bireyin korunması hakkının *"özel yaşama saygı gösterilmesi hakkının"* özel olarak şekillendirilmiş kısmi bir alanını oluşturmaktadır[199].

Burada yer alan "saygı gösterilmesi" ifadesi, devletin sadece müdahalede bulunmamasını değil, aynı zamanda bu hakların fiilen ve gerçekten kullanılmasına imkan tanıyacak önlemleri alma konusunda pozitif bir yükümlülüğü olduğunu belirtmektedir. Bu bağlamda, devletin negatif yükümlülüğü özel yaşamın korunmasına yönelik eylemlerden sakınması yani kişisel verileri Sözleşme'ye aykırı şekilde toplamasını, saklamasını ve işlemesini engellerken, pozitif yükümlülüğü ise, özel yaşam hakkına saygıyı güvence altına almak için gerekli önlemleri almasına işaret eder[200].

Avrupa İnsan Hakları Mahkemesi (AİHM) Kararları

AİHS'de kişisel verilerin korunmasına dair açıkça ve ayrıca bir düzenleme yer almamış olsa da, 8'inci maddeye dayandırılarak oluşturulan AİHM içtihatları ile bu kavram sözleşme kapsamında yorumlanmaktadır. Buna göre AİHM önüne gelen davalarda ilk olarak fiilin 8'inci maddede yer alan özel yaşam hakkına yönelik bir müdahale oluşturup oluşturmadığını değerlendirmekte, bir müdahale olduğuna kanaat getirdiği takdirde, bu müdahalenin ulusal yasalara uygunluğunu incelemektedir[201]. Ancak, müdahalenin ulusal yasalara uygunluğunu yeterli bulmamakta ve hem AİHS, hem de 108 sayılı

[197] Avrupa İnsan Hakları Sözleşmesi, http://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf, (Erişim Tarihi): 01.04.2019.
[198] Küzeci, s.136.
[199] Şimşek, s.31.
[200] Atak, s.102.
[201] Akgül, Kişisel Verilerin Korunması, s.123.

Sözleşme'ye uygun olup olmadığını değerlendirmektedir[202]. Bu bağlamda AİHM, kişisel verilerin kullanımı ve kayıt altına alınması hususunda bireylerin denetim hakkını kabul etmektedir[203].

Bu konuda ele alınacak ilk dava örneği, 6 Eylül 1987 tarihinden verilen Klass ve Diğerleri v. Almanya kararıdır[204]. İstihbarat örgütlerinin milli güvenlik ihtiyacı nedeniyle bireyleri gizli izlemeye (telgraf ve mektupların okunması, telefon görüşmelerinin dinlenmesi ve kaydedilmesi) tabi tutmasının söz konusu edildiği davada, Mahkeme, bu izlemenin birey haklarına müdahalesinin etkin bir denetime tabi tutulması gerektiğini belirtmiş ve Avrupa ülkelerinin her durumda milli güvenlik ihtiyacına başvurup uygun gördükleri her tedbiri alamayacaklarına hükmetmiştir[205]. Buna göre AİHM, bireylerin özel yaşamı kapsamındaki bilgilere yönelik kamusal müdahaleleri bireyin koruyucu uygun ve etkili yasal düzenlemeler bulunmadığı sürece 8'inci maddenin ihlâli olarak kabul etmektedir[206].

Leander'in İsveç aleyhinde başvurusuna dair AİHM'nin 26 Mart 1987 tarihli kararı bir başka önemli örnektir[207]. Buna göre başvurucu, kendisine dair güvenlik soruşturması sonucunda askeri güvenlik bölgesinde yer alan denizcilik müzesindeki görevinden atılmış olup, soruşturmaya konu olan bilgileri talep ettiğinde ise bilgiler kendisine verilmemiştir. Başvurucu kendisi hakkında bilgi toplanmasının, toplanan bilgilerin içeriklerinin kendisiyle paylaşılmasının ve bilgilerin yanlışlığını kanıtlama hakkının kendisine tanınmamasının özel yaşam hakkını ihlal ettiğini iddia etmiştir. Mahkeme kararında özel yaşam hakkına yönelik müdahale olduğunu kabul ederken, bu müdahalenin "ulusal güvenlik" gerekçesiyle haklı koşulları olduğuna hükmetmiştir[208]. Bu karar yargı yolu kullanmaksızın da etkili bir denetim yolunun sağlanabileceğinin

[202] Atak, s.103.
[203] Küzeci, s.123.
[204] "Case of Klass and Others v. Germany", Başvuru No: 5029/71, 06.9.1978, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}, (Erişim Tarihi): 01.04.2019.
[205] Atak, s.103.
[206] Kılınç, s.1099-1100.
[207] "Leander v Sweeden", Başvuru No: 9248/81, 26.3.1987, https://swarb.co.uk/leander-v-sweden-echr-26-mar-1987, (Erişim Tarihi): 01.04.2019.
[208] Aysun, s.120.

örneği olarak kabul edilmekteyse de, verildiği tarihte birçok eleştirinin hedefi olmuştur. Ancak, Mahkeme bu davada devletin negatif yükümlülüğüne referans vermiştir[209].

Devletin pozitif yükümlülüğüne referans verilen bir dava örneği ise, Gaskin v. Birleşik Krallık davasıdır[210]. Bu dava, AİHM'nin kişisel verilere erişim hakkını tartıştığı bir karar niteliğinde olup, AİHM başvurucunun, ulusal makamlar tarafından tutulan ailevi ilişkilerine dair kişisel verilerine ulaşmasının engellenmesini AİHS'nin 8'inci maddesinin ihlali olarak görmüştür[211]. Buna göre başvurucu Bay Gaskin çocukluğunu sosyal hizmetlerin bakımı altında geçirmiş olup, o gün yaşadığı sorunların çözülebilmesi için geçmişi hakkında bilgi sahibi olması gerektiği argümanıyla kendisiyle ilgili raporları ilgili mercilerden talep etmiştir fakat ilgili merciler bu talebe olumsuz cevap vermiştir. Bu noktada başvurucunun şikayeti devletin eylemi değil, eylemsizliğidir ve bu nedenle 8'inci maddeyi ihlâli bu perspektiften incelenmelidir. Mahkeme, Gaskin'in çocukluğuna ilişkin veri talebini yaşamsal bir fayda olarak değerlendirmiştir ve buna göre devlet böyle bir talebi karşılamakla yükümlüdür. Bu nedenle ilgili raporların hazırlanmasına katkı sunan kişiler bunu açıklamaya rıza göstermiyor ya da cevap vermiyorsa buna ilişkin nihai karar bağımsız bir otorite tarafından verilmelidir. Mahkeme bu şartların yerine getirilmemesinden dolayı 8'inci maddenin öngördüğü pozitif yükümlülüğün ihlaline karar vermiştir[212].

108 Sayılı AK Sözleşmesi

Teknolojideki yüksek hızlı gelişmeler sonrası bireylerin kişisel verilerin korunma şartları daha da zorlaşmış ve bu ihtiyaç artık AİHS'nin 8'inci maddesi ile giderilememeye başlamıştır. Özellikle, özel sektörde kişisel verilerin bilgisayar ortamına işlenmesi süreci beraberinde birçok sorunu gündeme getirmiştir. Bu bağlamda, AK açısından dönüm noktası 28 Ocak 1981 tarihinde 108 sayılı *"Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşmeyi"* (ETS 108) kabul etmesidir. Sözleşme 5 Konsey üyesi ülke İsveç, Norveç,

[209] Atak, s.104-105.
[210] "Case of Gaskin v. the United Kingdom", Başvuru No: 10454, 7.7.1989, http://www.juridischeuitspraken.nl/19890707EHRMGaskin.pdf, (Erişim Tarihi): 01.04.2019.
[211] Akgül, Kişisel Verilerin Korunması, s.124.
[212] Atak, s.106-107.

Fransa, Almanya ve İspanya'nın oylaması sonucunda 1 Ekim 1985 tarihinde yürürlüğe girmiştir[213]. Bu sözleşmenin OECD ve BM düzenlemelerine göre, en önemli ve ayırıcı özelliği kişisel verilerin korunması hakkında hukuki bağlayıcılığı olan ilk metin olmasıdır. 108 sayılı Sözleşmenin 4. maddesine göre, taraf devletler sözleşme metninde yer alan verilerin korunmasına ilişkin ilkelere işlerlik kazandıracak önlemleri alma yani yasal düzenlemeler ile iç hukuklarını bu sözleşmeye uygun hale getirmek zorundadır. Diğer yandan, 11. madde ise taraf devletlere sözleşmenin öngördüğü korumadan çok daha fazla koruma sağlama imkanı tanımaktadır[214].

Sözleşmenin bir diğer önemli özelliği ise, hem özel hem kamu sektörüne yönelik ele alınmasının yanı sıra, sadece otomatik verilerle sınırlandırılmaması yarı otomatik işleme süreçlerini de kapsam içerisine almasıdır. Ancak, elle işlenen veriler kapsam dışıdır[215].

Sözleşmenin 5'inci maddesine göre veriler; haklı ve yasal yollarla elde edilmeli, işlenmeli, kaydedilmeli, haklı amacı dışında kullanılmamalı, uğruna kaydedildikleri amaç her neyse onu gerçekleştirmeye elverişli olmalı, yalnızca gerektiği kadar kaydedilmeli, doğru ve güncel olmalı, ilgili kişinin kimliğine ulaşabilecek biçimde ve doğru süreyle sınırlı olmalıdır[216]. Bu madde, aynı zamanda işleme tabi tutulacak verilerin kalitesinin sağlanmasını amaçlamaktadır[217].

Sözleşmenin 6'ıncı maddesi "hassas veriler" kavramına yer vermekte olup, bu kavram kapsamına ilgili kişilerin etnik kökenleri, ideolojileri, dini değer ve inançları, sağlık ve cinsel yaşamları, ceza mahkumiyetleri girmektedir. Bu veriler, iç hukukta uygun güvence sağlanmadıkça otomatik işleme tabi tutulamazlar[218]. Diğer yandan, 7'inci madde ise devletlerin bu verileri kazaen veya izinsiz olarak yok edilmesi, elde edilmesi, değiştirilmesi, izinsiz olarak dağıtılmasına karşı uygun güvenlik önemleri alma zorunluluğu getirmiştir[219].

---

[213] Küzeci,s.126; Aysun, s.50.
[214] Develioğlu, s.9.
[215] Küzeci, s.134.
[216] Ayözger, s.76.
[217] Aksoy, s.100.
[218] Akgül, Kişisel Verilerin Korunması, s.131.
[219] Aysun, s.51.

Sözleşmenin 8'inci maddesi ilgili kişiler hakkında ek güvencelere işaret etmekte olup, bu ek güvenceler; ilgili kişinin kendisine ait otomatik olarak işlenen veri olup olmadığını, işlenme amacını, veri yöneticisinin kimliğini öğrenme; işlenen verilerin kendisine bildirilmesini sağlama; gerektiği durumlarda işlenen veriler üzerinde düzeltme, eksikleri tamamlatma; hukuka aykırı olarak işlenmesi durumunda verileri sildirtme ve bu talepleri yerine getirilmediği durumda yasal yollara başvurma olarak sıralanmaktadır[220].

Sözleşme uyarınca 5'inci, 6'ıncı ve 8'inci maddelere istisna getirilebilmektedir. Bunun için gerekli olan koşullar; devlet ve kamu güvenliği, devletin mali menfaati, suçların önlenmesi, ilgili kişinin korunması, başkalarının hak ve özgürlüklerinin korunması ve demokratik bir toplumun işleyişi için zorunlu durumlar olarak sıralanmaktadır[221]. Diğer yandan, Sözleşmenin 12'inci maddesi taraf devletler arasında sınır ötesi veri akışını engellemeyi yasaklarken, bunun için belirtilen istisnalar ise; 6'ıncı maddede belirtilen alıcı ülkenin yasalarının yeterli korumayı garanti etmemesi ve aktarımın sözleşmenin tarafı olmayan bir ülke aracılığıyla yapılmasıdır[222].

Sözleşme kapsamında bir Danışma Komitesi ve sözleşmeye yapılan ek protokol ile bağımsız kontrol organları oluşturulmuştur. Komitenin görevleri; sözleşmenin uygulanmasını kolaylaştırmak, geliştirmek ve bu amaçla önerilerde bulunmak, sözleşmede değişiklik önerisinde bulunmak, değişiklik önerileri hakkında görüş bildirmek, sözleşmenin uygulanması ile ilgili sorular hakkında görüş bildirmek olarak sıralanmaktadır[223].

Diğer yandan; AK'nin sözleşmede ortaya konan asgari standartları geliştirmek amacıyla çeşitli tavsiye kararları aldığı görülmektedir. Bu kararların bir kısmı şu şekilde sıralanmaktadır;

- *Doğrudan Pazarlama Amacıyla Kullanılan Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı.*

[220] Aysun, s.51.
[221] Küzeci, s.133.
[222] Aşıkoğlu, Ş. İpek: Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, On İki Levha Yayıncılık, İstanbul 2018, s.43.
[223] Akgül, Kişisel Verilerin Korunması, s.145.

- *Sosyal Güvenlik Amacıyla Kişisel Verilerin Korunması Konusunda Tavsiye Kararı.*
- *Emniyet Alanında Kişisel Verilerin Kullanımının Düzenlenmesine İlişkin Tavsiye Kararı.*
- *İstihdam Amacıyla Kullanılan Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı.*
- *Ödeme ve Diğer İşlemler İçin Kullanılan Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı.*
- *Kamu Makamlarının Elinde Bulunan Kişisel Verilerin Üçüncü Kişilere İletilmesine İlişkin Tavsiye Kararı.*
- *Telefon Hizmetleri Alanındaki Kişisel Veriler Başta Olmak Üzere, Telekomünikasyon Hizmetleri Alanındaki Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı.*
- *Tıbbi Verilerin Korunmasına İlişkin Tavsiye Kararı.*
- *İstatistiksel Amaçlarla Toplanan ve İşlenen Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı.*
- *İnternette Özel Yaşamın Korunmasına İlişkin Tavsiye Kararı. Sigorta Amacıyla Toplanan ve İşlenen Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararı*[224].

"*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun*[225]"un yayınlanması ile Türkiye de sözleşmeyi imzalayıp yürürlüğe koyan AK'ye üye devletler arasına katılmış ve böylece istisna ülke kalmamıştır.

Son olarak 18 Mayıs 2018 tarihinde AK Bakanlar Komitesi tarafından 108 Sayılı Sözleşme'yi Yenileyen Protokol (CETS N.223) kabul edilmiştir[226]. Bu protokolün amacı uluslararası bir standart kurmak olup, sadece Konsey üyesi ülkelerde değil, küresel düzeyde veri akışının kurallarının belirlenmesi olarak öne çıkmaktadır. Metinde; insan

[224] Aysun, s.52.
[225] Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, R.G. 29703, 05.05.2016.
[226] "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, (Erişim Tarihi): 26.04.2019.

onuruna ve bireysel özerkliğe daha fazla vurgu yapılırken, uluslararası kuruluşların Sözleşme'ye taraf olmasına imkan tanınmış, veri işleme süreçlerinde şeffaflığı arttırmaya yönelik yeni kurallar getirilmiştir. Genetik ve biyometrik verilerle birlikte özel nitelikte kişisel veri kategorisi genişletilirken, ayrımcılık riskine karşı güvence vurgusu yapılmıştır. Bunlara ilaveten veri kişisinin temel haklarına müdahale olarak değerlendirilebilecek veri sızıntılarının gecikme olmadan bildirilmesi yükümlülüğü getirilmiştir. KÜZECİ'nin görüşü, 108+1 olarak da tanımlanan bu protokolün Türkiye tarafından da onaylanacağı yönündeyken[227], DÜLGER, 108 sayılı Sözleşmede yaşanan gecikmenin bu protokolün imzasında yaşanmayacağını ve iç hukuka dahil edileceğini belirtmektedir[228].

Avrupa Birliği (AB)

Kişisel verilerin korunmasına yönelik önemli önlemleri hayata geçirmiş bir diğer uluslararası kuruluş ise Avrupa Birliği'dir. 20. yüzyılda totaliter rejimler nedeniyle kişisel verilere erişimin ortaya çıkardığı büyük yıkımlara maruz kalan Avrupa, bu olumsuz deneyimleri gidermek amacıyla kişisel verilerin kontrolsüz kullanımını önlemek için birçok önlemi hayata geçirmektedir[229].

Bugün Avrupa'nın kalıcı bir barış için hayata geçirdiği en büyük proje olan AB'nin temel amacına ulaşabilmesi için kişilerin, hizmetlerin, malların ve sermayenin serbest dolaşımı gerekmekte olup, bunun için verilerin işlenmesi ve korunması önem arz etmektedir. AB üyesi devletler aynı zamanda AK'nin de üyesi olduğundan 108 Sayılı Sözleşme'yi onaylamıştır. Ancak, üye ülkelerin iç hukuklarından verilerin korunmasına ilişkin farklılıklar sürmekte olup, bu durum beraberinde bütüncül ve etkin koruma sorunu doğurmuştur[230].

---

[227] Elif Küzeci, "Avrupa Konseyi'nin 108 Sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter kararı ve diğer bazı gelişmelere ilişkin bir değerlendirme", https://medium.com/@elfkzc/avrupa-konseyinin-108-say%C4%B1l%C4%B1-ki%C5%9Fisel-verilerin-korunmas%C4%B1-s%C3%B6zle%C5%9Fmesi-yenilendi-bc8daad9decc, (Erişim Tarihi): 26.04.2019.
[228] Dülger, Kişisel Verilerin Korunması, s.54.
[229] Tekin, Nurullah: "Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", Uyuşmazlık Mahkemesi Dergisi 4, Ankara 2014, s.224.
[230] Akgül, Danıştay ve Avrupa, s.211.

Dolayısıyla, AB bu alandaki sorunları gidermeye yönelik düzenlemeleri hayata geçirmeyi sürdürmektedir. Bugün Avrupa kişisel verilerin korunması ülküsünün anavatanı olarak kabul edilebilecek oldukça gelişmiş bir mevzuata sahiptir[231]. Aşağıda bu mevzuatı oluşturan düzenlemelere yer verilecektir.

95/46/AT Sayılı Veri Koruma (Direktifi)

AB bünyesindeki ülkelerde kişisel verileri korumaya yönelik mevzuat bulunmaktaysa da, her ülkede başka bir yaklaşımı yansıtmaktadır. Örneğin; Almanya, Fransa ve İskandinav ülkelerinde kişisel verilerin korunması hakkı bir insan hakkı olarak kabul edilirken, B. Krallık'ta bu düzenleme uluslararası ticaretin korunmasını hedeflemektedir. Dolayısıyla bu yaklaşım farklılıkları veri akışı ile hak ve özgürlükler arasında çatışma ortamını doğurmakta, bu da AB'nin temel felsefesi olarak "Ortak Pazar" ve kişisel hak ve özgürlüklerin hayata geçirilmesini aksatmaktadır[232].

Bu aksaklıkları gidermek amacıyla Avrupa Birliği bünyesinde ilk girişim Avrupa Birliği Komisyonu tarafından 1990 yılında hazırlanan ilk kişisel veri koruma taslağı olup, bu taslak 24 Ekim 1995 tarihinde kabul edilerek üç yıl sonra yürürlüğe konmuştur. 25 Ekim 1998 tarihi itibariyle veri koruma kanunu tüm Avrupa'da daha güçlü bir konuma gelmiştir. İlgili Direktif bir çerçeve metin niteliğinde olup, üye ülkelerin metin öngördüğünün üzerinde bir koruma düzeyi öngörmektedir. Nitekim, AB'de direktifler, kanun yapma araçlarından biri olup, doğrudan bağlayıcı olmamasının yanı sıra birer uyumlaştırma aracıdır[233]. Bu Direktif, kişisel verilerin korunması hukukundaki en etkili düzenleme niteliğine sahiptir ve en önemli özelliği, üye ülkelerde kişisel verilerin korunmasına dair asgari standartları belirlemesidir[234].

Direktif'te kullanılan anahtar terimler ve içerikleri şu şekilde sıralanmaktadır;

- *Kişisel Veri:* Bir kimlik numarası ile ilişkilendirilmek veya fiziksel, psikolojik, ekonomik, kültürel kimliği yansıtan bir içerik taşımak sureti ile bir kişiyi belirli veya belirlenebilir kılan gerçek kişiye ilişkin herhangi bir bilgi (isim, pasaport,

[231] Küzeci, s.154.
[232] Aşıkoğlu, s.57-58.
[233] Tekin, s.226.
[234] Develioğlu, s.10.

sosyal güvenlik numarası, telefon, motorlu taşıt plakası, fotoğraf, ses, özgeçmiş, parmak izi, genetik bilgiler)

- *İşleme:* Kişisel verilerin toplanması, elde edilmesi, kaydedilmesi, saklanması, organizasyonu, değiştirilmesi, kullanılması, transferi, yayılması, kombinasyon, blokaj, silinme, yok edilmesi gibi her türlü işlem
- *Verilerin otomatik olarak işlenmesi:* Bilgisayar vb. otomasyon sistemleri gibi yöntemlerle işlenmesi
- *Verilerin otomatik olmayan araçlarla işlenmesi:* Otomasyon sistemlerine başvurulmadan alfabetik ya da kronolojik olarak verilerin işlenmesi[235].

Bu bağlamda Direktif; genel hükümler, kişisel verilerin işlenmesinin yasallığı, yargı yolları, sorumluluk ve müeyyideler, kişisel verilerin üçüncü ülkelere transferi, etik kurallar, denetleyici makam, çalışma grubu ve Birlik uygulama önlemleri olmak üzere yedi bölüm ve toplam otuz dört maddeden oluşmaktadır. Direktif'in koruma düzeyi hem kamu hem de özel sektör için aynı olup, 3/1'inci maddesinde "*bütünüyle veya kısmen otomatik araçlarla, ve ..bir dosyanın parçasını oluşturan veya bir dosyanın parçasının olmasının istendiği kişisel verilerin otomatik araçlarının haricinde her türlü yolla"* ibaresiyle işlemler arasında da ayrım ortadan kaldırılmıştır. Buna göre, elle veri işleme sadece kişisel veri dosyalama sisteminin bir parçası ise işin içine girmektedir[236].

Bununla birlikte Direktif'e koruma, ses ve görüntüler yoluyla da olsa belirli veya belirlenebilen gerçek bir kişiyle ilişkin herhangi bir bilgi olarak "kişisel veri" ile sınırlı tutulmuştur. Dolayısıyla, bankaların kurduğu güvenlik kameraları, dijital imzalar ya da veri öznesinin rızasıyla bile olsa tutulan kayıt sistemlerine ilişkin istisna ya da rehber ilke içermemektedir[237].

İstisna kapsamına alınacak ve Direktifin uygulanmayacağı hususlar ise; ceza hukuku alanındaki devlet faaliyetleri, devlet güvenliği, savunma, kamu güvenliği ile ilgili verilerin işlenmesi ve AB hukuku kapsamı dışında düşen bir faaliyet ve gerçek bir kişi tarafından, tamamen kişisel veya ev içi faaliyet esnasında yapılan (Örneğin; mezuniyet

[235] Başalp, Kişisel Verilerin Korunması, s.33.
[236] Develioğlu, s.11.
[237] Tekin, s.227.

partisi davetleri için bilgisayarda hazırlanmış bir elektronik çizelge vb.) olarak sıralanmaktadır[238].

Direktif'in getirdiği diğer yenilikler; erişim hakkı, verilerin düzeltilmesi, silinmesi ve bloke edilmesini isteme hakkı ve itiraz hakkı gibi bir takım haklardır. Erişim hakkı aynı zamanda veri öznesinin kişisel verilerine serbestçe ulaşılabilmesi hakkı olup bu nedenle verilerin hangi amaçla işlendiği, bu amaç için hangi işlemlerin sıralandığı ve veri kişisinin istememesi durumunda ne gibi işlemlerin yapıldığının bildirilmesini kapsamaktadır. Veri kişisi bu hakka dayanarak bu bilgileri çeşitli aralıklarla tekrardan öğrenebilme hakkına sahiptir[239].

Bir diğer önemli yenilik ise gelişen teknolojiler sonucunda oldukça karmaşık sorunlar doğurabilen kişisel verilerin üçüncü ülkelere aktarımı ile ilgilidir. AB üyesi ülkelerde veri aktarımının bir çeşit veri işleme olarak kabul edilmektedir[240]. Dolayısıyla, kişisel verilerin korunma düzeyi zayıf ülkelere bir kez transferi durumunda geleceğinin belirsizleşmesi en temel endişe nedeni olup, bu Direktif ile aktarım yapılacak AB dışı ülkenin koruma seviyesinin Direktif ile uyumlu olması gerekliliği aranmaya başlanmıştır. Buna göre aktarımın yapılacağı AB dışı ülkelerde; verinin niteliği, ilgililerin kimliğinin bilinebilirliği, amaca bağlılık, ilgililerin erişim hakkının bulunup bulunmadığı, veri işleme faaliyetinin hukukiliğini denetleyen makam bulunup bulunmadığı ve bu makamların etkinliği ile hukuka aykırı işleme faaliyetlerine yönelik yaptırımların varlığı hususlarının değerlendirilmesi gerekmektedir[241].

Yapılan inceleme sonucunda "yeterli koruma düzeyi" tespit edilemezse, bu değerlendirmeyi yapan Komisyon'un ve üye devletlerin birbirilerini haberdar etme yükümlülükleri bulunmaktadır[242]. Direktif'in 26'ıncı maddesinde bu şartları haiz olmayan üçüncü ülkelere veri transferine dair istisnalar belirlenmiş olup, bunlar; veri sahibinin açık rızasının olması, veri sahibi ile veri işleyen arasındaki bir sözleşmenin ifası, veri sahibinin hayati menfaati, veri işleyen ile üçüncü taraf arasında

[238] Aşıkoğlu, s.62.
[239] Aysun, s.59.
[240] Küzeci, s.174.
[241] Başalp, Kişisel Verilerin Korunması, s.68-69.
[242] Küzeci, s.176.

gerçekleştirilen sözleşmenin ifası, hukuki veya kamu yararı ya da kamuya açık sicildeki bir bilgi olması durumudur[243].

Direktif sadece AB sınırları kapsamında değil bu sınırlar dışında da kişisel verilerin korunmasına yönelik genel bir anlayışın oluşmasına katkı sağlamıştır. Dolayısıyla, bu Direktif'ten esinlenen ve veri koruma kanununa sahip AB dışı ülkelerde de bu yaklaşım genel kabul görmüştür[244]. Nitekim, AB'nin vize muafiyetinden çeşitli müzakere fasıllarının açılmasına kadar geniş bir alanda kişisel verilerin korunmasına yönelik yasal ve yönetsel düzenleme talebi bir baskı faktörüne dönüşerek, Türkiye'de bu alandaki düzenlemelere şekil verdiği belirtilmektedir[245].

2016/679 Sayılı Genel Veri Koruma Tüzüğü (GVKT)

AB içerisinde 108 Sayılı Sözleşme ve Direktif'in kişisel verileri koruma mevzuatına önemli açılımlar getirse de, ülkeler arasındaki farklı pratikler ve veri aktarımının düşük koruma düzeyi olan ülke üzerinden gerçekleştirilmeye çalışılması gibi nedenlerle AB'nin "dijital ortak pazar stratejisine" yönelik risk son bulmamış ve kişisel verilerin korunması alanındaki reform ihtiyacı sürmüştür[246]. Reform ihtiyacına binaen 2010 yılında başlanan çalışmalar 2012 yılında AB Komisyonu tarafından kabul edilen GVKT taslağı ile karşılık bulmuştur. 27 Nisan 2016 tarihinde ise Direktif'te belirtilen ilkelerin geliştirilmesi ve teknolojik gelişmeler karşısında daha etkin koruma sağlanması amacıyla 2016/679 sayılı GVKT, 25 Mayıs 2018 tarihinde yürürlüğe girmek üzere kabul edilmiştir ve bu yeni düzenleme ile Direktif ilga edilmektedir[247].

GVKT'nın en temel amacı "küresel veri akışı ve yeni bilişim teknolojilerinin hızlı gelişimi nedeniyle karşılaşılan sorunların aşılmasının sağlanması" iken[248], en önemli özelliği AB'nin bu kez bir Direktif değil, sektörel konularda kullandığı tüzük formunu

[243] Aksoy, s.104.
[244] Başalp, Nilgün: "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri" (Avrupa Birliği), Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 1 (21), İstanbul 2015, s.81.
[245] Kutlu, Önder ve Kahraman, Selçuk: "Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi", Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi 5, İstanbul 2017, s.46.
[246] Küzeci, s.200; Dülger, Kişisel Verilerin Korunması, s.64.
[247] Aşıkoğlu, s.64.
[248] Küzeci, s.201.

tercih etmesidir. Bu tercihle, AB ilgili mevzuatın üye ülkelerde doğrudan uygulanabilir olmasını sağlamak istemektedir[249].

Nitekim GVKT, Avrupa Birliği'nin İşleyişi Hakkındaki Antlaşma'nın 288'inci maddesi uyarınca genel uygulama alanına sahip olup bağlayıcı niteliktedir ve üye ülkelerde uygulanacaktır. Bununla birlikte, metnin uluslar üstü yapısını korumak adına üye ülkelerin GVKT hükümlerini kendi iç hukuklarına aktarmaları engellenmiştir. İç hukukla GVKT arasında bir farklılık bulunması durumunda GVKT'nın esas alınması kararı verilmiştir. Bunun tek istisnası, devletin iç hukukundaki veri koruma düzenlemelerinin GVKT'ya göre daha kapsamlı olduğu durumlardır. Bu bağlamda, özel ya da tüzel gerçek hukuk kişilerinin idareye açacağı ya da birbirlerine karşı açacakları davalar GVKT'ya dayandırılabilir ve mahkeme kararını GVKT'yı esas alarak verebilir[250].

