T.C.

SELÇUK ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ÖZEL HUKUK ANABİLİM DALI

ÖZEL HUKUK BİLİM DALI

KİŞİSEL VERİLERİN KORUNMASI

Yasemin AVCI

YÜKSEK LİSANS TEZİ

DANIŞMAN

Dr. Öğr. Üyesi Nurşen AYAN

KONYA 2019

T. C.

SELÇUK ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü

Bilimsel Etik Sayfası

Öğrencinin	Adı Soyadı	Yasemin AVCI
	Numarası	144233001007
	Ana Bilim / Bilim Dalı	Özel Hukuk / Özel Hukuk
	Programı	Tezli Yüksek Lisans ■ Doktora □
	Tezin Adı	Kişisel Verilerin Korunması

Bu tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını bildiririm.

Yasemin AVCI

T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

Yüksek Lisans Tezi Kabul Formu

Öğrencinin	Adı Soyadı	Yasemin AVCI
	Numarası	144233001007
	Ana Bilim / Bilim Dalı	Özel Hukuk/Özel Hukuk
	Programı	Tezli Yüksek Lisans ☒ Doktora ☐
	Tez Danışmanı	Dr. Öğr. Üyesi Nurşen AYAN
	Tezin Adı	Kişisel Verilerin Korunması

Yukarıda adı geçen öğrenci tarafından hazırlanan **Kişisel Verilerin Korunması** başlıklı bu çalışma **03.07.2019** tarihinde yapılan savunma sınavı sonucunda oybirliği/oyçokluğu ile başarılı bulunarak, jürimiz tarafından yüksek lisans tezi olarak kabul edilmiştir.

Ünvanı, Adı Soyadı	Danışman/Üye	İmza
Dr. Öğr. Üyesi Nurşen AYAN	Danışman	
Dr. Öğr. Üyesi Sinan Sami AKKURT	Üye	
Dr. Öğr. Üyesi Süheyla ZORLU	Üye	

T. C.

SELÇUK ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü

Öğrencinin	Adı Soyadı	Yasemin AVCI
	Numarası	144233001007
	Ana Bilim / Bilim Dalı	Özel Hukuk / Özel Hukuk
	Programı	Tezli Yüksek Lisans ■ Doktora ☐
	Tez Danışmanı	Dr. Öğr. Üyesi Nurşen AYAN
	Tezin Adı	Kişisel Verilerin Korunması

ÖZET

Kişisel veri, belirli veya belirlenebilir nitelikteki gerçek kişiye ilişkin verileri ifade eder. Söz konusu tanım, uluslararası düzenlemeler ışığında hazırlanmış olan ve 2016 yılında kabul edilen Kişisel Verilerin Korunması Kanunu tarafından esas alınmıştır. Bu çalışma ile kişilerin, anayasal bir hak olan kişisel verilerin korunmasını talep etme hakkının ileri sürebileceği yollar açıklanmaya çalışılmıştır. Kişisel Verilerin Korunması adlı bu çalışma üç bölümden oluşmaktadır. Birinci bölümde, kişisel veri kavramı, unsurları, türleri ve ilgili diğer kavramlar açıklanmış, kişisel verilerin korunması isteminin tarihî gelişimi ile ulusal ve uluslararası kaynakları incelenmiş ve kişisel verilerin hukukî niteliği belirlenmeye çalışılmıştır. İkinci bölümde, kişisel verilerin işlenmesinde göz önüne alınacak temel ilkeler açıklanmış, kişisel verilerin işlenmesinin, aktarılmasının, imha edilmesinin şartları incelenmiş ve bu bağlamda ilgili kişinin haklarına ve veri sorumlusunun yükümlülüklerine yer verilmiştir. Üçüncü ve son bölümde ise, kişisel verilerin hukuka aykırı olarak işlenmesi sebebiyle başvurulabilecek koruma yolları incelenmiştir. Koruma yolları açıklanırken kişisel verilerin korunması hukukuna ek olarak, medenî hukuk, iş hukuku ve Kişisel Verilerin Korunması Kanununun yaptığı atıf çerçevesinde ceza hukuku hükümlerine yer verilmiştir.

Anahtar Kelimeler: Kişisel Veri, Özel Hayatın Gizliliği, Kişisel Verilerin İşlenmesi, Veri Koruma Hukuku, Kişilik Hakkı

T. C.

SELÇUK ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü

Öğrencinin	Adı Soyadı	Yasemin AVCI
	Numarası	144233001007
	Ana Bilim / Bilim Dalı	Özel Hukuk / Özel Hukuk
	Programı	Tezli Yüksek Lisans ■ Doktora ☐
	Tez Danışmanı	Dr. Öğr. Üyesi Nurşen AYAN
	Tezin İngilizce Adı	Protection of Personal Data

SUMMARY

Personal data refers to data relating to an identified or identifiable natural person. This definition is based on the Law on the Protection of Personal Data, which was adopted in 2016 in light of international regulations. In this study, it is tried to explain how the persons whose personal data are processed can claim the right of protection of personal data which is a constitutional right. This study, called Protection of Personal Data, consists of three parts. In the first part, the concept of personal data, its elements, types, and other related concepts are examined, the historical development of the request for protection of personal data and national and international sources are examined and the legal quality of personal data is tried to be determined. In the second section, the basic principles to be considered in the processing of personal data are explained, the conditions of processing, transferring, destruction of personal data are examined and the rights of the person concerned and the responsibilities of the data controller are given. In the third and the last part, protection methods that can be used due to unlawful processing of personal data are examined. While explaining the ways of protection, in addition to the protection of personal data law, the provisions of civil law, labor law and the protection of personal data are included in the criminal law provisions.

Key Words: Personal Data, Privacy of Private Life, Personal Data Processing, Data Protection Law, Personality Rights

İÇİNDEKİLER

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN

HUKUKA AYKIRI OLARAK İŞLENMESİNE KARŞI

KORUMA YOLLARI

KISALTMALAR

108 sayılı Sözleşme	: 108 sayılı Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısınıda Bireylerin Korunması Sözleşmesi *(Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)*
1995/46 sayılı Yönerge	: 1995/46 sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunması Hakkında Avrupa Parlamentosu ve Konseyi Yönergesi *(Directive 95/46/EC of the European Parliament and of The Council on The Protection of İndividuals with regard to the Processing of Personal Data and on the Free Movement of Such Data)*
1997/66 sayılı Yönerge	: Telekomünikasyon Sektöründe Gizliliğin Korunması ve Kişisel Verilerin İşlenmesi Hakkında Avrupa Parlamentosu ve Konseyi Yönergesi Yönergesi *(Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector)*
2002/58 sayılı Yönerge	: Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönerge *(Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector)*
AAD.	: Avrupa Adalet Divanı
AB.	: Avrupa Birliği
AİHM.	: Avrupa İnsan Hakları Mahkemesi
AİHS.	: Avrupa İnsan Hakları Sözleşmesi

BK.	: 6098 sayılı Türk Borçlar Kanunu
bkz.	: bakınız
BM.	: Birleşmiş Milletler
C.	: Cilt, Information and Notices, Case
CD.	: Yargıtay Ceza Dairesi
CK.	: 5237 sayılı Türk Ceza Kanunu
D.	: Daire
dn.	: dipnot
E.	: Esas
EURODAC.	: European Asylum Dactyloscopy Database *(Avrupa İltica Parmak İzi Veri Tabanı)*
f.	: fıkra
GVKT.	: Genel Veri Koruma Tüzüğü *(General Data Protection Regulation)*
HD.	: Yargıtay Hukuk Dairesi
HMK.	: 6100 sayılı Hukuk Muhakemeleri Kanunu
K.	: Karar
kn.	: kenar numarası
Kurul	: Kişisel Verileri Koruma Kurulu
KVKK.	: 6698 sayılı Kişisel Verilerin Korunması Kanunu
L.	: Legislation *(Mevzuat)*
MK.	: 4721 sayılı Türk Medenî Kanunu
OJ.	: Official Journal of The European Union / Official Journal of The European Communities *(Avrupa Birliği Resmi Gazetesi / Avrupa Toplulukları Resmi Gazetesi)*
p.	: page *(sayfa)*

RG.	: Resmî Gazete
s.	: sayfa
S.	: Sayı
TK.	: 6102 sayılı Türk Ticaret Kanunu
V.	: Volume *(Cilt)*
vd.	: ve devamı
VERBİS.	: Veri Sorumluları Sicil Bilgi Sistemi
VSSHY.	: Veri Sorumluları Sicili Hakkında Yönetmelik
WP.	: Working Party *(Çalışma Grubu)*

GİRİŞ

Günümüzde, bilişim teknolojilerinin kullanımı verilerin işlenmesini de kaçınılmaz kılmaktadır. Verilerin işlenmesi, özellikle bilişim sistemleri göz önüne alındığında, büyük miktarda verilerin muhafaza edilmesini, arşivlenmesini, aktarılmasını, açıklanmasını kolaylaştırmaktadır. Sözü edilen olumlu yönlerinin yanında, olumsuz bir takım yönler de açığa çıkmaktadır. İşlenen verilerin kişiyi belirli veya belirlenebilir kıldığı göz önüne alındığında, bu verileri hukuka aykırı olarak elde eden, kullanan, depolayan veya aktaran kişilerin menfaat elde etme amaçları ortaya çıkmıştır. Nitekim, yeni dünyada petrol niteliğine sahip olduğu ifade edilen veri, gücü de beraberinde getirmektedir. Bunu öngören teşebbüsler ve kurumlar, kişisel verileri kullanarak hedef kitlesini kolaylıkla tespit etmeyi, sundukları hizmetin kalitesini artırmayı ve bu bilgileri satarak ticarî kazanç elde etmeyi hedeflemişlerdir. Bu durumlar, teşebbüsler açısından bir kazanç elde etme yöntemi hâlini almakla birlikte, kişiler açısından ihlâlleri ve zararları da beraberinde getirmektedir.

Gücün peşinde ilerleyen kitleler, bu yolda bireyin temel hak ve özgürlüklerini hiçe sayarak farklı yollarla veri işlemeyi sürdürürken, kişilerin, ayırt edici özellikleri üzerinden ayrımcılığa maruz kalmaları veya toplumdan dışlanmaları söz konusu olmuştur. Bu durum, gerek kamu sektöründe gerekse özel sektörde, kişisel verilerin işlenmesi karşısında bireyin temel hak ve hürriyetlerinin korunmasını gerektirmiştir. Ancak, bu koruma amacının mutlak olmadığı da ifade edilmelidir. Zira, başlangıçta da belirtildiği gibi, günümüzde veri paylaşımı gerekli ve kaçınılmazdır. Bu sebeple, kişiye ilişkin temel hak ve hürriyetlerin ihlâlinin önüne geçilmesi ve veri akışının devam etmesi hedeflenmiştir. İşte bu amaçlarla, özellikle, yirminci yüzyılın ikinci yarısından itibaren, kişisel veri koruma mevzuatı, uluslararası alanda gelişmeye başlamıştır.

Özellikle, Avrupa Birliği bünyesinde ortaya çıkan gelişmeler ve bu gelişmeleri takip eden düzenlemeler, kişisel verilerin korunması alanında yön belirleyici olmuştur. Türkiye'de ise, uluslararası alanda atılan adımlara yabancı kalmamak ve ihtiyaçları karşılamak amacıyla, 2016 yılında, doğrudan kişisel verilerin korunmasını

düzenleyen 6698 sayılı Kişisel Verilerin Korunması Kanunu kabul edilmiştir. Söz konusu kanunun kabulü, temelde, anayasal bir hak olan kişisel verilerin korunmasını talep etme hakkına dayanmaktadır.

6698 sayılı Kişisel Verilerin Korunması Kanunu ile bireyin temel hak ve özgürlüklerinin korunması, verileri işleyenlerin uyacakları usul ve esasların belirlenmesi hedeflenmiştir. Ayrıca, kişisel verilerin korunmasını talep etme hakkının ileri sürülmesine ilişkin yollara da yer verilmiştir. Kişisel verilerin korunmasını talep etme hakkının temelde bir kişilik hakkı olduğu göz önüne alınarak, anayasa hukukunu, medenî hukuku, ceza hukukunu ve idare hukukunu ilgilendiren çok yönlü bir hak olduğu söylenebilir.

Kişisel Verilerin Korunması'nı konu alan ve üç bölümden oluşan bu çalışmamızda, Kişisel Verilerin Korunması Kanunu çerçevesinde, kişisel verilerin korunmasının nasıl sağlanacağı incelenmeye çalışılmıştır. Bu kapsamda, çalışmanın birinci bölümünde, kişisel veri kavramı unsurları ve türleri ile birlikte incelenmiş ve ilgili diğer kavramlar açıklanmıştır. Daha sonra, kişisel verilerin korunmasının tarihî gelişimi ile ulusal ve uluslararası kaynakları belirlenmiştir. Söz konusu kaynaklardan Kişisel Verilerin Korunması Kanununun temel aldığı kaynaklar ile günümüzde en etkili korumayı sağlayan kaynaklar ayrıntılı olarak incelenmeye çalışılmıştır. Kişisel verilerin korunmasını talep etme hakkının hukukî niteliğine ilişkin belirlemeler ile birinci bölüm sona erdirilmiştir.

İkinci bölümde ise, kapsam itibariyle geniş bir alanı ihtiva eden kişisel verilerin işlenmesi incelenmiştir. Bu bölümde, kişisel verilerin işlenmesinde esas alınması gereken genel ilkeler açıklanmış ve kişisel verilerin işlenmesinin, kural olarak, hukuka aykırı olduğu belirlenmiştir. Daha sonra, söz konusu hukuka aykırılığı kaldıran hâllerin, kanundaki ifadesiyle, kişisel verilerin işlenmesine ilişkin şartların incelenmesine geçilmiştir. Ayrıca, kişisel verilerin işlenmesinde veri sorumlusunun uymak durumunda olduğu yükümlülükler ve ilgili kişinin hakları açıklanmıştır.

Üçüncü ve son bölümde ise, kişisel verilerin hukuka aykırı olarak işlenmesi sebebiyle, ilgili kişinin başvurabileceği koruma yolları açıklanmıştır. Kişisel Verilerin Korunması Kanununda öngörülen veri sorumlusuna başvuru ve Kişisel

Verileri Koruma Kurulu'na şikâyet yolları incelendikten sonra, kişisel verilerin medenî hukuk kuralları çerçevesinde korunmasına ilişkin yollar belirlenmiştir. Bu yollar belirlenirken, özellikle, kişisel verilerin işlenmesinin niteliği göz önünde bulundurularak kişilik hakkının korunması amacıyla öngörülen davalar irdelenmiştir. Daha sonra, iş ilişkisindeki bağımlılık unsuru dikkate alınarak, işçinin kişisel verilerinin işlenmesinde başvurulan yöntemler ve işçinin kişisel verilerinin korunması açıklanmaya çalışılmıştır. Son olarak, Kişisel Verilerin Korunması Kanununun yaptığı atıf çerçevesinde, ceza hukuku hükümleri uyarınca öngörülen suçlara yer verilmiştir.

BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL AÇIKLAMALAR

§ 1. KİŞİSEL VERİLERE İLİŞKİN KAVRAMLAR

I. GENEL OLARAK KİŞİSEL VERİ KAVRAMI VE TANIMI

Kişisel veri *(personal data)* ifadesinden kişiye ilişkin veriler anlaşılmakla birlikte, veri kavramının açıklanması gerekir. Kaynağını aldığı Latince'de *"datum, dati"* olarak kullanılan bu kavram, İngilizce'ye *"debit"*, *"that which is a given"* şeklinde çevrilmiştir[1]. Daha sonra, İngilizce'de de *"datum"* ve *"data"* olarak kullanılmaya başlanmıştır[2]. Kelime anlamı olarak datum, *"bilginin bir parçası"*; data ise, *"referans veya analiz için bir araya toplanmış olgular ve istatistikler"* şeklinde ifade edilebilir[3].

Kavramsal açıklamalardan sonra, ulusal ve uluslararası düzenlemelerde yer alan kişisel veri tanımına değinmek gerekir. Zira, düzenlemeler kavramı oluşturan her bir kelimeye ilişkin açıklamaların kapsamını aşacak nitelikte tanımlara yer vermiştir. 1981 yılında Avrupa Konseyi tarafından imzaya sunulan 108 sayılı Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesine göre[4], kişisel veri, *"kimliği belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgileri ifade eder"*. 2016 yılında ülkemizde kabul edilen 6698 sayılı

---

1 http://www.latin-dictionary.net/search/latin/datum (Erişim Tarihi: 17.7.2018). Debit kelimesi *"deftere kaydedilen borç, zimmetine geçirmek, borçlandırmak"*; present/ gift kelimesi, *"armağan, hediye"*; veri kelimesiyle yakın anlama sahip olan that which is a given ise, *"verilen*" olarak çevrilebilir. https://tureng.com/tr/turkce-ingilizce (Erişim Tarihi: 17.7.2018).

2 Data kelimesi, Latince'den alındığı ilk zamanlarda datum kelimesinin çoğulu olarak kullanılmakla birlikte, günümüzde, İngilizce'de tekil fiil alan bir topluluk ismi hâline gelmiştir. Bkz., https://en.oxforddictionaries.com/definition/data (Erişim Tarihi: 17.7.2018). Hatta, Güncel Türkçe Sözlük, veri kavramını açıklarken *"bilgi, data"* ifadelerine yer vermektedir. Günümüzde data ifadesinin veri kavramı yerine geçecek şekilde kullanıldığı söylenebilirse de, çalışmamızda, veri veya bilgi kavramları tercih edilmiştir.

3 Bkz., https://en.oxforddictionaries.com/definition/datum, https://en.oxforddictionaries.com/definition/data (Erişim Tarihi: 17.7.2018). Bir başka sözlüğe göre, datum, *"done, baz, haber"* gibi anlamlara gelirken; data, *"bilgi, veri, bir araştırmanın temeli olan öge"* anlamlarına gelmektedir. https://tureng.com/tr/turkce-ingilizce/datum, https://tureng.com/tr/turkce-ingilizce/data (Erişim Tarihi: 17.7.2018).

4 RG. 17.3.2016, S. 29656. Sözleşmenin onaylanmasının uygun bulunmasına dair kanun için bkz., RG. 18.2.2016, S. 29628.

Kişisel Verilerin Korunması Kanunu[5] da benzer ifadelerle, *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"*yi kişisel veri olarak nitelendirmiştir. Bununla birlikte, kişisel verilerin unsurlarını ve kapsamını farklılaştıran tanımlara da rastlamak mümkündür. Mesela, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelikte[6] *"belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler"* kişisel veri olarak değerlendirilmiştir. Dolayısıyla, tüzel kişiler de bu yönetmelik uyarınca kişisel verilerinin korunmasını talep edebileceklerdir. Bazı düzenlemelerde ise, kişisel veri olarak değerlendirilen bir takım veriler sayılarak tanımlama yoluna gidilmiştir. Örneğin, 2016 yılında Avrupa Birliği tarafından kabul edilen Genel Veri Koruma Tüzüğüne göre[7] *"özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak belirli veya belirlenebilir gerçek kişiye ilişkin herhangi bir bilgi"* kişisel veri olarak değerlendirilmiştir. Yine, 1995 yılında Avrupa Birliği bünyesinde kabul edilen 1995/46 sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunması Hakkında Avrupa Parlamentosu ve Konseyi Yönergesi[8] de benzer bir tanıma yer vermiştir. Bu düzenlemeler, kişiyi belirli veya belirlenebilir kılacak bazı verileri örnek kabilinden saymak suretiyle tanım yapmıştır. Her türlü bilgi veya herhangi bir bilgi *(any information)* ifadelerinden de anlaşılacağı üzere kişisel veriler bu tanımlarda yer alan verilerle sınırlı değildir[9]. Dolayısıyla, kişiyi belirli veya belirlenebilir kılan bilgiler tanımda yer almasa dâhi kişisel veri olarak nitelendirilir. Bu kabul, teknolojik gelişmeler ışığında kişiyi belirli veya belirlenebilir kılan yeni verilerin de kişisel veri olarak nitelendirilmesini kolaylaştıracaktır[10].

---

5 RG. 7.4.2016, S. 29677.
6 RG. 24.7.2012, S. 28363.
7 OJ. 4.5.2016, L. 119, V. 59, p. 1-88.
8 OJ. 25.11.1995, L. 281, V. 38, p. 31-50.
9 Hayrunnisa **Özdemir,** Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara 2009, s. 124.
10 Hüseyin Can **Aksoy**, Medeni Hukuk ve Özellikle Kişilik Haklarının Korunması Yönünden Kişisel Verilerin Korunması, Ankara 2010, s. 12.

Söz konusu düzenlemeler ışığında kişisel veriyi açıklarken *kimliği belirli veya belirlenebilir nitelikteki gerçek kişiye ilişkin herhangi bir bilgi* tanımı esas alınabilir[11]. Bu tanımdan yola çıkarak, kişisel verinin, *"bilgi", "kimliği belirli veya belirlenebilir kişi"* ve *"bilginin kişiye ilişkin olması"* unsurlarından oluştuğu söylenebilir[12]. Kişisel veri kavramını anlaşılır kılmak amacıyla bu unsurlara değinmek gerekir.

II. KİŞİSEL VERİNİN UNSURLARI

A. Bilgi

Kişisel verinin ilk unsuru olan bilgi, bilişim alanında *"kurallardan yararlanarak kişinin veriye yönelttiği anlam"* olarak ifade edilmiştir[13]. Veri ise, bilişim hukukunda *"olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi"* şeklinde tanımlanmıştır[14]. Diğer bir söyleyişle, veri, kişilerin iletişimde, yorumda veya işlemde kullanmak amacıyla anlamlandırabilecekleri olgu, kavram ve komutlardan ibarettir. Yer verilen tanımlardan anlaşılacağı üzere, üst bir kavram olan bilgi, kişilerin veriye yükledikleri anlam olarak açıklanabilir[15]. Dolayısıyla, bilgi ve veri kavramlarının farklı anlamlara geldiği noktasında şüphe yoktur. Kişisel verilerin korunması açısından iki kavram

---

11 **Aksoy,** Veri, s. 12. Süheyla **Zorlu,** İnternet Yoluyla Kişilik Hakkının İhlâli ve Korunması, (Yayınlanmamış Yüksek Lisans Tezi), Konya 2010, s. 70.

12 1995/46 sayılı Yönergenin 29 uncu maddesi uyarınca kurulan Çalışma Grubu, kişisel verinin bu üç unsuruna ek olarak gerçek kişi unsuruna yer vermektedir. Bkz., **Article 29 Data Protection Working Party**, Opinion 4/2007 on The Concept of Personal Data, WP 136, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (Erişim Tarihi: 20.7.2018), s. 6, 21. Bazı yazarlar ise, bilgi ve kimliği belirli veya belirlenebilir kişi unsurlarını yeterli bulmuşlardır. Bkz., A. Çiğdem **Ayözger Öngün,** Kişisel Verilerin Korunması Hukuku, Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil, 2. Baskı, İstanbul 2019, s. 7 vd..

13 http://www.tdk.gov.tr/index.php?option=com_gts&kelime=B%C4%B0LG%C4%B0 (Erişim Tarihi: 18.7.2018).

14 http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c7002d658c422.12950514 (Erişim Tarihi: 18.7.2018).

15 Veri, enformasyon ve bilgi ile ilgili ayrıntılı bilgi için bkz., Elif **Küzeci**, Kişisel Verilerin Korunması, 2. Baskı, Ankara 2018, s. 9-13.

arasında herhangi bir fark gözetilmediği için, bu çalışmada her ikisi de birbirinin yerine geçecek şekilde aynı anlamda kullanılmıştır[16].

Kişisel veri tanımına yer veren düzenlemeler, herhangi bir ayrıma gitmeksizin bütün bilgileri kişisel veri kapsamına almıştır. Bu açıdan, kişinin maddî, manevî veya iktisadî bütünlüğüne ilişkin bilgileri kişisel veri kapsamında değerlendirilebilir[17]. Bu kapsamda, kişinin sağlığı, adı, resmi, meslekî veya iktisadî sır çevresine ilişkin bilgileri kişisel veriye örnek olarak gösterilebilir. Yine, 1995/46 sayılı Yönergenin 29 uncu maddesi uyarınca kurulan Çalışma Grubu *(Working Party)*[18], kişiye ilişkin objektif veya sübjektif değerlendirmelerin, görüşlerin ya da bilgilerin kişisel veri olarak nitelendirilebileceğini ifade etmiştir[19]. Örneğin, kişiye yapılan kan testi sonucunda elde edilen objektif veriler kadar, kişinin güvenilir veya güvenilmez olduğuna dair sübjektif bilgiler de kişisel veri niteliği taşır. Kredi başvuru işlemlerinde kişinin borçlarını zamanında ödeyip ödemediğine dair sübjektif bilgi, bankanın başvuracağı önemli kişisel verilerdendir.

Sözü edilen bilgilerin doğru veya kanıtlanmış olmasına gerek yoktur. Çalışma Grubuna göre, veri koruma kurallarıyla bilginin yanlış olma ihtimali göz önüne alınmıştır. Diğer bir deyişle, kişisel veriler açısından amaçlanan koruma, yanlış olan bilginin düzeltilmesini de kapsamaktadır. Dolayısıyla, bilginin yanlış veya kanıtlanmamış olması onu kişisel veri olmaktan çıkarmaz[20]. Kişisel veri alanındaki düzenlemelerin, ilgili kişiye düzeltme hakkı (KVKK.m.11/I-d) tanımış olması, bu

---

16 Nitekim, Güncel Türkçe Sözlük'te yer verilen diğer açıklamalara göre, bilgi ve veri eş anlamlı olarak kullanılmaktadır. Bkz., http://sozluk.gov.tr/ (Erişim Tarihi: 12.3.2019).

17 **Özdemir,** s. 125. Ayrıca bkz., Mehmet **Ayan** / Nurşen **Ayan**, Kişiler Hukuku, 8. Baskı, Ankara 2016, s. 91-101; **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 6.

18 1995/46 sayılı Yönergenin 29 uncu maddesi çerçevesinde kişisel verilerin işlenmesine dair bireylerin korunması amacıyla kurulan danışma statüsüne sahip, bağımsız bir grubu ifade eder.

19 **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 6. Aynı yönde bkz., **Aksoy**, Veri, s. 14; **Özdemir,** s. 125; Songül **Atak,** Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri, Bahçeşehir Üniversitesi Hukuk Fakültesi Kazancı Hakemli Hukuk Dergisi, S. 59-60, 2009, s. 207.

20 **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 6; **Aksoy**, Veri, s. 14-15. Güncel Türkçe Sözlük'te bilgiye ilişkin verilen diğer açıklamalarda, bilginin gerçek olması gerektiği ifade edilse de, bu durum, kişisel verilerin sınırlandırılmasına yol açar. Ancak, bu sınırlama Kanunun koruma amacı ile bağdaşmaz. Kanunkoyucunun herhangi bir ayrıma gitmeksizin her türlü bilgiyi kapsama alması da kişisel verilerin kapsamını sınırlandırmak istemediği gösterir. Bkz., Hale **Akdağ**, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2013, s. 11.

görüşü destekler niteliktedir[21]. Örneğin, bir kimsenin, gerçeği yansıtmasa dâhi, rüşvet aldığını konu alan haberler de kişisel veri olarak değerlendirilir. Aynı şekilde, bir verinin açığa çıkarılmış veya gizli olması da kişisel verilerin korunması açısından önem arz etmez[22]. Bu durumda, örneğin, HIV virüsü taşıyan kişinin bu bilgiyi gizlemesi veya diğer kişilerle paylaşması yahut üçüncü bir kişinin bu bilgiyi diğer kişilere açıklaması arasında kişisel veri olma niteliği açısından fark yoktur.

Kişisel verilerin kapsamını belirlerken o verinin şekli, tutulduğu yer veya işlenme biçimine de değinmek gerekir. Alfabetik, sayısal, grafiksel, fotografik veya akustik olarak hangi biçimde olursa olsun mevcut veriler kişisel veri kapsamında değerlendirilecektir[23]. Bu verilerin, kâğıt üzerinde veya bilgisayar ortamında tutulması arasında bir fark yoktur. Örneğin, kişinin günlüğüne yazdığı bilgiler, kişiye ait güvenlik kamerası görüntüleri, müşteri hizmetleri kapsamında tutulan ses kayıtları veya kişinin kredi kartından yaptığı harcamalara ilişkin grafik kişisel verilerdendir. Yine, kişinin parmak izi, yüz veya el yapısı, konuşma şekli, yürüyüş tarzı, ıslak imzası gibi biyometrik veriler de kişisel veri kapsamındadır[24].

Ayrıca, verinin otomatik olan veya olmayan yollarla işlenmesi de kişisel veri olma niteliğini değiştirmez. Ancak, burada, Kişisel Verilerin Korunması Kanunu tarafından getirilen bir sınır söz konusudur. Gerçekten, Kişisel Verilerin Korunması Kanununun 2 nci maddesi ise, *"...tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan*

---

21 **Akdağ**, s. 12; **Aksoy,** Veri, s. 15, dn. 11; Doğan **Kılınç,** Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 61, S. 3, 2012, s. 1159.

22 Çalışma Grubu, Avrupa İnsan Hakları Mahkemesinin Amann / İsviçre kararına atıf yaparak, özel hayat kavramının diğer insanlarla ilişki kurma ve geliştirme durumlarını da içine alacak şekilde geniş yorumlanması gerektiğini belirtmiştir. Çalışma Grubu'nun görüşü için bkz., **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 7. Amann / İsviçre kararı için bkz., https://hudoc.echr.coe.int/ (Erişim Tarihi: 20.8.2018).

23 **Aksoy,** s. 16.

24 Murat **Doğan**, İnternette Şahsiyet Haklarının İhlali, Bilgi Toplumunda Hukuk, Ünal Tekinalp'e Armağan, C. II, 2003, s. 481; Aydın **Akgül**, Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı, Türkiye Barolar Birliği Dergisi, S. 118, Mayıs-Haziran 2015, s. 202. Biyometrik veriler, bireye ilişkin kesin sonuçlar sağlaması sebebiyle kişisel veriler açısından büyük öneme sahiptir. Bununla birlikte, bireye ait doku örnekleri tek başına kişisel veri değildir. Başka bir ifadeyle, kişiden alınan kan örneği sonucunda elde edilen bilgiler kişisel veri kapsamında korunurken, kişiye ait kanın, doku örneği alınması ve toplanması kurallarına göre korunması gerekir. Bkz., **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 7-9.

yollarla…" veriler üzerinde gerçekleştirilen her türlü eylemi kişisel veri kategorisinde değerlendirmiştir[25].

B. Belirli veya Belirlenebilir Kişi

Kişisel verinin ikinci unsuru, kişinin belirli veya belirlenebilir kılınmasıdır. Bu kapsamda, öncelikle, kişi kavramından ne anlaşılması gerektiği belirlenmelidir. Bu belirleme, kişisel verilerin işlenmesi sebebiyle öngörülen korumadan kimlerin faydalanabileceğini de tespit edeceği için önemlidir. Bu konuda, öğreti ve mevzuatta görüş birliği bulunmamaktadır. Gerçekten, Kişisel Verilerin Korunması Kanunu *"gerçek kişiye ilişkin her türlü bilgi"*yi kişisel veri kabul ettiği için sadece gerçek kişileri koruma kapsamına almıştır. Buna göre, veri sahibi, veri öznesi gibi tamlamalar ile ifade edilen ilgili kişi[26], kişisel verisi işlenen gerçek kişiyi ifade eder (KVKK.m.3/I-ç). 108 sayılı Sözleşme, 1995/46 sayılı Yönerge ve Genel Veri Koruma Tüzüğü de gerçek kişilere ait kişisel verileri korumaktadır. 2002 yılında Avrupa Birliği bünyesinde kabul edilen 2002/58 sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönerge[27] ise, tüzel kişilerin de çıkarlarının korunmasını amaçladığını belirtmiştir.

Öğretide ise, tüzel kişilerin kişisel verilerinin korunması noktasında farklı görüşler bulunmaktadır. Bu görüşlere yer vermeden önce, tüzel kişilerin sahip olabilecekleri haklar ve bunların korunması hususu değerlendirilmelidir. Türk Medenî Kanununun 48 inci maddesine göre, tüzel kişiler yaradılış gereği insana özgü niteliklere bağlı olanlar haricindeki haklara sahip olabilirler. Bu durumda, tüzel kişiler, sağlık, cinsiyet, doğum gibi değerlere sahip olamadıkları için, sağlık ve cinsiyet bilgisi veya doğum tarihi gibi bir bilgiye de sahip olamazlar. Öte yandan, tüzel kişilerin, isim, vatandaşlık, meslek, şeref ve haysiyet gibi değerlere sahip

---

25 Genel Veri Koruma Tüzüğünün 2 nci maddesinin birinci fıkrasında da benzer bir durum söz konusudur. Bununla birlikte, bazı düzenlemeler otomatik olmayan yollarla işlenen verileri kapsamın dışında tutmuştur. Örneğin, 108 sayılı Sözleşme ile kişisel verilerin otomatik işleme tâbi tutulması karşısında bireyi korumak amaçlanmıştır.

26 Veri sahibi ifadesi, veriye eşya olma niteliği yüklendiği; veri öznesi ise, verinin nesnelere ait bilgileri kapsamayacağı şeklinde şeklinde bir izlenim yaratması sebebiyle tercih edilmemiştir.

27 OJ. 31.7.2002, L. 201, V. 45, p. 37-47.

olacağı kabul edilir[28]. Dolayısıyla, tüzel kişiler, sahip olabilecekleri bu değerlerin ihlâli durumunda, kişilik hakkının korunmasını sağlamak için dava açabilirler[29].

Tüzel kişilerin kişisel verilerin korunması hakkı ile ilgili ileri sürülen ilk görüşe göre, kişisel verilerin korunmasının kapsamına tüzel kişiler girmemektedir[30]. Tüzel kişilerin şeffaflık ilkesine tâbi olduğu için özel hayatı olmayacağını ifade eden bu görüş, tüzel kişiler için ticari gizliliğin korunması hükümlerinin uygulanması gerektiğini savunmaktadır. Yer verilen görüşe farklı eleştiriler getirilebilir. Öncelikle, özel hayat ve kişisel veri kavramı aynı anlamlara gelmemektedir. Bir kişi, özel hayat kavramının dışında kalan kişisel verilere sahip olabilir. Ayrıca, hem ideal amaç güden tüzel kişilerin, hem de iktisadî amaç güden tüzel kişilerin ticarî gizliliğin korunması hükümlerine başvurması mümkün değildir[31]. Diğer görüşe göre[32], tüzel kişilere ilişkin verilerle gerçek kişiye ulaşmak mümkünse bu veriler koruma kapsamına alınmalıdır. Görüldüğü üzere bu görüş, esasen gerçek kişiye sağlanan koruma dâhilinde ulaşılabilecek bir sonucu ortaya koymaktadır. Zira, kişisel veri, gerçek kişiyi belirli veya belirlenebilir kılan her türlü veriyi kapsar. Dolayısıyla, burada sağlanan koruma yine gerçek kişiye aittir. Ayrıca, bu görüş, tüzel kişiliğin gerçek kişiye ulaşma imkânı sağlamayan bilgileri açısından bir çözüm sunmamaktadır. Bir diğer görüşe göre[33] ise, tüzel kişiler, sadece insana özgü olan değerler hariç olmak üzere, sahip olduğu değerler açısından kişilik hakkının korunmasını talep edebilir. İdeal amaç güden tüzel kişilere ait veriler 4721 sayılı Türk Medenî Kanununun[34] 23 - 24 üncü ve 6098 sayılı Türk Borçlar Kanununun[35] 48 inci maddesi uyarınca, iktisadi amaç güden tüzel kişilere ait veriler, kural olarak,

---

28 Ferit H. **Saymen,** Türk Medenî Hukuku, C. 2, Şahsın Hukuku, 2. Baskı, İstanbul 1960, s. 309-311; **Ayan/ Ayan,** s. 206.

29 **Saymen,** s. 312; **Ayan/ Ayan,** s. 208;

30 Durmuş **Tezcan**, Bilgisayar Karşısında Özel Hayatın Korunması, Anayasa Yargısı Dergisi, C. 8, 1991, s. 389.

31 Furkan Güven **Taştan**, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 2. Baskı, İstanbul 2017, s. 33.

32 **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 23; Nilgün **Başalp**, Kişisel Verilerin Korunması ve Saklanması, Ankara 2004, s. 35; Oğuz **Şimşek**, Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008, s. 90-91.

33 **Ayan / Ayan**, Kişiler, s. 208. Benzer bir görüş için bkz., **Taştan**, s. 33.

34 RG. 8.12.2001, S. 24607.

35 RG. 4.2.2011, S. 27836.

6102 sayılı Türk Ticaret Kanununun[36] haksız rekabeti düzenleyen hükümleri uyarınca korunmalıdır. Sonuç olarak, Kişisel Verilerin Korunması Kanununun ve Genel Veri Koruma Tüzüğünün açık ifadesi gereği, tüzel kişiler, kişi bakımından kapsama dâhil edilmemiştir[37]. Nitekim, Kişisel Verileri Koruma Kanununun 2008 yılında sunulan tasarı metninde tüzel kişiler kapsama alınmasına rağmen kanunlaşan metinde tüzel kişilere yer verilmemiş olması, kanunkoyucunun bu yöndeki iradesini gösterir[38].

Kişi kavramına ilişkin açıklamalarda, son olarak, ölülere ve cenine ilişkin verilere değinmek gerekir. Çalışma Grubu, ölülere ve cenine ilişkin verilerin korunmasının her ülkenin ulusal mevzuatı çerçevesinde mümkün olabileceğini ifade etmiştir[39]. Bu sebeple, Türk hukukunda, ceninin ve ölülerin durumunun değerlendirilmesi gerekir. Medenî Kanunun 28 inci maddesine göre, cenin, sağ ve tam doğma koşuluyla ana rahmine düştüğü andan itibaren hak ehliyetini elde eder. Diğer bir deyişle, kişiliğin kazanılması, ceninin doğal veya yapay yollarla ana rahmine düştüğü ana kadar geriye yürür[40]. Söz konusu düzenleme ile cenin, üçüncü kişilerin haksız fiil teşkil eden müdahaleleri neticesinde, *sağ ve tam doğup kişilik kazandıktan sonra kanunî temsilcisi* aracılığıyla tazminat talep edebilir. Cenine ilişkin kişisel verilerin korunması hususunda da bu esas benimsenebilir. Bununla birlikte, sadece cenine ilişkin verilerin, sağ ve tam doğum gerçekleşmeden anne aracılığıyla korunması mümkün gözükmemektedir. Hem anneye hem de cenine ilişkin verilerin annenin kişilik hakkı temelinde korunması ise mümkündür. Ölülere ilişkin kişisel veriler ise, kişilik sona erdiği için, kural olarak, koruma kapsamında değildir. Ancak, ölüye ilişkin bilgiler yakınlarını belirli veya belirlenebilir kılacak

---

36 RG. 14.2.2011, S. 27846.

37 *Ayözger Öngün'e* göre, kanun kapsamında veri koruma kurallarından yararlanabileceklerin gerçek kişilerle sınırlı tutulması doğru bir yaklaşımdır. Tüzel kişilere ait verilerin koruması, elektronik haberleşme sektöründe olduğu gibi özel mevzuat hükümleri ile sağlanmalıdır. bkz., **Ayözger Öngün,** s. 10. Aksi görüş için bkz., Ersan **Şen,** Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, İstanbul Barosu Dergisi, C. 83, S. 3, 2009, s. 1201.

38 **Aksoy,** Veri, s. 20.

39 **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 23.

40 **Ayan / Ayan**, Kişiler, s. 44; Rona **Serozan,** Medenî Hukuk, Genel Bölüm / Kişiler Hukuku, 8. Baskı, İstanbul 2018, s. 422; Mustafa **Dural /** Tufan **Öğüz,** Türk Özel Hukuku, C. 2, 15. Baskı, İstanbul 2004, s. 28; Jale **Akipek /** Turgut **Akıntürk /** Derya **Ateş,** Türk Medenî Hukuku, Başlangıç Hükümleri, Kişiler Hukuku, C. 1, 14. Baskı, İstanbul 2018, s. 244.

nitelikteyse korunması söz konusu olacaktır[41]. Örneğin, ölüye ilişkin genetik veriler, sağ olan altsoyunu veya üstsoyunu da belirli kılabilecek nitelikte olduğu için korunmalıdır.

Belirli veya belirlenebilir olmak[42] ise, bireyle ilişkilendirilen mevcut verilerin o kişiyi tanımlaması veya tanımlanabilir kılmasını ifade eder. Kişi, kimlik veya pasaport numarası, parmak izi gibi verilerle doğrudan belirli kılınabileceği gibi, doğum tarihi, anne babasına ait isimler, adres gibi verilerle dolaylı olarak belirlenebilir. Ancak, kişisel verileri korunması açısından bu ayrımın bir önemi yoktur. Herhangi bir verinin kişiyi belirli veya belirlenebilir kılması her somut olay açısından ayrıca değerlendirilmelidir[43]. Örneğin, kişiye ait takma ad, kullanıldığı yörede onu belirli kılarken, aynı takma ad nüfus müdürlüklerinde kişiyi belirlemeye yetmeyebilir. Bu noktada, tanımlama işleminin kim tarafından ve ne kadar çaba gösterilerek gerçekleştirileceği belirlenmelidir. Buna göre, 1995/46 sayılı Yönergenin başlangıç hükümlerinin 26 ncı maddesinde bahsedildiği üzere, *"kimliği tespit etmeye çalışan herhangi bir kişi tarafından kullanılması muhtemel makul tüm vasıtalar"* dikkate alınmalıdır. O hâlde, dönemin teknolojik imkânları ve kullanılabilecek makul tüm vasıtalar dikkate alınarak mevcut veriden gerçek kişi tespit edilebiliyorsa, belirli veya belirlenebilir olma unsuru sağlanmıştır[44]. Yine, 1995/46 sayılı Yönergenin başlangıç hükümlerinin 26 ncı maddesine göre, anonim veri olarak adlandırılan kişi ile ilişkisi sağlanamayan verilerin kişisel veri olarak nitelendirilmesi mümkün değildir[45].

---

41 **Özdemir,** s. 125-126.

42 Belirlenebilir olma unsurunun nasıl sağlanacağı konusunda ileri sürülen mutlak belirlenebilirlik ve nisbi belirlenebilirlik görüşleri için bkz., M. Serdar **Çekin**, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu, İstanbul 2018, s. 35 vd..

43 **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 12.

44 **Aksoy**, Veri, s. 24.

45 Çalışma grubu, bu noktada takma ad kullanılan verilere, şifrelenmiş verilere ve anonim verilere ilişkin bir karşılaştırmada bulunmuştur. Buna göre, takma ad kullanılan ve şifrelenmiş verilerde, takma adın veya şifrenin bilinmesi veri ile kişi arasındaki ilişkiyi sağlayacaktır. Diğer bir söyleyişle, kişiyi belirli veya belirlenebilir kılmak mümkündür. Bu sebeple, takma ad kullanılan veriler ve şifreli veriler kişisel veri olarak nitelendirilir. Bkz., **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 32.

C. Bilginin Kişiye İlişkin Olması

Kişisel verinin son unsuru bilginin kişiye ilişkin olmasıdır. Öncelikle, bilginin özne ile ilgili olması ve nesne ile ilgili olması arasındaki fark incelenmelidir. Daha önce verilen örneklerden anlaşılacağı üzere, bilgi genellikle özne ile ilgilidir. Örneğin, kişinin sağlık bilgisi, cinsiyet bilgisi, ceza mahkumiyeti bilgisi özne ile ilgilidir. Öte yandan, nesne ile ilgili bilgiler de kişiyi belirli veya belirlenebilir kılıyorsa kişisel veri olarak kabul edilmektedir[46]. Zira, kişiye ilişkin olma unsuru, doğrudan kişi hakkındaki bilgilerle sağlanabileceği gibi bazı durumlarda kişinin sahip olduğu nesne hakkındaki bilgilerle de sağlanabilir. Örneğin, kişiye ait evin değeri sebebiyle yükümlü olduğu vergi, kişisel veri teşkil edebilir. Aynı şekilde, bir aracın plakası, kilometre bilgisi de aracın sahibi olan gerçek kişiyi belirli kılabilir. Bu kapsamda hangi bilgilerin kişiye ilişkin olduğunu her somut olay çerçevesinde değerlendirmek gerekir.

Çalışma grubu *"içerik", "amaç"* veya *"sonuç"* açısından kişi ile bilgi arasında bağlantı bulunabileceğini ifade etmiştir[47]. İçerik unsuru, bilginin içeriğinin kişi hakkında olmasını ifade eder. Örneğin, yakın gelecekte nüfus cüzdanlarına yerleştirilmesi planlanan ve radyo frekansları ile tanımlama yapabilen mikroçiplerle *(RFID-Radio Frequency Identification)* kişiye ilişkin birçok içeriğe (varlık bilgisi, konum bilgisi gibi) ulaşılabilir. Amaç unsuru, kişinin durumunu veya davranışını değerlendirmek, belirli bir şekilde değiştirmek veya etkilemek amacıyla toplanan her türlü bilginin kişiye ilişkin olmasını ifade eder[48]. Fabrikada bulunan bir makinenin üretim faaliyetini belirlemek için toplanan veri, çalışanların verimliliğini belirlemek amacıyla kullanılıyorsa, o veri işçi açısından kişisel veri nitelliğine sahiptir. Son olarak, kişiye ilişkin verilerin kullanılması durumunda, ona karşı diğer insanlardan farklı davranılması söz konusu olacaksa sonuç unsuru oluşmuştur[49]. Müşteri konumuna yakın araç tahsisi ve yakıt tasarrufu amacıyla ticarî taksilere yerleştirilen

---

46 **Akdağ,** s. 13.
47 **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 9.
48 **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 9, 10.
49 **Article 29 Data Protection Working Party**, Opinion 4/2007, s. 11.

cihazlardan elde edilen veriler, sürücülerin performans değerlendirmesini de mümkün kıldığı için kişiye ilişkin olma unsurunu sağlarlar.

III. KİŞİSEL VERİLERİN TÜRLERİ

Kişisel veri, ihtiyaç duyduğu korumadan yola çıkarak ikili bir ayrıma tâbi tutulmuştur. Bu ayrım düzenlemelerde açıkça görülmemekle birlikte, bazı kategorideki verilerin korunması amacıyla özel işlenme şartları belirlenmiştir. Gerçekten, 108 sayılı Sözleşmede ve 1995/46 sayılı Yönergede *özel tür veri*, *özel veri kategorileri* gibi kavramlara yer verilmiştir. Karşıt anlamından ise *genel tür veri, genel veri kategorileri* gibi kavramlar ortaya çıkmıştır. Türk Hukukunda, *özel nitelikli kişisel veri - genel nitelikli kişisel veri* veya *hassas veri - hassas olmayan veri*[50] şeklinde ayrımlara rastlamak mümkündür. Bu çalışmada, Kişisel Verilerin Korunması Kanunu tarafından benimsenen, veri kavramına ilişkin ayrımın temeline uygun olan *özel nitelikli kişisel veri - genel nitelikli kişisel veri* ayrımı esas alınmıştır.

A. Özel Nitelikli Kişisel Veriler

Kişisel veri alanındaki düzenlemelerde tanımına yer verilmeyen özel nitelikli veriler, genel nitelikli verilere nazaran özel bir koruma gerektirmektedir. Bu özel korumanın sebebi, Kişisel Verilerin Korunması Kanununun 6 ncı maddesinin gerekçesinde ifade edilmiştir. Buna göre, özel nitelikli veriler başkaları tarafından öğrenildiği takdirde ayrımcılığa ve mağduriyete sebep olabilecek verilerdir. Bu sebeple söz konusu veriler ile ilgili işlemler özel kurallara tâbi kılınmıştır. Söz konusu kurallara kişisel verilerin işlenilmesi başlığında değinileceği için, bu kısımda özel nitelikli kişisel verileri tespitle yetinilecektir.

Öncelikle, ne tür verilerin özel nitelikli olduğunun belirlenmesi gerekir. Türk Hukukunda özel nitelikli kişisel veri kategorilerine, uluslararası düzenlemelerle genel itibariyle örtüşür şekilde, sınırlı sayıda yer verilmiştir[51]. Gerçekten, Kişisel Verilerin

---

[50] Verilerin bu şekilde nitelendirilmesinin sebebi, 1995/46 sayılı Yönerge'de *sensitive categories of data, sensitive data* şeklinde ifade edilmesidir.

[51] **Ayözger Öngün,** s. 23. Özel nitelikli verilerin sınırlı sayıda olmaması gerektiğine dair görüşler için bkz., **Aksoy**, Veri, s. 33-34; Nafiye **Yücedağ,** Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 75, S. 2, 2017, s. 768.

Korunması Kanununun 6 ncı maddesinin birinci fıkrasına göre, *"kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri"* özel nitelikli kişisel veridir[52]. Örneğin, kişilerin dergi veya gazete aboneliklerine ilişkin bilgilerden siyasî görüşleri hakkında bilgi edinilebiliyorsa, abonelik bilgisi özel nitelikli kişisel veri olarak değerlendirilmelidir. Yine, bir kişiyi öldürdüğü ve bu sebeple ceza aldığı bilinen kişinin toplumdan dışlanması, iş bulamaması sıklıkla karşılaşılan bir durumdur. Benzer şekilde, bir topluluktan farklı dinî inanış, mezhep veya diğer inançları benimseyenlerin bilinmesi, bu kişiler için o toplulukta yaşamayı zorlaştırır.

Hükümden de anlaşılacağı üzere, bu kategorilerden birinde yer almayan bilginin özel nitelikli veri sayılması mümkün değildir. Kişisel Verilerin Korunması Kanunu, 1995/46 sayılı Yönerge ve 108 sayılı Sözleşmeden farklı olarak, ilgili kişinin kılık kıyafeti, biyometrik ve genetik verilerini de özel nitelikli verilerin kapsamına almıştır. Bu noktada, teknolojik ve bilimsel gelişmelerle birlikte günümüzde önemli bir yere sahip olan biyometrik ve genetik verilere değinmek gerekir. Genel Veri Koruma Tüzüğünün 4 üncü maddesine göre, genetik veri, *"bir*

---

[52] *Küzeci'ye* göre, bir verinin, bu kategorilerde yer alması, özel nitelikli kişisel veri olarak değerlendirilmesi için yeterli değildir. Yazara göre, o verinin bu niteliği dikkate alınarak kullanılması gerekir. Dolayısıyla, özel nitelikli kişisel veri, her somut olay açısından ayrıca değerlendirilmeye muhtaçtır. Örneğin, bir kişinin gözlük kullandığına dair bilgi, göz sağlığının yerinde olmadığının göstergesidir. Ancak, bu verinin özel nitelikli kişisel veri olarak nitelendirilmesi, bu yönde bir değerlendirmeye bağlıdır. Bkz., **Küzeci,** Kişisel Veri, s. 251-252. Aynı yönde bkz., **Yücedağ,** s. 769. Avrupa Birliği Adalet Divanı ise, özel nitelikli kişisel verileri geniş yorumlama eğilimindedir. Örneğin, *Lindquvist* kararında, kişinin ayağının kırık olduğuna dair bilgi sağlık verisi olduğu için, özel nitelikli kişisel veri olarak kabul etmiştir. İlgili karar için bkz., AAD., C-101/01 (Criminal Proceedings Against Bodil Lindqvist), 13.5.2014, bkz., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1557095979675&uri=CELEX:62001CJ0101 (Erişim Tarihi: 20.9.2018), kn. 52-71. Kişisel Verilerin Korunması Kanununun 6 ncı maddesinin birinci fıkrasından anlaşılacağı üzere, özel nitelikli kişisel veriler açısından bir değerlendirmede bulunulması için, verilerin sayılan kategorilere ait olması dışında herhangi bir sınırlama getirilmemiştir. Dolayısıyla, kategorilere ilişkin tüm veriler, özel nitelikli kişisel veri olarak kabul edilmelidir. Hatırlanacağı üzere, kişisel verilerin hukuka aykırı olarak işlenme tehlikesi, kişisel verilerin korunmasındaki temel amaçlardandır. Dolayısıyla, herhangi bir hukuka aykırı amaç güdülmese de ilgili kurallara uyulması aranmalıdır. Örneğin, bir sağlık kuruluşu, kişinin psikolojik durumuna ilişkin veriyi işlerken kullanım amacına bakmaksızın özel nitelikli kişisel verilerin tâbi olduğu işleme şartlarına uygun davranmalıdır. Ayrıca bkz., Cemil **Kaya,** Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 69, S. 1-2, 2011, s. 322-323.

gerçek kişinin fizyolojisi veya sağlığı ile ilgili eşsiz bilgiler sağlayan ve özellikle söz konusu gerçek kişiden alınan bir biyolojik numunenin analiziyle o kişinin kalıtım yoluyla aldığı veya edindiği genetik özellikleri ile ilgili verilerdir". Bu verilerle kişide oluşan ve oluşabilecek hastalıklar teşhis edilebilir, soybağı kesin olarak belirlenebilir. Söz konusu veriler, ilgili kişinin ve onun dâhil olduğu grubun kalıtımsal özelliklerini ortaya koyduğu için, belirli bir grup açısından kişisel veri teşkil eder[53]. Ancak, bu veriler her zaman kişi yararına kullanılmazlar. Kişi, genetik özellikleri sebebiyle sosyal hayattan dışlanma, iş hayatına atılamama gibi olumsuz sonuçlarla karşılaşabilir. Bu sebeple, kişinin gen özelliklerini barındıran veriler özel nitelikli kişisel veriler kategorisinde sayılmıştır.

Biyometrik veri ise, *"yüz görüntüleri veya daktiloskopik veri gibi gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden, o kişinin fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel verilerdir"*. Diğer bir söyleyişle, biyometrik veri, fiziksel, psikolojik veya davranışsal özellikler aracılığıyla kişiyi eşsiz bir şekilde tanımlayan veya tanımlanmış kişiyi doğrulayan verilerdir[54]. Örneğin, kişiye ilişkin parmak izi, el geometrisi, yüz, retina, vücut kokusu, imza, yürüyüş tarzı gibi bilgiler biyometrik verilerdendir[55]. Bununla birlikte, kişiye ilişkin her fotoğraf biyometrik veri olarak değerlendirilmez. Fotoğraf, yalnızca kişinin benzersiz bir biçimde tanımlanmasına veya doğrulanmasına izin veren belirli bir teknik yöntemle işlendiğinde biyometrik veri kapsamında değerlendirilmesi söz konusu olur[56]. Aksi hâlde, genel nitelikli veri olduğu söylenebilir. Biyometrik veri niteliğine sahip olmayan bir fotoğrafın, diğer özel nitelikli kişisel veri kategorilerinden biri (örneğin, kılık kıyafete ilişkin olması) sebebiyle özel nitelikli veri olarak kabul edileceği unutulmamalıdır.

---

53 Nüket **Örnek Büken** / Çağrı **Zeybek Ünsal,** Kişisel Verilerin Korunması Kanununun Biyomedikal Alana Yansımaları Açısından Değerlendirilmesi, Hacettepe Hukuk Fakültesi Dergisi, C. 7, S. 2, 2017, s. 42.

54 **Örnek Büken / Zeybek Ünsal**, s. 41.

55 **Akgül**, Biyometrik, s. 202.

56 Genel Veri Koruma Tüzüğünün 51 inci paragrafı.

B. Genel Nitelikli Kişisel Veriler

Kişisel Verilerin Korunması Kanununda veya diğer düzenlemelerde, özel nitelikli kişisel veriler *(sensitive data - hassas veri)* dışındaki verileri belirtmek için herhangi bir kavrama yer verilmemiştir. Bununla birlikte, Kişisel Verilerin Korunması Kanununun 5 inci maddesinde kişisel verilerin işlenme şartları belirlendikten sonra özel nitelikli verilerin işlenme şartlarının düzenlenmesi böyle bir ayrımı gerekli kılmaktadır. Ancak, ayrım sonucunda kişisel veriler, önemli veriler ve önemsiz veriler şeklinde nitelendirmemelidir. Zira, belirli veya belirlenebilir nitelikteki kişiye ilişkin tüm veriler önemlidir[57]. Bu durumda, genel nitelikli kişisel veriler, özel nitelikli kişisel veriler haricindeki tüm veriler olarak tanımlanabilir. Bu veriler ile ilgili işlemeler ve hukuka aykırı işlemede sağlanan koruma genel veri koruma kurallarına (KVKK.m.5) tâbidir. Örneğin, kişinin kimlik numarası, plaka bilgisi, alışveriş alışkanlıkları, telefon görüşmeleri, biyometrik fotoğraf dışında kişiyi belirli kılabilen fotoğrafı bu kapsamda sayılabilir.

IV. KİŞİSEL VERİYE İLİŞKİN DİĞER BAZI KAVRAMLAR

A. Veri Sorumlusu

Veri sorumlusu *(data controller)*, kişisel verilerin işlenmesinden doğan sorumlulukta önemli bir yere sahiptir. Kişisel Verilerin Korunması Kanununun 3 üncü maddesine göre, veri sorumlusu, *"kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak tanımlanmıştır[58]. Bu durumda veri sorumlusunu anlamlandırabilmek için, veri kayıt sisteminin tanımına başvurmak gerekir. Kişisel Verilerin Korunması Kanununun 3 üncü maddesinin birinci fıkrasının h bendine göre, veri kayıt sistemi, *"kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder"*. Kayıt sistemi, fiziksel veya elektronik ortamda oluşturulabilir. Veri kayıt sisteminin yapılandırılacağı kriterler

---

57 **Küzeci**, Kişisel Veri, s. 253.

58 Veri sorumlusunu tarif etmek için Genel Veri Koruma Tüzüğü'nde de benzer bir tanıma yer verilmiştir. Ancak, veri sorumlusunu yerine *denetçi, yönetici, kontrol birimi, kontrolör* anlamlarına gelen *controller* kavramı kullanılmıştır.

her bir alana göre değişiklik gösterebilir. Örneğin, bir banka, kredi kartı borcunu zamanında ödemeyen kişileri esas alarak, ödeme tarihine göre bir kayıt sistemi öngörebilir. Aynı şekilde, nüfus müdürlükleri tarafından kimlik numarasına veya cinsiyete göre, kayıt sistemi oluşturulabilir[59]. Bu durumda, veri sorumlusu, verilerin hangi amaçlarla ve araçlarla işleneceğini belirleyen, verilerin kaydedilmesi de dâhil olmak üzere sistemin nasıl işleyeceğini belirleyen gerçek veya tüzel kişidir. Bu kapsamda, kamu kurum ve kuruluşları, şirketler, dernekler veya esnaflar veri sorumlusu olarak nitelendirilebilir. Hatta, Avrupa Birliği Adalet Divanı, bir kararında internet arama motorlarını da veri sorumlusu olarak nitelendirmiştir[60]. Benzer şekilde, internet servis sağlayıcıları[61] yahut sosyal medya alanında ortaya konulan uygulama sağlayıcıları yahut yöneticileri de veri sorumlusu olarak nitelendirilmiştir[62].

Veri sorumlusunun belirlenmesi, kişisel verilerin işlenmesi sebebiyle ortaya çıkacak olan yükümlülüklerin yerine getirilip getirilmediğini tespit etmek ve getirilmemişse sorumluya uygulanacak yaptırımlar açısından önem arz eder.

B. Veri İşleyen

Kişisel Verilerin Korunması Kanununun 3 üncü maddesinin birinci fıkrasına göre, veri işleyen *(data processor)*, *"veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"*yi ifade eder. Kişisel Verilerin Korunması Kanununun 3 üncü maddesinin gerekçesinde belirtildiği üzere, bir kişi aynı kişisel veriler açısından hem veri sorumlusu hem de veri işleyen olabilir. Diğer bir söyleyişle, veri sorumlusu, veri işleme faaliyetini kendisi yerine getiriyorsa veri işleyen sıfatını da alır. Veri sorumlusunda olduğu gibi, veri işleyen gerçek veya

---

59 Kişisel Verilerin Korunması Kanununun 3 üncü maddesinin gerekçesi.

60 AAD., C-131/12 *(Google Spain SL ve diğer şirket /Agencia Espanola de Proteccion de Datos (AEPD) ve diğerleri)*, 13.5.2014, bkz., http://www.abgm.adalet.gov.tr/abadaletdivani/abadaletdivani.html (Erişim Tarihi: 22.9.2018), kn. 21-41.

61 **Article 29 Data Protection Working Party,** Privacy on the Internet, WP 37, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (Erişim Tarihi: 27.2.2019), s. 11-12.

62 Kemal **Atasoy,** Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cevdet Yavuz'a Armağan, C. 22, S. 3, 2016, s. 283.

tüzel kişi olabilir. Veri sorumlusu, veri işleme faaliyeti için çalışan istihdam edebilir veya ayrı bir kişiden hizmet satın alabilir[63]. Örneğin, bir kurum, çalıştırdığı personele ilişkin verilerin işlenmesinde başka bir personeli görevlendirebilir. Bu durumda, veri sorumlusu, verilerin işlenmesindeki amaç ve araçlarını belirleyen kurumdur. Personel ise, veri işleyendir. Yahut, bir şirket, verilerin işlenmesini sağlamak üzere başka bir şirket ile anlaşabilir[64]. Bu durumda, veri işleyen şirket, veri sorumlusu şirket adına işleme yaptığı için veri sorumlusu sıfatını almaz. Ancak, bu şirket, kişisel verileri kendi adına işlerse, örneğin, veri sorumlusu adına işlediği telefon numaralarına kendi şirketinin reklamını içeren bir mesaj gönderirse veri sorumlusu olarak kabul edilecektir[65].

§ 2. KİŞİSEL VERİLERİN KORUNMASININ TARİHÎ GELİŞİMİ VE KAYNAKLARI

I. GENEL OLARAK

Kişisel veri kavramı, günümüzdeki gibi ifade edilmese dâhi, tarihsel süreçte her zaman yerini ve önemini korumuştur. Bireyler, kişiliklerine özgü bazı değerleri, giz alanlarını diğer bireylere açarken dâhi bir güven ilişkisi aramıştır. Örneğin, Hipokrat Yemini olarak ifade edilen metinde, hekim, insanlarla ilişkisi çerçevesinde öğrendiği bilgileri sır olarak saklayacağına ilişkin söz vermektedir[66]. Böylece, hastalara ilişkin bilgiler korunarak, hastaların zarar görmemesi amaçlanmıştır. Hekim için öngörülen bu yükümlülük zamanla, banka memurları[67], avukatlar[68] gibi bazı

---

63 Bkz., Kişisel Verilerin Korunması Kanununun 3 üncü madde gerekçesi.

64 Bu durumda, veri işleyen ile veri sorumlusu arasında kişisel verilerin işlenmesini konu alan bir sözleşme kurulur. Bu sözleşmeye *(kişisel veri işleme sözleşmesine)* uygulanacak hükümler ile ilgili ayrıntılı bilgi için bkz., **Taştan,** s. 117 vd..

65 Hüseyin Murat **Develioğlu**, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul 2017, s. 42.

66 Metnin tamamı için bkz., İlyas **Altuner**, Hipokrat Yemini, Iğdır Üniversitesi Sosyal Bilimler Dergisi, S. 7, 2015, s. 4.

67 5411 sayılı Bankacılık Kanununun 73 üncü maddesinin birinci fıkrasına göre, "Kurul başkan ve üyeleri ile Kurum personeli, Fon Kurulu başkan ve üyeleri ile Fon personeli görevleri sırasında öğrendikleri bankalara ve bunların bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıkları ve müşterilerine ait sırları bu Kanuna ve özel kanunlarına göre yetkili olanlardan başkasına açıklayamaz ve kendilerinin veya başkalarının yararlarına kullanamazlar".

68 1136 sayılı Avukatlık Kanununun 36 ncı maddesinin birinci fıkrasına göre, "Avukatların, kendilerine tevdi edilen veya gerek avukatlık görevi, gerekse, Türkiye Barolar Birliği ve barolar

meslek gruplarına da getirilmiştir. Temelde, bu meslek gruplarına duyulan güveni de koruma amacı güden yükümlülükler ancak istisnaî hâllerde ortadan kalkmaktadır[69]. Bulaşıcı bir hastalıkla karşılaşan hekimin bunu tedavi etmek ve diğer kişilere bulaşmasını önlemek için bildirimde bulunması veya onlara açıklaması istisnaî hâle örnek olarak verilebilir.

Öte yandan, günümüzdeki anlamıyla kişisel verilerin korunmasına ilişkin gelişmeler 1960 lı yıllarda başlamıştır. Birçok ülkedeki kanunlaşma hareketlerini, 1995/46 sayılı Yönergeyi de etkileyen Alman Federal Anayasa Mahkemesinin 15.12.1983 tarihli *"Nüfus Sayımı Kanunu"*na ilişkin kararı takip etmiştir[70]. Söz konusu karara[71] göre, ülkede nüfus sayımı yoluyla bilgilerin elde edilmesi, temel hak ve özgürlüklerin görmezden gelinmesi demektir. Meşru bir temele dayanmayan veri toplama faaliyetleri, kişinin maddî, manevî varlığını koruma ve geliştirme hakkına zarar verdiği için kabul edilemez. İnsan onurunun, kişilik haklarının bir gereği olarak kişinin kendisine ilişkin *verilerin geleceğini serbestçe belirleme hakkı* kabul edilmelidir. Bu sebeple, Alman Federal Anayasa Mahkemesi, kişisel verilerin korunmasını talep etme hakkının bir temel hak olduğunu ifade etmiştir.

Federal Mahkemenin bu belirlemesinden sonra, kişisel verilerin korunması hakkı, kişilik hakkı çerçevesinde değerlendirilerek çağdaş toplumlarda çeşitli ulusal ve uluslararası düzenlemelere konu edilmiştir. Üstelik bu düzenlemeler, kişisel verilerin sadece devlete karşı değil, özel kişi ve kuruluşlara karşı korunmasını da kapsayacak niteliktedir. Bu başlık altında, kişisel verilerin korunması hakkı açısından önem arz eden uluslararası düzenlemelere değindikten sonra, Türkiye'de kişisel verilerin korunmasına ilişkin düzenlemelere yer verilecektir.

---

organlarındaki görevleri dolayısiyle öğrendikleri hususları açığa vurmaları yasaktır". 1512 sayılı Noterlik Kanununun 54 üncü maddesinde de benzer bir yükümlülüğe yer verilmiştir.

69 Gerçekten, 1593 sayılı Umumî Hıfzıssıhha Kanununun 57 inci ve devamı maddelerine göre, bulaşıcı hastalıkların bildirilmesi yükümlülüğü ortaya çıkar. Yine, Bankacılık Kanununun 73 üncü maddesinin ikinci ve devamı fıkralarında, Avukatlık Kanununun 36 ncı maddesinin ikinci fıkrasında öngörülen hâllerde sır saklama yükümlülüğü ortadan kalkar.

70 **Çekin**, Kişisel Veri, s. 6-7; **Şimşek**, s. 9; Elif **Küzeci,** İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı, İnsan Hakları Yıllığı, C. 32, 2014, s. 54.

71 Karar ile ilgili ayrıntılı bilgi için bkz., **Küzeci,** Bilgilerin Geleceği, s. 54-62.

II. ULUSLARARASI DÜZENLEMELER AÇISINDAN

A. Avrupa İnsan Hakları Sözleşmesi[72]

Kişisel veri alanında dolaylı koruma sağlayan düzenlemelerden İnsan Haklarının ve Temel Özgürlüklerin Korunması Sözleşmesi, Türkiye tarafından 1954'te onaylanmıştır. Sözleşme metninde kişisel veri ile yakından ilgili olan *"özel hayata ve aile hayatına saygı hakkı"* düzenlenmiştir. *"Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir"* hükmü gereği özel hayat, aile hayatı, konut ve haberleşme şeklinde dört husus koruma altına alınmıştır (AİHS.m.8/I)[73]. Bununla birlikte, Avrupa İnsan Hakları Mahkemesi birçok kararında[74] özel hayata ve aile hayatına saygı hakkı kapsamında kişisel veri teşkil eden bilgilerin korunması gerektiğine hükmetmiştir. Diğer bir söyleyişle, Avrupa İnsan Hakları Sözleşmesinde, kişisel verileri doğrudan ve bağımsız bir şekilde koruyan hüküm bulunmamaktadır[75]. Bu sebeple, Avrupa İnsan Hakları Sözleşmesi açısından kişisel veriler, ancak AİHM'in kişisel veri değerlendirmeleri ve kararları çerçevesinde korunur. Dolayısıyla, kararların kapsamı dışında kalan kişisel veriler için aynı korumadan bahsetmek mümkün değildir[76].

B. Ekonomik İşbirliği ve Kalkınma Örgütü[77] Rehber İlkeleri

Ekonomik İşbirliği ve Kalkınma Örgütü, ülkelerin sorunlarını tanımlamak, tartışmak, analiz etmek ve bunları çözmek için uygulanabilecek politikaları

---

72 RG. 19.3.1954, S. 8662.

73 Söz konusu hususlara ilişkin müdahaleler, AİHS.m.8/II hükmüne göre, "ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın ve ahlakın veya başkasının hak ve hürriyetlerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla" hukuka uygun kabul edilirler.

74 Kişinin özel hayatı veya iş hayatına dair telefon görüşmelerinin dinlenmesi ile ilgili Niemietz/ Almanya Kararı için bkz., http://hudoc.echr.coe.int/tur?i=001-57887 (Erişim Tarihi: 30.8.2018); Kişisel verilerin hukuka aykırı olarak elde edilmesi, arşivlenmesi veya uzun süre tutulması ile ilgili Amann/ İsviçre Kararı için bkz., http://hudoc.echr.coe.int/tur?i=001-58497 (Erişim Tarihi: 30.8.2018).

75 **Şimşek,** s. 30.

76 **Küzeci**, Kişisel Veri, s. 133. Zira, AİHM, öncelikle başvuru konusu olayın özel hayat, aile hayatı, konut ve haberleşme konularına ilişkin olup olmadığını belirler. Bkz., A. Şeref **Gözübüyük** / A. Feyyaz **Gölcüklü,** Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, Avrupa İnsan Hakları Mahkemesi İnceleme ve Yargılama Yöntemi, 10. Baskı, Ankara 2013, s. 333.

77 The Organisation for Economic Co-operation and Development (OECD).

geliştirmek amacıyla ekonomik alanda faaliyet göstermektedir. Örgüt, uluslararası veri işlenmesinin ekonomik yönünü dikkate alarak 1980 yılında Özel Yaşamın Gizliliğinin ve Sınırötesi Veri Akışının Korunmasına İlişkin Rehber İlkeleri kabul etmiştir[78]. Söz konusu ilkeler, veri koruma hukuku açısından tavsiye niteliğindeki asgarî standartları belirlediği için, üye devletler bu ilkeleri destekleyici ek düzenlemeler yapabilirler.

Rehber İlkeler, kişisel verilerin korunmasına ilişkin uluslararası ilk düzenleme niteliği taşıyan sekiz ilkeden oluşmaktadır. Bunlar; veri toplamanın sınırlı olması, verinin belirli niteliklere haiz olması, belirli amaca uygun olması, veri kullanımının sınırlı olması, veri güvenliği, açıklık ilkesi, bireysel katılım ilkesi ve hesap verebilirlik ilkesinden ibarettir[79]. Örgüt, kişisel verilerin ekonomilerdeki ve toplumlardaki rolünü dikkate alarak 2013 yılında rehber ilkeleri güncellemiştir. Yeni Rehber İlkelerde, ilk sekiz ilkeye ek olarak, ulusal gizlilik stratejileri, gizlilik yönetimi programları ve veri güvenliği ihlâl bildirimi kavramlarına yer verilmiştir[80].

C. 108 sayılı Sözleşme

Kişisel verilerin korunması alanında bağlayıcı ilk düzenleme olan 108 sayılı Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, Avrupa Konseyi tarafından 28 Ocak[81] 1981'de Strazburg kentinde imzaya açılmıştır[82]. Aynı tarihte Türkiye tarafından imzalanan 108 sayılı Sözleşme, gerçek kişilere ilişkin kişisel verilerin otomatik işleme tâbi tutulması karşısında özel hayata saygı hakkını güvence altına almayı amaçlamaktadır. Bununla birlikte, her

---

78 **Küzeci**, Kişisel Veri, s. 120.

79 Bkz., http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Erişim Tarihi: 31.8.2018); **Küzeci**, Kişisel Veri, s. 121.

80 https://www.oecd.org/sti/ieconomy/privacy.htm (Erişim Tarihi: 31.8.2018).

81 28 Ocak, Avrupa Konseyi tarafından, verilerin korunması alanındaki önemine binaen, Veri Koruma Günü olarak kararlaştırılmıştır. Bkz., https://www.coe.int/en/web/portal/28-january-data-protection-day (Erişim Tarihi: 31.8.2018). Türkiye'de ise, Kişisel Verilerin Korunması Kanununun kabul edildiği tarih olan 7 Nisan, Kişisel Verileri Koruma Günü olarak kutlanmaktadır. Bkz., Millî Eğitim Bakanlığı Eğitim Kurumları Sosyal Etkinlikler Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik.

82 https://www.coe.int/en/web/data-protection/convention108-and-protocol (Erişim Tarihi: 2.9.2018). Avrupa Konseyi üyesi olmayan ülkeler de bu sözleşmeye taraf olabilir. Bkz., **Şimşek,** s. 22.

devlet, Avrupa Konseyi Genel Sekreterini muhatap alarak sözleşmenin uygulanacağı kapsama ilişkin beyanlarda bulunabilir. Sözleşmenin belirli kişisel veri kategorilerine uygulanmayacağı, gerçek veya tüzel kişiler hakkında uygulanacağı yahut otomatik bilgi işleme konu olmayan kişisel veriler hakkında uygulanacağı bildirilebilir (108 sayılı Sözleşme m.3/2)[83]. 2001 yılında kişisel verilerin uluslararası akışını düzenleyen ve denetleyici makamlar öngören ek bir protokol kabul edilmiştir. 181 sayılı Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol[84] olarak ifade edilen bu düzenlemeye göre, taraf devletler, verilerin korunmasına ilişkin iç hukuktaki önlemlere uyulması amacıyla bir veya birden fazla denetleyici makam belirler. Ayrıca, sözleşmenin taraflarının yetki alanına girmeyen alıcılara, yeterli seviyede korunması garanti edilmesi şartıyla veri transferi yapılır.

Avrupa Konseyi, yeni bilgi ve iletişim teknolojilerinin kullanılması sebebiyle karşılaşılan zorluklarla başa çıkmak, 108 sayılı Sözleşmenin etkin bir şekilde uygulanmasını sağlamak amacıyla 108 sayılı Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunması Sözleşmesini değiştiren Protokol'ü Danimarka'nın Helsingör kentinde kabul etmiştir[85]. *"Modernize edilen 108 sayılı Sözleşme"* veya *"Sözleşme 108 +"* olarak ifade edilen bu düzenleme, 10 Ekim 2018 tarihinde imzaya açılmıştır[86]. Modernize edilen 108 sayılı Sözleşme, veri işlemenin şeffaf olması (m.8), verilerin orantılı ve asgari düzeyde işlenmesi (m.5) , veri sorumlusunun hesap verebilirliği (m.10), tasarıma göre gizlilik[87] (m.10) gibi

---

83 Türkiye tarafından sunulan 108 sayılı Sözleşme ile İlgili Beyanlara göre, "Türkiye Cumhuriyeti Sözleşmenin aşağıda bulunan kişisel verilere uygulanmayacağını beyan eder: a) gerçek kişilerin tamamen kişisel veya aynı konutta yaşayanlarla ilgili faaliyetlerine ilişkin olarak işlenmesine, b) Kanun tarafından öngörülen kamu kayıtlarına, c) Kanuna uygun olarak kamu bilgisine sunulan bilgilere, d) devlet kurumlarınca milli güvenlik, savunma ile soruşturma ve suç önleme amacıyla işlenen kişisel verilere". Devamında ise, sözleşmenin otomatik olmayan yollarla işlenen kişisel verilere de uygulanacağı bildirilmiştir.

84 RG. 5.5.2016, S. 29703. Protokol metnine ulaşmak için bkz., http://www2.tbmm.gov.tr/d26/1/1-0692.pdf (Erişim Tarihi: 2.9.2018).

85 https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108 (Erişim Tarihi: 3.9.2018).

86 Sözleşme metni için bkz., https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (Erişim Tarihi: 3.9.2018).

87 Modernize Edilen 108 sayılı Sözleşme'nin 10 uncu maddesinin ikinci paragrafında düzenlenen tasarıma göre gizlilik (*privacy by design)* ilkesi, veri sorumlularının (ve varsa veri işleyenlerin),

yenilikleri barındıran ilkelerle ilgili kişinin güvenini sağlamayı ve onu korumayı amaçlamıştır. Söz konusu düzenleme, Rusya, Almanya, İngiltere, İspanya, İtalya, Fransa, Avusturya ve hatta Avrupa Konseyi üyesi olmayan Uruguay'ın da içinde bulunduğu 26 ülke tarafından imzalanmıştır. Ancak, Türkiye sözleşmeye henüz taraf olmamıştır[88].

D. Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler

Birleşmiş Milletler, kişisel verilerin işlenmesi sırasında bireylerin kişisel verilerinin korunması amacıyla, 45/95 sayılı Genel Kurul Kararı ile 1990 yılında Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri[89] kabul etmiştir. Söz konusu düzenlemede, kişisel verilerin işlenmesinde dikkate alınması tavsiye edilen ilkelere ve önlemlere yer verilmiştir. Buna göre, öncelikle verilerin işlenmesinde hukuka ve dürüstlük kurallarına uygunluk aranmıştır. Devamında ise, işlenen verilerin doğru olmasına, amaçla sınırlı olarak işleme yapılmasına değinilmiştir. Kişisel verisi işlenen kişiye, veriye erişim hakkının verilmesi, yanlış verilerin düzeltilmesini talep etme hakkı tanınması da öngörülmüştür. Diğer bir ilke ise, özel nitelikli kişisel verilerin işlenerek ayrımcılığa yol açmasının önlenmesine ilişkindir. Bu kapsamda, özel nitelikli kişisel verilerin işlenmesi hâlinde ortaya çıkabilecek bazı zararlı sonuçlar önlenmeye çalışılmıştır. Kişisel veriler işlenirken, verilerin güvenliğini sağlanmasına yönelik tedbirlerin alınması gerektiği ifade edilmiştir. Ayrıca, yetkili kişi veya organların denetlemelerde bulunularak yaptırımlar uygulamasının gerekliliğine yer verilmiştir. Bilgisayarla İşlenen Kişisel

---

işlemenin ilgili kişinin temel hak ve hürriyetleri üzerindeki etkilerini dikkate alarak, teknik ve örgütsel önlemler çerçevesinde işlemeyi tasarlamalarını ifade eder. Bkz., https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (Erişim Tarihi: 5.3.2018). Örneğin, Amerika Birleşik Devletleri'nde gizli tanığa ilişkin bilgiler sisteme aktarılırken, görevli memurun dosyalama sistemindeki bir kutuya tıklamayı unutması sebebiyle gizli tanığa ilişkin bilgiler sanığa gönderilmiş ve gizli tanık öldürülmüştür. Haber metni için bkz., https://www.washingtonpost.com/nation/2019/02/22/court-official-failed-click-box-witness-paid-with-his-life/?noredirect=on&utm_term=.e4f 4a371830e (Erişim Tarihi: 25.2.2019). Bu noktada, veri sorumlusu olan kurum, veri işlemeye başlamadan önce, gizli tanığa ilişkin bilgilerin öğrenilmesi riskini ve bu durumun onun ölümüne sebep olacak derecede önemli olduğunu göz önüne almalı ve veri işleme sistemini buna göre tasarlamalıdır.

88 Bkz., https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures (Erişim Tarihi: 18.3.2019).

89 *Guidelines for the Regulation of Computerized Personal Data Files*, Düzenleme metni için bkz., https://digitallibrary.un.org/record/43365/files/E_CN.4_Sub.2_1988_22-EN.pdf (Erişim Tarihi: 5.9.2018).

Veri Dosyalarına İlişkin Rehber İlkeleri, gerek kamu sektöründe gerekse özel sektörde yapılan otomatik yolla veya otomatik olmayan yollarla veri işlemeyi kapsar. Düzenlemenin 10 uncu maddesine göre, iç hukukta yapılacak düzenlemelerde tüzel kişilerine ilişkin kişisel verilerin de korunabileceği ifade edilmiştir.

E. 1995/46 sayılı Yönerge

Kişisel veri alanında önemli bir etki gücüne sahip olan 1995/46 sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunması Hakkında Avrupa Parlamentosu ve Konseyi Yönergesi, 24 Ekim 1995 tarihinde kabul edilmiştir[90]. Bu kapsamda, her devletin özel hayatın gizliliğinin korunması amacıyla yaptığı düzenlemeler arasındaki önemli farklılıklara son vermek ve asgarî veri koruma ilkelerini düzenlemek amaçlanmıştır[91].

Avrupa Birliğinin İşleyişi Hakkında Anlaşmanın[92] 288 inci maddesi gereğince yönergeler, üye devletler açısından çerçeve nitelik taşır. Diğer bir söyleyişle, Avrupa Birliği, çıkardığı yönerge ile ulaşılması gereken sonucu belirler, şekli ve yöntemini ise üye devletin iç hukukuna bırakır[93]. Bu kapsamda, 1995/46 sayılı Yönerge, üye devletler açısından asgarî veri koruma ilkeleriyle amaçlanan korumayı sağlama noktasında bağlayıcı nitelik taşımaktadır. Bununla birlikte, üye devletler iç hukuklarındaki düzenlemeler çerçevesinde sağlanan korumanın kapsamını genişletme noktasında serbesttir.

1995/46 sayılı Yönergenin 3 üncü maddesinin birinci fıkrasına göre, tamamen veya kısmen otomatik yollarla işlenen kişisel veriler ve veri kayıt sisteminin parçası olmak kaydıyla otomatik yolla işlenmeyen kişisel veriler uygulama alanı içerisindedir. Günümüzde, veri işleme faaliyetinin çoğunlukla otomatik yollarla gerçekleştirildiği ve fizikî arşivlerin hızla bilgisayar ortamına aktarıldığı

---

90 Genel Veri Koruma Tüzüğü uyarınca, 25 Mayıs 2018 tarihi itibariyle 1995/46 sayılı Yönerge yürürlükten kaldırılmıştır.

91 1995/46 sayılı Yönerge'nin 7 nci paragrafı. Ayrıca bkz., **Küzeci**, Kişisel Veri, s. 167, 168; **Başalp,** Veri, s. 26; Leyla **Keser Berber** / Mahir M. **Ülgü** / Cüneyd **Er**, Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği, İstanbul 2009, s. 115.

92 OJ. 24.12.2002, C. 325.

93 Işıl **Özkan**, Avrupa Birliği Kamu Hukuku, Lizbon Anlaşmasındaki Son Değişiklerle, Ankara 2011, s. 117; Enver **Bozkurt** / Mehmet **Özcan** / Arif **Köktaş**, Avrupa Birliği Hukuku, Ankara 2001, s. 118.

düşünüldüğünde, hangi yollarla işlendiğinden bağımsız olarak bütün kişisel verilerin kapsam dâhilinde olduğu söylenebilir[94]. 1995/46 sayılı Yönergenin kişi bakımından uygulama alanına bakıldığında, sadece gerçek kişilere ilişkin kişisel veriler açısından koruma sağladığı görülür (m.3/II).

Kişisel verilerin işlenmesinde uyulması gereken genel ilkeler ise, verinin kalitesine ilişkin ilkeler başlığıyla 1995/46 sayılı Yönergenin 6 ncı maddesinde düzenlenmiştir. Hükme göre, kişisel verileri, hukuka ve dürüstlük kuralına uygun, belirli ve açık ve meşru amaçlarla, amaç ile bağlantılı ve ölçülü şekilde, doğru ve gerektiğinde güncel olmak üzere sınırlı sürelerle işlenebilirler. Genel ilkelerin devamında, kişisel verilerin işlenebileceği hâller başta olmak üzere, özel nitelikli veriler, ilgili kişinin hakları, veri sorumlusunun yükümlülükleri gibi birçok önemli konuya yer verilmiştir.

Bahsi geçen önemli konulardan biri de Çalışma Grubu'nun oluşturulmasıdır. Avrupa Parlamentosu ve Konseyi, 1995/46 sayılı Yönergenin 29 uncu maddesi uyarınca Kişisel Verilerin İşlenmesine Dair Bireylerin Korunması Hakkında Çalışma Grubu *(Article 29 Data Protection Working Party)* kurulmasını öngörmüştür. Her devletin birer temsilcisinin de yer aldığı danışma statüsüne sahip olan Çalışma Grubu, bağımsız olarak hareket eder. Çalışma Grubu, kişisel verilerin korunması hususunda tavsiyelerde bulunabilir, görüş bildirebilir veya yıllık raporlar sunabilir. 1995/46 sayılı Yönergenin uygulanmasında ve kapsamının belirlenmesinde 2016 yılına kadar faaliyet gösteren Çalışma Grubunun önemli bir yeri olduğu söylenebilir[95]. 25 Mayıs 2018 tarihi itibariyle Genel Veri Koruma Tüzüğü Yürürlüğe girdiği için Çalışma Grubu'nun yerini Avrupa Veri Koruma Kurulu[96] almıştır.

Avrupa Birliği, 1997 yılında, 1995/46 sayılı Yönergeyi telekomünikasyon alanında tamamlayan 1997/46 sayılı Telekomünikasyon Sektöründe Gizliliğin Korunması ve Kişisel Verilerin İşlenmesi Hakkında Avrupa Parlamentosu ve

---

94 **Küzeci**, Kişisel Veri, s. 169; **Şimşek,** s. 43. Bununla birlikte, 1995/46 sayılı Yönerge, topluluk hukukunun kapsamının dışındaki bir alanda, genel asayiş, savunma, kamu güvenliğine ilişkin verilerin işlenmesi durumlarında uygulanmaz (m.3/II).

95 Çalışma Grubu'nun faaliyet gösterdiği yıllara ilişkin arşive ulaşmak için bkz., http://ec.europa.eu/justice/article-29/documentation /index_en.htm (Erişim Tarihi: 6.9.2018).

96 Europan Data Proteciton Board (EDPB).

Konseyi Yönergesi Yönergesini[97] kabul etmiştir. 2002 yılına gelindiğinde, elektronik haberleşme sektöründeki düzenlemeleri içeren 2002/58 sayılı Yönerge kabul edilmiş ve bu yönerge ile 1997/46 sayılı Yönerge yürürlükten kaldırılmıştır[98].

F. Avrupa Birliği Temel Haklar Şartı[99]

Avrupa Birliği, bireylerin kişisel, medenî, politik, ekonomik ve sosyal haklarının tamamını içeren Avrupa Birliği Temel Haklar Şartını 2007 yılında kabul etmiştir. Düzenlemede haysiyet, özgürlükler, eşitlik, dayanışma, vatandaşlık hakları ve adalet başlıklarına yer verilmiştir. Kişisel verilerin korunması ise, özgürlükler başlığı altındaki 8 inci madde uyarınca düzenlenmiştir. Bu kapsamda, bireylerin kişisel verilerin korunmasını talep etme hakkının bulunduğuna, kişisel verilerin işlenmesinin belirli amaçlarla adil şekilde gerçekleştirilmesi gerektiğine, ilgili kişinin verilere erişme ve verilerin düzeltilmesini talep etme hakkına değinilmiştir. Ayrıca, sağlanan korumanın bağımsız bir makam tarafından denetlenmesi gerektiğine işaret edilmiştir. AİHS ile temelde aynı hususları düzenleyen Avrupa Birliği Temel Haklar Şartı, temel hak ve özgürlükleri belirgin ve açık hâle getirerek korumayı güçlendirmeyi hedeflemektedir[100].

G. Avrupa Birliği Genel Veri Koruma Tüzüğü

1. Genel Olarak

Avrupa Birliği kapsamında, 1995/46 sayılı Yönerge başta olmak üzere, kişisel verilerin korunması sağlamak amacıyla birçok düzenleme kabul edilmiştir. Kişisel verilerin işlenmesinde uyulması gereken genel ilkeler düzenlenmiş ve hatta 1995/46 sayılı Yönerge ile kişisel veri türleri, ilgili kişi ve veri sorumlusu konularında ayrıntılı hükümlere yer verilmiştir. Daha sonra, yeni teknolojilerin ortaya çıkış hızı ve veri kullanım alanlarının genişlemesi, üye devletlerin iç hukuklarında oluşan

---

97 OJ. 30.1.1998, L. 24.

98 Bu durumda, 1995/46 sayılı Yönergenin genel, 2002/58 sayılı Yönergenin ise özel bir düzenleme olduğu göz önünde bulundurularak her somut olayda uygulanacak hükümler tespit edilmelidir. Bkz., **Küzeci,** Kişisel Veri, s. 191.

99 OJ. 26.10.2012, C. 326.

100 Ayrıntılı bilgi için bkz., https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en (Erişim Tarihi: 6.9.2018). Ayrıca bkz., **Keser Berber / Ülgü / Er**, s. 114, 115.

uygulama farklılığı gibi sebeplerle 1995/46 sayılı Yönergenin sorunların çözümünde yetersiz kaldığını anlayan[101] Avrupa Birliği, 2016/679 sayılı Kişisel Verilerin İşlenmesi ve Bu Verilerin Serbest Dolaşımı Konusunda Gerçek Kişilerin Korunması ve 1995/46 sayılı Yönergenin Yürürlükten Kaldırılması Hakkında Avrupa Parlamentosu ve Avrupa Konseyi Tüzüğünü 2016 yılında kabul etmiştir. Genel Veri Koruma Tüzüğü olarak kısaltılan düzenlemenin iki yıllık bir geçiş sürecinden sonra 25 Mayıs 2018 tarihinde yürürlüğe girmesi hüküm altına alınmıştır (GVKT.m.99). Genel Veri Koruma Tüzüğü ile bireylerin haklarını ve Avrupa Birliği iç pazarını güçlendirmek, veri koruma kurallarının uygulanabilirliğini arttırmak, veri transferini kolaylaştırmak amaçlanmıştır. Aynı zamanda, rızaları alınmaksızın verilerin toplanması, arşivlenmesi veya kullanılması ihtimaline karşı, bireylere kişisel veriler üzerinde daha fazla kontrol imkânı sunulmuştur.

Düzenlemenin yönergelerden farklı olarak *tüzük* şeklinde düzenlenmesinin temel sebebi dikkat çekicidir. Avrupa Birliği'nin İşleyişi Hakkında Anlaşmanın 288 inci maddesine göre, *"Tüzükler, genel uygulama alanına sahiptir. Bütünüyle bağlayıcıdır ve tüm üye devletlerde doğrudan uygulanır"*. Bu sebeple, Genel Veri Koruma Tüzüğü, küresel veri koruma standardı oluşturmayı hedefleyen diğer düzenlemelerden ayrılır. Böylece, veri koruma standartlarını belirleyen metinlerde ortaya konulan kuralların her ülkede farklı uygulanmasının önüne geçilmeye çalışılmıştır. Diğer bir söyleyişle, Genel Veri Koruma Tüzüğünün kabulü ile üye ülkeler açısından bağlayıcı niteliğe sahip, yeknesak bir düzenleme metni ortaya konulmuştur[102].

Öncelikle, düzenlemenin Avrupa Birliği kapsamındaki bir işletmenin kişisel veri işleme faaliyetleri dışında da uygulanmasını mümkün kılan[103] ve böylece etki alanını önemli derecede genişleten bölgesel kapsam başlıklı Genel Veri Koruma Tüzüğünün 3 üncü maddesine değinmek gerekir. Buna göre, Genel Veri Koruma Tüzüğü, Avrupa Birliği içerisinde bulunan ilgili kişilerin (veri öznelerinin) kişisel

---

101 Nilgün **Başalp,** Avrupa Birliği Veri Koruması Genel Regülâsyonu'nun Temel Yenilikleri, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 21, S. 1, 2015, s. 82.

102 **Özkan**, s. 116; **Bozkurt / Özcan / Köktaş**, s. 119.

103 **Başalp,** Avrupa Birliği, s. 88.

verilerinin Avrupa Birliği içerisinde kurulu olmayan işletmeler tarafından belirli hususların işlenmesine uygulanır (GVKT.m.3/2). Belirli hususlar ise, işleme faaliyetinin ilgili kişiye mal veya hizmet sunulmasından ya da ilgili kişinin Avrupa Birliği içerisindeki davranışlarının izlenmesinden ibarettir (GVKT.m.3/2-a,b). Kısaca ifade etmek gerekirse, Avrupa Birliği içerisindeki ilgili kişiye mal veya hizmet sunulması ya da davranışlarının izlenmesi konularında, Avrupa Birliği Hukukuna tâbi olmayan işletmelerin o kişiye ilişkin verileri işlemelerinde Genel Veri Koruma Tüzüğü uygulama alanı bulacaktır. Ulaşılan sonuç, Avrupa Birliği içerisindeki ilgili kişilere özellikle mal veya hizmet sunan işletmelerin, iç hukuklarında düzenlenen veri koruma kurallarına ek olarak Genel Veri Koruma Tüzüğüne uygun davranmalarını gerektirir. İşletmelerin üye devletlerin bir veya birkaçında kullanılan dili, para birimini esas alarak Avrupa Birliği içerisindeki ilgili kişileri hedef alan mal veya hizmet sunması sebebiyle kişisel verileri işlemesi hâlinde çıkabilecek uyuşmazlıklara Genel Veri Koruma Tüzüğü uygulanabilecektir[104]. Örneğin, merkezi Amerika Birleşik Devletleri'nde bulunan Google, Genel Veri Koruma Tüzüğünde yer alan yükümlülüklerden bazılarını ihlâl ettiği gerekçesiyle, Fransa Veri Koruma Kurulu *(CNIL)* tarafından 50 milyon Euro ödemeye mahkûm edilmiştir[105].

1995/46 sayılı Yönergeyi ilga ederek yürürlüğe giren Genel Veri Koruma Tüzüğü, Çalışma Grubunun yerini almak üzere, Avrupa Birliği Veri Koruma Kurulu'nu öngörmüştür. Genel Veri Koruma Tüzüğünün 68 inci ve devamı maddelerine göre, Avrupa Veri Koruma Kurulu, Avrupa Birliği genelinde veri koruma kurallarının tutarlı bir şekilde uygulanmasına katkıda bulunan ve Avrupa Birliği'nin veri koruma makamları arasında işbirliğini teşvik eden bağımsız bir

---

104 **Develioğlu**, s. 18.

105 Google, şeffaflık ve bilgi yükümlülüklerini ihlâl etmesi ve kişiselleştirilmiş reklamlar için aldığı rızanın geçersiz olması sebebiyle Genel Veri Koruma Tüzüğü'nü ihlâl etmiştir. Yükümlülüklerin ihlâli ile ilgili ayrıntılı bilgi için bkz., https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en (Erişim Tarihi: 29.1.2019). Ayrıca bkz., Çağrı **Zeybek Ünsal,** Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri ile Uyumluluğu ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi, Hacettepe Hukuk Fakültesi Dergisi, C. 3, S. 1, 2013, s. 118-120.

Avrupa organıdır. Söz konusu kurul, ulusal veri koruma makamlarının temsilcilerinden ve Avrupa Veri Koruma Denetleyicisi'nden[106] oluşur.

2. Genel Veri Koruma Tüzüğünde Yer Alan Önemli Konular

Genel Veri Koruma Tüzüğü, 1995/46 sayılı Yönergede sağlanan korumayı güncellemek ve karşılaşılan sorunları çözmek amacıyla yeni kavramlara yer vermiş veya mevcut korumanın kapsamını genişletmiştir. Tüzüğün Avrupa Birliği dışındaki etki gücü düşünüldüğünde söz konusu yeniliklere ve sağlanan haklara değinmek gerekir.

a. Kişisel Verilerin İşlenmesinde Rıza

Kişisel veriler, kanunî dayanak olmadıkça veya ilgili kişinin rızası alınmadıkça işlenemezler. Doğuracağı sonuçların önemi dikkate alınarak, kişisel verilerin işlenmesinde rızadan ne anlaşılması gerektiği ve geçerli rızanın şartları Genel Veri Koruma Tüzüğü ile ayrıntılı olarak düzenlenmiştir. Genel Veri Koruma Tüzüğünün 4 üncü maddesinin onbirinci fıkrasına göre rıza, *"veri sahibinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık göstergedir"*[107]. Söz konusu hüküm ile paralel nitelik arz eden Çalışma Grubu'nun rıza ile ilgili kabul ettiği ilkelere göre, geçerli bir rıza, serbest iradeye dayanan, belirli, aydınlatılmış, açık olma unsurlarını taşımalıdır. Söz konusu ilkeler daha sonra Avrupa Birliği Veri Koruma Kurulu tarafından güncelleştirilerek kabul edilmiştir.

Genel Veri Koruma Tüzüğü, işlemeye müsaade edildiğinin açıkça ortaya konulmasını aradığı için, kişinin susması şeklinde gerçekleşen eylemsizlikleri geçerli bir rıza olarak nitelendirmez[108]. Örneğin, kişisel verilerin işlenmesine rıza gösterildiğini ifade eden önceden işaretlenmiş kutudaki işareti kaldırmayan kişinin eylemsizliği, rıza kapsamında değerlendirilemez.

---

106 *European Data Protection Supervisor (EDPS).*

107 Bkz., **Article 29 Data Protection Working Party**, Guidelines on Consent under Regulation 2016/679, WP 259, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030 (Erişim Tarihi: 8.9.2018), s. 5.

108 Genel Veri Koruma Tüzüğü 32 nci paragraf.

Söz konusu düzenlemede, işlenme sebebiyle ortaya çıkabilecek riskleri algılamak ve bu yönde hareket edilmesini sağlamak amacıyla, çocuklar için özel bir koruma öngörülmüştür[109]. Gerçekten, Genel Veri Koruma Tüzüğünün 8 inci maddesinin birinci fıkrasına göre, doğrudan çocuğa sunulan bilgi toplumu hizmetleri hususunda 16 ve üzeri yaştaki çocuklardan alınan rıza ile yapılan veri işleme faaliyeti hukuka uygundur. Ancak, çocuk 16 yaşından küçük ise, işleme faaliyetlerinin hukuka uygun olması için velayet hakkı sahibinin izni veya icazeti gerekir. Tüzük, belirlenen sınırın 13 yaşa kadar indirilebileceğini öngörmüştür.

b. Unutulma Hakkı

Kendisini farklı sebeplerle kişisel verilerini paylaşma ihtiyacı içerisinde hisseden bireyler, hayatlarının geri kalanında bu durumun olumsuz sonuçları ile karşılaşabilirler. Kişisel verilerin paylaşılması, kişinin iradesi dışındaki sebeplerden de kaynaklanabilir. Her ne sebeple olursa olsun, ilgili kişi, bu olumsuz sonuçları hayatından çıkarmayı ve geri kalan hayatı için beyaz bir sayfa açmayı isteyebilir[110]. İşte bu amaçları gerçekleştirmek için güvence oluşturan unutulma hakkı, Genel Veri Koruma Tüzüğünde tanınmıştır[111]. İlgili kişiye sağlanan haklar arasında önemli bir

---

109 GVKT'den önce, 1995/46 sayılı Yönerge'de çocuklar için özel koruma maddelerine yer verilmemiştir. Ancak, Çalışma Grubu'na göre, mevcut kurallar çocukların verilerini çoğu durumda korur. Diğer durumlarda ise, çocuğun çıkarlarına ve diğer kurallara (Birleşmiş Milletler Çocuk Hakları Sözleşmesi gibi düzenlemelere) atıfta bulunarak çözüm aranmalıdır. Ayrıntılı bilgi için bkz., **Article 29 Data Protection Working Party**, Working Document 1/2008 on the Protection of Children's Personal Data, WP 147, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf (Erişim Tarihi: 8.9.2018), s. 17, 18.

110 **Küzeci,** Kişisel Veri, s. 231; Sinan Sami **Akkurt,** 17.06.2015 Tarih, E. 2014/4-56, K. 2015/1679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı ve Mukayeseli Hukuk Çerçevesinde "Unutulma Hakkı", Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 64, S. 4, 2016, s. 2615; **Başalp,** Avrupa Birliği, s. 93.

111 Bu hakkın tanınmasında, AAD'ın Google İspanya ve Google Inc. kararının da etkisi büyüktür. Söz konusu davada, kişinin borçları nedeniyle açık artırmaya çıkarılan evi ile ilgili ilanın arama motorundan kaldırılması talep edilmiştir. Zira, kişi evini geri aldığını ve bu bilgilerin artık gereksiz olduğunu ileri sürmektedir. Mahkeme, burada, arama motorunun veri sorumlusu olduğunu ve kişilerin kendileriyle ilgili bağlantıların arama motorlarından kaldırılmasını talep etme haklarının olduğunu ifade etmiştir. Karar için bkz., AAD., C-131/12 (Google Spain SL ve diğer şirket /Agencia Espanola de Proteccion de Datos (AEPD) ve diğerleri), 13.5.2014, bkz., http://www.abgm.adalet.gov.tr/abadaletdivani/abadaletdivani.html (Erişim Tarihi: 22.9.2018). Karar ile ilgili ayrıntılı değerlendirmeler için bkz., **Küzeci**, Kişisel Veri, s. 230 vd.; Aydın **Akgül,** Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" ve Adalet Divanı'nın "Google Kararı", Türkiye Barolar Birliği Dergisi, S. 116, 2016, s. 30 vd.; Unutulma hakkının tarihi ile ilgili ayrıca bkz., **Başalp,** Avrupa Birliği, s. 94 vd..

yeri olan *unutulma hakkı*, kişisel verilerin silinmesinin, işlenmesinin ve yayılmasının durdurulması hususunda ilgili kişiye haklar tanır ve hakkın kullanılması hâlinde kişisel verilerin gecikmesizin silinmesi noktasında veri sorumlusunu yükümlü kılar (GVKT.m.17). Buna göre, Genel Veri Koruma Tüzüğünün 17 nci maddesinin birinci fıkrasında yer verilen hâllerde, veri sorumlusu, ilgili kişiye ilişkin verileri gecikmeksizin silmekle yükümlü kılınmıştır. Ayrıca, silme talebini alan veri sorumlusu, kişisel veriye yönelik her türlü bağlantının[112] veya nüshanın silinmesi hususunda diğer veri sorumlularını da bilgilendirmelidir. Aynı maddenin üçüncü fıkrasına göre, ifade özgürlüğünün korunması, kamu sağlığı, tarihsel, istatistiksel ve bilimsel amaçların gerekli kılması gibi durumlarda veri sorumlusu, unutulma hakkının gereğinin yapılmasından imtina edebilir. Bir diğer deyişle, mutlak bir unutulma hakkından bahsedilemez. Genel Veri Koruma Tüzüğünün 17 nci maddesinin üçüncü fıkrasında yer alan durumlar ile unutulma arasında gözetilecek menfaat dengesi sonucunda unutulma hakkına yer verilmelidir[113].

c. Veri Taşınabilirliği Hakkı

Genel Veri Koruma Tüzüğünde tanınan diğer bir yeni hak, veri taşınabilirliği hakkıdır. Veri taşınabilirliği hakkı, *"kişinin veri sorumlusuna sağladığı verileri farklı hizmetlerde kendi amaçları doğrultusunda kullanmak için, yapılandırılmış, yaygın olarak kullanılan ve makinede okunabilir bir biçimde alma ve verileri başka bir veri sorumlusuna aktarma hakkını ifade eder"* (GVKT.m.20). Hükmün devamında, söz konusu hakkın kullanımına ilişkin sınırlara yer verilmiştir. Buna göre, işlemenin kanunî dayanağı rıza veya sözleşmenin ifası ise ya da işleme otomatik yöntemlerle gerçekleştiriliyorsa bu hak kullanılabilir (GVKT.m.20/1-a,b). Böylece, verilerin

---

112 Genel Veri Koruma Tüzüğünün yürürlüğe girmesinden önce, Çalışma Grubu unutulma hakkının kullanılmasına ilişkin ilkeler yayınlamıştır. Buna göre, sadece kişinin adını temel alarak yapılan aramalar açısından bu hak kullanılabilir. Bkz., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf (Erişim Tarihi: 22.3.2019). Bu sınırlama, ad dışındaki kriterlerle yapılan aramalarda kaynak bilgiye ulaşımı mümkün kılacaktır. Bkz., **Küzeci,** s. 233.

113 **Başalp,** Avrupa Birliği, s. 101. Ayrıca bkz., **Develioğlu,** s. 92.

kullanılabilirliği etkilenmeden, bir ortamdan diğer bir ortama kolay ve güvenli bir şekilde aktarma, kopyalama veya taşıma imkânı sağlanmıştır[114].

d. Tasarıma Dayalı ve Varsayılan Olarak Veri Koruma

Tasarım yoluyla ve varsayılan olarak göre veri koruma *(data protection by design and by default)*, Genel Veri Koruma Tüzüğünde veri sorumlusunun uyması gereken genel yükümlülükler başlığı altında ele alınmıştır. Genel Veri Koruma Tüzüğünün 25 inci maddesinin birinci fıkrasında düzenlenen *tasarım yoluyla veri koruma*, veri işleme faaliyetine ilişkin sistemin tasarlanması aşamasında ve daha sonra kullanım ömrü boyunca, veri koruma ilkelerini ve kişilik haklarının dikkate alınmasını ifade eder[115]. Tasarım yoluyla veri koruma, ilgili kişileri korumaya yönelik teknik ve örgütsel önlemlerin alınmasını ve uygulanmasını kapsar. Veri sorumluları, kişisel veri işleme sistemlerini, stratejilerini, politikalarını, süreçlerini bu yaklaşıma göre geliştirmek ve fiziksel bir tasarım ortaya koymakla yükümlüdür. Örneğin, kişiyi tanımlayan isimler yerine takma adların kullanılmasına ilişkin bir veri işleme sistemi tasarlanabilir. Aynı şekilde, sadece yetkili kişilerin okuyabileceği şifrelenmiş mesajlardan oluşan veri işleme sistemi kurulabilir. Aslında bu yaklaşım, veri kayıt sisteminin, verileri güvenli bir şekilde muhafazası için gerekli olan her türlü önlemin alınmasını içerir. Bu durumda, verilerin işlenmeye başlanmasından önce, sistemin olası açıkları tespit edilmelidir.

Genel Veri Koruma Tüzüğünün 25 inci maddesinin ikinci fıkrasında düzenlenen *varsayılan olarak veri koruma* ise, güdülen amaç doğrultusunda işlenmek istenen belirli verilerin yüksek gizlilikte işlenmesi gerektiğini esas alan yaklaşımdır[116]. Bu yaklaşıma göre, veriler, amacı gerçekleştirmek için gerekli olan seviyede işlenmeli, başlangıçta belirlenecek kısa süreye uygun şekilde depolanmalı

---

114 Söz konusu hak ile ilgili ayrıntılı bilgi için bkz., **Article 29 Data Protection Working Party**, Guidelines on the Right to Data Portability, WP 242, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 (Erişim Tarihi: 10.9.2018).