Dijital çağın en kapsamlı hukuk uyumlaştırma projelerinden biri olarak nitelendirilen[251] GVKT'nın içerdiği en önemli yenilikler; veri kişisinin haklarının daha etkin korunabilmesi amacıyla veri işleyen ve veri kontrolörünün sorumluluklarının arttırılmış olması, veri kontrolörünün veri sahibine haklarına ilişkin bilgilendirme ve bunu belgelendirme yetkisi getirilmesi, veri sahibinin verilerinin işlenmesi için iznin zorunlu kılınması, unutulma hakkı- Ücretsiz, hızlı ve kolay biçimde veri sahibinin sistemden çıkış hakkı (opt-in), verilerin işlenmesi için veri sahibinin rızasının özgürce, aydınlatılmış ve amacı konusunda kesin bilgilendirilmiş şekilde alınması (Rıza koşulunun güçlendirilmiş olması), veri işleyenlerin tamamının veri işlemeden sorumlu tutulması, veri sahibine verileri taşıma hakkı tanınması, veri kontrolörünün yapacağı ihlallerin temel hak ve özgürlükleri tehdit etme riski doğurması durumunda 72 saatten geç olmamak kaydıyla veri sahibinin bilgilendirilmesi, veri kontrolörünün riskli işleme faaliyetlerinden önce veri koruma etki değerlendirmesi yapma sorumluluğunun getirilmesi, AB üye ülke vatandaşlarına ait verilerin sınır ötesine aktarımının daha sıkı koşullara bağlanması, verilerin hukuka aykırı şekilde işlenmesi durumunda veri sahibine tazminat hakkı düzenlemesinin getirilmesi ve rücu imkanı tanıması ve daha

[249] Develioğlu, s.12.
[250] Aysun, s.61.
[251] Başalp, Avrupa Birliği, s.77.

ağır yaptırımlara zemin sağlaması ve kişisel verilerin korunmasına ilişkin daha elverişli mekanizmaların öngörülmesi olarak sıralanmaktadır[252].

Ancak, bunların arasında en önemlisi 17'inci maddede yer alan silinme ya da unutulma hakkı olarak kabul edilmektedir[253]. Unutulma hakkı ve kişisel verilerin gerektiği ölçüde ve sürede saklanması konuları, kişisel verilerin korunması hakkının çatısı olarak tarif edilmektedir[254]. Bu bağlamda, unutulma hakkı; " dijital ya da yarı fiziksel hafızada yer alan bireylere ait rahatsız edici her türlü kişisel içeriğin, yine bireylerin talebi üzerine bir daha geri getirilemeyecek biçimde ortadan kaldırılması/silinmesi" olarak tanımlanmaktadır[255]. KÜZECİ ise bu hakkın, "yaşamda beyaz sayfa açabilme hakkı" olarak anlaşıldığını belirtmektedir[256].

Özetle unutulma ya da silinme hakkı toplanma amacı bakımından artık ihtiyaç bulunmayan verilerin tamamen silinmesi hakkı olup, GVKT'nın 17'inci maddesiyle bireylere kişisel verileri çok uzun süredir toplanma amaçları ile bağlantılı şekilde kullanılmıyorsa ve veri sahibini ilgili verilerin toplanmasına rızası yoksa bu verilerin silinmesini sağlama ve daha fazla yayılmasına engel olma konusunda bir hakkı ilk kez tanımıştır. Bununla birlikte GVKT, önceki metinlere göre veri sahibinin rızayı geri çekebilmesi, işlemeye itiraz edebilmesi ve bu durumda veri kontrolörü gecikmesizin bu verileri silme yükümlülüğünü de içerecek şekilde geliştirilmiştir[257].

Bu hakkın kullanımına dair en önemli örnek AB hukukunun uygulanmasında son sözü söyleyen yargı organı niteliğindeki Avrupa Birliği Adalet Divanı (ABAD) tarafından verilen 13 Mayıs 2014 tarihli "Google Kararı"dır[258]. İspanyol Vatandaşı Costeja Gonzalez tarafından İspanya Veri Koruma Ajansı'na (İVKK) Google İspanya, Google Inc. ve La Vanguardia adında bir günlük gazeteye aleyhinde yapılan şikayetten türeyen

[252] Develioğlu, s.13; Aysun, s.62-63.
[253] Develioğlu, s.13.
[254] Akgül, Aydın: "Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" ve AB Adalet Divanı'nın "Google Kararı" (Unutulma Hakkı), Türkiye Barolar Birliği Dergisi, 116, Ankara 2016, s.14.
[255] Gülener, s.226.
[256] Küzeci, s.231.
[257] Elmalıca, Hasan: "Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı", Ankara Üniversitesi Hukuk Fakültesi Dergisi 65, Ankara 2016, s.1612.
[258] ABAD, C-131/12 Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131, (Erişim Tarihi): 13.5.2014.

davanın konusu bu mecralarda ilgili şahsa yönelik sosyal güvenlik borçları nedeniyle uygulamaya konulan haciz işleminin bilgilerinin yer almasıdır. Arama motorlarında ismi arandığında bu haberle karşılaşılan Gonzalez, Direktif'e dayanarak gazeteden bu sayfaların kaldırılmasını ya da kendisiyle ilgili kişisel verilerin görünmeyecek şekilde revize edilmesini talep etmişti. İVKK, gazete hakkındaki şikayet, İspanyol hukukundaki düzenlemelere dayanarak reddetmiş ancak Google İspanya ve Google Inc. şirketleri hakkındaki şikayeti kabul etmiştir. İVKK şirketlerden bu haberdeki kişisel verilerin silinmesini talep etmiş, buna karşılık şirketler İspanya Ulusal Mahkemesi nezdinde dava açmıştır. İspanya Yüksek Ulusal Mahkemesi bu davaları birleştirmiş ve konu hakkında görüş bildirmesi için ABAD'a taşımıştır[259].

ABAD, Direktif'e dayanarak aldığı "unutulma hakkına" ilişkin kararında[260];

- Arama motorlarının faaliyetlerinin bir kişisel veri işleme faaliyeti olduğu ve bu nedenle Direktif'in 2. maddesine göre veri kontrolörü niteliğini haiz olduğu,
- Arama motorlarının Direktif'in 12. maddesine göre erişim hakkı kapsamında yetersiz, ilgisiz, geçersiz verilerin silinmesi veya düzeltilmesinden sorumlu oldukları,
- İlgili verilerin "üstün kamu yararı" kavramı ile bir ilgisi olmadığı ve bu nedenle tüm bu verilerin arama sonuçlarına ilişkin dökümlerden çıkarılması gerektiği belirtilmiştir ve bu karar ilgili hakkın kullanılması konusunda mihenk taşı olarak kabul edilmektedir.

Bu başvuru sonucunda ABAD'ın verdiği karar, sadece "unutulma hakkı" için değil, yabancı bilişim şirketlerinin AB topraklarındaki faaliyetleri üzerinde de önemli bir etkiye neden olmuştur[261].

Amerika Birleşik Devletleri (ABD)

ABD'de kurumsal bir veri koruma düşüncesi hala uygulamaya geçmemiş olup, anayasal olarak da korunmamaktadır. ABD'de verilerin korunması Avrupa'ya kıyasla çok daha

[259] Elmalıca, s.1613-1614.
[260] Akgül, Unutulma Hakkı, s.31.
[261] Küzeci, s.232.

esnek bir yaklaşımla gerçekleştirilirken, bu yaklaşım doğrultusunda ABD, OECD Rehber İlkeleri'ni 1981 yılında imzalamış ancak iç hukukuna dahil etmemiştir[262]. Federal düzeyde sektör bazlı düzenlemeler bulunmaktaysa da, ABD'de özellikle Bilgi Edinme Hakkı Kanunu (The Freedom of Information Act) nedeniyle kişisel verilerin korunmasının olumsuz olarak etkilendiği savunulmaktadır[263].

Diğer yandan, ülkede kişisel verileri korumaya ilişkin çerçeve metinler şunlardır;

- *ABD Anayasası'nın 4. Eki:* Kişisel verilerin korunması kapsamında kişilerin evleri ve belgeleri hukuk dışı aramalara karşı koruma altındadır ancak bireyin bu korumadan faydalanması için meşru bir beklentisi olmalıdır.

- *Özel Yaşamın Gizliliği Kanunu (The Privacy Act):* Kişilerin isimleri, kimlik numaraları, parmak izi, ses kaydı veya fotoğraf gibi belirleyici hususları, eğitimi, finansal işlemleri, sağlığı, adli sicili ve iş hayatlarına dair bilgilerin toplanmasını düzenleyen bir kanun olup, özel şirketlere karşı tüketicinin haklarını düzenleyecek şekilde genişletilmektedir. Ancak bu kanun, sınırlı bir uygulama alanına sahip olması itibariyle eleştirilmiştir[264].

- *Safe Harbor İlkeleri:* AB yaklaşımının aksine verilerin üçüncü ülkelere aktarımı ile ilgili ABD'de, ülke vatandaşı olmayan bireylerin kapsam dışı bırakılması, bağımsız bir denetleme mekanizması olmaması, amaca bağlılık ve amacın gerektirdiğinden daha uzun süre elde tutulamaması gibi ilkelerin hiç olmaması ya da eksik düzenlenmesi söz konusudur. AB ile ABD arasında bu gibi farklılıkları gidermek amacıyla yedi temel maddeden oluşan ilkeler yürürlüğe konulmuş olup, buna göre ABD, AB'den veri transfer ederken veri öznelerini bilgilendirecek, öznenin izni olmayan üçüncü ülkelerle bu verileri paylaşmayacak, bu şartlar sağlansa bile daha düşük koruma düzeyi olan üçüncü ülkelere bu verileri aktarmayacak ve veri öznelerinin şikayetlerine karşılık verecek bağımsız denetim organları kuracaktır[265]. Bu ilkeler ABD menşeli

[262] Aşıkoğlu, s.54.
[263] Aysun, s.69'dan naklen Schwartz ve Reidenberg'in görüşü alınmıştır.
[264] Aşıkoğlu, s.54.
[265] Aksoy, s.106.

Google, Amazon, Facebook gibi dünyanın en büyük veri işleme şirketleri için de bağlayıcılığa sahiptir[266].

ABD'de özel yaşamın korunmasına yönelik bu düzenlemelerin, hukuki yapılanmanın ifade özgürlüğü temelinde kurulması nedeniyle kısıtlı kaldığı ifade edilmektedir[267]. Ancak, son yıllarda ABD mahkemeleri tarafından verilen kararlarla birlikte ABD'deki kişisel verilerin korunması hukukunda da yaklaşım değişiklikleri görülmeye başlanmıştır. Carpenter v. B. ABD kararı uyarınca cep telefonu baz istasyonu verileri aracılığıyla veri kişisinin konum bilgisine erişebilmek için kural olarak kolluk güçlerinin arama emrine sahip olmaları gerekmekte olup, bu kararlar kişilerin konum verilerine devletin sınırsız erişimi reddedilmektedir[268].

Asya-Pasifik Ekonomik İşbirliği (APEC) Örgütü Çerçeve Belgesi

Asya-Pasifik bölgesinde ekonomik gelişim ve refahı desteklemek amacıyla 1989 yılında Avustralya, Brunei Darülselam, Kanada, Endonezya, Japonya, Güney Kore, Malezya, Yeni Zelanda, Filipinler, Singapur, Tayland ve ABD öncülüğünde kurulan ve bugün 21 üyesi bulunan APEC bünyesinde elektronik ticaretin üye ülkeler arasında yaygınlaştırılması amacıyla 2005 yılında *"Özel Yaşamın Gizliliği Çerçeve Belgesi (APEC Privacy Framework)"* kabul edilmiştir. Direktif doğrultusunda veri akışının sağlanması ve özel hayatının gizliliğinin korunmasını amaçlayan belge, OECD Rehber İlkeleri'nden esinlenerek oluşturulmuştur[269].

Üye ülkeler açısından bağlayıcılığı olmayan ve iki bölümden oluşan belgenin ayrıştırıcı özelliği kişisel verileri koruma konusunda AB ülkelerine göre daha dağınık ve etkisiz bir koruma düzeyi olan Asya-Pasifik ülkelerinde daha güçlü yasal düzenlemeleri

[266] Ayözger, s.85; Aysun, s.71.
[267] Aşıkoğlu, s.53.
[268] Elif Küzeci, "Avrupa Konseyi'nin 108 Sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter kararı ve diğer bazı gelişmelere ilişkin bir değerlendirme", https://medium.com/@elfkzc/avrupa-konseyinin-108-say%C4%B1l%C4%B1-ki%C5%9Fisel-verilerin-korunmas%C4%B1-s%C3%B6zle%C5%9Fmesi-yenilendi-bc8daad9decc, (Erişim Tarihi): 26.04.2019.
[269] Küzeci, s.150.

desteklemesi ve serbest ticaret ile kişisel hak ve özgürlükler arasında denge tesis etme yönünde hukuki bir girişim olmasıdır[270].

2.2.2. Ulusal düzenlemeler

Kişisel veriler sadece uluslararası düzenlemeler ile koruma altına alınmamış olup, AB dışı ülkelerin de kendi iç hukukları bu yöndeki düzenlemeleri içermektedir. Türkiye de AB etkisinde olmakla birlikte bu alandaki düzenlemelerini kanunlaştırma yoluna giden ülkelerden biridir. DÜLGER'e göre Türkiye'de ilgili konulardaki kanunlaşmanın Avrupa ülkelerine göre daha geriden gelmesinin nedeni bu ülkelerdeki teknolojik ve hukuki gelişmelerin hızıdır. Dolayısıyla, bu ülkelerdeki ihlaller arttıkça hukuk da buna cevap vermek için daha hızlı cevap vermeye çalışmaktadır. Ancak Türkiye 108 Sayılı Sözleşme'ye imza atan ilk ülkelerden biri olmakla birlikte, uzun süre kişisel verilerin korunması ile ilgili somut bir adım atmamıştır[271].

Aşağıda Türkiye'de kişisel verilerin korunmasına yönelik mevzuatın gelişim aşamaları niteliğindeki metinlere yer verilecektir.

1982 Türkiye Cumhuriyeti Anayasası

Kişisel verilerin korunmasını talep etme hakkı AB üye devletlerinde temel bir insan hakkı olarak kabul görmesine karşın sadece bazı üye ülkelerin anayasalarında temel bir insan hakkı olarak düzenlenmiştir[272]. Türkiye'de ise anayasal gelişmeler içerisinde bu hakkın zamanla kendisine yer bulduğu ve olgunlaştığı görülmektedir. Bu bağlamda, 1982 Anayasası'nda doğrudan kişisel veriye atıf yapmayan ama kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakta olup, bunlar; hukuk devleti ilkesi, insan onuru ve kişinin maddi ve manevi varlığını serbestçe geliştirme hakkı (md.5, md.17), özel hayatın gizliliği (m.20), konut dokunulmazlığı (m.21), haberleşmenin gizliliği (md.22), din ve vicdan hürriyeti (m.24), düşünce ve kanaatleri açıklamaya zorlanmama hakkı (m.25, m.26) gibi anayasal güvencelerdir[273].

[270] Uncular, s.82.
[271] Dülger, Kişisel Verilerin Korunması, s.69.
[272] Aşıkoğlu, s.96.
[273] Aksoy, s.93.

Bu bağlamda, Anayasa'nın 17'inci maddesinde şu ifadelere yer verilmektedir[274];
"*MADDE 17- Herkes, yaşama, maddî ve manevî varlığını koruma ve geliştirme hakkına sahiptir. Tıbbî zorunluluklar ve kanunda yazılı haller dışında, kişinin vücut bütünlüğüne dokunulamaz; rızası olmadan bilimsel ve tıbbî deneylere tâbi tutulamaz. Kimseye işkence ve eziyet yapılamaz; kimse insan haysiyetiyle bağdaşmayan bir cezaya veya muameleye tâbi tutulamaz. (Değişik: 7/5/2004-5170/3 md.; 16/4/2017-6771/16 md.)*".

20'inci maddede ise özel hayatın gizliliği ve korunması hakkının ihlaline ilişkin hükümler söz konusudur.

"*MADDE 20- Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Mülga cümle: 3/10/2001-4709/5 md.) (Değişik: 3/10/2001-4709/5 md.) Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar*".

Görüldüğü üzere, Anayasa'nın 20'inci maddesine göre; "kişisel verilerin korunmasını talep etme hakkı, özel hayatın gizliliğinin korunması hakkından doğan temel hak ve özgürlüklerden birisi" olarak öne çıkmaktadır[275].

Günümüzde akıllı telefonlar ve e-postalar üzerinden gerçekleşen büyük kişisel veri trafiğine karşılık haberleşmenin gizliliği önem arz etmektedir. Anayasa'nın 22'inci maddesi kişisel verilerin korunmasına yönelik bu konuyla ilgili hükmü içermekte olup, bu hüküm şu şekildedir;

[274] T.C. Anayasası, Kanun No: 2709, Kabul Tarihi: 7.11.1982
[275] Oğuz, s.123.

"*MADDE 22- (Değişik: 3/10/2001-4709/7 md.) Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de 5 kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir*".

2010 yılında yapılan referandum sonucunda Anayasa'nın 20'inci maddesine eklenen ve doğrudan kişisel verilerin korunmasına atıf yapan ek fıkra aşağıdaki gibi olup;
"(Ek fıkra: 12/9/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir". Bu ek fıkra ile kişisel verilerin korunması hakkı ülkemizde ilk defa açıkça anayasal güvence altına alınmıştır[276]. Bazı sorunlu yanları olmakla birlikte, bu hükmün kişisel verilerin korunmasına yönelik bazı temel ilkeleri kapsaması dolayısıyla daha etkin bir koruma yolunda önemli bir adım olduğu ifade edilmektedir[277].

Bu fıkranın gerekçesi ise, Anayasa'da kişisel verilerin korunmasına yönelik dolaylı hükümler yer almakla birlikte yeterli olmaması, mukayeseli hukuk ve uluslararası düzenlemeler uyarınca herkesin kişisel verilerinin korunmasını isteme hakkının anayasal bir hak olarak teminat altına alınmasıdır. Bu şekilde kişisel verilerin korunması hakkı temel insan hakkı olarak anayasal güvence altına alınmıştır. Bu düzenleme ile garanti alınan haklar kapsamına; veri ilgilisinin bilgilendirilmesi, verilere erişmesi,

[276] Aydın, s.58.
[277] Küzeci, s.296.

verilerin hatalı olması halinde düzeltilmesini istemesi, gerektiği takdirde silinmesini talep etmesi ve hangi amaçlarla kullanıldığını öğrenme hakkı alınmıştır[278].

Diğer yandan düzenlemenin eleştiriye uğrayan yönleri ise; kişisel verilerin işlenmesi hususunda bağımsız bir denetim makamını öngörmemesi ve Anayasanın 13'üncü maddesindeki temel hak ve özgürlüklerin sadece Anayasa'nın ilgili maddelerindeki sebeplere bağlı olarak sınırlanabileceğine hükmüne karşın kişisel verilerin kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebileceği ifadesidir[279]. Bu ucu açık ifadeler aynı zamanda bir kişisel verileri işleme kanununa olan ihtiyacın da ifadesi niteliğindedir[280].

5237 Sayılı Türk Ceza Kanunu

Kişisel verilerin korunmasına ilişkin mevzuatın bir diğer bağlayıcı unsuru ise TCK'dır. 765 sayılı TCK'da kişisel verilerin korunması ile ilgili hükümler sadece; "Hürriyet Aleyhine İşlenen Cürümler" kapsamında beşinci fasıl içerisinde "Sırrın Masuniyeti Aleyhine Cürümler" kapsamında düzenlemiştir. Buna göre fiilen cezayı düzenleyen bazı hükümler söz konusudur. Buna göre; "*kişinin kendisine gönderilmemiş mektup, telgraf ya da kapalı zarfı kasten açması ya da başka bir şahsın, posta ve telgrafla vâkı açık muhabere evrakını anlamak için hukuka aykırı olarak ele geçirmesi* (md.195); *kendisine gönderilmiş olmayan posta ve telgraf muhaberesini ortadan kaldırması* (md.196) ve *bu evrakın ifşa edilmesi* (md.197) ile ilgili düzenlemeler bu bağlamda değerlendirilmektedir[281]. Ancak bu düzenlemeler kişisel verilerin korunmasına ilişkin hükümler içermemeleri ve yeterli addedilemedikleri için kişisel verilerin izinsiz olarak kaydedilmesi ve paylaşılması ceza hukuku alanında değerlendirilme imkanına sahip olamamıştır. Bu bağlamda, daha kapsamlı ayrıntılı bir düzenleme için 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı TCK beklenmiştir[282]. Yeni TCK ile, 765 sayılı TCK'nın doğrudan koruma ihtiyacı duymadığı kişisel verilerin hukuka aykırı olarak işlenmesi eylemleri suç olarak düzenlenmiştir. Nitekim, 6698 sayılı KVKK da işlenen

[278] Dülger, Kişisel Verilerin Korunması, s.70.
[279] Küzeci, s.266.
[280] Aydın, s.61.
[281] Aysun, s.77.
[282] Aşıkoğlu, s.101.

suçlar bakımından 5237 sayılı TCK'ya atıf yapmaktadır[283]. Bu şekilde, her iki yasa arasında doğrudan bir ilişki kurulmaktadır[284].

Yeni TCK'da kişisel verileri korumaya ilişkin düzenlemeler md.135, md.136 ve md.138'de kendisine yer bulmakta olup, bu maddeler Türk hukukunda kişisel verilerin korunmasına dair gerçekleştirilen ilk somut kanuni düzenlemeler olarak kabul edilmektedir[285]. 135'inci madde ile düzenlenen "gerçek kişiye ilişkin her türlü bilgi olarak" kişisel verilerin, herhangi bir araç ile ve herhangi bir formatta hukuka aykırı olarak kaydedilmesidir. Bu verilerin kişilerin siyasi, felsefi, dini görüşleri, etnik ve dini kökenleri, ahlaki eğilim, cinsel yaşam, sağlık durumları ya da sendikal bağlantılarına ilişkin olması durumunda cezayı ağırlaştırıcı neden söz konusudur. Bu madde kapsamında suç işleyen kimseye bir yıldan üç yıla kadar hapis cezası öngörülürken, işlenen verinin hassas veri olması durumunda ceza yarı oranında artırılmaktadır. Bu suçla korunan hukuki değer, toplumsal düzenin devamı için bir ceza normuyla korunması elzem olan soyut, manevi, ideal değerlerdir[286]. Ancak, bu maddeye ilişkin doktrinde de tartışmalar söz konusudur. Bir görüşe göre, kişisel veriler gizli olarak kabul edilen hayat alanımıza dahil sır niteliğindeki bilgilerdir ancak madde gizli veya sır kapsamına referans vermemektedir. Bir diğer görüş ise, kişisel verinin konusunu oluşturan değere göre korunan hukuki değerin belirlenmesini savunmaktadır[287].

TCK'nın 136'ıncı maddesinde ise kişisel verilerin hukuka aykırı olarak verilmesi, yayılması ve ele geçirilmesi suç olarak düzenlenmiştir. Bu düzenlemenin amacı, kişisel verilerin yetkisiz üçüncü kişilerin eline geçmesinin ve içeriklerinin öğrenilmesinin engellenmesi iken, korunan hukuki değer ise Anayasa'da dayanağı bulunan özel hayatın gizliliğinin korunmasının bir parçasını oluşturan kişisel verilerin korunması hakkıdır. Bu madde kapsamında suç işleyen kimse iki yıldan dört yıla kadar hapis cezası ile cezalandırılmaktadır[288]. Bu maddenin gerekçesinde özellikle hastaneler, sigorta

[283] Sarıusta, s.104.
[284] Küzeci, s.402.
[285] Aksoy, s.113.
[286] Sert, s.99-100.
[287] Sarıusta, s.116-117'dan naklen Tütüncübaşı'nın görüşü alınmıştır.
[288] Sert, s.136.

şirketleri, bankalar, mağazalar gibi çeşitli kurum ve kuruluşların veri işleme ve bu verileri paylaşma sürecinin oluşturabileceği zararlara atıfta bulunulmaktadır[289].

Bir diğer önemli hüküm ise "Verileri yok etmeme" başlıklı 138'inci maddede yer almaktadır. Bu madde ile hukuka uygun olarak kaydedilen kişisel verilerin, kaydedilme veya elde edilme amacının gerçekleştirilmesi, amacın ortadan kalkması, o veriye ihtiyacın kalmaması veya kişisel verinin saklanmasına imkan tanıyan kanuni düzenleme ile öngörülen saklama süresinin dolmasına rağmen verinin imha edilmemesi durumunda ortaya çıkan suçlar düzenlenmektedir. Bu suçla korunan hukuki değer, özel hayatın gizliliği başta olmak üzere kişisel verilerin korunması hakkıdır. Bu madde kapsamında suç işleyen kimseye bir yıldan iki yıla kadar hapis cezası öngörülürken, yok edilmeyen verinin CMK'ya göre ortadan kaldırılması veya yok edilmesi gereken bir veri olması durumunda ceza bir kat artırılmaktadır[290].

Ayrıca, 132'inci maddede haberleşmenin gizliliğini ihlal, 133'üncü maddede kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, 134'üncü maddede özel hayatın gizliliğin ihlal suçları düzenlenmiştir. Buna ilaveten TCK 137'inci maddeye göre bahsi geçen suçlar kamu görevlisi tarafından ve görevinin verdiği yetkinin kötüye kullanılması suretiyle veya belli bir mesleğin ve sanatın sağladığı kolaylıktan yaralanmak suretiyle işlenmişse cezanın yarı oranında arttırılması söz konusu olacaktır[291].

Diğer Kanunlardaki Kişisel Verilerin Korunmasına İlişkin Düzenlemeler

Kişisel verilerin korunmasına dair kanuni düzenlemeler yukarıda sayılanlarla sınırlı olmayıp, aşağıda diğer ilgili düzenlemeler de sıralanmaktadır.

4857 sayılı İş Kanunu (İK)

AİHM içtihadında da belirtildiği üzere iş bulmak, işsiz kalmamak ve huzurlu bir iş düzenine sahip olmak bireysel tatmin açısından önem arz etmekte olup, iş; sağlık ve aile

[289] Aşıkoğlu, s.101.
[290] Sert, s.152.
[291] Uncular, s.94-95.

yaşamından sonra en önde gelen konu niteliğindedir. Diğer yandan, iş ilişkisinin ayırt edici özelliği olarak işçinin ekonomik ve hukuki bağımlılığı söz konusudur[292]. Bu bağlamda, 10 Haziran 2003 tarihinde yürürlüğe giren İK'nın 75'inci maddesine göre işveren çalıştırdığı her işçi için bir özlük dosyası düzenlemekte olup, işçinin kimlik bilgilerinin yanı sıra çeşitli belge ve kayıtları eklemektedir. Bunların İş Kanunu ve diğer kanunlar uyarınca tutulması gereken kayıtlar olduğu ve amaca bağlılık ilkesine riayet edilmesi gerektiği unutulmamalıdır. Dolayısıyla, amaca bağlı olmayan verilerin (örneğin; işçilerin ruhsal, sosyal, fiziksel, ekonomik vb. verileri) bu dosyada tutulması bir ihlâldir. Bu belge ve kayıtlar istendiği takdirde yetkili memur ve mercilere gösterilmek zorundadır. Buna göre işveren, tüm bu belge ve kayıtları kaydetme, saklama, üçüncü kişilere aktarma gibi hususlarda "dürüstlük kuralları ve hukuka uygun olarak kullanmak zorundadır". Bununla birlikte işverenin özlük dosyasında bulundurduğu ve gizli kalmasında işçinin haklı çıkarı olan bilgileri açıklamamakla yükümlü olması bir tür sır saklama yükümlülüğü olarak kabul edilmektedir[293]. Bu bağlamda, kişisel verileri hukuka uygun olarak işlenmeyen ve tutulmayan işçinin İş Kanunu'nun madde 24/II çerçevesinde iş akdini haklı nedenle feshedebileceği ve genel hükümlere göre zararın tazminini talep edebileceği görüşü öne çıkmaktadır[294].

6098 sayılı Türk Borçlar Kanunu (TBK)

Bu kanunun 417'inci maddesinin 1. fırkası uyarınca; "*İşveren, hizmet ilişkisinde işçinin kişiliğini korumak ve saygı göstermek ve işyerinde dürüstlük ilkelerine uygun bir düzeni sağlamakla, özellikle işçilerin psikolojik ve cinsel tacize uğramamalarını ve bu tür tacizlere uğramış olanların daha fazla zarar görmemeleri için gerekli önlemleri almakla yükümlü"* kılınmıştır[295].

419'uncu maddede ise *"İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. Özel kanun hükümleri saklıdır"* denmekte olup buna göre, işverenin işçiye ait kişisel verileri

[292] Küzeci, s.384.
[293] Başalp, Kişisel Verilerin Korunması, s.77.
[294] Manav, Eda: "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", Gazi Üniversitesi Hukuk Fakültesi Dergisi, 2, Ankara 2015, s.106.
[295] Uncular, s.88-89.

işçinin kişiliğinin korunması bağlamında koruma yükümlülüğü söz konusudur. Ancak bu maddede yer alan "işçinin işe yatkınlığı" ve "sözleşmenin ifası için zorunlu olduğu ölçüde" ifadeleri uluslararası düzenlemelere göre daha belirsiz bir içeriğe sahiptir ve bu nedenle etkin bir koruma öngörmemektedir[296].

Burada bahsedilebilecek diğer düzenlemeler ise; 5070 sayılı Elektronik İmza Kanunu, 1512 sayılı Noterlik Kanunu, 5411 sayılı Bankalar Kanunu, 3682 sayılı Adli Sicil Kanunu ve 1587 sayılı Nüfus Kanunu olarak sıralanmaktadır[297].

6698 Sayılı Kişisel Verilerin Korunması Kanunu

Avrupa'nın birçok ülkesinde kişisel verilerin korunması ile ilgili kanunların geçmişi neredeyse yarım yüzyıla ulaşmıştır. Bu yöndeki gelişmelerin sebebi; bazı ülkelerin geçmişindeki otoriter deneyimler nedeniyle bireysel hak ve özgürlüklerin korunmasına verilen önem; elektronik ticaret başta olmak üzere teknolojinin yarattığı riskleri engellemek ve Avrupa ile ticaret yapmak isteyen üçüncü ülkelere veri aktarımının koruma altına alınmak istenmesidir. Türkiye'de de bir kişisel verileri koruma kanunu için tüm bu nedenler bulunmaktadır[298].