115 **Develioğlu,** s. 101, 102; Leyla **Keser Berber,** Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, İstanbul 2014, s. 21.

116 **Develioğlu,** s. 102; Leyla **Keser Berber,** Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, İstanbul 2014, s. 24.

ve özellikle belirsiz sayıda kişinin erişimine açılmamalıdır. Örneğin, üyelik kaydı oluşturan sosyal medya platformları, kayıt için gerekli bilgilerin amaca uygun ve asgari düzeyde olmasına dikkat etmelidir. Aynı zamanda, üyenin müdahalesi olmaksızın, profilinde yer alan kişisel verilerin sınırsız erişime açılmamasını sağlamalıdır. Örneğin, Facebook veya Twitter gibi sosyal platformlar, hesap oluşturan her bir kişinin hesabının ve paylaşımlarının gizli olmasını kural hâline getirmelidir. Bir diğer deyişle, oluşturulan hesap, kural olarak *"herkese açık"*sa ve ilgili kişi aktif davranışıyla bunu istediği kişilerin erişimine sunabiliyorsa, bu durum varsayılan olarak veri koruma ile bağdaşmaz. Varsayılan olarak veri koruma, oluşturulan hesabın sadece ilgili kişinin istediği kişilerin erişimine açık olmasını, ilgili kişinin aktif davranışıyla herkesin erişimine sunabilmesini öngörür.

Tasarım yoluyla ve varsayılan olarak veri koruma, veri işlemelerinde ortaya çıkan hukuka aykırılıklara sonradan tepki göstermek yerine, gizlilik bilinci ile hareket ederek ileriye etkili olarak önlem almayı içerir. Böylece, verilerin korunması için herhangi bir adım atmaya gerek duymaksızın gizliliğin korunduğu bir sistem oluşturulmak istenmektedir.

e. Veri İhlal Bildirimi

Veri ihlal bildirimine ilişkin açıklamalardan önce, kişisel veri ihlalinin ne anlama geldiğini belirlemek gerekir. *Veri ihlali (data breach)*, kişisel verinin kazara veya kanuna aykırı bir şekilde imha edilmesine, kaybolmasına, değiştirilmesine, izinsiz olarak ifşa edilmesine veya erişilmesine neden olan bir güvenlik ihlali anlamına gelir (GVKT.m.4/XII). Kişisel veri ihlali mümkün olan en kısa sürede giderilmezse, bu durum, ayrımcılık, dolandırıcılık, takma adın öğrenilerek kişisel verilere ulaşılması, itibarın zedelenmesi veya korunan meslekî sırların açığa çıkması gibi sebeplerle maddî, manevî veya iktisadî zararlara yol açabilir[117].

---

[117] Genel Veri Koruma Tüzüğü'nün 85 inci paragrafı. Verilerin hukuka aykırı olarak elde edilmesi amacıyla izlenen yöntemler her geçen gün farklılaşmakla birlikte, bilgisayar ortamında sıkça rastlanılan bazı yöntemler bulunmaktadır. Oltalama *(phishing)* olarak ifade edilen yöntemde genellikle, kişilere resmi bir kurum veya banka tarafından gönderildiği izlenimiyle elektronik posta gönderilmekte ve içerikteki bağlantı aracılığıyla kişilerin kullanıcı adı ve şifre bilgisi gibi verilerine ulaşılmaktadır. Verilere ulaşmak için, *klavye hareketlerinin, ekran görüntüsünün izlenmesi* gibi yöntemlerin kullanılması da sıkça görülür. Bu yöntemlerle klavyenin veya ekranın

Genel Veri Koruma Tüzüğünün 33 üncü maddesi, bahsi geçen veri ihlallerine ilişkin denetim makamına yönelik bildirim sistemini düzenlemektedir. Buna göre, veri sorumlusu, veri ihlalinin gerçek kişilerin hak ve hürriyetleri açısından riske sebebiyet verme ihtimali yüksekse, ihlalden haberdar olduğu andan itibaren gereksiz gecikmeye mahal vermeksizin, en geç 72 saat içerisinde durumu denetim makamına bildirmelidir[118]. Veri ihlal bildirimi, 72 saat içerisinde yapılmamışsa, bildirimde gecikme sebebine de yer vermelidir. Veri ihlalini fark eden veri işleyen, gecikmeksizin veri sorumlusuna bildirmelidir (GVKT.m.33/II). Örneğin, verilerin arşivlenmesi ve kaydının tutulması noktasında veri sorumlusunun anlaştığı bilişim teknolojileri firması (veri işleyen), veri ihlalini tespit ettikten sonra derhal veri sorumlusuna bu durumu bildirmelidir. Veri sorumlusu ise, denetim makamına veri ihlal bildirimlerini gerçekleştirir. Veri sorumlusu, veri ihlalinin hak ve hürriyetler açısından yüksek risk teşkil etmesi ihtimalinde, gereksiz gecikmeye mahal vermeksizin durumu ilgili kişiye de bildirmelidir (GVKT.m.34).

f. Veri Koruma Görevlisi

Genel Veri Koruma Tüzüğünün getirdiği diğer bir yenilik ise, veri koruma görevlisi *(data protection officer)* atama yükümlülüğüdür. *Veri koruma görevlisi*, işleme faaliyetinde bulunan çalışanların bilgilendirilmesi, bilinçlendirilmesi, eğitilmesi, çalışanlara tavsiyede bulunulması ve işleme faaliyetinin tâbi olunan veri

izlenmesi için öncelikle, virüs, bukalemun, truva atı veya çerez olarak adlandırılan programların arka planda çalışır durumda bulunması gerekecektir. Ayrıntılı bilgi ve diğer yöntemler ile ilgili olarak bkz., Osman **Açıkgöz,** Kişisel Verilerin Hukuka Aykırı Şekilde Elde Edilmesi ve İnternet Bankacılığında Kullanılması Sonucu Malvarlığı Zarara Uğratılan Bankaya Karşı Mevduat Sahibinin Hukukî Sorumluluğu, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 22, S. 1, 2016, s. 396 vd..

118 Örneğin, ilgili kişi, veri sorumlusunun hizmetine ilişkin kişisel verileri içeren ve veri sorumlusunu taklit eden bir elektronik posta aldığı konusunda veri sorumlusunu uyarmıştır. Bu durumda, veri sorumlusu, kişisel verilere yetkisiz erişim veya kendi ağına izinsiz giriş olduğuna dair kanıtları araştırır. Eğer kişilerin hak ve hürriyetleri açısından riske sebebiyet verecek bir ihlal söz konusuysa, bu andan itibaren gecikmesizin 72 saat içersinde denetim makamına bildirimde bulunmalıdır. Denetim makamı, Tüzüğün 51 inci ve devamı maddelerinde düzenlenen, üye devletler tarafından kurulan, bağımsız bir kamu kuruluşudur (GVKT.m.4/21). Bkz., **Article 29 Data Protection Working Party**, Guidelines on Personal Data Breach Notification Under Regulation 2016/679, WP 250, https://ec.europa.eu/newsroom/document.cfm?doc_id=47741 (Erişim Tarihi: (10.9.2018), s. 9.

koruma hükümlerine uyumluluğunun izlenmesi[119] gibi amaçları yerine getirmekle görevli kişidir (GVKT.m.39). Veri sorumlusunun çalışanı olan veya hizmet sözleşmesiyle görevini yerine getiren veri koruma görevlisi bağımsızdır, herhangi bir talimat almaz. Tüzüğün 37 nci maddesine göre, üç grup veri koruma görevlisi atama yükümlülüğü altındadır. Bunlar; kamu kurum veya kuruluşları (yargı yetkisi çerçevesinde hareket eden mahkemeler hariç), büyük ölçekli olarak düzenli ve sistematik veri izleme faaliyeti gerçekleştiren kuruluşlar ve özel nitelikli kişisel verileri büyük ölçekli olarak işleyen kuruluşlar. Hükümde sözü geçen üç grup dışında işleme faaliyeti gerçekleştiren kuruluşlar ise, isteğe bağlı olarak veri koruma görevlisi atayabilirler.

g. Öngörülen Cezalar

Genel Veri Koruma Tüzüğünün ihlali hâlinde, denetim otoritesi en uygun kararı[120] almak konusunda yetkilidir. Denetim otoritesi sadece söz konusu kararları verebilir veya bunlara ek olarak para cezası öngörebilir. Denetim otoritesi, söz konusu kararı alırken ihlal ile eşdeğer nitelikte etkili, orantılı, caydırıcı yaptırımlar

---

119 Veri koruma görevlisi, veri koruma yükümlülüklerini yerine getirme hususunda önemli bir rol oynasa dâhi veri koruma kurallarının ihlâlinden şahsen sorumlu değildir. Bu durumda, sorumluluk veri sorumlusuna aittir. Bkz., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/ (Erişim Tarihi: 10.9.2018).

120 Genel Veri Koruma Tüzüğünün 58 inci maddesinin ikinci fıkrasına göre, ihlâl hâlinde denetim otoritesi şu hususlarda yetkilidir: *"(a) bir kontrolör veya işleyiciye amaçlanan işleme faaliyetlerinin bu Tüzük'ün hükümlerini ihlal etmesinin muhtemel olduğu hususunda ihtarlarda bulunulması; (b) işleme faaliyetlerinin bu Tüzük'ün hükümlerini ihlal etmiş olduğu hallerde, bir kontrolör veya işleyiciye kınama cezaları verilmesi; (c) veri sahibinin bu Tüzük uyarınca sahip olduğu haklarının kullanımına ilişkin taleplerine uyulması hususunda kontrolör veya işleyiciye talimat verilmesi; (d) işleme faaliyetlerinin, uygun olduğu hallerde, belirtilen bir şekilde ve belirtilen bir süre içerisinde bu Tüzük'ün hükümlerine uyumlu hale getirilmesi hususunda kontrolör veya işleyiciye talimat verilmesi; (e) bir kişisel veri ihlalinin veri sahibine iletilmesi hususunda kontrolöre talimat verilmesi; (f) bir işleme yasağı da dahil olmak üzere geçici veya kati bir sınırlama getirilmesi; (g) 16, 17 ve 18. maddeler uyarınca kişisel verilerin düzeltilmesi ya da silinmesi veya işleme faaliyetinin kısıtlanması ve 17(2) maddesi ile 19. madde uyarınca söz konusu işlemlerin kişisel verilerin açıklandığı alıcılara bildirilmesi yönünde talimat verilmesi; (h) 42 ve 43. maddeler uyarınca sağlanan bir belgelendirmenin geri çekilmesi veya belgelendirme organına söz konusu belgelendirmenin geri çekilmesi yönünde talimat verilmesi, veya belgelendirme gerekliliklerinin yerine getirilmediği veya artık yerine getirilmediği hallerde, belgelendirme organına belgelendirme sağlamaması yönünde talimat verilmesi; (i) her münferit durumun koşullarına dayalı olarak, bu paragrafta atıfta bulunulan tedbirlere ek olarak veya bu tedbirler yerine 83. madde uyarınca bir idari para cezası kesilmesi; (j) üçüncü bir ülkedeki bir alıcıya veya uluslararası bir kuruluşa yönelik veri akışlarının askıya alınması yönünde talimat verilmesi".*

öngörmeli ve her bir durumu kendi içerisinde değerlendirmelidir[121]. Genel Veri Koruma Tüzüğünün idarî para cezası verilmesinin genel koşullarını düzenleyen 83 üncü maddesine göre, idari para cezasının meblağına karar verilirken belirli hususlar göz önünde bulundurulmalıdır. Buna göre, ihlâlin niteliği, ağırlığı ve süresinin yanında ihlalden etkilenen ilgili kişilerin sayısı ve ilgili kişilerin uğradığı zararın seviyesi dikkate alınmalıdır. Ayrıca, ihlalin kasıtlı nitelik arz edip etmediği, veri sorumlusunun geçmişte konuyla ilgili ihlalleri, veri sorumlusunun ihlalin yol açtığı olumsuz etkilerin azaltılması için yaptığı işlemler, ihlalden etkilenen veri kategorileri, veri ihlal bildiriminin yapılıp yapılmadığı ve içeriği gibi durumun özellikleri açısından geçerli diğer ağırlaştırıcı ve hafifletici etkenler dikkate alınmalıdır (GVKT.m.83/II-a ve k).

Genel Veri Koruma Tüzüğünde veri ihlali sonucunda verilecek idari para cezaları için iki farklı azamî meblağ kabul edilmiştir. Tüzüğün 83 üncü maddesinin dördüncü fıkrasında yer alan ihlaller[122] için, 10 milyon Euro'ya kadar veya bir teşebbüsün söz konusu olduğu durumlarda, bir önceki mali yılın dünya çapında toplam yıllık cirosunun %2 sine kadar idari para cezasına hükmedilebilir. Tüzüğün 83 üncü maddesinin beşinci fıkrasında yer alan ihlaller[123] için ise, 20 milyon Euro'ya kadar veya bir teşebbüsün söz konusu olduğu durumlarda, bir önceki mali yılın dünya çapında toplam yıllık cirosunun %4 üne kadar idari para cezasına hükmedilebilir. Azamî meblağ belirlenirken her bir fıkrada yer verilen iki seçenekten hangisi daha yüksekse o dikkate alınır.

---

121 Ayrıca, denetim otoritelerinin aralarındaki bilgi alışverişine aktif katılımda bulunması verilen cezaların uyumlulaştırılması açısından fayda sağlar. Bkz., **Article 29 Data Protection Working Party**, Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679, WP 253, https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 (Erişim Tarihi: 11.9.2018), s. 5 vd.

122 "*(a) kontrolör veya işleyicinin 8, 11, 25 ila 39 ile 42 ve 43. maddeler uyarınca yükümlülükleri; (b) belgelendirme organının 42 ve 43. maddeler uyarınca yükümlülükleri; (c) izleme organının 41(4) maddesi uyarınca yükümlülükleri"*.

123 "(a) 5, 6, 7 ve 9. maddeler uyarınca rıza koşulları da dâhil olmak üzere işleme faaliyetine ilişkin temel ilkeler; (b) veri sahiplerinin 12 ila 22. maddeler uyarınca hakları; (c) 44 ila 49. maddeler uyarınca bir üçüncü ülkedeki bir alıcıya veya bir uluslararası kuruluşa yönelik kişisel veri aktarımları; (d) üye devlet hukuku uyarınca Bölüm IX çerçevesinde kabul edilen her türlü yükümlülük; (e) 58(2) maddesi uyarınca denetim makamının bir emri veya geçici ya da kesin işleme sınırlaması veya veri akışlarını askıya almasına uyumlu hareket edilmemesi veya 58(1) maddesinin ihlal edilmesi suretiyle erişim sağlanmaması".

III. ULUSAL DÜZENLEMELER AÇISINDAN

A. Genel Olarak

Uluslararası alanda verilerin korunmasına yönelik düzenlemelere Türkiye de yabancı kalmamıştır. Kişisel veriler alanında Türkiye tarafından ilk adım, 108 sayılı Sözleşmenin 28 Ocak 1981 tarihinde imzalanması ile atılmıştır. Düzenlemenin onaylanması ise, uzun yıllar sonra 2 Şubat 2016 tarihinde gerçekleştirilmiştir. Bu süreçte, kişisel veri alanında ilk düzenleme 2004 yılında Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik[124] ile getirilmiştir. Söz konusu düzenleme, telekomünikasyon sektörüne ilişkin olmayan kişisel veriler açısından uygulama alanı bulamamıştır. Aynı yıl kabul edilen 5237 sayılı Türk Ceza Kanununun[125] *"Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar"* başlığını taşıyan bölümünde, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme suçları düzenlenmiştir. Ancak, kişisel verilerin tanımını, işlenme şartlarını, aktarılmasını, yok edilmesini ve dolayısıyla kişisel verilerin hukuka aykırı olarak işlenmesini açıklayan herhangi bir düzenleme bulunmadığı için suçun oluşumu noktasında yapılacak olan değerlendirmeler eksik kalmıştır[126].

2010 yılına gelindiğinde, Anayasanın[127] 20 nci maddesinin üçüncü fıkrası uyarınca, kişisel verilerin korunmasını talep hakkı tanınmıştır[128]. Buna göre, *"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"*. Hükümde, kişisel

---

124 RG. 6.2.2004, S. 25365.
125 RG. 12.10.2004, S. 25611.
126 Kişisel Verilerin Korunması Kanununun Genel Gerekçesi, s. 5.
127 RG. 9.11.1982, S. 17863.
128 Anayasada kişisel verilerin korunmasını talep hakkı tanınmadan önce, özel hayatın gizliliği ve kişilik haklarının korunması çerçevesinde korunması söz konusu olmuştur. Ayrıntılı bilgi için bkz., **Başalp**, Veri, s. 100 vd..

verilerin korunmasını talep hakkı başta olmak üzere, bilgi edinme hakkı, erişim hakkı, düzeltilmesini ve silinmesini talep etme hakkına yer verilmiştir. Ayrıca, işlemenin açık rıza bulunan veya kanunda öngörülen hâllerde amaca uygun olarak yapılacağı ifade edilmiştir.

2012 yılında elektronik haberleşme sektörüne yönelik olarak Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik kabul edilmiştir. Bu düzenleme ile birlikte Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik yürürlükten kaldırılmıştır. Görüldüğü üzere, söz konusu yönetmeliklerin kapsam itibariyle kişisel verilerin korunması alanında tam koruma sağlamaktan yoksun olması, Türk Ceza Kanununda yer verilen kavramların özel bir kanunla açıklanma gereksinimi gibi sebeplerle, kanun seviyesinde bir düzenleme ihtiyacı belirginleşmiştir. Öte yandan, uluslararası düzenlemelerle uyumun sağlanmasının yanında, toplumun gereksinimleri de bir düzenleme ihtiyacını zorunlu kılmıştır[129]. Gerçekten, en son TUİK verilerine[130] göre, bilişim teknolojisi bulunmayan hanelerin %3,5 olduğu düşünüldüğünde veri paylaşım oranının ve bu doğrultuda ihlâllerin yüksek olması da kaçınılmazdır. Tüm bu sebeplerle, 2016 yılında Kişisel Verilerin Korunması Kanunu kabul edilmiştir.

B. 6698 sayılı Kişisel Verilerin Korunması Kanunu

Kişisel verilerin korunması alanında uluslararası düzenlemeler, uygulamalar ve çağın getirisi olan ihtiyaçlar göz önüne alarak, iç hukukta kapsamlı bir düzenleme ihtiyacı doğmuştur. Bunun üzerine, kişisel verilerin işlenmesinde, kişilerin temel hak ve hürriyetlerini korumak amacıyla 23 Mart 2016 tarihinde 6698 sayılı Kişisel

---

129 Serpil **Karlıdağ,** Ekonomi Politik Açıdan Kişisel Verilerin Korunması, Amme İdaresi Dergisi, C. 46, S. 1, 2013, s. 146-147; Mehmet **Demir,** Kişiliğin Korunması ve Sağlık Bilişim(i) Hukuku Açılarından Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirilmesi, Prof. Dr. Ejder Yılmaz'a Armağan, C. 1, 2014, s. 747-748; Yener **Ünver,** Kişisel Verilerin Korunması, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, S. 1, 2008, 194; Yasemin **Durak,** İnternet Yoluyla Kişilik Haklarına Saldırı ve Hukukî Koruma, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 22, S. 1, 2014, s. 112, 121; **Zorlu,** s. 140.

130 2016 yılında yapılan araştırma sonuçlarına ulaşmak için bkz., www.tuik.gov.tr/HbGetir.do?id=21779&tb_id=3 (Erişim Tarihi: 12.9.2018).

Verilerin Korunması Kanunu kabul edilmiştir[131]. Kişisel Verilerin Korunması Kanunu, özellikle 1995/46 sayılı Yönerge ve 108 sayılı Sözleşme dikkate alınarak hazırlanmış, çerçeve niteliğine sahip bir metindir. Ancak, Genel Veri Koruma Tüzüğünün yürürlüğe girmesiyle birlikte, temel alınan düzenlemelerden biri olan 1995/46 sayılı Yönerge yürürlükten kalkmıştır.

Kanunun kapsam başlıklı 2 nci maddesine göre, *"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 veya tüzel kişiler"* hakkında bu Kanun hükümleri uygulanır. Hükmün açık ifadesinden yola çıkarak, kişisel verileri işlenen gerçek kişiler herhangi bir ek şart aranmaksızın bu Kanun kapsamında değerlendirilmelidir. Veri sorumluları (ve veri işleyenler) açısından ise bir sınırlama getirilmiştir. Kısmen veya tamamen otomatik yollarla ya da veri kayıt sistemine otomatik olmayan yollarla hem kamu sektöründe hem de özel sektörde[132] veri işleyen gerçek veya tüzel kişiler hakkında bu Kanun hükümleri uygulanacaktır[133].

Ayrıca, uygulama alanı dışında tutulan hâller KVKK.m.28 hükmünde istisnalar başlığıyla düzenlenmiştir. Hükmün, birinci fıkrada öngörülen hâller, Kanunun tamamen uygulama alanı dışında tutulurken, ikinci fıkrada öngörülen hâller ise, Kanunun kısmen uygulama alanı dışında tutulmuştur. Birinci fıkrada istisna tutulan ilk hâl, bir gerçek kişinin, tamamen kendisi veya aynı konutta yaşayan aile fertleriyle ilgili kişisel verileri işlemesidir. Bu yolla, maddî, manevî veya iktisadî değerlere yönelik değerlerin işlenmesi mümkündür[134]. Ancak, bunun için, işleyen kişinin veri güvenliğini sağlaması ve kişisel verileri üçüncü kişilerle paylaşmaması gerekir. Bu

---

131 Ülkemizde KVKK'dan başka kişisel veriye ilişkin hükümler içeren farklı kanunlar da bulunmaktadır. Banka Kartları ve Kredi Kartları Kanunu m. 23, Kan ve Kan Ürünleri Kanunu m. 3, Elektronik Haberleşme Kanunu m. 51, 55, 56, Bilgi Edinme Hakkı Kanunu m. 21, Elektronik İmza Kanunu m. 12, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun m. 10, Nüfus Hizmetleri Kanunu m. 45, Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun m. 35, Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun m. 23 bahsi geçen düzenlemelere örnek olarak sayılabilir.

132 İbrahim **Korkmaz,** Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, Türkiye Barolar Birliği Dergisi, S. 124, 2016, s. 88.

133 Hükmün aksi yöndeki ifadesinden, herhangi bir veri kayıt sisteminin parçası olmaksızın otomatik olmayan yollarla veri işleme faaliyetlerinin Kanunun kapsamına girmediği söylenebilir.

134 **Çekin,** Kişisel Veri, s. 26, 27.

durumda, bir babanın çocuklarının eğitim durumuna ilişkin bilgileri, not durum belgelerini ve bunlara ilişkin tuttuğu kayıtları övünmek amacıyla sosyal platformlarından paylaşmasında kişisel veri işleme söz konusu olabilir. İkinci olarak, kişisel verilerin resmî istatistik amacıyla işlenmesi ile anonim hâle getirilmek suretiyle araştırma planlama ve istatistik gibi amaçlarla işlenmesinde de Kanun hükümleri uygulanmayacaktır.

Kişisel Verilerin Korunması Kanununun 28 inci maddesinin birinci fıkrasında öngörülen bir diğer hâl, kişisel verilerin *"milli savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlâl etmemek ya da suç teşkil etmemek kaydıyla, sanat tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi"*dir. Bu hâlde, veri işlemenin ihlâl niteliği taşıyıp taşımadığına veya suç oluşturup oluşturmadığına ilişkin değerlendirme her somut olay çerçevesinde hâkim tarafından yapılmalıdır[135]. Yine, kişisel verilerin *"milli savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi"* hâlinde de Kanun uygulama alanı bulmayacaktır. Son olarak, *"kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi"* hâlinde Kanun hükümleri uygulanmayacaktır.

Hükmün ikinci fıkrasına göre, Kişisel Verilerin Korunması Kanunun 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri, fıkrada dört bent hâlinde düzenlenen durumlarda uygulanmayacaktır. Öngörülen bu durumlarda veri güvenliğini sağlama yükümlülüğü devam eder. Ayrıca, kişisel verilerin hukuka aykırı olarak işlenmesi sebebiyle ortaya çıkan zararın giderilmesi talep edilebilecektir. Hükümde öngörülen durumlar, *"Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması, ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi, kişisel veri işlemenin*

---

[135] *Çekin'e* göre, burada bir menfaat dengesi kurulmalı ve çatışan iki farklı değerin ölçülülük ilkesine göre makul bir dengeye oturtulması gerekir. Bkz., **Çekin,** Kişisel Veri, s. 27, 13, 14.

*kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması ve kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak devletin ekonomik ve mali çıkarlarının korunması için gerekli olması"*ndan ibarettir (KVKK.28/II). Öte yandan, ikinci fıkrada öngörülen bu durumlarda veri işleme, Kanunun amacına, temel ilkelerine uygun ve orantılı olmalıdır. Aksi takdirde, kişisel verilerin işlendiği bu durumlarda da aydınlatma yükümlülüğü ve Veri Sorumluları Siciline kayıt yükümlülüğü devam edecek, ilgili kişi de 11 inci maddede öngörülen haklarını kullanabilecektir.

Kişisel Verilerin Korunması Kanununun geçici 1 inci maddesinde, Kanununun yürürlüğe girmesinden önce işlenen kişisel verilerin, işleme faaliyetinin ve işlemeye verilen rızaların akıbeti belirlenmiştir. Buna göre, Kanunun yayımından önce işlenmiş veriler yayım tarihinden itibaren iki yıl içerisinde uygun hâle getirilmelidir. Kanun hükümlerine aykırı olarak işlendiği tespit edilen veriler ise, derhâl silinmeli, yok edilmeli veya anonim hâle getirilmelidir. Kanunun yayım tarihinden önce kişisel verilerin işlenmesi için hukuka uygun şekilde açıklanmış rızalar, bir yıl içerisinde aksine irade açıklamasında bulunulmazsa geçerli sayılacaktır.

Kişisel Verilerin Korunması Kanununu takiben, Kurum tarafından 31 inci maddeye istinaden birçok yönetmelik[136] çıkarılmış ve 25 inci maddeye istinaden birçok karar[137] alınmıştır. Böylece, çerçeve niteliğine sahip kanunun uygulanması amacıyla adımlar atıldığı söylenebilir.

---

136 Bkz., Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik, Veri Sorumluları Sicili Hakkında Yönetmelik Kişisel Verileri Koruma Uzmanlığı Yönetmeliği, Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği, Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Ünvan Değişikliği Yönetmeliği, Kişisel Verileri Koruma Kurumu Disiplin Amirleri Yönetmeliği.

137 Söz konusu kararlara ilgili konu başlıkları altında değinilecektir. Yayınlanan kararlara ulaşmak için bkz., https://kvkk.gov.tr/Icerik/5419/Kurul-Kararlari?&page=2 (Erişim Tarihi: 17.3.2019).

§ 3. KİŞİSEL VERİLERİN KORUNMASINI TALEP ETME HAKKININ HUKUKÎ NİTELİĞİ

I. GENEL OLARAK

Kişisel verilerin korunması, kişiyi belirli veya belirlenebilir kılan bilgilerin korunmasını ifade eder. Söz konusu korumanın ayrıntılarına değinmeden önce, temelinde yer alan hakkın niteliğinin belirlenmesi gerekir. Öğretide, kişisel verilerin temelinde yer alan hakkın *mülkiyet hakkı*, *fikri mülkiyet hakkı* ve *kişilik hakkı* olduğuna dair görüşler ileri sürülmüştür[138].

Mülkiyet hakkı olduğuna dair görüş[139], özellikle Amerikan hukukunda kabul görmektedir. Bu görüşe göre, kişisel veriler, kişinin şahısvarlığı değerlerinin yanında malvarlığının da konusunu oluşturur. Buradan yola çıkarak, her ilgili kişi, kendisine ilişkin kişisel verilerin mülkiyet hakkını elinde bulundurduğu için mülkiyet hakkının sağladığı yetkileri kullanabilmelidir. Mülkiyet hakkının, hak sahibine sağladığı kullanma, yararlanma ve tasarruf etme yetkilerini kişisel veriler üzerinde kullanmasını ifade eder. Günümüzde, bilgiye sahip olanın elde ettiği güç düşünüldüğünde, teşebbüsler bu tür yollarla verilerin elde edilmesini amaçlayabilir. Teşebbüsler bu yolla pazarlama stratejileri belirlenmekte ve hatta kişisel verileri tekrar satarak gelir elde etmektedir[140]. Fikri mülkiyet hakkı olduğunu savunan görüşe[141] göre ise, kişisel verilerin korunması, fikri mülkiyet hakkına konu değerlerin

---

138 Görüşlerle ilgili ayrıntılı bilgi için bkz. **Aksoy,** Veri, s. 57-61; **Küzeci,** Kişisel Veri, s. 64-68.

139 Jerry **Kang**, Information Privacy in Cyberspace Transaction, Stanford Law Rewiew, C. 50, 1998, s. 1256-1257; Jessica **Litman,** Information Privacy / Information Property, Stanford Law Rewiew, C. 52, 2000, s. 1283. Yapılan bir araştırmaya göre, sosyal medya hesabına, banka hesabına ilişkin veya sağlık kayıtlarına ilişkin bilgilerin belirli miktarlar karşılığında satılması mümkün. Her bir veri için öngörülen miktarlara ulaşmak için bkz., https://www.fortinet.com/blog/industry-trends/the-true-value-of-data.html (Erişim Tarihi: 25.2.2019). Bir başka şirket ise, günlük internet geçmişi, fare imleci hareketine ilişkin kayıt ve konum bilgisi karşılığında en az 5 Dolar ödemeyi teklif ediyor. Bkz., https://www.kickstarter.com/projects/1461902402/a-bit-e-of-me (Erişim Tarihi: 26.2.2019).

140 M. Paul **Schwartz,** Property, Privacy and Personal Data, Harward Law Rewiew, C. 117, 2004, s. 2056. Türkiye açısından, kişilerin promosyon, taksit gibi olanaklardan faydalanmak amacıyla katıldıkları bir kart organizasyonunun, krizden etkilenmeyerek 2002 yılında 75 milyon Dolara satılması bu durumun en çarpıcı örneklerindendir. Bkz., **Karlıdağ,** s. 142-143.

141 Corien **Prins**, When Personal Data, Behaviour and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?, Script-ed, C. 3, S. 4, 2006, s. 279 vd.

korunmasıyla benzer nitelik taşır. Diğer bir deyişle, her ikisinde de bilgi üzerindeki kontrolün nasıl sağlanacağı, nasıl sınırlandırılacağı hususları düzenlenir.

Her iki görüş, öğretide eleştirilere maruz kalmıştır. Öncelikle, mülkiyet hakkı, malike, eşya üzerinde kullanabileceği bazı yetkiler tanır. Mülkiyet hakkının iç muhtevası olarak adlandırılan yetkiler, malike kullanma, yararlanma ve tasarruf etme yetkisi sağlar. Mülkiyet hakkının dış muhtevası ise, üçüncü kişilerin haksız saldırılarına karşı eşyayı koruma yetkisi verir[142]. Mülkiyet hakkının malike sağladığı tasarruf yetkisi, kişisel veriler açısından öngörülemez. Zira, kişisel verilerin üzerinde tasarruf edilebileceğinin kabulü, kişisel verinin ilişkin olduğu kişinin rızası aranmaksızın üçüncü bir kişiye satışı sonucunu da doğurur[143]. Bu sonuç ise kişisel veri ile ilgili kişi arasındaki bağlantıyı ortadan kaldırır[144]. Fikri mülkiyet hakkına yöneltilen eleştiriler ise, irade unsuruna dayanmaktadır. Buna göre, fikri mülkiyet hakkının konusunu oluşturan değerler, kişinin iradî olarak sarf ettiği çabanın bir ürünü olarak ortaya çıkar. Kişisel veriler ise, kişi olmanın veya toplum içinde yaşamanın doğal sonucu olarak ortaya çıkar[145].

Kişisel verilerin ilk defa gündeme geldiği Nüfus Sayımı Kanununa ilişkin karardan itibaren ileri sürülen diğer bir görüş ise, kişisel verilerin temelde kişilik hakkı olduğuna dair görüştür[146]. Bu görüşe ilişkin açıklamalara geçmeden önce, kişilik hakkına ilişkin açıklamalara yer verilecek ve kişisel veriler ile ilişkisi değerlendirilecektir.

II. KİŞİLİK HAKKI KAPSAMINDA KİŞİSEL VERİLER

Hukukumuzda kişilik hakkını (ve korunmasını) düzenleyen hükümlerde (MK.m.23-25), kişilik hakkına ilişkin herhangi bir tanıma yer verilmemiştir. Öğretide ise, farklı şekillerde tanımlanmıştır[147]. Genel olarak, kişilik hakkı, *"kişinin,*

---

142 Mehmet **Ayan**, Eşya Hukuku, C. 2, Mülkiyet, 9. Baskı, Ankara 2016, s. 64.
143 **Prins,** s. 293.
144 **Aksoy,** Veri, s. 64, 65.
145 **Prins,** s. 6.
146 **Küzeci,** Kişisel Veri, s. 70.
147 *Dural / Öğüz'e* göre, "kişinin toplum içindeki saygınlığını ve kişiliğini serbestçe geliştirmesini temin eden varlıkların tümü üzerindeki hakkı" ifade eder. Bkz., **Dural / Öğüz,** C. 2, s. 100; *Serozan'a* göre, "insanı insan yapan, kişinin kişiliğini oluşturan korunası tüm soylu değerlere

kişisel değerleri üzerinde sahip olduğu mutlak ve tekelci haktır"[148] şeklinde tanımlanabilir. Kişilik hakkının kapsamında birçok kişisel değerden bahsedilebilir. Ancak, bu durumda, kişisel değer sayısınca kişilik hakkından bahsedilemez[149]. Bir diğer söyleyişle, kişilik hakkı kapsamında sayılan kişisel değerler, genel nitelikteki kişilik hakkının yansımasıdır[150]. Sağ ve tam doğan herkes, ek bir şart aranmaksızın kişilik hakkını kazanır[151].

Kişilik hakkını diğer haklardan ayıran ilk özellik, mutlak nitelik taşımasıdır. Bir diğer deyişle, kişilik hakkı, herkese karşı ileri sürülebilir. Aynı zamanda, herkesin bu hakkı ihlâl etmeme, ona saygı gösterme yükümlülüğü vardır[152]. Kişilik hakkının diğer bir özelliği ise, şahısvarlığı haklarına dâhil olmasıdır[153]. Bu sebeple, kişilik hakkının değeri para ile ölçülemez. Kişilik hakkından tümüyle vazgeçilmesi veya devredilmesi mümkün değildir. Bu sebeple, kişiye sıkı şekilde bağlı haklardandır. Kişiliğin sona ermesiyle ortadan kalkacak bu hakkın mirasçılara geçmesi de mümkün değildir[154].

Kişilik hakkının konusunu oluşturan değerlere Medenî Kanunda yer verilmemiştir. Öğretide, bu yaklaşımın isabetli olduğu ifade edilmektedir. Zira, kişilik hakkının konusunu oluşturan değerler, sınırlı sayı ilkesine tabi değildir[155]. Kişisel değerlerin niteliğinden yola çıkılarak, maddî bütünlüğe ilişkin değerler, manevî bütünlüğe ilişkin değerler ve iktisadî bütünlüğe ilişkin değerler şeklinde bir

---

ilişkin hakkı" ifade eder. Bkz., **Serozan,** s. 454; *Akipek / Akıntürk / Ateş'e* göre, "kişinin hak süjesi olarak herkes tarafından tanınmasını istemek ve bu sıfatla itibar görmek konusundaki menfaat ve yetkileri anlamına da gelir". bkz., **Akipek / Akıntürk / Ateş**, s. 341, 342.

148 Aydın **Zevkliler** / M. Acabey **Acabey** / K. Emre **Gökyayla,** Medenî Hukuk, Giriş, Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku, 5. Baskı, İzmir 1997, s. 445.

149 **Dural / Öğüz,** C. 2, s. 101; **Akipek / Akıntürk / Ateş**, s. 343.

150 M. Kemal **Oğuzman** / Özer **Seliçi** / Saibe **Oktay -Özdemir**, Kişiler Hukuku, (Gerçek ve Tüzel Kişiler), 14. Baskı, İstanbul 2014, s. 155; **Ayan / Ayan**, Kişiler, s. 86.

151 **Ayan / Ayan,** Kişiler, s. 87; **Dural Öğüz,** C. 2, s. 103.

152 **Akipek / Akıntürk / Ateş**, s. 347; **Oğuzman / Seliçi / Oktay-Özdemir**, s. 155; **Ayan / Ayan**, Kişiler, s. 88.

153 **Oğuzman / Seliçi / Oktay-Özdemir**, s. 155.

154 **Dural Öğüz,** C. 2, s. 103; **Serozan,** s. 455; **Ayan / Ayan,** Kişiler, s. 88; **Oğuzman / Seliçi / Oktay-Özdemir,** s. 156. Kişisel veri niteliğindeki sosyal medya hesaplarının mirasçılara geçmesi gerektiği ile ilgili bkz., Nurten **İnce Akman,** Mirasbırakanın Dijital Bilgilerinin Mirasçılara Geçişi (Dijital Tereke), İnönü Üniversitesi Hukuk Fakültesi Dergisi, C. 9, S. 2, 2018, s. 557.

155 **Serozan**, s. 455; **Ayan / Ayan**, Kişiler, s. 90; **Oğuzman / Seliçi / Oktay-Özdemir**, s. 157.

ayrım benimsenebilir[156]. Bu durumda, hayat, beden tamlığı, sağlık gibi değerler maddî bütünlüğe ilişkin değerleri; ehliyetler, özgürlükler, şeref ve haysiyet, ad, resim, sır çevresi gibi değerler manevi bütünlüğe ilişkin değerleri, iktisadî hürriyet ve varlık, meslekî şeref ve haysiyet, meslekî ve ticarî sır ise, iktisadî bütünlüğe ilişkin değerleri ifade eder. Bu değerler içerisinde, kişisel verilerin işlenmesi açısından önem arz eden özel hayat veya özel hayata ilişkin sır çevresi olarak ifade edilen kavram ayrıca açıklanacaktır.

Özel hayat, insanın yakınları ile birlikte yaşadığı ve onlarla paylaştığı hayat alanı olarak tanımlanabilir[157]. Kişinin yaşadığı bu hayat alanı içerisinde, diğer kişilerle paylaştığı olayların açıklanması, hukuka aykırı nitelik taşımaz. Öte yandan, diğer kişilerle paylaşmadığı olayların bilinmesi, açıklanması kişilik hakkının ihlâli anlamına gelir[158]. Örneğin, kişiye ilişkin özel yazışmalar, ailevî sorunlar, banka hesap bilgileri bu kapsamda değerlendirilir.

Kişisel verilerin temelde bir kişilik hakkı olduğu görüşünü savunanlar, görüşlerini özel hayatın gizliliği kavramı çerçevesinde temellendirmektedir. Kişisel veri kavramı ile özel hayatın gizliliği kavramı, aralarındaki sıkı ilişkiye rağmen farklı kavramlardır[159]. Çalışma Grubu'na göre, özel hayatın gizliliğini ihlâl amacıyla açıklanmak istenen ve fakat gerçeği yansıtmayan bir veri, özel hayatın gizliliğini ihlâl etmez. Ancak, toplumda oluşan kanaat sebebiyle, ilgili kişi olumsuz etkilenebilir. Bu durumda, kişisel verilerin korunması hakkı çerçevesinde sorun çözümlenmeye çalışılmalıdır[160]. Nitekim, 1995/46 sayılı Yönergenin 1 inci maddesinde temel hak ve özgürlüklerin (özellikle özel hayat hakkının) korunması amaçlanmıştır. Bu durum da kişisel verilerin özel hayatın gizliliği kavramından daha geniş bir amaca hizmet ettiğini gösterir[161].

Kişisel verilerin kişilik hakkı olduğunu savunanlardan bir diğer grup, dayandırdıkları temel açısından diğerlerinden farklılaşmaktadır. Bu görüş

---

156 **Ayan / Ayan**, Kişiler, s. 91; **Akipek / Akıntürk / Ateş**, s. 346.
157 **Oğuzman / Seliçi / Oktay-Özdemir**, s. 178.
158 **Dural Öğüz,** C. 2, s. 135.
159 **Aksoy,** s. 62.
160 **Article 29 Data Protection Working Party**, 4/2007, s. 7; **Akdağ**, s. 12, 13.
161 **Aksoy,** Kişisel Veri, s. 62.

taraftarları[162], Nüfus Sayımı Kanununa ilişkin kararda da belirtildiği üzere kişisel verilerin, isabetli olarak, verilerin geleceğini belirleme hakkı *(Right of Informational Self-Determination)* ile ilişkilendirilmesi gerektiğini savunmaktadır. Bu hak, temelde, bireylerin kendileriyle ilgili verilerin işlenip işlenemeyeceği, kim tarafından ve hangi şartlar altında işleneceği ile ilgili karar verme yetkisi tanır[163]. Bu hak temelinde, özel hayatın gizliliği çerçevesinde korunması gereken veya kamusal alanda bulunan verilerin yanlış olup olmadığına bakılmaksızın korunması söz konusu olacaktır. Şüphesiz, bu hak ile birey kişisel veriler üzerinde sınırsız bir yetkiye sahip olmaz. Bu hakkın sınırlarının hukukî çerçevede Devlet tarafından belirlenmesi gerekecektir[164].

---

162 Paul **Schwartz**, The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, American Journal of Comparative Law, C. 37, S. 4. 1989, s. 687. Aynı yönde bkz., **Ayözger Öngün,** s. 18, 19.

163 **Schwartz,** Self-Determination, s. 689-690.

164 **Schwartz,** Self-Determination, s. 690.

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN İŞLENMESİ, AKTARILMASI, SİLİNMESİ, YOK EDİLMESİ VEYA ANONİM HÂLE GETİRİLMESİ İLE İLGİLİ KİŞİNİN HAKLARI VE VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

§ 4. KİŞİSEL VERİLERİN İŞLENMESİ

I. KİŞİSEL VERİLERİN İŞLENMESİ KAVRAMI VE KİŞİSEL VERİLERİN İŞLENMESİNE HÂKİM OLAN İLKELER

A. Kişisel Verilerin İşlenmesi Kavramı

Türk hukukunda veri koruma kurallarının yöneldiği temel amaç, kişisel verilerin işlenmesi karşısında temel hak ve hürriyetleri korumak, kişisel verileri işleyen kişilerin uyacakları usul ve esası belirlemektir (KVKK.m.1). Hâl böyle olunca, kişisel verilerin işlenmesi kavramının neyi ifade ettiğinin ve kapsamının ne olacağının belirlenmesi gerekir. Kişisel Verilerin Korunması Kanununa göre kişisel verilerin işlenmesi, *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi"* ifade eder.

Görüldüğü üzere, hükümde, birçok veri işleme türüne yer verilmiş ancak veri işleme faaliyeti bunlarla sınırlandırılmamıştır. Bu durumda, kişisel veriler üzerinde gerçekleştirilen her türlü işlemin Kişisel Verilerin Korunması Kanunu kapsamında değerlendirilmesi gerekir. Örneğin, kişiye gönderilen tebligata ulaşılarak ceza mahkûmiyetine ilişkin bilginin elde edilmesi, bu verinin ileride kullanılmak üzere kaydedilmesi, kişiye ilişkin siyasî parti üyeliğine ilişkin bilgi ile birleştirilmesi bu bilgilerin bir gazetedeki köşe yazısı üzerinden açıklanması gibi veri üzerindeki her bir işlem, kişisel verilerin işlenmesi niteliği taşır. Yine, kişinin mezuniyet bilgilerinin

yer aldığı sistemde bulunan verilerin kullanılmasının engellenmesi de kişisel verilerin işlenmesi olarak değerlendirilmelidir. Öte yandan, kişisel veriler üzerindeki her türlü işlemin kişisel veri olarak nitelendirilmesindeki tek sınır, veri işleme faaliyetinin *tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla* gerçekleştirilmiş olmasıdır[1]. Kişisel Verilerin Korunması Kanunu, otomatik olan veya otomatik olmayan yollara ilişkin dair bir tanıma veya açıklamaya yer vermemiştir.

Öğretiye göre, otomatik yollarla kişisel verilerin işlenmesinden, verilerin insan müdahalesi olmaksızın elektronik sistemler aracılığıyla işlenmesi anlaşılmalıdır. Kısmen otomatik yollarla işlemede ise, elektronik sistemlere ek olarak manüel bir işleme söz konusu olur[2]. Kişilerin plaka bilgisinin bir kişi aracılığıyla sisteme kaydedilmesi kısmen otomatik yollarla işlemeye, plaka okuyan kameralar aracılığıyla insan müdahalesi olmaksızın sisteme kaydedilmesi ise, tamamen otomatik yollarla veri işlemeye örnek verilebilir. Buradaki işlemeye aracı olan sistem bir kamera, bilgisayar, dron olabileceği gibi akıllı ev sistemi veya sürücüsüz olarak kullanılabilen bir araba da olabilir[3]. Kanunun açık ifadesi gereği, tamamen veya kısmen otomatik yollarla yapılan işlemeler uygulama alanı içerisindedir. Otomatik olmayan yollarla kişisel verilerin işlenmesi ise, bir veri kayıt sisteminin söz konusu olduğu hâllerde uygulama alanı içerisinde değerlendirilebilecektir. Veri kayıt sisteminin, verilerin belirli bir kritere göre yapılandırılarak işlendiği sistemi ifade ettiğine daha önce değinmiştik. Bu durumda, kişisel verilerin, örneğin, doğum yeri veya tarihi, borç bilgisi, kimlik numarası, eğitim durumu, dernek üyeliği veya belirli bir hastalığa sahip olma gibi belirlenmiş bir kritere göre manüel olarak işlenmesi de kişisel verilerin işlenmesi olarak değerlendirilir.

Genel Veri Koruma Tüzüğünde de benzer bir yaklaşıma yer verilmiştir. Tüzüğe göre, veri işleme, otomatik yöntemlerle olsun veya olmasın kişisel veri üzerinde gerçekleştirilen herhangi bir işlem veya işlem dizisidir. Kişisel veriler

---

1 Şüphesiz bu sınır, Kişisel Verilerin Korunması Kanunundan kaynaklanan bir sınırdır. Başka bir düzenlemede, otomatik olan veya olmayan yollarla veri üzerinde gerçekleştirilen her türlü işlem kişisel verilerin işlenmesi olarak nitelendirilebilir.

2 **Develioğlu,** s. 40, dn. 41; **Çekin,** Kişisel Veri, s. 22.

3 **Çekin,** Kişisel Veri, s. 22.

üzerinde gerçekleştirilen işleme faaliyetlerine örnek olarak toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletişim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi işlemler verilmiştir.

B. Kişisel Verilerin İşlenmesine Hâkim Olan İlkeler

1. Genel Olarak

Etkili veri koruma uygulamaları, kişisel verilerin işlenmesine hâkim olan ilkelere uyulmasıyla doğru orantılıdır. Bu sebeple, kişisel verilerin korunması amacıyla birçok uluslararası düzenlemede veri işleme ilkelerine yer verilmiştir. Güncel ve dönemin ihtiyaçlarını karşılamaya yönelik hükümlerin yer aldığı Genel Veri Koruma Tüzüğünde, "hukuka uygun olma, hakkaniyet ve şeffaflık", "amaç ile sınırlı olma", "veri minimizasyonu", "doğruluk", "sınırlı süre saklama", "bütünlük ve gizlilik" ve "sorumluluk" ilkelerine yer verilmiştir (m.5).

Kişisel Verilerin Korunması Kanununun 4 üncü maddesinde kişisel verilerin işlenmesine uyulması gereken genel ilkeler düzenlenmektedir. Buna göre, kişisel veriler işlenirken bu Kanunda ve diğer kanunlarda yer alan usul ve esaslara uyulmalıdır. Kanunda yer alan işleme ilkeleri ise, *"hukuka ve dürüstlük kurallarına uygun olma"*, *"doğru ve gerektiğinde güncel olma"*, *"belirli, açık ve meşru amaçlar için işlenme"*, *"işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma"* ve *"sınırlı süre muhafaza edilme"* ilkelerinden ibarettir.

2. Hukuka ve Dürüstlük Kurallarına Uygun Olma

Kişisel veriler üzerindeki işlemelerin hukuk kurallarına uygun olması kişisel verilerin korunmasına ilişkin temel ilkelerdendir. Kişisel veri üzerinde gerçekleştirilen her türlü faaliyetin Kişisel Verilerin Korunması Kanunu başta olmak üzere ilgili hukukî düzenlemelere uygun olmasını ifade eder[4]. Dürüstlük kurallarına uygun olma ise, Medenî Kanunun 2 nci maddesinden yola çıkarak, kişisel verilerin insanların makul beklentilerine uygun olarak ele alınmasını ve kişisel verilerin

---

4 **Küzeci**, s. 196.

işlenmesinin kötüye kullanılmaması gerektiğini ifade eder[5]. Bu durumda, kişisel verilerin elde edilmesinden başlayarak veri üzerinde gerçekleştirilen her türlü faaliyet bu ilkeye uygun olmalıdır[6]. Örneğin, kullanılacağı alan, tutulacağı süre veya aktarılması gibi hususlarda yanlış bilgilendirmeye dayanılarak kişisel veri elde edilmişse dürüstlük kuralına uygun davranılmadığından söz edilebilir.

Genel Veri Koruma Tüzüğünde, Kanunda yer alanlara ek olarak *şeffaflık* ilkesine yer verilmiştir. Şeffaflık ilkesi ise, kişisel verilerin işlenmesiyle ilgili her türlü bilgi ve iletişimin kolayca erişilebilir olmasını ve bu süreçte anlaşılır, net ve sade bir dil kullanılmasını ifade eder[7]. Söz konusu ilke, ilgili kişinin verinin nasıl ve kim tarafından elde edildiği, işlendiği ve kullanıldığı bilgilerine kolayca erişmesini sağlar[8]. Kişisel Verilerin Korunması Kanununda bu ilkeye yer verilmemiştir. Bununla birlikte, kişisel veri işleme süreçlerinin şeffaf olması ve veri sorumlusunun (veya veri işleyenin) bilgilendirme ve uyarı yükümlülüklerini yerine getirmesi, dürüstlük kurallarına uygun olmanın bir sonucu olarak görülebilir[9].

3. Doğru ve Gerektiğinde Güncel Olma

Kişisel verilerin doğru olması, özellikle ilgili kişinin çıkarlarını korumayı amaçlar. Veri sorumlusu, veri işleme ile hedefledikleri sonuçlara ulaşabilmek için verilerin doğru tutulmasını sağlamalıdır. Zira, kârı artırmak, müşterinin ilgi alanına uygun ürün temin etmek, satılan ürünlere ilişkin istatistikî bilgileri elde etmek gibi amaçlarla veri işleyen veri sorumlularının verilerin doğru tutulmasında çıkarı bulunmaktadır. Ayrıca, bilgilerin doğru olmasına ek olarak gerektiğinde güncel olması veri sorumlusunun yükümlülüğündedir. Güncellemenin *"gerektiğinde"* yapılması için, bilgi öznel nitelik taşımayan veya zamanla değişebilen özelliklere sahip olmalıdır[10]. Örneğin, taşıma şirketinde kayıtlı olan adrese teslim yapılabilmesi için onun güncel olması gerekir. Yine, bir çalışanın ücretinin zamanında ödenmesi

---

5 **Özdemir,** s. 138.
6 **Özdemir,** s. 136, 137.
7 **Develioğlu,** s. 44.
8 Genel Veri Koruma Tüzüğünün 39 uncu paragrafı.
9 **Keser Berber / Ülgü / Er**, s. 126; **Küzeci**, Kişisel Veri, s. 207.
10 Bkz., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/ (Erişim Tarihi: 15.9.2018).

için bordro bilgilerinin güncellenmesi gerekir. Söz konusu verilerin doğru veya güncel tutulmaması, veri işleyenden kaynaklanabileceği gibi teknik donanımdan da kaynaklanabilir[11]. Kanun, bu konuda herhangi bir ayrım yapmaksızın, gerçeği yansıtmayan verilerin doğru hâle getirilmesini veya eksik verilerin tamamlanmasını işlemede uyulacak genel ilkeler kapsamında saymıştır.

Verilerin doğru ve gerektiğinde güncel olup olmadığını en iyi şekilde değerlendirecek olan kişi veri öznesi olduğu için, veriye erişim hakkı ile söz konusu ilke arasında yakın bir ilişki bulunmaktadır[12]. Nitekim, Kanun, ilgili kişinin haklarını düzenleyen 11 nci madde ile bilgi edinme hakkına ek olarak, eksik veya yanlış bilgilerin düzeltilmesini talep etme hakkı ve kişisel verilerin silinmesini veya yok edilmesini talep etme hakkı tanımıştır.

Genel Veri Koruma Tüzüğünün 5 inci maddesinde doğruluk ilkesi olarak adlandırılan benzer bir yaklaşım benimsenmiştir. Kanuna ek olarak, yanlış tutulan bilgilerin gecikmeksizin düzeltilmesi veya silinmesi ilke kapsamında değerlendirilmiştir[13]. Örneğin, hastalık yanlış teşhis edilmiş ve bu yönde tedavi uygulanmışsa, bu bilgilerin silinmeyip doğru tedaviye ilişkin bilgilerle düzeltilmesi gerekir. Böylece, yanlış tedavinin sebep olduğu etkilerin gözlemlenmesi ve teşhisi sağlanabilir.