Ülkemizde kişisel verileri koruma yönünde çeşitli kanun çalışmaları olmakla birlikte bunlar zamanın ruhunu yakalamaktan uzak kalmıştır. Özellikle, teknolojik ve toplumsal gelişmeler sonucunda "verinin" kazandığı içerik beraberinde hukuki bir çerçeveye olan ihtiyacı da arttırmıştır. Türkiye'nin taraf olduğu uluslararası sözleşmeler, veri akışındaki muhatap ülkelerin hukuklarında konuya yönelik düzenlemeler ve verilerin işlenmesi gerekliliği ile kişisel verilerin korunması hakkının karşı karşıya gelmesi ülkemizin de bu yönde bir düzenleme yapmasını zorunlu kılmıştır[299].

KVKK'yı doğuran nedenler; insan haklarının korunması bilinciyle birlikte kişisel verilerin korunması noktasında artan önem, Türkiye'de kişisel verilerin korunmasına

[259] Uncular, s.88-89.
[297] Aksoy, s.113-115.
[298] Korkmaz, İbrahim: "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme" (Kişisel Verilerin Korunması), Türkiye Barolar Birliği Dergisi 124, Ankara 2016, s.84-85.
[299] Küzeci, s.305-306.

ilişkin alanı bütüncül olarak düzenleyen özel bir kanun ve etkin bir denetim mekanizmasının olmaması, TCK'da 135'inci ve takip eden maddelerde düzenlenmiş suçlara yönelik özel bir kanun bulunmamasının getirdiği karışıklıklar, AB'ye tam üyelik sürecinde gerçekleştirilen müzakere fasıllarının ilerletilmesi gerekliliği, uluslararası suçluların takip edilebilmesini sağlayan EUROPOL sisteminde Türkiye ile veri paylaşılan ülke arasında hukuki uyumsuzlukların olması, sağlık kuruluşlarında çok sayıda özel nitelikli kişisel veri olmasına karşın bunun hukuki bir dayanağa sahip olmaması, Türkiye'de yaşayan yabancılar ile yurtdışında yaşayan Türklerle ilgili verilerin paylaşımında sorun yaşanması, Türkiye'nin 2003 Ulusal Programında kişisel veriler konusunda kanun hazırlama taahhüt etmesi, yabancı sermaye çekebilmek ve bu yatırımların etkin yönetimi için mevzuatın buna uygun olması ve Türkiye'nin birçok kişisel veri koruma konulu uluslararası düzenlemenin tarafı olması ve iç hukukunu buna uydurması gerekliliği olarak sıralanmaktadır[300].

Türkiye'de kişisel verileri korumaya yönelik kanun çalışmaları 1989 yılına kadar götürülebilse de[301], en geniş kapsamlı ve Türk kişisel verilerin korunması hukukunun temel düzenlemesi olan[302] KVKK'nın geçmişi 13 Eylül 1995'e kadar geri gitmektedir. Bu tarihte "Kişisel Verilerin Korunması Kanun Tasarısını" hazırlamak üzere TBMM bünyesinde komisyon oluşturulmuş, çalışmalarını tamamlayamadan dağılan bu komisyon 18 Eylül 2000 tarihinde yeniden kurularak üç yıllık bir çalışma sonucu 2003 yılında bir kanun tasarısı hazırlamıştır. Bu kanun tasarısının TBMM Başkanlığına iletilmesi ise 2008 yılını bulmuş, Başkanlık tasarıyı esas komisyon olarak Adalet Komisyonu'na, tali komisyon olarak AB Uyum Komisyonu'na göndermiş ancak gündemin yoğunluğu ve TBMM seçimleri sebebiyle tasarı hükümsüz kalmıştır. Sonrasında Adalet Bakanlığı tarafından revize edilen tasarı Başbakanlık tarafından ikinci kez TBMM Başkanlığı'na gönderilmiş ancak benzer sebeple yeniden hükümsüz kalmıştır. Son olarak 18 Ocak 2016 tarihinde TBMM Başkanlığı'na gönderilen tasarı 24 Mart 2016 tarihinde TBMM Genel Kurul'unda kabul edilerek kanunlaşmış olup,

[300] Dülger, Kişisel Verilerin Korunması, s.107.
[301] Uncular, s.97.
[302] Develioğlu, s.15.

kanunlaşma gerekçesi olarak 108 Sayılı AK Sözleşmesi'nde ve 95/46 sayılı Direktif'e atıf yapılmıştır[303].

Diğer yandan, KVKK'nın kanunlaşma sürecinin hızlanmasında asıl etken, vize muafiyeti sağlamak üzere AB standartlarına uygun bir Kanun'un yürürlüğe girmesi gerekliliği olarak belirtilmektedir[304]. Ancak bu düzenlemeye rağmen, AK'nin 2016 tarihli raporunda kolluk kuvvetlerinin yasa kapsamında olmaması ve bağımsız veri koruma otoritesinin bulunmaması nedeniyle KVKK'nın yeniden gözden geçirilmesi gerektiğine vurgu yapıldığı görülmektedir[305].

Bununla birlikte, KVKK'nın 25 Mayıs 2018'de ilga edilecek Direktif'ten hareketle hazırlanması daha baştan değişiklik gerektirecek bir Kanun olduğu şeklinde yorumlanmaktadır. Çünkü, Türk mevzuatı ile uyumlu olmayan ve Direktif'in yerine geçen GVKT, veri öznelerine tanınan hakları genişletmiş ve veri sorumlularına yüklenen yükümlülükleri ise arttırmıştır. Bu uyumsuzluğun doğurabileceği en temel risklerin başında ise AB üyesi ülkeler ile Türkiye arasında veri aktarımını engelleyecek olan ve GVKT'nın 83'üncü maddesi uyarınca bu ihlâli gerçekleştirenler için gündeme gelebilecek 20 milyon euro'ya ulaşabilecek para cezalarıdır[306].

KVKK'nın amacı 1'inci maddede; *"kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek*" olarak açıklanırken, amaç Anayasa'nın 20'inci maddesi çerçevesinde düzenlenmiştir. Ayrıca, Direktif'in 1'inci maddesi ve AB Kişisel Verilerin Korunması Yönetmelik Taslağı'nın 1'inci maddesi ile paralellik arz etmektedir[307].

KVKK'da yer verilen veri kişilerinin temel hak ve özgürlüklerini koruma amacını yerinde bulmakla birlikte, kişisel verilerin korunması hakkının bir insan hakkı olarak açıkça ifade edilmediğini belirtilmektedir. Dolayısıyla, bu hakkın temel bir insan hakkı

[303] Korkmaz, Kişisel Verilerin Korunması, s.86.
[304] Küzeci, s.311.
[305] Uncular, s.98.
[306] Aysun, s.80.
[307] Korkmaz, Kişisel Verilerin Korunması, s.86.

olarak altının çizilmesi kişisel verilerin korunmasına ilişkin farkındalığın artmasına ve zihniyet gelişimine katkı sağlayacaktır[308].

KVKK'nın kapsamı ise 2'inci maddede; "*kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler*" olarak tanımlanmıştır. Bu bağlamda, kanun gerçek kişiler ile bu verileri işleyen gerçek ve tüzel kişiler hakkında uygulanacak olup, kamu ve özel sektör ayrımı yapılmamıştır. Ayrıca, kişisel verilerin otomatik ya da herhangi bir veri kayıt sisteminin parçası olması kaydıyla otomatik olmayan yollarla işlenmesi de kapsama girmektedir.

Çalışmanın üçüncü bölümünde KVKK, kişisel verilerin korunması alanına getirdiği yenilikler ve kendinden önceki mevzuatla kurduğu ilişki itibariyle tüm boyutlarıyla ele alınacaktır.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

Ulusal düzenlemelerden bir diğeri ise KVKK'nın 7/3'üncü ve 22/1'inci maddelerine dayanarak hazırlanmış olan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik olup, veri sorumluları hakkında uygulanır[309]. Yönetmeliğin amacı, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemektir. Yönetmelikte asgari olarak veri sorumluları tarafından yürütülecek kişisel veri saklama ve imha politikasının; hazırlanma amacı, kayıt ortamı, saklama ve imha süreçleri ile süreler ve ilgili idari ve teknik tedbirlere dair bir çerçeve çizilmektedir.

Yönetmeliğe göre kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme ya da anonim hale getirme yükümlülüğünün

[308] Uncular, s.99.
[309] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, R.G.: 30224, 28.10.2017.

ortaya çıktığı tarihi takip eden ilk imha işleminde kişisel verileri siler, yok eder ya da anonim hale getirir. Periyodik imha süreleri; altı ayı geçemez. Yükümlülüğü olmayan veri sorumlusu ise yükümlülüğün ortaya çıktığı tarihi takip eden üç ay içinde silme, yok etme ya da anonim hale getirme işlemini yerine getirmektedir.

Yönetmeliğe göre ilgili kişinin silme ya da yok etme talebi olması durumunda, kişisel veri işleme şartları tamamen ortadan kalkmışsa, bu talep en geç otuz gün içerisinde sonuçlandırılarak ilgili kişiye bilgi verilir. Bu veriler üçüncü kişiye aktarılmışsa, üçüncü kişiler bilgilendirilir ve Yönetmelik kapsamında gerekli işlemlerin yapılması temin edilir. Ancak kişisel veri işleme şartları tamamen ortadan kalkmamışsa bu talep veri sorumlusu tarafından KVKK'nın 13/3'üncü maddesi uyarınca gerekçe açıklanarak reddedilebilir ve en geç otuz gün içerisinde yazılı ya da elektronik ortamda ilgili kişiye bildirilir.

Yönetmelik, 28.04. 2019 tarihinde Resmi Gazete'de yayınlanan Yönetmelik ile değiştirilmiş olup, kişisel veri işleme envanterinin kapsamı genişletilmiş ve kişisel veri işlenmesinin hukuki sebebi gibi unsurlar da envantere eklenmiştir. Ayrıca, veri sorumlusuna, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemler veya anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklama yükümlülüğü getirilmiştir[310].

Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik

Kişisel veriler alanının önemli bir boyutunu oluşturan ve özel nitelikli veriler arasında yer alan kişisel sağlık verilerinin işlenmesinde, bu verilere erişim için kurulacak sistem, kişisel sağlık verisi kaydı tutulan sistemlerin güvenliği ve denetimi ile sağlık hizmeti sunumundaki personel hareketlerinin Sağlık Bakanlığı'na bildirilmesine ilişkin

[310] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik, R.G.: 30758, 28.04.2019.

işlemlerde uyulacak usul ve esasları düzenleyen bu Yönetmelik[311], birçok eleştiriye maruz kalmıştır. Bunlar; henüz KVKK'nın yeni yürürlüğe girmiş olması, kavram ve terimlerin henüz yeterince anlaşılmamış olması, Kişisel Verileri Koruma Kurulu'nun işleyişi başta olmak üzere usul ve esaslarının belirlenmemiş olması ve bu Kurul'un görüşünün alınmamış olması olarak sıralanmaktaydı[312]. Yukarıda da görüldüğü üzere ilgili yönetmelik birçok tartışmayı ve yönetmeliğin iptali hakkındaki davaları beraberinde getirmiştir. Bu yönde yapılan yönetmeliğin muhtelif maddelerinin ve tümünün yürütmesinin durdurulması ve iptaline dair bir davada davacılar, Anayasa'da kişisel verilerin otomatik işleme tabi tutulmasına dair usul ve esasların ancak kanunla düzenlenebileceğinin belirtilmesine rağmen, sağlık verilerinin işlenme ve korunma kurallarının yönetmelikle düzenlendiğini; Kişisel Veri Koruma Kurulu oluşturulmadan alana dair düzenleme yapıldığını; Kanun'un 22/1'inci maddesine göre diğer kurum ve kuruluşların kişisel verilere dair hüküm içeren mevzuat taslakları hazırlanırken Kurul'dan görüş alınmasının zorunlu olduğu; yönetmelik hazırlanırken hekimlerin başta sır saklama olmak üzere mesleki hak ve yükümlülükleri ile veri sahibi hastalarının haklarının yok sayıldığı ve bu durumun Anayasa'nın 56'ıncı maddesinde güvence altına alınan sağlık hakkının ihlâli anlamına geldiği; sağlık verilerinin rıza alınmaksızın işlenebileceği istisnai hallerin 108 Sayılı Sözleşme'ye aykırı olarak çok geniş tutulduğu; hiçbir istisna hali bırakmaksızın kişisel sağlık verilerinin kamu kurumları ve uluslararası güçler arasında paylaşılmasının insanları sağlık hizmeti almaktan alıkoyabileceği yani bazı temel hak ve hürriyetleri kullanmaktan imtina edebileceği; yönetmeliğin sağlık verilerinin korunmasına dair yeterli ve objektif hükümler içermediği; yönetmeliğin dayandığı KVKK'nın birçok hükmünün ana muhalefet partisi tarafından AYM'ye götürüldüğü gerekçelerini öne sürmüştür. Buna karşılık Sağlık Bakanlığı, Anayasa'nın 20'inci maddesi ile KVKK'nın 20'inci maddesi uyarınca yönetmeliğe imkan tanıyan ön şartların hazır olduğunu; itirazların içeriğinin Türkiye'de hiçbir kurum tarafından sağlık verisi işlenemeyecek bir çerçeve çizeceğini; Kurul'un işleyişinin usul ve esaslarının düzenlenmemiş olmasının bir gerekçe olarak sunulmasının tutarlı bir yanı

[311] Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, R.G.:29863, 20.10.2016.

[312] Dülger, M. Volkan, " Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik'in Getirdikleri ve Dikkat Edilmesi Gereken Hususlar",http://dulger.av.tr/2018/07/12/kisisel-saglik-verilerinin-islenmesi-ve-mahremiyetinin-saglanmasi-hakkinda-yonetmelikte-degisiklik-yapilmasina-dair-yonetmelikin-getirdikleri-ve-dikkat-edilmesi-gereken-hususlar/ (Kişisel Sağlık), (Erişim Tarihi): 21.04.2019.

bulunmadığını; ayrıca davacının iddiasının aksine mevzuat taslaklarını hazırlarken Kurul'dan görüş alınmasının KVKK'da bir zorunluluk olarak belirtilmediğini ve bu anlama gelmeyeceğini savunmasında belirtmiştir. Tüm bu sav ve savunmalar ışığında Danıştay Onbeşinci Dairesi ise kararında Kurul'ın henüz oluşmadığını, KVKK'nın 6/4'üncü maddesine göre kişisel verileri korumaya ilişkin yeterli önlemlerin Kurul tarafından belirlenmediğini, yönetmelik hazırlanırken genel nitelikte bir kontrol ve denetim yetkisine sahip olan Kurul'dan şart olmasına karşın görüş alınmadığını ve bu nedenlerle yürütmenin durdurulması isteminin kabul edilmesine, yönetmeliğin yürürlüğünün durdurulmasına oy çokluğu ile karar vermiştir[313].

Danıştay'ın kararı, Kurul için seçilen üyelerin 12 Ocak 2017 tarihinde yemin ederek göreve başlaması, 28 Ekim 2017 tarihinde "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"in yayınlanması ve 16 Kasım 2017 tarihinde "Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik"in yayınlanması ile birlikte söz konusu yönetmelikte uyumlaştırma amacıyla bazı değişiklikler yapılması zorunlu hale gelmiş; bu nedenle yönetmelikte değişiklik yapan yönetmelik yürürlüğe girmiştir[314]. Ancak, yeni yönetmelik kişisel sağlık verilerinin korunması bakımından tatmin edici yenilikler sağlamaması nedeniyle Türk Tabipler Birliği ve Türk Dişhekimleri Birliği tarafından dava konusu edilmiştir. İptal talebine konu olan hükümler, Yönetmelik'te m. 5/8; m.7/1 ve m.8/1'e ilişkinken, bu talebe dair gerekçeler ise; kişisel verilerin merkezi sağlık veri sistemine aktarılması kuralının özünde hukuka aykırı olması, merkezi veri sistemine aktarım faaliyetinde anonimleştirmenin öngörülmemiş olması, idarenin erişimine herhangi bir sınırlama getirilmemiş olması, sağlık hizmeti sunucularının kullanmaları gereken yazılım standartlarının belirtilmemiş olması, m.7/1 ve m.8/1 ile aktarım zorunluluğu getirilmiş olması, sağlık hizmet sunucuları tarafından yapılacak kayıt yükümlülüğünün belirsiz olması, ilgili hükümlerin temel hakkın özüne zarar veren müdahale niteliğinde olması olarak sıralanırken, Danıştay Onbeşinci Daire, kararında, yürütmesi durdurulan bir

[313] Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmeliğin Yürütmesinin Durdurulması Hakkında Danıştay Kararı, Danıştay 15. Daire; E. 2016/10500, 6.7.2017.
[314] Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik, R.G.:30250, 24.11.2017.

düzenlemede kısmi değişiklikler yapmak suretiyle hukuka aykırılığı saptanmış olan düzenlemenin canlandırılmasının hukuken mümkün olmadığını belirtmiştir[315].

DÜLGER, Danıştay'ın iptali istenen hükümler hakkında herhangi bir inceleme yapmamış olmasını, iptali istenen hükümlerin yer aldığı Yönetmeliğin tamamı hakkında daha önceden yürütmenin durdurulması kararı vermiş olmasına bağlamaktır. İlgili düzenlemede kişisel verileri koruma mevzuatının aksine, kişisel verilerin işlenmesi istisna değil, kural haline gelmekteyse de, Sağlık Bakanlığı'nın Karar'daki hususları dikkate alıp yeni bir yönetmelik yayınlayarak yola devam etmeye çalışacağını tahmin etmektedir[316]. Bizim görüşümüz de, sağlık verilerinin işlenmesini düzenleyen bir yönetmeliğin her yönüyle açık, net ve belirli olması, ayrıca genel mevzuatla her aşamada uyumuna dikkat edilmesi gerektiği şeklindedir.

[315] Kişisel Sağlık Verileri Yönetmeliğinin Yürütmesinin Durdurulmasına İlişkin Karar, Danıştay 15. Daire; 2018/1490 Y.D., 9.10.2018.
[316] Dülger, Kişisel Sağlık.

ÜÇÜNCÜ BÖLÜM: KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDA KİŞİSEL VERİLERİNİN İŞLENMESİNİN ŞARTLARI

3.1. Kişisel Verilerin Korunmasına İlişkin Temel İlkeler

Kişisel verilerin korunmasına yönelik düzenlemelerde temel amaç, verilerle ilgili işlemlerin insan onuru ve değerlerine uygun yapılmasıdır[317]. Doktrine göre, bu uygunluğu sağlamak amacıyla dağınık olarak düzenlemelerde kişisel verilerin korunmasında genel ilkeler belirlenmiştir. Bunlar; dürüst toplama, asgarilik, amaca bağlılık, sınırlı kullanım, doğruluk, koruma (güvenlik), bireyin katılması ve sorumluluk ilkesi olarak sıralanmakta olup[318], bu ilkelere uyulmadığı takdirde, kişisel verilerin iyi niyetle ve hukuka uygun işlenmediği ve kötüye kullanım şüphesine imkân tanıyan bir ortamın oluştuğu öngörülmektedir[319]. Diğer yandan, genel ilkeler tek başına hukuka uygunluk sebebi değilse de, rıza alındığı durumlarda bile, genel ilkelere uyulmuyorsa, hukuka aykırı veri işleme söz konusu olacaktır. Bu bağlamda, bu ilkelerin en temel özelliği; kişisel verilerin elde edilme aşamasından, veriler üzerinde gerçekleştirilen tüm işlemlere kadar uyulması gereken kuralların belirlenmesini sağlamasıdır. Bir diğer deyişle, kişisel veriler sadece kanuni düzenlemelerin öngördüğü temel ilkeler kapsamında ve bu usul ile esaslara uygun olarak işlenip, korunabilir[320].

İlkeler aynı zamanda bir ülke ya da uluslararası kuruluşun kişisel veri koruma hukukuna dair bakış açısını ortaya koymaktadır. Buna göre, bir kişisel verileri koruma mevzuatına hâkim olan genel ilkeler incelendiğinde, aynı zamanda o ülkenin kişisel verileri nasıl ve ne ölçüde korumaya çalıştığı ve veri koruma hukukundaki amacı anlaşılmaktadır[321]. Bu ilkelerin birbirinden kesin çizgilerle ayrılması zor olup, bazı ilkeler diğerlerine kaynaklık etmekte, bazıları ise, tamamlayıcı role sahip olmaktadır[322]. Bununla birlikte,

[317] Ketizmen, Muammer: Türk Ceza Hukukunda Bilişim Suçları, Adalet Yayınevi, Ankara 2008, s.269.
[318] Oğuz, s.129.
[319] Korkmaz, Kişisel Verilerin Korunması, s.99.
[320] Develioğlu, H. Murat: Avrupa Birliği Genel Veri Koruma Tüzüğü, Oniki Levha Yayıncılık, İstanbul 2017, s.44.
[321] Dülger, Kişisel Verilerin Korunması, s.108.
[322] Küzeci, s.195.

bu ilkeler verilerin sahip olması gereken nitelikleri düzenlemekte ve verilerin kaliteli olması ilkesi olarak da tanımlanmaktadır[323].

Kişisel verilerin toplanması ve işlenmesine yönelik genel ilkeler, büyük ölçüde 108 sayılı Sözleşme'ye uyumlu ve Direktif'ten iktibas edilerek oluşturulan KVKK'nın 4'üncü maddesinde kendisine yer bulmuştur[324]. Bu ilkeler, KVKK'ya esas olan aşağıdaki alt başlıklarla ele alınacaktır.

3.1.1. Hukuka ve dürüstlük kurallarına uygun olması

Kişisel verilerin korunması ile ilgili birçok metinde birbirine yakın ifadelerle yer verilen bu ilke[325], diğer birçok ilkeyi kapsaması ve kaynak oluşturması nedeniyle kişisel verilerin korunması hukukunun çekirdeği olarak değerlendirilmektedir[326]. KVKK'nın 4'üncü maddesinde kendine yer bulan bu ilke, kişisel verilerin işlenmesi faaliyeti esnasında kanun ve diğer hukuki düzenlemelere uygun olarak hareket edildiğinin teminatı niteliğindedir[327]. Bu bağlamda, hukuka uygunluk sıfatı, veri işlemenin kast edilen her türlü pozitif hukuk kuralı, uluslararası ve ulusal yasalar ve diğer düzenlemelerde öngörülen ilkelere uygun olarak gerçekleştirildiğini belirtirken, dürüstlük kuralına uygun olma ise, veri öznesinin menfaati ile makul beklentilerinin dikkate alınmasını ifade etmektedir[328]. Her iki nitelik bir arada kullanıldığında, kişisel verilerin hukuka ve dürüstlük kuralına uygun olarak işlenmesi ile referans verilen husus, veri sorumlularının verileri işlerken "adil davranmakla" yükümlü olması, yani "haklı menfaat" ve "haklı beklenti" arasında denge kurulmasını sağlamasıdır[329]. Bu nedenle, veri sorumlusu mümkün olan en az miktarda veri işlerken, veri sahibinin çıkarlarını ve beklentilerini gözetmelidir[330].

---

[323] Aysun, s.84.
[324] Oğuz, s.129.
[325] Bazı metinlerde hukuka ve objektif iyi niyet kurallarına uygunluk olarak ifade edilmektedir. Bkz. Başalp, s.37.
[326] Korkmaz, Kişisel Verilerin Korunması, s.100; Başalp, Kişisel Verilerin Korunması, s.37.
[327] Küzeci, s.196.
[328] Develioğlu, s.44.
[329] Küzeci, s.196.
[330] Oğuz, s.132.

Bu ilkelere şeffaflık (açıklık) ilkesi de eklenmiş olup, ilkenin eklenme amacı veri kişisinin verilerinin hangi maksatla işlendiğinin bilinmesini sağlamaktır. Şeffaflık ilkesi Direktif'te ifade edilmese de, GVKT'da ayrıntılı bir şekilde düzenlenmiştir. KVKK'nın 4'üncü maddesinde de ilk olarak bu ilkeye yer verilmiştir[331]. Bu bağlamda, veri işleme süreci şeffaf yürütülmeli; veri işleme sorumluları veri işlemeye başlamadan önce, ilgili kişiyi, veri işlemenin amacı, veri sorumlusunun kimliği ve adres bilgileri gibi hususlarda bilgilendirmeli, kanunun açıkça öngördüğü haller haricinde veri işlemede gizlilik ve üstü kapalılık gözetilmemeli ve ilgili kişiye verilere erişim hakkı tanınması sağlanmalıdır[332]. Özellikle son yıllarda, müşteri bilgilerinin reklam amacıyla dürüstlük kuralına aykırı olarak kullanılmasına yönelik düzenleme getiren bu ilke ile, veri kişisinin kendisi hakkında veri toplayan kişiyi bilmesi, bilgi edinmesi, yanlış bilgileri düzeltmesi ve sildirmesi gibi katılım haklardan faydalanması da kolaylaşmıştır.

Bu bağlamda, kişisel verilerin hukuka aykırı olarak toplanması, kayıt altına alınması ve işlenmesi faaliyeti, aynı zamanda kişinin Anayasa'nın 17'inci maddesi ile teminat altına alınan, maddi ve manevi varlığını koruma ve geliştirme hakkı ile 20 ile 22'inci maddelerinde koruma altına alınan, özel hayatın gizliliği ve korunması hakkının ihlali anlamına gelecektir. Nitekim TCK'nın 135'inci maddesi ile hukuka ve dürüstlük kurallarına uygun olmayan veri işleme faaliyeti, cezai müeyyideye tabi tutulmuştur. Bu ilkenin istisnası, veri sorumlusunun kanun hükmünü yerine getirmesi ya da sözleşmenin ifası gereği verilerin açıklanma zorunluluğudur[333].

3.1.2. Doğru ve gerektiğinde güncel olma

Kişisel verilerin güncel ve doğru olarak işlenmesi, hem veri öznesinin temel hak ve özgürlükleri ile manevi ve ekonomik durumu üzerindeki etkisi hem de veriyi işleyenin kaliteli veriye erişimi açısından önemlidir. Verilerin doğru tutulmaması durumunda ilgili kişinin temel hak ve özgürlükleri ile özellikle ekonomik faaliyet ve manevi bütünlüğüne karşı riskler ortaya çıkmaktadır. Diğer yandan, kişisel verilerin yanlış olması ise veri sorumlusunun çıkarlarını zedeleyecektir[334]. Örneğin; adres bilgileri

[331] Develioğlu, s.44-45.
[332] Aysun, s.84.
[333] Oğuz, s.132.
[334] Korkmaz, Kişisel Verilerin Korunması, s.101; Küzeci, s.208.

yanlış tutulan birine gönderilecek önemli bir tebligatın, üçüncü bir tarafın eline geçmesi ciddi bir zarar oluşturacaktır. Nitekim KVKK'nın 11'inci maddesinde bu denge, ilgili kişi için *"..kişisel verilerin yanlış ya da eksik işlenmiş olması halinde bunların düzeltilmesini isteyebilir"* şeklindeki hükümle düzenlenmiştir.

Bir diğer önemli ilke ise, güncellik olup; güncellik ilkesi ile kişisel verilerin maddi doğruluğunun gerçekleştirilmesi yani verilerin güncel ve doğru olması teminat altına alınmaktadır[335]. Bu bağlamda KVKK, kişisel verilerin doğru ve gerektiğinde güncel olarak tutulmasını veri sorumlusunun devredilemeyecek yükümlülükleri arasında saymıştır. Ancak, verilerin güncelliğinin sağlamasını yapmak için, veri sorumlusu sürekli bir takip faaliyeti içerisinde de olamaz. Bu durum ise verilerin doğruluk ve güncelliğinin belirlenmesini sıkıntıya sokmaktadır. Unutulmamalıdır ki, verilerin güncelliğini denetleyebilecek olan ilgili kişinin kendisidir. Bilgilerine ulaşamayan kişi ise, bu denetim imkânından yoksun kalmaktadır. Bu ilkeye uyumluluğun tesis edilebilmesi için veri sorumlusu, ilgili kişinin bilgilerine ulaşabileceği ve onları denetleyebileceği bir sistem oluşturma çözümüne başvurabilir[336]. Bu nedenle, "gerektiğinde güncel olma" ilkesinin gerçekleştirilmesi için ilave bir düzenleme yapılmasının gerekliliğine vurgu yapılmaktadır[337]. Şahsi kanaatimiz de böyle bir ilave düzenlemenin sistemin doğru ve güncel bilgilerden oluşmasının tesis edilmesi açısından gerekli olduğu yönündedir.

GVKT'de verilerin doğru ve güncel tutulması ile ilgili öne çıkan ve dikkat edilmesi gereken hususlar şu şekilde sıralanmaktadır[338];

- Verilerin ilk elde edilmesi aşamasında veri doğrudan ilgili kişiden rızası dâhilinde ediniliyorsa; söz konusu veri, ilgili kişi tarafından doğru bir şekilde verilmelidir. Bunu kontrol etme yükümlülüğü veri sorumlusu üzerinde olsa her veri için bu ayrı ayrı mümkün olmayacaktır.

- Yanlış veri işlediğini anlayan bir veri sorumlusu GVKT'ye göre yanlış verileri işleneceği amaçlarla ilgili bir gecikme yaşanmasına imkân tanımaksızın silinmesi ya da

[335] Başalp, Kişisel Verilerin Korunması, s.38.
[336] Küzeci, s.220.
[337] Oğuz, s.133'den naklen Bainbridge'in görüşü alınmıştır.
[338] Dülger, Kişisel Verilerin Korunması, s.131.

düzeltilmesi için gerekli girişimleri yapmalıdır. Tüzük düzenlemesi gecikmeyi yasaklamakta ve veri sorumlularına veri varlıklarını daha aktif yönetmeye sevk etmektedir.