4. Belirli, Açık ve Meşru Amaçlar İçin İşlenme

Kişisel verilerin elde edilmesiyle başlayan sürecin tamamında amacın belirli, açık ve meşru olması gerekir. Buna göre, amaç belirlenirken belirsiz ve birbiri ile ilgisi olmayan genel ifadelerden kaçınılmalıdır[14]. Bu ilke, amaç belirlenmeksizin *"bir gün gerekli olur"* düşüncesi ile hareket edilerek bütün verilerin işlenmesini engeller[15]. Ayrıca, belirlenmiş olan açık amacın meşru olması gerekir. Buna göre,

---

11 **Özdemir,** s. 139.

12 **Küzeci**, Kişisel Veri, s. 220.

13 Ayrıca, Genel Veri Koruma Tüzüğünün 16 ncı ve 17 nci maddelerinde de ilgili kişiye düzeltme hakkı ve unutulma (silme) hakkı tanınmıştır.

14 **Başalp,** Veri, s. 38.

15 **Küzeci**, Kişisel Veri, s. 209; **Başalp,** Veri, s. 38. **Özdemir,** . 142. Verilerin anonimleştirilmeksizin olası kullanımları düşünerek depolamak da bu ilkenin ihlali anlamına gelir. Bkz., **Keser Berber / Ülgü / Er**, s. 126.

kanunî bir temele dayalı olarak belirlenen amaç ile işlemeden kaynaklanan çıkar arasında uygun bir denge bulunması gerekir[16]. Belirli, açık amacın kapsamını aşarak işleme yapılması, alınan rızanın veya öngörülen hukuka uygunluk sebebinin geçersizliği sonucunu doğurabilir[17]. Örneğin, kişinin gelişiminin takip edilmesi amacıyla eğitim bilgilerinin işlenmesi için alınan rızaya dayanılarak eğitim görmek için kaldığı yere ilişkin bilgiler işlenemeyecektir.

Genel Veri Koruma Tüzüğü ile belirli, açık, meşru amaçlara yönelik olarak işlemenin gerçekleştirileceği, bu amaçlara uygun olmayan bir şekilde işlenemeyeceği belirtilmiştir (m.5/1-b). Devamında ise, üç kategorideki amaçların başlangıçta belirlenen amaç ile uyumlu amaçlardan kabul edileceği ifade edilmiştir. Buna göre, kamu yararına arşivleme amaçları, bilimsel ve tarihî araştırma amaçları ve istatistiksel amaçlar *uyumlu amaçlardan* kabul edilirler[18]. Bu kategoriler dışındaki işleme amaçlarının uyumlu amaçlardan sayılıp sayılmayacağının ayrıca değerlendirilmesi gerekir. GVKT.m.6/f.4 e göre yapılan bu değerlendirmede, asıl amaç ile yeni amaç arasında bir bağlantı bulunması, yeni işleme amacı ilgili kişinin makul beklentisiyle uyuşması, yeni işlemlerin bireyler için olası etkileri ve şifreleme veya takma ad kullanımı gibi yöntemlerle uygun korumanın sağlanması gibi hususlar dikkate alınır[19]. Uyumlu amaç olduğu sonucuna ulaşılırsa, işleme yapılabilir. Ancak, yeni amacın asıl amaç ile uyumlu olmadığı sonucuna ulaşılıyorsa, ilgili kişinin verilerini yeni amaca uygun olarak işlemek için rızasının alınması gerekir (GVKT.m.6/4)[20]. Örneğin, güvenlik amacıyla giriş katını gösteren kapalı devre televizyon sistemi kurulmuş olan bir otelde, resepsiyon görevlisinin görevini gereği gibi yerine getirip getirmediğinin izlenmesi asıl amaç ile bağdaşmaz. Yine,

---

16 **Küzeci**, Kişisel Veri, s. 209. Buna karşılık, Kişisel Verilerin Korunması Kanununun 4 üncü maddesinin gerekçesinde amacın meşru olması, veri sorumlusunun yaptığı iş veya sunmuş olduğu hizmetle bağlantılı ve söz konusu iş veya hizmet için gerekli olması şeklinde ifade edilmiştir.

17 **Özdemir,** 142; **Zorlu,** s. 74.

18 Genel Veri Koruma Tüzüğünün 89 uncu maddesinin birinci fıkrası gereği, uyumlu amaçlardan kabul edilen bu kategoriler doğrultusunda işleme faaliyeti, veri sahibinin hakları ve özgürleri açısından uygun güvenlik önlemlerinin alınmasını gerektirir. Veri minimizasyonu ilkesi başta olmak üzere, takma ad kullanımı veya ilgili kişinin kimlik bilgilerinin saptanmasına imkân vermeyen yöntemlerle gerekli tedbirler alınmalıdır.

19 Ayrıca bkz., Genel Veri Koruma Tüzüğünün 50 nci paragrafı.

20 Aynı yönde bkz., **Özdemir,** s. 141.

sığınmacıların Avrupa Birliğine üye olan birden fazla devlete aynı anda sığınma başvurusunda bulunmalarını önlemek amacıyla kurulan ve sığınmacıların parmak izlerinin bulunduğu EURODAC isimli veri tabanının kolluk kuvvetlerinin erişimine açılması, asıl amaç ile uyumlu değildir[21].

5. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Kişisel verilerin işlenmesinde esas alınacak bir diğer ilkeye göre, işleme, amaçla bağlantılı, sınırlı ve ölçülü olarak gerçekleştirilmelidir. Buna göre, öncelikle, işlemin amacı başka yollarla makul bir şekilde yerine getirilemezse kişisel veriler işlenmelidir[22]. Amacı gerçekleştirmek için işleme gerekliyse, belirlenen amaçların gerçekleştirilmesi için elverişli olan verileri işlemek, amacın gerçekleştirilmesine herhangi bir katkısı olmayan verileri ise işlemekten kaçınmak gerekir. Örneğin, üremeye yardımcı tedavilerde bulunan bir merkezin, kişilerin ad soyad, yaş veya ilgili sağlık bilgilerini işlemeleri mümkündür. Ancak, bu tedavilere başvuran kişilerin meslek bilgisinin işlenmesi, asıl amaç ile bağdaşmayacaktır[23].

Genel Veri Koruma Tüzüğünde veri minimizasyonu olarak ifade edilen bu ilke kapsamında yeterli, yerinde ve gerekli bilgilerin işlenmesi gerekir. Diğer bir söyleyişle, işleme gerekliyse, asgarî miktarda veri kullanılarak yapılmalıdır[24]. Söz konusu minimizasyon, amaçla bağlantılı olan minimum düzeyde veri işlemeyi ve işlenen verilerin kapsamının sınırlı olmasını ifade eder. Örneğin, iş veya burs başvuru formlarında amaç ile bağlantısı bulunmayan bilgilerin talep edilmemesi gerekir. Talep edilen bilgiler ise, amacı gerçekleştirecek seviyede tutularak amaçla bağlantısı olmayan ayrıntıları içermemelidir. Söz konusu örnekte, kişiye, kaç kardeşi

---

21 **Article 29 Data Protection Working Party**, Opinion 03/2013 on Purpose Limitation, WP 203, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (Erişim Tarihi: 16.9.2019), s. 68.

22 **Küzeci**, Kişisel Veri, s. 241; **European Data Protection Supervisor**, Opinion on The Data Protection Reform Package, bkz., https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf (Erişim Tarihi: 16.9.2018), kn. 114.

23 Emel **Badur,** Üremeye Yardımcı Tedavi Uygulamalarında Kişisel Verilerin Korunması, Evrensel Hukuk İlkeleri Işığında Türk Medenî Hukukunda Değişimler Sempozyumu, 10-11 Haziran 2016, Çankaya Üniversitesi Hukuk Fakültesi, 2016, s. 181. Burada, tedavi merkezi, meşru bir amaç doğrultusunda, örneğin, mesleklerin doğurganlığa etkisini tespit amacıyla ilgili kişilerin rızasını alarak meslek bilgisini işleyebilir.

24 **Kaya,** s. 324.

olduğunun, ikamet ettiği evin kendisine ait olup olmadığının sorulması ve bu verilerin işlenmesi amaç ile bağdaşmaz. Yahut, anne babasının hangi mesleği yaptıklarına dair sorular amacı gerçekleştirmek için gerekli değildir. Benzer şekilde, bir okula girişte kartlı geçiş kullanılabiliyorken, biyometrik yöntemlerle geçişin sağlanması amacı gerçekleştirmek için gereken veri işlemenin üzerinde olup ölçülü değildir.

6. Sınırlı Süre Muhafaza Edilme

Kişisel veriler diğer ilkelere uygun olarak işlense dahi ilgili kişiler açısından risk teşkil etmeye devam eder. Gerçekten, kişisel verilerin hukuka aykırı olarak uzun süre kullanımları, depolanmaları, kişinin maddî ve manevî bütünlüğü, özel yaşamın gizliliği gibi değerlerinin zarar görmesine yol açar[25]. Verilerin gerekenden uzun süre muhafazası, ilgili kişiler kadar veri sorumlular açısından da olumsuz sonuçlar doğurur. Gerçekten, her bir verinin depolaması, güvenliğinin sağlanması sebebiyle ortaya çıkan maliyet, bilgi edinme ve erişim hakkının kullanılması sebebiyle harcanan zaman, veri sorumlusunu olumsuz yönde etkiler. Bu yüzden, işlenen kişisel veriler, ilgili mevzuatta öngörülen veya işlendikleri amacın gerçekleştirilmesi için gerekli olan süre kadar muhafaza edilmelidir (KVKK.m.4/1-d). Mevzuatta öngörülen sürelere ek olarak, *"amacın gerçekleştirilmesi için gerekli olan"* sürenin belirlenmesinde veri sorumlusu rol oynayacaktır. Gerçekten, veri sorumlusunun her bir kişisel veri kategorilerinin muhafaza edileceği süreleri belirlemesi ve bunu saklama politikaları kapsamında ilgili kişinin erişimine sunması, bu ilkeye uygun davranmayı kolaylaştıracaktır[26]. Kaldı ki, VERBİS'e kayıt yükümlülüğü bulunan veri

---

25 Zira, kişiler, kendileriyle ilgili verilerin tutulduğu, depo edildiği, kullanıldığı hissiyle hareket edeceklerdir. Bu durum, ütopik bir sistemin ve mimarinin anlatıldığı Panoptikon kadar kabul edilemez niteliktedir. Panoptikon, temelde, mahkûmların disiplini ve eğitimi için öngörülmüş olan bir sistemdir. Bu sistemde, dairesel biçimde öngörülen hapishanenin ortasında bir kule bulunmaktadır ve kişilerin her hareketi izlenmektedir (Ancak, kulede birinin olup olmadığı dâhi bilinememektedir). Bu durumda, cezalandırılacaklarından korkan mahkûmların, kurallara uyduğu gözlemlenir. Panoptikon için bkz., Jeremy **Bentham** / Catherine **Pease - Watkin** / Simon **Werret**, Panoptikon, Gözün İktidarı, (Çev. Barış Çoban / Zeynep Özarslan), 2. Baskı, İstanbul 2016, s. 14 vd.. Bu sistem kadar katı kurallara tâbi olmamakla birlikte, günümüz dünyasında kişisel verilerin süresiz olarak bulundurulması, bireylerin özgürce hareket etme kabiliyetini sınırlandıracak ve bilgiyi elinde tutan kişilerin veya kurumların çizdiği sınırlar içinde hareket etmesine sebep olacaktır.

26 **Küzeci**, Kişisel Veri, s. 222.

sorumlularının *"veri saklama ve imha politikası"* hazırlama yükümlülüğü bulunmaktadır[27]. Veri saklama ve imha politikası hazırlama yükümlülüğü altında olmayan veri sorumluları ise, kişisel verinin işlemeye ilişkin her aşamasında bu ilkeyi göz önüne almalıdır.

Kişisel veriler, mevzuatta belirlenen süreler geçtikten veya amaç gerçekleştikten sonra, olası kullanımlar düşünülerek saklanamaz[28]. Kişisel verinin işlenmesini gerektiren sebepler ortadan kalkmışsa kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir (KVKK.m.7). Genel Veri Koruma Tüzüğünde de bu ilkeye yer verilmiştir (GVKT.m.5/1-e). Ayrıca, Tüzükte, kamu yararına arşivleme amaçları, bilimsel veya tarihî araştırma amaçları ve istatistiksel amaçlar ile yapılan işlemelerin daha uzun süreler boyunca saklanabilmesine imkân tanınmıştır. Bu durumda, GVKT m.89/1 hükmünde yer verilen güvencelere uyulması gerekir.

II. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI[29]

Günümüzde, özellikle bilişim sistemleri aracılığıyla işlenen kişisel veriler sebebiyle, başta özel hayatın gizliliği olmak üzere, temel hak ve hürriyetlerin ihlali ile karşı karşıya kalınmaktadır. Bu sebeple, kişisel verilerin işlenememesi asıldır. Bununla birlikte, gerek özel sektör gerek kamu sektörü tarafından kişilere mal veya hizmet sunulması gibi sebeplerle kişisel verilerin işlenmesi gerekebilir. Genel Veri Koruma Tüzüğünün 4 üncü paragrafında bu durum şu şekilde özetlenmiştir: *"Kişisel verilerin işlenmesi, insanlığa hizmet edecek şekilde tasarlanmalıdır. Kişisel verilerin korunması hakkı mutlak bir hak değildir; toplumdaki işleviyle ilişkili olarak düşünülmeli ve orantılılık ilkesine uygun olarak diğer temel haklara karşı dengeli olmalıdır"*. Kişisel Verilerin Korunması Kanunun 4 üncü maddesi de, verilerin

---

27 Bkz., Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik m.5/1.

28 **Korkmaz**, s. 104.

29 Kişisel Verilerin Koruması Kanununda kişisel verilerin işlenebileceği hâller, *kişisel verilerin işlenme şartları* başlığında ele alınmıştır. Öğretide ise, bu hâller, kişisel verilerin işlenmesinde hukuka uygunluk sebepleri olarak değerlendirilmiştir. Bkz., **Özdemir,** s. 165; **Develioğlu,** s. 51; .Kişisel verilerin işlenebileceği hâllerde, kişisel verilerin işlenmesinde esas alınan genel ilkelere uygun davranma yükümlülüğü devam eder. Bir diğer deyişle, bu hâller tek başına hukuka aykırılığı ortadan kaldırmaz. Bu sebeple, çalışmamızda, kişisel verilerin işlenmesi başlığında, genel nitelikli ve özel nitelikli kişisel verilerin işlenme şartları başlığına yer verilmiştir.

işlenmesine ilişkin durumların istisnaî nitelik taşıması sebebiyle, kanunlarda yer alan usul ve esaslara göre işlenebileceğine hükmünde yer verilmiştir[30].

Kanunun 5 inci maddesinde kişisel verilerin işlenmesine ilişkin şartlar, 6 ncı maddede ise özel nitelikli kişisel verilerin işlenmesine ilişkin şartlar belirlenmiştir. Bu sebeple, kişisel verilerin işlenmesi, *genel nitelikli kişisel verilerin işlenmesi* ve *özel nitelikli kişisel verilerin işlenmesi* olarak iki başlıkta incelenmiştir. Kişisel veri üzerindeki her türlü faaliyet kişisel verilerin işlenmesi kapsamında değerlendirilmesine rağmen, *kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi* (m.7), *kişisel verilerin aktarılması* (m.8) ve *kişisel verilerin yurt dışına aktarılması* (m.9) ayrıca düzenlendiği için, bu faaliyetlere ilişkin şartlara farklı başlıklarda yer verilmiştir.

A. Genel Nitelikli Kişisel Verilerin İşlenmesi

1. Genel Olarak

Genel nitelikli kişisel veriler, kural olarak, *açık rıza* olmaksızın işlenemez. Ancak, Kanunun 5 inci maddesinin ikinci fıkrasında yer alan durumlardan birinin varlığı hâlinde, açık rıza olmaksızın kişisel verilerin işlenmesi mümkündür. Buna göre, *"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", "ilgili kişinin temel hak ve hürriyetlerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması"* hâlinde kişisel veriler işlenebilir. Kişisel Verilerin Korunması Kanunu açısından 5 inci maddede sayılanlar,

---

30 Anayasal bir hak olan kişisel verilerin işlenmesine ilişkin şartların da Anayasa ile belirlenmesi gerektiğine ilişkin görüş için bkz., Sultan **Tahmazoğlu Üzeltürk,** Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği, Legal Hukuk Dergisi, S. 93, 2010, s. 3155.

herhangi bir öncelik sonralık ilişkisi olmaksızın, kişisel verilerin işlenmesine ilişkin seçeneklerden ibarettir[31]. Anayasanın 20 nci maddesinde yer verilen *veya* ifadesi de bu sonucu doğrular niteliktedir. Veri işlemeye ilişkin hangi yol tercih edilirse edilsin, kişisel veri işleme ilkelerine uygun davranma yükümlülüğü devam etmektedir. Diğer bir söyleyişle, veri sorumlusu, KVKK.m.5 hükmünde sayılan hâllerde, veri işlemenin gerekli, orantılı, hukuka ve dürüstlük kurallarına uygun olup olmadığını dikkate almalıdır[32]. Ayrıca, kişisel verilerin işlenmesinde temel alınan sebebin geçersizliği, KVKK.m.10 hükmünde öngörülen aydınlatma yükümlülüğünün de geçersizliğini doğuracağı için, veri sorumlularının hukukî sebebe ilişkin belirlemeleri önem arz eder[33].

2. Kişisel Verilerin İşlenme Şartları

a.Açık Rıza

Kişisel verilerin işlenebilmesi, öncelikle ilgili kişinin açık rızasına bağlanmıştır. Bu durumda, kişisel verilerin işlenmesinde önemli bir yeri olan rızanın, neyi ifade ettiği ve hangi unsurları taşıması gerektiği belirlenmelidir.

1995/46 sayılı Yönergenin 2 inci maddesinin birinci fıkrasının h bendi ile aynı tanımı esas alan Kişisel Verilerin Korunması Kanununa göre açık rıza, *"belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızayı"* ifade eder (KVKK.m.3/1-a). Genel Veri Koruma Tüzüğüne göre ise, kişinin kişisel verilerinin işlenmesine onay verdiğini gösteren serbestçe verilen, belirli konu ile ilgili, bilgilendirilmiş ve belirsizlik içermeyen açıklamalardır. Tüzükte, bu açıklamanın, ilgili kişinin ifadesiyle, açık bir olumlu eylemiyle veya kişisel verilerin işlenmesini öngören anlaşmanın imzalanması suretiyle gerçekleştirilebileceği ifade edilmiştir (GVKT.m.4/XI). Düzenlemeler ışığında, açık rıza, *belirli bir konuya ilişkin kişisel verilerin işlenmesine müsaade edildiğini açıkça ortaya koyan,*

---

31 **Yücedağ,** s. 773. Bununla birlikte, açık rızanın diğer işleme şartları açısından bir ön şart olduğu yaklaşımını benimseyen ülkeler de bulunmaktadır. Bkz., **Article 29 Data Protection Working Party**, Definition of Consent, s. 7.

32 GVKT ise, rızanın koşullarını düzenlediği m.7/II hükmü ile rızanın Tüzüğü ihlal eden hiçbir kısmının bağlayıcı olmayacağını ifade etmiştir.

33 **Yücedağ,** s. 773.

bilgilendirilme sonucunda serbestçe verilmiş irade açıklamaları olarak tanımlanabilir[34].

aa. Açık Rızanın Unsurları

Kanunun 3 üncü maddesinde açık rızanın tanımı, belirli bir konuya ilişkin olma, aydınlatılmış olma ve özgür irade ile açıklanmış olma şeklinde üç temel unsurdan yola çıkarak yapılmıştır. Kanunun 5 inci maddesinin gerekçesinde ise, 1995/46 sayılı Yönergeye atıf yapılarak, rızanın tereddüde yer bırakmayacak açıklıkta olması gerektiği ifade edilmiştir. Bu sebeple, kişisel verilerin işlenmesini konu alan geçerli bir açık rızanın *belirli bir konuya ilişkin olma*, *aydınlatılmış olma*, *özgür irade ürünü olma* ve *belirsizliğe yer vermeyecek şekilde ifade edilmiş olma* unsurlarından oluştuğu söylenebilir[35].

aaa. Belirli Bir Konuya İlişkin Olma

Geçerli bir rıza, veri koruma ilkeleriyle[36] örtüşür şekilde belirli konuya ilişkin olarak verilmelidir. Bu sebeple, veri işlemeye ilişkin rıza alınmadan önce amacın belirli ve açık olması sağlanmalı, daha sonra, amaç doğrultusunda verilerin işlenmesi için rıza talep edilmelidir. Verilen rıza, amaç ile bağlantılı şekilde veri işlemeyi mümkün kılar. Ancak, amaç ile bağlantılı olmayan hususlardaki işlemeler için ayrıca rıza talebinde bulunulmalıdır[37]. Belirsiz içeriğe sahip olan veya genel nitelikteki rıza açıklamaları geçerli değildir[38]. Rıza gösterilecek belirli konunun içeriğine de değinmek gerekir. Medenî Kanunun 23 üncü maddesinden yola çıkarak, kişilik hakkını hukuka veya ahlaka aykırı olarak sınırlamayı konu alan kişisel veri işlemelerine gösterilen rıza geçersizdir. Bu durum, aynı zamanda veri koruma ilkelerinden olan hukuka ve dürüstlük kuralına uygun olma ilkesinin de ihlâli anlamına gelir.

---

34 **Develioğlu**, s. 52.

35 Çalışma Grubu ve Avrupa Birliği Veri Koruma Kurulu da geçerli bir rızanın bu dört unsuru barındırması gerektiğini ifade etmiştir. Bkz., **Article 29 Data Protection Working Party**, Guidelines on Consent, s. 5. Ayrıca bkz., **Atasoy,** s. 290 vd..

36 Özellikle belirli, açık amaçlarla işlenme ve işlendikleri amaçla bağlantılı, sınırlı olma ilkeleriyle rıza kavramı birlikte düşünülmelidir.

37 **Article 29 Data Protection Working Party**, Guidelines on Consent, s. 12.

38 **Özdemir,** s. 168; **Atasoy,** s. 292.

bbb. Aydınlatılmış Olma

Belirli konuya ilişkin rıza alınmadan önce, ilgili kişinin bilgilendirilmesi gerekir. Kişisel verilerin işlenmesinden önce bilgilendirme, ilgili kişilerin rıza gösterdikleri konuyu anlamalarını ve bu yönde bilinçli karar almalarını sağlar[39]. Bilgilendirmenin içeriğinin belirlenmesinde ise, Kanunun veri sorumlusunun aydınlatma yükümlülüğü başlığını taşıyan 10 uncu maddesi esas alınır. Buna göre, rıza talebinde, *"a) veri sorumlusunun ve varsa temsilcisinin kimliği, b) kişisel verilerin hangi amaçla işleneceği, c) işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, ç) kişisel veri toplamanın yöntemi ve hukukî sebebi, d) 11 inci maddede sayılan ilgili kişinin diğer hakları"* ile ilgili bilgiler yer almalıdır. Aydınlatma metninin içeriği somut olayın özelliklerine göre, 10 uncu maddede sayılanların dışına çıkmayı gerektirebilir[40]. Örneğin, verilerin hangi amaçla işlenebileceğine ilişkin bilgiler verilirken, pazarlama veya profil çıkarma *(profiling)* gibi amaçlarla kullanılıp kullanılmayacağı hususu önemle belirtilmelidir[41].

Aydınlatmanın şekline ilişkin Kanunda hüküm bulunmamaktadır. Çalışma Grubuna göre, aydınlatma, yazılı veya sözlü olarak yapılabileceği gibi, görüntülü veya sesli mesajlar yoluyla da iletilebilir[42]. Genel Veri Koruma Tüzüğünün rızanın koşullarını düzenleyen 7 nci maddesinin ikinci fıkrasına göre, ilgili kişinin rızasının yazılı olarak alınması gerekiyorsa, rıza talebi diğer hususlardan açıkça ayırt edilebilir, anlaşılır ve kolayla erişilebilir bir biçimde, açık ve sade bir dil kullanılarak sunulmalıdır. Söz konusu düzenlemeden ve Çalışma Grubuna ait görüşlerden yola çıkarak, aydınlatma görevini yerine getirecek kalitede kelimeleri, ortalama bir kişinin kolayca anlayabileceği şekilde bir araya getirerek aydınlatma metni hazırlanmalıdır. Aynı zamanda, bu bilgilendirmenin kişinin kolayca erişebileceği ve görebileceği

---

39 **Çekin,** Big Data, s. 640.

40 **Yücedağ,** s. 774.

41 **Atasoy,** s. 295. **Çekin,** Big Data, s. 641.

42 **Article 29 Data Protection Working Party**, Guidelines on Consent, s. 13. Çalışma Grubunu rızanın tanımına ilişkin açıklamalara yer verdiği görüşüne göre, aydınlatma metninde, bilginin kalitesi, veriliş şekli, erişilebilirliği ve görünürlüğü önem arz eder. Buna göre, anlaşılır şekilde aydınlatma görevini yerine getirebilecek bilgilerin kişiye sunulması gerekir. Bkz., **Article 29 Data Protection Working Party**, Definition of Consent, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (Erişim Tarihi: 8.9.2018), s. 20.

şekilde sunulması gerekir[43]. Bu sebeple, bilgilendirmede, küçük puntolarla yazılmış uzun paragraflar veya dikkat çekmeyen dipnotlar tercih edilmemelidir. Bunun yerine, bilgilendirmeye ayrı bir sayfa ayrılmalı veya diğer hususlardan ayırt edilebilir şekilde yer verilmelidir. Bilgilendirmeye ilişkin yükümlülüklerin ihlâli, rızayı geçersiz kılar. Rızanın geçersiz olması işlemenin geçersizliği sonucunu doğuracağı için, bu durumda hukuka aykırı işlemeye ilişkin hükümler uygulama alanı bulur.

ccc. Özgür İrade Ürünü Olma

Kişisel verilerin işlenmesine gösterilecek olan rıza, özgür iradeye dayanmalıdır. Özgür irade, iradeyi sakatlayan herhangi bir etki altında kalmaksızın alınan gönüllü kararları ifade eder. Bu sebeple, hile veya tehditle elde edilen rıza, kişisel verilerin işlenmesine imkân sağlamaz. Aynı şekilde, rıza verilmemesi hâlinde olumsuz bir sonuçla karşılaşma riski varsa, gerçek bir tercih söz konusu değildir.

Bir hizmetin alınması veya bir sözleşmenin kurulması gibi sebeplerle söz konusu husus ile ilgili olmayan veri işlemeye rıza gösterilmesi durumunda da gerçek bir iradeden bahsedilemez[44]. Bu durum, genellikle, veri sorumlusu ile eşit konumda yer almayan ilgili kişinin, bahsi geçen sebeplerle veri işlemeye rıza göstermek zorunda hissetmesi şeklinde gerçekleşir. Rıza gösterilmemesi hâlinde, ilgili kişi, hizmetten veya sözleşme ile kararlaştırılan ifadan mahrum kalabilmektedir[45]. Genel Veri Koruma Tüzüğü, bu durumun ortaya çıkaracağı mağduriyetleri gidermek amacıyla, söz konusu durumların serbest irade kapsamında değerlendirilmemesi noktasında azamî önem gösterilmesi gerektiğini belirtmiştir[46]. Tüzüğün 7 nci maddesinin dördüncü fıkrasında belirtilen bu durum *bağlama yasağı (prohibition of coupling or tying)* olarak ifade edilmektedir. Örneğin, sözleşme ile doğrudan ilgisi bulunmayan kişisel verilerin işlenmesine rıza gösterilmesi halinde sağlık sigortasına

---

43 **Ayözger Öngün**, s. 135.

44 Mesut Serdar **Çekin,** 6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestîsi Açısından Değerlendirilmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 74, S. 2, 2016, s. 637; **Yücedağ,** s. 775.

45 **Çekin,** Big Data, s. 637. Örneğin, Avrupalı havayollarının uçuştan önce verileri yetkililere göndermek zorunda kalması aksi hâlde uçuşun hiç veya zamanında gerçekleştirilememesi nedeniyle, uçmak isteyen yolcuların gerçek bir seçeneğine sahip olmadıkları ifade edilebilir. Bkz., **Article 29 Data Protection Working Party**, Opinion 15/2011 on the Definition of Consent, WP 187, s. 16.

46 Genel Veri Koruma Tüzüğü 43 üncü paragraf.

ilişkin sözleşmenin kurulacağını ifade eden sigorta şirketine verilen rıza, serbest irade ürünü olarak değerlendirilemez. Bir sözleşmenin ifası için gerekli olmayan veri işlemelerinde gösterilen rıza da aynı sonuca tâbidir.

Kişisel verilerin işlenmesine rıza göstermek, kişiye sıkı şekilde (münhasıran) bağlı hakların kullanılması niteliğinde olduğu için[47], ilgili kişinin özgür iradeyi açıklamaya ehil olup olmadığının belirlenmesi gerekir. Fiil ehliyetine göre kişilerden tam ehliyetliler ve sınırlı ehliyetliler, kendileriyle ilgili olan kişisel verilerin işlenmesine rıza gösterebilirler. Sınırlı ehliyetsizlerin durumu ise, ayrıca değerlendirilmelidir. Kişiye sıkı şekilde bağlı hakkın kullanılması niteliğindeki işlemler, kural olarak, sınırlı ehliyetsizlerin tek başlarına yapabilecekleri işlemlerdendir. Ancak, bu durumda, sınırlı ehliyetsizin çıkarlarının korunması amacıyla kanunî temsilcinin izninin aranması kabul edilmektedir[48]. Rıza kişisel verilerin işlenmesinden önce verilmesi gerektiği için, kanunî temsilci rızadan sonra verdiği izin (icazet) işlemi geçerli kılmaz[49]. Tam ehliyetsizler ise, kişisel verilerin işlenmesine rıza gösteremez[50].

ddd. Belirsizliğe Yer Vermeyecek Şekilde Açıkça İfade Edilmiş Olma

Türk hukukunda, hukuka aykırılığı ortadan kaldıracak olan rıza açıklaması, açık veya örtülü olabilir (TBK.m.1/II ve 63/II). Kişisel verilerin işlenmesi açısından, açık rıza beyanının bu unsuru karşılayacağına şüphe yoktur. Örtülü irade beyanını ise, ayrıca değerlendirmek gerekir. Kanundaki açık rıza tanımında yer almamakla birlikte, geçerli bir rıza belirsizliğe yer vermeyecek şekilde ve açıkça ifade edilmiş

---

47 Hüseyin Can **Aksoy,** Kişisel Verilerin İşlenmesi Kapsamında Rıza Unsuru ve Sınırlı Ehliyetsizlerin Durumu, Haluk Konuralp Anısına Armağan, C. 3, Ankara 2009, s. 57.

48 **Ayan / Ayan**, Kişiler, s. 119. *Aksoy'a* göre, ilgili kişinin sınırlı ehliyetsiz olması durumunda bir örtülü boşluktan söz edilir. Her ne kadar kişiye sıkı şekilde bağlı bir hakkın kullanılması söz konusuysa da, evlenme ve nişanlanmada olduğu gibi sınırlı ehliyetsizin rızasını tek başına açıklaması, onun maddî ve manevî zarara uğramasına sebep olabilecektir. Hâkim, sınırlı ehliyetsizin korunma gereğini de göz önüne alarak bu boşluğu doldurmalıdır. Ulaşılabilecek en uygun sonuç ise, sınırlı ehliyetsizin yasal temsilcisinin de rızasını alarak irade açıklamasında bulunmasıdır. Ayrıntılı açıklamalar için bkz., **Aksoy,** Rıza, s. 56 vd.. Ayrıca GVKT.m.8 hükmü de benzer bir sonuç öngörmektedir.

49 **Ayan / Ayan**, Kişiler, s. 119.

50 **Ayan / Ayan**, Kişiler, s. 118.

olmalıdır[51]. Örtülü irade beyanının bir türü olan susma, kural olarak, kabul niteliğinde bir irade beyanı olarak nitelendirilemez[52]. Genel Veri Koruma Tüzüğüne göre de, susma veya aktif davranışta bulunmama (eylemsizlik) gibi durumlar, kişisel verilerin işlenmesinde geçerli rızayı yansıtmaz[53]. Susma dışındaki örtülü irade beyanlarının, kişisel verilerin işlenmesinde açık rıza teşkil edip etmeyeceğini hususunda görüş birliği yoktur. Bir görüşe göre[54], belirsizliğe yer bırakmayacak şekilde ortaya konulan örtülü rıza, bu unsuru sağlar. İsabetli olan diğer görüşe göre[55] ise, örtülü rıza kişisel verilerin işlenmesinde geçerli bir rıza değildir. Sonuç olarak, kişisel verilerin işlenmesi hususunda rızanın içeriği ile ilgili tereddüt yaşanıyorsa bu unsur sağlanmadığı için rıza geçersiz kabul edilmelidir. Örneğin, bir otele kayıtta, formda istenen kişisel veriler doldurularak imza atılırsa, kişisel verilerin işlenmesinde aranan kesin, açık ve yazılı bir rıza beyanı elde edilmiş olur. İşlemeye rıza gösterme hâli imza ile sınırlı değildir. Mesela, bir internet sitesine girişte, IP bilgilerinin işleneceğini veya tercihlerin kaydedileceğini gösteren aydınlatma metninin altındaki kabul ediyorum butonu veya işaretlenmesi için bırakılan kutu rıza açıklama yollarındandır. Yine, indirimlerden haberdar olmak için telefon numarasının listeye kaydedilmesini isteyip istemediğinizi soran kasiyere, numarayı söylemek rıza vermeye örnek gösterilebilir.

Kanun, kural olarak, rıza açıklamasını herhangi bir şekil şartına bağlamamıştır. Bu sebeple, yazılı veya sözlü olarak ifade edilen ya da sesli veya görüntülü mesaj yoluyla iletilen rıza açıklamaları geçerliliği etkilemez. Yeter ki, kişisel verilerin işlenmesine izin verildiği hususu açıklık ve kesinlik arz etsin[56]. Bununla birlikte, herhangi bir uyuşmazlık hâlinde, GVKT.m.7/I hükmü gereğince, rızanın alındığını

---

51 **Kılınç,** s. 1149.

52 Bu kurala getirilen istisnalar için bkz., Fikret **Eren**, Genel Hükümler, 18. Baskı, Ankara 2015, s. 125.

53 Genel Veri Koruma Tüzüğü, 32 nci paragraf. Çalışma Grubu da susma hâlinde geçerli bir rızadan bahsedilemeyeceğini ifade etmiştir. Bkz., **Article 29 Data Protection Working Party**, Opinion 5/2004 on Unsolicited Communications for Marketing Purposes Under Article 13 of Directive 2002/58/EC, WP 90, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp90_en.pdf (Erişim Tarihi: 10.9.2018), s. 5.

54 **Başalp**, Veri, s. 39,40; **Küzeci**, Kişisel Veri, s. 240.

55 **Özdemir,** s. 169; **Akdağ,** s. 113-114; **Yücedağ,** s. 775; **Atak,** s. 211.

56 **Başalp,** Veri, s. 40

kanıtlama yükümlülüğü veri sorumlusuna ait olduğu için[57], veri sorumlusu, rızanın şekli ve kayıt altında tutulmasına ilişkin prosedürler geliştirmelidir[58]. KVKK veya 1995/46 sayılı Yönerge'de ise bu şekilde bir ispat yükü bulunmamakla birlikte, Genel Veri Koruma Tüzüğünde yer verilen hüküm doğrultusunda, ispat yükünün veri sorumlusuna ait olduğu söylenebilir.

bb. Rızanın Geri Alınması

Kişilik hakkına yönelik saldırılarda verilen rıza, serbestçe geri alınabilir[59]. Kişisel verilerin işlenmesini mümkün kılan rıza da herhangi bir sebeple geri alınmak istenebilir. Kişisel Verilerin Korunması Kanununda rızanın geri alınmasına ilişkin bir hüküm bulunmamaktadır. Çalışma Grubu, bu durumu 2002/58 sayılı Yönergenin 9 uncu maddesini esas alarak çözümlemeye çalışmıştır. Buna göre, rıza, her zaman ve ücretsiz olarak geri alınabilir[60]. GVKT.m.7/III hükmüne göre ise, geri alma beyanının rıza açıklaması kadar kolay kullanılması sağlanmalıdır. Bu kapsamda, örneğin, çevrimiçi bilet satışı yapan bir internet sitesinden bilet satın alınması esnasında, veri işlemeye izin verildiğine dair kutunun işaretlenmesi rıza açıklamasıdır. Bu rızanın geri alınması için, çalışma saatleri içerisinde müşteri hizmetlerine ulaşılmasına ilişkin gereklilik, anılan hükme aykırıdır. Bu durumda, ilgili kişi, site üzerinden işlemeye rıza gösterdiğine dair kutudaki işareti kaldırarak rızasını geri alabilmelidir[61].

b. Açık Rızanın Aranmadığı Hâller

aa. Kanunlarda Açıkça Öngörülmüş Olması

Kişisel veriler, açık rıza aranmaksızın, kanunlarda açıkça öngörülen hâllerde işlenebilir. Hükümde geçen "kanun" ifadesinden anlaşılması gereken, Anayasanın 13 üncü maddesi uyarınca belirlenmelidir. Kişisel verilerin korunmasını talep etme

---

57 Ayrıca bkz., Genel Veri Koruma Tüzüğünün 42 nci paragrafı. Örneğin, ilgili kişilerin işlemeye rıza gösterdiklerine dair telefon görüşmelerinin kaydı ispat açısından yeterlidir. Ancak, söz konusu ispat yükü sebebiyle, veri sorumlusu gerekenden fazla veri işlememelidir. Bkz., **Article 29 Data Protection Working Party**, Guidelines on Consent, s. 20, 21.

58 **Kaya,** s. 326.

59 **Oğuzman / Seliçi / Oktay-Özdemir**, s. 192; **Dural / Öğüz**, Kişiler, s. 139.

60 **Article 29 Data Protection Working Party**, Definition of Consent, s. 33.

61 **Article 29 Data Protection Working Party**, Guidelines on Consent, s. 22.

hakkı, temel hak ve hürriyetler kapsamında sayıldığı için, ancak kanunla sınırlanabilir[62].

Türk Hukukunda kişisel verilerin işlenmesini konu alan birçok kanun hükmü bulunmaktadır[63]. Örneğin, Yabancılar ve Uluslararası Koruma Kanununun 69 uncu maddesinin ikinci fıkrasında uluslararası korumaya başvuran kişilerin kimlik ve seyahat bilgilerinin kaydedileceği ifade edilmiştir. Ayrıca, aynı maddenin dördüncü fıkrasına göre, kişinin ülkesini terk etme sebepleri, terkten sonra başına gelen olaylar ve başvurmasına sebep olan olaylar, Türkiye'ye giriş şekli ve güzergâhı gibi ek bilgiler de alınır. Yine Türk Sivil Havacılık Kanunun[64] 40 ıncı maddesinin dördüncü fıkrası uyarınca, havayolu ile seyahat edecek kişilerin bilgileri toplanabilir, kaydedilebilir, işlenebilir ve paylaşılabilir. Üçüncü ülkeler ile paylaşımda ise, İçişleri Bakanlığının uygun görüşü aranır.

bb. Kişinin Kendisinin ya da Bir Başkasının Hayatının veya Beden Bütünlüğünün Korunması için Veri İşlemenin Zorunlu Olması

Kişisel Verilerin Korunması Kanunun 5 inci maddesinin 2 nci fıkrasının b bendi uyarınca, *"fiilî imkânsızlık sebebiyle rızasını açıklayamayacak durumda bulunan veya rızasına hukukî geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı ve beden bütünlüğünün korunması"* için kişisel verilerin işlenmesi zorunluysa işleme yapılabilir. Gerçekten, kişinin yaptığı kaza yaptığı ancak bedeninin bulunamaması gibi durumlarda fiilî imkânsızlık sebebiyle rıza açıklanamadığı için kimlik verileri veya plaka bilgisi işlenebilir. Yine, ailesini arayarak intihar edeceğini belirten bir kişinin bulunamaması hâlinde, konum verilerinin işlenmesi de mümkündür. Rızaya hukukî geçerlilik tanınmayan durumlar ise, tam ehliyetsizlerin veya kanunî temsilcisinin iznini almayan sınırlı ehliyetsizlerin rıza açıklamalarında görülür. Buna göre, örneğin, kaybolduğu anlaşılan bir sınırlı ehliyetsizi bulan kişilerin, sınırlı ehliyetsize ait kimlik bilgilerini elde ederek,

---

62 Şüphesiz, kişisel verilerin işleneceğine ilişkin ana çerçeve kanunla çizildikten sonra ayrıntılı hükümler yönetmelikle düzenlenebilir. Aksi hâlde, Anayasanın 13 üncü maddesine ek olarak, 7 nci maddesinin de ihlâli söz konusu olur.

63 Türk Silahlı Kuvvetleri İç Hizmet Kanununun m.34/A/2.

64 RG. 14.10.1983, S. 18196.

paylaşması hukuka aykırı nitelik taşımaz. Bu bent uyarınca verilerin işlenebilmesi için, hayat veya beden bütünlüğüne yönelik tehdidin yakın nitelik taşımasının gerekip gerekmediğine ilişkin herhangi bir belirleme bulunmamaktadır. Ancak, bu işleme hâli, tedbir almak için veya geniş çapta veri işlemek için kullanılmamalıdır[65].

Genel Veri Koruma Tüzüğüne göre, başkasının hayat ve beden bütünlüğünün korunması amacıyla kişisel verilerin bu bent kapsamında işlenmesi, işlemenin başka bir yasal temele dayanmaması hâlinde tercih edilmelidir[66]. Kişisel Verilerin Korunması Kanununda ise, açık rızanın aranmayacağı[67] bir durum olarak öngörülmüş olup, herhangi bir ön şarta yer verilmemiştir.

cc. Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesinin Gerekli Olması

Kişisel verilerin açık rıza aranmaksızın işlenebileceği diğer bir durum, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olmasıdır. Bu durumda veri işleme, sözleşmenin kurulmasıyla veya ifasıyla *doğrudan doğruya* ilgili olmalıdır (KVKK.m.5/II-c). Bu kapsamda, örneğin, iş sözleşmesinin kurulmasında ilgili kişinin kimlik bilgilerinin, eğitim bilgisinin, sağlık raporunun işlenmesi mümkündür. Benzer şekilde, kredi sözleşmelerinde, kredi alan kişinin kimlik bilgileri, gelir durumunu gösterir belge ve kredi türüne göre taşınmaza ait tapunun fotokopisi işlenebilir. Bununla birlikte, ileride yapılacak bir sözleşme gerekçe gösterilerek veri araştırması yapılması mümkün değildir[68].

Bir sözleşmenin ifası için gerekli olan işlemelere örnek olarak, alıcının adres ve iletişim bilgilerinin, satıcının ise hesap numarası bilgisinin alınması verilebilir. Ancak, kişinin satın aldığı eşyalardan yola çıkarak, kişisel zevkine ve yaşam tarzına ilişkin seçimlerin bu kapsamda işlenmesi mümkün değildir. Yine, internetten kredi

---

65 **Article 29 Data Protection Working Party**, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, WP 217, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (Erişim Tarihi: 15.9.2018), s. 20.

66 Genel Veri Koruma Tüzüğünün 46 ncı paragafı.

67 Bu bent uyarınca ilgili kişinin imkânı olsaydı rıza göstereceği faraziyesinden yola çıkarak işleme yapılır. Bu sebeple, işlemeden sonra kişinin rızası alınmazsa işleme hukuka aykırı kabul edilmelidir. Bkz., **Başalp**, Veri, s. 44; **Özdemir**, s. 128.

68 **Özdemir,** s. 182.

kartıyla alışveriş yapılmasında kredi kartı bilgilerinin alınması, sözleşmenin kurulması ve ifası için gereklidir. Bununla birlikte, kredi kartı bilgilerinin kaydedilmesi veya arşivlenmesi ifa ile doğrudan doğruya ilgili olmadığı için, ilgili kişinin açık rızasına bağlıdır.

dd. Veri Sorumlusunun Hukukî Yükümlülüğünü Yerine Getirebilmesi için Veri İşlemenin Zorunlu Olması

Veri sorumlusu, hukukî yükümlülüğünü yerine getirebilmek için zorunlu olması hâlinde, açık rıza aranmaksızın kişisel verileri işleyebilir. Veri sorumlusu, kanundan doğan veya sözleşmeden doğan hukukî yükümlülüklere sahip olabilir ve bu yükümlülükler çerçevesinde veri işleyebilir[69]. Çalışma Grubuna göre, hukukî yükümlülük ifadesinden anlaşılması gereken - sözleşmeden doğan yükümlülüklerin yerine getirilmesi için gerekli olan işlemenin ayrı bir bentte düzenlenmesi sebebiyle - kanundan doğan yükümlülükler olduğu ifade edilmektedir[70]. Veri sorumlusunun söz konusu yükümlülüğünü yerine getirme noktasında tercih hakkının bulunması hâlinde, bu bent uyarınca yapılan işleme hukuka aykırı nitelik taşır[71].

Veri sorumlusunun hukukî yükümlülüklerine örnek olarak, 4857 sayılı İş Kanununa[72] göre, işverenin işçi özlük dosyasında yer alan her türlü bilgi ve belgeyi saklama ve istenildiğinde yetkili memura gösterme zorunluluğu verilebilir. Buna göre, yetkili memurun kişisel verilere erişiminin sağlanması, kanundan doğan yükümlülüğün yerine getirilmesi sebebiyledir. Yine, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun[73] 78 inci maddesi gereğince, Sosyal Güvenlik Kurumu ile sözleşmesi olan tüm sağlık hizmeti sunucularının hizmet sunduğu kişilere ait sözleşmede yer alan bilgileri Sosyal Güvenlik Kurumuna gönderme yükümlülüğü vardır. 4904 sayılı Türkiye İş Kurumu ile İlgili Bazı Düzenlemeler

---

69 **Yücedağ,** s. 778.

70 **Article 29 Data Protection Working Party**, Legitimate Interests, s. 19. Nitekim, bu bent kapsamında veri sorumlusunun kanundan doğan yükümlülüklerinin yerine getirilmesi sebebiyle işleme hâlleri, *"kanunlarda açıkça öngörülmüş olma"* sebebiyle işleme hâlleri ile çoğunlukla örtüşür niteliktedir.

71 **Yücedağ,** s. 778-779.

72 RG. 10.6.2003, S. 25134.

73 RG. 16.6.2006, S. 26200.

Hakkında Kanunun[74] 21 inci maddesi uyarınca, Türkiye İş Kurumu tarafından kamu veya özel işyerlerinden iş ve işgücü konularında bilgi istendiğinde bilgi verilmesi zorunludur.

5352 sayılı Adli Sicil Kanununun[75] 3 üncü maddesine göre, mahallî adlî siciller, sicildeki bilgilerin bilgisayara girmeli, Merkezî Adlî Sicile aktarılması ve ilgili şahıs ve kurumlara iletmelidir. Benzer bir yükümlülük, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun[76] 6 ncı maddesinde öngörülmüştür. Buna göre, yükümlüler[77] taraf oldukları veya aracılık ettikleri işlemlerden, Maliye Bakanlığınca belirlenecek tutarı aşanları, Malî Suçları Araştırma Kurulu Başkanlığına bildirmek zorundadırlar.

ee. Kişisel Verilerin İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması

Kişisel Verilerin Korunması Kanununun 5 inci madde gerekçesine göre, alenileştirme, *kişisel verilerin herhangi bir şekilde kamuoyuna açıklanmasını ve herkes tarafından bilinebilecek hâle gelmesini* ifade eder. Gerekçeye göre, alenileştirilmiş kişisel verilerin işlenmesinde, ilgili kişinin korunmaya değer hukukî yararı ortadan kalkmıştır. Bu sebeple, kişisel verilerin alenileştirilmesi, kişisel verilerin işlenebileceği bir diğer durum olarak değerlendirilmiştir. Bu bende göre, hukuka aykırılığın ortadan kalkması için, kişisel verilerin ilgili kişinin *kendisi* tarafından alenileştirilmiş olması gerekir (KVKK.m.5/II-d). Bu durumda, örneğin, başvurulan kadro sebebiyle, kimlik bilgilerinin ve eğitim bilgilerinin kurum tarafından ilan edilmiş olması, alenileştirme şartını sağlamaz. Öte yandan, alenileştirme fiilinden ne anlaşılması gerektiğine dair bir belirleme yoktur. Kişinin yakın arkadaşları ile paylaştığı bir bilgiyi, alenileştirilmiş veri olarak

---

74 RG. 5.7.2003, S. 25159.
75 RG. 1.6.2005, S. 25832.
76 RG. 18.10.2006. S. 26323.
77 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun m.2/1-d hükmüne göre, yükümlü, *"Bankacılık, sigortacılık, bireysel emeklilik, sermaye piyasaları, ödünç para verme ve diğer finansal hizmetler ile posta ve taşımacılık, talih ve bahis oyunları alanında faaliyet gösterenler; döviz, taşınmaz, değerli taş ve maden, mücevher, nakil vasıtası, iş makinesi, tarihi eser, sanat eseri ve antika ticareti ile iştigal edenler veya bu faaliyetlere aracılık edenler ile noterler, spor kulüpleri ve Cumhurbaşkanınca belirlenen diğer alanlarda faaliyet gösterenleri ifade eder"*.

nitelendirmemek gerekir[78]. Alenileştirmeden anlaşılması gereken, verinin kamunun ulaşabileceği şekilde açıklanması, sınırsız sayıda kişinin erişimine açılması olarak ifade edilebilirse de, alenileştirmenin gerçekleşip gerçekleşmediğinin her somut olay açısından değerlendirilmesi gerekecektir[79].

Ayrıca, alenileştirme şartının sağlandığı her durumda kişisel verilerin işlenip işlenemeyeceğinin belirlenmesi gerekecektir. Örneğin, verilerin, ilgili kişinin kendisi tarafından alenileştirilmesinin, genellikle, sosyal medya üzerinden gerçekleştirildiği düşünüldüğünde[80], kamuoyu ile paylaşılan ve kişisel veri teşkil eden bir fotoğrafın veya bilginin başka sitelerde kullanılıp kullanılamayacağının belirlenmesi gerekecektir. Bir görüşe göre[81], burada alenileştirme sebebinin dikkate alınması gerekir. Verilerin, alenileştirme sebebi ile bağlantılı, sınırlı ve ölçülü olarak işlenmesi gerekir[82]. Sosyal medya örneği üzerinden değerlendirilirse, alenileştirme amacının sosyalleşme, görme ve görünme arzusu olduğu söylenebilir[83]. Bu durumda, alenileştirilmiş bir verinin görme ve görünmeyi sağlayan bütün amaçlarla işlenmesinin mümkün olduğunu kabul etmek mi gerekecektir? Örneğin, bir işletmenin sahibinin sosyal medyada paylaştığı ad soyad ve iletişim bilgilerinin, ahlaka uygun olmayan sitelerde yer almasının açıklanması güçleşecektir. Daha isabetli olan diğer görüşe göre[84], işlemeye ilişkin ilgili kişinin makul beklentisinin esas alınması gerekir. Eğer, makul bir kişi, somut olayın özelliklerini dikkate alarak yaptığı değerlendirmelerde, veri sorumlusunun amaçları doğrultusunda alenileştirilen verileri işleyebileceği sonucuna ulaşıyorsa, kişisel verilerin işlenmesi mümkündür.

---

78 Ayözger Öngün, s. 30.

79 **Ayözger Öngün**, s. 30, dn. 122; **Yücedağ,** s. 779.

80 We Are Social adlı şirketin 2019 yılının Ocak ayına ait sosyal medya kullanım istatistiklerine yer verdiği raporuna göre, Türkiye'de nüfusun %63'ü aktif olarak sosyal medya kullanmaktadır. Bkz., https://www.slideshare.net/DataReportal/digital-2019-turkey-january-2019-v01?qid=d245c79d-af8e-4135-b55b-0968825c3e50&v=&b=&from_search=1&fbclid=IwAR2vwXfikiWfIo4sI9jGWaAgC_lSAmkDl6pCq0o6rGlO7_VwTUoCxodvJec (Erişim Tarihi: 15.3.2019), s. 15.

81 **Küzeci,** s. Kişisel Veri, s. 344.

82 **Küzeci**, Kişisel Veri, s. 348.

83 Gerçekten, sosyal medya kullanımının sebeplerini ortaya koyan 2015 yılındaki bir araştırmaya göre, kişiler, fotoğraf veya video, günlük yaşantıya ilişkin ayrıntılar ve düşüncelerinden oluşan bir dizi verilerini paylaşmak gibi amaçlarla sosyal medya kullanmaktadır. Söz konusu araştırmaya ulaşmak için bkz., https://wearesocial.com/uk/blog/2015/04/top-10-reasons-social-media (Erişim Tarihi: 17.9.2018).

84 **Yücedağ,** s. 779-780.