- GVKT'ye göre verilerin güncel tutulması doğru tutulmasına göre daha az gerekli olmakla birlikte, "gerektiğinde" ifadesi verilerin kamu ya da özel çıkarları ilgilendiren operasyonları aksatmayacak şekilde tutulması gerekliliğini doğurmaktadır.

Verilerin güncel tutulmasıyla ilgili sorumluluk bariz şekilde veri sorumlularında olmayıp, veri kişisi tarafından en güncel verilerin iletilmesi gerektiği açık olsa da, DÜLGER sorun yaşanmaması adına veri sorumlusunun 6 ay ya da 12 ay gibi periyotlarla elindeki veri varlığını güncelleyecek şekilde veri kişilerine ulaşması gerektiğini önermektedir[339]. Şahsi kanaatim de, doğru ve gerektiğinde güncel olma ilkesinin işleyişi açısından böyle bir yöntemin sorumluluğun doğru paylaşımına katkı sağlayacağı yönündedir.

3.1.3. Belirli, açık ve meşru amaçlar için işlenme

Bu ilkeye göre, veri işleme faaliyeti en başından itibaren belirli, açık ve meşru amaçlar için gerçekleştirilmeli, veri işleme faaliyetinin hedefi belirlenmiş olmalıdır[340]. Dolayısıyla veri sorumlusu, kişisel verileri işlerken amacını açık ve kesin olarak belirlemeli, belirsiz ifadelerden kaçınmalı, veri işleme faaliyetini meşru bir amaca dayandırmalıdır. Amacın meşruluğu, veri toplamanın yasal bir temele sahip olması, hukuki düzenlemelerde öngörülen gerekliliklere uygun olması ve veri işleme faaliyetinin hedefiyle dengeli olmasını ifade etmektedir[341]. Nitekim veri sorumlusu, kişisel verileri belirttiği amaçlar dışında işlerse, bundan sorumlu tutulacaktır[342]. Amaca bağlılık ilkesi, aynı zamanda kişisel verilerin dürüst ve hukuka uygun olarak işlenmesinin denetlenmesine yönelik tamamlayıcı ilke niteliğini de haizdir[343].

Bununla birlikte, kişiler verilerin işlenmesi için alınan rıza belirli bir ya da iki amaçla sınırlı olmalı ve bu amaç en geç veri toplanırken belirlenmiş olmalıdır. Mevcut durumda

[339] Dülger, Kişisel Verilerin Korunması, s.133.
[340] Aydın, s.113.
[341] Küzeci, s.199.
[342] Korkmaz, Kişisel Verilerin Korunması, s.101.
[343] Ketizmen, s.225.

olmayan ve gelecekte ortaya çıkabilecek amaçlar için veri işlenemez. Buradan hareketle, her yeni amaç için belirlilik, açıklık ve meşruluk kriterlerine bir kez daha uyulması ve muhakkak yeni bir rızanın alınması gerekliliğine ulaşılmaktadır[344]. Meşruluk ise, kamu menfaatinin bulunması ve kişi hak ve özgürlüklerini ilgilendirmesi ile sağlanmaktadır. Örneğin; bir havayolu firması yolcularının daha sağlıklı bir yolculuk geçirmesi için koltuk numarası, engelli yolcu bulunup bulunmadığı, alkollü içecek ya da helal yiyecek tercihlerine uygunluk amacıyla bu bilgileri talep edebilirken, bu bilgilerin gidilen ülkenin göçmen bürosu tarafından talep edilmesi mümkün olmayıp, yeni ve ayrı bir hukuki temele dayandırılması gerekir[345].

Bu bağlamda, bir diğer çarpıcı örnek ise AİHM'nin Peck v. B. Krallık kararıdır[346]. Buna göre, başvurucu güvenlik kamerası tarafından kaydedildiğini bilmeden sokakta bileklerini kesmek istemiş ancak durumu fark eden polisler tarafından kurtarılmıştır. Bu olayın medyada aktörlerin yüzleri sansürlenmeden kullanılması üzerine, başvurucu durumu mahkemeye intikal ettirmiş ve mahkeme bu görüntülerin doğrudan ifşa edilmesinin meşru bir amaca dayanmadığını belirterek, Sözleşme'nin ihlâl edildiğine karar vermiştir.

Görüldüğü üzere, belirlenen amacın sonradan değiştirilmesi ancak açıklanan amaçla uyum gösterdiği sürece uygunluk kazanabilecektir[347]. Bu durum değerlendirilirken, koşullar tüm yönleriyle dikkate alınmalıdır. Bu bağlamda, kişisel verinin toplanması amacı ile ilerdeki işlem amaçları arasındaki ilişki; kişisel verilerin toplandığı bağlam ve veri konularının ilerideki kullanımlarına ilişkin makul beklentileri; kişisel verilerin doğası ve veri konularıyla ilgili diğer işlemlerin etkisi; veri kişileri üzerinde herhangi bir uygunsuz etkinin oluşmasını engellemek amacıyla adil işlemeyi sağlamak için veri sorumlusu tarafından benimsenen güvenceler göz önünde bulundurulmalıdır. Dolayısıyla, son tahlilde belirleyici olan somut olaydan hareketle yorum ilkesi olup, nitekim Direktif açısından da her bir somut olayda amaçlar arasında ilişkinin incelenmesi ve "uyumluluk" tespit edilmesi tavsiye edilmektedir[348]. Ayrıca, kişisel

[344] Oğuz, s.134; Başalp, Kişisel Verilerin Korunması, s.38.
[345] Aysun, s.85-86.
[346] "Case of Peck v. The United Kingdom", Başvuru No: 44647/98, 28.1.2003, https://www.5rb.com/wp-content/uploads/2013/10/Peck-v-UK-ECHR-28-Jan-03.pdf, (Erişim Tarihi): 14.04.2019.
[347] Başalp, Kişisel Verilerin Korunması, s.38.
[348] Dülger, Kişisel Verilerin Korunması, s.123.

veriler toplanırken ortaya çıkabilecek ve başlangıçta olmayan bir amaca dönük toplama yasağının "ölçülülük" ilkesi kapsamında değerlendirilmesi gerektiğini belirtmektedir[349]. Direktif ise üye devletlerin uygun önlemleri almaları şartıyla kişisel veriler tarihsel, istatistik ve bilimsel amaçlarla sonradan işlemelerine istisna tanımaktadır[350].

Bir diğer önemli husus ise, amaçların ayrıntı seviyesidir. Diğer hususları göz önünde bulundurmak şartıyla, amaçların ayrıntı seviyesini belirlemek için dikkat edilmesi gereken faktörler DÜLGER tarafından, veri öznesinin sayısı, coğrafi alan, farklılıkların (yaş, cinsiyet) yönetilebilmesi için amaçların daha net şekilde belirlenmesi; veri işlemi geleneksel olanı aşma durumundaysa, daha fazla ayrıntıya ihtiyaç olması; veri işleme amacı alt amaçlara ayrılarak, amacın anlaşılabilirliği arttırılmalısı; katmanlı mahremiyet bildirimleri ile veri öznelerine "öz" düzeyinde ve kullanıcı dostu şekilde anahtar bilgiler verilmesi ve bu sayede şeffaflık sağlanması olarak sıralanmaktadır[351].

KÜZECİ'nin önemle altını çizdiği konu ise, bu ilkenin etkin bir şekilde uygulanabilmesi için veri sorumluluklarının yükümlülüklerinden önce yasal düzenlemelerin amacının belirli ve açık olması gerekliliğidir. Çünkü açık ve belirli tanımlanmamış bir çerçevede veri sorumlularının ilgili ilkeye uygun hareket etmeleri beklenemeyecektir. Böyle bir durum veri sorumlusunu hali hazırdaki sınırlı ilkelerden hareket etmek zorunda bırakacaktır ki, bu da ilkenin doğru şekilde hayata geçirilmesini engelleyecektir[352]. Dolayısıyla, öncelikle mevzuat bu ilkelere uygun olmalı yani yasal düzenlemeler aracılığıyla kanun hükümleri açıklığa kavuşturulmalıdır.

3.1.4. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma

"Veri minimizasyonu" ya da "verilerin asgarileştirilmesi" olarak da ifade edilen[353] bu kavram, Direktif'te *"toplandığı ve/veya ayrıca işlendiği amaçlara ilişkin olarak yeterlidir, ilgilidir ve bu amacı aşamaz"* şeklinde düzenlenirken, GVKT'da ise, *"işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanlar sınırlıdır"*

[349] Akdağ, s.78.
[350] Korkmaz, Kişisel Verilerin Korunması, s.102.
[351] Dülger, Kişisel Verilerin Korunması, s.118.
[352] Küzeci, s.209.
[353] Oğuz, s.134.

şeklinde ifade edilmektedir[354]. KVKK'da ise, kişisel verilerin "*işlendikleri amaçlar bağlantılı, sınırlı ve ölçülü olma"* ilkesi olarak ifade edilmiştir. Burada işaret edilen hususlar; veri işleme faaliyetinin amaçla bağlantısı bulunması, işlenen kişisel veri ile işleme hedefi arasında illiyet bağı bulunması ve hedefe ulaşmak için ilgili kişisel veriyi işlemenin gerekli olmasıdır[355]. Dolayısıyla, amaçları gerçekleştirmeye imkân tanıyan kişisel veriler işlenmeli, amaçla ilgisiz ya da amacın gerçekleştirilmesine hizmet etmeyecek kişisel veriler işlenmesinden kaçınılması gerekmektedir[356]. Şayet kişisel veriler toplanma nedeninden başka bir amaç için kullanılacaksa, bunun yasal ve meşru bir temele sahip olması gerekmektedir[357].

Bu bağlamda, veri sorumluları kişisel veri toplama faaliyetine başlamadan önce verilerin kullanılma gerekliliğine bakmalı, kişisel verilerden amacına ulaşmasına yetecek kadarını toplayarak işlemeli ve gereğinden fazla veri toplamamalıdır[358]. Veri sorumlularının bu ilkelerle uyum içerisinde hareket edip etmediklerini belirleyebilmeleri için iki aşama söz konusudur. Bunlardan ilki, ilgili amaç veya amaçların tespit edilmesidir. Buna göre "veri sorumlusunun ulaşmak istediği hedef nedir ve bu hedefe ulaşmak için hangi kişisel veri işleme faaliyetlerini yerine getirmelidir?" sorusuna doğru cevap verilmelidir. İkinci aşamada ise amaçlar belirlendikten sonra her bir işleme aktivitesinin ne kadar gerekli olduğunun tespit edilmesidir. Veri sorumlusu, bu tespitleri dışında kalan amaçları yerine getirmek için gerekli olmayan herhangi bir veriyi toplar ya da kullanırsa ilke, ihlal edilmiş olacaktır. Dolayısıyla, kişisel verinin hangi amacın gerçekleştirilmesine yönelik olduğu açıklanmışsa veri sorumlusu bu amaç için yeterli olduğu noktada işleme faaliyetini sınırlamalıdır[359]. İlke gereği belirlenen amaca kişisel verilerin işlenmesi dışında bir araçla ulaşılabiliyorsa, öncelikle bu araçların tercih edilmesi tavsiye edilmektedir. Ayrıca, bu araçlar kişisel verilerin korunmasının hedefi olan temel hak ve özgürlüklere daha az müdahil oluyor ya da hiç müdahale etmiyorsa, bu da onlara öncelik tanınmasını gerektirmektedir[360]. Ancak, veri işleme bir mecburiyetse, bu durumda da en az sayıda veri işlenmeye dikkat edilmelidir.

---

[354] Oğuz, s.12.
[355] Aysun, s.87.
[356] Korkmaz, Kişisel Verilerin Korunması, s.103.
[357] Küzeci, s.208.
[358] Akgül, Kişisel Verilerin Korunması, s.158.
[359] Dülger, Kişisel Verilerin Korunması, s.127.
[360] Oğuz, s.134.

3.1.5. İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar saklanma

KVKK'nın 4'üncü maddesinde yer alan bu ilkeye göre kişisel verilerin gerektiğinden daha fazla kayıtlı bulundurulmaması ve saklanmaması gerekmektedir. Kişisel verilerin saklanması, ulaşılmak istenen amaç gerçekleşene kadar hukuka uygun sayılacaktır[361]. Buna göre, bir amaçla ilgili olarak toplanan kişisel veriler, bu amaç sağlandığında, kanuni bir zorunluluk söz konusu değilse, daha fazla bulundurulmamalı, imha edilmeli, imha edilmese bile, kişinin kimliği ile arasındaki bağlar koparılmalıdır. Anonimleştirme olarak ifade edilen bağların koparılması, kişisel verilerin belirli alanlarının silinerek ya da yıldızlanarak kişinin belirlenemez hale geldiği "maskeleme" ya da verinin "başka adlar altında toplanması" olarak kullanılabilir. Bu durum aynı zamanda kişilerin "unutulma hakkı" ile doğrudan ilintilidir ve yerine getirilmediğinde hukuka aykırılık söz konusu olacaktır. Kişisel verilerin gelecekte yararlanma ihtimaline binaen saklanması da, bu hukuka aykırı durumun bir parçasıdır. Dijitalleşmenin hızla arttığı ve beraberinde dijital riskleri gündeme getirdiği bu dönemde bu verilerin öngörülen süreden daha fazla depolanması aynı zamanda veri sorumlusu adına da önemli bir sorumluluk doğurmaktadır[362].

Kişisel verilerin işlenme sürelerinin belirlenmesinde kural olarak kanunlarda yazılı olan sürelerin dikkate alınması gerekli olup, bunun dışında kalan alanlarda Kişisel Verilerin Korunması Kurulunun aldığı ilke kararı ile de süre belirlenebilmektedir. Ancak böyle bir sınırlama söz konusu değilse, veri sorumlusu verileri ancak işlediği amaçla sınırlı olan süreyle saklayabilmektedir[363]. KVKK'nın 16'ıncı maddesine göre, veri sorumluları verileri saklama süresini bildirmekle yükümlü olup, azami süre, verinin mevcut ve gelecekteki değeri, saklama ve güncellemeyi sürdürme durumunda oluşacak maliyet ve risk ve sorumluluğu gibi faktörler göz önünde bulundurularak belirlenir[364]. Kişisel verilerin saklanacağı süre ile ilgili olarak bir diğer düzenleme ise, 28 Ekim 2017 tarihli

[361] Başalp, Kişisel Verilerin Korunması, s.39.
[362] Aysun, s.87-88.
[363] Küzeci, s.203; Develioğlu, s.49.
[364] Oğuz, s.135.

"Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" olup, bu yönetmelikle, amaç için verileri ne kadar süreyle saklanacağına dair kuralın uygulanması sağlanmaya çalışılmıştır[365].

3.1.6. Hesap verebilirlik ve sorumluluk

Yukarıda sayılan ilkelere, Direktif'in 5'inci maddesinin 2'inci fıkrasıyla getirilen hesap verilebilirlik (accountability) ilkesi de ilave edilebilir. Bunun nedeni, yukarıda da belirtildiği üzere bazı ilkelerin diğer ilkelere kaynaklık etmesi ve diğer bir ilkenin onun için tamamlayıcı role sahip olmasıdır. Buna göre KVKK'da düzenlenmeyen, dolayısıyla birebir karşılığı olmayan verilerin *bütünlük ve gizlilik* içinde işlenmesi ile *sorumluluk* ilkeleri GVKT'da düzenlenmiştir[366]. Bütünlülük ve gizlilik ilkesinde amaç; kaybolma, yetkisiz kişilerin erişimi, tahrip, kullanma, değiştirilme, ifşa gibi işlemlere karşı güvenlik tedbirlerinin alınmasıdır. Bu bağlamda, veri sorumluları ve veri işleyenlerden kişisel verilerinin korunmasına yönelik kurumsal politikalar geliştirmesi, teknik ve organizasyonel tedbirler alınması, yüksek riskli işletmeler için öz denetim mekanizmaları kurmaları talep edilmektedir. Örneğin; bir sağlık işletmesinin bünyesindeki özel nitelikteki kişisel verileri korumaya yönelik kurumsal bir politika geliştirmesi ve kişisel verileri "maskeleyerek" sınıflandırması ya da bir bilginin sadece hastayla ilgilenen sorumlu kişilerin erişimine açık olması bu önlemler arasında sayılabilecektir[367].

Sorumluluk ilkesi ise, veri sorumlusu ve veri işleyenin ilgili ilkelere uygun hareket etme yönünde sorumluluk taşıdığını ve bu yönde hareket ettiğini gösteren bir ilkedir. Bunun en önemli göstergesi ise kurumsal tedbirlerin alınması ve bu tedbirlere ilişkin kayıtlar oluşturulmasıdır. Bu ilkeyi benimsemiş kurumlar, veri sorumluları ve veri işleyenlere karşı idari yaptırımlar öngörmektedir[368].

[365] R.G. 30224, 28.10.2017.
[366] Oğuz, s.129.
[367] Develioğlu, s.50.
[368] Develioğlu, s.51.

3.2. Kişisel Verilerin İşlenmesinin Hukuka Uygunluğu

KVKK'nın 5'inci ve 6'ıncı maddelerinde kişisel verilerin işlenmesinde hukuka uygunluk halleri düzenlenmiş olup, buna göre kural olarak kişisel verilerin ilgili kişinin açık rızası olan durumlar ya da bazı istisnalar dışında işlenmesi hukuka aykırıdır. Dolayısıyla, öncelikli olarak bir hukuka uygunluk göstergesi olan (açık) rızanın varlığı ele alınacaktır.

3.2.1. Açık rıza

Kişisel verilerin işlenmesinde esas olan, işleme faaliyetinin hukuka uygun olmasıdır. Bu bağlamda, kural olarak verileri işlenen kişinin verilerinin işlenmesine rıza göstermesi gerekmektedir[369]. Rıza, Direktif'te *"kendisine dair kişisel verilerin işlenmesi için veri öznesinin kabulüne işaret eden, özgürce ve bilgilendirme yapıldıktan sonra alınan beyan*" olarak tanımlanırken, kişisel verileri koruma hukukunda en güncel metin niteliğindeki GVKT'nın 4/11'inci maddesinde ise, "*kendisi ile ilgili kişisel verilerin işlenmesine yönelik olarak veri öznesinin bir beyan veya net biçimde onay ifade eden bir işlemi vasıtası ile özgürce verilmiş, spesifik, bilgilendirmeye dayalı ve açık kabul"* olarak ifade edilmiştir. KVVK'da ise açık rıza, "*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*" olarak tanımlanmaktadır. Her iki uluslararası metinle kıyaslandığında, açık rızanın tanımı çok daha genel bir şekilde yapılmaktadır[370].

Bu bağlamda, KVKK'nın 3'üncü maddesinde açık rıza, hem özel hem de genel nitelikli kişisel verilerin işlenmesinin hukuka uygun hale getirilmesi için şart koşulmaktadır. Ancak önemle altı çizilmelidir ki, veri öznesinin rıza göstermesi veri işleme faaliyetini hukukileştirse de, bu rıza veri işleme faaliyetinde belirleyici olan ilkelerden feragat edilmesi anlamına gelmeyecektir. Bu bağlamda, kişisel verilerin işlenmesinde ilgili kişinin usule uygun açık rıza göstermesinin işlemenin baştan hukuka uygun hale gelmesinin yeterli olacağı kabul edilirken[371], ilgili kişinin rızası en önemli meşruiyet

[369] Başalp, Kişisel Verilerin Korunması, s.39.
[370] Aysun, s.89.
[371] Develioğlu, s.51.

şartı olarak belirtilmektedir[372]. Diğer yandan, kişisel verilerin işlenmesi yasağının uygulama alanını daraltan en kapsamlı unsurun ilgili kişinin verilerinin işlenmesine karşı rızası olduğunun altını çizilmektedir[373]. Daha önceki bölümde belirtildiği üzere, kişisel verilerin işlenmesinde hukuki meşruiyet sağlanması için, ilgili kişinin rızası en önemli unsur olduğu ancak bazı durumlarda hukuka uygunluğun tek başına teminatı olamayacağı yönündeki görüşe katılıyorum.

Bu bağlamda, kişisel verilerinin işlenmesine yönelik ilgili kişi tarafından verilen rızanın "açık rıza" niteliğini haiz olabilmesi için; rızanın serbestçe verilmesi, bir konuya özgü olması, kişinin aydınlatılmasına dayanması ve kişi tarafından şüphe olmaksızın kabul edilmesi gerekmektedir. Açık rıza, bu yönüyle aynı zamanda, kişisel verilerin "amaçla bağlılık" ilkesine uygun işlenmesinin de teminatı niteliğindedir[374]. Ancak rıza, genel olmamalı, konuya özel ve aydınlatmaya dayalı olmalıdır. Özellikle, belirli veya belirlenebilir bir işleme faaliyetine yönelik rızada bu husus belirtilmelidir. KVKK'nın 10'uncu maddesi bu doğrultuda bir düzenleme içermekte olup, buna göre veri sorumluları, kişisel veri paylaşımının kapsamı ve sonuçlarından ilgili kişileri aydınlatmakla yükümlüdür. Bilgilendirme metninde yer alması gereken bilgiler ise; veri sorumlusunun kimliği, verinin hangi amaçla ne kadar süre işleneceği, kimlere hangi amaçla aktarılabileceği, kişisel verileri toplama yöntemi ve hukuki sebebi gibi hususlar olmalıdır. Ancak, somut olayın özelliği doğrultusunda bilgilendirmede yer alması gereken hususlar bunlarla sınırlı olmayabilir[375].

Yine açık rıza, veri işlenmeye başlanmadan önce alınmalıdır. Yazılı olması zorunlu olmamakla birlikte, rızanın anlaşılır, yalın ve güncel sözcükler kullanılarak alınması gerekmektedir. Nitekim KVKK, rızayı bir şekil şartına bağlamamış olup, özgür iradeyle, açık ve şüpheye yer bırakmayacak şekilde açık olması durumunda sözlü, yazılı ya da elektronik ortamda alınabilmektedir[376]. Ancak, *"Kişisel verilerimin işlenmesini onaylıyorum/kabul ediyorum*" ya da *"Bütün kişisel verilerimin her türlü konuya ilişkin işlenmesine rıza gösteriyorum"* gibi genel ifadeler KVKK'nın aradığı niteliği haiz

[372] Küzeci, s.240.
[373] Başalp, Kişisel Verilerin Korunması, s.39.
[374] Akdağ, s.34.
[375] Yücedağ, s.774.
[376] Develioğlu, s.51.

değildir. Veri ilgilisinin veri sorumlusuna olumlu cevap vermesi de geçerli bir rıza talebi olmayacaktır. Bu nedenle hangi bilgilerin hangi konu için işlenebileceği rızada açıkça belirtilmelidir[377].

Örtülü beyanın yeterli olup olmadığı ise bir başka tartışma konusu olup, KÜZECİ ve KORKMAZ bu noktada şüpheye yer bırakmayacak kadar veri sahibinin iradesini ortaya koyan örtülü beyanın rıza olarak kabule yeterli olduğunu belirtmekteyken[378]; TAŞTAN ise, özel nitelikli kişisel veriler açısından örtülü beyanın açık rızanın kabulü anlamına gelmeyeceğini belirtmektedir[379]. Benim görüşüm, kişinin rızasını ne için verdiğini açık bir şekilde göstermesi gerektiği yönünde olup, bazı hizmetlerin doğası gereği örtülü beyanın açık rıza anlamına gelebileceğini kabul etmekteyim.

Diğer yandan, kişinin sessiz kalmasının kişisel verisinin işlenmesine onay verdiği anlamına gelmediği unutulmamalıdır. Buna göre, açık rıza gerektiren bir durumda ilgili kişinin susması kabul değil, ret olarak yorumlanmalı[380]. Kişinin sorulan sorular karşısında hareketsiz kalması ise bir rıza göstergesi sayılmamalıdır[381]. Bu durumda, örneğin, internet ortamında verilen rıza beyanları da tartışmaya açıktır. Buna göre, bir web sitesi ya da aplikasyonun bilgilendirme metninde yer alan bilgiler aşırı uzun, kapalı, site içerisindeki yönlendirmeleri zorlaştıran veya aşırı teknik bir dille yazılmışsa, bu durum daha zayıf bir koruma öngörmekte ve AB mevzuatına göre rıza beyanı geçersiz sayılmaktadır[382]. Ayrıca Kişisel Verileri Koruma Kurumu, sözleşmelerde ilgili kişilerin anlayamayacağı terimlerin kullanılması ya da rızanın yazılı istenmesi durumunda metinlerin 12 puntodan küçük olmasını da kabul etmemektedir[383].

Ayrıca, kişisel verinin üçüncü bir kişi ile paylaşılması ya da yurtdışına aktarılması söz konusuysa, ilgili kişinin yeniden rızasının alınması gerekmektedir[384]. Açık rıza kavramı, hem özel nitelikli (hassas) hem de genel nitelikteki kişisel verilerin işlenmesi için şart

[377] Uncular, s.144.
[378] Küzeci, s.222; Korkmaz, Kişisel Veriler ve Ceza, s.45.
[379] Taştan, s.156.
[380] Küzeci, s.221.
[381] Uncular, s.144.
[382] Korkmaz, Kişisel Verilerin Korunması, s.108.
[383] Aşıkoğlu, s.120.
[384] Erdinç, s.21.

niteliğinde temel kuraldır[385]. Ancak, genel nitelikteki kişisel verilerin işlenmesinde genel bir rıza beyanı aranırken, hassas verilerin işlenmesinde "açık rıza" beyanı gerekmektedir[386].

Açık rızaya ilişkin bir başka şart ise, veri kişisinin beyan esnasında hiçbir baskı altında bulunmaması, veri işleme faaliyetinin amacı ve sonuçları hakkında açıkça bilgilendirilmesi ve rıza beyanının sonuçlarının makul ölçüde somutlaşmış olmasıdır. Ancak, özellikle sağlık sektöründeki veri talepleri ile işçi-işveren ilişkisinden kaynaklı veri paylaşımında "açık rıza" kavramının tehdit altında olduğu görülebilmektedir. Özellikle, işçi-işveren ilişkisinde beyandan kaçınmak ya da rıza vermemek haksız iş akdi feshine neden olmakta, dolayısıyla işçiler bunun korkusuyla özgür iradesi olmaksızın beyan vermektedir. Bu nedenle, işverenler tüm işçilerine eşit ve açık bir biçimde rıza gösterme hakkı tanımalı ve rıza göstermedikleri takdirde olumsuz sonuçlarla karşılaşmayacakları konusunda garanti vermelidir. Ancak işverenin Kanun'dan doğan işleme hakkı söz konusuysa (Örn; özlük dosyasındaki verilerin işlenmesi, iş sağlığı ve güvenliği ile iş yerinin ve işin kontrol, deneyim ve güvenliğini sağlamak amacıyla sesli ve görüntülü kayıt sistemleri kurulmasına yönelik parmak izi, retina taraması vb. yapılabilmesi), işçinin açık rızasına ihtiyaç duymayabileceği bilinmelidir. İşçi buna rağmen açık rıza vermiyorsa, işçinin haklı olduğu söylenemeyeceği gibi, işçi-işveren ilişkisinin sürmesi de beklenemeyecektir[387].

Diğer yandan, sağlık sektöründe ise, karşı tarafından talep ettiği verileri paylaşmadığı taktirde eksik tedavi görme, tedavi görmeme ya da önyargıya maruz kalma çekincesi öne çıkmakta olup, bu da açık rıza şartları üzerinde bir risk faktörü olarak belirmektedir. KVKK'nın 6/3'üncü maddesi ile kişinin sağlığı ve cinsel hayatına ilişkin kişisel veriler açısından açık rıza kuralına dair bir istisna daha söz konusudur. Buna göre bu veriler kamu sağlığını doğru planlamak, finanse etmek, yönetmek; koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi adına sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurumlarca işlenebilmektedir[388]. Bu bağlamda, *Z. v.*

[385] Oğuz, s.131.
[386] Başalp, Kişisel Verilerin Korunması, s.44.
[387] KVKK, s.27.
[388] Dülger, Ceza Normu, s.145-146.

Finlandiya kararında bu tür verilerin korunmasının sahip olduğu ayrı öneme dikkat çekilmiştir. Bu kararda, başvurucunun eski eşi HIV virüsü taşımakta olup, başvurucunun eski eşine cinsel saldırısı nedeniyle kamu davası açılmıştır. Bu doğrultuda, doktorlardan tıbbi veri talep edilmiş ve bu veriler dava dosyasına dahil edilmiştir. Temyiz mahkemesi de bu verilere dosyada yer verilmesini uygun bulmuş ve AİHS'nin 8'inci maddesinin ihlal edilmediğine karar vermiş ancak kararın üzerinden on yıl geçmeden açıklanması yasaklanmıştır[389].

Burada temel gerekçe, bu tip hassas verilerin açıklanmasının bireyin toplumdan dışlanmasına kadar varabileceği olup, kişinin özel yaşamı ile kamu yararı arasında ince bir denge tesis edilmesi gerektiğidir. Ancak, Helsinki Temyiz Mahkemesi ise, bu verilerin on yıl sonra kamuya açılacak olmasının başvurucunun, özel ve aile yaşamına saygı hakkının aleyhine ölçüsüz bir müdahale olduğuna işaret etmiştir[390]. Ayrıca, sağlık çalışanları mesleğini uygularken öğrendiği sırları, sır saklama yükümlülüğü gereği saklama zorunluluğuna sahip olup, hastanın ölümü halinde bile bunlar saklı kalmalı ve ifşa edilmemelidir[391].

Çocukların açık rızası Direktif'te ilk kez uluslararası boyutta ele alınırken, çocukların rıza talebiyle karşılaşması durumunda rıza ehliyeti ancak en az 16 yaşında olan çocuklara tanınmıştır. Dolayısıyla, hukuka uygunluğun sağlanması için çocuğun en az 16 yaşında olması gerekmekte ya da velayet sahibi kişilerin izin veya rızası gündeme gelmelidir. KVKK'da bu konuda herhangi bir hüküm bulunmamakta olup, bu düzenleme ihtiyacı olan bir alana işaret etmektedir[392]. Şahsi kanaatim, dijital medyada çocuklara yönelik istismarların bu kadar genişlediği bir dönemde bu boşluğun giderilmesi yönünde olacaktır.