Ayrıca, bir kişisel verinin işlenmesi (alenileştirilmesi)[85], verinin *kişisel veri olma* niteliğini değiştirmeyeceği için, veri sorumlusu açısından KVKK.m.5/II hükmünde yer verilen ilkelere uyma yükümlülüğü devam eder[86]. Zira, kişisel verilerin alenileştirilmesi, Kanunun uygulama alanından kısmen istisna tuttuğu hâllerdendir. Bu sebeple, veri sorumlusunun ilkelere uyumlu davranma yükümlülüğü devam eder.

ff. Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Veri İşlemenin Zorunlu Olması

Bir hakkın tesisi, kullanılması veya korunması için veri işleme zorunluysa, kişisel veriler açık rıza olmaksızın işlenebilir. Bu duruma, örneğin bir hakkın korunması için açılan davada gerekli olan kimlik bilgilerin veya adres bilgisinin işlenmesi verilmektedir. Yine, mülkiyet hakkını kuracak olan tapu sicilinde gerçekleştirilecek bir tescil işlemi, kimlik bilgilerinin işlenmesini gerektirir.

gg. Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlemenin Zorunlu Olması

Kişisel verilerin açık rıza olmaksızın işlenebileceği son hâl, ilgili kişinin temel hak ve hürriyetlere zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatlerinin işlemeyi zorunlu kılmasıdır (KVKK.m.5/II-f). Meşru menfaate dayalı olarak veri işleme, kişisel verilerin açık rıza olmaksızın işlenebileceğini öngören en esnek ve kapsamlı kategori olarak ifade edilebilir. Bununla birlikte, bu özellikler uygulanabilirliği beraberinde getirmemektedir. Nitekim, bu bent uyarınca kişisel verilerin işlenebilmesi için, veri sorumlusunun[87] meşru menfaatinin bulunması, bu menfaatin işlemeyi zorunlu kılması ve işleme sebebiyle ilgili kişinin temel hak ve özgürlüklerine zarar verilmemesi gerekir.

---

85 KVKK.m.3/I-e hükmü gereği, kişisel verilerin açıklanması şeklinde gerçekleşen alenileştirme de kişisel verilerin işlenmesi olarak kabul edilmelidir.

86 **Başalp**, Veri, s. 45; **Yücedağ,** s. 779.

87 GVKT.m.6/I-f hükmüne göre, veri sorumlusuna ek olarak, üçüncü kişilerin meşru menfaatlerinin gerektirmesi sebebiyle kişisel veriler işlenebilir. Ancak, kamu kurum ve kuruluşlarının meşru menfaate dayalı olarak veri işlemesi mümkün değildir. Bkz., Genel Veri Koruma Tüzüğünün 47 nci paragrafı. KVKK ise, istisnaların düzenlendiği hâller (m.2) dışında kamu sektörü veya özel sektör ayrımına yer vermemiştir. Bu sebeple, Türk hukuku açısından kamu kurum ve kuruluşları da meşru menfaate dayalı olarak kişisel verileri işleyebilir. Bkz., **Korkmaz,** s. 88.

Menfaat kavramı, veri sorumlusunun işleme sebebiyle elde edeceği tüm çıkarları ifade eder[88]. İşlemeyi mümkün kılacak menfaatin meşru olması için ise, hukuka uygun, açık, gerçek ve güncel olması gerekir[89]. Çalışma Grubuna göre, ifade özgürlüğünün kullanılması, pazarlama, güvenlik ve yönetim alanlarında çalışanların izlenmesi, fiziksel güvenliğin veya ağ güvenliğinin sağlanması gibi hâllerde meşru menfaatin varlığı kabul edilir[90]. Örneğin, mobil telefonda bulunan bir uygulama aracılığıyla kıyafet siparişinde adres ve kredi kartı bilgileri verilmiştir. Daha sonra, verilen adrese gönderilen indirim kuponu ve broşür, veri sorumlusunun pazarlama amacı güden meşru menfaatlerinin bir gereği olarak kabul edilmelidir. Benzer şekilde, çalışanlar arasındaki rekabeti artırmak gibi amaçlarla ayın elemanı seçiminde, çalışanların kişisel verilerinin işlenmesi meşru menfaat olarak değerlendirilebilir. Şüphesiz, meşru menfaatin bulunduğu her hâlde, kişisel veriler işlenemez. Ek olarak, veri sorumlusunun meşru menfaati kişisel verilerin işlenmesini zorunlu kılmalıdır. Eğer, temel hak ve hürriyetlerin daha az zarara uğrayacağı bir yol varsa, işleme yerine bu yol tercih edilmelidir.

Son olarak, ilgili kişinin temel hak ve hürriyetlerine zarar verilmemesi kaydıyla meşru menfaate dayalı olarak kişisel veriler işlenebilir. Esasen, kişisel verilerin işlenmesinde temel hak ve hürriyetlerin ihlâli kaçınılmazdır. Bu sebeple, bu hüküm ile öngörülenin bir şart olarak algılanmaması gerekir[91]. Bunun yerine, veri sorumlusunun elde edeceği *meşru menfaat* ile ilgili kişinin *temel hak ve hürriyetlerinin* ihlâli arasında bir menfaat dengesi gözetilmelidir. Gözetilen bu denge sonucunda, hangi değerin üstün tutulacağı belirlenmeli ve buna göre kişisel verilerin işlenip işlenmeyeceğine karar verilmelidir. Eğer, veri sorumlusunun meşru menfaati üstün tutularak verilerin işlenmesine karar verilirse, veri sorumlusunun ilgili kişiye ek korumalar sağlaması gerekebilir[92]. Örneğin, bir şirketin üst düzey yöneticilerinin maaşlarını kamuya açıklamasında, veri sorumlusunun meşru menfaati vardır. Bu

---

88 **Çekin,** Veri, s. 72.

89 **Article 29 Data Protection Working Party**, Legitimate Interests, s. 25.

90 **Article 29 Data Protection Working Party**, Legitimate Interests, s. 24.

91 Nitekim, Kanunun temel aldığı 1995/45 sayılı Yönergenin 7 inci maddesinin birinci fıkrasının f bendinde bu durum, menfaat dengesini gözetecek şekilde kaleme alınmıştır. Buna göre, veri sorumlusunun meşru menfaati, ilgili kişinin temel hak ve özgürlüklerinden kaynaklanan çıkarları tarafından geçersiz kılınmadıkça, kişisel verilerin işlenmesi mümkündür.

92 **Article 29 Data Protection Working Party**, Legitimate Interests, s. 42.

durumda veri sorumlusu şeffaflığı sağlayarak kendisine duyulan güveni sağlamlaştırır. Ancak, böyle bir hâlde veri sorumlusu, kişinin adını ve soyadını anonimleştirerek her pozisyona ait maaş bilgisini açıklamalıdır.

B. Özel Nitelikli Kişisel Verilerin İşlenmesi

Özel nitelikli verilerin işlendikleri takdirde, ayrımcılığa ve mağduriyete sebep olabileceğini daha önce ifade etmiştik. Bu sebeple, kişisel verilerin korunmasını öngören düzenlemeler, özel nitelikli verilerin işlenme şartlarına ayrı bir maddede yer vermiştir[93]. Gerçekten, Kişisel Verilerin Korunması Kanununun 6 ncı maddesinin birinci fıkrasında, özel nitelikli kişisel veriler tahdidi olarak sayılmış, daha sonra, özel nitelikli kişisel verilerin işleneceği hâllere yer verilmiş (f.2,3) ve özel nitelikli verilerin işlendiği her hâlde yeterli önlemlerin alınmasının gerekliliğine değinilmiştir (f.4).

Kural olarak, özel nitelikli kişisel verilerin açık rıza olmaksızın işlenmesi yasaktır[94]. Genel nitelikli kişisel verilerde olduğu gibi, açık rızanın, belirli konuya ilişkin olarak verilmesi ve bilgilendirmeye dayalı serbest irade ürünü olması gerekir. Ayrıca, açık rızanın, özel nitelikli verilerin işlenmesine izin verildiğine dair belirsizliğe yer vermeyecek şekilde açıkça ifade edilmesi gerekir.

Özel nitelikli kişisel verilerin açık rıza aranmaksızın işlenmesine, Kişisel Verilerin Korunması Kanununun 6 ncı maddesinin üçüncü fıkrasında ikili bir ayrımla yer verilmiştir. Buna göre, sağlık ve cinsel hayat dışındaki veriler, kanunlarda öngörülmesi hâlinde işlenebilir. Hatırlanacağı üzere, genel nitelikli kişisel verilerin işlenebileceği hâllerden biri, *kanunlarda açıkça öngörülmesi* idi. Daha sıkı koruma kurallarına tâbi olan özel nitelikli verilerde ise, *kanunlarda öngörülmesi*nin yeterli bulunmasının koruma amacı ile bağdaşmadığı isabetli olarak ifade edilmektedir[95]. Bu

---

93 Gerçekten, 108 sayılı Sözleşmenin 6 ncı maddesinde, 1995/46 sayılı Yönergenin 8 inci maddesinde ve Genel Veri Koruma Tüzüğünün 9 uncu maddesinde özel nitelikli kişisel verilerin işlenmesi düzenlenmiştir.

94 Kanunun yasak içeren ifadesi gereği, bu durum öğretide *kesin işlem yasağı* olarak adlandırılmaktadır. Bkz., **Özdemir**, s. 127; **Zorlu,** s. 152.

95 **Küzeci,** s. 353.

durumda, kanunlarda açıkça öngörülme şartının özel nitelikli kişisel veriler açısından evleviyetle aranması gerekir.

Örneğin, 2559 sayılı Polis Vazife ve Salâhiyet Kanununun[96] 5 inci maddesine göre, hükümde sayılan kişilerin biyometrik veri kategorisinde yer alan parmak izlerinin kimlik bilgileriyle birlikte sisteme kaydedilmesi öngörülmüştür. 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 67 nci maddesine göre, genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden yararlanması için biyometrik yöntemlerle veya kanunda sayılan diğer yöntemlerle kimlik doğrulaması zorunludur. Danıştay, kanunda yer alan diğer yöntemlerle (nüfus cüzdanı, evlenme belgesi, sürücü belgesi gibi) kesin bir şekilde kimlik doğrulanabiliyorsa, bu yöntemde ısrar edilmesinin mümkün olmadığını belirterek yürütmenin durdurulmasına karar vermiştir[97]. Zira, kişiyi eşsiz bir şekilde tanımlayan veya doğrulayan bu yöntemlerle elde edilen verilerin muhafazası bazı zorlukları beraberinde getirir. Yine, 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununun[98] 8 inci maddesine göre, sendika kurucu üyelerine ilişkin bilgilerin sendika tüzüğüne işlenmesi de kanunlarda öngörülmeye örnek olarak verilebilir. Benzer şekilde, 5352 sayılı Adli Sicil Kanununun 4 üncü maddesi uyarınca, özel nitelikli kişisel verilerden olan ceza mahkûmiyetlerinin sicile kaydedileceğine yer verilmiştir[99].

Sağlık ve cinsel hayat ile ilgili verilerin işlenmesi ise, amaç ve işleyecek kişi bakımından sınırlandırılmıştır. Buna göre, sağlık ve cinsel hayata ilişkin bilgiler, *"ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanın planlanması ve yönetimi amacıyla"*[100] işlenebilir. *Ancak* ifadesi sağlık ve cinsel hayata ilişkin kişisel verilerin

---

96 RG. 14.7.1934, S. 2751.

97 15. D. 8.7.2014, E. 2014/1150.

98 RG. 7.11.2012, S. 28460.

99 Mahkûmiyet kararları ve suçlara ilişkin kişisel verilerin işlenmesi, Genel Veri Koruma Tüzüğünün 10 uncu maddesinde ayrıca düzenlenmiştir. Buna göre, mahkûmiyet kararları ve suçlara ilişkin kişisel veriler, ilgili kişinin temel hak ve hürriyetlerinin korunmasına ilişkin güvenceler sağlayan birlik veya üye devlet hukuku tarafından izin verildiği hâllerde işlenmesi öngörülmüştür.

100 Hükümde, açık rıza aranmaksızın sağlık ve cinsel hayata ilişkin verilerin işlenmesini mümkün kılan amaçlara kapsamı geniş ifadelerle yer verilmesi eleştirilmektedir. Zira, burada özel niteliğe

yalnızca bu amaçlarla işlenebileceğini ifade etmek için kullanılmıştır. Öte yandan, KVKK.m.5 hükmünün gerekçesinde, fiilî veya hukukî olarak geçerli bir iradeden bahsedilemeyen, hayat ve beden bütünlüğünün korunması gereken durumlarda yapılacak işlemelere, kişinin sağlık bilgisinin işlenmesi örnek olarak verilmiştir. Bu durumda, özel nitelikli verilerin işlenmesinde genel nitelikli verilerin işlenme şartlarını düzenleyen hükmün uygulanıp uygulanmayacağı sorusu gündeme gelecektir. Sağlık ve cinsel hayata ilişkin verilerin, KVKK.m.5 hükmünde yer verilen şartlarla da işlenebileceğinin kabulü hem KVKK.m.6 lafzına hem de kanun sistematiğine uygun olmadığı için[101], kişilerin hayat ve beden bütünlüğünün korunması gerekçesiyle sağlık ve cinsel hayat bilgilerinin işlenmesi - gerekçede belirtilenin aksine - KVKK.6 hükmünde verilen kurallara tâbi olmalıdır.

Kişisel Verilerin Korunması Kanununun 6 ncı maddesinin gerekçesine göre, sağlık ve cinsel hayata ilişkin işleme hâllere örnek olarak, sağlık kuruluşları ve Sosyal Güvenlik Kurumu tarafından tutulan veriler gösterilebilir. Hükmün açık ifadesinden de anlaşılacağı üzere, burada veri işlemeyi gerçekleştirmeye yetkili olan kişi, *sır saklama yükümlülüğü altında olan kişiler veya yetkili kurum ve kuruluşlar*dır. Sağlık ve cinsel hayata ilişkin her işleme faaliyetinde bu iki unsur birlikte aranmalıdır. Bu yükümlülüğün gereklerinin yerine getirilmesine ayrıca özen gösterilmelidir. Zira, hem Yargıtay[102] hem de Danıştay[103] tarafından verilen kararlarda görüldüğü üzere, bu yükümlülüğün ihlâli ağır sonuçları da beraberinde getirmektedir.

---

sahip olduğu ifade edilen verilerin işlenmesinde amaçlanan sınırlamanın genişliği, onu sınırlama olmaktan çıkaracak niteliktedir. Bkz., **Badur,** s. 189. Kişiyi eşsiz bir şekilde belirlemede kullanılan biyometrik verilerin işlenmesinde de kapsam itibariyle geniş bir alanı ifade eden işlenme şartlarına bağlanmasına ilişkin eleştiriler için bkz., **Örnek Büken / Zeybek Ünsal**, s. 50-51. *Yücedağ'a* göre, bu durumda, özel nitelikli verilerin işlenebileceği hâller, KVKK.m.5/II hükmü ile birlikte düşünülmelidir. Dolayısıyla, *kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanın planlanması ve yönetimi amacıyla* özel nitelikli kişisel verilerin işlenmesi için, genel nitelikli verilerin açık rıza aranmaksızın işlenebileceği hâllerin (KVKK.m.5/II) varlığı aranmalıdır. Bkz., **Yücedağ,** s. 773.

101 **Badur,** s. 193.

102 HGK. 4.4.2001, E.2001/4-333, K.2001/335, (www.lexpera.com, Erişim Tarihi: 18.9.2019). Karara konu olayda, davacının AIDS olduğuna dair bilginin basında yer alması üzerine davalı devlet hastanesinin ödediği tazminatın, sır saklama yükümlülüğünü ihlâl eden başhekime rücu edilerek tahsil edilmesine karar verilmiştir.

103 10.D. 28.12.2007, E.2005/8407, K.2007/6526, (www.lexpera.com, Erişim Tarihi: 18.9.2019).

Özel nitelikli kişisel verileri gerek açık rızaya dayalı olarak gerek KVKK.m.6/III hükmüne dayalı olarak işleyen veri sorumlusunun, *yeterli önlemler*i alması şarttır. Yeterli önlemlerin içeriği Kişisel Verileri Koruma Kurulu tarafından belirlenir (KVKK.m.22/I). Bu amaçla Kurul, Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler ile ilgili 31.1.2018 tarihli ve 2018/10 sayılı Kararı yayınlanmıştır[104]. Buna göre, veri sorumluları öncelikle, *özel nitelikli verilerin işlenmesini öngören ayrı bir veri koruma politikası* belirlemelidir.

Çalışanlara yönelik olarak alınacak yeterli önlemlerin başında, özel nitelikli kişisel *verileri işleyenlere verilmesi gereken eğitimler* bulunmaktadır. Söz konusu eğitimler sonucunda *verilere erişim yetkisine sahip kişiler, yetkilerinin kapsamı ve süresi net olarak belirlenmeli*dir. Bu kapsamda, yetkili kişiler ile veri sorumlusu arasında *gizlilik sözleşmesinin* imzalanması gerekir. Veri sorumlusu, periyodik yetki kontrolleri gerçekleştirmeli ve özel nitelikli verilerin işlenmesinde görevli olmayan kişilerin verilere erişim yetkisini derhal kaldırmalıdır.

Özel nitelikli kişisel verilerin işlenmesi elektronik ortamda sağlanıyorsa, *kriptografik yöntemlerin kullanılması* ve *kriptografik anahtarların güvenli ve farklı ortamlarda tutulması* gerekir. Kriptografi, şifrelemeye ilişkin yöntemlerin bütünü olarak tanımlanabilir. Bu yolla, özel nitelikli kişisel veri teşkil eden ifadenin harflerinin yerine sayıların, şekillerin veya başka bir alfabenin yerleştirilmesiyle ya da harflerinin yerinin değiştirilmesiyle şifreleme yapılabilir[105]. Özel nitelikli kişisel verilerin işlendiği tüm hâllerde, örneğin, hastanın HIV virüsü taşıdığına dair teşhisi sisteme kaydeden bir hekim de uygun yeterli önlemleri almalıdır.

Kriptografik yöntemlere ek olarak, veriler üzerinde gerçekleştirilen *tüm işlem kayıtlarının güvenli olarak loglanması* sağlanmalıdır. Ayrıca, *"elektronik ortamda*

---

104 RG. 7.3.2018, S. 30353.

105 Ayşe **Coşkun** / Ülkü **Ülker,** Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti, Bilişim Teknolojileri Dergisi, C. 6, S. 2, Mayıs 2013, s. 31-39, s. 33. Bu yöntemlerle oluşturulan şifrelemelerden en bilineni, Roma İmparatoru Julius Caesar'ın algoritmasıdır. Buna göre, alfabede, her harfin yerine kendisinden belirli sayı sonraki harf yazılarak algoritma oluşturulur. Bkz., Vasif **Nabiyev,** Yapay Zeka, Ankara 2012, s. 260 vd.. Örneğin, belirlenen sayı üç ise, "A, B, C, Ç, D, …" harflerinin yerine sırasıyla, "Ç, D, E, F, G, …" harfleri gelir.

tutulan verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması, test sonuçlarının kayıt altına alınması, verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması, test sonuçlarının kayıt altına alınması, verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması" gerekir.

Özel nitelikli verilerin işlenmesi fizikî ortamda sağlanıyorsa, elektrik kaçağı, yangın, su baskını, hırsızlık gibi durumlara karşı yeterli güvenlik önlemlerinin alınması ve bu ortama yetkisiz giriş çıkışların engellenmesi gerekir. Son olarak, veri sorumlusu, Kurulun internet sitesinde yer alan Kişisel Veri Güvenliği Rehberi'nde[106] yer alan teknik ve idarî tedbirleri de dikkate almalıdır.

§ 5. KİŞİSEL VERİLERİN AKTARILMASI

I. GENEL OLARAK

Kişisel verilerin aktarılması, kişisel verilerin işlenmesi kapsamında sayılan faaliyetlerdendir (KVKK.m.3/I-e). Bununla birlikte, kişisel verilerin üçüncü kişilerin hâkimiyetine geçmesi ve üzerinde gerçekleştirebilecekleri işlemler göz önüne alınarak kişisel verilerin aktarılması ayrı bir madde ile düzenlenmiştir[107]. Buna göre, Kişisel Verilerin Korunması Kanununun 8 inci maddesinde kişisel verilerin yurt içine aktarılmasına, 9 uncu maddesinde ise, kişisel verilerin yurtdışına aktarılmasına ilişkin şartlara yer verilmiştir. Her iki hükümden yola çıkarak, gerek yurt içine gerek yurt dışına aktarımı düzenleyen diğer kanunlardaki hükümlerin öncelikli olarak uygulanması gerektiği ifade edilmelidir.

---

106 Bkz., https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf (Erişim Tarihi: 19.9.2018).

107 Bu durum, bazı yazarlar tarafından haklı olarak eleştirilmiştir. Kanunkoyucunun, söz konusu hükümde kişisel verilerin işlenmesine ilişkin şartlara atıf yaparak düzenlemesi, kişisel verilerin aktarılmasına özel önem atfettiğinin kabulünü zorlaştırmaktadır. Bu durumda, kişisel verilerin işlenmesine ilişkin tanımdan aktarmanın çıkarılması önerilmektedir. Bkz., **Badur,** s. 180. Ancak, kişisel verilerin işlenmesi tanımından aktarılmanın çıkarılması, kişisel verilerin işlenmesinde esas alınması gereken genel ilkelere uyma yükümlülüğünü de ortadan kaldıracağı için isabetli görünmemektedir. Bunun yerine, kanunkoyucunun, kişisel verilerin aktarılmasını düzenleyen hükümlerde, yurtdışına veya yurtiçine aktarımdan ne anlaşılması gerektiğine ve bu aktarımın şartlarının ne olacağına ilişkin özel hükümlere yer vermesi düşünülebilir.

Söz konusu hükümlere geçmeden önce, kişisel verilerin aktarılması ifadesinden ne anlaşılacağı belirlenmelidir. Kanunda veya 1995/46 sayılı Yönergede kişisel verilerin aktarılmasına ilişkin bir tanıma yer verilmemiştir. Ancak, Avrupa Birliği Adalet Divanı bir kararında, bir üye devlet toprağından üçüncü bir ülkeye kişisel verilerin iradî bir şekilde aktarılmasını, yurt dışına aktarım olarak ifade etmiştir. Öte yandan, somut uyuşmazlıktan yola çıkarak, yurt dışındaki kişilere doğrudan gönderilmeksizin sadece internet ortamında verilerin yayınlanmasını, yurt dışına aktarım olarak değerlendirmemiştir[108]. Buradan yola çıkarak *aktarım*, verilerin yurt içindeki veya yurtdışındaki gerçek veya tüzel kişiye iradî olarak iletilmesi şeklinde açıklanabilir.

II. KİŞİSEL VERİLERİN YURT İÇİNE AKTARILMASI

Kişisel verilerin yurt içine aktarılması, ilgilinin açık rızasına tâbidir. Kişisel verilerin aktarılmasını düzenleyen KVKK.m.8 hükmü, açık rıza aranmaksızın kişisel verilerin aktarılmasında ise, genel ve özel nitelikli verilerin açık rıza aranmaksızın işlenmesini öngören hükümlere atıfla yetinmiştir. Bir diğer deyişle, genel nitelikli veriler, Kanunun 5 inci maddenin ikinci fıkrasında yer verilen hâllerde açık rıza aranmaksızın aktarılabilir. Bu kapsamda, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun 6 ncı maddesinde göre, belirlenen tutarı aşanların Maliye Bakanlığına bildirilmesi, genel nitelikli verilerin aktarılması olarak değerlendirilebilir.

Özel nitelikli veriler ise, yeterli önlemler alınmak kaydıyla, Kanunun 6 ncı maddesinin üçüncü fıkrasında yer verilen hâllerde açık rıza aranmaksızın aktarılabilir. Kurul, Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler ile ilgili 31.1.2018 tarihli ve 2018/10 sayılı Kararında özel nitelikli kişisel verilerin aktarılmasına ilişkin yeterli önlemlere yer vermiştir. Buna göre, *"verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta*

---

[108] AAD., C-101/01 (Criminal Proceedings Against Bodil Lindqvist), 13.5.2014, bkz., https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1557095979675&uri=CELEX:62001CJ0101 (Erişim Tarihi: 20.9.2018), kn. 52-71.

(KEP) hesabı kullanılarak aktarılması, taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması, farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi, verilerin kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın gizlilik dereceli belgeler formatında gönderilmesi gerekir".

5352 sayılı Adli Sicil Kanununun 3 üncü maddesi uyarınca, mahallî adli siciller tarafından, sicildeki bilgilerin Merkezî Adlî Sicile aktarılması ve ilgili şahıs veya kurumlara iletilmesinde kullanılan araca göre, yeterli önlemlerin alınması gerekir. Günümüzde, adli sicil kayıtlarının bilgisayar ortamında tutulduğu göz önüne alındığında, taşınabilir bellek, CD, DVD ile aktarımda kriptografik yöntemlerin kullanılması gerekir. Yine, 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununun 20 nci maddesinin dördüncü fıkrası uyarınca, konfederasyonlara üye olma, üyelikten çekilme ve çıkarılma kararlarının Çalışma ve Sosyal Güvenlik Bakanlığına bildirilmesi elektronik posta ile sağlanıyorsa, belgenin şifrelenmesi gerekir.

III. KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASI

Kişisel veri üzerinde gerçekleştirilen diğer tüm faaliyetlerde olduğu gibi, kişisel verilerin aktarılması da, kural olarak, mümkün değildir. Bununla birlikte, Kişisel verilerin Korunması Kanununun 9 uncu maddesinde, kişisel verilerin yurt dışına aktarılabileceği hâller öngörülmüştür. İlk olarak, ilgilinin açık rızasının bulunması hâlinde kişisel veriler yurt dışına aktarılabilir.

Veri aktarımını öngören diğer hâl, verilerin aktarılacağı ülkede yeterli korumanın bulunup bulunmadığından yola çıkarak düzenlenmiştir. Bir ülkede yeterli korumanın bulunup bulunmadığını belirleme yetkisi Kurula verilmiştir. KVKK.m.9/4 hükmüne göre, Kurul bu belirlemeyi yaparken, Türkiye'nin taraf olduğu uluslararası sözleşmeleri, veri aktarımına ilişkin karşılıklılık ilişkisini, kişisel verinin niteliği ile işlenme amaç ve süresini, aktarım yapılacak ülkenin veri koruma

mevzuatı ve uygulamasını, aktarılacak ülkedeki veri sorumlusunun taahhüt ettiği önlemleri dikkate alacaktır[109]. Kurul gerekli görürse ilgili kurum ve kuruluşların da görüşünü alabilir. Buna göre, verilerin aktarılacağı ülkede *yeterli koruma* varsa, KVKK.m.5/II ve m.6/III hükümlerinde yer alan şartlara göre açık rıza aranmaksızın aktarım yapılabilir. Verilerin aktarılacağı ülkede yeterli koruma yoksa açık rıza aranmaksızın veri aktarımı için, KVKK.m.5/II ve m.6/III hükümlerinde yer alan şartlara ek olarak veri sorumlularının yazılı taahhütte[110] bulunmaları ve Kurul tarafından izin[111] verilmesi gerekir.

Verilerin aktarımı, Türkiye'nin veya ilgili kişinin menfaatlerine ciddi şekilde zarar verecekse, yurt dışına aktarım, ilgili kamu kurum ve kuruluşunun görüşü alınarak Kurul'un izniyle gerçekleşir. Kişisel verilerin yurt dışına aktarılmasını öngören uluslararası sözleşme hükümlerinin varlığı hâlinde de veriler yurt dışına aktarılabilecektir.

§ 6. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VEYA ANONİM HÂLE GETİRİLMESİ

Usulüne uygun olarak işlenen kişisel veriler, sınırlı süre muhafaza edilme ilkesinin bir gereği olarak belirli süre tutulabilirler. Bu durum, Kişisel Verilerin Korunması Kanununun 7 nci maddesi ile hüküm altına alınmıştır. Buna göre, işlenme sebeplerinin ortadan kalkması hâlinde, kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir. Bu kısımda, hükümde sözü edilen silme, yok etme ve anonim hâle getirme kavramları açıklanmalıdır. Bu kavramların tanımına,

---

109 Kurul, 2 Mayıs 2019 tarih 2019/125 sayılı Kararı ile Yeterli korumanın bulunduğu ülkelerin tayininde kullanılmak üzere oluşturulan formu kabul etmiştir. Formda, KVKK.m.9/4 hükmündekilere ek olarak bazı kriterlere yer vermiştir. Örneğin, verilerin aktarılacağı ülkede bağımsız bir veri koruma otoritesinin bulunması, küresel ve bölgesel örgütlere üye olma durumu ve o ülke ile yürütülen ticaret hacmi de göz önünde bulundurulacaktır. Kurul'un ilgili kararına ulaşmak için bkz., https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/60d987a1-ba9d-4285-a8ce-c3f41ff4e47f.pdf (Erişim Tarihi: 12.6.2019).

110 Söz konusu taahhütname, hem Türkiye'den veri aktaran veri sorumlusu tarafından hem yabancı ülkede veri aktarılan veri sorumlusu tarafından imzalanmalıdır. Taahhütnamenin içermesi gereken asgarî unsurlara ilişkin Kurul tarafından yayınlanan metin için bkz., https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar (Erişim Tarihi: 3.10.2018).

111 Kurul yurt dışına aktarıma izin verirken KVKK.m.9/4 hükmünde yer alan kalemleri değerlendirir.

KVKK.m.7 hükmünün gerekçesinde yer verilmiştir. Buna göre, *kişisel verilerin silinmesi,* kişisel verilerin ilgili kullanıcılar[112] için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. *Kişisel verilerin yok edilmesi*, verileri içeren materyalin yok edilmesini ifade eder. *Kişisel verilerin anonim hâle getirilmesi* ise, başka verilerle eşleştirilse dahi, verinin hiçbir şekilde gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder. Bu durumda, belirli veya belirlenebilir kılma özelliğini kaybeden veri, kullanılabilir vaziyettedir. Bazı yazarlara göre, verilerin anonim hâle getirilmesi verilerin imhası açısından yeterli değildir[113]. Zira, büyük veri *(big data)* olarak adlandırılan veriler, anonimleştirilmiş olsa dâhi, veri ile kişi arasındaki bağlantıyı kurabilmektedir.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi, kanuna uygun olarak işlenmelerine rağmen işlenme sebebinin ortadan kalktığı veriler üzerinde gerçekleşir (KVKK.m.7/I). Kanunlarda açıkça öngörülen bir sebebe dayalı olarak işleme yapılırken kanun hükmünün ilga edilmesi durumunda, işleme ile hedeflenen amacın gerçekleştirilmesi veya imkânsız hâle gelmesinde ya da açık rızaya dayalı olarak yapılan işlemede rızanın geri alınması hâlinde kişisel verilerin işlenme sebebinin ortadan kalktığı kabul edilmelidir. Yine, verilerin muhafazası noktasında kanunda belirlenmiş bir süre varsa[114], kişisel verilerin imha edilmesi gerekir. Kanun hükümlerine aykırı olarak yapılan işlemelerde ise, bu hükmün evleviyetle uygulanması gerekir. Buna göre, hukuka ve dürüstlük kurallarına aykırı olarak, verilen rızanın sınırları aşılarak veya geçersiz sözleşmeye dayanarak işleme yapılmışsa, işleme hukuka aykırıdır. Bu hâlde de, kişisel verilerin sadece silinmesini talep etme hakkı vardır. Kişisel verilerin anonimleştirilmesi, silinmesi, yok edilmesi

---

112 Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmeliğe göre, ilgili kullanıcı, *"Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri"* ifade eder.

113 **Çekin,** Big Data, s. 635. Nitekim, Netflix tarafından anonimleştirilerek yayınlanan veriler, veri uzmanları tarafından diğer veriler (örneğin, IMDB kullanıcı bilgileri) ile birleştirilerek Netflix kullanıcılarının bir kısmına ulaşılmıştır. Bkz., Boris **Lubarsky**, Re-Identification of "Anonymized" Data, GeorgeTown Law Technology Review, C. 202, 2017, s. 211-212.

114 Örneğin, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 6 ncı maddesine göre, *"erişim sağlayıcıları, sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla yükümlü"*dür.

veri sorumlusu tarafından resen gerçekleştirilebileceği gibi, ilgili kişinin talebiyle de sağlanabilir. Bu işlemin resen gerçekleştirilmesi aynı zamanda veri sorumlusunun yükümlülüğü olarak değerlendirilmiştir (KVKK.m.10,11).

İmha işlemlerine ilişkin ayrıntılı hükümlere Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelikte[115] yer verilmiştir. Yönetmelik'in resen imha etme sürelerini düzenleyen 11'inci maddesi, kişisel veri saklama ve imha politikası[116] hazırlama yükümlülüğüne göre bir ayrım yapmıştır. Buna göre, kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olan veri sorumlusu, işlenme sebebinin ortadan kalkmasını takip eden ilk periyodik imha[117] işleminde; kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu ise, işlenme sebebinin ortadan kalkmasından itibaren üç ay içerisinde uygun yöntemi seçerek kişisel verileri siler, yok eder veya anonim hâle getirir.

İlgili kişinin talebiyle kişisel verilerin imhası ise, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik'in 12 nci maddesinde düzenlenmiştir. Buna göre, ilgili kişi imha talep ettiğinde işlenme sebepleri ortadan kalkmışsa, veri sorumlusu en geç otuz gün içinde uygun yöntemi seçip gerekçesini bildirerek verileri siler, yok eder veya anonimleştirir. İşlenme şartları ortadan kalkmamışsa, veri sorumlusu en geç otuz gün içinde gerekçesini açıklayarak ilgili kişinin talebini reddedebilir.

Kişisel Verilerin Korunması Kanununda yer verilmemekle birlikte, gerek yargı kararları gerekse kişisel verilerin silinmesini talep etme hakkını ele alan düzenlemeler çerçevesinde unutulma hakkına değinmek gerekir.

---

115 RG. 28.10.2017, S. 30224.

116 Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi Hakkında Yönetmelik'in 4 üncü maddesinin birinci fıkrasının f bendine göre, kişisel verileri saklama ve imha politikası, *"Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azamî süreyi belirleme işlemi ile silme, yok etme ve anonim hâle getirme işlemi için dayanak yaptıkları politikayı ifade eder"*. VERBİS'e kayıt yükümlülüğü olan veri sorumluları bu politikayı hazırlamakla yükümlüdür.

117 Periyodik imha sürelerine, kişisel veri saklama ve imha politikasında yer verilmelidir. Bu süreler, her hâlde altı ayı geçemez.

§ 7. İLGİLİ KİŞİNİN HAKLARI VE VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

I. GENEL OLARAK

Kişisel verilerin işlenmesi sürecinde, ilgili kişiye haklar tanınmış ve veri sorumlusuna yükümlülükler getirilmiştir. Gerçekten, Kişisel Verilerin Korunması Kanununun 11 inci maddesiyle ilgili kişiye bilgi edinme, erişim, düzeltme talep etme, silinmesini veya yok edilmesini talep etme, bildirimde bulunulmasını talep etme, itiraz etme ve zararın giderilmesini talep etme hakkı tanınmıştır. Hatta, Anayasa'nın 20 nci maddesi gereği, ilgilinin haklarından olan *bilgi edinme, erişme, düzeltilmesini veya silinmesini talep etme* de anayasal haklar statüsündedir. Öte yandan, bu haklarla sağlanmaya çalışılan koruma mekanizması, veri sorumlusunun vereceği bilgilere bağlıdır. Bir diğer söyleyişle, hüküm kapsamında sayılan haklarını kullanan ilgili kişi, veri sorumlusundan net veya gerçeği yansıtan cevaplar alamayabilir. Bu durumda, Kurula şikâyet hakkı bulunmakla birlikte, bu yol, bilgi edinmesini sağlamayabilir. Bunun için, ilgili kişi ile veri sorumlusu arasında interaktif bir iletişimin kurulması önerilmektedir[118]. Veri sorumlusunun ise, Kanunun 10 uncu maddesinde aydınlatma yükümlülüğü, 12 inci maddesi kapsamında veri güvenliğine ilişkin yükümlülükleri ve 16 ncı maddesinde ise veri sorumluları siciline kayıt yükümlülüğü düzenlenmiştir. Söz konusu hükümlerde yer verilmese de, ilgili kişilerin başvurularına cevap verme, Kurul kararlarına uyma gibi yükümlülükler de veri sorumlusunun yükümlülükleri arasında sayılabilir.

Kural olarak, kişisel verisi işlenen her gerçek kişi sayılan hakları kullanabilir. Aynı şekilde, her veri sorumlusunun öngörülen yükümlülükleri yerine getirmesi gerekir. Bununla birlikte, KVKK.m.28/II hükmünde dört bent ile öngörülen hâllerde ilgili kişi, zararın giderilmesi istemi haricinde, 11 inci maddede sayılan haklarını kullanamaz[119]. Yine bu hâllerde, veri sorumlusunun aydınlatma ve veri sorumluları siciline kayıt yükümlülüğünü düzenleyen maddeler uygulanmaz. Öte yandan,

---

118 **Çekin,** s. 638.

119 Alenileştirme hâlinde kişisel verileri işlenen kişinin her durumda, zararın giderilmesi dışındaki haklarını kullanamayacak olmasının isabetli olmadığına dair bkz., **Yücedağ,** s. 781.

öngörülen hâllerde Kanunun amacına ve temel ilkelerine uygun davranma yükümlülüğü devam etmektedir. Bu durumda, mesela, veri sorumlusu, ilgili kişiye aydınlatmada bulunmak zorunda değildir. Bu durumda, ilgili kişi de verilerin silinmesini ve yok edilmesini veri sorumlusundan talep edemez.

II. İLGİLİ KİŞİNİN HAKLARI

A. Bilgi Edinme Hakkı

Kişisel verilerin işlenmesinde, korunma taleplerinin temelini *bilgi edinme hakkı* oluşturur. Bilgi edinme hakkı kapsamında ilgili kişi, öncelikle, kendisine ilişkin kişisel verilerin işlenip işlenmediğini öğrenebilir. Kişisel verileri işleniyorsa, işlenen veri kategorilerini, işlenme amacını, işlemenin hukukî sebebini de içeren bilgiler talep edilebilir. Bu durumda, ilgili kişi, veri kategorisine göre işlenme şartlarının gerçekleşip gerçekleşmediğini, işlenme amacının *belirli, açık, meşru amaç* ilkesi ile uyumluluğunu ve işlemenin *amaç ile bağlantılı, sınırlı ve ölçülü* olup olmadığını değerlendirebilir. Aynı zamanda, veriler yurtiçine veya yurtdışına aktarılıyorsa, aktarıldığı kişileri bilme hakkına sahiptir. Bilgi edinme hakkını kullanan ilgili kişiye verilen cevap açık ve anlaşılır olmalıdır[120]. İlgili kişi aldığı cevap ve yaptığı değerlendirme sonucunda, 11 inci maddede sayılan diğer haklarını kullanabilir.

B. Verilerin Düzeltilmesini, Silinmesini veya Yok Edilmesini Talep Etme Hakkı

Kişisel verilerin doğru ve gerektiğinde güncel tutulması veri sorumlusunun yükümlülüğündedir. Bu durum, hem ilgili kişinin hem de veri sorumlusunun menfaatinedir. Bununla birlikte, veri sorumlusu bünyesinde tutulan verilerin eksik, yanlış olması veya güncel olmaması hâlinde ilgili kişiye *düzeltilmesini talep etme hakkı* tanınmıştır. Daha önce de bahsedildiği üzere, verilerin eksik veya yanlış tutulması mümkündür. Bu durum, verilerin kişisel veri olma niteliğini değiştirmez. Nitekim, Kanun düzeltme hakkını kabul ederek bu durumu öngörmüştür. Kişi eksik

---

120 **Başalp**, Veri, s. 49.

verilerin tamamlatılması, yanlış bilgilerin düzeltilmesine ilişkin talep ileri sürdükten sonra, veri sorumlusu talebin gereğini yapar. Veri sorumlusu, verilerin eksik veya yanlış işlenmesi hususunda direnirse hukuka aykırı işleme ortaya çıkar. Artık, ilgili kişi, ortaya bir zarar çıkmışsa zararın giderilmesini genel hükümlere göre talep eder. Yahut, Kişisel Verileri Koruma Kurulu'na şikayet yolunu kullanır.

İlgili kişi, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde, kişisel verilerin silinmesini veya yok edilmesini veri sorumlusundan talep edebilir. Veri sorumlusu, kişisel verilerin düzeltilmesi, silinmesi veya yok edilmesi talepleri doğrultusunda işlemler yapabilir. Söz konusu işlemlerden önce verilerin aktarılması söz konusuysa, ilgili kişi bu işlemlerin aktarılan veri sorumlusuna bildirilmesini de talep edebilir.

C. İtiraz Hakkı

İtiraz etme hakkı, işlenen kişisel verilerin münhasıran otomatik sistemler aracılığıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasında tanınmıştır. Kişisel Verilerin Korunması Kanununun 11 inci maddesinin gerekçesinde, bir çalışanın yaptığı işlerin otomatik sistemler aracılığıyla analiz edilerek performansının değerlendirilmesi örnek gösterilmiştir. Bu durumda, çalışanın itiraz hakkını kullanması için, çalıştığı pozisyondan alt pozisyona geçirilmesi, ücretinin azaltılması gibi aleyhe sonuçların ortaya çıkması gerekir. İtiraz hakkının kullanılmasının sonucunda veri sorumlusu, yapılan işlemlerde itiraz edilen verileri dikkate alamayacaktır[121]. Örneğin, iş başvurusu sırasında yapılan sistem tarafından gerçekleştirilen psikolojik test sonucu işe uygun olmadığı belirlenen kişi, bu sebeple reddedilirse buna itiraz etme hakkı vardır. Bu durumda, işveren bu sonucu dikkate almaksızın iş başvurusunu tekrar değerlendirmeli veya başka bir sebebe dayanmalıdır.

Burada dikkat edilmesi gereken husus, hakkın kullanımının, otomatik sistemler aracılığıyla analiz yapılmasına bağlanmış olmasıdır. Bu sebeple, örneğin, bir çalışan hakkında doldurulan müşteri memnuniyeti anketlerinin, performans değerlendirme

---

121 **Başalp**, Veri, s. 51.

yazılımları aracılığıyla analiz edilmesi sebebiyle alt pozisyona geçirilmesine veya işten çıkarılmasına çalışanın itiraz etme hakkı vardır. Aynı anketlerin, otomatik olmayan yöntemler aracılığıyla değerlendirilmesi sebebiyle ortaya çıkan aleyhe sonuçlara maruz kalınması hâlinde ise itiraz edilemeyecektir.

D. Zararın Giderilmesini Talep Etme Hakkı

İlgili kişiye tanınan bir diğer hak, verilerin kanuna aykırı olarak işlenmesi sebebiyle ortaya çıkan zararın giderilmesini veri sorumlusundan talep etme hakkıdır[122]. Bu hakkın kullanılabilmesi için, kanuna aykırı olarak kişisel verilerin işlenmesi, failin kusurlu olması, ilgili kişinin zarara uğraması ve bu zararın kanuna aykırı işleme sebebiyle ortaya çıkması (illiyet bağı) gerekir. Bu kısımda, öncelikle, zararın giderilmesine ilişkin talebin veri sorumlusuna başvuru yoluyla mı yoksa dava yoluyla mı ileri sürüleceğinin belirlenmesi gerekir.

Kişisel Verilerin Korunması Kanununun 13 üncü maddesine göre, zararın giderilmesi istemi, ilgili kişiye tanınan diğer haklarda olduğu gibi, veri sorumlusuna başvuru yoluyla ileri sürülmelidir. Bu başvuru, Kurula şikâyet yolunun kullanılabilmesi için bir önşart niteliği taşır (KVKK.m.14/II). Bununla birlikte, veri sorumlusuna zararın giderilmesi istemiyle başvuruda, sorumluluğun türünü belirlemek ve değerlendirmek, tazminat miktarını belirlemek gibi hususlar gündeme geldiği için, bu hakkın dava yolu ile kullanılması gerektiği ileri sürülmüştür[123]. Bu görüş, mehaz 1995/46 sayılı Yönergenin 55 inci paragrafında[124] yer verilen açıklamalara da uygundur. Öte yandan, KVKK.11/I-g hükmünün bu görüşe göre

---

122 Daha önce bahsedildiği üzere, Kişisel Verilerin Korunması Kanununun 28 inci maddesinde öngörülen durumlardan biri olan alenileştirmede, ilgili kişi, sadece zararın giderilmesi hakkını kullanabilecektir. *Yücedağ'ın* isabetli olarak belirttiğine göre, bu hakkın tanınması için, işlemenin hukuka aykırı nitelik taşıması gerekir. Ancak, daha önce de bahsedildiği üzere, burada kişisel verilerin işlenmesinde hukuka aykırılığı kaldıran bir sebep bulunmaktadır. İşlemenin hukuka uygun olmasına rağmen tazminat borcunun ortaya çıktığı hâllerin (hakkaniyetin gerektirdiği durumların) işletilmesi ise, kanunun amacı göz önüne alındığında mümkün görünmemektedir. Bkz., **Yücedağ,** s. 781. Kanaatimizce, kanunkoyucu, alenileştirilmiş verinin genel ilkelere aykırı olarak işlenmesi sebebiyle ortaya çıkan zararın giderilmesi hususunu göz önüne alarak böyle bir düzenleme getirmiştir. Alenileştirilmiş verinin genel ilkelere uygun şekilde işlenmesi hâlinde, fiil hukuka uygun olduğu için zararın giderilmesi isteminden bahsedilemeyecektir.

123 **Taştan,** s. 199.

124 Buna göre, "Veri sorumlusu, ilgili kişilerin haklarını gözetmezse, ulusal mevzuat bir yargı yolu sağlamalıdır".

sağladığı koruma, hâlihazırda genel hükümlere göre tazminat istemini saklı tutan KVKK.m.14/III hükmü ile öngörülmüştür. Bir diğer deyişle, bu görüşün kabulü hâlinde KVKK.m.11/I-g hükmü, KVKK.m.14/III hükmü karşısında işlevsizleşir. Bu sebeple, zararın giderilmesi isteminin, doğrudan veri sorumlusuna başvuru yoluyla kullanılacak bir hak olarak öngörüldüğü de kabul edilebilir. Hakkın başvuru yoluyla kullanımı, veri sorumlusunun kanuna aykırı şekilde kişisel verileri işlediği ve bu sebeple ortaya çıkan zararın giderilmesi istemiyle birlikte bilgilendirme işlevi de görür. Bu durumda, veri sorumlusu, talep doğrultusunda zararın tazminini sağlarsa bir sorun çıkmaz. Bu amaçla, ilgili kişi ile veri sorumlusu arasında zararın giderilmesini amaçlayan genel hükümlere tâbi bir anlaşma yapılabilir[125]. Ancak, veri sorumlusu talebi reddederse, süresinde cevap vermezse veya talep yeteri kadar karşılanmazsa, ilgili kişinin Kurula şikâyet yoluna başvurması mümkündür. Aynı zamanda, ilgili kişi, bunlardan bağımsız olarak genel hükümlere göre tazminat talep edebilir (KVKK.m.14/III). Sonuç olarak, ilgili kişi KVKK.m.11/I-g hükmünde öngörülen veri sorumlusuna başvuru hakkını kullanarak veya KVKK.m.14/III hükmüne göre genel hükümlerde öngörülen dava yolunu kullanarak zararın tazminini sağlayabilir.

III. VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

A. Aydınlatma Yükümlülüğü

Veri sorumlusunun yükümlülüklerinden ilki olan aydınlatma yükümlülüğü, kişisel verilerin elde edilmesi sırasında ilgili kişilere bilgi verilmesini amaçlar. Bu kapsamda veri sorumlusu veya yetkilendirdiği kişi, Kanunun 10 uncu maddesinde sayılan *"veri sorumlusunun ve varsa temsilcinin kimliği, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel verileri toplamanın yöntemi ve hukukî sebebi ile 11 inci maddede sayılan ilgili kişinin diğer hakları"* ile ilgili bilgileri ilgili kişiye vermekle yükümlüdür. Bu durum, dürüstlük kurallarına uygun olarak işleme ilkesi ve her ne kadar genel ilkelerde yer

---

125 **Ayan**, Borçlar, s. 312.

verilmemiş olsa da şeffaflık ilkesinin bir gereğidir[126]. Yükümlülüğün yerine getirilmesiyle, ilgili kişi, verilerinin kimler tarafından ve nasıl elde edildiğini, hangi amaçla ve yöntemle işleme yapılacağını, işlemenin hukuka uygun olup olmadığını öğrenebilir. Şüphesiz, ilgili kişinin bilgi edinme hakkını kullanarak bu bilgilere ulaşması mümkündür. Nitekim, aydınlatma yükümlülüğü ile bilgi edinme hakkı birbirini tamamlar niteliktedir. Bununla birlikte, aydınlatma yükümlülüğünün sadece kişisel verilerin elde edildiği aşamada yerine getirilmesi aranır. Bilgi edinme hakkı açısından böyle bir sınırlamaya yer verilmediği için, her zaman kullanılabileceği kabul edilmelidir.

Bu noktada değinilmesi gereken bir diğer husus, verilerin elde edildiği kişiye göre aydınlatma yükümlülüğünün kapsamının değişip değişmeyeceğidir. Başka bir söyleyişle, verilerin ilgili kişiden elde edilmesiyle, başka bir kişi veya kurumdan elde edilmesi arasında aydınlatma yükümlülüğü açısından fark ortaya çıkacak mıdır? Bu sorunun ortaya çıkmasında, 1995/46 sayılı Yönergenin ve Genel Veri Koruma Tüzüğünün aydınlatma yükümlülüğünü düzenlerken ilgili kişiden elde edilip edilmediğini dikkate alması etkili olmuştur[127]. Kanun herhangi bir ayrıma gitmediği için, açık rızaya veya diğer durumlara dayalı olarak kişisel verilerin elde edilmesi hâlinde aydınlatma yükümlülüğü yerine getirilmelidir. Bu sebeple, kişisel verileri elde eden bir şirket veya kamu kurumu, kanunda açıkça öngörülen bir sebebe dayalı olarak işlem yapsa dâhi sayılan hususları içeren bir aydınlatmada bulunmakla yükümlüdür. Aydınlatma yükümlülüğünün yerine getirilmesinde uyulması gereken bir şekil şartına yer verilmediği için sözlü veya yazılı olarak yerine getirilebilmelidir.

---

126 **Çekin**, Kişisel Veri, s. 103.

127 Gerçekten her iki düzenlemeye göre, kişisel verilerin elde edilmesinde aydınlatma yükümlülüğü, asgarî unsurları barındıracak şekilde yerine getirilir. Bununla birlikte, kişisel verilerin ilgili kişiden elde edilmediği bazı hâllerde, aydınlatma yükümlülüğü ortadan kalkar. İlgili kişinin hâlihazırda bu bilgilere sahip olması ya da bilgilerin sağlanmasının imkânsız olması veya ölçüsüz bir çaba gerektirmesi bu hâllerdendir. Bkz., 1995/46 sayılı Yönerge m.10-11 ve GVKT.m.13-14. Bu düzenlemelerden yola çıkarak, bilgilerin sağlanmasının imkânsız olması veya aşırı bir çaba gerektiriyorsa, aydınlatma yükümlülüğünün ortadan kalkacağına ilişkin bkz., **Başalp**, Veri, s. 47-48.

B. Veri Güvenliğine İlişkin Yükümlülükler

Veri güvenliğine ilişkin yükümlülükler, Kanunun 12 nci maddesinde düzenlenmiştir. Hükme göre, veri sorumlusunun uygun güvenliği sağlamak amacıyla gerekli teknik ve idari tedbirleri alması, Kanun hükümlerini uygulamak amacıyla denetimlerde bulunması, verileri hukuka aykırı olarak başkalarına açıklayamayıp, kullanamaması ve verilerin hukuka aykırı olarak elde edilmesi hâlinde bu durumu Kurula bildirmesi veri güvenliği yükümlülüklerindendir. Görüldüğü üzere, veri güvenliği kişisel verilerin elde edilmesinden başlayarak imha edilmesine kadar devam eden ve üçüncü kişiler tarafından erişilmesini ve kullanılmasını önlemeye yönelik yükümlülüklerin toplamını ifade eder. Söz konusu yükümlülüklere uygun tedbirlerin kişisel verilerin elde edilmesinden önce alınması isabetli olur. Zira, elde etme aşamasındaki veri sızıntılarını veya veri ihlallerini önlemek amacıyla önceden bir veri işleme sistemi kurulmalıdır. Daha sonra, verilerin elde edilmesinde bu sistem uyarınca koruma gerçekleştirilmelidir. Söz konusu yükümlülükler, kişisel verilerin ve dolaylı olarak kişiliğin korunmasına hizmet ettikleri için veri koruma hukukunda önemli bir yere sahiptir[128].

1. Tedbir Alma Yükümlülüğü

Veri güvenliğinin sağlanması amacıyla yerine getirilmesi gereken yükümlülüklerden ilki tedbir alma yükümlülüğüdür. Tedbir alma yükümlülüğü, veri sorumlusunun kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemek ve güvenli bir şekilde muhafazasını sağlamak için gerekli her türlü idarî ve teknik tedbiri almasını ifade eder. Bu kapsamda gerek fizikî ortamda tutulan gerekse elektronik ortamda tutulacak veriler açısından kişisel verinin kategorisine göre mevcut riskler ve hukuka aykırı erişim hâlinde ortaya çıkabilecek zararlar göz önüne alınmalıdır. Fizikî ortamda tutulan verilerin güvenliğinin sağlanmasında alınacak tedbirler sınırlıdır. Zira, fizikî ortamda bulunan veri ihlâlleri gözle görülür şekilde gerçekleşmektedir. Çalışanların şifreleme yöntemlerini kullanarak verileri kaydetmesi, ortamın anahtar veya güvenlik görevlisi aracılığıyla güvenliğinin sağlanması fizikî ortamda alınabilecek önlemlerden bazılarıdır. Bununla birlikte,

---

[128] **Çekin,** Kişisel Veri, s. 14.

günümüzde verilerin kaydedilmesini, yönetilmesi, aktarılması gibi tüm işlemler için bilişim sistemlerinin sağladığı kolaylıklar, kamu sektörünün ve özel sektörün elektronik ortama yönelimini hızlandırmıştır.

Elektronik ortamda tutulan verilerin güvenliğinin sağlanması ise, fizikî ortama nispeten daha zordur. Zira, elektronik ortama yönelik ihlâller her geçen gün nitelik değiştirmektedir. Bu sebeple, veri sorumluları riskleri en aza indirebilecek bir kayıt ve yönetim sistemi tasarlama yoluna gitmelidir. Bu sistemin tasarlanmasında, gerekirse yazılım mühendislerinden yardım alınmalıdır. Söz konusu sisteme kayıtta ve verilerin yönetilmesinde, veri sorumlusunun politikası çerçevesinde hareket edilmelidir. Sisteme, veri minimizasyonu ilkesinin bir gereği olarak, veri sorumlusunun hukuka uygun amacını gerçekleştirmeye yetecek en az sayıda veri kayıt edilmelidir. Böylece, olası ihlâller sebebiyle ortaya çıkacak zarar en aza indirilebilir.

Sisteme giriş yapma yetkisi verilen çalışanlar, veri güvenliği uzmanlarından seçilmeli ve her bir çalışanın görev tanımları ve sorumluluklarının sınırları belirlenmelidir. Sisteme giriş yetkisi olan çalışanlar tarafından yüksek güvenlikli şifreler veya tek kullanımlık şifreler tercih edilmesi gerekir. Bu sayede hukuka aykırı olarak veriye erişim engellenebilir. Sisteme giriş saati ve çıkış saati de dâhil olmak üzere, çalışanların veri üzerinde gerçekleştirdiği işlemlerin kayıtları alınmalıdır. Aynı zamanda, çalışanların veri güvenliğini sağlamaya yönelik güncel gelişmeleri esas alan eğitimlere katılımı sağlanmalıdır. Tasarlanan sisteme internet üzerinden gelebilecek veri ihlâllerini bertaraf etmek için ise, güvenli olmayan sitelere girişi ve üçüncü kişilerin ağa sızmasını engelleyen bilgi teknolojileri güvenlik şirketlerinden yardım alınabilir. Veri sorumlusu, olası veri ihlâllerinin sebep olacağı etkileri en aza indirmek için, ihlâl anında sergilenecek tutum ve yapılacak işlemleri de önceden belirlemeli ve çalışanlarını bilgilendirmelidir.

Kişisel Verilerin Korunması Kanununun 12 nci maddesinin 2 nci fıkrası uyarınca, veri işleme, veri sorumlusu adına başka bir gerçek veya tüzel kişi tarafından gerçekleştiriliyorsa, bu kişiler, söz konusu tedbirlerin alınmasında veri sorumlusu ile birlikte müştereken sorumlu tutulmuştur. Bu hükümle, veri sorumlusu, veri ihlâlinden kendisi adına kişisel veri işleyeni sorumlu tutamayacaktır. Aynı

zamanda, veri işleyen, genellikle, verilerin işlendiği anda yapılması önem arz eden veri güvenliğine ilişkin yükümlülükleri yerine getirmekle yükümlü olacaktır.

2. Denetleme Yükümlülüğü

Veri güvenliğinin sağlanması amacıyla yerine getirilmesi gereken bir diğer yükümlülük, denetleme yükümlülüğüdür. Denetleme yükümlülüğü, gerek verilerin işlenmesi aşamasında gerekse yükümlülüklerin yerine getirilmesinde, Kanun hükümlerine uygunluğun gerekli denetimlerle sağlanmasını ifade eder (KVKK.m.12/III). Denetleme yükümlülüğü, veri sorumlusu tarafından yerine getirilebileceği gibi, veri sorumlusunun belirlediği bir kişi tarafından da yerine getirilebilir. Denetleme yükümlülüğü kapsamında, genel ilkeler, işleme şartları ve yükümlülükler gibi Kanunda yer verilen hususlara uygunluk denetlenecektir. Denetleme sonucunda Kanuna aykırılık tespit edilirse, bunun düzeltilmemesinden doğan sorumluluk veri sorumlusuna ait olacaktır. Bir diğer deyişle, veri sorumlusunun denetleme görevlisi ataması, sorumluluğunu ortadan kaldırmayacaktır. Veri sorumlusu bu durumda, denetleme görevi bulunan kişi ile arasındaki ilişkiye istinaden sözleşmeden doğan sorumluluk hükümlerine başvurabilir. Daha önce değinildiği üzere, Genel Veri Koruma Tüzüğünde kamu kurum ve kuruluşları gibi belirli veri sorumluları açısından bu denetimleri yapma görevi, veri koruma görevlisine bırakılmıştır. Özellikle büyük miktarda veri işleyen kamu kurumları göz önüne alındığında, Türk hukukunda Veri Sorumluları Siciline kayıt yükümlülüğü bulunan veri sorumluları açısından benzer bir uygulamanın getirilmesi, kanaatimizce, veri koruma kurallarının uygulanmasını kolaylaştıracaktır.

3. Sır Saklama Yükümlülüğü

Kişisel Verilerin Korunması Kanununun 12 nci maddesinin dördüncü fıkrasında düzenlenen sır saklama yükümlülüğü, kişisel verilerin Kanun hükümlerine aykırı olarak başkasına açıklanamamasını ve işleme amacı dışında kullanılamamasını ifade eder. Bu yükümlülük, kişisel verilerin korunmasındaki asıl amacın doğal bir sonucudur. Gerçekten, kişisel veriler, Kanunun öngördüğü durumlar dışında veya Kanunun yetkilendirdiği kişiler dışındakilere açıklanamaz. Bu yükümlülüğe göre, örneğin, veri sorumlusu veya veri işleyen kendisi ile aynı yerde çalışan diğer kişilerle

kişisel verileri paylaşamayacaktır. Aynı zamanda, kişisel veriler, işlenmesindeki temel amaca uygun olarak işlenebilir. Bu durum, kişisel verilerin amaç ile bağlantılı, sınırlı ve ölçülü olma ilkesinin bir gereğidir. Örneğin, 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununun 20 nci maddesinin dördüncü fıkrası uyarınca bir kişinin konfederasyona üye olma kararı Çalışma ve Sosyal Güvenlik Bakanlığına bildiriliyorsa, Bakanlık bu bilgiyi işe alımda kullanamaz.

Hükme göre, veri sorumluları ve veri işleyenler sır saklama yükümlülüğü altındadır. Bu sebeple, veri işleyen, sır saklama yükümlülüğünü ihlâl ederse Kanun hükmü gereğince sorumlu tutulabilir. Bununla birlikte, veri sorumlusu, veri işleyen ile sır saklama yükümlülüğünü düzenleyen bir gizlilik anlaşması yapmışsa, bu durumda veri işleyen sözleşmeden doğan sorumluluk hükümlerine de başvurabilir.

4. Bildirimde Bulunma Yükümlülüğü

Kişisel verileri işleme ve verilere erişme yetkisi, veri sorumlusuna ve veri işleyene aittir. Bununla birlikte, veri sorumlusunun kazara veya kasıtlı davranışı sebebiyle, üçüncü kişilerin kişisel verilere erişmesi söz konusu olabilir. Örneğin, kişisel verilerin yanlış bir kişiye aktarılması, verileri içeren aygıtın çalınması, veri kayıt sistemine ilişkin ağa izinsiz olarak girilmesi gibi hâllerde kanuna aykırı erişimden bahsedilir.

Kişisel veriler veri sorumlusunun muhafazası altındayken üçüncü kişiler tarafından kanuna aykırı olarak elde edilirse, veri sorumlusu bu durumu ilgili kişiye ve Kurula bildirmekle yükümlüdür (KVKK.m.12/VI). Hüküm, kişisel verilerin kanuna aykırı olarak elde edilmesinden bahsetmekle birlikte, Genel Veri Koruma Tüzüğünde bu durum, *imha edilmesi, kaybolması, değiştirilmesi, izinsiz olarak ifşa edilmesi veya erişilmesi*ni de kapsayacak şekilde ele alınmıştır. Bu durumda, örneğin, çekiliş yoluyla hediye vermek isteyen bir kişinin sistemine girilerek, ilgili kişilerin ad soyad, adres ve telefon numarası bilgilerinin silinmesi de veri ihlâli olarak değerlendirilmelidir. Bu sebeple, KVKK.m.12/V hükmünde yer alan elde edilme kavramı GVKT.m.4/XII hükmüne paralel bir şekilde geniş yorumlanmalıdır.

Kanunda yer verilen bildirim yükümlülüğü, ihlâlin ağırlığına bakılmaksızın her durum için öngörülmüştür. Örneğin, bir hastane kayıtlarının yanlışlıkla üçüncü

kişilere açıklanmasında, hastane yönetimi ilgili kişilere bildirimde bulunulmasını sağlamalıdır. Ancak, bir üniversite personelinin mezun bilgi sisteminden yanlışlıkla mezunlara ilişkin bilgileri silmesi hâlinde bildirimde bulunulacak mıdır? Bilgilerin mevcut evraklardan sisteme aktarılması imkânı ve silinme sebebiyle ilgili kişilerin temel hak ve hürriyetleri üzerindeki etkileri göz önüne alındığında, bildirimde bulunulmasını beklemek, veri sorumlusu açısından ilgili kişilerin korunma amacını aşacak nitelikte geniş bir sorumluluk doğurur[129]. Bu sebeple, ihlâlin temel hak ve hürriyetler üzerindeki etkisi göz önüne alınarak bildirim sisteminin düzenlenmesi isabetli olur[130].

Bildirim yükümlülüğünün yerine getirilmesinde veri sorumlusunun kusuru önem arz etmez[131]. Diğer bir söyleyişle, veri sorumlusu her türlü tedbiri almakta özenli davranmış olsa dâhi, veri ihlâli hâlinde ilgili kişiye ve Kurula bildirim yükümlülüğü bulunmaktadır. Veri sorumlusu, söz konusu bildirimi en kısa sürede gerçekleştirmelidir. Kurul, Genel Veri Koruma Tüzüğündeki veri ihlal bildirimini düzenleyen hükümleri esas alarak, Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin 24.1.2019 tarihli ve 2019/10 sayılı Kararında[132] en kısa sürenin en geç 72 saat şeklinde yorumlanması gerektiğini ifade etmiştir. Veri sorumlusu bu süreye uymazsa, veri ihlal bildiriminde gecikme sebeplerine de yer vermelidir. Kurul aynı kararda, veri ihlâliyle karşılaşan veri işleyenin bu durumu veri sorumlusuna derhal bildirmesi gerektiğine de yer vermiştir.

C. Veri Sorumluları Siciline Kayıt Yükümlülüğü

Kişisel Verilerin Korunması Kanununun 16 ncı maddesinde, Veri Sorumluları Siciline kayıt yükümlülüğü düzenlenmiştir. Söz konusu yükümlülüğe ilişkin açıklamalardan önce Veri Sorumluları Siciline değinmek gerekir. Veri Sorumluları Sicili, veri sorumlularının kayıt işlemlerini gerçekleştirdikleri ve işleme faaliyetleri

---

129 **Çekin**, Kişisel Veri, s. 112.

130 Kurul, Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin 24.1.2019 tarihli ve 2019/10 sayılı Kararında, ihlalin temel hak ve hürriyetler üzerindeki etkisini göz önüne alacak şekilde hazırlanmış Kişisel Veri İhlâli Bildirim Formuna yer vermiştir. İlgili forma ulaşmak için bkz., https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi# (Erişim Tarihi: 15.2.2019).

131 **Çekin,** Kişisel Veri, s. 112.

132 Karara ulaşmak için bkz., https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi# (Erişim Tarihi: 15.2.2019).

ile ilgili bilgileri beyan ettikleri bir sicildir. Kişisel Verileri Koruma Kurumu Başkanlığı nezdinde tutulan bu sicil, Veri Sorumluları Sicili Bilgi Sistemi (VERBİS)[133] adı verilen internet üzerinden erişim sağlanan bir bilişim sistemi aracılığıyla yönetilmektedir. Her ilgili kişi, VERBİS'e internet üzerinden erişerek, veri sorumluları ile ilgili bilgileri edinebilir. Veri Sorumluları Siciline kayıt yükümlülüğü kapsamında, öncelikle sicile kayıt olma yükümlülüğü bulunan kişileri, bu kişilerin sisteme kayıt başvurusunu ve kayıt bildiriminin içeriğini açıklamaya çalışacağız.

1.Veri Sorumluları Siciline Kayıt Yükümlülüğü Bulunan Kişiler

Kişisel Verilerin Korunması Kanunun 16 ncı maddesinin ikinci fıkrasına göre, kişisel verileri işleyen her gerçek veya tüzel kişi, kişisel verileri işlemeye başlamadan önce VERBİS'e kaydolmak zorundadır. Kişisel Verileri Koruma Kurulu'na, objektif kriterleri göz önüne alarak kayıt yükümlülüğüne istisna getirme yetkisi verilmiştir. Buna göre, Kişisel Verileri Koruma Kurulu, verinin türü, sayısı, işlemenin kanundan kaynaklanması gibi bazı hususları göz önünde bulundurarak VERBİS'e kayıttan muaf tutabilecektir. Kişisel Verileri Koruma Kurulu'nun kararları doğrultusunda, *"herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler; 1512 sayılı Noterlik Kanunu uyarınca faaliyet gösteren noterler; 5253 sayılı Dernekler Kanununa göre kurulmuş derneklerden, 5737 sayılı Vakıflar Kanununa göre kurulmuş vakıflardan ve 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler; 2820 sayılı Siyasi Partiler Kanununa göre kurulmuş siyasi partiler; 1136 sayılı Avukatlık Kanunu uyarınca faaliyet gösteren avukatlar; 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu uyarınca faaliyet gösteren Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler"*[134],

---

133 Bkz., https://verbis.kvkk.gov.tr/ (Erişim Tarihi: 18.8.2018).

134 Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 2.4.2018 tarihli ve 2018/32 sayılı Kararı.

"arabulucular"[135]*, "4458 sayılı Gümrük Kanunu uyarınca faaliyet gösteren gümrük müşavirleri"*[136] *ve "yıllık çalışan sayısı 50'den ve yıllık mali bilanço toplamı 25 milyon TL'den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar"*[137] VERBİS'e kayıt yükümlülüğünden istisna tutulmuştur. Kayıt yükümlülüğünden istisna tutulan veri sorumlularının Kanuna uygun davranma yükümlülüğü ortadan kalkmaz. Bu kişiler, kişisel verilerin işlenmesinde genel ilkelere ve işlenme şartlarına uygun bir şekilde faaliyet göstermek, Kanunda yer verilen diğer yükümlülüklerini yerine getirmek zorundadır.

2. Veri Sorumluları Siciline Kayıt

a. Veri Sorumluları Siciline Kayıt Başvurusu

Sicile kayıtla yükümlü olan bir gerçek veya tüzel kişi, Veri Sorumluları Siciline VERBİS aracılığıyla kayıt olmalıdır. Sistem kayıt yükümlülüğü bulunan veri sorumlularını, yerleşim yeri yurt içinde olan gerçek veya tüzel kişiler, yerleşim yeri yurt dışında olan gerçek veya tüzel kişiler ve kamu kurumları şeklinde gruplandırmıştır. Sicile ilişkin diğer usul ve esasların düzenlendiği Veri Sorumluları Sicili Hakkında Yönetmelik'in[138] 11 inci maddesinde bu grupların sicil başvurusunu nasıl gerçekleştireceği açıklanmıştır.

Yerleşim yeri yurt içinde bulunan gerçek kişiler, bizzat veri sorumlusu olarak kayıt başvurusunda bulunabilir. Tüzel kişiler ise organları aracılığıyla ve tüzel kişilik adına kayıt başvurusunda bulunmalıdır. Tüzel kişilik adına gerek kayıt başvurusu için gerekse Kanundan doğan yükümlülükleri yerine getirmek için bir veya daha fazla kişinin görevlendirilmesi mümkündür. Ancak, bu durumda Kanuna aykırı davranış sebebiyle sorumluluk yine tüzel kişiliğe aittir (VSSHY.m.11/I).

---

135 Arabulucuların Veri Sorumluları Siciline Kayıt Zorunluluğundan İstisna Tutulması ile ilgili Kişisel Verileri Koruma Kurulunun 5.7.2018 tarihli ve 2018/75 sayılı Kararı.

136 Gümrük Müşavirlerinin Sicile Kayıt İstisnası Hakkında Görüş Talebi" ile ilgili Kişisel Verileri Koruma Kurulunun 28.6.2018 tarihli ve 2018/68 sayılı Kararı.

137 Veri Sorumluları Siciline Kayıt Yükümlülüğünden İstisna Tutulacak Veri Sorumluları ile ilgili Kişisel Verileri Koruma Kurulunun 19.7.2018 tarihli ve 2018/87 sayılı Kararı.

138 RG. 30.12.2017, S. 30286.

Yerleşim yeri yurt dışında bulunan gerçek veya tüzel kişi veri sorumlusunun, Veri Sorumluları Siciline kayıt dâhil olmak üzere KVKK.m.11/III[139] hükmünde yer verilen hususları yerine getirmek amacıyla, veri sorumlusu temsilcisi ataması gerekir. Veri sorumlusu temsilcisi olarak yerleşim yeri yurt içinde yer alan tüzel kişi veya Türkiye Cumhuriyeti vatandaşı olan gerçek kişi atanabilir (VSSHY.m.4/I-p).

Ayrıca, söz konusu veri sorumluları sicile kayıtta bir irtibat kişisi belirleyerek sicile bildirirler. *İrtibat kişisi*, ilgili kişilerin veri sorumlusuna yönelteceği taleplerin cevaplandırılması konusunda iletişimi sağlayan kişiyi ifade eder. Veri sorumlusu temsilcisinden farklı olarak irtibat kişisi, mevzuata göre veri sorumlusunu temsile yetkili değildir (VSSHY.m.11/IV).

b. Veri Sorumluları Siciline Kayıt Bildiriminin İçeriği

Kişisel verileri işleyen gerçek veya tüzel kişinin Veri Sorumluları Siciline kayıt yükümlülüğünün bulunduğuna dair tespitten sonra, kayıt yükümlülüğünün yerine getirilmesinde hangi bilgilerin sicile işlenmesi gerektiğinin belirlenmesi gerekir. Kişisel Verilerin Korunması Kanununun 16 ncı maddesi kayıt bildiriminin içeriğini düzenlenmektedir. Buna göre, veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri, kişisel verilerin işlenme amacı, ilgili kişi grupları ve bu grupların işlenen kişisel veri türleri, aktarılacak kişisel veri türü, kişisel verilerin aktarılacağı alıcılar, veri güvenliğine ilişkin tedbirler ve kişisel verilerin muhafaza edileceği süre bildirimin içeriğini oluşturur. Bu bilgilerde bir değişiklik meydana gelirse, bu durum derhâl ve en geç 7 gün içerisinde VERBİS üzerinden Kişisel Verileri Koruma Kurumu Başkanlığına bildirilmelidir (VSSHY.m.13).

---

[139] Veri sorumlusu temsilcisi atanmasına ilişkin kararda VSSHY.m.11/III hükmünde yer verilen asgarî şartların bulunması gerekir. *"a) Kurum tarafından yapılan tebligat veya yazışmaları veri sorumlusu adına tebellüğ veya kabul etme, b) Kurum tarafından veri sorumlusuna yöneltilen talepleri veri sorumlusuna iletme, veri sorumlusundan gelecek cevabı Kuruma iletme, c) Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilerin Kanunun 13 üncü maddesinin birinci fıkrası uyarınca veri sorumlusuna yönelteceği başvuruları veri sorumlusu adına alma ve veri sorumlusuna iletme, ç) Kurul tarafından başkaca bir esasın belirlenmemiş olması halinde; ilgili kişilere Kanunun 13 üncü maddesinin üçüncü fıkrası uyarınca veri sorumlusunun cevabını iletme, d) Veri sorumlusu adına Sicile ilişkin iş ve işlemleri yapma"*.

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN HUKUKA AYKIRI OLARAK İŞLENMESİNE KARŞI KORUMA YOLLARI

§ 8. GENEL OLARAK

Türk hukukunda kişisel verilerin korunmasını talep etme hakkının tanınması, özel veya genel nitelikli hükümlerle korunması sonucunu doğurmuştur. Bu düzenlemeler başında yer alan Anayasa'nın 20 nci maddesinin ikinci fıkrasına göre, bireyler kişisel verilerin korunmasını talep etme hakkına sahiptir. Bu hakkın kullanılmasını sağlamak amacıyla, önceki bölümlerde ayrıntıları ile açıklanan 6698 sayılı Kişisel Verilerin Korunması Kanunundaki hükümlere yer verilmiştir. İlgili kişiye tanınan hakların kullanılmasını sağlamak amacıyla veri sorumlusuna başvuru yolu ve Kişisel Verileri Koruma Kuruluna şikâyet yolu sağlanmıştır.

Öte yandan, Anayasa ile doğrudan doğruya korunan bu hakkın nitelik itibariyle bir kişilik hakkı olması sebebiyle, Türk Medenî Kanunu ve Türk Borçlar Kanununda öngörülen hükümler çerçevesinde korunması mümkündür. Gerçekten, kişiliğin korunmasını düzenleyen Medenî Kanunun 23, 24 ve 25 inci maddeleriyle ve Borçlar Kanununun 49 uncu maddesiyle anılan koruma sağlanır.

Çalışmamızın bu bölümünde, öncelikle, veri sorumlusuna başvuru ve Kurula şikâyet yolları ile kişisel verilerin korunmasının sağlanması açıklanacak, daha sonra kişinin rızasıyla veya rızası dışında gerçekleştirilen ihlâllere karşı korunmasını ve bu korumaya başvurunun temel şartı olan kişisel verilerin işlenmesinde hukuka aykırı fiil (işlem) kavramını ele alacağız. Kişisel verilerin işlenmesinde hukuka aykırılığı ortadan kaldıran hâllere değineceğiz. Hukuka aykırılığı ortadan kaldıran bir sebep bulunmuyorsa, kişisel verilerin kişinin kendi eliyle korunması ve devlet eliyle korunmasına ilişkin ayrımı esas alarak, saldırıya yönelik ve saldırının sonucuna yönelik davalara ilişkin açıklamalara yer vereceğiz.

Son olarak, işçinin kişisel verilerin işlenmesine yol açan uygulamalar ve işçinin kişisel verilerinin korunmasını, daha sonra, kişisel verilerin hukuka aykırı olarak

işlenmesi sebebiyle oluşabilecek suç türlerine Türk Ceza Kanununun ilgili hükümlere değineceğiz.

§ 9. 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU AÇISINDAN KORUMA YOLLARI

I. VERİ SORUMLUSUNA BAŞVURUDA BULUNMA

Kişisel Verilerin Korunması Kanununun 13 üncü maddesine göre, ilgili kişi, kanunun uygulanmasıyla ilgili taleplerini, veri sorumlusuna başvuru yoluyla iletir. Bu durumda, ilgili kişi işlenen kişisel verileri ile ilgili bilgi edinme, düzeltilmesini, silinmesini veya yok edilmesini isteme, işlemeye itiraz etme veya zararın giderilmesini talep etme haklarını veri sorumlusuna başvurarak kullanacaktır.

Veri sorumlusuna başvuru, yazılı olarak veya Kurul tarafından belirlenecek diğer yöntemlerle yapılır. Kurul tarafından belirlenen diğer yöntemlere, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin[1] 5 inci maddesinin birinci fıkrasında yer verilmiştir. Buna göre, kayıtlı elektronik posta adresi (KEP), güvenli elektronik imza, mobil imza aracılığıyla veri sorumlusuna başvuru yapılabilir. İlgili kişinin elektronik posta adresiyle başvuruda bulunması için ise, bu adresinin daha önce veri sorumlusuna bildirilmiş ve veri sorumlusunun sistemine kaydedilmiş olması gerekir. Taleplerin ileri sürülmesi amacıyla yazılım veya uygulama geliştirilmişse, ilgili kişi, bu yollarla da veri sorumlusuna başvurabilir. İlgili kişi başvuruda bulunurken ad soyad gibi zorunlu içeriğin[2] yanında, talep konusuna ilişkin bilgi ve belgeleri de sunar.

İlgili kişinin başvurusunu alan veri sorumlusu, başvuruda yer alan talepleri en kısa sürede sonuçlandırır (KVKK.m.13/II). Bu süre, yazılı başvurularda, başvurunun veri sorumlusuna veya temsilcisine tebliğ edildiği tarihten itibaren, diğer yöntemlerle

---

1 RG. 10.3.2018, S. 30356.

2 Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin 5 inci maddesinin ikinci fıkrasına göre, "Ad, soyad ve başvuru yazılı ise imza, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirime esas elektronik posta adresi, telefon ve faks numarası ve talep konusu" başvurunun zorunlu içeriğini oluşturur.

yapılan başvurularda ise, başvurunun veri sorumlusuna ulaştığı tarihten[3] itibaren otuz günü geçemez. Başvuruya ilişkin işlem, ayrıca bir maliyet gerektirmedikçe[4], ücretsiz olarak sonuçlandırılır. Ayrıca bir maliyet gerektiren durumlarda, başvuru veri sorumlusunun hatasından kaynaklanmışsa, ilgili kişiye ücret iade edilir.

Veri sorumlusu, talebi kabul ederse, bu durumu ilgili kişiye yazılı olarak veya elektronik ortamda bildirir ve talebin gereğini yerine getirir. Talebi kabul etmezse, ilgili kişiye bildirimde bulunurken red gerekçesine de yer verir (KVKK.m.13/III).

II. KİŞİSEL VERİLERİ KORUMA KURULUNA ŞİKÂYETTE BULUNMA

Kişisel Verilerin Korunması Kanununun 13 üncü maddesi çerçevesinde ilgili kişi, veri sorumlusuna başvurduktan sonra, süresi içerisinde başvuruya cevap verilmezse veya verilen cevap yetersiz bulunursa Kurul'a şikâyette bulunabilir (KVKK.m.14). Şikâyet yolu, veri sorumlusu tarafından cevabın öğrenildiği tarihten itibaren otuz, her halükarda, başvuru tarihinden itibaren altmış gün içinde kullanılmalıdır. Bu noktada, Kurul, ilgili kişinin şikâyeti üzerine veya res'en harekete geçebilir. Şikâyet yolu, 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6 ncı maddesinde yer verilen şartlara uygun şekilde kullanılmalıdır. Aksi takdirde, inceleme yapılmaz. İlgili kişi veri sorumlusuna başvuru ve Kurul'a şikâyet yollarını kullanmaksızın genel hükümlere göre tazminat da isteyebilir (KVKK.m.14/III).

İnceleme sonucunda Kurul, Kişisel Verilerin Korunması Kanununun ihlâl edildiği sonucuna varırsa, hukuka aykırılığın giderilmesine karar verir ve bu kararı ilgililere tebliğ eder. Eğer, Kurul, ihlâlin yaygın olduğu sonucuna varırsa, bu konuda ilke kararı yayınlayabilir. Ayrıca, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması hâlinde, veri işlenmesinin veya yurt dışına aktarılmasının durdurulmasına da karar verebilir (KVKK.m.15).

---

3 Bkz., Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ m.5/IV.

4 İşlem herhangi bir maliyet gerektiriyorsa, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğin 7 nci maddesine göre, *"İlgili kişinin başvurusuna yazılı olarak cevap verilecekse, on sayfaya kadar ücret alınmaz. On sayfanın üzerindeki her sayfa için 1 Türk Lirası işlem ücreti alınabilir. Başvuruya cevabın CD, flash bellek gibi bir kayıt ortamında verilmesi halinde veri sorumlusu tarafından talep edilebilecek ücret kayıt ortamının maliyetini geçemez"*.

§ 10. 4271 SAYILI TÜRK MEDENÎ KANUNU AÇISINDAN KORUMA YOLLARI

I. GENEL OLARAK

Kişisel verilerin, hukukî nitelik olarak kişilik hakları içerisinde yer aldığına daha önce değinmiştik. Bu kabul sonucunda, kişisel verilerin, öncelikle, Medenî Kanunun 23 ila 25 inci maddeleri uyarınca kişilik haklarına sağlanan korumadan faydalanması gerektiği ifade edilmelidir. Öğretide ağırlıklı olarak kabul edilen görüşe göre, Medenî Kanunun 23 üncü maddesinde yer alan koruma, kişinin kendi rızasına dayalı olarak üçüncü kişilerden gelebilecek saldırılara karşı; 24 ve 25 inci maddesinde yer alan koruma ise, kişinin rızası dışında üçüncü kişilerden gelebilecek saldırılara karşı öngörülmüştür[5]. Medenî Kanunun 23 üncü maddesinde öngörülen koruma uyarınca, kişisel verilerden tümüyle vazgeçilmesi veya kişisel verilerin hukuka ve genel ahlaka aykırı olarak sınırlandırılması sonucunu doğuracak hukukî işlemler yapılamayacaktır[6]. Bununla birlikte, hukuka ve ahlaka aykırı olmamak kaydıyla, kişisel veriler, örneğin, bir sözleşme konusu yapılabilecektir[7]. Örneğin, kişinin iktisadî bütünlüğüne ilişkin değerlerinden bir veya bir kaçının işlenmesi hususunda bir bilişim uzmanı ile anlaşması geçerlidir.

Buna göre, kişinin rızasına dayalı olarak kişisel verilerin işlenmesindeki sınır Medenî Kanunun 23 üncü maddesine göre belirlenir. Dolayısıyla, kişisel verilerden vazgeçmeyi, onları hukuka ya da ahlaka aykırı olarak sınırlamayı konu alan hukukî işlemler kesin hükümsüzlük yaptırımına tâbi olacaktır. Kişisel Verilerin Korunması Kanunu çerçevesinde öngörülen kişisel verilerin işlenebileceği hâller, kişisel verilerin hukuka uygun olarak sınırlandırılmasına örnek olarak verilebilir. Bununla birlikte, özellikle Amerika'da yaygın olan kişisel veriler üzerindeki mutlak ve tekelci

---

5 Ergun **Özsunay,** Gerçek Kişilerin Hukukî Durumu, 4. Baskı, İstanbul 1979, s. 151; **Zevkliler / Acabey / Gökyayla**, s. 453. Diğer görüşe taraftarları ise, MK.m.23 hükmünün kişinin kendisinden gelebilecek saldırılara karşı koruduğunu, MK.m.24-25 hükmünün ise, hariçten gelebilecek saldırılara karşı koruduğunu savunmaktadır. Bkz., **Ataay,** Şahıslar, s. 148.

6 Aslında, MK.m.23 hükmünde sayılan hususlar, çoğunlukla, Kişisel Verilerin Korunması Kanununun 4 üncü maddesinde öngörülen genel ilkelerde yerini almıştır. Ancak, genel ilkelerde yer verilmemiş olsaydı dâhi, Medenî Kanununun 23 üncü maddesi kapsamında kişisel verilerden açık rıza ile vazgeçilemeyeceğine, hukuka ve genel ahlaka aykırı sınırlandırılamayacağına ulaşılır.

7 **Zevkliler / Acabey / Gökyayla**, s. 455.

haktan vazgeçme karşılığında para ödenmesini içeren sözleşmelerin hukukumuz açısından geçersiz olduğunu söylemek gerekir. Öte yandan, BK.m.26 ile düzenlenen sözleşme özgürlüğü çerçevesinde kişisel verilerin sözleşmeye konu edilmesi, MK.m.23 ve BK.m.27 hükümlerine uygun olmak kaydıyla mümkündür[8]. Eğer, kişisel veriler MK.m.23 hükmünde yer verilen sınırı aşacak şekilde işlenirse, kişilik haklarının rıza dışında yapılan saldırılara karşı korunmasına ilişkin hükümler uygulama alanı bulacaktır.

Çalışmanın asıl konusunu oluşturan ilgili kişinin rızası olmaksızın kişisel verilerin işlenmesi sebebiyle kişilik hakkının ihlâl edilmesinde ise, Medenî Kanunun 24 üncü maddesinde düzenlenen korumaya başvurulması gerekir. Bu hâlde, kişilik hakkı ihlal edilen kimse, Medenî Kanunun 25 inci maddesinde öngörülen davalara başvurarak kişisel verilerinin korunmasını sağlayacaktır. Bu durumda, kişilik hakkını ihlâl eden fiil, temelde haksız fiil teşkil ettiği için Borçlar Kanununun 58 inci maddesi de uygulama alanı bulur[9]. Şüphesiz, ilgili kişi hukuk düzeninin çizdiği sınırlar dâhilinde hakkını kendi eliyle de koruyabilir. Ancak, kişisel verilerin korunması özelinde, ilgili kişinin hakkını kendi eliyle korumasına pek rastlanmaz.

II. VERİ İHLÂLLERİNE KARŞI KİŞİSEL VERİLERİN KORUNMASI

Kişinin rızası dışında yapılan saldırılara karşı korunması, Medenî Kanunun 24 ve 25 inci maddeleri uyarınca sağlanır. Bu hükümler gereğince korumaya başvurulabilmesi için, öncelikle, rıza dışı bir saldırı gerekir. Rıza dışı olma unsuru, rızanın hiçbir şekilde bulunmaması, bulunmasına rağmen geçersiz olması veya sınırlarının aşılması hâlinde söz konusu olur[10]. Bu durumda, Kişisel Verilerin Korunması Kanununda öngörülen açık rızanın alınmaması, aydınlatma yükümlülüğünün yerine getirilmemesi sebebiyle geçersiz olması gibi durumlarda yapılan işlemeler açısından bu unsur sağlanır. Aynı şekilde, geçerli bir şekilde alınan

---

8 Kişisel veri üzerindeki mutlak ve tekelci haktan vazgeçilmeksizin, kişisel verilerin işlenmesini konu alan sözleşmelerde de hukuka aykırı fiille kişilik hakkına saldırıda bulunabilir. Bu durumda yine kişilik hakkını koruyan davalara başvurulabilir. Eğer, kişilik hakkını ihlal etmemekle birlikte, kişisel verilerin işlenmesinde sözleşmeye aykırılık varsa, sözleşmeden doğan sorumluluk hükümlerine başvurulabilmelidir.

9 **Zevkliler / Acabey / Gökyayla,** s. 493.

10 **Ayan / Ayan,** s. 110.

açık rızanın sınırları aşılarak kişisel veriler işlenmişse, rıza dışı olma unsuru sağlanmıştır. Dolayısıyla, kişisel veri ihlâllerinde aşağıda açıklanacak olan koruma yollarına başvurulabilir.

Kişilik hakları temelinde kişisel verilerin korunması, ilgili kişinin eliyle veya devlet eliyle sağlanabilir. Kişisel verilerin ilgili kişi eliyle korumasında hukuka aykırı bir saldırıyı defetmek amacı vardır[11]. Devlet eliyle korunmasını sağlamak için açılan saldırıya yönelik ve saldırının sonucuna yönelik davalarda[12], hukuka aykırı bir saldırının varlığı şarttır. Görüldüğü üzere, hangi hukukî koruma yolu tercih edilirse edilsin, kişisel verilerin korunmasını talep etmek için öncelikle hukuka aykırı bir fiilin (işlemin) bulunması gerekir. Kişisel verilerin hukuka aykırı olarak işlenmesinde, bir fiilden ziyade işleme söz konusu olduğu için işlemin hukuka aykırı olması aranmalıdır.

A. İşlemin Hukuka Aykırı Olması

Hukuka aykırı fiile ilişkin tanıma yer vermek için, öncelikle hukuka aykırılığı açıklayan objektif ve sübjektif teoriye değinmek gerekir. Sübjektif teoriye göre, zarar verenin zarar verici davranışa açıkça yetkili olmaması hâlinde hukuka aykırılıktan bahsedilir[13]. Öğretide hâkim olan objektif teoriye göre ise, hukuka aykırılık, başkasına zarar vermeyi doğrudan veya dolaylı olarak yasaklayan genel bir davranış kuralının ihlâlini ifade eder[14].

Kişisel verilerin korunmasında, saldırının hukuka aykırı olması ile kastedilen, kişisel verilerin hukuka aykırı olarak işlenmesidir. Daha önce de bahsedildiği üzere, kişisel verilerin işlenmesi, kural olarak, hukuka aykırıdır. Bu açıdan genel nitelikli kişisel veriler ile özel nitelikli kişisel veriler arasında bir fark yoktur (KVKK.m.5, 6). Bu hukuka aykırılığın ortadan kalkması için kanunda öngörülen hâllerden birinin bulunması gerekir. Aksi hâlde, kişisel veri üzerinde gerçekleştirilen elde etme,

---

11 **Zevkliler / Acabey / Gökyayla,** s. 491-492.
12 **Zevkliler / Acabey / Gökyayla,** s. 496.
13 **Eren,** s. 585-586.
14 **Eren,** s. 584; Safa **Reisoğlu,** Türk Borçlar Hukuku, Genel Hükümler, 23. Baskı, İstanbul 2012, s. 165.

toplama, arşivleme, aktarma, açıklama gibi her türlü işlem kişisel veri ihlâli niteliğindedir.

Bu noktada, hâkim, öncelikle, verinin kişiyi belirli veya belirlenebilir kılıp kılmadığını tespit edecektir. Daha sonra, kişisel verileri işleme faaliyetini değerlendirecek ve bu işlemenin hukuka aykırılığını ortadan kaldıran sebepleri göz önüne alacaktır. Hâkim bu değerlendirmeyi yaparken, Kişisel Verilerin Korunması Kanununda yer alan hukuka aykırılığı kaldıran sebepleri, kişisel verilerin işlenmesinde esas alınan temel ilkelerle birlikte düşünmelidir. Bir diğer deyişle, hukuka uygunluk sebeplerinin hukuka aykırılığı ortadan kaldırabilmesi için, hukuk düzeninin çizdiği sınırlar dâhilinde kişisel veriler işlenmelidir.

B. Hukuka Aykırılığı Ortadan Kaldıran Hâller

Kişisel verilerin işlenmesinin hukuka aykırı olduğunu tespit ettikten sonra, bu hukuka aykırılığı ortadan kaldıran hâllere değinmek gerekir. Kişisel Verilerin Korunması Kanunu, kişisel verilerin işlenme şartlarını düzenlediği 5 inci ve devamı maddelerinde aslında hukuka aykırılığı ortadan kaldıran hâllere yer vermiştir. Ayrıca, kişisel verilerin işlenmesi, temelde kişilik hakkına saldırı teşkil ettiği için genel hükümlerde yer verilen hukuka uygunluk sebepleri göz önüne alınmalıdır.

Kişisel Verilerin Korunması Kanununda hukuka aykırılığı kaldıran hâllere, 5 ila 9 uncu maddelerinde yer verilmiştir. Söz konusu hükümlere göre, *zarar görenin açık rızası*, *kanunda açıkça öngörülmesi*, *üstün özel yarar*, *üstün kamu yararı*, *sözleşmenin kurulması veya ifası için gerekli olması*, *hukukî yükümlülüğün yerine getirilmesi*, *alenileştirme*, *hakkın tesisi, kullanılması, korunması* ve *veri sorumlusunun meşru menfaatlerinin gerektirmesi* durumlarında kişisel verilerin işlenmesi hukuka aykırı kabul edilmeyecektir. Yeter ki, Kişisel Verilerin Korunması Kanununun genel ilkelerine ve veri güvenliği ilkelerine uygun hareket edilmiş olsun. Aksi hâlde, kişisel verilerin işlenmesinde amaçlanan hukuka uygunluk sebepleri oluşmaz. Örneğin, kişisel verilerin kanunda açıkça öngörülmesine dayalı olarak işlenmesinde, amaçla bağlantılı olmayan veriler elde edilirse, hukuka aykırılık ortadan kalkmaz. Bu durumda, ilgili kişi, MK.m.24 ve 25 inci maddeler uyarınca kişisel verilerinin korunmasını talep edebilmelidir.

Kişilik haklarına yönelik saldırılarda hukuka aykırılığı ortadan kaldıran hâller, Borçlar Kanununun 63 üncü maddesinde düzenlenmiştir. Hükme göre, *hukuk düzeninin verdiği yetkinin kullanılması*, *zarar görenin rızası*, *üstün kamu yararının bulunması* ve *vekâletsiz iş görme* durumlarında kişilik hakkına yönelik saldırılar açısından hukuka aykırılık ortadan kalkar[15]. Ancak, söz konusu durumlarda hukuka aykırılığın ortadan kalkması için her bir hukuka uygunluk sebebini oluşturan şartlara riayet edilmesi gerekir. Örneğin, yetkinin sahibi tarafından sınırı aşılmaksızın kullanılması, geçerli rızanın sınırları dâhilinde kullanılması ve üstün kamu yararına dair sınırlamanın kanunla getirilmesi gerekir[16].

Görüldüğü üzere, genel hükümlerde öngörülen hukuka aykırılığı kaldıran hâller, Kişisel Verilerin Korunması Kanunundaki hâller ile genel itibariyle benzese de iki farklı hüküm bulunmaktadır. Bu durumda, Kişisel Verilerin Korunması Kanununun 5 ila 9 uncu maddelerinde öngörülen hâller özel hüküm olduğu için öncelikle uygulanmalıdır. Öte yandan, Kişisel Verilerin Korunması Kanununda yer verilmeyen hususlar açısından genel hükümlere başvurulması gerekir.

Çalışmamızda, her iki kanunda yer verilen hukuka uygunluk sebeplerine kişisel verilerin işlenmesi başlığında yer verildiği için, söz konusu başlığa atıfla yetiniyoruz. Borçlar Kanununda öngörülmekle birlikte Kişisel Verilerin Korunması Kanununda yer verilmeyen hukuka uygunluk sebepleri de vardır. Özel hukuk tarafından sağlanan yetkinin kullanılması niteliği taşıyan *haklı savunma (meşru müdafaa)*, *zorunluluk (zaruret) hâli* ve *kendi hakkını korumak için kuvvet kullanma* gibi sebepler bu duruma örnek olarak gösterilebilir. Bu durumda, kişisel veriler haklı savunma, zorunluluk hâli ve kendi hakkını korumak için kuvvet kullanma durumlarına dayanılarak işlenebilecek midir? Başka bir söyleyişle, bu durumlar, kişisel verilerin işlenmesi açısından hukuka uygunluk sebebi teşkil edecek midir? Bu soruya cevap verebilmek için öncelikle, her üç sebebin hukuka uygun sayılabilmesi için aranan şartlara değinmek gerekir. Haklı savunma hâlinde, *bir kişinin kendisinin veya başkasının şahısvarlığı veya malvarlığı değerlerine yönelik olarak başlamış ya da*

---

15 Haluk **Tandoğan,** Türk Mes'uliyet Hukuku, 1961 yılı Birinci Baskıdan Tıpkı Baskı, İstanbul 2010, s. 30; **Ayan / Ayan,** Kişiler, s. 112; **Oğuzman / Seliçi / Oktay-Özdemir,** s. 195.

16 **Ayan / Ayan,** Kişiler, s. 113, 117, 119, 120.

başlaması kuvvetle muhtemel bir saldırıyı defetmek amacıyla hareket edilir[17]. Bu hâlde, haklı savunmada bulunan kişi, saldırganın şahısvarlığı veya malvarlığı değerlerine yönelik savunmada bulunabilir (BK.m.64/I). Veri koruma hukuku açısından düşünüldüğünde, bir kişinin şahısvarlığı veya malvarlığı değerlerine saldıran (ilgili) kişiye ilişkin kişisel verilerin işlenmesi yoluyla saldırı fiilinin ortadan kaldırılması pek mümkün görünmemektedir. Zira, bu hâle dayanılarak kişisel verilerin işlenmesi, çoğu durumda saldırıyı defetme amacına hizmet edecek nitelikte değildir. Kişinin kendi hakkını kullanması için kuvvet kullanmasında da benzer bir durum vardır. Zorunluluk hâline dayanılarak yapılan fiilin hukuka uygun olması için ise, sakınılmak istenen tehlikeyle ilgisi bulunmayan üçüncü kişinin sadece malvarlığı değerlerine zarar verilebilir (BK.m.64/II). Bu durumda, zorunluluk hâline dayalı olarak da kişisel verilerin işlenmesi mümkün değildir. Zira, kişisel verilerin işlenmesi hâlinde, *kişisel verilerin hukukî nitelik itibariyle kişilik hakkı olmasının doğal sonucu olarak,* ilgili kişinin temelde şahısvarlığı değerleri ihlâl edilir.

Bu durumda, zorunluluk hâline dayalı olarak kişisel verilerin işlenmesi teorik açıklamalar sebebiyle mümkün değildir. Haklı savunmaya ve kendi hakkını kullanmak için kuvvet kullanmaya dayalı olarak kişisel verilerin işlenmesinin ise, pratik açıdan uygulama alanı bulmayacağı söylenebilir.

C. Öngörülen Hukukî Koruma

1. Genel Olarak

Kişisel verilerin korunmasını talep etme hakkının anayasal bir hak olduğuna daha önce değinmiştik. Bu hakkın korunmasını sağlamak amacıyla Kişisel Verilerin Korunması Kanununda ilgili kişiye tanınan haklar tanınmıştır. Ancak, kişisel verileri hukuka aykırı olarak işlenen ilgili kişinin başvurabileceği ayrıca korumaya yer verilmemiştir. Bu sebeple, Anayasa tarafından öngörülen bu hakkın korunması için genel hükümlerde öngörülen koruma yollarına başvurması mümkündür. Bu koruma yollarına başvuru için, kişisel verilerin işlenmesinin hukuka aykırı olması temel şarttır. Kişilik hakkını ihlâl eden böyle bir işlemle karşılaşan kişinin Medenî

---

17 **Ayan / Ayan,** Giriş, s. 210.

Kanunun 25 inci ve Borçlar Kanununun 58 inci maddesinde öngörülen davaları açması mümkündür. Bununla birlikte, Borçlar Kanununun 63-64 üncü maddesinde öngörülen üç hâlde, kişilik hakkını kendi eliyle de koruyabilir.

2. Kişisel Verilerin Hak Sahibi Eliyle Korunması

İlgili kişinin kendi eliyle kişisel verilerini koruması, haklı savunma, zorunluluk hâli ve kendi hakkını korumak için kuvvet kullanma ile gerçekleşebilir. Bu duruma verilebilecek en güzel örnek, kişinin kendisini ve ailesini görüntülemek isteyen kişiye karşı haklı savunmada bulunmasıdır[18]. Bu durumda, görüntüleyen kişinin fotoğraf makinesinin kırılması veya görüntü almasını engelleyecek basit yaralama fiilleri hukuka uygun kabul edilmelidir. Yine, ilgili kişinin şeref ve haysiyetini zedeleyen haberin ortadan kaldırılması ve gerçek durumun ortaya çıkarılması için, söz konusu muhabirin yalan haberler yayınladığı yönünde ilgili kişinin açıklamalarda bulunması haklı savunma olarak değerlendirilebilir[19].

Günümüzde, kişisel verilerin işlenmesi genellikle bilişim sistemleri aracılığıyla sağlandığı için, verilerin kişinin kendi eliyle korunmasına sık rastlanmamaktadır. Zira, ilgili kişi, çoğu zaman kişisel verilerin işlendiği konusunda bilgi sahibi değildir. Üstelik, kişisel verilerin işlenmesi hazır olmayanlar arasında gerçekleştiği bu durumda, saldırı fiilini defetmek amacıyla yapılabilecekler sınırlıdır. Örneğin, bir kişinin bilgisayarının kamerasına veya mikrofonuna izinsiz giriş yapan saldırganın hukuka aykırı fiilini defetmek amacıyla haklı savunmada bulunabilmek için öncelikle saldırganın kim olduğunu bilmek gerekir. Eğer, saldırganın kim olduğu tespit edilebiliyorsa, izinsiz giriş yaptığı aygıta bağlantı üzerinden virüs gönderilmesi de haklı savunma kapsamında değerlendirilebilmelidir. Bu gibi durumlarda, görüntülenme, görüntünün kaydedilmesi, arşivlenmesi gibi işlemler devam ettikçe, hukuka aykırılık da devam edeceği için ilgili kişinin haklı savunmada bulunabileceği kabul edilmelidir. Ancak, haklı savunmada bu savunma fiilinin hukuka aykırı fiille orantılı olması arandığı için[20], virüs yazılımının sistemin çökmesine sebep

---

18 **Ayan**, Kompüter, s. 83.
19 **Durak,** s. 120.
20 **Ayan / Ayan,** Giriş, s. 211.

olmaksızın, hukuka aykırı fiili ortadan kaldırmaya yönelik olması gerekir. Bir diğer söyleyişle, bu hâllerde kişinin hakkını koruması, hukuk düzeninin sınırları içerisinde kalmalıdır. Aksi hâlde, ilgili kişinin sınırı aşan fiilleri açısından Borçlar Kanununun 49 uncu maddeleri uyarınca sorumluluğu söz konusu olur[21].

3. Kişisel Verilerin Devlet Eliyle Korunması

Kişisel verilerin kişilik hakkının konusu olmasının sonucu, kişilik hakkının korunmasını öngören davalar yoluyla korunmasıdır. Kişilik hakkının devlet eliyle korunması ise, Medenî Kanunun 25 ve Borçlar Kanununun 58 inci maddesinde yer alan *"önleme davası"*, *"saldırıya son verme davası"*, *"tespit davası"*, *"tazminat davaları"* ve *"vekâletsiz iş görmeye dayanan dava"* aracılığıyla sağlanır[22]. Çalışmamızın devamında, saldırıya yönelik davalar başlığında önleme davası, saldırıya son verme davası ve tespit davasına; saldırının sonucuna yönelik davalar başlığında ise, tazminat davaları ve vekâletsiz iş görmeye dayanan davalara değinilecektir.

a. Saldırıya Yönelik Davalar

aa. Önleme Davası

Medenî Kanunun 25 inci maddesinde düzenlenen önleme davası, kişilik hakkı hukuka aykırı saldırıya uğrama tehlikesi içinde bulunan kişinin açabileceği davadır. Bu davayı açabilmek için kişilik hakkına yönelik saldırı fiili gerçekleşmemiştir ancak, gerçekleşmesi kuvvetle muhtemeldir[23]. Kuvvetle muhtemel olan saldırıyı önlemek, engellemek için açılan bu davada failin kusurlu olması aranmaz. Henüz saldırı gerçekleşmediği için zarar da aranmaz. Bu davanın açılması için kişilik haklarına yönelik gerçekleşmesi kuvvetle muhtemel saldırının hukuka aykırı olması yeterli ve gereklidir. Bu sebeple, hukuka uygunluk sebebine dayanılarak kişilik hakkına yönelen saldırılar açısından önleme davası açılamaz[24]. Dava sonucunda

---

21 **Ayan / Ayan**, Giriş, s. 212.

22 **Ayan / Ayan**, Kişiler, s. 123-124. *Dural / Öğüz'e* göre, burada sebepsiz zenginleşme davası da açılabilmelidir. Bkz., **Dural / Öğüz,** s. 160.

23 **Ayan / Ayan**, Kişiler, s. 124.

24 **Ayan / Ayan,** Kişiler, s. 125.

hâkim, gerçekleşmemiş bu saldırının engellenmesi, yasaklanması yönünde karar verir. Önleme davasının açılabileceği süreye ilişkin bir hüküm bulunmamakla birlikte, kişilik hakkına yönelik kuvvetli saldırı ihtimalinin bulunduğu hâllerde önleme davasının açılabileceği kabul edilmektedir[25].

Kişisel verilerin korunması açısından, kişisel verilerin hukuka aykırı olarak işlenme ihtimalinin kuvvetle muhtemel olduğu her hâlde önleme davası açılabilmelidir[26]. Kişisel verileri hukuka aykırı olarak işlemesi kuvvetle muhtemel olan kişilerin belirli olması hâlinde, dava onlara karşı yöneltilmelidir. Örneğin, daha önce yetkisiz kişiler tarafından erişilmeye çalışılan ve kişilerin parmak izlerinin kayıt edildiği bir sistemde güvenlik açığı bulunduğunun tespiti hâlinde önleme davası kime yöneltilecektir? Günümüzde, veri ihlâlini gerçekleştirme ihtimali bulunan kişiler, genellikle bilgisayar korsanı olarak ifade edilen, kimliği belirsiz kişilerden oluştuğu için bu soruya verilecek cevap önem arz eder. Saldırı fiilini gerçekleştirme ihtimali kuvvetle muhtemel olan kişi belirli olmadığı için, davanın veri sorumlusuna yöneltilmesi düşünülebilir. Zira, kişisel verilerin hukuka aykırı olarak açıklanması, aktarılması kişisel veri işleme faaliyetlerindendir. Veri sorumlusunun bu duruma kastı veya ihmaliyle sebebiyet vermiş olması da önem taşımaz. Dava sonucunda verilecek karar ise, kişisel verilerin hukuka aykırı olarak işlenmesinin yasaklanmasını içerecektir[27]. Üstelik, ilgili kişi, Medenî Kanunun 25 inci maddesinin ikinci fıkrası gereği, bu durumun yayımlanmasını talep ederek, belirli olmayan üçüncü kişilere karşı da önleme davasının hüküm doğurmasını sağlayabilir.

bb. Saldırıya Son Verme Davası

Medenî Kanunun 25 inci maddesinin birinci fıkrasında öngörülen bir diğer dava, saldırıya son verme davasıdır. Bu dava, kişilik hakkına yönelik başlamış olan saldırıya son verilmesi için açılır. Bu sebeple, saldırının henüz başlamadığı veya sona erdiği hâllerde, saldırıya son verme davası açılamaz[28]. Davanın açılmasında, kişilik

---

25 **Ayan / Ayan,** Kişiler, s. 125.
26 **Özdemir,** s. 190.
27 **Özdemir,** s. 191.
28 **Ataay,** s. 151; Necip **Kocayusufpaşaoğlu,** Borçlar Hukuku Genel Bölüm, C. 1, İstanbul 2010**,** s. 151.

hakkına yönelik saldırının hukuka aykırı olması yeterlidir[29]. Saldırıya son verme davasının açılabilmesi için failin kusurlu olması veya saldırının sonucunda zararın meydana gelmesi aranmaz. Öte yandan, fail kusurluysa ve saldırı sebebiyle zarar meydana gelmişse saldırıya son verme davasıyla birlikte, tazminat davası da açılması mümkündür[30].