Son olarak, açık rızanın geri alınıp alınamayacağı bir başka sorun alanını oluşturmaktadır. Kişinin kendi verileri üzerinde hâkimiyet kurabilme ve verilerinin geleceğini belirleyebilme hakkı ışığında, verilerinin işlenmesini durdurma talebinin yerine getirilmesi en temel hakları arasındadır. Ancak, bu haklar ileriye doğru

---

389 "Case of Z v. Finland", Başvuru No: 22009/93, 25.1.1997, http://www.worldlii.org/eu/cases/ECHR/1997/10.html, (Erişim Tarihi): 14.04.2019.
390 Aydın, s.115-116.
391 Güven, Vesile: Sağlık Hukukunda Tıbbi Kayıtların Tutulmasından ve Saklanmasından Doğan Sorumluluk, Ankara 2016, s.99.
392 Sarıusta, s.38.

işleyebilmektedir. İlgili kişi böyle bir talep geliştirdiğinde KVKK'nın yürürlüğe girdiği 7 Nisan 2016 tarihinden daha önceden kaydedilen verilerden hareketle oluşacak sonuçlar engellenemez. Çünkü ilgili kayıtlar işlenirken bu rıza alınmıştır. Bu nedenle veri sorumlusu rızanın geri alınması yönündeki beyan kendisine ulaştığı andan itibaren veri işleme faaliyetlerini durdurmak zorundadır. Durdurmadığı takdirde idari yaptırım gündeme gelecektir[393]. KVKK yürürlüğe girdiği tarihten sonra işlenecek veriler Kanun'un öngördüğü şekilde işlenmelidir. Bununla beraber KVKK'nın yayımından önce işlenmiş olan veriler ise yayım tarihinden itibaren iki yıl içinde Kanun hükümlerine uygun hale getirilmelidir. Buna göre, 7 Nisan 2018 tarihine kadar hukuka aykırı olarak işlenmiş verilerin hukuka uygunluğunun sağlanması talep edilmiştir. Diğer yandan Kanun'un yayın tarihinden itibaren veri kişisinin rızası Kanun'a uygun şekilde alınmışsa ve bir yıl içerisinde ilgili kişinin aksi yönde bir irade beyanı yoksa bu veri geçerli sayılacaktır[394].

3.2.2. Diğer hukuka uygunluk halleri

İlgili kişinin rızası olmamasına rağmen yapılan işlemenin hukuka uygun olacağı haller yani özel nitelikteki kişisel verilerin işlenmesi yasağının istisnaları, KVKK'nın 5'inci maddesinin 2'inci fıkrasında belirtilmiş olup; *"(..) Aşağıdaki şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür"* ifadelerine yer verilmektedir. Bu şartlar şöyle sıralanmaktadır[395];

- *Kanunlarda açıkça öngörülmüş olması;* KVKK 5'inci maddede yer alan gerekçede, bu duruma örnek olarak 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun 5'inci maddesindeki şüphelilerin parmak izlerinin alınması ya da 5352 sayılı Adli Sicil Kanunu uyarınca Adalet Bakanlığı'nın kişilerin ceza mahkûmiyet bilgilerini işlemesi verilmiş olup, burada kanunlarda açıklıkla öngörülmüş olması hukuka uygunluk sebebidir. Ayrıca, kanunlardan yetki almamış herhangi bir yönetmelik ile veri işlemesi de Anayasa'ya aykırılık teşkil edecektir[396]. KÜZECİ ise, KVKK dışında başka yasalarda konuya ilişkin açıkça

[393] KVKK, s.29; Aysun, s.89.
[394] Yücedağ, s.770.
[395] Develioğlu, s.58.
[396] Aşıkoğlu, s.122-124.

düzenleme şartına dikkat çekmekte ve genel bir yetkinin meşru işleme nedeni olmayacağını belirtmektedir[397]. Veri işlemenin KVKK dışında diğer kanunlarda da çerçevesinin tam olarak çizilmesi yönündeki eğilimi doğru bulmaktayım.

- *Fiili imkânsız nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması;* Direktif ile paralellik arz eden bu düzenleme ilgili kişinin rızasını açıklayamayacak olması ya da rızasına sonuç bağlanamayacak olması durumunda kişisel verilerinin işenebileceğini kabul etmektedir[398]. Bu haller KVKK'da; kişinin bilincinin yerinde olmaması, akıl hastası olması ya da tıbbi müdahale esnasında kan grubu veya ameliyat öncesi kullandığı ilaçların işlenmesi olarak somutlaştırılmıştır. Buna göre yaralanan ve yanında kimse bulunmayan bir hastaya doktora müdahale etmesinde üstün nitelikte özel yarar bulunmaktadır[399]. Ancak, bu verilerin özel nitelikli kişisel verileri içermesi nedeniyle KVKK'nın 8'inci maddesinin nasıl yorumlanacağı konusunda belirsizlik doğmakta olup, bu örneklerin sehven mi yoksa bilinçli olarak mı belirtildiği hususu netleştirilmeye ihtiyaç duymaktadır. Bu bağlamda, hukuka uygunluğun sabit olabilmesi için fiili imkansızlık ya da ilgili kişi veya üçüncü kişinin hayatı ya da beden bütünlüğünün korunması için gerekli olan hallerin tespiti önem kazanmaktadır[400]. Bu bağlamda, sağlık verilerinin işlenmesi KVKK'nın 6'ıncı maddesi uyarınca bu başlıkta yazılandan farklı bir usule tabi tutulmalıdır[401].

- *Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması;* Veri sorumlusunu, sözleşme öncesinde ya da sözleşme esnasında ilişkide olduğu ya da ileride olabileceği kişi ile ilgili gerekli bilgilere (ödeme gücü, krebilitesi, uzmanlık alanı, iş ahlakı vb.) erişmesi durumunda oluşabilecek

[397] Küzeci, s.345.
[398] Korkmaz, Kişisel Verilerin Korunması, s.109.
[399] Sert, s.122.
[400] Aşıkoğlu, s.126.
[401] Küzeci, s.346; Sağlık verilerinin işlenmesinin şartları sonraki başlıklarda ele alınacaktır.

risklere karşı korumayı amaçlayan bu hüküm[402], KVKK'nın 5/2'inci maddesine kendisine yer bulmuştur. Bu doğrultuda, sözleşme kurulmaz ise bu veriler imha edilmeli ya da ilgili kişiye iade edilmelidir. Bu bağlamda, bir sigorta şirketinin poliçe göndermek için ilgili kişinin adresini talep etmesi, hukuka uygunluk arz ederken, sağlık bilgilerine erişmesi ise açık rızaya tabidir. Diğer yandan, bu verilerin harici danışman, dağıtıcı, tedarikçi gibi üçüncü kişilere aktarılması durumunda da hukuka uygunluk devreye girmekte olup, müşterisine sattığı malı teslim etmesi için kargo şirketine müşterinin adresini vermek, buna en uygun örnektir[403].

- *Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması;* KVKK'nın 5/a maddesi uyarınca, veri sorumlularının hukuki yükümlülüklerini yerine getirmeleri için kişisel verileri işlemeleri zorunluysa bu durum veri işleme faaliyetine hukuka uygun hale getirmektedir. Kanun'un gerekçesinde bu hallere işverenin maaş tespiti için, çalışanının medeni durum, sosyal sigorta numarası, banka hesap numarası gibi verilerini işlemesi ya da vergi denetimi sırasında müfettişlere çalışanları ve müşterilerine ilişkin bilgileri sunmak zorunda olması, örnek olarak gösterilmektedir[404]. Bu bağlamda, özel nitelikli kişisel verilerin veri sorumlusunun hukuki yükümlülüğü kapsamında işlenmesi hukuka uygunluk sebepleri arasında gösterilmemektedir[405]. Bununla birlikte, mahkeme tarafından talep edilen bir bilgi hukuki yükümlülük kategorisine girse de, zorunlu ve talep edilen belgelerin dışında fazla bilgi ve belge sunulması hukuka aykırılık teşkil etmektedir. Bu doğrultuda, Yargıtay 12'inci Hukuk Dairesi bir kararında borçlu bir şirketin telefon numarası, adresi, çek hesabı dışında hesap bilgileri, borçlu ortaklarının hesap bakiye bilgilerinin 2004 sayılı İcra ve İflas Kanunu'nun 367'inci maddesinde yer alan[406], *"İcra ve İflas dairelerinin borçlunun mevcuduna dair isteyeceği bütün malumatı hakiki*

[402] Başalp, Kişisel Verilerin Korunması, s.41.
[403] Develioğlu, s.60-62.
[404] Başalp, Kişisel Verilerin Korunması, s.41.
[405] Aşıkoğlu, s.129.
[406] R.G.: 2128, 19.06.1932.

ve hükmi her şahıs derhal vermeğe ve talep halinde mevcudu bu dairelere teslime mecburdur" hükmü kapsamında istenemeyeceği hükmüne varmıştır[407].

Şüphesiz veri sorumlusu hukuki yükümlülük kapsamında olsa bile kişisel verilerin işlenme amacı ile bağlantılı olarak gerekli süre kadar saklanması ilkesine uymalıdır.

- *İlgili kişinin kendisi tarafından alenileştirilmiş olması;* KVKK'ya göre, veri sahibi tarafından kamuya açıklanmış yani alenileştirilmiş olması durumunda genel nitelikli kişisel verilerin işlenmesi hukuka uygun olarak kabul edilmektedir. Dolayısıyla, burada korunması gereken bir hukuki yararın bulunmadığı belirtilmektedir. Diğer yandan, doktrindeki tartışmalara göre; bir verinin veri sahibi tarafından alenileştirilmesi, veriye ve ilgili kişiye dair koruma alanını ortadan kaldırmamaktadır[408]. DÜLGER de, kamuya mal olmuş kişiler istisna olmak üzere, kişinin verilerini alenileştirmesinin herkes tarafından kullanılmasına açık rızası olması anlamına gelmeyeceğini belirtirken, karşıt görüş olarak KARAGÜLMEZ ise verilerini paylaşan kişinin bunun başkalarınca da paylaşılmasına rıza gösterdiğine atıfta bulunmaktadır[409]. Nitekim Yargıtay'ın benzer kararı söz konusudur[410];

  "Oluşa ve dosya kapsamına göre; mankenlik mesleğini icra etmesi ve 2009 yılında yapılan bir güzellik yarışmasında ikinci olmasından dolayı kamuoyu tarafından tanınan, özellikle magazin basını tarafından zaman zaman haberleri yapılan katılan Senem ile onunla aynı mesleği icra eden tanık Ebru'nun, facebook adlı sosyal paylaşım sitesinde birbirlerini arkadaş olarak ekledikleri, tanık Ebru'nun, üniversite öğrencisi olan sanık Serap ile aynı evi paylaştığı 2009 yılı Haziran ayında, facebook oturumunu açık bırakmasından faydalanan sanık Serap'ın, tanık Ebru'dan habersiz, onun arkadaş listesinde yer alan katılan Senem'in sayfasına girip, katılana ait 20 adet fotoğrafı, kendi elektronik posta hesabına gönderdikten sonra, aynı sitede, katılan adına ve onun bilgisi

[407] Yargıtay 12. Hukuk Dairesi, Esas Sayısı: 2015/16404, Karar Sayısı: 2015/28245, 16.11.2015.
[408] Yücedağ, s.780.
[409] Dülger, Ceza Normu, s.142.
[410] 12. CD. 17.2.2014, E. 2013/7765, K. 2014/3758.

dışında oluşturduğu sahte profile, ele geçirdiği katılana ait fotoğrafları koymak suretiyle verileri hukuka aykırı olarak verme veya ele geçirme suçunu işlediği iddia ve kabulüne konu olayda, Katılanın rızasına aykırı olarak ele geçirdiği fotoğraflarını, onun isim ve soy ismiyle birlikte, belirli olmayan ve birden fazla kişi tarafından algılanabilme imkânı bulunan facebook adlı sosyal paylaşım sitesinde, hukuka aykırı olarak yayan sanığın eyleminin verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğunun kabulünde bir isabetsizlik görülmediğinden, temyiz itirazlarının reddine".

Bu bağlamda bizim görüşümüz, ilgili kişinin kişisel verilerini alenileştirme maksadının ve hangi bağlamda gerçekleştiğinin her somut olayda bir kez daha ele alınması yönünde olacaktır.

- *Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması;* KVKK'nın 5/e maddesinde belirtilen ancak Direktif ve GVK'te karşılığı bulunmayan bir diğer hukuka uygunluk sebebi ise, kişisel veri işlemenin bir hakkın tesisi, kullanılması ve korunması için zorunlu olarak gerçekleştirilmesidir. Veri sorumlusunun hukuki yükümlülüğü ve kanunlarda açıkça öngörülme hukuka uygunluk sebeplerinden farklı olarak burada, hakkın veri sorumlusuna mı yoksa ilgili kişiye mi ait olduğuna ilişkin bir ayrım yapılmadığı görülmektedir. Nitekim KVKK'nın gerekçesinde, bir şirkete çalışan tarafından açılan bir davada ispat için, çalışanın kişisel verilerini kullanması ya da kısıtlı bir kişinin haklarını savunmak amacıyla kayyım ya da vasinin kısıtlı kişinin bilgilerine erişebilmesi, bu hukuka uygunluk sebebine örnek olarak verilmiştir. Böyle durumlarda, işle ilgili sınırlı kalmak kaydıyla veri işleme hukuka uygunluk arz ederken, bu verilerin ölçülü olması ve işlem için zorunlu olması şartının gözetilmesi gerekmektedir[411]. Bu bağlamda, hekimlik ya da avukatlık mesleğinin icrası kapsamında kayıt altına alınan verilerin hak teşkil etmesinden ötürü suç oluşturmadığını belirtilmektedir[412]. Ancak, KVKK gerekçesinde yer verilen "bazı veriler" ifadesi muğlak bulunmakta ve hangi

[411] Aşıkoğlu, s.133.
[412] Sert, s.118'ten naklen Şen'in görüşü alınmıştır.

hakkın tesisi, kullanılması ya da korunmasının söz konusu olduğunun incelenmesi gerektiğine dair şerh düşülmektedir[413].

- *İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması;* KVKK'nın 5/f maddesi uyarınca ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması halinde rıza aranmaksızın hukuka uygunluk sebebi gerçekleşmiş olmaktadır. Örneğin; kamuya açık bir şirketin şeffaflık politikası doğrultusunda yöneticilerine ödediği maaşı hisse sahiplerine açıklaması hem bir zorunluluk hem de meşru menfaat nedenidir[414]. Ancak meşru menfaat deyimi tartışmaya açık bir konu olup[415], meşru menfaatin kime ait olduğu önem arz etmektedir. Bu yönüyle doktrinde bu hak, meşru ticari çıkarlar olarak da ifade edilmektedir[416]. Bu bağlamda, GVKT'nın aksine KVKK'da meşru menfaat sahibi, veri sorumlusu olarak işaret edilmektedir[417]. Buna göre bir şirket sahibi temel hak ve özgürlükleri zedelememek kaydıyla, çalışanlarının terfi, maaş zammı ve diğer sosyal hakların düzenlenmesi ile işletmenin organizasyon yapısını etkinleştirmek için kişisel verileri işleyebilir. Bu bağlamda, işletmenin yeniden yapılandırılması veya liyakatli çalışanların terfi almaları, veri sorumlusu olan şirket sahibinin meşru menfaatinedir[418]. Bir diğer sorun alanı ise "zorunluluk" şartlarının neler olduğudur. ÇEKİN'e göre gereklilik ve ölçülülük ilkesi göz önünde bulundurularak bu verilerin ve veri işleme faaliyetinin gerçekten gerekli olup olmadığı değerlendirilmelidir[419]. YÜCEDAĞ ise şirket birleşmelerinde gerçekleştirilecek veri aktarımlarını zorunluluk dairesinde kabul ederken,

[413] Küzeci, s.348.
[414] Develioğlu, s.67.
[415] Çekin, s.72.
[416] Küzeci, s.211.
[417] Yücedağ, s.783.
[418] Eralp, Özgür: "Veri Sorumlusunun Meşru Menfaatleri için Veri İşlenmesinin Zorunlu Olması", , https://www.ozgureralp.com.tr/soru-327-ilgili-kisinin-temel-hak-ve-ozgurluklerine-zarar-vermemek-kaydiyla-veri-sorumlusunun-mesru-menfaatleri-icin-veri-islenmesinin-zorunlu-olmasi-ne-anlama-gelmektedir/, (Erişim Tarihi): 15.04.2019.
[419] Çekin, s.72.

devralınacak şirketin bünyesindeki tüm bilgilere erişim ve kayıt hakkı talep edilmesini orantılılık ilkesi ile bağdaşmaz bulmaktadır[420].

Ancak yukarıda sayılan tüm bu durumlarda, işleme faaliyetinin sadece "mümkün" olduğu ve son tahlilde somut vakadan hareketle, hâkimin hukuka uygunluk nedeninin değerlendirilmesinde takdir yetkisi olduğu unutulmamalıdır. Dolayısıyla, bu maddede sayılan durumlarda bile hâkim, kişisel verilerin hukuka aykırı olarak işlendiğine kanaat getirebilecektir[421]. Dolayısıyla, bu hukuka uygunluk halleri, her halükarda kişisel veri işleme faaliyetinde güdülen amaca yönelik olmalı ve kişi bu doğrultuda bilgilendirilmelidir. Bu aynı zamanda "belirli, açık ve meşru amaçlarla işlenme" ilkesinin bir görünümü olan aydınlatma yükümlülüğü ile de düzenlenmektedir[422]. İşlemenin amaca uygunluğunun tespitinde ise; kişisel verilerin elde edilmesindeki amaç ve sonradan işlenmesinde güdülen amaç arasındaki bağlantılar, kişisel verilerin elde edildiği şartlar ile kişiler ile veri sorumlusu arasındaki ilişki, kişisel verilerin doğası ve bazı özel veri kategorilerinin veya cezai hükümler ve suçlara ilişkin verilerin işlenip işlenmediği, planlanan işlemeni ilgili kişiler açısından olası sonuçları ve kriptolama ya da psödonimleştirme[423] dâhil uygun tedbirlerin varlığı göz önünde bulundurulacaktır[424].

3.2.3. Ağırlaştırılmış hukuka uygunluk halleri

KVKK'da yer verilen iki düzenleme, işlemenin hukuka uygunluğunu daha ağır şartlara tabi tutarken, bunlardan ilki özel nitelikli kişisel verilerin işlenmesi, diğeri ise kişisel verilerin yurtdışına aktarılmasına ilişkindir.

Özel Nitelikli Kişisel Verilerin İşlenmesi Bakımından

KVKK'nın 6/4 maddesinde, özel nitelikli kişisel verilerin tanımı verilmemiş ancak nelerin özel nitelikte kişisel veri kapsamına girdiği sayılmış olup, bunlar "kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve

[420] Yücedağ, s.784-785.
[421] Develioğlu, s.58.
[422] Aşıkoğlu, s.118.
[423] Kriptolama ile ilgili kişilerin bilgilerinin şifrelenmesine atıfta bulunurken, psödonimleştirme ise kişilere mahlas (takma isim) takılması yoluyla verileri ile bağlantılarının kopartılması işlemidir.
[424] Develioğlu, s.68.

kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir.

KVKK'nın 6/3'üncü maddesinde açık rıza aranmaksızın özel nitelikli kişisel verilerin işlenebileceği haller düzenlenmiştir. Bu bağlamda, sağlık ve cinsel hayat dışındaki kişisel veriler kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmadan işlenebilecek, sağlık ve cinsel hayata ilişkin kişisel veriler ise kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin işleyişi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebilecektir.

Bununla birlikte, KVKK 6/4'üncü maddede özel nitelikli kişisel verilerin işlenmesi için Kişisel Verileri Koruma Kurulu'nun belirlediği yeterli önlemlerin alınmasın şart olduğuna dair bir düzenleme söz konusudur[425]. KÜZECİ, genel nitelikli verilerde kanunda "açıkça" öngörülme koşulu aranması, buna karşın sağlık ve cinsel hayat dışındaki özel nitelikli veriler için "kanunda öngörülmenin" yeterli görülmesinin, hassas verilerin daha etkin korunması ilkesine zarar verici nitelikte olduğunu belirtmektedir. Bu bağlamda, açıkça öngörülme koşulu tüm hassas veriler için öncelikli olmalıdır[426]. Bu yöndeki bir düzenlemeye ihtiyaç olduğu açıktır.

Bu bağlamda, özel nitelikli veriler olarak sağlık ve cinsel yaşam verilerinin işlenmesi önemli bir konu başlığı olup, kişinin gündelik hayatta en çok işlenen verileri niteliğindeki bu veriler, diğer kişisel verilere göre özel bir koruma gerektirmektedir[427]. GVKT'de sağlık verileri, "sağlığa ilişkin kişisel veriler" olarak tanımlanırken, atıfta bulunulan, "gerçek bir kişinin sağlık durumu hakkında bilgi ortaya koyan sağlık hizmetleri kayıtları dâhil olmak üzere kişinin fiziksel veya akıl sağlığına ilişkin verilerdir". Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in 4/1'inci maddesinde kişisel sağlık verilerinin işlenmesi, "*kişisel sağlık verilerinin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt*

[425] Korkmaz, Kişisel Verilerin Korunması, s.118.
[426] Küzeci, s.353.
[427] Başalp, Kişisel Verilerin Korunması, s.43.

sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi sağlık verileri üzerinden gerçekleştirilen her türlü işlem" olarak tanımlanmaktadır. Bu düzenleme KVKK'daki tanımla birebir aynıdır[428].

Buna göre sağlıkla ilgili kişisel veriler, gerçek kişiye ait hastalığın türü, hasta ve hastalığın öyküsü, teşhis, tedavi, psikolojik göstergeler, organ eksiklikleri, muayene ve tıbbi tahlil sonuçları, görüntüleme filmleri vb'dir[429]. Bir AIDS hastasına ilişkin verilerin ilgili sürece dâhil ve sır saklama yükümlülüğüne sahip kişiler haricindeki kişilerle paylaşılması, hastanın toplumdan yalıtılması ve maddi ve manevi varlığının zarara uğramasına neden olabilecektir. Bu nedenle, bu veri kategorisinin işlenmesinde ayrı bir hassasiyet söz konusudur. Nitekim, Campbell v Mirror Group davasına neden olan süreçte bir İngiliz gazetesi, uyuşturucu bağımlılarına yönelik bir rehabilitasyon merkezi çıkışında çektiği fotoğrafları kamuyla paylaşmış, veri kişisinin tedavisine ilişkin ayrıntıları içeren bu fotoğraf ve haber, hassas veri olarak kabul edilmiştir[430].

Diğer yandan; davacıların yakınlarının bir Devlet Hastanesinde yaptırdığı HIV testinin sonucunun pozitif çıktığını öğrenmesinin etkisiyle intihar etmek suretiyle yaşamını yitirmesi sebebiyle uğranıldığı ileri sürülerek maddi ve manevi zararın tazmini istemiyle açılan davada[431] Danıştay; "*olayda, davacılar yakınının Devlet Hastanesinde yapılan ve pozitif çıkan HIV testinin sonucunun, davacıların yakını da dâhil olmak üzere doğrulama testi yapılmadan hiç kimseye açıklanmaması ve ilgilinin doğrulama testi için bir üst basamak sağlık kuruluşuna sevki gerekirken, laboratuvar teknisyeni tarafından doğrulama testi yapılmadan önceki aşamada pozitif çıkan test sonucunun açıklanmasının neden ve etkisiyle davacılar yakını intihar etmek suretiyle yaşamını yitirdiği, dava konusu olayın oluş şekli, hastalığın niteliği ve özelliği dikkate alındığında, davacılar yakının idarenin ağır hizmet kusurunun neden ve etkisiyle intihar etmek suretiyle yaşamını yitirmesi sonucunda doğan zarar ile idari faaliyet arasında*

[428] Dülger, Ceza Normu, s.111.
[429] Akgül, Kişisel Verilerin Korunması, s.11.
[430] "Case of Campbell v. Mirror Group Newspapers", Başvuru No: UKHL 22, 6.5.2004, , https://www.5rb.com/case/campbell-v-mgn-ltd-hl/, (Erişim Tarihi): 16.04.2019.
[431] Danıştay 10.D., 28.12.2005, E:2005/8407, K: 2007/6526, Y.K.

uygun nedensellik bağı bulunduğu" gerekçesiyle aksi yöndeki idare mahkemesi kararın bozulmasına hükmetmiştir[432].

Benzer şekilde, davacıya AIDS teşhisi konulup, bu teşhisin kesinleşmesi beklenmeden basın aracılığıyla ilgili durumun duyurulmasını müteakip, davacının işsiz kalması sonucu uğranıldığı öne sürülen maddi ve manevi zararı tazmin istemiyle açılan davada İdare Mahkemesi'nin verdiği karar önem arz etmektedir. Buna göre, davalı idare tarafından olayın kendi görevlileri tarafından basına intikal ettirilmediğini savunulmasına rağmen, davalı idare, savunmasında olayın hastane görevlileri tarafından basın mensuplarına şahsın fotoğrafı ve mesleki bilgileriyle açıkça belirtildiğine ve henüz kesinleşmeyen bu tanının basının sızdırılmasında idarenin hizmet kusurunun açık olduğuna, davacının bu olay nedeniyle işsiz kalması sonucu uğradığı maddi zararın ve duyduğu elem üzüntü ve sarsıntı nedeniyle uğradığı manevi zararın tazmininin gerektiğine, İdare Mahkemesince karar verilmiş ve bu karar Danıştay tarafından da onaylanmıştır[433].

Burada da görüldüğü üzere, kişisel verinin kişinin sağlık durumuna ilişkin bilgi içermesi durumunda, korunan hukuki fayda kişinin sağlık hakkıdır[434]. Kişinin sağlık bilgilerinin kişi ile ilişkili tutulması, hasta açısından fayda sağlarken; kişinin tıbbi verilerinin yeterince korunmadığına dair bir düşüncesi, onu sağlık hizmetinden faydalanmamaya teşvik edebilecektir[435].

KVKK kapsamında özel nitelikli kişisel verilerden olan sağlık verilerinin hukuka aykırı olarak kaydedilmesini cezayı arttıran bir nitelikli hal olarak kabul etmektedir. Diğer yandan, sağlık durumu bilgisi bir kişiye yönelik değil, anonim veri olarak kaydedilip istatistik amaçlara hizmet etmekteyse, bu maddeye göre suç oluşmamakta olup, veriler kişisel veri niteliğini kaybetmektedir[436]. Ancak bir görüş ise sağlık verileri gibi özel verilerde karşılaşılabilecek rahatsızlıkların sadece TC kimlik numarası veya adresi silmekle "anonimleştirme" için yeterli olmayacağını ve binlerce satıra ulaşabilen

[432] Akgül, Kişisel Verilerin Korunması, s.233.
[433] Danıştay 10. D., 31.1.1996, E: 1994/5314, K: 1996/29, Y.K.
[434] Sarıusta, s.117.
[435] Korkmaz, Kişisel Verilerin Korunması, s.115.
[436] Dülger, Ceza Normu, s.137'den naklen Karagülmez'in görüşü alınmıştır.

verilerde anonimleştirme için sadece hukukçu ya da teknik kişinin değil, bir tıp hekiminin de devreye girmesi gerektiğini belirtmektedir. Ayrıca, anonimleştirmenin silme ya da yükleme işleminden daha önce mi yoksa sonra mı geleceğine, neyin silinip neyin anonimleştirileceğine kimin karar vereceği de bir başka sorun alanını oluşturmaktadır[437].

Bir başka önemli konu ise, verilerin korunamaması durumunda kişinin cinsel yaşamından kaynaklı ayrımcılığa tutulması riskidir. Özellikle eşcinsel bireyler, birçok toplumda sapkın, toplumsal cinsiyet kalıplarına tehdit kişiler olarak görülmekte, istihdam, eğitim, askerlik hizmeti ve sağlık alanlarında çeşitli sorunlarla karşılaşmaktadır[438]. AİHM'nin karara bağladığı X. v. Türkiye davasında tutuklu bir eşcinsel olan başvurucu, cinsel eğilimi nedeniyle diğer mahkûmların şiddet ve taciz eylemlerine maruz kaldığını, bunun üzerine cezaevi yönetiminden diğer eşcinsel mahkûmlarla aynı koğuşa konulmasını talep ettiğini, buna karşılık sekiz ay on gün boyunca daha kötü fiziksel şartlarda tecrit muamelesiyle karşılaştığını belirtmiştir. AİHM ise kararında, başvurucunun cinsel yönelimi nedeniyle ayrımcılığa tabi tutulduğun ve Sözleşme'nin 3'üncü ve 14'üncü maddelerinin ihlal edildiğini belirtmiştir[439]. Bu somut olay, kişinin cinsel yaşamına ilişkin kişisel verilerinin özel nitelikli veri olarak kabul edilmesinin ne kadar yerinde olduğunu gösteren bir örnektir.

Kişisel Verilerin Yurtdışına Aktarılması Bakımından

Kişisel verilerin aktarılması daha önce de belirtildiği üzere kişisel verilerin işlenme türlerinden biridir[440]. Bununla birlikte, Kanun'da aktarıma ilişkin hükümler diğer işleme türlerinden ayrı olarak düzenlenmiştir. Bu bağlamda, KVKK'nın 9'uncu maddesi, ilgili kişinin açık rızası bulunmadan kişisel verilerin yurtdışına aktarılamayacağını belirtmekte olup, genel nitelikteki veriler için KVKK'nın 5/2'inci maddesindeki; *Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden*

[437] Şıracı, Sertel: "Açık Rıza Bağlamında Fiziki ve Sanal Ortamda Uygulama Sorunları", Kişisel Sağlık Verileri 3. Ulusal Kongresi Bildiri Kitabı, İstanbul 2018, s.23.
[438] Aysun, s.137.
[439] X/Türkiye, Başvuru No: 24626/09, 9.10.2012.
[440] Arslan, s.41; Küzeci, s.355.

bütünlüğünün korunması için zorunlu olması ya da özel nitelikli veriler için KVKK 6/3'üncü maddesindeki; *"Sağlık ve cinsel hayata ilişkin kişisel veriler ise, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir"* hükme uygunluk söz konusuysa ve kişisel verinin aktarılacağı ülkede yeterli koruma bulunuyorsa ya da yeterli koruma olmadığı durumlarda, Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulunun izni bulunması kaydıyla ilgili kişinin açık rızası olmadan yurtdışına aktarım mümkündür.