Kişisel verilerin korunması açısından, saldırıya son verme davası kişisel verilerin hukuka aykırı olarak işlenmesi sonucunu doğuran durumlarda söz konusu olacaktır[31]. Kişiye ilişkin veriler kanunda öngörülmeyen bir sebebe dayanılarak işlenmişse saldırıya son verme davası açılabilecektir. Kişisel veriler başlangıçta doğru kayıt edilmekle birlikte, durumun değişmesi sebebiyle eksik veya yanlış hâle gelmişse güncelleme noktasında direnen veri sorumlusuna karşı yine söz konusu dava açılabilmelidir[32]. Dolayısıyla, bu davanın açılması için kişisel verilerin işlenmesinin baştan itibaren hukuka aykırı olması ile sonradan hukuka aykırı hâle gelmesi arasında fark yoktur. Örneğin, bir işletmenin kampanyalarından haberdar olmak için rıza vermeyen kişi ile verdiği rızayı geri alan kişiye gönderilen bilgilendirme mesajları sebebiyle de saldırıya son verme davası açılabilecektir. Saldırıya son verme davasında hâkim, kişisel verilerin hukuka aykırı olarak işlenmesine son verilmesi yönünde ve gerektiğinde kişisel verilerin silinmesi veya yok edilmesi yönünde karar verecektir[33]. Örneğin, dava kişisel verilerin eksik veya yanlış tutulması sebebiyle açılmışsa, kişisel verilerin tamamlanması veya yanlışlığın giderilmesi yönünde karar verilecektir. Dava, kanunda öngörülmeyen bir sebebe dayanılarak kişisel verilerin işlenmesine son verilmesi sebebiyle açılmışsa, hüküm saldırıya son verme ve işlenen kişisel verilerin silinmesine veya yok edilmesine ilişkin kararı içermelidir.

Kişisel veriler açısından saldırıya son verme davasıyla öngörülen korumaya ulaşmak için, Kişisel Verilerin Korunması Kanununda ilgili kişiye bazı haklar

---

29 Saldırıya son verme davasında hukuka aykırı fiile ek olarak, saldırının durdurulmasının mümkün olmasının da aranması gerektiğine ilişkin bkz., Ahmet, **Kılıçoğlu,** Borçlar Hukuku, Genel Hükümler, 18. Baskı, Ankara 2014, s. 208. Ayrıca bkz**., Özdemir,** s. 194.

30 **Zevkliler**, Gerçek Kişiler, s. 350; **Ayan / Ayan**, Kişiler, s. 126.

31 **Özdemir,** s. 193.

32 **Ayan**, Kompüter, s. 91.

33 **Özdemir,** s. 194, 195.

tanınmıştır. Gerçekten, Kişisel Verilerin Korunması Kanununun 11 inci maddesinde öngörülen kişisel verilerin düzeltilmesini, silinmesini ve yok edilmesini talep etme veya işlemeye itiraz etme hakkının kullanılmasıyla hukuka aykırı işlemenin önüne geçilebilir. Bununla birlikte, MK.m.25 kapsamında kişisel verilerin işlenmesi sebebiyle saldırıya yönelik davaların açılması ile KVKK.m.11 hükmünde öngörülen hakların kullanımı açısından bazı farklılıklar söz konusudur. İlk olarak, Kişisel Verilerin Korunması Kanunu kapsamında hakların kullanımı veri sorumlusuna başvuru yoluyla gerçekleştirilebilirken, MK.m.25 hükmüne göre saldırının sona erdirilmesine ilişkin talep dava yoluyla ileri sürülmelidir. Ayrıca, MK.m.25 hükmüne göre, saldırıya son verme davası açılabilmesi için kişisel verilerin hukuka aykırı olarak işlenmesi şartken, kişisel verilerin düzeltilmesini, silinmesini veya yok edilmesini talep etmek için ya da işlemenin aleyhe sonuç doğurmasına itiraz etmek için hukuka aykırılık unsuru her durumda aranmaz. Örneğin, işçinin evlenmesi hâlinde evli olduğuna dair bilginin işlenmesini (düzeltilmesini) işverenden talep etmesi, hukuka uygun işleme hâlinde gerçekleşir. Bu durumda, işvereni güncel durum ile ilgili bilgilendirme amacı da güdülür. Benzer şekilde, itiraz etme hakkı, kişisel verilerin hukuka uygun olarak işlenmesi esnasında *otomatik yöntemlerle analiz edilmesi sebebiyle ilgili kişi aleyhine sonuç doğmasına itiraz edilmesi* söz konusudur. Son olarak, ilgili kişi, Kişisel Verilerin Korunması Kanunu kapsamında kişisel verilerin düzeltilmesine, silinmesine veya yok edilmesine ilişkin durumun, *kişisel verilerin aktarıldığı kişilere bildirilmesi*ni sağlayabilir. İlgili kişi, bu durumun (aktarılan kişi dâhil olmak üzere) üçüncü kişilere bildirilmesini, yayımlanmasını Medenî Kanunun 25 inci maddesinin ikinci fıkrasıyla da sağlayabilecektir. Hükme göre, "*Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir*". Bu durumda, düzeltmeye ilişkin bildirimin yapılmasına veya kararın yayımlanmasına ilişkin gereklilik hâkim tarafından takdir edilecektir.

cc. Tespit Davası

Kişilik hakkına yönelik saldırılar karşısında açılabilecek bir diğer dava, tespit davasıdır. Bu dava, kişilik hakkına yönelik bir saldırının varlığının mahkeme kararıyla belirlenmesi amacıyla açılır[34]. Bu davanın açılması için kusur ve zarar aranmaz. Ancak, hukuka aykırı saldırıya ek olarak, saldırının tespitinde hukukî yararın varlığı ve ispat edilmesi şarttır[35]. Hâkim, bu dava sonucunda hukuka aykırı saldırının varlığının tespiti ile yetinir. Bir diğer söyleyişle, tespit davası sonucunda verilen karar eda hükmü içermez. Tespit davası, niteliği gereği saldırı başladıktan sonra açılır. Bununla birlikte, saldırının sona ermesi hâlinde saldırının tespitinin talep edilip edilemeyeceği hususunda görüş birliği yoktur. Bir görüşe göre[36], saldırının tamamlanması hâlinde, tespit davası açılabilmelidir. Bu görüş, temelini, sona ermesine rağmen etkileri devam eden saldırının hukuka aykırılığının tespitine müsaade eden Medenî Kanunun 25 inci maddesinin birinci fıkrasından almaktadır. Bu görüş taraftarlarına göre, sona eren saldırının etkilerinin tespiti, hukuka aykırı saldırıyı gerçekleştiren kişilerin kusursuz olması hâlinde önem arz eder. Zira, bu hâlde, kusuru temel şart olarak öngören tazminat davaları açılamayacaktır. Bu durumda, kusurun aranmadığı davalardan olan tespit davasının açılması mümkün olmalıdır. Diğer görüşe göre[37] ise, saldırı sona erdikten sonra tespit davasının açılamaması gerekir. Zira, sona eren bir saldırının ardından tespiti talep edilecek konu ortadan kalkmıştır.

Kişisel verilerin korunması açısından, kişisel verilerin hukuka aykırı olarak işlendiğinin tespiti, Kişisel Verilerin Korunması Kanununun 11 inci maddesinde düzenlenen bilgi edinme hakkı çerçevesinde sağlanabilir. Bununla birlikte, hukuka aykırı saldırının tespitinde hukukî yararı olan ilgili kişi, tespit davası da açabilmelidir. Örneğin, kişisel verilerinin işlenip işlenmediğini öğrenmek isteyen kişi veri sorumlusuna başvurmasına rağmen cevap alamamışsa veya aldığı cevap yetersiz kalıyorsa kişisel verilerinin işlendiğinin tespitini hâkimden talep edebilmelidir. Veri

---

34 **Ayan / Ayan,** Kişiler, s. 126.
35 **İmre**, Giriş, 456, **Ayan**, Kompüter, s. 88.
36 **Ayan / Ayan,** Kişiler, s. 127.
37 **Dural / Öğüz**, s. 155.

sorumlusunun aldığı tüm tedbirlere rağmen, veri kayıt sistemindeki bilgilerin üçüncü kişiler tarafından elde edilmesi hâlinde tespit davası açılabilecektir. Şüphesiz, ilgili kişi, bu durumlarda Kurula şikâyet yoluna da başvurabilir.

b. Saldırının Sonucuna Yönelik Davalar

aa. Tazminat Davası

Kişilik hakkına yönelik hukuka aykırı bir saldırı sonucu ortaya çıkan zararın giderilmesi gerekir[38]. Zararın giderilmesi yönündeki talebin temeli, Medenî Kanunun 24-25 inci ve Borçlar Kanununun 49 uncu maddesine dayanmaktadır. Bu amaçla açılacak tazminat davası, kişilik hakkına yönelik saldırı sonucunda ortaya çıkan zararın karşılanmasını öngören bir alacak davası niteliğindedir[39]. Hukuka aykırı fiille kişinin malvarlığı üzerinde meydana gelen zararlar açısından maddî tazminat davası, şahısvarlığı üzerinde meydana gelen zararlar açısından manevî tazminat davası açılabilir.

1995/46 sayılı Yönergenin 23 üncü maddesinin birinci fıkrasına göre, bu yönerge uyarınca kabul edilen ulusal mevzuata aykırı olarak kişisel verilerin işlenmesi sebebiyle zarara uğrayan ilgili kişi, veri sorumlusundan tazminat almaya hak kazanır. İkinci fıkrasında ise, veri sorumlusuna sorumluluktan kurtulma imkânı getirilmiştir. Buna göre, veri sorumlusu zarardan sorumlu olmadığını ispat ederse, kısmen veya tamamen sorumluluktan kurtulabilecektir. Genel Veri Koruma Tüzüğünün 82 inci maddesinde de benzer bir tazmin borcuna yer verilmiştir. Kişisel Verilerin Korunması Kanunu açısından zararın giderilmesi hususunda ayrı bir dava yolu öngörülmemiş, genel hükümlere atıfla yetinilmiştir (KVKK.m.14/3). Bu sebeple, Medenî Kanunun 25 inci ve Borçlar Kanununun 49 uncu maddeleri çerçevesinde tazminat davalarına ilişkin hükümler değerlendirilecektir.

aaa. Tazminat Davasının Şartları

Kişilik hakkı saldırıya uğrayan kişiler, Medenî Kanunun 25 inci maddesinin üçüncü fıkrasına göre, maddî ve manevî tazminat isteminde bulunabilirler. Bu

---

38 **Kocayusufpaşaoğlu**, s. 152; **Zevkliler / Acabey / Gökyayla**, s. 475.
39 **Ayan**, Kişiler, s. 128.

davaların açılabilmesi için genel haksız fiil sorumluluğuna ilişkin (BK.m.49) şartlar aranmaktadır. Borçlar hukukuna hâkim olan ilkelerden kusur sorumluluğu ilkesi[40] gereği, kusura dayanan sorumluluk hükümleri çerçevesinde tazminat davası açılabilmesi için gereken şartlara yer vereceğiz. Bu durumda, kişilik hakkına yönelik bir saldırı sonucunda ortaya çıkan zararın giderilmesi istemi için, *fiilin hukuka aykırı olması*, *failin kusurlu olması*, *zarar meydana gelmiş olması* ve *illiyet (nedensellik) bağının bulunması* gerekir. Kusursuz sorumluluk hâllerinde ise, kusur bir şart olarak aranmayacaktır.

i. Fiilin Hukuka Aykırı Olması

Haksız fiil sorumluluğuna gidilebilmesi için ilk şart, *fiilin hukuka aykırı olması*dır. Daha önce değinildiği üzere, fiile ilişkin hukuka aykırılık, kişilik hakkını doğrudan veya dolaylı olarak korumayı amaçlayan emredici hukuk kurallarına aykırılık şeklinde ortaya çıkar. Kişisel verilerin işlenmesinin kural olarak hukuka aykırı olduğu düşünüldüğünde, kanunda öngörülmeyen sebeplere dayanılarak yapılan işlemeler açısından bu şart oluşacaktır. Öte yandan, kişisel verilerin hukuka aykırılığı kaldıran sebeplerle birlikte kanun hükümlerine uygun bir şekilde işleniyorsa, hukuka aykırılıktan bahsedilemeyecektir. Hukuka aykırı fiili doğuran davranışlarda olduğu gibi kişisel verilerin hukuka aykırı işlenmesi de, yapma veya yapmama şeklinde ortaya çıkabilir[41]. Kişisel verilerin işlenmesinde genellikle *"yapma"*yı içeren davranışlar ile karşılaşılır. Zira, yapmamaya ilişkin davranışın hukuka aykırı nitelik taşıyabilmesi için, hukuk kurallarının yapmaya ilişkin bir görev yüklemesi gerekir[42]. Kişisel Verilerin Korunması Kanununun kişisel verilerin işlenmesinde uyulması gereken genel ilkelerini düzenleyen 4 üncü maddesi, yapmaya ilişkin görev yükleyen hukuk kuralına örnek verilebilir. Gerçekten, kişisel verilerin doğru ve gerektiğinde güncel olmasını öngören ilke bağlamında, kişisel verilerin güncel bir şekilde işlenmemesi de hukuka aykırılığı doğuracaktır. Ancak, tazminat istemi için diğer şartların da gerçekleşmesi gerekir.

---

40 **Ayan**, Borçlar, s. 38.
41 **Oğuzman / Öz**, II, s. 13.
42 **Ayan**, Borçlar, s. 251.

ii. Failin Kusurlu Olması

Sorumluluğun ikinci unsuru, *failin kusurlu olması*dır. Tanımına kanunda yer verilmediği için kusur, öğretide iki şekilde tanımlanmıştır. Buna göre, kusur, hukuk düzeni tarafından hoş görülmeyen, kınanması gerektiği ifade edilen davranıştır[43]. Diğer tanıma göre, kusur, hukuka aykırı sonucu isteyen veya istememekle birlikte hukuka aykırı davranıştan kaçınmak için iradesini yeterince kullanmamış kişinin davranış biçimidir[44]. Kusura ilişkin ikinci tanım, kusurun dereceleri olarak ifade edilen kast ve ihmal göz önüne alınarak yapılmıştır. Buradan yola çıkarak kastta, failin hukuka aykırı sonucu bilmesinden ve istemesinden bahsedilir[45]. İhmalde ise, failin hukuka aykırı sonucu istememekle birlikte, bu sonucun meydana gelmemesi için şartların gerekli kıldığı özeni göstermemesinden söz edilir[46]. Bununla birlikte, kusur sorumluluğunda kast veya ihmal sorumluluğu etkilemez, sadece tazminatın hesaplanmasında dikkate alınır (BK.m.51/I).

Öte yandan, kişisel verilerin hukuka aykırı olarak işlenmesi sebebiyle ortaya çıkan zararlarda failin kusurunun aranıp aranmayacağı hususunda görüş birliği yoktur. Daha önce değinildiği üzere, mehaz 1995/46 sayılı Yönergenin 23 üncü maddesinin birinci fıkrasında ise, zararın giderilmesi gerektiği ve veri sorumlusunun zarardan sorumlu olmadığını ispat etmesi hâlinde bu zarardan muaf tutulacağı ifade edilmiştir. Görüldüğü üzere, 1995/46 sayılı Yönergede de açıkça bir sorumluluk türüne yer verilmemiştir. Bir görüşe göre, burada kusur sorumluluğuna ilişkin hükümler uygulanmalıdır. Bu görüşü savunanlara göre, 1995/46 sayılı Yönergede herhangi bir belirlemede bulunulmayarak bu sorumluluğun türünün belirlenmesini üye ülkelerin iç hukukuna bırakmıştır[47]. Türk hukukunda ise, kusur sorumluluğu kural, kusursuz sorumluluk istisnaidir[48]. Bu sebeple, herhangi bir belirlemede bulunulmadığı için kişisel verilerin işlenmesinden doğan zararlar, kusura dayanan

---

43 **Oğuzman / Öz**, II, s. 55; **Eren**, s. 569; **Kılıçoğlu**, s. 200.

44 Hüseyin **Hatemi** / Emre **Gökyayla,** Borçlar Hukuku, Genel Bölüm, 3. baskı, İstanbul 2015, s. 146; **Oğuzman / Öz**, II, s. 55; **Eren**, s. 569-570; **Kılıçoğlu**, s. 200; **Tandoğan**, s. 45.

45 **Ayan**, Borçlar, s. 272; **Hatemi / Gökyayla**, s. 146; **Oğuzman / Öz**, II, s. 56; **Eren**, s. 574; **Kılıçoğlu**, s. 202.

46 **Ayan**, Borçlar, s. 273; **Hatemi / Gökyayla**, s. 147; **Oğuzman / Öz**, II, s. 56; **Eren**, s. 576.

47 **Özdemir,** s. 215; **Ayözgör Öngün,** s. 269, dn. 176.

48 **Oğuzman / Öz**, II, s. 138; **Hatemi / Gökyayla**, s. 149; **Ayan**, Borçlar, s. 250.

sorumluluk çerçevesinde talep edilecektir[49]. Ayrıca, 1995/46 sayılı Yönergenin 23 üncü maddesinin ikinci fıkrası ile veri sorumlusuna zararlı sonuçtan sorumlu olmadığını ispatlama yetkisi verilmesinin kusur sorumluluğuna işaret ettiği ifade edilmiştir.

Diğer görüşe göre, kusursuz sorumluluğa ilişkin hükümler uygulanmalıdır. Bu görüş taraftarları da kusursuz sorumluluğun bir özen sorumluluğu mu yoksa bir tehlike sorumluluğu mu olduğu noktasında ikiye ayrılmaktadır. Özen sorumluluğunu savunanlara göre, veri sorumlusu, veri güvenliğini sağlamaya yönelik tedbirleri almakla sorumluluktan kurtulur[50]. Bir diğer deyişle, gerekli tedbirleri alan veri sorumlusu neticeden sorumlu tutulamamalıdır. Aksi hâlde, veri sorumlusunu tedbir almakla yükümlü kılınması bir anlam ifade etmeyecektir[51]. Tehlike sorumluluğu görüşü taraftarlarına göre ise, 1995/46 sayılı Yönergenin 23 üncü maddesinde açıkça kusur şartına yer verilmemesinin kusursuz sorumluluğu haklı kıldığı ifade edilmektedir[52]. Ancak, bu belirleme tek başına yetersiz olacaktır. Zira, Türk hukukunda kusursuz sorumluluk hâlleri istisnaî nitelik taşır. Hatta, bazı yazarlara göre, kusursuz sorumluluk hâllerinin kanunda açıkça öngörülmesi gerekir[53].

Kusursuz sorumluluk, temelde teknolojik gelişmeler karşısında kusurun ispatının zorluğu sebebiyle öngörülmüştür. Kişisel verilerin işlenmesi açısından, verilerin işlenmesinin kişilik hakkı üzerinde yarattığı tehlike sebebiyle kusursuz sorumluluk hâline yer verilmesi gerekir[54]. Mehaz 1995/46 sayılı Yönergenin 55 inci paragrafında yer verilen ifade de bu durumu destekler niteliktedir. Söz konusu ifadeye göre, kişisel verileri hukuka aykırı olarak işleyen veri sorumlusu, ilgili kişinin maruz kaldığı zararlardan sorumludur. Veri sorumlusu, mücbir sebebin veya ilgili kişinin (zarar görenin) kendi kusurunun varlığını ispatlarsa sorumluluk ortadan

---

49 **Ayözger Öngün**, s. 269; **Taştan,** s. 182, dn. 556; Damla **Gürpınar,** Kişisel Verilerin Korunamamasından Doğan Hukukî Sorumluluk, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Şeref Ertaş'a Armağan-I, C. 19, Özel Sayı, 2017, s. 690.

50 **Çekin,** Kişisel Veri, s. 105.

51 **Çekin,** Kişisel Veri, s. 105, dn. 227.

52 **Başalp,** Veri, s. 66.

53 **Oğuzman / Öz,** II, s. 7.

54 **Ayan,** Kompüter, s. 112.

kaldırılabilir[55]. Görüldüğü üzere, burada veri sorumlusu açısından sorumluluğu ortadan kaldıran, veri sorumlusunun kusurunun olmadığını değil, illiyet bağının kesildiğini ispatlamasıdır[56]. Türk hukukunda da tehlike sorumluluğunu doğuran, tehlikeli işletme ile zarar arasında illiyet bağının bulunmasıdır[57]. Veri sorumlusunun sorumluluktan kurtulması için tek yol illiyet bağının kesilmesidir[58]. Tüm bu sebeplerle, kişisel verilerin işlenmesinden doğan sorumluluk, tehlike sorumluluğu olarak değerlendirilmelidir.

iii. Zararın Meydana Gelmiş Olması

Sorumluluğun üçüncü unsuru, *zararın meydana gelmiş olması*dır. Haksız fiil sorumluluğuna gidilebilmesi için zorunlu unsur, bir zararın meydana gelmiş olmasıdır. Zarar ise, şahısvarlığı ve malvarlığı değerlerinde irade dışı azalma olarak ifade edilebilir[59]. Malvarlığında meydana gelen irade dışı azalmalar maddî zararı, şahısvarlığında meydana gelen irade dışı azalmalar ise, manevî zararı ifade eder. Kişisel verilerin işlenmesi sebebiyle ortaya her iki zarar türü de çıkmakla birlikte, manevî zararlara daha sık rastlanmaktadır. Örneğin, kişinin borçlarının açıklanması sebebiyle işlerindeki azalma maddî zarara, duyduğu üzüntü ise manevî zarara örnek verilebilir.

iv. İlliyet Bağının Bulunması

Sorumluluğun son unsuru, *illiyet (nedensellik) bağının bulunması*dır. İlliyet bağı, zarar ile zarara sebebiyet veren olay arasında sebep sonuç ilişkisini ifade eder. Bununla birlikte, öğretide, zarara sebebiyet veren her türlü olayın illiyet bağı açısından sebep sayılamayacağı kabul edildiği için sorumluluğu sınırlandıran uygun illiyet bağı teorisi tercih edilmiştir[60]. Uygun illiyet bağı ise, hayatın normal akışı ve

---

55 Veri sorumlusunun tazminat sorumluluğunda, illiyet bağını kesen sebeplerden üçüncü kişinin ağır kusuruna yer verilmemiştir. Böylece, genellikle, veri sorumlusunun muhafazası altındayken üçüncü kişiler tarafından gerçekleştirilen veri ihlâlleri, veri sorumlusunun sorumluluğunu ortadan kaldırmayacaktır. Bkz., **Gürpınar,** s. 692-693.

56 **Başalp**, Veri, s. 66, 67.

57 **Eren,** s. 617 vd..

58 **Ayan,** Borçlar, s. 299.

59 **Oğuzman / Öz**, II, s. 38; **Eren,** s. 520.

60 **Tandoğan,** s. 76 vd..; **Eren,** s. 540.

hayat tecrübelerine göre, sonucu meydana getirmeye elverişli şart ile sonuç arasındaki bağı ifade eder[61].

Bu durumda, veri sorumlusunun haksız fiil sorumluluğundan bahsedebilmek için, kişisel verilerin hukuka aykırı olarak işlenmesi ile ilgili kişinin zararı arasında uygun illiyet bağı bulunmalıdır[62]. Başka bir ifadeyle, ilgili kişinin zararı, hukuka aykırı işlemenin normal sonucu olmalıdır. Öte yandan, ilgili kişinin zararı, hukuka aykırı birden fazla işlemenin sonucu da olabilir. Bu durum, bütün sebeplerin bir araya gelerek zararlı sonucu gerçekleştirmeye elverişli olmaları (ortak illiyet) veya her sebebin tek başına zararlı sonucu gerçekleştirmeye elverişli olması şeklinde ortaya çıkabilir[63]. Örneğin, kişinin önceden çalıştığı şirketin, dernek üyeliği bilgisini hâlihazırda çalışılan şirkete hukuka aykırı olarak aktardığını düşünelim. Çalışanının fikirleri hakkında şüpheye düşen yeni şirket, kişinin din bilgisiyle dernek üyeliği bilgisini birleştirerek yaptığı değerlendirmeler sonucunda ilgili kişiyi işten çıkarmışsa ortak illiyet bağının varlığından söz edilebilir. Aynı şirketin, din bilgisi veya dernek üyeliğine ilişkin bilginin herhangi birine dayanarak ilgili kişiyi işten çıkarması ise, her sebebin tek başına zararlı sonucu gerçekleştirmeye elverişli olmasına örnek verilebilir.

İlliyet bağı, gerek kusura dayanan gerekse kusura dayanmayan haksız fiil sorumluluğu için olmazsa olmaz bir unsurdur. Bu unsuru ortadan kaldıran, bir diğer deyişle illiyet bağını kesen hâller ise mücbir sebep ve zarar görenin ağır kusurundan ibarettir. Mücbir sebep öğretide, sorumlu veya borçlunun faaliyeti ve işletmesi dışında meydana gelen, genel bir davranış normunun veya borcun ihlâline mutlak ve kaçınılmaz bir şekilde sebep olan, öngörülmesi veya kaçınılması mümkün olmayan olağanüstü olay şeklinde tanımlanmaktadır[64]. Kişisel verilerin işlenmesi açısından, depremde göçük altında kalan ilgili kişilere ilişkin verilerin işlenmesi mücbir sebebe örnek verilebilir. Bir kişinin elektronik posta hesabına girişte internet güvenliğini sağlamaması veya zararlı yazılımları önlemeye yönelik programları kullanmaya

---

61 **Eren**, s. 541; **Oğuzman / Öz**, II, s. 45; **Hatemi / Gökyayla**, s. 137; **Kılıçoğlu**, s. 215; **Ayan,** s. 283.

62 **Özdemir,** s. 211.

63 **Ayan,** Borçlar, s. 283-284.

64 **Eren**, s. 557; **Kılıçoğlu,** s. 220.

dikkat etmemesi sonucunda ortaya çıkan zararlarda, zarar görenin kusuru olduğu söylenebilir[65].

bbb. Tazminat Davasının Türleri

i. Maddî Tazminat Davası

Kişisel verilerin işlenmesinden doğan maddî zararın giderilmesine ilişkin talebin hukukî dayanağını 1995/46 sayılı Yönergenin 23 üncü maddesinin birinci fıkrasına ek olarak KVKK.m.14/III ve GVKT.m.82 hükmü oluşturmaktadır. KVKK.m.14/III hükmünün genel hükümlere yaptığı atıf gereği, Medenî Kanunun 25 inci maddesinin üçüncü fıkrasında öngörülen maddî tazminat davası açılabilecektir. Öte yandan, kişilik hakkına saldırı sebebiyle uğranılan zararı giderme amacıyla açılan maddî tazminat davası, Borçlar Kanununun 49 uncu ve devamı maddelerinde düzenlenen maddî tazminat davası ile benzerdir. Bu sebeple, bu davanın açılmasında haksız fiile ilişkin *"fiilin hukuka aykırı olması", "zararın meydana gelmiş olması"* ve *"uygun illiyet bağının bulunması"* şartları aranacaktır[66].

Maddî tazminat davası ile kişilik hakkının ihlâli sebebiyle malvarlığında meydana gelen irade dışı azalmanın giderilmesi amaçlanmaktadır[67]. Kişisel verilerin işlenmesi sebebiyle malvarlığında meydana gelen azalma, malvarlığının fiilen azalması (fiilî zarar) veya malvarlığının artması gerekirken artmaması (mahrum kalınan kâr - kazanç kaybı) şeklinde ortaya çıkabilir[68]. Bir kişinin telefon konuşmalarının yayınlanması sebebiyle, intihara kalkışması sonucunda ortaya çıkan tedavi masrafları veya fizikî yahut ruhsal sağlığının bozulması fiilî zarar olarak nitelendirilebilir[69]. Bir kişinin cinsel tercihine ilişkin bilginin yayınlanması sebebiyle işten çıkarılması veya iş bulamamasında ise, mahrum kalınan kâr söz konusudur[70].

---

65 Benzer bir karar için bkz., 4.HD. 4.3.2004, E.2003/12313 K.2004/2672 (Kazancı İçtihat Bilgi Bankası, www.kazanci.com, Erişim Tarihi: 14.01.2019). İlgili kişinin alması gereken bazı önlemler için bkz., **Açıkgöz,** s. 414-420.

66 Söz konusu şartlara ilişkin açıklamalara ve kusura ilişkin değerlendirmelere ulaşmak için bkz.,

67 **Tandoğan**, s. 315; **Eren**, s. 729;

68 **Kılıçoğlu**, s. 210; **Ayan**, Borçlar, s. 216.

69 **Özdemir,** s. 219.

70 **Ayan,** Kompüter, s. 95.

Kişisel verilerin hukuka aykırı şekilde işlenmesi sebebiyle, nadiren de olsa beden bütünlüğüne ilişkin bir zarar ortaya çıkmışsa maddî tazminat davası açılabilir. Örneğin, gerçekte böyle bir hastalığa sahip olmamasına rağmen, kişinin bulaşıcı hastalığa sahip olduğuna dair bilginin sisteme kaydedilmesi hâlinde, kişinin maruz kaldığı tedaviler de hukuka aykırı hâle gelecektir. Yahut, ilgili kişinin gizli tanık olarak yer aldığı bir davada, kişisel verilerinin gereği gibi korunamamasını fırsat bilen sanık gizli tanığa ilişkin bilgilere ulaşarak onun beden bütünlüğünü ihlâl edici davranışlarda bulunabilir. Bu durumda, kişisel verilerin hukuka aykırı işlenmesi sebebiyle zarar ortaya çıkar. İlgili kişi, fiziksel veya ruhsal sağlığının bozulması sonucu ortaya çıkan tedavi giderlerini, o süreçte çalışamaması sebebiyle mahrum kaldığı kârı talep edebilecektir (MK.m.54). Bu durumda, beden bütünlüğünü ihlâl eden fiil sonucu, manevî tazminata da karar verilebilir (MK.m.56).

Zarar gören ilgili kişi, açtığı maddî tazminat davasında kişisel verilerin işlenmesinin hukuka aykırı olduğunu, zararı ve hukuka aykırı fiille zarar arasındaki illiyet bağını ispatlayacaktır (MK.m.6 ve BK.m.50/I). Kişisel verilerin işlenmesi sebebiyle ortaya çıkan sorumluluğun kusura dayanan sorumluluk olduğu kabul ediliyorsa, kusurun da ispatı gerekir. Medenî Kanunun 50 nci maddesinin ikinci fıkrasına göre, zarar gören, uğradığı zararın miktarını tam olarak ispatlayamıyorsa, hâkim, zararın miktarını hakkaniyete uygun olarak belirleyecektir. Bu durumda, hâkim, olayların olağan akışı ve zarar görenin aldığı önlemleri de dikkate alır.

Tazminatın hesaplanmasında, failin kusurunun varlığı ve derecesi, zarar görenin rızası, zarar görenin ortak kusuru ve tazmin yükünün faili aşırı sıkıntıya sokması da göz önünde tutulur (BK.m.51-52). Bu durumda, veri sorumlusunun kusurunun ağırlığı ile tazminat miktarı doğru orantılıdır. Veri sorumlusu, kişisel verilerin işlenmesinde kast veya ihmalden sorumlu tutulacaktır. Zarar görenin rızası, genel hukuka uygunluk sebebi ve kişisel verilerin işlenmesinde hukuka uygunluk sebebi olduğu için burada kastedilenin hukuka aykırı nitelik taşıyan rıza olduğu ifade edilmektedir[71]. Bir diğer deyişle, kişisel verilerin işlenmesine rıza göstermeye yönelik beyan, açık değilse, aydınlatılmamışsa, sonradan verilmişse bu rıza,

---

[71] **Ayan,** s. 332.

tazminatın hesaplanmasında göz önünde tutulabilir. Yoksa, geçerli bir rıza beyanı kişisel verilerin işlenmesinde hukuka aykırılığı ortadan kaldıracağı için, veri sorumlusunun tazminat sorumluluğu da söz konusu olmayacaktır. İlgili kişinin, veri güvenliğini sağlamaya yönelik adımlar atmaması da zarar görenin kusuru olarak nitelendirilebilir. Bu üç durumda, tazminat miktarı indirilebilir veya ortadan kaldırılabilir (BK.m.52/I). Bununla birlikte, Medenî Kanunun 52 inci maddesinin ikinci fıkrasına göre, fail hafif kusuruyla zarara sebep olmuşsa ve tazminat ödediğinde yoksulluğa düşecekse ve hakkaniyet de gerektirirse, tazminat miktarı indirilebilir (BK.m.52/II).

Hâkim bu belirlemeler sonucunda tazminata hükmederse ödenme biçimini de belirleyecektir. Zararın giderilmesi için, aynen tazmin veya nakden tazmin şeklinde karar verebilir[72]. Aynen tazminde, zarar verilen hak veya hukukî değer yeniden kurulmaktadır[73]. Kişisel verilerin işlenmesi açısından düşünüldüğünde, zararın aynen tazmini pek mümkün değildir. Bu konuda hâkim, genellikle, zararın bir miktar para ödetilerek karşılanmasını öngören nakden tazmine karar verir. Hâkim, öngördüğü tazminatın tek seferde veya irat şeklinde ödenmesine de karar verecektir. Öte yandan, irat biçimde ödenmesine karar verilirse, veri sorumlusu güvence göstermekle yükümlüdür (BK.m.51/II).

ii. Manevî Tazminat Davası

Kişisel verilerin işlenmesinden doğan manevî zararın giderilmesine ilişkin talebin hukukî dayanağını, 1995/46 sayılı Yönergenin 23 üncü maddesinin birinci fıkrasına ek olarak KVKK.m.14/III ve GVKT.m.82 hükmü oluşturmaktadır. Öte yandan, yönergede açıkça manevî zarardan söz edilmediği için manevî tazminat talep edilip edilemeyeceği hususu öğretide tartışılmıştır[74]. Kişisel verilerin hukuka aykırı işlenmesi sebebiyle çoğunlukla manevî zararın ortaya çıktığı düşünüldüğünde, zarar kavramından maddî ve manevî zarar anlaşılmalıdır[75]. Bu durumda, KVKK.m.14/III hükmünün yaptığı atıf gereği, genel hükümlere (MK.m.25/III ve BK.m.58) göre

---

72 **Eren,** s. 741.
73 **Eren,** s. 740; **Kılıçoğlu,** s. 424.
74 Söz konusu tartışma için bkz., **Özdemir,** s. 222-223.
75 **Özdemir**, s. 223.

manevî zararın giderilmesi talep edilebilecektir. Dolayısıyla, davanın açılabilmesi için *"fiilin hukuka aykırı olması", "zararın meydana gelmiş olması"* ve *"uygun illiyet bağının bulunması"* gerekir.

Manevî tazminat davasında, kişilik hakkına yönelik saldırı sonucu ortaya çıkan manevî zararın giderilmesi amaçlanır[76]. Manevî zarardan ne anlaşılması gerektiği hususu ise, öğretide tartışmalıdır. Bir görüşe göre, bir kişinin şahısvarlığına yönelen saldırı sonucu meydana gelen irade dışı eksilmeyi ifade eder[77]. Örneğin, sağlık veya cinsel yönelime ilişkin bilginin açıklanması veya siyasî parti üyeliğine dair bilginin yayınlanması halinde şahısvarlığı değerlerindeki azalma sebebiyle manevî tazminat davası açılabilecektir. Diğer görüşe göre, manevî zarar, kişilik değerleri hukuka aykırı olarak saldırıya uğrayan kişinin bu saldırı sebebiyle hissettiği acı ve ıstıraplar ile yaşama sevincinin azalmasını ifade eder[78]. Bu görüşün kabulü hâlinde, acı, ıstırap ile yaşama sevincinin azalması gibi hisleri yaşamaktan mahrum olan ayırt etme gücünden yoksun olanların (ve tüzel kişilerin) manevî tazminat talep edemeyeceği ve tazminatın devredilemeyeceği şeklinde bir sonuç ortaya çıkmaktadır[79]. Bununla birlikte, Medenî Kanunun 25 inci maddesinin dördüncü fıkrası uyarınca, manevî tazminat isteminin karşı tarafça kabul edilmesi hâlinde devredilebileceği ve mirasbırakan tarafından ileri sürülmesi hâlinde mirasçılara geçeceği hüküm altına alınmıştır. Bu sebeple, kanunkoyucunun birinci görüş doğrultusunda manevî zararı düzenlediği kabul edilmektedir[80].

Manevî tazminatın hesaplanmasında da maddî tazminata ilişkin hükümler geçerli olmakla birlikte, kendisine özgü bazı durumlar söz konusudur. Gerçekten, maddî tazminatın aksine manevi tazminatta zarar miktarı tam olarak hesaplanamayacağı için, hâkimin geniş bir takdir yetkisinin varlığından söz edilebilir. Hâkim, maddî tazminattaki hesaplama araçlarına ek olarak, işlenen verinin niteliğini de dikkate alabilir[81]. Burada bir miktar paranın ödetilmesi şeklinde

---

76 **Özsunay**, s. 155
77 **Eren,** s.
78 **Kılıçoğlu**, s. 300.
79 **Ayan,** Borçlar, s. 280.
80 **Ayan,** Borçlar, s. 281.
81 **Çekin**, Kişisel Veri, s. 103.

gerçekleşen nakden tazmine hükmedilir (BK.m.58). Borçlar Kanunun 58 inci maddesinin ikinci fıkrasına göre, hâkim, nakden tazmin yerine, farklı bir giderim biçimi kararlaştırabilir veya bu giderimi nakden tazmine ekleyebilir. Bununla birlikte, manevî tazminatın irat şeklinde ödenmesine karar verilemez.

ccc. Tazminat Davasında Taraflar

i. Davacı

Tazminat davasında *davacı,* kural olarak, haksız fiil sebebiyle kişilik hakkı ihlâl edilen, ihlâlden doğrudan zarar gören kişi veya kişilerdir[82]. Bununla birlikte, zarar gören kişinin davacı olabilmesi için, taraf ehliyetine sahip olması gerekir. Dava ehliyeti, medenî hakları kullanma ehliyeti olarak ifade edilen fiil ehliyetine göre belirlenir (HMK.m.51). Bu sebeple, gerçek kişilerin ve tüzel kişilerin fiil ehliyeti açısından bir değerlendirme yapmak gerekir. Fiil ehliyetine göre gerçek kişilerden tam ehliyetliler, sınırlı ehliyetliler veya sınırlı ehliyetsizler kişilik hakkının ihlâlinden doğan zararın giderilmesini tek başlarına talep edebilirler (MK.m.16/I). Tam ehliyetsizlerin uğradığı zararların giderilmesine yönelik davaların ise, kanunî temsilci tarafından açılabileceği kabul edilmektedir[83]. Tüzel kişiler ise, zorunlu organlarının kurulumu ile fiil ehliyetini kazanırlar (MK.m.49). Dolayısıyla, dava ehliyetini de zorunlu organlarının kurulumu ile kazanacaklar ve bu organları aracılığı ile kullanabileceklerdir (MK.m.50/I). Kişisel Verilerin Korunması Kanunu, kişisel verilerin kapsamını sadece gerçek kişilerle sınırlı tuttuğu için, bu kapsamda tüzel kişilerin dava hakkının bulunmadığı söylenebilir[84].

Tazminat isteminin devredilmesinde, maddî ve manevî tazminatı ayrı ayrı değerlendirmek gerekir. Maddî tazminat isteminin devredilebileceği ve miras yoluyla

---

82 **Reisoğlu,** s. 266.

83 **Ayan,** Borçlar, s. 326.

84 Her ne kadar Kişisel Verilerin Korunması Kanununda tüzel kişiler kapsam dışı bırakılmışsa da, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik, tüzel kişilere ilişkin verileri de koruma kapsamına almıştır. Bu durumda tüzel kişiler, bu yönetmelik kapsamında koruma talep edebileceklerdir. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik uyarınca tüzel kişilerin de tazminat davasını açabileceklerine ilişkin ayrıntılı bilgi için bkz., **Ayözger Öngün,** s. 299, 300.; **Özdemir,** s. 232.

intikal edebileceği kabul edilirken[85], manevî tazminat açısından daha önce değindiğimiz MK.m.25/IV hükmünde yer verilen sınırlama geçerlidir. Yani, manevî tazminat isteminin sağlararası hukukî işlemle devrinde diğer tarafın kabulü aranacaktır. Mirasçılara intikal edebilmesi için ise, mirasbırakanın ileri sürmesi gerekecektir. Burada, zarar gören kişiye tanınan tazminat isteminin başkasına devri söz konusudur. Öte yandan, bazı hâllerde haksız fiilden dolaylı olarak zarar gören kişilerin kendilerine tazminat talep etme hakkı tanınmıştır. Gerçekten, BK.m.53/3 hükmüne göre, haksız fiil sonucunda ölüm gerçekleşmişse, ölenin desteğinden yoksun kalan kişilerin bu sebeple uğradıkları kayıplar tazminat olarak talep edilebilir. Yine, BK.m.56/II hükmünde öngörülen manevî tazminat istemi, zarar görenin veya ölenin yakınlarına tanınmış bir haktır. Hükme göre, *"ağır bedensel zarar veya ölüm hâlinde, zarar görenin veya ölenin yakınlarına da manevî tazminat olarak uygun bir miktar paranın ödenmesine karar verilebilir"*.

ii. Davalı

Tazminat davasında *davalı* ise, esas itibariyle kişisel veriyi işleyen kişi veya kişilerdir. Kişisel verilerin korunması açısından davalı, kişisel verileri hukuka aykırı bir şekilde işleyen veri sorumlusudur. Veri sorumlusu olabilecek kişiler dikkate alındığında, davalının gerçek veya tüzel kişi olması arasında bir fark yoktur. Kişisel verileri hukuka aykırı olarak işleyen organın bu fiili sonucunda tüzel kişilere karşı tazminat davası açılabilecektir (TMK.50/II).

Bazı durumlarda, kişisel verilerin işlenmesi sebebiyle sorumluluk birden fazla kişiye ait olabilir. Kişisel Verilerin Korunması Kanununun 12 nci maddesinin ikinci fıkrasında bu durum düzenlemektedir. Hükme göre, *"veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması noktasında bu kişilerle birlikte müştereken sorumludur"*. Daha önce de bahsedildiği üzere, veri sorumlusu, kişisel verileri işleme faaliyetini bizzat gerçekleştirebileceği gibi, kendisi adına başka bir kişiye de bırakabilir. Bu durumda, veri işleyen ile veri sorumlusu farklı kişilerden oluşur. KVKK.m.12/II ile veri sorumlusu ve veri işleyen, kişisel verilerin hukuka aykırı

[85] **Oğuzman / Öz**, II, s.

olarak işlenmesi ve erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun teknik ve idarî tedbirleri alma hususunda müştereken sorumlu tutulmuştur. Bu hükmün konulmasındaki temel amaç veri sorumlusu ve veri işleyen arasındaki sorumsuzluk iddialarıdır. Gerçekten, veri sorumlusu, hukuka aykırı kişisel veri işleme faaliyetini doğrudan gerçekleştiren veri işleyenin sorumlu olduğunu iddia ederek sorumluluktan kurtulamayacaktır. Veri işleyen ise, işleme faaliyetinin yürütülmesinden kaynaklanan sorumluluğun veri sorumlusuna ait olduğunu iddia ederek sorumluluktan kurtulamayacaktır.

Bu durumda, hükümde yer verilen *müştereken* ifadesinden ne anlaşılması gerektiği belirlenmelidir. Öğretideki genel yönelim, bu ifade ile müteselsil sorumluluğun kastedildiği yönündedir[86]. Müteselsil sorumluluk, Borçlar Kanununun 61 ve 62 nci maddelerinde düzenlenmiştir. Buna göre, *"Birden çok kişi birlikte bir zarara sebebiyet verdikleri veya aynı zarardan çeşitli sebeplerden dolayı sorumlu oldukları takdirde, haklarında müteselsil sorumluluk hükümleri uygulanır"*. Birden fazla kişinin müteselsil sorumluluğu kanundan kaynaklanabileceği gibi, sözleşmeden de kaynaklanabilir[87]. Kişisel Verilerin Korunması Kanunun 12 nci maddesinin ikinci fıkrası, müteselsil sorumluluğun kanundan kaynaklanmasına örnek olarak verilebilir. Bu durumda, kişisel verileri hukuka aykırı olarak işlendiği için zarara uğrayan kişi, veri sorumlusuna veya veri işleyene karşı tazminat davası açabilecektir. Bu durumda, o dilerse her ikisinde karşı da dava açar[88]. Şüphesiz, birden fazla veri sorumlusunun işleme amaç ve vasıtalarını belirleyerek kişisel verileri hukuka aykırı işlemelerinde de müteselsil sorumluluk söz konusu olacaktır[89].

ddd. Tazminat Davasının Açılabileceği Süre

Kişilik hakkına yönelik saldırılar sonucunda talep edilebilecek tazminat açısından bazı süreler öngörülmüştür. Kişisel verilerin işlenmesi sebebiyle zarara

---

86 **Develioğlu,** s. 102; **Çekin**, Kişisel Veri, s. 110. Burada, hükmün ifade tarzından kısmî (müşterek) borçluluktan bahsedildiği düşünülebilirse de kısmî sorumluluktaki gibi veri işleyen ile veri sorumlusu arasındaki yükümlülüklerin bölünmesi ve her birinin kendi payına düşen yükümlülükleri yerine getirmesiyle sorumluluğunun kalkması bu hükmünün amacı ile bağdaşmaz.

87 **Ayan,** Borçlar, s. 60.

88 **Ayan,** Borçlar, s. 328.

89 **Develioğlu**, s. 102.

uğrayan kişi öngörülen süreler içerisinde dava açmazsa, alacak hakkı zamanaşımına uğrayacaktır. Gerçekten, Borçlar Kanununun 72 nci maddesinin birinci fıkrasına göre, tazminat istemlerinde zamanaşımı süresi iki ve on yıldır. İki yıllık zamanaşımı süresinin başlangıcında, zarar görenin zararı ve tazminat yükümlüsünü öğrendiği tarih esas alınır. On yıllık zamanaşımı süresinin başlangıcında ise, fiilin işlendiği tarih esas alınır. Bununla birlikte, bahsi geçen hükmün devamında *"tazminat ceza kanunlarının daha uzun bir zamanaşımı öngördüğü cezayı gerektiren bir fiilden doğmuşsa, bu zamanaşımı uygulanır."* hükmüne yer verilmiştir. Bu durumda, tazminat talebinin temelindeki fiilin ceza kanunlarına göre suç teşkil etmesi hâlinde, ceza davası zamanaşımı süresi daha uzunsa, ceza kanunlarında öngörülen zamanaşımı süresi tazminat davalarında da uygulanacaktır[90]. Bu durumda, tazminata sebep olan kişisel veri işleme faaliyeti, kişisel verilerin kaydedilmesi suçu (TCK.m.135), kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu (TCK.m.136,137) ve verilerin yok edilmemesi suçu (TCK.m.138) kapsamında değerlendirilebiliyorsa ve ceza zamanaşımı süresi, TBK.m.72/I hükmünde öngörülen sürelerden uzunsa, bu süreler dikkate alınacaktır[91].

Ayrıca, Borçlar Kanununun 73 üncü maddesi kapsamında bir rücu zamanaşımına yer verilmiştir. Hükme göre, *"Rücu istemi, tazminatın tamamının ödendiği ve birlikte sorumlu kişinin öğrenildiği tarihten başlayarak iki yılın ve her hâlde tazminatın tamamının ödendiği tarihten başlayarak on yılın geçmesiyle zamanaşımına uğrar (f.1). Tazminatın ödenmesi kendisinden istenilen kişi, durumu birlikte sorumlu olduğu kişilere bildirmek zorundadır. Aksi takdirde zamanaşımı, bu bildirimin dürüstlük kurallarına göre yapılabileceği tarihte işlemeye başlar (f. 2)"*. Bu durumda, veri işleyen veya veri sorumlusundan tazminat davası kendisine yöneltilen her biri, rücu istemini hükümde yer verilen süre ve şartlarda diğerine yöneltebilecektir. Zarardan birden fazla veri sorumlusunun sorumlu olduğu durumlarda da aynı esas geçerli olacaktır.

---

90 **Kılıçoğlu**, s. 494 vd..; **Ayan,** Borçlar, s. 335.

91 Kişisel veriler ile ilgili Türk Ceza Kanununda öngörülen suçlara ilişkin zamanaşımı süreleri için bkz., Alaattin **Bük,** Bilişim Alanında Kişisel Verilerin Korunması, Ankara 2018. s. 240 vd..

eee. Tazminat Davasında Yetkili ve Görevli Mahkeme

Tazminat davasına ilişkin birden çok yetki kuralı bulunmaktadır. Gerçekten, tazminat davası, genel yetkili mahkeme olan *davalının dava açıldığı tarihteki yerleşim yeri mahkemesi*nde açılabilir (HMK.m.6). Davalı birden fazla ise, dava bunlardan birinin yerleşim yeri mahkemesinde açılabilir (HMK.m.7/I). Kişisel verilerin hukuka aykırı olarak işlenmesinin temelde bir haksız fiil olduğundan hareketle, *haksız fiilin işlendiği veya zararın meydana geldiği yahut gelme ihtimalinin bulunduğu yer ya da zarar görenin yerleşim yeri mahkemesi*nde de açılabilir (HMK.m.16). Ayrıca, Medenî Kanunun 25 inci maddesinin beşinci fıkrası gereği, kişilik hakkının korunması söz konusu olduğu için, *davacının kendi yerleşim yeri mahkemesi*nde de açılabilir. Tazminat davasının açılabileceği görevli mahkeme ise, dava konusunun değer ve miktarına bakılmaksızın asliye hukuk mahkemesidir (HMK.m.2/I).

bb. Vekâletsiz İş Görme Davası

Kişilik hakkına yönelik saldırılar sebebiyle kişinin zarara uğrayabileceğini ifade etmiştik. Medenî Kanunun 25 inci maddesinin üçüncü fıkrasına göre, kişilik hakkı ihlâl edilen kişi, bu zararlara ek olarak, hukuka aykırı saldırı sebebiyle elde edilmiş kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesini talep edebilir. Bu durumda, kişisel verileri hukuka aykırı olarak işlenen kişi, bu sebeple elde edilmiş kazancın kendisine verilmesini talep edebilecektir. Kanun hükmü gereği, bu talebin ileri sürülebilmesi için vekâletsiz iş görme hükümlerine başvurulacaktır. Bununla birlikte, burada, iş sahibinin açık ya da örtülü bir yasaklamasının olmadığı durumlarda, iş sahibine ait bir işin, iş sahibinin menfaatine olarak görülmesi söz konusu olduğu için[92], gerçek olmayan vekâletsiz iş görmeye ilişkin (MK.m.530) hükümler uygulanacaktır. Bu hüküm çerçevesinde vekâletsiz iş görmeye dayalı olarak dava açılabilmesi için ise, kişilik hakkının ihlâli yolu ile iş

---

92 Serap **Helvacı** / Gülşah Sinem **Aydın**, Kişilik Hakkı İhlâlinden Doğan Vekâletsiz İşgörmede Kusurun Bir Şart Olarak Aranıp Aranmayacağı Sorunu, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 23, S. 1, s. 265-301, s. 271.

görme, kazanç elde edilmesi ve illiyet bağının bulunması gerekir[93]. Kişisel verilerin işlenmesi açısından, vekâletsiz iş görme hükümlerine başvurulması için, kişisel verileri hukuka aykırı olarak işleyen veri sorumlusu, iş görmesi sonucunda bir kazanç elde etmelidir. Örneğin, reklam için uygun bir yüze sahip olmasına rağmen bu işi tercih etmeyen kişinin resimlerinin bir reklamda kullanılması sonucu elde edilen gelir, ilgili kişi tarafından MK.m.530 hükmü çerçevesinde talep edilebilecektir[94].