Bu şartları taşıyan ülkeler, Kurul tarafından belirlenerek ilan edilecektir. Bu bağlamda, kişisel verilerin yurtdışına aktarılmasına ilişkin diğer kanun hükümleri saklı tutulurken, uluslararası sözleşme hükümleri saklı kalmak üzere Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda aktarım için kamu kurum veya kuruluşu ile Kurum'un izninin alınması öngörülmektedir[441]. Ancak, Türkiye'nin ya da ilgili kişinin menfaatlerinin zarar göreceği durumları objektif olarak saptayabilecek bir ölçütün ne olduğunu belirlemek güç olup, elinde herhangi bir ölçüt olmayan ve yasaya uygun hareket etmeye çalışan iyi niyetli veri sorumlusunun, hukuka aykırı etkinlikleri öngörebilme açısından sorunlarla karşılaşacağı açıktır[442].

3.2.4. İstisnalar

KVKK'da çeşitli hükümlerin uygulanmasına ilişkin istisnalar getirilirken, 28/1'inci maddede ayrı bir başlık altında genel ve özel nitelikteki tüm kişisel verilerin tamamından istisna edilen bazı işleme faaliyetleri söz konusu edilmiştir. Bunlara aşağıda yer verilmektedir;

- *Gerçek kişinin kendisiyle veya aynı konutta yaşayan aile bireyleriyle ilgili verileri işlemesi;* KVKK'nın ilgili hükmü, kişisel verilerin üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlere uyulmak kaydıyla gerçek

[441] Develioğlu, s.80.
[442] Küzeci, s.357.

kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesinin istisna kapsamına girdiği yönündedir. DÜLGER, hem veri ilgilisinin hem de veri işleyen kişinin menfaatlerini gözettiğini belirttiği bu hükmün, aile içerisinde veri işleme prosedürünün ve gündelik hayatın kolaylaştırılması amacı taşıdığı ve bu nedenle Anayasa'ya aykırı bir yönü bulunmadığını belirtmektedir[443]. KÜZECİ, AB mevzuatında benzer hükümlerde "kişisel amaçlarla işlenen" verilerden söz edildiğini yani maddi çıkar olmadan ve ev içi amaçlarla işlenen verilere atıfta bulunulduğunu ifade ederekn, aynı konutta yaşayan kişilerle değil, aile fertleriyle ibaresine yer verilmesi TMK kapsamında aile ferdi olmayan ancak aynı konutta yaşayan unsurların kişisel verilerinin işlenmesi faaliyetinin üzerinde belirsizlik oluşturduğunun altını çizmektedir[444].

- *İstatistik, araştırma ve planlama amacıyla verilerin işlenmesi;* KVKK'da resmi istatistikler ve anonimleştirmek koşuluyla araştırma, planlama ve istatistik amacıyla diğer veri işlemeler, kanundan istisna edilmiştir. Resmi istatistik konusu beraberinde birçok tartışmayı getirmiştir. Bir görüşe göre, anonimleştirmeden kaydedilecek kişisel verilerin resmi istatistik kategorisine girmesi; TÜİK, Çalışma ve Sosyal Güvenlik Bakanlığı gibi kurumlar tarafından işlenen verilerin kapsam dışı bırakılması içindir[445]. Özellikle, TÜİK'in veri toplama faaliyetleri daha önce de AYM'ye başvuru konusu olmuş ve AYM 2008 yılında verdiği ilk kararda, "bir ülkede en güçlü veri tekelinin idare olduğuna ve bu gücün sınırlandırılmasının özel yaşamın ve düşünce ve kanaat özgürlüğünün korunması bakımından önemli olduğuna" hükmetmiştir[446]. Diğer yandan, anonimleştirme kaydıyla istisna edilen diğer unsurlar yeterince açık olmayıp, anonimleştirilmiş bir veri kişisel veri niteliğini yitirmektedir[447]. DÜLGER de seçim zamanlarında anket yapan ve siyasi düşünce bilgisi toplayan şirketler örneğinden hareketle, bu bilgilerin başlangıçta anonim halde toplanabileceğini

[443] Dülger, Kişisel Verilerin Korunması, s.202.
[444] Küzeci, s.333-334.
[445] Şeker, A. Ömer, "Bilimsel Araştırmalarda Kişisel Veri", https://medium.com/@aseker/bilimsel-ara%C5%9Ft%C4%B1rmalarda-ki%C5%9Fisel-veri-e3fc72a616eb, (Erişim): 21.04.2019.
[446] AYMK, E. 2006/167, K.2008/86, 20.3.2008.
[447] Küzeci, s.335.

veya toplanıp amaca ulaştıktan sonra anonimleştirilebileceğini belirtmektedir. Bu şekilde, veri işlenmesinin yeterli kabul edilmesi durumunda, bu verilerin ilgili amaçlarla doğrudan toplanmamasının altı çizilmiştir[448].

- *Sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında verilerin işlenmesi;* KVKK'da milli savunma, milli güvenlik, kamu güvenliği, kamu düzeni, ekonomik güvenlik, özel hayatın gizliliği veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi durumunda, ilgili işlemeyi istisna saymaktadır. Bu istisna, birçok tartışmayı beraberinde getirmektedir. Sanat, tarih, edebiyat veya bilimin milli savunma, güvenlik ve kamu düzenini tehdit etme ölçüsü muğlak olup, buna kimin tarafından karar verileceği oldukça tartışmalıdır. Dolayısıyla, bu karmaşık durum bizi düşünceyi açıklama özgürlüğü tartışmalarına ulaştırmaktadır. Bu noktada düşünceyi açıklama özgürlüğü ile kişisel verilerin korunması hakkı bazı durumlarda birbirlerini destekleyen, bazense birbirleriyle yarışan haklar olarak öne çıkmaktadır. Dolayısıyla, iki hak arasında hassas bir denge kurmaya yönelik hükümlerin bulunması doğal kabul edilmektedir. Ancak KÜZECİ, maddenin kaleme alınış şekli itibariyle bazı durumlarda dengenin, düşünceyi açıklama özgürlüğünün aleyhine gelişebileceği endişesi taşıdığını belirtmekte ve kişisel verilerin korunması hakkı ile tüm bu özgürlüklerin yarıştığı durumlarda, insan haklarının temel ilkeleri ışığında somut vakaya göre değerlendirme yapmayı tavsiye etmektedir. Unutulmamalıdır ki, düşünceyi açıklama özgürlüğünde olduğu gibi, bilim, sanat, edebiyat gibi alanlardaki faaliyetler de anayasal güvence altındadır[449].

  Diğer yandan, bilimsel araştırmalarda kişisel veri işlemenin belirli şartlar dâhilinde gerçekleşmesi kabul edilebilir olsa da, aslında buradan bilimsel

[448] Dülger, Kişisel Verilerin Korunması, s.203.
[449] Küzeci, s.337.

araştırmalar için bir istisna çıktığı değil, kırmızı çizgilerin belirlendiği yönünde yorum yapılmaktadır[450]

- *Önleyici, koruyucu ve istihbari faaliyetler kapsamında verilerin işlenmesi;* KVKK'da milli, ekonomik ve kamu güvenliğini, kamu düzenini sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşlarının yürütmesine izin verilen bu istisna, oldukça geniş bir alanı KVKK kapsamı dışına almaktadır. Dolayısıyla, bu hükümdeki soyut, belirsiz ve geniş kapsamlı ifadeler keyfi uygulamalara hatta fişlemelere kadar varabilecek sorunları beraberinde getirebilecek, istisna ya da yetki sınırının olmaması, yetki aşımı ve kötüye kullanımlara karşı etkin koruma yollarının belirlenmemesi ve bireyin devlet otoritesi karşısında korumasız bırakması nedeniyle, denge kişisel verilerin korunması hakkının aleyhine kullanılabilecektir. Bu nedenle her somut olay, insan hakları, veri koruma hukukunun temel ilkeleri hakkaniyet esas alınarak dar yorumlanmalı ve titizlikle değerlendirilmelidir[451].

- *Soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin verilerin işlenmesi;* Yargı makamları ve infaz mercileri tarafından gerçekleştirilen işlemlere uygulanan bu istisna, kişisel verilerin işlendiği önemli bir alanı ilgilendirmekte olup, bu alanın veri koruma ilkelerinin dışında kalması birçok hak ihlaline imkân tanıyacak bir zeminin oluşmasına neden olabilecektir. KÜZECİ, bu faaliyetleri yürüten kurumların nitelikleri göz önünde bulundurularak, veri işleme faaliyetinin hukuki güvence altına alınacağı düzenlemeler yapılabileceğini, bu doğrultuda 2016/680 sayılı AB Direktifi'nin göz önünde bulundurulabileceğini belirtmektedir[452].

Diğer yandan, KVKK'nın 28/2'inci maddesinde, bazı madde hükümlerinin uygulanmayacağı belirtilmektedir. Bunlar; suç işlenmesinin önlenmesi veya suç soruşturma için gerekli olması; ilgili kişinin kendisi tarafından alenileştirilmesi; işleme

[450] Şeker, A. Ömer, "Bilimsel Araştırmalarda Kişisel Veri", , https://medium.com/@aseker/bilimsel-ara%C5%9Ft%C4%B1rmalarda-ki%C5%9Fisel-veri-e3fc72a616eb, (Erişim): 21.04.2019.
[451] Uncular, s.100-101.
[452] Küzeci, s.337-338.

kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme ve düzenleme görevlerinin yürütülmesi ile disiplin soruşturma ve kovuşturması için gerekli olması ve işleme bütçe, vergi ve mali konulara ilişkin olarak devletin ekonomik ve mali çıkarlarının korunması için gerekli olmasıdır. Ancak ikinci fıkrada düzenlenen istisnalar, birincisindeki gibi tamamen veri koruma kapsamı dışında olmayıp, aydınlatma yükümlülüğü, ilgilinin hakları ve sicile kayıt yükümlülüğü açısından hukuka uygunluk sebebi oluşturmaktadır[453].

KVKK'nın gerekçesinde de belirtildiği gibi, kişiler verilerin korunması hakkının sınırsız korunan bir hak olmadığı ve belirli koşullar altında müdahale edilmesinin mümkün olduğunun altı çizilmekte, bu yönden istisnaların, bu hak ile diğer kamusal ve kişisel menfaatler arasından denge ve ölçülülük sağlanması açısından gerekli olduğuna vurgu yapılmaktadır[454]. Diğer yandan 28'inci maddenin (c), (ç) ve (d) bentleriyle Direktif ile karşılaştırıldığında, KVKK'nın çok geniş bir istisnalar listesi düzenlediği ve bunun Kanun'un uygulanma alanını daralttığı belirtilmektedir[455].

KVKK'nın istisnalarının kişisel verilerin korunması hakkının aleyhine yorumlanabilecek çeşitli soyut, belirsiz ve geniş kapsamlı ifadeleri içerdiği şeklindeki görüşe katılırken, bu hükmün, kişisel verilerin korunması amacından çok, kamu kurum ve kuruluşları tarafından kişisel verilerin serbestçe işlenebilmesine meşruluk kazandırma amacı taşıdığı izlenimine neden olduğunu belirtmek gerekmektedir.

3.3. Veri Sorumlusunun Yükümlülükleri

KVKK'nın "Tanımlar" başlıklı 3'üncü maddesinin 1'inci fıkrasının (ı) veri sorumlusu; "*kişisel verilerin işleme amaçlarını ve araçlarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak ifade edilmektedir. Tüzel kişiler, kişisel verileri işleme konusundaki faaliyetleri ile bizatihi veri sorumlusu olarak kabul etmekte ve hukuki sorumluluk tüzel kişilik şahsına

[453] Sert, s.126.
[454] Korkmaz, Kişisel Verilerin Korunması, s.148'den naklen Dağ'ın görüşü alınmıştır.
[455] Aysun, s.81.

doğmaktadır. Veri sorumlusu; kişisel verilerin işlenme amacını ve yöntemini belirlemektedir. Veri sorumlusunun tespiti için, kişisel verilerin toplanması ve toplama yöntemi, toplanacak kişisel veri türleri, toplanan verilerin hangi amaçlarla kullanılacağı, hangi bireylerin kişisel verilerinin toplanacağı, toplanan verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kiminle paylaşılacağı ve saklanma süresi konularında kimin karar verdiği önem arz etmektedir.

3.3.1. Aydınlatma yükümlülüğü

Kişisel verilerin işlenmesi sırasında ilgili kişinin bilgilendirilmiş olması, kişinin haklarını gerçek anlamda kullanabilmesine imkân tanımaktadır. Bu nedenle kişinin veri sorumlusu tarafından bilgilendirilmiş olması bir ön koşuldur. Bununla birlikte, idarenin şeffaflığı da sağlanmaktadır[456]. KVKK'nın 10'uncu maddesinde Direktif'le paralel şekilde, veri kişisinin veri sorumlusu tarafından bilgilendirilmesi zorunluluğu, aydınlatma yükümlülüğü olarak ifade edilmektedir. Veri sorumlusu, aydınlatma yükümlülüğü uyarınca; veri sorumlusu ya da varsa veri temsilcisinin kimliği, kişisel verilerin işlenme amacı, bu verilerin kimlere ve hangi amaçlarla aktarılabileceği, kişisel veri toplama yöntemi ve hukuki dayanağı, kişisel verilerin işlenmesinin sonuçları ve KVKK 11'inci maddede yer verilen hakları gibi konularda veri kişisini bilgilendirmeli ve bu bilgilendirme yapılmaksızın kişisel veri toplanmamalı ve işlenmemelidir[457]. BAŞALP, özellikle veri kişisinin hak arama yolları konusunda aydınlatılmış olması gerektiğini yani veri işlemeye itiraz, düzeltme, silme, yok etme hakkını kullanmak istiyorsa bu bilgilerin mutlak surette aydınlatma yükümlülüğü belgesi içerisinde olması gerekliliğinin altını çizmekte, bu yönüyle aydınlatma yükümlülüğü belgesinin kısa değil, uzun bir belge olması gerektiğini belirtmektedir[458].

Bütün bu bilgiler sonucunda, ilgili kişi aydınlatılmış veya işlemeye dair bilinç sahibi olarak rıza göstermiş olmalıdır[459]. Bu bağlamda kişinin, verilerin işlenmesine yönelik talebin hangi amaçla ve kimin tarafından yapıldığını, işlemenin içeriğini, saklı tutulma

[456] Küzeci, s.224.
[457] Yücedağ, s.774; Dülger, Kişisel Verilerin Korunması, s.112
[458] Başalp, Açık Rıza, s.23.
[459] Başalp, Kişisel Verilerin Korunması, s.39.

süresi ve verilerin ne surette kullanılacağı hususunda tam aydınlatılmış olması gerekmektedir[460].

KVKK'da genel hatlarıyla düzenlenmiş olması nedeniyle çeşitli belirsizlikler içeren bu hükmün uygulanmasına dair usul ve esaslar, Kurum tarafından "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"[461] ile düzenlenmiştir. Buna göre aydınlatma yükümlülüğü uyarınca, bilgilendirme veri sorumlusu tarafından sözlü, yazılı, ses kaydıyla, çağrı merkeziyle vb. fiziksel ya da dijital mecralardan yapılabilmektedir.

Bu bağlamda, açık rıza ya da diğer kanuni işleme şartlarına bağlı olarak veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilecek olup, bir faaliyet kapsamında birden fazla kez veri işlenecekse bilgilendirmenin sadece faaliyet kapsamında yapılması yeterli olacak ancak kişisel veri işlemenin amacı değişirse veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilecektir. Yine veri sorumlusunun farklı birimlerinde aynı veri işlenecekse aydınlatma yükümlülüğü her bir birim nezdinde yeniden devreye girecektir. Sicile kayıt zorunluluğu olduğu durumlarda, ilgili kişiye verilecek bilgiler, Sicile açıklanan bilgilerle uyumlu olmalıdır. Diğer yandan, aydınlatma yükümlülüğünün yerine getirilmesi ilgili kişinin talebinden bağımsızken, yerine getirildiğine dair ispat ise veri sorumlusuna aittir.

Diğer yandan, Tebliğ'de yapılan değişiklikle veri kayıt sistemi tanımı; kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi olarak değiştirilmiştir[462].

Bu noktada, açık rıza ile aydınlatma yükümlülüğü arasındaki ilişki önem arz etmektedir. Buna göre, kişisel veri işleme faaliyeti açık rıza şartına dayalı olarak gerçekleşirse, aydınlatma yükümlülüğü ve açık rıza talebi ayrı ayrı yerine getirilmelidir. Dolayısıyla, bu iki işlem birbirlerinin yerine ikame edilemeyecektir. Bununla birlikte, aydınlatma yükümlülüğü kapsamında gerçekleştirilecek veri işleme faaliyetinin belirli, açık ve

[460] Korkmaz, Kişisel Veriler ve Ceza, s.45.
[461] Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, R.G. 30356, 10.03.2018.
[462] Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğde Değişiklik Yapıldığına Dair Tebliğ, R.G. 30758, 20.04.2019.

meşru olması; bildirimin ise sade ve açık bir dil kullanılarak yapılması gerekmektedir. Bu bağlamda, veri sorumlusuna düşen bir başka yükümlülük ise, "hukuki dayanağın" belirtilmesidir. Bir diğer deyişle veri sorumlusu, KVKK 5'inci ve 6'ıncı maddelerinden hangisinden hareketle veri işleme faaliyeti gerçekleştirdiğini ilgili kişiye belirtmelidir. Ayrıca, kişisel verilerin aktarılma amacı ve aktarılacağı gruplar ile tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik yollardan hangisiyle elde edildiği açıkça belirtilmeli ve yükümlülük yerine getirilirken eksik, yanıltıcı ve yanlış bilgilere yer verilmemelidir.

Diğer yandan, kişisel veriler ilgili kişiden elde edilmiyorsa; veri sorumlusu, kişisel veriyi elde ettiği andan itibaren makul bir süre içerisinde ilgili kişiyi bilgilendirmeli, irtibat kurduğu ilk anda aydınlatma yükümlülüğünü yerine getirmeli ve ilgili kişinin üçüncü kişiden elde edilen verisi aktarılacaksa en geç veri aktarımının yapılacağı esnasında aydınlatma yükümlülüğü yerine getirilmelidir. Buna göre irtibat hiç kurulamazsa, aktarımın yapılamayacağı anlaşılmaktadır[463].

Aydınlatma yükümlülüğüne getirilen istisnalar, KVKK'nın 28'inci maddesinde tamamen veya kısmen getiriler istisnalarla aynı olup, bu durumlarda ilaveten aydınlatma yükümlülüğünün yerine getirilmesinden bahsetmek mümkün olmayacaktır.

3.3.2. Veri güvenliğine ilişkin yükümlülükler

GVKT'ye göre çok daha genel bir düzenleme öngören KVKK 12'inci maddesi; veri sorumlusuna kişisel verilerin kazara ortadan kaldırılma, yetkisiz erişim, değiştirme, silinme ve yayılmalarını önleyecek her türlü teknik ve idari tedbirleri alma yükümlülüğü getirmektedir. Bu bağlamda veri sorumlusu, ayrıca ilgili tedbirlerin alınmasında kişisel verileri kendi adına işleyen diğer gerçek veya tüzel kişilerle müştereken sorumlu tutulmuştur. Bununla birlikte, 12/3'üncü madde uyarınca, veri sorumlusu, kendi kurum veya kuruluşunda Kanun hükümlerinin uygulanmasını sağlamak için gerekli denetimleri yapmak veya yaptırmak zorundadır. Veri sorumluları ve veri işleyenler, veri işleme görevleri sırası ve sonrasında bu verileri başkalarına açıklayamazlar ve işleme amacı

[463] Develioğlu, s.100.

dışında kullanamazlar[464]. Bu yükümlülükle, aynı zamanda çeşitli tehditlere karşı kişisel verilerin güvenliğinin sağlanması yoluyla temel bir hak olan kişisel verilerin korunması hakkı da güvence altına alınmaktadır[465].

Veri güvenliği ilkesine aykırı davranan ve yükümlülüğü yerine getirmeyen veri sorumlularının, TCK 136'ıncı maddesi kapsamında sorumlu tutulmaları gerekmekte olup, KVKK 18'inci maddesine göre ise bu yükümlülüklere aykırı davranılması kabahat olarak düzenlenmiştir. Bu kabahatle korunmak istenen hukuki fayda kamusal, kişilerin kamusal makamlara olan güveni; TCK 136'ıncı maddede tarifi verilen suçla korunan hukuki fayda ise kişilerin özel yaşam gizliliği ve kişisel verilerin korunması hukukudur. Bu doğrultuda Kurum'un yorumu failin, sadece suç oluşturan fiilden sorumlu tutulması yönündeyken, bir başka görüş ise hem suçtan hem de kabahatten dolayı ayrı ayrı cezalandırılması gerektiği yönünde bir kanaat söz konusudur[466].

3.3.3. Özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken önlemler

KVKK'nın 6/4'üncü maddesinde "Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır" ifadesi yer almaktadır. Bu çerçevede, KVKK'nın 22/1'inci maddesi (ç) ve (e) bentleri uyarınca kapsamında özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması gereken yeterli önlemler, Kurul tarafından alınan karar[467] ile belirlenmiştir olup, altı ana maddeden oluşmaktadır.

Buna göre özel nitelikli kişisel veri sorumluları ilk olarak; özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net şekilde belirlenmiş, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedür belirlemelidir. Bununla birlikte, özel nitelikli kişisel veri işleme sürecinde yer alan çalışanlarla gizlilik sözleşmesi yapılmalı, onlara

[464] Küzeci, s.267.
[465] Akgül, s.172.
[466] Sarıusta, s.149-150.
[467] Kişisel Verileri Koruma Kurulu,'nın 2018/10 sayılı Kararı, "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler", K.T.: 31.01.2018, R.G.: 30353,

düzenli eğitimler verilmeli, verilere erişebilen kullanıcıların yetki kapsamları ve süreleri net olarak belirlenmeli, periyodik yetki kontrolleri gerçekleştirilmeli, işten ayrılan ya da görev değişikliği olan çalışanların yetkileri hızla kaldırılmalı, veri sorumlusu tarafından tahsis edilen envanter iade alınmalıdır.

Bununla birlikte, özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ya da erişildiği ortamlar elektronik ise; veriler kriptografik yöntemlerle muhafaza edilmeli, veriler üzerindeki tüm hareketlerin işlem kayıtları güvenli olarak loglanmalı, verilerin bulunduğu ortama ait güvenlik güncellemeleri sürekli takip edilmeli ve bu doğrultuda gerekli güvenlik testleri yapılarak bunlar kayıt altına alınmalı, verilere erişim bir yazılımla yapılmaktaysa yetkilendirilmeler yapılmalı, bu yazılımın güvenlik testleri düzenli olarak yapılmalı ve test sonuçları kayıt altına alınmalıdır. Ayrıca, veriler uzaktan erişim gerektiriyorsa, en az iki kademeli kimlik doğrulama sistemi sağlanmalıdır.

Diğer yandan ilgili ortamlar fiziksel ise; ortamın niteliğine göre elektrik kaçağı, yangın su baskını, hırsızlık vb. durumlara karşı yeterli güvenlik önlemi alındığına emin olunması ve bu durumu tehdit eden yetkisiz giriş çıkışların engellenmesi gerekmektedir.

Bir diğer husus ise bu verilerin aktarımına ilişkin olup; verilerin e-posta ile aktarılması durumunda şifreli olarak kurumsal e-posta ya da kayıtlı elektronik posta (KEP) ile; taşınabilir bellek, DVD, CD vb. ortamlarla aktarılması kriptografik yöntemlerle şifrelenerek ve kriptografik anahtarın başka yerde tutulduğu şekilde; farklı fiziksel ortamlardaki sunucular arası aktarım söz konusuysa VPN kurma ya da güvenli dosya taşıma protokolü (sFTP) yöntemiyle; veriler kağıtla aktarılıyorsa çalınma, kaybolma, yetkisiz kişilerin eline geçme risklerine karşı engel alınarak ve "gizlilik dereceli belgeler" formatında aktarımı gerekmektedir[468].

Tüm bu önlemlere ek olarak, Kurul, Kişisel Veri Güvenliği Rehberi'nde belirtilen uygun güvenlik düzeyinin teminine yönelik teknik ve idari tedbirlerin de dikkate alınması gerektiğini belirtmektedir.

[468] Kişisel Verileri Koruma Kurulu, "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler", K.T.: 31.01.2018, R.G.: 30353,

3.4. İlgili Kişilerin Hakları

KVKK'ya göre ilgili kişi; kişisel verisi işlenen gerçek kişi olup, kanun sadece gerçek kişilerin verilerini korumaktadır. Bu bağlamda, KVKK'daki kişisel veri tanımı gereği tüzel kişilere ait bir verinin gerçek kişiyi belirlemesi ya da belirlenebilir kılması halinde ise bu veriler de koruma kapsamına girmektedir. Ancak, korunan menfaat tüzel kişiye değil, düzenleme gereği belirlenen ya da belirlenebilecek gerçek kişiye ait olacaktır.

Bu doğrultuda, ilgili kişilerin hakları; bilgi edinme, erişim, düzeltme, unutulma, işlemenin sınırlandırılması, verilerin taşınması, itiraz ve irade sergileyebilme ve otomatik karar alınmasını kısıtlama olarak sıralanmakta olup, sırasıyla incelenecektir.

3.4.1. Bilgi edinme hakkı

İlgili kişilerin kendilerine ait hangi kişisel verilerin, hangi şartlarda, kim tarafından ve ne amaçla işleneceğini bilmesi hayati öneme sahiptir. Bu bilgilere sahip olan ilgili kişi, hukuki dayanaklardan hareketle haklarını kullanarak kişisel verilerinin akıbeti üzerinde söz sahibi olabilecektir[469]. Bu yönüyle bilgi edinme hakkı, verilerin korunmasına dair diğer ilke ve haklara kaynaklık eden, işlerlik kazandıran bir ana ilke konumundadır[470]. Bu ilke ışığında, veri sorumlusu, işleme faaliyetini hukuka uygun, adil ve şeffaf biçimde yürütmelidir[471].

KVKK'nın ana ilkelerini şekillendiren GVKT'da, veri sorumlusu tarafından ilgili kişiye sağlanması gereken bilgilerin başında veri sorumlusunun ya da temsilcisinin kimliği ile iletişim bilgileri yer almaktadır. Ayrıca, bilgi güvenliliği sorumlusunun iletişim bilgileri de buna ilave edilmektedir. Bununla birlikte, hedeflenen amaç, işlemenin hukuki dayanağı, verilerin aktarıldığı kişi ya da kişi kategorileri, veri sorumlusunun meşru menfaati söz konusuysa bu menfaatin ne olduğu, üçüncü ülkelere aktarım söz konusuysa ABK'nın uygunluk kararı, aktarım tedbirleri ve bunlara ne şekilde erişilebileceği düzenlenmiştir[472].

---

[469] Şimşek, s.83.
[470] Küzeci, s.229.
[471] Dülger, Kişisel Verilerin Korunması, s.152.
[472] Develioğlu, s.80-81.

KVKK'nın 10'uncu maddesi de, ilgili kişilere bilgi verilmesi gerekliliğini, veri sorumlusunun yükümlülükleri arasında düzenlemiştir. Daha önce de belirtildiği üzere bu hak, aydınlatma yükümlülüğü ile mütekabiliyet ilişkisi içerisinde olup, ana amacı şeffaflığı tesis etmek ve ilgili kişinin haklarını etkin bir şekilde kullanmasını sağlamak olan aydınlatma yükümlülüğü yerine getirilmediğinde, işleme faaliyeti hukuka aykırı olmaktadır. Bununla birlikte bilgilendirme, dürüstlük kuralının da bir gereğidir[473].

Bu bağlamda, KVKK'da veri sorumlusu veya yetkilendirilen kişiler, ilgili kişileri şekil şartı öngörülmeksizin; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin işlenme amacı, işlenen verilerin kimlere hangi amaçlarla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki dayanağı ile KVKK'nın 11'inci maddesindeki hakları hakkında bilgilendirmekle yükümlüdür. Gereken bilgilerin verildiğine ilişkin ispat yükü ise, veri sorumlusu ya da veri sorumlusu temsilcisine aittir.

3.4.2. Erişim hakkı

Bu hak ile özellikle teknolojik gelişmelerle dolaşımı risk altına giren kişisel verilerin kötüye kullanılmasını önlemek amaçlanmaktadır. Bu nedenle veri sorumlusu tarafından ilgili kişinin kişisel verilerinin, şeffaf ve erişime açık tutulması gerekmektedir[474]. Veri öznesi, kişisel verilerinin işlenmesine ilişkin bilgilere erişemiyorsa, kişisel verilerin korunduğu var sayılamayacaktır[475].

Kişinin verilerinin herhangi bir işleme faaliyetinin konusu olup olmadığı ile başlayan bu hak kapsamında, GVKT'nın 15'inci maddesi ilgili kişilere; işlemenin amaçları, veri kategorileri, verilerin ifşa edildiği veya edileceği, aktarım durumunda aktarılan kategoriler, mümkünse kişisel verilerin saklanma süresi değilse saklanma kriterleri, veir sorumlusundan düzeltme, silme, işlemenin sınırlandırılmasını talep etme ve işlemeye itiraz haklarının varlığı, denetim makamına şikayette bulunma hakkı, verilerin ilgili kişiden elde edilmediği durumlarda kimden edinildiğine dair bilgiler,

[473] Korkmaz, Kişisel Verilerin Korunması, s.129.
[474] Küzeci, s.95.
[475] Şimşek, s.88.

otomatikleştirilmiş karar vermenin uygulanıp uygulanmadığı ve bu uygulamanın mantığı, işlemenin önemi ve ilgili kişi açısından doğuracağı sonuçlara ilişkin bilgilere erişme hakkı tanımaktadır[476].

Nitekim GVKT ile paralel şekilde, KVKK 11'inci maddede de ilgili kişilerin; kişisel verilerinin işlenme durumu, işlenmişse buna ilişkin belgeler, işlenme amacı ve amaca uygunluğa ilişkin bilgiler, yurtiçi veya yurtdışında kişisel verilerin aktarıldığı üçüncü kişileri öğrenme hakkına sahip olduğu belirtilmektedir.

3.4.3. Düzeltme hakkı

Bu hak bilgi edinme hakkı kapsamında kabul edilmekte olup, bireyler kendilerine ilişkin verilerin hatalı ya da eksik olması halinde bunları düzelttirebilme hakkına sahiptir[477]. Direktif, ilgili kişiye bu durumda düzeltme ve silme talep edebilme hakkıyla birlikte veriye erişimin engellenmesi isteme hakkı da tanımıştır[478]. GVKT 5/1'inci maddesinde yer alan "doğruluk" ilkesi bağlamında, ilgili kişiye doğru olmayan kişisel verilerin gecikmeden düzeltilmesini talep etme hakkı tanımaktadır[479]. KVKK'da da paralel şekilde, ilgili kişilerin verilerinin eksik ya da yanlış işlendiği kanaatine vardıkları takdirde bunların düzeltilmesini isteme hakkına sahip olduğu açıkça belirtilmektedir.

3.4.4. Sildirme ya da unutulma hakkı

Direktif'in 12'inci maddesi ve GVKT'nin 17'inci maddesinde yer verilen "sildirme" ya da "unutulma hakkı" kavramı, ilgili kişinin kurallara uygun olmayan şekilde işlenen, eksik veya yanlış olan kişisel verilerinin silinmesini talep etme hakkıdır. Bu yanıyla GVKT, Direktif'e göre bireylerin bu tip bilgilerin silinmesi talep etme hakkını çok daha ayrıntılı şekilde düzenlemiş, kişilerin bu hakkı kullanması durumunda kişisel verilerin

[476] Develioğlu, s.87.
[477] Akgül, Kişisel Verilerin Korunması, s.170.
[478] Sarıusta, s.48.
[479] Develioğlu, s.88.

mümkün olan en kısa zamanda silinmesi konusunda veri sorumlusunun yükümlü olduğunun altını çizmiştir[480].

KVKK'nın 11'inci maddesinde ilgili kişi, veri sorumlusuna başvurarak kendisiyle ilgili verilerin 7'inci maddede öngörülen şartlar çerçevesinde silinmesi ya da yok edilmesini talep etme hakkına sahiptir. Bu durum, kişisel veriler hukuka uygun işlenmiş olsalar ve işlenmeyi gerektiren sebepler ortadan kalksa bile değişmeyecektir. Dolayısıyla, böyle bir taleple karşılaştığında veriler, veri sorumlusu tarafından silinmeli, yok edilmeli ya da anonim hale getirilmelidir. Veri sorumlusu bu işlemi res'en yapabileceği gibi, ilgili kişinin talebiyle de gerçekleştirebilir.

KVKK'nın 7/3'üncü ve 22/1'inci maddelerine dayanarak hazırlanmış olan ve veri sorumluları hakkında uygulanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği ile tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlenmiş, asgari olarak veri sorumluları tarafından yürütülecek kişisel veri saklama ve imha politikasının; hazırlanma amacı, kayıt ortamı, saklama ve imha süreçleri ile süreler ve ilgili idari ve teknik tedbirlere dair bir çerçeve çizilmiştir.

Yönetmeliğe göre kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme ya da anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk imha işleminde kişisel verileri siler, yok eder ya da anonim hale getirir. Periyodik imha süreleri; altı ayı geçemez. Yükümlülüğü olmayan veri sorumlusu ise yükümlülüğün ortaya çıktığı tarihi takip eden üç ay içinde silme, yok etme ya da anonim hale getirme işlemini yerine getirmektedir. Ayrıca, ilgili kişinin silme ya da yok etme talebi olması durumunda, kişisel veri işleme şartları tamamen ortadan kalkmışsa, bu talep en geç otuz gün içerisinde sonuçlandırılarak ilgili kişiye bilgi verilir. Bu veriler üçüncü kişiye aktarılmışsa, üçüncü kişiler bilgilendirilir ve Yönetmelik kapsamında gerekli işlemlerin yapılması temin edilir. Ancak kişisel veri işleme şartları tamamen ortadan kalkmamışsa bu talep veri sorumlusu tarafından

[480] Develioğlu, s.90.

KVKK'nın 13/3'üncü maddesi uyarınca gerekçe açıklanarak reddedilebilir ve en geç otuz gün içerisinde yazılı ya da elektronik ortamda ilgili kişiye bildirilir.

Yargıtay Genel Kurulu'nun unutulma hakkını ve bununla ilişkili olan kişisel verilerin gerektiği ölçüde ve en kısa süreliğine depolanması veya tutulması kararını kişisel verilerin korunması hakkının çatısı sayan kararına[481] rağmen, KVKK'da unutulma hakkına yer verilmemesi, Kanun bakımından bir eksiklik olarak eleştirilmektedir. Buna göre KVKK'nın tanıdığı hak GVKT'da yer alan unutulma hakkından daha çok, Direktif'te yer alan silinme hakkına daha yakın görülmektedir[482]. Nitekim aynı kararda, kişiye unutulma hakkının sağlanması ile birlikte özel hayatın gizliliğin de korunmuş olacağı tasdik edilmektedir.

3.4.5. İşlemenin sınırlandırılması hakkı

GVKT 4/3'üncü maddeye göre bu kavram ile depolanmış kişisel verilerin, ileride işlenmelerini sınırlandırmak amacıyla işaretlenmesine referans verilmektedir. Bu hak; verilerin bloke edilmesi, veri sorumlusunun veri işleme yetkisinin devretmesi, verilerin sadece veri sorumlusunun kontrolünde sınırlı amaçlarla kullanılabilmesi ve işlemenin engellenmesi anlamlarına da gelmektedir[483]. Buna göre ilgili kişi, kişisel verilerinin doğru olmadığını belirttiğinde, ilgili kişi verilerin doğruluğunu teyit etmek için elverişli bir süre boyunca veri işlemeyi sınırlandırmaktadır. İşleme hukuka aykırıysa ve ilgili kişiden gelen bir itiraz söz konusuysa yine işleme sınırlandırılmaktadır[484].

İlgili kişinin itirazı durumunda veri sorumlusunun meşru menfaatlerinin daha baskın olup olmadığı tayin edilene kadar veri işlemeye devam etmenin tek istisnası ilgili kişinin rızası ve gerçek veya tüzel kişilik haklarının korunması veya Birlik veya Üye Devlet'in önemli kamu menfaatleridir. Diğer yandan, KVKK'da bu hakka referans veren bir düzenleme bulunmamaktadır.

---

[481] Yargıtay Hukuk Genel Kurulu, "Unutulma Hakkına İlişkin Yargıtay Hukuk Genel Kurul Kararı", 2014/4-E. 2015/1679 K.
[482] Akgül, Danıştay ve Avrupa, s.93.
[483] Başalp, s.90.
[484] Develioğlu, s.94.

3.4.6. Bildirimde bulunulmasını talep etme hakkı

GVKT'nin 19'uncu maddesine göre veri sorumlusu, imkânsız olmadıkça ya da orantısız bir çaba gerektirmediği takdirde, ilgili kişiye verilerini düzeltme, silme ve işlemenin sınırlanması ve aktarım hallerini talep üzerine bilgilendirmekle yükümlüdür. KVKK'nın 11'/1'inci maddesinde bu hak, 7'inci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesi ya da yok edilmesi hakkının bir uzantısı olarak yer almaktadır. Buna göre ilgili kişilerin kişisel verileri hakkındaki işlemlerin, verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme hakkı bulunmaktadır[485].

3.4.7. Verilerin taşınması hakkı

Direktif'te olmayıp, ilk kez GVKT'nın 20'inci maddesinde düzenlenen verilerin taşınması hakkıyla, rızaya veya sözleşmeye dayalı olarak ve ilgili kişiden otomatik yöntemlerle elde edilen verilerin engelsiz şekilde başka bir veri sorumlusuna iletilmesine imkan tanınmaktadır. Bunun dışında kişisel verilerin taşınabilirliği hakkının başka bir hukuki dayanağı bulunmamaktadır[486]. Bu hak ilgili kişinin veri transferini talep etme hakkı olarak da ifade edilmektedir. Bu hak aynı zamanda ilgili kişinin memnun olmadığı bir bilgi teknolojileri sisteminden verilerini çekip alarak bir diğerine taşıması, kopyalaması ya da aktarılması ile servis sağlayıcıları arasında geçiş yapmayı sağlamaktadır. Bir diğer deyişle, memnun olmadığı servis sağlayıcıyı değiştirmesine elverişli bir ortam yaratarak, servis sağlayıcılar arasındaki rekabet ortamını da düzenlemektedir[487]. Bu durumun ilgili kişiyi kişisel verilerinin kontrolü konusunda güçlendirme hedefi taşıdığı ve AB içinde özgür veri akışını destekleyeceği öngörülmüştür[488].

Bu bağlamda veri sorumlusu, ilgili kişiden gelen kişisel verilerin bir başka veri sorumlusuna aktarılmasına talebine engel olmamalıdır. Ancak kişisel verilerin gerçekten talep edenin kontrolünde olduğundan, kişisel ve ailevi amaçlarla istendiğinden ve aktarılan veri sorumlusunun çıkarına ve amacına hizmet etmeyeceğinden emin

[485] Develioğlu, s.95.
[486] Dülger, Kişisel Verilerin Korunması, s.160-161.
[487] Sarıusta, s.53.
[488] Küzeci, s.230.

olunmalıdır. Böyle bir durumda da, aktarım işlemi hukuka aykırılık arz edecektir[489]. Bu hakkın kullanılması, GVKT'nin 17'inci maddesinde belirtilen ilgili kişinin kişisel verilerinin silinmesini talep etme hakkını kullanması açısından bir engel oluşturmamaktadır[490]. Diğer yandan, KVKK'da bu hakkın düzenlendiği bir madde bulunmamaktadır.

3.4.8. İtiraz ve irade sergileyebilme hakkı

GVKT'nin 21'inci maddesinde düzenlenen bu hakka göre ilgili kişiler; meşru menfaatlerinin korunması gerekçesiyle kişisel verilerinin işlenmesine itiraz etme hakkına sahiptir[491]. Bu bağlamda veri sorumlusu, ilgili kişi kendi hakkındaki verilerin işlenmesine itiraz ediyorsa ve bu itiraz haklı bulunuyorsa bu verilere dayanarak işleme faaliyeti gerçekleştiremez. Dolayısıyla, kanuni düzenlemeler ışığında kamu yararı gerekçesiyle kişisel verilerin işlenmesine imkan tanınmışsa bile, ilgili kişinin itiraz hakkı hukuki düzenlemelere aykırı veri işleme faaliyetine karşı, hak ve özgürlüklerin korunmasını sağlamaktadır[492].

Direktif'in 14/a hükmüne göre ilgili kişi belirli durumlarda verilerinin işlenmesine itiraz edebileceği gibi, 14/b hükmüne göre ise işlenme doğrudan pazarlama amacıyla yapılmışsa, ilk kez açıklanmışsa, üçüncü kişilere doğrudan pazarlama amacıyla aktarılmışsa, bu itiraz hakkı bedelsiz bir şekilde kullanılmaktadır. Direktif, aynı zamanda ilgili kişinin bu hakkı ile ilgili veri sorumlusu tarafından bilgilendirilmesi gerektiğini de belirtmektedir[493].

KVKK'nın 11'inci maddesi ile ilgili kişilerin, otomatik sistemler aracılığıyla analiz edilmesi suretiyle aleyhinde oluşabilecek bir sonucun oluşmasına itiraz etme hakkı bulunmaktadır[494].

---

[489] Sarıusta, s.54.
[490] Develioğlu, s.96.
[491] Başalp, s.96.
[492] Şimşek, s.94.
[493] Küzeci, s.236.
[494] Develioğlu, s.98.

3.4.9. Otomatik karar alınmasını kısıtlama hakkı

Bu hakkın temel amacı, kişilerin otomatik surette değerlendirilmesiyle (profil çıkartılması) verilecek kararlara karşı irade göstererek bireysel özerkliğin korunması ve onları basit bir veri objesine dönüştürülmesini engellemesidir[495]. Bu bağlamda Direktif'in 15/1'inci maddesi ile her birey kendisini etkileyerek hukuki sonuçlara oluşturan otomatikleştirilmiş veri işlemesine dayanan kısıtlamalara tabi olmama hakkına sahip olmaktadır[496]. İlgili kişileri kısıtlayan otomatik veri işlemelere örnek olarak kredi itibarı, iş performans raporları, psikolojik testler örnek olarak verilebilecek olup, bu verilerden hareketle kişiler işe alınamamakta ya da kendilerine kredi verilmeyebilmektedir. Bu nedenle, ilgili hakkın kişisel verilerin korunması açısından pozitif anlamda yeni bir bakış açısı sağladığı belirtilmektedir[497].

Diğer yandan GVKT'nin 22'inci maddesinde bu hakkın kullanılmasına ilişkin istisnalar düzenlenmiş olup, bunlar; ilgili kişinin açık rızasının bulunması, sözleşmenin ifası için gerekli olması ve uygun tedbirleri alması halinde veri sorumlusunun meşru menfaatinin gözetilmesidir. Bu durumlarda veri kişisi otomatik karar alınmasına ve profil çıkartmaya itiraz edemeyecektir[498]. Bununla birlikte, KVKK'da bu hakla ilgili bir düzenleme yapılmadığı görülmektedir.

3.5. Öngörülen Denetim ve Yaptırım Mekanizması

Uluslararası ve ulusal ölçekte kişisel verilerin korunmasına yönelik tüm kanunların gereğinin yerine getirilip getirilmediğini denetlemek çeşitli veri koruma otoriteleri öngörülmüş olup, bu otoriteler; denetleyecekleri verilerin niteliğine göre ayrılmaktadır. Bununla birlikte çeşitli kanun ve diğer mevzuatla, KVKK'da çerçevesi çizilen kişisel verilerin işlenmesi ve korunmasına dair ihlallere yönelik hukuki, idari ve cezai yaptırımlar düzenlenmiştir. Sırasıyla öngörülen denetim ve yaptırımlara aşağıda yer verilecektir.

[495] Şimşek, s.47.
[496] Küzeci, s.236-237.
[497] Dülger, Kişisel Verilerin Korunması, s.175.
[498] Sarıusta, s.55-56.

3.5.1. Kişisel Verileri Koruma Kurumu ve teşkilatı

Kanunun 20'inci maddesi ile kişisel verilerin korunması bakımından uygulamalar ve mevzuatla ilgili gelişmelerin takip edilmesi, paydaşlarla işbirliği yapılması amacıyla mali ve idari özerkliğe sahip ve kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumu kurulmuş olup, 21'inci maddesi ile ise Kurumun gerek bu Kanun gerekse diğer mevzuattan doğan yetkilerini kendi sorumluluğu altında bağımız olarak yerine getireceği ve uygulayacağı belirtilmiştir[499]. Bu yapının kurulmasına gerekçe olarak, 108 Sayılı Sözleşme ile Direktif'e atıfta bulunulduğu görülmektedir[500].

Kurum, karar organı niteliğini haiz, Kişisel Verileri Koruma Kurulu ve Başkanlıktan oluşmaktadır. Kurumun görevleri KVKK'nın 20'inci; Kurulun görevleri 22'inci; Başkan'ın görevleri 24'üncü; Başkanlık organizasyonu ise 25'inci maddelerinde düzenlenmiştir[501].

KVKK 20'inci madde uyarınca; Kurumun görevleri daha ziyade ilgili alanda araştırma yapma, ulusal ve uluslararası alandaki gelişmeleri takip etme gibi konularla sınırlı olup, hazırladığı yıllık faaliyet raporunun muhatabı Cumhurbaşkanlığı, TBMM İnsan Hakları İnceleme Komisyonu ve Başbakanlık'tır. Bununla birlikte, diğer kanunlarda Kurum'un aynı zamanda KVKK'da yer alan ek görevlerle donatılabileceğinin altı çizilmiştir.

KVKK 22'inci madde uyarınca; Kurul ise dokuz üyeden oluşmaktadır. Beş üyesi TBMM, iki üyesi Cumhurbaşkanı, diğer iki üyesi ise Bakanlar Kurulu tarafından seçilmektedir. Kurul'a üye olarak seçilmek için; görev alanındaki konularda bilgi ve deneyim sahibi olmak, devlet memuru olmaya ilişkin genel şartları taşımak, herhangi bir siyasi parti üyesi olmamak, en az dört yıllık lisans düzeyinde yükseköğrenim görmüş olmak ve kamu kurum ve kuruluşlarında, uluslararası kuruluşlarda, sivil toplum kuruluşlarında ve kamu kurumu niteliğindeki meslek kuruluşlarında ya da özel sektörde toplamda en az on yıl çalışmış olmak gerekmektedir[502].

[499] Aysun, s.104-105.
[500] Dülger, Kişisel Verilerin Korunması, s.175.
[501] KVKK, Kişisel Verileri Koruma Kurulu'nun Yapısı ve Görevleri, s.3-4.
[502] KVKK, Kişisel Verileri Koruma Kurulu'nun Yapısı ve Görevleri, s.3-5.

Kurul'un geniş bir görev alanı bulunmakta olup, bunlar şöyle sıralanmaktadır[503];

- *Denetleme:* Bu görev kapsamında Kurul; kişisel verilerin temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak, kişisel verilerle ilgili hak ihlaline uğradığını ileri sürenlerin şikâyetlerini karara bağlamak, şikayet üzerine veya ihlal iddiasını öğrenmesi durumunda res'en görev alanına giren konularla kişisel verilerin kanunlara uygun işlendiğini incelemek ve gerekirse geçici önlemler almak, KVKK'da öngörülen yaptırımları belirlemek ve Veri Sorumluları Sicili'nin tutulmasını sağlamakla görevlidir.

- *Düzenleme:* Kurul; özel nitelikli kişisel verilerin işlenmesi için yeterli önlemleri belirlemek, Kurul'un görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri, veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem, veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmaktan ve diğer kurum ve kuruluşlar tarafından hazırlanan ve kişisel verilere ilişkin hükümler içeren mevzuat taslakları hakkında görüş bildirmek görevlerini üstlenmiştir.

- *Yönetim:* Kurul'un diğer görevleri ise yönetimle ilgili olup; kurumun stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifini görüşmek ve karara bağlamak, kurum performans, mali durum, yıllık faaliyet ve ihtiyaç duyduğu konular hakkında hazırlanan rapor taslaklarını onaylamak ve yayınlamak, taşınmaz alım-satımı ve kiralanması konularında önerileri görüşerek karara bağlamak olarak sıralanmaktadır.

KVKK 24'üncü madde uyarınca; bir diğer önemli aktör ise Kurul Başkanı olup, kendi üyeleri arasından Kurul tarafından seçilir. Kurul'un Başkanı aynı zamanda Kurum'un da Başkanıdır. Başkan, Kurum ve Kurul'un işleyişi açısından geniş yetkilerle donatılmış olup, bunlar; Kurul toplantılarını idare etmek, Kurul kararlarının tebliğini ve Kurulca gerekli görülenlerin kamuoyuna duyurulmasın sağlamak ve uygulanmalarını izlemek, Başkan Yardımcısını, daire başkanlarını ve Kurum personelini atamak, hizmet birimlerinden gelen önerilere son şeklini vererek Kurula sunmak, stratejik planın

[503] Küzeci, s.364-366.

uygulanmasını sağlamak, hizmet kalite standartları doğrultusunda insan kaynakları ve çalışma politikalarını oluşturmak, belirlenen stratejilere, yıllık amaç ve hedeflere uygun olarak Kurumun yıllık bütçesi ile mali tablolarını hazırlamak, Kurul ve hizmet birimlerinin uyumlu, verimli, disiplinli ve düzenli bir biçimde çalışması amacıyla koordinasyonu sağlamak, Kurumun diğer kuruluşlarla ilişkisini yürütmek, Kurum Başkanı adına imzaya yetkili personelin görev ve yetki alanını belirlemek ve Kurumun yönetim ve işleyişine ilişkin diğer görevleri yerine getirmektir[504].

KVKK 25'inci madde uyarınca; Kurumun ve Kurulun büro ve sekretarya işlemlerini yürütmek, Kurumun tarafı olduğu davalar ile icra takiplerinde avukatlar aracılığıyla Kurumu temsil etmek, davaları takip etmek veya ettirmek, hukuk hizmetlerini yürütmek ve Veri Sorumluları Sicilini tutmak gibi işlerden sorumlu Başkan Yardımcısı ve hizmet birimlerinden oluşan Başkanlık oluşturulmuş olup, bu yapı denetim organı açısından büyük önem arz etmektedir[505].

Bu bağlamda, kişisel verileri işleyen gerçek ya da tüzel kişilerin, işleme sürecine başlamadan önce tescil edecekleri bir sicilin oluşturulması gerekmekte olup, bu bağlamda denetim mekanizması içerisinde bir diğer önemli unsur ise Veri Sorumluları Sicili'dir. Kişisel Verileri Koruma Kurulu gözetiminde Başkanlık tarafından kamuya açık olarak tutulacak Veri Sorumluları Siciline kayıt olacak tüzel kişiler için bir ayrım öngörülmemiş olup, kamu ve özel olmak üzere bu yükümlülük tüm tüzel kişileri kapsamaktadır. Ancak, Kurul tarafından sicile kayıta dair istisnalar getirilebilmektedir. Bu istisnaların belirlenmesinde kişisel verilerin niteliği, sayısı, hukuki dayanağı ve üçüncü kişilere aktarılması gibi objektif ölçülere referans verilmektedir. Ayrıca; kişisel verilerin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması, kişinin kendisi tarafından alenileştirilmiş olması, kamu kurum ve kuruluşları tarafından denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması, kişisel verilerin bütçe, vergi ve mali konulara ilişkin olarak devletin ekonomik ve mali çıkarlarının korunması için gerekli olması durumunda kayıt yükümlülüğü uygulanmamaktadır. Veri Sorumluları Siciline kayıt başvurusu yapılırken veri sorumlusu ya da veri temsilcisinin, kimliğini ve veri işleme amacı gibi konular hakkında bildirim yapması zorunlu olup, bu alandaki usul ve esaslar bir

[504] KVKK, Kişisel Verileri Koruma Kurulu'nun Yapısı ve Görevleri, s.7-8.
[505] Küzeci, s.367.

Yönetmelik ile düzenlenmiştir[506]. Diğer yandan, Yönetmelikte yapılan güncel değişiklik ile irtibat kişisi, veri sorumlusu temsilcisi gibi kavramlar yeniden düzenlenmiş ve Başkanlık tarafından Veri Sorumluları sicilinde yer alan ve kamuya açıklanan bilgilere KEP adresi ilave edilmiştir[507].

Veri Kurulu Sicilinin oluşturulması, GVKT ile bir yükümlülük olmaktan çıkartılmıştır. Buna karşın KVKK'da bu işleme yer verilmesi, tartışmaya açık kabul edilmektedir. Ayrıca, AB'de yirmi yıldan fazla süre uygulanmış ve konuya ilişkin önemli bir farkındalık ve güven ortamı oluşturmuş olan bu organın kişisel verilerin korunması mevzuatına yeni adapte olan bir ülkede var olması gerektiği belirtilmektedir[508].

KVKK kapsamında ilgili kişiye bazı haklar ve bu haklarla ilişkili olarak başvuru ve şikâyet usulleri öngörülmekte olup, 11'inci maddede ilgili kişi kanun kapsamındaki taleplerini yazılı olarak ya da Kurum tarafından belirlenecek diğer yöntemleri kullanarak veri sorumlusuna iletebilir. Veri sorumlusu otuz günü geçmemek kaydıyla mümkün olan en kısa sürede talebi kabul etme (ki bu durumda veri kişisinin başka bir makama başvurmasına gerek yoktur) ve gerekçesini açıklamak koşulu ile talebi reddetme yönündeki kararını yazılı olarak ya da elektronik ortamda bildirmelidir. Burada "bildirilmeli" ifadesinin kullanılmasının nedeni veri sorumlusunun 7201 sayılı Tebligat Kanunu hükümlerine tabi olmayan gerçek kişi ya da özel hukuk tüzel kişisi olmasından kaynaklanmaktadır. Talep kabul edildiği takdirde veri sorumlusu tarafından yerine getirilecek olup, veri sorumlusunu başvuru kurula şikâyetin ön koşuludur. Nitekim veri sorumlusunun talebi reddetmesi durumunda gerekçesinin yetersiz olması ya da otuz günde cevap vermemesi gibi durumlarda veri kişisinin Kişisel Verileri Koruma Kurulu'na şikâyet hakkı doğmaktadır. Ancak, Kurul 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun'un 6. maddesindeki şartları taşıyan ihbar ve şikâyetlere altmış gün içerisinde cevap vermediği takdirde veri kişisinin talebi reddedilmiş sayılacaktır. Şayet ihlalin varlığına karar verilirse Kurul bu durumu veri

[506] Veri Sorumluları Sicili Hakkında Yönetmelik, R.G: 30286, 30.12.2017.
[507] Veri Sorumluları Sicili Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik, R.G: 30758, 28.04.2019.
[508] Dülger, Kişisel Verilerin Korunması, s.19.

sorumlusuna tebliğ edecek ve en geç otuz gün içerisinde haklı bulunan talep yerine getirilecektir[509].

Diğer yandan, KVKK'nın 15'inci maddesine göre; Kurul ihlâlin yaygın olduğuna karar vermesi halinde ilke kararı alabilecek olup, yanı sıra telafisi güç ya da imkânsız bazı özel durumlarda ya da açık hukuka aykırılık durumlarında veri işleme ya da yurtdışına aktarımı durdurmaya karar vermeye de yetkilidir.

3.5.2. Kişisel verilerin hukuka aykırı olarak işlenmesinin hukuki sonuçları

KVKK'da kişisel verilerin hukuka aykırı olarak işlenmesine yönelik tazminat, idari yaptırım ve cezai yaptırım başlıkları altında çeşitli yaptırımlar öngörülmekte olup, bunlara sırasıyla aşağıda yer verilmektedir.

Tazminat

Kişisel verilerin hukuka aykırı olarak işlenmesi sonucunda ilgili kişiler maddi ve manevi zararlara uğrayabilmektedir. Buna göre; TMK çerçevesinde kişisel verileri hukuka aykırı olarak işlenen kişilerin Genel Hükümler kapsamında her zaman tazminat talep etme hakkı bulunmakta olup, bu genel Hükümler; TMK'nın 24'üncü ve 25'inci maddeleri ile BK'nın 53'üncü, 54'üncü, 56'ıncı ve 58'inci maddeleridir[510]. KVKK 11'inci madde çerçevesinde; "*kişisel verilerin kanuna aykırı olarak işlenmesi halinde zararın giderilmesini talep etme hakkı"* düzenlenmiştir. Dolayısıyla, KVKK yürürlüğe girmeden önce TMK kapsamındaki hükümlerden hareketle oluşan bu hukuki yola, kanundan sonra daha sık başvurulacağı öngörüler arasındadır[511].

Bunun yanı sıra, KVKK'nın 14/3. maddesi uyarınca kişilik hakkı ihlal edilenlerin genel hükümlere göre tazminat hakkının saklı olduğu belirtilse de, genel hükümler uyarınca talep edilecek tazminat bakımından öncelikle veri sorumlusuna başvurulmasının gerekip

[509] Aysun, s.101-102.
[510] Gürpınar, s.689.
[511] Küzeci, s.369.

gerekmediği konusunda kanun yeterince açık değildir. Ancak, *"Başvuru yoluna gitmenin zorunlu, şikâyet yoluna gitmenin ise ihtiyari olması sebebiyle, başvurusu zımnen veya açıkça reddedilen ilgili kişinin bir yandan doğrudan adli veya idari yargı yoluna gidebilmesi mümkün olacaktır. Ancak, ilgililerin masrafsız ve daha hızlı sonuç alınması mümkün olan şikâyet yolunu tercih edecekleri değerlendirilmektedir"* şeklindeki görüş göz önünde bulundurulduğunda kurula şikâyette olduğu gibi, tazminat davasının da veri sorumlusuna başvuru önkoşuluna bağlandığı söylenebilmektedir. Nitekim idare tarafından kamu hizmetinin sağlıklı sunulabilmesi için toplanan kişisel verilerin korunamaması ve üçüncü kişilere açıklanması tam yargı davalarının konusu olmuş ve Danıştay tarafından kişilik haklarının ihlal edilmesi ile ilgili hizmet kusurunun bulunduğu tespit edilmiştir[512].

Diğer yandan, kişisel verilerinin hukuka aykırı işlenmesinden dolayı zarar gören kişiler, şayet bu zarar malvarlığının eksilmesi şeklindeyse, maddi zararın tazmin edilmesi mümkündür. Bunun için zarar görenin mülkiyet veya zilyetlik gibi temel koruma normları tarafından korunan hukuki değerlerinden birinin ihlal edilmesine gerek yoktur. Bu yönüyle, KVKK aynı zamanda zarar görenin mal varlığını korumaya dönük bir özel koruma normu olarak da değerlendirilmektedir[513].

İdari Yaptırım

KVKK'nın 18'inci maddesi kişisel verilerin işlenmesinde veri sorumlusu olan gerçek kişiler ve özel hukuk tüzel kişileri tarafından gerçekleştirilebilecek ihlâllere yönelik kabahatler düzenlenmiş olup, Kurul tarafından değişen oranlarda idari para cezaları, idari yargı yolu açık olmakla birlikte verilecektir. Öte yandan, kamu kurum ve kuruluşları ile bu nitelikteki meslek kuruluşları bünyesinde böyle bir ihlal işlenmesi halinde ise disiplin sorumluluğu gündeme gelmektedir.

---

[512] "..olayda, davacıya ait röntgenlerin hasta dosyası içerisinde yer almaması ve idare tarafından ibraz edilememesi hizmet kusurunu oluşturduğundan yapılan tıbbi müdahalenin irdelenme imkanını ortadan kaldırdığı, tıbbi müdahalenin irdelenmemesine yol açan grafiklerin saklanmaması şeklindeki hizmet kusuru sonucu davacıların mevcut belirsizlikten dolayı duyduğu üzüntü ve sıkıntıların kısmen de olsa giderilebilmesi için mahkemece takdir edilecek manevi tazminatın ödenmesi gerektiği..", Danıştay 10. D., 27.12.2011, E: 2009/9151, K: 2011/5976.

[513] Gürpınar, s.690.

Bu kapsamda veri sorumlusu; aydınlatma, veri güvenliği, veri sorumluları siciline kayıt ve bildirim yükümlülükleri ile kurul tarafından verilen kararları yerine getirmediği takdirde 5,000 ila 1,000,000 Türk Lirası arasında değişen cezalarla karşılaşmaktadır. Buna göre aydınlatma yükümlülüğün ihlâli, 5,000-10,000 TL; veri güvenliğine ilişkin yükümlülüklerin ihlâli 15,000 TL-100,000 TL; Kurul tarafından verilen kararların yerine getirilmemesi 25,000-1,000,000 TL ve sicile kayıt ve bildirim yükümlülüğünün yerine getirilmemesi ise 20,000-1,000,000 TL arasında idari para cezasına çarptırılmaktadır.

Ancak, KVKK'daki bazı düzenlemelerin idari açıdan yaptırıma tabi olmadığı görülmektedir. Buna göre, verileri meşru amaçlar için işlemeyen ve KVKK 4/2'inci maddedeki hükme aykırı hareket eden veri sorumluları için idari para cezası öngörülmemektedir. Diğer yandan cezaların aralığının geniş tutulması ile alt ve üst sınırlarının uygulanmasında temel alınacak kriterlerin kanunda gösterilmemesi bir başka belirsizliktir. Bir görüşe göre bu ölçütlerin kanunda ekonomik güce ilişkin somut göstergelerle belirlenmesinin yerinde olduğu belirtilmekte ve GVKT örneği sunulmaktadır[514]. Buna göre GVKT'de cezaların üst sınırları şirketlerin cirolarına oranla belirlenirken, idari para cezasında ihlal süresi, ağırlığı, kapsamı gibi hususlar göz önünde bulundurulmuştur.

Bir başka açık olmayan husus ise, idari cezaların eylem temelli mi yoksa ilgili kişi temelli mi uygulanacağı konusu olup, Kabahatler Kanunu'nun 15'inci maddesindeki bir fiilin birden fazla işlenmesi halinde en ağır idari para cezası verileceği hükmünden hareketle hemen hemen her durumda en üst sınır olan 1,000,000 TL'nin uygulanması gerekecektir ki, bu da hakkaniyete uygunluk ilkesiyle çelişmektedir. Bu bağlamda GVKT'de idari para cezası miktarı üzerinde; ihlalin niteliği, ağırlığı, süresi, işlenilen veri türü, işleme amacı, ihlalden zarar gören kişi sayısı ve zarar miktarı hususları göz önünde bulundurulmaktadır.

[514] Küzeci, s.370.

Diğer yandan, ilgili ihlalin kamu kurumunda gerçekleşmesi halinde memur ya da diğer kamu görevlileri hakkında disiplin hükümlerine göre işlem yapılacak ve sonuç Kurula bildirilecekken, kurumda yaygınlık söz konusuysa nasıl bir yaptırım uygulanacağı yeterince açık bulunmamaktadır. Bu bağlamda en büyük veri tekeli olan idarenin idari para cezası almayacağı kabul edilse de, idarenin tekelindeki kişisel verilerin genel ilkelere göre işlenmesini sağlayacak bir yapıya ihtiyaç duyulduğu açıktır[515].

Cezai Yaptırım

KVKK'da ihlal hallerine dair cezai yaptırımlar TCK'nın 135 ila 140'ıncı madde hükümlerine atıfla "Suçlar" başlıklı 17'inci maddede belirtilmiştir. Bu suçlar; kişisel verilerin kaydedilmesi, hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi ile verileri yok etmemedir. Buna göre TCK'nın 135'inci maddesi, bireylerin kişisel verilerinin amaca aykırı bir biçimde kullanılması ve kaydedilmesinin önlenmesi amacıyla düzenlenmiş olup, kişisel verilerin hukuka aykırı olarak kaydedilmesinin fiili suç olduğuna hükmetmekte ve hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası öngörmektedir. Diğer yandan, özel nitelikli kişisel kaydedilmesi durumunda verilecek ceza yarı oranında artırılmaktadır.

Ancak, KVKK'daki ve TCK'daki özel nitelikli veriler arasında uyuşmazlık söz konusu olup, ahlaki eğilimler TCK'da özel bir kategoriyken, KVKK'da değildir. Öte yandan KVKK uyarınca özel nitelikli kişisel veriler olan etnik köken, mezhep ve diğer inanç, kılık-kıyafet, dernek ya da vakıf üyeliği, güvenlik tedbirleri, biyometrik ve genetik verileri TCK'da belirtilen hükümde yer almamaktadır. Bu da KVKK'da aynı kategoride yer alan ve aynı düzenlemenin konusu olan kişisel verilerin farklı cezai yaptırımlar karşılaşması sonucunu doğurmaktadır[516].

TCK'nın 136'ıncı maddesinde ise kişisel verilerin başkasına verilmesi ve yayılması yani korunmasına yönelik ihlaller suç olarak düzenlenmiştir. İlgili maddede suç tipi; kişisel verilerin verilmesi, yayılması ve ele geçirilmesi seçimlik hareketli suçlar olarak tarif

[515] Küzeci, s.373.
[516] Küzeci, s.373.

edilmektedir ve bu hareketlerin gerçekleştirilmesi ile suçun tamamlandığı kabul edilmektedir. Bu suça dair cezai yaptırım ise 2 yıldan 4 yıla kadar hapis cezasıdır[517].

KVKK'nın 7'inci maddesine aykırı şekilde kişisel verileri silmeyen ya da anonim hale getirmeyenler TCK'nın 138'inci maddesine göre bir yıldan iki yıla kadar hapisle cezalandırılmaktadır. Suçun konusu CMK hükümlerine göre ortadan kaldırılması ya da yok edilmesi gereken veri ise verilecek ceza bir kat artmaktadır.[518].

Ayrıca, TCK'nın 140'ıncı maddesi yukarıdaki maddelerde sayılan suçların işlenmesi nedeniyle tüzel kişilerin hakkında bunlara özgü güvenlik tedbirlerine hükmedileceği düzenlenmiş olup, bu tedbirler TCK 60'ıncı maddede; kamu kurumu tarafından verilen veri işleme izninin iptali, eşya ve kazanç müsaderesi düzenleneceği özel hukuk tüzel kişileri de kapsayacak şekilde belirtilmiştir[519]. TCK'nın 139'uncu maddesi ile söz konusu suçların şikâyete bağlı olmadığı kabul edilmiştir[520]. Diğer yandan, TCK'da kişisel verilerin işlenmesi ihlaline ilişkin suçlar bakımından TCK ve CMK hükümleri uyarınca cezanın ertelenmesi ve hükmün açıklanmasının geri bırakılması uygulanmayabileceğinden, hüküm kesinleşirse hapis cezası kaçınılmaz olabilmektedir. Ancak, kişisel verileri ihlal eden birinin hapis cezası ile cezalandırılması nadir görülen bir uygulama olup, yaptırım sisteminin etkili olabilmesi için cezanın caydırıcılığının yanı sıra, orantılı olması da gözetilmelidir[521].

[517] Dülger, Ceza Normu, s.132.
[518] Küzeci, s.375.
[519] Çal, Alp: "Kişisel Verileri Koruma Kanunu'na Aykırılık, Yaptırımlar ve Yargı Yolu", https://www.ozbek.av.tr/kvk-blog/kisisel-verileri-koruma-kanununa-aykirilik-yaptirimlar-ve-yargi-yolu/, (Erişim Tarihi): 27.04.2019.
[520] Develioğlu, s.126.
[521] Küzeci, s.373.

SONUÇ

Tarihin en eski dönemlerine dayanan ve idari süreçleri kolaylaştırmayı amaçlayan kişisel verilerin kayıt altına alınması ve buna karşın hukuka uygun şekilde idari tekel haricinde bu verilere erişilmemesine yönelik kişisel verilerin korunması hakkı büyük önem arz etmektedir. Bu hakkın, özellikle II. Dünya Savaşı'ndan önce yükselen totaliter eğilimlerle birlikte büyük toplumsal yıkımlara sebebiyet verecek şekilde ihlâl edildiği görülmektedir. Savaş sonrasında, dünya barışını yeniden tesis etmek üzere oluşturulan kurumların gerçekleştirdiği düzenlemelerde ve yargı kararlarında bu hakkın korunması yönünde gelişmelerin söz konusu olduğu, ancak bilgi teknolojilerindeki gelişmeler ve küreselleşmeyle birlikte kişisel verilerin tanımının geliştiği, buna karşılık ilgili verilerin korunması hakkına karşı yeni riskler ve tehditler oluştuğu görülmektedir. Bugün bir yanda kamu düzeni, bir yanda ticari girişimlerin hukuka aykırı ya da uygun kişisel veriye erişim talebi, diğer yanda ise kişilerin kişilik hakkının bir parçası olarak kişisel verileri koruma hakkı bulunmaktadır.

Kimliği belirli veya belirlenebilir nitelikteki bir gerçek kişiye ilişkin her türlü bilgi olan kişisel verilerin korunması hakkı, kişilerin toplum içerisinde mahremiyetlerine dönük endişe yaşamadan ve kişiliklerini serbestçe geliştirmelerine imkân tanıyan bir haktır ve hukuki dayanağını kişilik hakkı ve özel hayatın gizliliği hakkı oluşturmaktadır. Sınırsız bir şekilde korunmayan bu hak, OECD, BM, AB gibi uluslararası kurumların düzenlemelerinde ve başta Avrupa ülkeleri olmak üzere devletlerin ulusal hukuklarında uzun süredir yer almaktadır. Bazı ülkelerin geçmişindeki otoriter deneyimler nedeniyle bireysel hak ve özgürlüklerin korunmasına verilen önem; elektronik ticaret başta olmak üzere teknolojinin yarattığı riskler ve Avrupa ile ticaret yapmak isteyen üçüncü ülkelere veri aktarımının koruma altına almak isteyen bu düzenlemeler ışığında bir kişisel verileri koruma kanunu için gerekli ortam Türkiye'de de bulunmaktadır.

Nitekim ilgili hak, 2010 yılında gerçekleştirilen referandum sonrası Anayasa'nın 20'inci maddesine eklenen fıkrayla bu yöndeki çalışmaların 1989 yılına kadar geri götürülebileceği Türk hukukunda anayasal güvence altına alınmış, KVKK'nın kabulüyle birlikte özel bir kanuni düzenlemeye sahip olmuştur. Bu sayede, 108 sayılı AK Sözleşmesi'nin 4'üncü maddesinde belirtilen yükümlülük ile Anayasa'nın 20'inci maddesinde belirtilen kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği hükmü yerine getirilmiştir.

Görüldüğü üzere Türkiye'de gerek geçmişteki fişleme iddialarına kadar varan gelişmeler ve devletin merkezi rolü gerekse de bağlı olunan uluslararası anlaşmalar ve örgütlerin perspektifleri itibari ile kişisel verilerin korunması hakkı dinamik bir kategori olmayı sürdürmektedir. Nitekim Türkiye bu alanda son yıllarda büyük bir gelişme kaydetse de, bu alanda düzenleyici asıl kanun olan KVKK'nın bugün Direktif, GVKT ve 108 sayılı sözleşmeye kıyasla birçok geriden gelen boyutu olduğu, KVKK'nın ilga edilen Direktif'ten hareketle hazırlanması, KVKK ile GVKT arasındaki uyumsuzluklar hem doktrindeki tartışma konuları arasındadır hem de AB raporlarında eksiklikler olarak şerh düşülmüştür. KVKK'da daha geniş tanımıyla unutulma hakkının yerine sildirme hakkıyla sınırlı kalınması, şeffaflık ilkesinin ayrıntılı şekilde düzenlenmemesi, hesap verilebilirlik ilkelerine yer verilmemesi, bir hakkın tesis, kullanılması veya korunması için veri işlemenin zorunlu olması istisnası, çocukların açık rızasına dair bir düzenleme yapılmaması, veri güvenliğine ilişkin yükümlülüklerin çok daha genel şekilde düzenlenmesi, işlemenin sınırlandırılması hakkına, otomatik karar alınmasını kısıtlama hakkına ve verilerin taşınması hakkına yer verilmemesi vb. buna örnek olarak verilebilir.

Bununla birlikte KVKK 28/1'inci maddesindeki, kişisel verilerin işlenmesinde istisna durumlar gelmektedir. Örneğin; kişisel verilerin sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi hususu bunlardan biridir. Buna göre, KVKK'da "milli savunma, milli güvenlik, kamu güvenliği, kamu düzeni, ekonomik güvenlik, özel hayatın gizliliği veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla" ibaresi, bu ölçütleri muğlak kılmakta ve kimin tarafından karar verileceği tartışmasını beraberinde getirmektedir. Metnin kaleme ele alınış biçimi,

bazı durumlarda düşünce özgürlüğünün aleyhine bir işleyişe imkân tanımaktadır. Benzer şekilde "önleyici, koruyucu ve istihbari faaliyetler kapsamında verilerin işlenmesine" istisna tanıyan fıkra da, içerdiği soyut, belirsiz ve geniş kapsamlı ifadeler, istisna ya da yetki sınırının olmaması, yetki aşımı ve kötüye kullanımlara karşı etkin yolların belirlenmemesi ve bireyin devlet otoritesi karşısında korumasız bırakılması itibari ile keyfi uygulamalara ve fişlemelere kadar varabilecek bir zemin sağlamaktadır. Bu bağlamda, gerek VKY gerekse onu ilga eden GVKT ile karşılaştırıldığında KVKK'nın çok geniş bir istisnalar listesi düzenlendiği ve bunun aslında Kanun'un uygulama alanını daralttığı görülmüştür.

Bir diğer sorun ise KVKK öncesi ulusal mevzuat ile KVKK'da ele alınan bazı kategorilerin uyuşmaması, bununsa hukuki sonuçlar itibari ile uygulama alanını daraltmasıdır. Örneğin; TCK'daki özel nitelikli kişisel veri kategorisi ile KVKK'dakiler arasındaki ayrışma, cezai yaptırım konusunda uyumsuzluklar oluşturmaktadır. KVKK'da GVKT'ye kıyasla ilgili kişilerin haklarının çok daha sınırlı sayıda düzenlenmiş olması ise bir başka güncellik sorunudur.

Türkiye'nin özellikle AB üyelik sürecinde gerçekleştirdiği reformlarla ciddi bir mesafe kaydettiği aşikar olmakla birlikte, merkezi devlet yapısı, güçlü güvenlik paradigması, keyfi uygulamalara açık zemin ve geniş istisnalar listesi KVKK'nın uygulanması üzerindeki gölgeler olarak öne çıkmaktadır. Şahsi kanaatimiz, tüm bu olumlu ve olumsuz eleştirilere rağmen KVKK'nın yürürlüğe girmesi Türk hukukunda çok büyük bir boşluğu doldurduğu yönündedir. Ayrıca, her ne kadar içerdiği bazı unsurların (Örn; Veri Sorumluları Sicili) güncel AB mevzuatında yer almaması tartışma konusu edilse de, bu alanda yeni mesafe kat etmeye başlamış bir ülkede farkındalık düzeyini arttırmaya katkı sağlayacağı açıktır.

Unutulmamalıdır ki, kişisel verilerin etkin şekilde korunmasının yolu, bu bağlamda bir toplumsal kültür oluşmasına bağlıdır. Bunun yolu ise ulusal mevzuatın uyumlaştırılması ve kişilerin kişisel verileri hakkında bilinçlenmesiyle ilişkilidir. Nitekim KVKK ile oluşturulan Kurum, bu yönde öncü çalışmalar yapmakta ve böyle bir kültürün oluşmasına katkı sağlamaktadır. Bu kültür sadece ilgili kişilerin değil aynı zamanda veri sorumluları ve varsa veri temsilcilerinin de gerek özel gerek kamu sektörü olarak

bilinçlenmesiyle tesis edilecektir. Bu sayede kişisel veri koruma kültürünün güçlenmesi ve kişisel verilerin korunması hakkına karşı ihlâllerin sayısının azalması beklenmektedir. Bu amaç, ülkemizin insan haklarına saygılı, demokratik bir hukuk devleti olma idealinin gerçekleşmesine büyük katkı sağlayacaktır.

KAYNAKÇA

Kitaplar

Akdağ, Hale: Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Adalet Yayınevi, Ankara 2013.

Akgül, Aydın: Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması (Danıştay ve Avrupa), Beta Basım Yayın, İstanbul 2016.

Aksoy, H. Can: Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara 2010.

Aşıkoğlu, Ş. İpek: Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, On İki Levha Yayıncılık, İstanbul 2018.

Aydın, S. Erdem: Kişisel Verilerin Kaydedilmesi Suçu, Oniki Levha Yayıncılık, İstanbul 2015.

Aysun, M. Köse: Kişisel Verilerin Kaydedilmesi Suçu, Seçkin Yayınevi, Ankara 2018.

Başalp, Nilgün: Kişisel Verilerin Korunması ve Saklanması (Kişisel Verilerin Korunması), Yetkin Yayınları, Ankara 2004.

Bayram, M. Hanifi: Avrupa Birliği ve İnternet Hukuku, Seçkin Yayınevi, Ankara 2011.

Çekin, M. Serdar: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, Oniki Levha Yayıncılık, İstanbul 2018.

Develioğlu, H. Murat: Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Kanunu, Oniki Levha Yayıncılık, İstanbul 2017.

Dülger, M. Volkan: Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi Yayınları, İstanbul 2019 (Kişisel Verilerin Korunması).

Güven, Vesile: Sağlık Hukukunda Tıbbi Kayıtların Tutulmasından ve Saklanmasından Doğan Sorumluluk, Adalet Yayınevi, Ankara 2016.

Ketizmen, Muammer: Türk Ceza Hukukunda Bilişim Suçları, Adalet Yayınevi, Ankara 2008.

Kişisel Verileri Koruma Kurumu: Kişisel Verilerin Korunması Kanunu ve Uygulaması Kitapçığı, Ankara 2017.

Korkmaz, İbrahim: Kişisel Verilerin Ceza Hukuku Kapsamında Korunması (Kişisel Veriler ve Ceza), Seçkin Yayınevi, Ankara 2017.

Küzeci, Elif: Kişisel Verilerin Korunması, Seçkin Yayınevi, 2. Baskı, Ankara 2018.

Şimşek, Oğuz: Anayasa Hukukunda Kişisel Verilerin Korunması, Beta Yayınevi, Ankara 2008.

Taştan, F. Güven: Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, Oniki Levha Yayıncılık, İstanbul 2017.

Makaleler

Akgül, Aydın: "Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" ve AB Adalet Divanı'nın "Google Kararı" (Unutulma Hakkı), Türkiye Barolar Birliği Dergisi 116, Ankara 2016, ss.11-38.

Akkurt, S. Sami: "Kişilik Hakkının Sosyal Medya Kullanıcıları Tarafından İhlâli Halinde Ortaya Çıkacak Cezaî Sorumluluğa Medeni Hukuk Bağlamında Bir Bakış", Selçuk Üniversitesi Hukuk Fakültesi Dergisi 25 (2), Konya 2017, ss.329-373.

Arslan, Çetin: "Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması", BAÜHF Kazancı Hakemli Hukuk Dergisi, Mart-Nisan, İstanbul 2011, ss.31-61.

Atasoy, Kemal: "Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 3, İstanbul 2016, ss.269-301.

Atak, Songül: "Avrupa Konseyi'nin Kişisel Verileri Açısından Sağladığı Temel Güvenceler", Türkiye Barolar Birliği Dergisi 87, Ankara 2010, ss.90-120.

Başalp, Nilgün: "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri" (Avrupa Birliği), Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 1 (21), İstanbul 2015, ss.77-105.

Belge, A. Merve: "Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlâli ve Korunması Yolları", D.E.Ü. Hukuk Fakültesi Dergisi, Özel Sayı, İzmir 2017, ss.1025-1051.

Büken N. Örnek ve Ünsal, Ç. Zeybek: "Kişisel Verilerin Korunması Kanunun Biyomedikal Alana Yansımaları Açısından Değerlendirilmesi, Hacettepe Hukuk Fakültesi Dergisi 7, Ankara 2017, ss.33-54.

Culnan, Mary J., "How Did They Get My Name?": An Exploratory Investigation of Consumer Attidudes toward Secondary Information Use", MIS Quarterly3, 1993, pp.341-363.

Doğan, Korcan ve Arslantekin, Sacit: "Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum", DTCF Dergisi 56, Ankara 2016, ss.15-36.

Doğan, P. Bahar: "Çatışan İki Değer: Haber Verme Hakkı ve Kişilik Hakkı", Ankara Barosu Dergisi 4, Ankara 2014, ss. 477-493.

Dülger, M. Volkan. "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 3 (2), İstanbul 2016, ss. 101-167 (Ceza Normu).

Elmalıca, Hasan: "Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı", Ankara Üniversitesi Hukuk Fakültesi Dergisi 65, Ankara 2016, ss.1603-1636.

Gülener, Serdar: "Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak Unutulma Hakkı", Türkiye Barolar Birliği Dergisi 102, Ankara, ss.219-240.

Gürpınar, Damla: "Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk", D.E.Ü. Hukuk Fakültesi Dergisi Özel Sayı, İzmir 2017, 679-694.

Kılınç, Doğan: "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", Ankara Üniversitesi Hukuk Fakültesi Dergisi 61 (3), Ankara 2012, ss.1089-1169.

Korkmaz, İbrahim: "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme" (Kişisel Verilerin Korunması), Türkiye Barolar Birliği Dergisi 124, Ankara 2016, ss.81-152.

Kutlu, Önder ve Kahraman, Selçuk: "Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi", Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi 5, İstanbul 2017, ss.45-62.

Manav, Eda: "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", Gazi Üniversitesi Hukuk Fakültesi Dergisi, 2, Ankara 2015, ss.95-136.

Oğuz, Habip: "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum", Uyuşmazlık Mahkemesi Dergisi, 3 (0), Ankara 2014, ss. 3-38.

Oğuz, Sefer: "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri", Bilgi ve Yönetim Dergisi 13 (2), Ankara 2018, ss.121-138.

Sancakdar, Oğuz: "Kamu Hukukunda Kişiliğin Korunması", İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi 16, İstanbul 2017, ss.39-67.

Şen, Ersan: "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", İstanbul Barosu Dergisi, 83 (3), İstanbul 2009, ss. 1197-1214.

Şıracı, Sertel: "Açık Rıza Bağlamında Fiziki ve Sanal Ortamda Uygulama Sorunları", Kişisel Sağlık Verileri 3. Ulusal Kongresi Bildiri Kitabı, İstanbul 2018.

Uncular, Selin: İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Seçkin Yayınevi, Ankara 2018.

Tekin, Nurullah: "Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", Uyuşmazlık Mahkemesi Dergisi 4, Ankara 2014, ss.222-262.

Tezcan, Durmuş: "Bilgisayar Karşısında Özel Hayatın Korunması", Anayasa Dergisi, Ankara 1991, ss.385-392.

Yücedağ, Nafiye: "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 2, İstanbul 2017, ss.765-790.

Tezler

Akgül, Aydın: Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi (Kişisel Verilerin Korunması), (Yayınlanmamış Doktora Tezi), Kocaeli 2013.

Ayözger, A. Çiğdem: Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması (Yayımlanmamış Doktora Tezi), İstanbul 2016.

Erdinç, G.H. 2017. Bilgi Güvenliği, Kişisel Verilerin Korunması ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler, Yayımlanmamış Yüksek Lisans Tezi, İstanbul: İstanbul Teknik Üniversitesi, Bilişim Uygulamaları Anabilim Dalı.

Henkoğlu, Türkay: Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi (Yayınlanmamış Doktora Tezi), Ankara 2015.

Sarıusta, Kader: Kişisel Verilerin Ceza Hukuku Yoluyla Korunması (Yayımlanmamış Yüksek Lisans Tezi), Gaziantep 2018.

Sert, Şeyma: Kişisel Verilerin 5237 Sayılı Türk Ceza Kanunu Kapsamında Korunması (Yayımlanmamış Yüksek Lisans Tezi), Erzurum 2018.

Online Kaynaklar

Avrupa İnsan Hakları Sözleşmesi,

http://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf, (Erişim Tarihi): 01.04.2019.

Avrupa Komisyonu'nun 09.11.2016 tarihli, SWD (2016), 366 nihai sayılı AB Genişleme Politikasına İlişkin 2016 Türkiye Raporu, https://www.ab.gov.tr/files/ceb/Progress_Reports/2016_ilerleme_raporu_tr.pdf, (Erişim Tarihi): 29.03.2018.

Çal, Alp: "Kişisel Verileri Koruma Kanunu'na Aykırılık, Yaptırımlar ve Yargı Yolu", https://www.ozbek.av.tr/kvk-blog/kisisel-verileri-koruma-kanununa-aykirilik-yaptirimlar-ve-yargi-yolu/, (Erişim Tarihi): 27.04.2019.

"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, (Erişim Tarihi): 26.04.2019.

Dülger, M. Volkan, "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik'in Getirdikleri ve Dikkat Edilmesi Gereken Hususlar",

http://dulger.av.tr/2018/07/12/kisisel-saglik-verilerinin-islenmesi-ve-mahremiyetinin-saglanmasi-hakkinda-yonetmelikte-degisiklik-yapilmasina-dair-yonetmelikin-getirdikleri-ve-dikkat-edilmesi-gereken-hususlar/ (Kişisel Sağlık), (Erişim Tarihi): 21.04.2019.

Eralp, Özgür: "Veri Sorumlusunun Meşru Menfaatleri için Veri İşlenmesinin Zorunlu Olması", https://www.ozgureralp.com.tr/soru-327-ilgili-kisinin-temel-hak-ve-ozgurluklerine-zarar-vermemek-kaydiyla-veri-sorumlusunun-mesru-menfaatleri-icin-veri-islenmesinin-zorunlu-olmasi-ne-anlama-gelmektedir/, (Erişim Tarihi): 15.04.2019.

Küzeci, Elif: "Avrupa Konseyi'nin 108 Sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter kararı ve diğer bazı gelişmelere ilişkin bir değerlendirme",

https://medium.com/@elfkzc/avrupa-konseyinin-108-say%C4%B1l%C4%B1-ki%C5%9Fisel-verilerin-korunmas%C4%B1-s%C3%B6zle%C5%9Fmesi-yenilendi-bc8daad9decc, (Erişim Tarihi): 01.04.2019.

Serozan, Rona: "Kişilik Hakkının Korunmasıyla İlgili Bazı Düşünceler", Mukayeseli Hukuk Araştırmaları Dergisi 14, 1977, ss.93-112,

http://dergipark.gov.tr/download/article-file/14235, (Erişim Tarihi): 31.03.2019.

Şeker, A. Ömer, "Bilimsel Araştırmalarda Kişisel Veri", https://medium.com/@aseker/bilimsel-ara%C5%9Ft%C4%B1rmalarda-ki%C5%9Fisel-veri-e3fc72a616eb, (Erişim Tarihi): 21.04.2019.

Türk Dil Kurumu:

http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c9894bf10f272.34340734, Erişim Tarihi (25.03.2019).

Yargı Kararları

ABAD, C-131/12 Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131, (Erişim Tarihi): 13.5.2014.

"BVerfGE 65, 1 (44)",

https://www.datenschutzbeauftragter-online.de/das-bundesdatenschutzgesetz-bdsg/urteile-des-bverfg-zur-informationellen-selbstbestimmung/ (Erişim Tarihi): 28.03.2019,

"Case of Campbell v. Mirror Group Newspapers", Başvuru No: UKHL 22, 6.5.2004, https://www.5rb.com/case/campbell-v-mgn-ltd-hl/, (Erişim Tarihi): 16.04.2019.

"Case of Gaskin v. the United Kingdom", Başvuru No: 10454, 7.7.1989, http://www.juridischeuitspraken.nl/19890707EHRMGaskin.pdf, (Erişim Tarihi): 01.04.2019,

"Case of Klass and Others v. Germany", Başvuru No: 5029/71, 06.09.1978,

https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}, (Erişim Tarihi): 01.04.2019.

"Case of Peck v. The United Kingdom", Başvuru No: 44647/98, 28.1.2003, , https://www.5rb.com/wp-content/uploads/2013/10/Peck-v-UK-ECHR-28-Jan-03.pdf, (Erişim Tarihi): 14.04.2019.

"Case of Z v. Finland", Başvuru No: 22009/93, 25.1.1997,

http://www.worldlii.org/eu/cases/ECHR/1997/10.html,

(Erişim Tarihi): 14.04.2019.

"Leander v Sweeden", Başvuru No: 9248/81, 26.03.1987, https://swarb.co.uk/leander-v-sweden-echr-26-mar-1987/, (Erişim Tarihi): 01.04.2019.

"S and Marper v UK, , https://justice.org.uk/s-marper-v-uk-2008/, (Erişim Tarihi): 03.04.2019.

X.v. Türkiye, Başvuru No: 24626/09, 9.10.2012.

Von Hannover vb. Germany, Başvuru No. 59320/00, 24.06.2004.

ÖZGEÇMİŞ

Kişisel Bilgiler
Adı Soyadı : Habip Bozkurt
Doğum Yeri ve Tarihi : İstanbul, 27.02.1980

Eğitim Durumu
Lisans Öğrenimi : İstanbul Üniversitesi Hukuk Fakültesi
Bildiği Yabancı Diller : İngilizce

İş Deneyimi
Çalıştığı Kurumlar ve Tarihleri: Küresel Hukuk Danışmanlık (2005-….)

İletişim
Telefon : 05327358017
E-posta Adresi : habipbozkurt@kureselhukuk.com