§ 11. 4857 SAYILI İŞ KANUNU AÇISINDAN KORUMA YOLLARI

Kişisel verilerin, her alanda olduğu gibi, iş ilişkisinde de korunması büyük önem arz etmektedir. 4857 sayılı İş Kanunun 8 inci maddesinin birinci fıkrasına göre, iş sözleşmesi, *"bir tarafın (işçi) bağımlı olarak iş görmeyi, diğer tarafın (işveren) da ücret ödemeyi üstlenmesinden oluşan sözleşmedir*". Yine, Borçlar Kanununun hizmet sözleşmesini düzenleyen 393 üncü maddesinin birinci fıkrasına göre, iş ilişkisinden bahsedilebilmesi için işçinin işverene hukukî bir bağımlılığının bulunması gerekir. Görüldüğü üzere, işçi ile işveren arasında iş ilişkisinden söz edilebilmesi için hukukî bir bağımlılığın bulunması gerekir. Bu bağımlılık, çoğu zaman ekonomik bağımlılığı da beraberinde getirmektedir[95]. Bu durum, işverene nazaran zayıf konumda olan işçinin kişisel verilerinin işlenmesini kolaylaştırmakta ve verilerin korunmasını gerektirmektedir. Öte yandan, işverenin eşit davranma, gözetme ve koruma gibi yükümlülükleri bulunmaktadır. Gerçekten, İş Kanununun 5 inci maddesinin birinci fıkrası gereği, işveren, aynı veya eşit durumda bulunanlar arasında *"dil, din, ırk, renk, cinsiyet, engellilik, siyasal düşünce, felsefi inanç, din ve mezhep ve benzeri sebeplere dayalı ayrım yapamaz"*. Aynı maddenin beşinci fıkrasında ise, cinsiyet veya gebelik sebebiyle farklı işlem uygulanamayacağı hüküm altına alınmıştır. Görüldüğü üzere, eşit davranma yükümlülüğüne göre, işveren, kişisel veri olarak değerlendirilen hususları göz önüne alarak işçileri arasında ayrım yapamaz. Gözetme ve koruma yükümlülüğüne göre ise, işveren işçinin kimliğini

---

93 Bu davanın açılabilmesi için kusurun aranmayacağı ile ilgili ayrıntılı açıklamalar için bkz., **Helvacı / Aydın,** s. 287 vd..

94 **Özdemir,** s. 204.

95 Tankut **Centel,** İş Hukuku: Bireysel İş Hukuku, C. 1, İstanbul 1994, s. 58.

korumak ve saygı göstermek zorundadır (BK.m.417). Bununla birlikte, işe alımda, iş sözleşmesinin devamında ve hatta sonrasında gerçekleştirilen uygulamalar sayılan yükümlülükleri ihlâl etmekle kalmayıp, işçinin kişisel verilerinin işlenmesi sebebiyle zarara uğramasına sebep olmaktadır[96]. Bu durumda, Kişisel Verilerin Korunması Kanunu kapsamında ilgili kişi olan işçinin kişisel verilerinin korunması sağlanmalıdır. Bu başlık altında, bir işçiye ilişkin kişisel verilerin işlenmesine yol açacak uygulamalara yer verilecek, daha sonra hem Kişisel Verilerin Korunması Kanunundaki hem de İş Kanunundaki koruma hükümlerine değinilecektir.

İşveren ile işçi arasındaki ilişki düşünüldüğünde, işçinin kişisel verilerine erişim imkânının çeşitliliği ve kolaylığı göze çarpacaktır. İşçiye yöneltilen sorular aracılığıyla, işçi üzerinde testler uygulayarak veya işçinin izlenmesi, dinlenmesi, gözetlenmesi suretiyle kişisel veriler işlenmektedir[97]. Gerçekten, işveren, işçiye kişisel durumu, sağlık durumu, ceza mahkûmiyeti, dini, siyasi görüşü, parti veya sendika üyeliği gibi birçok konuda sorular yöneltebilmektedir. Ancak, özel nitelikli veri kategorisinde yer alan bu verileri elde etmeye yönelik sorular sorulabilmesi için, Kişisel Verilerin Korunması Kanununun 6 ncı maddesinde yer verilen şartlar aranmalıdır. Genel nitelikli veriler açısından ise, Kişisel Verilerin Korunması Kanununun 5 inci maddesinde öngörülen şartlar sağlanmalıdır. Her iki kategoride yer alan verilerin işçinin açık rızasına dayalı olarak işlenmesi mümkündür[98]. İşveren, geçerli bir açık rızada bulunması gereken tüm unsurları sağlayarak işçinin açık rızasını almalı ve bu sınırlar içinde kişisel verileri işlemelidir. Burada, işçinin iş ilişkisinin kurulmasından önce ve iş ilişkisi devam ederken kişisel verilerinin işlenmesine verdiği rızanın serbest iradeye dayanıp dayanmadığına dikkat edilmelidir. Zira, işverene bağımlı olduğu için daha zayıf tarafı oluşturan işçi, kişisel verilerin işlenmesine rıza gösterme hususunda kendisini zorunlu hissedebilir. Öte yandan, işveren iş ilişkisinin kurulmasını veya devam etmesini işçinin veri işlemeye rıza göstermesine de bağlayabilir. Daha önce bağlama yasağı olarak ifade ettiğimiz

---

96 Selin **Uncular,** Kişisel Verilerin Korunması Kanunu ve AB Genel Veri Koruma Tüzüğü Kapsamında İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, 2. Baskı, Ankara 2018, s. 186.

97 İlke **Gürsel,** Kişisel Verilerin Korunması Hakkının İşçi ve İşveren İlişkisine Etkileri, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, C. 13, S. 50, 2016, s. 782.

98 **Gürsel,** s. 780.

bu gibi durumlarda serbest iradeden söz edilemeyeceği için, geçerli bir açık rızadan bahsedilemez. Dolayısıyla bu rızaya dayanılarak kişisel verilerin işlenmesi hukuka aykırı olacaktır[99]. Açık rızanın aranmadığı kişisel veri işleme sebeplerinden birine dayanılarak işleme yapılabilecektir. Bu noktada, kanunda öngörülen hâllerde işlemenin yapılması, sözleşmenin kurulması veya ifasıyla ilgili verilerin işlenmesi, meşru menfaate dayalı olarak işlemenin yapılması veya işverenin hukukî yükümlülüğünün gerektirmesi gibi durumlar iş ilişkisinde uygulanabilecek niteliktedir.

Elde etmek istenilen bilginin kategorisine göre işlemeye dayanak olacak hukukî sebebi belirledikten sonra, işverenin sorabileceği soruların sınırına değinmek gerekir. Bu sınırı belirlerken kişisel verilerin işlenmesinde genel ilkeleri düzenleyen KVKK.m.4 hükmü dikkate alınmalıdır. İşveren, öncelikle, hukuka, dürüstlük kurallarına ve amaca uygun, amaçla sınırlı ve ölçülü olarak işçiye soru sormalı ve bilgi edinmelidir[100]. İşverenin bu sınırlar dâhilinde sorduğu sorular, her somut olay açısından değerlendirilmek üzere, işçi tarafından cevaplandırılmalıdır. Örneğin, manken veya ses sanatçısı gibi işlerde bulunmak amacıyla yapılan başvurularda, hamileliğe ilişkin sorular işin niteliğinin bir gereği kabul edilmektedir[101].

İşverenin soru sormaya ilişkin sınırı aştığı hâlde, işçi kendisine yöneltilen bu sorulara cevap vermekten imtina ederse veya eksik yahut yanlış bilgiler verirse, işverenin iş sözleşmesini haklı sebeple fesh edip edemeyeceği gündeme gelecektir. İş Kanununun 25 inci maddesinin ikinci fıkrasının a bendi uyarınca, iş sözleşmesinin esaslı noktalarından biri ile ilgili işçinin verdiği bilgilerle işvereni yanıltması, iş sözleşmesinin feshi için haklı sebep sayılmıştır. Bu durumda, esaslı sayılmayan noktalarda yöneltilen sorular açısından işçinin kişisel verileri ile ilgili yanlış veya

---

99 **Gürsel,** s. 781.

100 Eda **Manav,** İş İlişkilerinde İşçinin Kişisel Verilerinin Korunması, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. 19, S. 2, 2015, s. 113; **Gürsel,** s. 808.

101 Ayşe Merve **Belge,** Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlâli ve Korunması Yolları, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Şeref Ertaş'a Armağan, C. 19, Özel Sayı, 2017, s. 1035; **Manav,** s. 117; **Gürsel,** s. 809.

eksik bilgiler vermesi yahut susması, haklı nedenle fesih sebebi olarak değerlendirilmemelidir[102].

Kişisel verilerin açık rıza aranmaksızın işlenebileceği hâller (KVKK.m.5/II) de burada uygulama alanı bulacaktır. Gerçekten, kanunlarda öngörülmesi hâlinde işveren işçinin kişisel verilerini işleyebilecektir. Örneğin, Borçlar Kanununun 419 uncu maddesinin birinci fıkrasına göre, *"İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir"*. Dikkat edilirse, hükümde yer alan sebep, hukuka uygun olarak elde edilen kişisel verilerin işçinin işe yatkınlığını belirlemek amacıyla *kullanılmasına* imkân tanımaktadır. Fıkranın ikinci kısmında düzenlenen hizmet sözleşmesinin ifası için zorunlu olma unsuru ise, hâlihazırda KVKK.m.5/II hükmünde açık rıza aranmaksızın kişisel verilerin işlenebileceği hâl olarak yer almaktadır. Gerçekten, iş sözleşmesinin kurulması veya ifası için kişisel veri işlemenin gerekli olduğu durumlarda hukuka aykırılıktan bahsedilemez. Üstelik bu durumlarda, işçinin açık rızası da aranmaz. Örneğin, işçinin adı, kimlik numarası veya sigorta numarası yahut hesap numarası bu kapsamda değerlendirilir. Yine, işverenin hukukî yükümlülüğünü yerine getirmesi amacıyla işçinin kişisel verilerinin işlenmesi mümkündür. Bu duruma, İş Kanununun 75 inci maddesinde düzenlenen işverenin özlük dosyası hazırlamasına ilişkin yükümlülüğü örnek olarak verilebilir. Aynı şekilde, işçinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, işverenin meşru menfaatinin zorunlu kılması hâlinde de işçiye ilişkin kişisel veriler işlenebilecektir. Örneğin, Kişisel Verilerin Korunması Kanunun 5 inci maddesinin gerekçesinde belirtilen işçilerin *terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması sürecinde görev ve rol dağıtımında esas alınmak üzere* kişisel verilerin işlenmesi, veri sorumlusu olan işverenin meşru menfaati kapsamında değerlendirilir. İşveren, bu durumlarda meşru menfaati ile işçinin temel hak ve özgürlükleri arasındaki dengeyi gözeterek kişisel verileri işleyebilecektir.

---

[102] **Küzeci,** Kişisel Veri, s. 387. **Uncular,** s. 78.

İşçinin işe uygunluğunu belirlemek, verimliliği artırmak gibi nedenlerle uygulanması planlanan alkol, uyuşturucu, HIV / AIDS testleri, genetik veya psikolojik testler sonucunda sağlık durumuna ilişkin bilgiler edinilmektedir. Bu durumda, özel nitelikli kişisel veri kategorisinde değerlendirilen bu verilerin KVKK.m.6 hükmünde yer alan hâllerde işlenmesi gerekir. Bu durumda, öncelikle, geçerli bir şekilde verilmiş açık rızaya dayanılarak KVKK.m.4 hükmünde yer alan sınırlar dâhilinde işçinin kişisel verilerinin işlenmesi akla gelir. Örneğin, ticarî taksi şoförü olarak çalıştırılan işçiye açık rızaya dayanılarak alkol testi uygulanabilmelidir. Ancak, bu kişiye HIV / AIDS, genetik testlerinin açık rızaya dayalı olarak yapılması mümkün değildir. Zira, işin niteliği ve görev tanımı veya amaç bu testin yapılmasına dair gereklilik doğurmaz[103]. Burada, veri işleme ilkelerinden hukuka ve dürüstlük kurallarına uygun olma ölçütünün sağlanmadığı söylenebilir. Genetik testler ise, açık rızaya dayalı olarak dâhi işlenememelidir[104]. Zira, İnsan Hakları ve Biyotıp Sözleşmesinin 12 nci maddesine göre, genetik testler, sağlık amaçlarıyla veya sağlık amaçlı bilimsel araştırmalar için ve uygun genetik danışmada bulunmak şartıyla yapılabilir. Bu sebeple, söz konusu testlerin kanunda öngörülen hâllerde (KVKK.m.6/II-III) uygulanması kişisel verilerin korunması açısından daha isabetlidir[105]. Bu durum, işçinin kişiliğine saygı gösterme ve onu koruma yükümlülüğü ile de bağdaşır niteliktedir.

İşçinin ses, video kaydı alan cihazlar aracılığıyla dinlenmesi, elektronik veya biyometrik giriş kontrol sistemleri aracılığıyla giriş çıkış saatlerinin takip edilmesi, konum bilgisi sunan cihazlar aracılığıyla yerinin belirlenmesi, telefonlarının dinlenmesi, internet geçmişinin denetlenmesi gibi uygulamalarla sıkça karşılaşılmaktadır. Bu uygulamalar, temelde, müşteriye daha iyi hizmet sunmak, fizikî güvenliği veya internet güvenliğini sağlamak, işverenin yönetim ve denetim hakkını[106] kullanması gibi gerekçelerle uygulanmaktadır. Örneğin, müşteriye yakın

---

103 **Gürsel,** s. 816-817.

104 **Gürsel,** s. 818.

105 **Uncular,** s. 60.

106 Borçlar Kanununun 399 uncu maddesine göre, *"İşveren, işin görülmesi ve işçilerin işyerindeki davranışlarıyla ilgili genel düzenlemeler yapabilir ve onlara özel talimat verebilir. İşçiler, bunlara dürüstlük kurallarının gerektirdiği ölçüde uymak zorundadırlar"*. Dolayısıyla, işverenin yönetim ve denetim hakkının sınırını MK.m.2 hükmünün oluşturduğu söylenebilir.

olan işçinin konumunun belirlenmesi için işçinin kullandığı araca takip cihazı yerleştirilmesi, işyerinde güvenliği sağlamak amacıyla güvenlik kameraları yerleştirilmesi[107], işçinin işe giriş çıkışların kontrol edilmesi amacıyla parmak izinin okutulması[108], işyerindeki bazı odalara retina taraması ile giriş yapılması hâlinde kişisel veriler işlenmektedir. Kişisel verilerin işlenmesi sonucunu doğuran bu uygulamaların gerçekleştirilebilmesi için kişisel veri işleme şartlarına (KVKK.m.5 vd.) uygun hareket edilmesi gerekir. Söz konusu örneklerde kişisel verilerin işlenmesi, veri sorumlusunun meşru menfaatinin kişisel veri işlemeyi zorunlu kılmasına dayanılarak gerçekleştirilebilir. Bu durumda, veri sorumlusunun meşru menfaatinin bulunması, işçinin temel hak ve özgürlüklerine zarar verilmemesi ve veri işlemenin zorunlu olması gerekir[109]. Sayılan durumlarda işverenin meşru menfaatinin bulunduğu kabul edilebilir. Bu menfaatlere dayalı olarak veri işlemenin temel hak ve özgürlüklere zarar vermemesi gerekir. Örneğin, hırsızlıkların önlenmesi için, işçilerin giyinme odasına güvenlik kamerası yerleştirilmesi mümkün değildir. Son olarak, bu yolla veri işlemenin zorunlu olması aranacaktır. Örneğin, parmak izi yerine kart kullanarak giriş çıkış kontrolleri güvenli bir şekilde sağlanabiliyorsa bu yol tercih edilmelidir.

İşveren sayılan uygulamalar yoluyla elde ettiği verileri, amacı dışında kullanamayacaktır. Örneğin, takip cihazının mesai saatleri dışında kapatılması, izlenmemesi gerekir. Aynı şekilde, güvenlik kameralarından işçinin çalışma yöntemi, hızı, mola süreleri takip edilemez. Bu durumlar, işverenin denetim ve yönetim hakkının kullanmasının ötesinde olup işçinin sürekli olarak gözetlenmesi sonucunu doğurur[110].

---

107 **Manav,** s. 128. **Belge,** s. 1037.

108 Kişisel Verilerin Korunması Kanununun yürürlüğe girmesinden önce Danıştay bir kararında, işe giriş ve çıkış saatlerinin kontrolünde parmak izinin kullanılmasını kişisel veri olarak nitelendirmiştir. Ayrıca, Danıştay, uygulamanın sınırlarını, usul ve esaslarını belirleyecek yasal dayanağın ve toplanan verilerin ileride başka bir şekilde kullanılmayacağına dair güvencenin bulunmamasını gerekçe göstererek uygulamayı hukuka aykırı bulmuştur. Bkz., 5.D. 10.12.2013, E.2013/5342 K.2013/9525, (www.lexpera.com, Erişim Tarihi: 15.1.2019).

109 **Akgül,** Biyometrik, s. 211; **Şimşek,** s. 99; **Manav,** s. 121; **Gürsel,** s. 790-791.

110 Bu uygulamalar, daha önce değinilen Panoptikon sistemini akla getirmektedir. *Jeremy Bentham*, bu sistemin fabrikalar açısından da uygulanabilir olduğunu savunmaktadır. Bkz., **Bentham / Pease - Watkin / Werret,** s. 61.

Hukuka aykırılığı ortadan kaldıran sebeplerden hangisine dayanılırsa dayanılsın, işveren, verilerin işlenmesine hâkim olan genel ilkelere uymak (KVKK.m.4) zorundadır. Örneğin, işçinin açık rızası ile yapılan işlemelerde, ileride işe yarayacağı düşünülen veya iş ilişkisiyle ilgisi bulunmayan bilgilerin talep edilmesi, kişisel verilerin hukuka aykırı işlenmesi sonucunu doğuracaktır. Bu duruma işçinin rıza göstermesi de sınırı aşan işleme açısından hukuka aykırılığı ortadan kaldırmaz. Benzer şekilde, hukuka uygun olarak elde edilmesine rağmen, hukukî dayanaktan yoksun bir şekilde işçinin verilerinin arşivlenmesinde veya yeni işverenlere aktarılmasında[111] hukuka aykırı işleme ortaya çıkar. Bu durumda, veri sorumlusu, işçinin maruz kaldığı zararı gidermekle yükümlüdür (KVKK.m.11/I-ğ ve KVKK.m.14/III).

İşveren, kanunlarda yer alan işleme şartlarına uygun olarak işlediği veriler ile ilgili olarak Kişisel Verilerin Korunması Kanununun 10 ve 12 inci maddelerinde yer alan yükümlülüklerine uygun hareket etmelidir. Örneğin, işveren, işçinin kişisel verilerin işlendiğine dair aydınlatma yükümlülüğünü yerine getirmelidir. Ayrıca, elde ettiği verilerin güvenliğini sağlamaya yönelik tedbirleri almalı, verilere erişim yetkisi olanları belirlemelidir. İşçi ise, ilgili kişinin haklarını düzenleyen hükümler çerçevesinde işverene başvurabilir. Kendisi ile ilgili verilerin işlenmesi, aktarılması gibi durumlarda bilgi edinme hakkını kullanabilir, verilerin düzeltilmesini isteyebilir. Yahut, işlenen verilerin otomatik sistemler aracılığıyla analiz edilmesi sonucunda kendisi aleyhine ortaya çıkan sonuca itiraz edebilir. Veri sorumlusuna başvuru yolunu tükettikten sonra, Kişisel Verileri Koruma Kuruluna şikâyet yolunu kullanabilir. Şüphesiz, işçi genel hükümler çerçevesinde (MK.m.24 ve 25) saldırıya yönelik ve saldırının sonucuna yönelik davalar aracılığıyla da kişisel verilerinin korunmasını sağlayabilir.

Ayrıca, Borçlar Kanununun 417 nci maddesi uyarınca işçinin kişiliğinin korunması sağlanabilir. Hükümde, işveren, işçinin kişiliğini korumak için bir dizi önlem almakla yükümlü kılınmıştır. Kişisel verilerin hukuka aykırı olarak

---

[111] Bu durumda, sözleşme sona erse dâhi işverenin sır saklama yükümlülüğü vardır. Öte yandan, işçi, yeni işverene başvururken eski işverenini referans göstermişse kendi hakkında bilgi verilmesine rıza gösterdiği kabul edilebilir. Bkz., **Küzeci,** Kişisel Veri, s. 398.

işlenmesini önlemek de bu yükümlülükler arasında sayılabilir. Bu yükümlülüklere, kanuna, sözleşmeye aykırı davranan işverenin sorumluluğu Borçlar Kanununun 417 nci maddesinin üçüncü fıkrasında düzenlenmiştir. Buna göre, işçinin kişisel verilerinin hukuka aykırı olarak işlenmesi sebebiyle kişilik haklarının ihlaline bağlı zararların tazmininde sözleşmeye aykırılık (BK.m.112 vd.) hükümleri uygulanacaktır. Dolayısıyla, işveren, kendisine hiçbir kusurun yükletilemeyeceğini ispat etmedikçe, işçinin zararını gidermekle yükümlüdür.

Son olarak, kişisel verileri hukuka aykırı olarak işlenen işçinin, İş Kanunu çerçevesinde başvurabileceği bir korumadan bahsedilebilir. İşçi, kişisel verilerin işlenmesi sebebiyle, Medenî Kanunun, Kişisel Verilerin Korunması Kanunu ve Borçlar Kanunu çerçevesinde birçok korumadan faydalanabilir. Bununla birlikte, tüm bu hâller, iş ilişkisini sona erdirmez. Sadece, işçiye başvuru veya şikâyet yolu sağlar ya da zararın giderilmesine ilişkin bir talep hakkı verir. Öte yandan, İş Kanununun 24 üncü maddesinde sayılan durumlarda işçiye haklı nedenle fesih hakkı tanınmıştır. Hükme göre, sağlık sebepleri, ahlak ve iyiniyet kurallarına uymayan hâller ve benzerleri ile zorlayıcı sebepler işçiye belirli veya belirsiz süreli bir iş sözleşmesini haklı sebeple feshetme yetkisi veren hâllerdir. Kişisel verilerin işlenmesi açısından ahlak ve iyiniyet kurallarına uymayan hâller ve benzerleri önem taşımaktadır. Örneğin, işveren, iş yerinde kullandığı iletişimin izlenmesi yöntemlerinden iş başvurusu görüşmesinde bahsetmemişse bu durum, İş Kanunu 24 üncü maddenin ikinci fıkrasının a bendi gereğince işçiye, kurulan iş sözleşmesini haklı sebeple feshi hakkı verir[112]. Yine, işveren, işçinin şeref ve haysiyetini zedeleyecek soyunma odası görüntülerini kaydederse, haberleşme içeriklerine veya internet geçmişine ulaşırsa ya da tüm bu verileri paylaşırsa, işçinin, İK.m.24/II-b hükmü gereğince, iş sözleşmesini haklı nedenle feshedebileceği kabul edilir[113].

İşçi, kişisel verilerinin hukuka aykırı olarak işlenmesi sebebiyle İK.m.24 hükmünde yer verilen haklı nedenle fesih hakkını, işverenin bu fiilini öğrendiği tarihten itibaren altı iş günü, her hâlde fiilin gerçekleştiği tarihten itibaren bir yıl

---

112 Fatma Burcu **Savaş**, İş Hukukunda Siber Gözetim, Çalışma ve Toplum Ekonomi ve Hukuk Dergisi, C.3, S. 22, s. 124; **Manav,** s. 131; **Belge,** s. 1047.

113 **Uncular,** s. 315; **Gürsel,** s. 839.

içerisinde kullanmak zorundadır (İK.m.26/I). Süresi içerisinde haklı sebeple iş sözleşmesini fesheden işçi, İK.m.26/II hükmü çerçevesinde tazminat talep edebilir.

§ 12. 5237 SAYILI TÜRK CEZA KANUNU AÇISINDAN KORUMA YOLLARI

I. GENEL OLARAK

Türk Hukukunda, 6698 sayılı Kişisel Verilerin Korunması Kanununun yürürlüğe girmesinden önce, kişisel verilerin işlenmesi kapsamındaki bazı fiiller 5237 sayılı Türk Ceza Kanununda suç olarak düzenlenmiştir. Gerçekten, Türk Ceza Kanunun 135 inci maddesinde *kişisel verilerin kaydedilmesi*, 136 ncı maddesinde *verileri hukuka aykırı olarak verme, yayma veya ele geçirme* ve 138 inci maddesinde *verileri yok etmeme suçu* yer almaktadır. Söz konusu suçların temel noktası kişisel veri olduğu için, kişisel verilerin tanımından ve kapsamından, işleme ifadesinden ne anlaşılması gerektiği, veri işlemenin ne zaman hukuka aykırı olacağı, verilerin tutulabileceği sürenin ne olacağı gibi hususlar önemli bir sorun olmuştur[114]. 6698 sayılı Kişisel Verilerin Korunması Kanununun kabul edilmesiyle birlikte, söz konusu suçların kapsamı ve sınırları belirlenebilir hâle gelmiştir. Ayrıca, Kişisel Verilerin Korunması Kanununun 17 nci maddesi uyarınca, Türk Ceza Kanunu ile Kişisel Verilerin Korunması Kanunu arasında doğrudan bir ilişki kurulmuştur[115]. Bu ilişki dikkate alınarak her iki kanunun ilgili hükümleri kapsamında, kişisel verilere ilişkin suçları ve ilgili hükümleri düzenleyen Türk Ceza Kanununun 135 inci ve devamı maddeleri incelenecektir.

II. KİŞİSEL VERİLERİN KAYDEDİLMESİ

Türk Ceza Kanununun 135 inci maddesinde düzenlenen kişisel verilerin kaydedilmesi suçu uyarınca, kişisel verileri hukuka aykırı olarak kaydeden kimseye bir yıldan[116] üç yıla kadar hapis cezası verilmesi öngörülmüştür. Maddenin ikinci fıkrasına göre ise, *"Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki*

---

114 **Ünver,** s. 190; **Küzeci,** Kişisel Veri, s. 401.

115 **Küzeci,** Kişisel Veri, s. 402.

116 21.2.2014 tarihli ve 6526 sayılı Kanunun 3 üncü maddesiyle hükmün önceki hâlindeki "altı aydan" ibaresi "bir yıldan" şeklinde değiştirilmiştir.

kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır"[117]. Görüldüğü üzere, kaydedilen verilerin özel nitelikli veri kategorisine dâhil bazı verilerden olması hâlinde cezanın yarı oranında artırılacağına yer verilmiştir.

Hükümde yer verilen kişisel verilerin *hukuka aykırı* olarak işlenmesi ifadesinden ne anlaşılacağını belirlerken KVKK hükümleri yol gösterici olacaktır[118]. Bir diğer deyişle, kişisel verilerin işlenmesinde genel ilkeler ve kişisel verilerin işlenme şartları gibi hukuk aykırılığı belirlerken esas alınan hükümler, burada da dikkate alınacaktır. Nitekim, hükmün gerekçesinde, açık rıza ve kanun hükümleri doğrultusunda yapılan kayıtların suçun konusunu oluşturmayacağına yer verilmiştir. Hukuka aykırılık açısından değerlendirilmesi gereken diğer husus ise, ikinci fıkrada yer verilen özel nitelikli kişisel veriler ve bu verilere ilişkin hukuka aykırılıktır. Öncelikle, ikinci fıkrada yer alan verilerin, KVKK.m.6/I hükmünde yer alan verilerin tamamını kapsamadığı görülecektir. Bir diğer deyişle, Ceza Kanununun 135 inci maddesi sadece, *kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin* verilerin kaydedilmesini cezanın artırılması sebebi olarak öngörmüştür. Bu durumda, sayılanlar dışındaki özel nitelikli kişisel veriler açısından ilk fıkra hükmü uygulanacaktır[119]. Hükmün ikinci fıkrasında sayılan özel nitelikli veriler açısından hukuka aykırılık unsurunun da değerlendirilmesi gerekir. Zira, hükümde, kişilerin *ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına* ilişkin kayıtlarda hukuka aykırılık aranırken, *siyasi, felsefi veya dini görüşlerine, ırki kökenlerine* ilişkin kayıtlarda aranmamıştır. Bu durumda, ilk grupta bulunan verilerin kaydedilmesinin her hâlükarda hukuka aykırı olacağı ileri sürülmüştür[120]. Ancak, daha önce değinildiği

---

117 Söz konusu hüküm ise, KVKK'nın yürürlüğe girmesinden sonra, bu hâlini almıştır. Gerçekten, Kişisel Verilerin Korunması Kanununun 30 uncu maddesiyle yapılan değişiklikten önce, ikinci fıkrada öngörülen verilerin kaydedilmesi birinci fıkradaki cezaya tâbi kılınmıştı.

118 **Küzeci,** Kişisel Veri, s. 403.

119 *Küzeci'ye* göre, bu durum uygulamada bazı sorunları da beraberinde getireceği için, CK.m.135/II hükmünün KVKK.m.6/I ile uyumlulaştırılması gerekir. Bkz., **Küzeci,** Kişisel Veri, s. 405-406.

120 **Küzeci,** Kişisel Veri, s. 403.

üzere, KVKK.m.6/II-III hükmünde yer alan şartların oluşmasıyla hukuka aykırılık ortadan kalkacaktır. Aksi hâlde, örneğin, kişilerin sağlık verilerini kanunda yer alan sınırlar dâhilinde işleyen kamu kurumları hakkında güvenlik tedbiri uygulanması gerekir. Bu durum, suçun oluşup oluşmadığı noktasında ciddi sorunları beraberinde getireceği için öğretide eleştirilmektedir[121].

Hükmün geneline bakıldığında, sadece kişisel verileri *kaydetme* işleminin suç olarak nitelendirildiği açıkça görülecektir. Söz konusu kaydetme işleminin, dijital veya fizikî ortamda olması arasında bir ayrım gözetilmediği yine gerekçede ifade edilmiştir. Bu noktada, kayıt yöntemi açısından da bir fark yoktur[122].

Kişisel verilerin kaydedilmesinin nitelikli hâline ise, Türk Ceza Kanununun 137 nci maddesinde yer verilmiştir. Buna göre, kişisel verilerin kaydedilmesi, *kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle* ya da *belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle* işlenirse, verilecek ceza yarı oranında artırılır.

III. VERİLERİ HUKUKA AYKIRI OLARAK VERME, YAYMA VE ELE GEÇİRME

Türk Ceza Kanununun 136 ncı maddesine göre, *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan[123] dört yıla kadar hapis cezası ile cezalandırılır"*. Bu noktada, hukuka aykırı olarak verme, yayma veya ele geçirme hareketleri - herhangi birini gerçekleştirmekle suç oluşacağı için - seçimlik hareketler olarak ifade edilmektedir[124]. Hüküm, hukuka uygun olarak elde edilse dâhi, kişisel verilerin üçüncü kişilere hukuka aykırı olarak verilmesini, yayılmasını ve üçüncü kişiler tarafından ele geçirilmesini önleme amacı

---

121 Bkz., **Küzeci,** Kişisel Veri, s. 403, dn. 329; **Şen,** s. 1205.

122 Muammer **Ketizmen,** Türk Ceza Hukukunda Bilişim Suçları, Ankara 2008, s. 233.

123 21.2.2014 tarihli ve 6526 sayılı kanunun 4 üncü maddesiyle fıkranın önceki hâlinde yer alan "bir yıldan" ibaresi "iki yıldan" şeklinde değiştirilmiştir.

124 **Küzeci,** Kişisel Veri, s. 406; **Şen,** s. 1209; Sabire Sanem **Yılmaz,** Tıp Alanında Kişisel Verilerin Açıklanması Suçu, Terazi Hukuk Dergisi, C. 11, S. 119, 2016, s. 278.

taşımaktadır[125]. Kanunun açık ifadesi gereği, kişisel verilerin kaydedilmesinde öngörülen nitelikli hâller (TCK.m.137) burada da uygulama alanı bulur.

IV. VERİLERİ YOK ETMEME

Türk Ceza Kanununun 138 inci maddesine göre, *"Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar[126] hapis cezası verilir"*. Bu hüküm, kişisel verilerin işlenmesinde uyulması gereken genel ilkeler kapsamında yer alan sınırlı süre muhafaza edilme ilkesini ile de bağdaşır niteliktedir. Gerçekten, kişisel veriler, işlenme amacı için gerekli olan veya ilgili mevzuatta yer verilen süre kadar tutulmalı ve daha sonra silinmeli, yok edilmeli veya anonimleştirilmelidir (KVKK.m.7). Hükümde yer alan *sistem içinde yok etme* ifadesinin dijital sistemleri çağrıştırması sebebiyle, otomatik yollarla işlenen veriler açısından bu suçun oluşabileceği gibi bir izlenim yarattığı ifade edilmektedir[127]. Öte yandan, sistemden anlaşılması gerekenin bir veri kayıt sistemi olduğu düşünüldüğünde, sistem, hem fizikî hem de elektronik ortam şeklinde ortaya çıkabilir (KVKK.m.3/I-h).

Bu noktada, Türk Ceza Kanununda yer alan kişisel verileri yok etmeme hâlinin suç olarak düzenlenmesi, silmeme ve anonimleştirmeme hâlinin de suçu oluşturup oluşturmayacağı sorusunu gündeme getirir. Kişisel Verilerin Korunması Kanunu ile Türk Ceza Kanunun aynı tarihlerde kabul edilmemesinin ortaya çıkardığı bu sorun, KVKK.m.17/II hükmü ile giderilmeye çalışılmıştır. Buna göre, kanunda yer verilen hükümler çerçevesinde, kişisel verileri silmeyen veya anonimleştirmeyen kişiler de TCK.m.138 hükmü çerçevesinde cezalandırılacaklardır.

---

125 **Ketizmen,** s. 240; **Yılmaz,** s. 280.

126 21.2.2014 tarihli ve 6526 sayılı kanunun 5 inci maddesiyle fıkranın önceki hâlinde yer alan "altı aydan bir yıla kadar hapis" ibaresi "bir yıldan iki yıla kadar hapis" şeklinde değiştirilmiştir.

127 *Ketizmen'e* göre, kişisel veriyi konu edinen diğer suçlarda yer almayan bu ifade, yok etmeme suçunun sadece otomatik yollarla işlenen kişisel verilere ilişkin olduğu gibi bir sonucu ortaya çıkarır. Bu sebeple, kanundan çıkarılması gerekir. Bkz., **Ketizmen,** s. 242; aynı yönde bkz., **Küzeci,** Kişisel Veri, s. 408.

SONUÇ

Kişisel veri, belirli veya belirlenebilir nitelikteki gerçek kişiye ilişkin her türlü bilgiyi ifade eder. Bu tanım, yanlış, açığa çıkarılmış, nesneye ait olsa bile kişiyi belirli kılabilecek her türlü bilgiyi kapsamında alacak niteliktedir. Bu tanımın yer verildiği 6698 sayılı Kişisel Verilerin Korunması Kanunu, çoğu uluslararası düzenlemede olduğu gibi, sadece gerçek kişiye ilişkin kişisel verileri koruma altına almıştır. Cenine ait veriler ise, sağ ve tam doğmak kaydıyla ana rahmine düştüğü andan itibaren korunabilecektir. Ölülere ilişkin veriler ise, kişilik sona erdiği için, kural olarak, koruma kapsamında değildir. Bununla birlikte, ölüye ilişkin veri, genetik veriler gibi hayatta olan yakınlarını belirli veya belirlenebilir kılacak nitelikteyse, korunmalıdır. Tüzel kişilere ilişkin kişisel veriler ise, her alana özgü düzenlemeler çerçevesinde korunabilir. Böyle bir düzenlemenin bulunmaması hâlinde, ideal amaç taşıyan tüzel kişilerin MK.m.23 ve 24 hükümleri çerçevesinde, iktisadî amaç taşıyan tüzel kişilerin ise, haksız rekabet hükümleri çerçevesinde korunmasına ilişkin görüş kabul edilebilir.

Kanunda özel nitelikli kişisel verilere ilişkin bazı kategoriler sınırlı sayıda verilmiştir. Bu kategorilere ait verilerin, kullanım amacından bağımsız olarak özel nitelikli kişisel veri olarak değerlendirilmesi ve özel nitelikli kişisel verilerin tâbi olduğu kurallara uygun olarak işlenmesi gerekir. Zira, bir veri hukuka uygun olarak işlenmesi, o verinin hukuka aykırı olarak işlenmesi riskini de beraberinde getirmektedir. Başka bir anlatımla, hukuka uygun olarak elde edilen cinsel hayata ilişkin bilgi nerede kullanılacağından bağımsız olarak özel nitelikli kişisel veridir. Onun ayrımcılığa sebep olmayacak şekilde genel nitelikli kişisel verilerin tabi olduğu kurallara göre işlenmesi, ilgili kişinin ileride ayrımcılığa uğramayacağını garanti etmeyecektir.

Kişisel verilerin korunmasını talep etme hakkı, aslında, temel hak ve özgürlüklerin korunmasını esas alan bir haktır. Genel yönelim, bu hakkın kişilik hakları içerisinde yer aldığı yönünde olmakla birlikte, nitelik açısından verilerin geleceğini belirleme hakkı çerçevesinde değerlendirilmesi gerektiğini ifade edilmektedir.

Kanunda kişisel verilerin işlenmesine ilişkin şartların düzenlendiği hükümlerden çıkarılabilecek ortak sonuç, kişisel verilerin işlenmesinin, kural olarak, hukuka aykırı olmasıdır. Bu hukuka aykırılığın ortadan kalkması ancak, kanunda düzenlenen hâllerde mümkün olacaktır. Bu hâllerin ilki ilgili kişinin açık rızasının bulunmasıdır. Açık rızanın hukuka aykırılığı ortadan kaldırması için gereken unsurlara dikkat edilmelidir. Bu noktada, ilgili kişilerin çoğu zaman zayıf konumda bulunduğu dikkate alınarak serbest iradenin oluşup oluşmadığı incelenmelidir. Diğer hukuka uygunluk sebepleri ile açık rıza arasında herhangi bir öncelik sonralık ilişkisi bulunmadığı için, veri sorumlusu, uygun olan hukukî sebebe dayanarak kişisel verileri işleyebilecektir. Bu noktada hangi hukukî sebebe dayanılırsa dayanılsın, genel ilkelere uygun davranma yükümlülüğü devam etmektedir.

İlgili kişinin Kişisel Verilerin Korunması Kanununda yer alan haklarının anayasa ile güvence altına alındığı önemle belirtilmelidir. Bu noktada, zararın giderilmesini talep etme hakkının da diğer haklar gibi veri sorumlusuna başvuru yoluyla kullanılması gerektiği söylenebilir. Zira, ilgili kişinin bu hakkını kullanmaksızın genel hükümler yoluyla zararın tazminini talep etme hakkı saklı tutulmuştur. Veri sorumlusu ise, bir takım yükümlülüklerin yerine getirilmesi hususunda yükümlü kılınmıştır. Bu yükümlülüklerden veri güvenliğini sağlamaya yönelik teknik ve idarî tedbirlerin alınması noktasında veri işleyen ile müştereken sorumlu tutulması, öğretide müteselsil sorumluluk şeklinde anlaşılmıştır. Herhangi bir yanlış anlaşılmaya sebebiyet verilmemesi için, olası bir kanun değişikliğinde müştereken ifadesinin müteselsilen şeklinde düzeltilmesi düşünülebilir.

Kişisel verilerin hukuka aykırı olarak işlenmesi sebebiyle, ilgili kişi veri sorumlusuna başvuru yolunu tükettikten sonra Kişisel Verileri Koruma Kuruluna şikâyet hakkını kullanabilir. İlgili kişi, dilerse genel hükümler çerçevesinde zararın giderilmesini de talep edebilir. Bu noktada, Kişisel Verilerin Korunması Kanunu herhangi bir sorumluluk türü belirlemediği için, kişisel verilerin hukuka aykırı olarak işlenmesinin temelde haksız fiil sorumluluğu olduğu göz önüne alınarak bazı belirlemelerin yapılması gerekir.

Borçlar hukukunda, kural olarak, kusur sorumluluğu ilkesi geçerlidir. Bazı istisnaî hâllerde kusurun ispatının zorluğu dikkate alınarak kanunda kusursuz

sorumluluk hâlleri öngörülmüştür. Her ne kadar Kişisel Verilerin Korunması Kanununda bir belirleme yapılmamışsa da kişisel verilerin hukuka aykırı olarak işlenmesinden doğan sorumluluğun bir kusursuz sorumluluk olduğunun kabulü gerekecektir. Zira, çoğu zaman verilerin işlendiğinden dâhi haberdar olmayan ilgili kişiye kusuru ispatlama yükümlülüğünün getirilmesi mümkün değildir. Ayrıca, kişisel verilerin işlenmesinden doğan sorumluluk, onun hukuka aykırı olarak işlenmesine ilişkin riskten kaynaklanmaktadır. Bu belirlemelerin bir görüşten öteye gitmesi için, Kişisel Verilerin Korunması Kanununda yapılacak bir değişiklikle bu hususların açıklığa kavuşturulması gerekir.

KAYNAKÇA

AÇIKGÖZ, Osman : Kişisel Verilerin Hukuka Aykırı Şekilde Elde Edilmesi ve İnternet Bankacılığında Kullanılması Sonucu Malvarlığı Zarara Uğratılan Bankaya Karşı Mevduat Sahibinin Hukukî Sorumluluğu, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 22, S. 1, 2016, s. 389-432.

AKDAĞ, Hale : Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2013

AKGÜL, Aydın : Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, İstanbul 2014. (Akgül, Veri)

AKGÜL, Aydın : Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı, Türkiye Barolar Birliği Dergisi, S. 118, s. 119-222. (Akgül, Biyometrik)

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

AKİPEK, Jale /

AKINTÜRK, Turgut /

ATEŞ, Derya : Türk Medenî Hukuku, C. 1, Başlangıç Hükümleri, Kişiler Hukuku, 12. Baskı, İstanbul 2015.

AKKURT, Sinan Sami : 17.06.2015 Tarih, E. 2014/4-56, K. 2015/1679 Sayılı Yargıtay Hukuk Genel Kurulu Kararı ve Mukayeseli Hukuk Çerçevesinde "Unutulma Hakkı", Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 64, S. 4, 2016, s. 2605-2635. (Akkurt, Yargıtay)

AKKURT, Sinan Sami : Türk Sivil Havacılık Mevzuatı ve Uluslararası Konvansiyonlar Kapsamında Sivil Havayolu ile Yolcu Taşımacılığından Kaynaklanan Hukukî Sorumluluk, Ankara 2014. (Akkurt, Sivil Havayolu)

AKSOY, Hüseyin Can : Kişisel Verilerin İşlenmesi Kapsamında Rıza Unsuru ve Sınırlı Ehliyetsizlerin Durumu, Haluk Konuralp Anısına Armağan, C. 3, Ankara 2009, s. 47-68. (Aksoy, Rıza)

AKSOY, Hüseyin Can : Medeni Hukuk ve Özellikle Kişilik Haklarının Korunması Yönünden Kişisel Verilerin Korunması, Ankara 2010. (Aksoy, Veri)

ALTUNER, İlyas : Hipokrat Yemini, Iğdır Üniversitesi Sosyal Bilimler Dergisi S. 7, Nisan 2015, s. 1-7.

ARBAY, Rona : İnsan Hakları Hukuku, 2. Baskı, İstanbul 2015.

ARTİCLE 29 DATA PROTECTİON WORKİNG PARTY : Guidelines on Personal Data Breach Notification Under Regulation 2016/679, WP 250, https://ec.europa.eu/newsroom/document.cfm?doc_id=47741

: Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679, WP 253, https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

: Guidelines on the Right to Data Portability, WP 242, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

: Opinion 03/2013 on Purpose Limitation, WP 203, https://ec.europa.eu/justice/article-

29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

: Opinion 4/2007 on The Concept of Personal Data, WP 136, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

:Guidelines on the Right to Data Portability, WP 242, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 (Erişim Tarihi: 8.9.2018)

:Opinion 06/2014 on the Notion of Legitimate İnterests of the Data Controller Under Article 7 of Directive 95/46/EC, WP 217, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (Erişim Tarihi: 15.9.2018),

:Opinion 5/2004 on Unsolicited Communications for Marketing Purposes Under Article 13 of Directive 2002/58/EC, WP 90, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp90_en.pdf (Erişim Tarihi: 10.9.2018)

:Working Document 1/2008 on the Protection of Children's Personal Data, WP 147, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf (Erişim Tarihi: 8.9.2018)

: Guidelines on Consent under Regulation 2016/679, WP 259,

https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030

ATAAY, Aytekin : Şahıslar Hukuku, Giriş - Hakikî Şahıslar, 3. Baskı, İstanbul 1978.

ATAK, Songül : Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Güvenceler, Türkiye Barolar Birliği Dergisi, S. 87, 2010, s. 90-120.

ATASOY, Kemal : Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cevdet Yavuz'a Armağan, C. 22, S. 3, 2016, s. 269-301.

AYAN, Mehmet **:** Borçlar Hukuku, Genel Hükümler, 11. Baskı, Ankara 2016. (Ayan, Borçlar)

AYAN, Mehmet **:** Eşya Hukuku, C. 2, Mülkiyet, 9. Baskı, Ankara 2016. (Ayan, Mülkiyet)

AYAN, Mehmet **:**Kişilik Hakkı Açısından Kompüter Gizliliği, Yayınlanmamış Yüksek Lisans Tezi, Diyarbakır 1986. (Ayan, Kompüter)

AYAN, Mehmet/

AYAN, Nurşen : Kişiler Hukuku, 8. Baskı, Ankara 2016. (Ayan / Ayan, Kişiler)

AYAN, Mehmet/

AYAN, Nurşen : Medenî Hukuka Giriş, 12. Baskı, Ankara 2016. (Ayan / Ayan, Medenî)

AYÖZGER ÖNGÜN,

A. Çiğdem : Kişisel Verilerin Korunması Hukuku, Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil, 2. Baskı, İstanbul 2019.

BADUR, Emel : Üremeye Yardımcı Tedavi Uygulamalarında Kişisel Verilerin Korunması, Evrensel Hukuk İlkeleri Işığında Türk Medenî Hukukunda Değişimler Sempozyumu, 10-11 Haziran 2016, Çankaya Üniversitesi Hukuk Fakültesi, 2016, s.173-194.

BAŞALP, Nilgün : Avrupa Birliği Veri Koruması Genel Regülâsyonu'nun Temel Yenilikleri, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 21, S. 1, 2015, s. 77-105. (Başalp, Avrupa Birliği)

BAŞALP, Nilgün : Kişisel Verilerin Korunması ve Saklanması, Ankara 2004. (Başalp, Veri)

BELGE, Ayşe Merve : Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlâli ve Korunması Yolları, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Şeref Ertaş'a Armağan, C. 19, Özel Sayı, 2017, s. 1025-1051.

BENTHAM, Jeremy /

PEASE - WATKİN, Catherine /

WERRET, Simon : Panoptikon, Gözün İktidarı, (Çev. Barış Çoban / Zeynep Özarslan), 2. Baskı, İstanbul 2016.

BÜK, Alaattin : Bilişim Alanında Kişisel Verilerin Korunması, Ankara 2018.

CENTEL, Tankut : İş Hukuku: Bireysel İş Hukuku, C. 1, İstanbul 1994.

ÇEKİN, Mesut Serdar : 6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestîsi Açısından Değerlendirilmesi, İstanbul Üniversitesi Hukuk

Fakültesi Mecmuası, C. 74, S. 2, 2016, s. 629-644. (Çekin, Big Data)

ÇEKİN, Mesut Serdar : Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu, İstanbul 2018. (Çekin, Kişisel Veri)

DEMİR, Mehmet : Kişiliğin Korunması ve Sağlık Bilişim(i) Hukuku Açılarından Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirilmesi, Prof. Dr. Ejder Yılmaz'a Armağan, C. 1, 2014, s. 743-754.

DEVELİOĞLU,

H. Murat : 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, İstanbul 2017.

DOĞAN, Murat : İnternette Şahsiyet Haklarının İhlali, Bilgi Toplumunda Hukuk, Ünal Tekinalp'e Armağan, C. II, 2003.

DURA, Cihan **/**

ATİK, Hayriye : Bilgi Toplumu, Bilgi Ekonomisi ve Türkiye, İstanbul 2002

DURAK, Yasemin : İnternet Yoluyla Kişilik Haklarına Saldırı ve Hukukî Koruma, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 22, S. 1, 2014, s. 101-126.

DURAL, Mustafa /

ÖĞÜZ, Tufan : Türk Özel Hukuku, Cilt 2, Kişiler Hukuku, 15. Baskı, İstanbul 2014.

EREN, Fikret : Borçlar Hukuku Genel Hükümler, 18. Baskı, Ankara 2015.

EUROPEAN DATA PROTECTİON SUPERVİSOR: Opinion on The Data Protection Reform Package, bkz., https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf (Erişim Tarihi: 16.9.2018)

FEYZİOĞLU,

F. Necmettin : Borçlar Hukuku Genel Hükümler, C. 2, 2. Baskı, İstanbul 1977.

GÜLTAN, Seçkin : Bilgi Toplumu Sürecinde Avrupa Birliği ve Türkiye, Ankara 2003.

GÜRPINAR, Damla : Kişisel Verilerin Korunamamasından Doğan Hukukî Sorumluluk, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Şeref Ertaş'a Armağan-I, C. 19, Özel Sayı, 2017, s. 679-694.

GÜRSEL, İlke : Kişisel Verilerin Korunması Hakkının İşçi ve İşveren İlişkisine Etkileri, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, C. 13, S. 50, 2016, s. 763-847.

HATEMİ, Hüseyin / **GÖKYAYLA,** Emre : Borçlar Hukuku, Genel Bölüm, 3. baskı, İstanbul 2015.

HELVACI, Serap /

AYDIN, Gülşah Sinem : Kişilik Hakkı İhlâlinden Doğan Vekâletsiz İşgörmede Kusurun Bir Şart Olarak Aranıp Aranmayacağı Sorunu, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 23, S. 1, s. 265-301, s. 271.

HENKOĞLU, Türkay : Bilgi Güvenliği ve Kişisel Verilerin Korunması, Ankara 2015.

İNCE AKMAN, Nurten : Mirasbırakanın Dijital Bilgilerinin Mirasçılara Geçişi (Dijital Tereke), İnönü Üniversitesi Hukuk Fakültesi Dergisi, C. 9, S. 2, 2018, s. 527-560.

KANG, Jerry :Information Privacy in Cyberspace Transaction, Stanford Law Rewiew, C. 50, 1998, s. 1193-1294.

KARAOSMANOĞLU,

Fatih : İnsan Hakları, 2. Baskı, Ankara 2012.

KARLIDAĞ, Serpil : Ekonomi Politik Açıdan Kişisel Verilerin Korunması, Amme İdaresi Dergisi, C. 46, S. 1, 2013, s. 127-152.

KARTAL, Mustafa Tevfik : Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme, Uluslararası Ekonomi ve Yenilik Dergisi, C. 4, S. 1, 2018, s. 1-18.

KAYA, Cemil : Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 69, S. 1-2, 2011, s. 317-334.

KESER BERBER, Leyla /

ÜLGÜ, Mahir M. /

ER Cüneyd : Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği, İstanbul 2009.

KESER BERBER, Leyla : Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması, İstanbul 2014.

KETİZMEN, Muammer : Türk Ceza Hukukunda Bilişim Suçları, Ankara 2008.

KILIÇOĞLU, Ahmet : Borçlar Hukuku, Genel Hükümler, 18. Baskı, Ankara 2014.

KILINÇ, Doğan : Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 61, S. 3, 2012, s. 1089-1169.

KOCAYUSUFPAŞAOĞLU,

Necip : Borçlar Hukuku Genel Bölüm, C. 1, İstanbul 2010.

KORKMAZ, İbrahim : Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, Türkiye Barolar Birliği Dergisi, S. 124, 2016, s. 81-152.

KÜZECİ, Elif : Kişisel Verilerin Korunması, 2. Baskı, Ankara 2018.

LİTMAN, Jessica : Information Privacy / Information Property, Stanford Law Rewiew, C. 52, 2000, s. 1283-1313.

LUBARSKY, Boris : Re-Identification of "Anonymized" Data, GeorgeTown Law Technology Review, C. 202, 2017, s. 202-213.

MANAV, Eda : İş İlişkilerinde İşçinin Kişisel Verilerinin Korunması, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. 19, S. 2, 2015, s. 95-136.

OĞUZMAN, M. Kemal /

SELİÇİ, Özer /

OKTAY -ÖZDEMİR, Saibe : Kişiler Hukuku, (Gerçek ve Tüzel Kişiler), 14. Baskı, İstanbul 2014.

ÖNOK, Murat : Kişisel Verilerin Korunması Bağlamında "Unutulma Hakkı" ve Türkiye Açısından Değerlendirmeler, İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi, C. 16, S. 1, Ocak 2017, s. 155- 188.

ÖRNEK BÜKEN, Nüket /

ZEYBEK ÜNSAL, Çağrı : Kişisel Verilerin Korunması Kanununun Biyomedikal Alana Yansımaları Açısından Değerlendirilmesi, Hacettepe Hukuk Fakültesi Dergisi, C. 7, S. 2, 2017, s. 33-54.

ÖZDEMİR, Hayrunnisa : Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara 2009.

ÖZKAN, Işıl : Avrupa Birliği Kamu Hukuku, Lizbon Anlaşmasındaki Son Değişikliklerle, Ankara 2011.

ÖZSUNAY, Ergun : Gerçek Kişilerin Hukukî Durumu, 4. Baskı, İstanbul 1979.

PRİNS, Corien : When Personal Data, Behaviour and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?, Script-ed, C. 3, S. 4, 2006, s. 270-303.

REİSOĞLU, Safa : Türk Borçlar Hukuku, Genel Hükümler, 23. Baskı, İstanbul 2012.

SAYMEN, Ferit H. : Türk Medenî Hukuku, C. 2, 2. Baskı, İstanbul 1960.

SCHWARTZ, M. Paul : Property, Privacy and Personal Data, Harward Law Rewiew, C. 117, 2004, s. 2056-2128. (Shwartz, Property)

SCHWARTZ, Paul : The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, American Journal of Comparative Law, C. 37, S. 4, 1989, s. 675-701. (Schwartz, Self-Determination)

SEROZAN, Rona **:** Kişiler Hukuku, 6. Baskı, İstanbul 2015.

ŞEN, Ersan : Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, İstanbul Barosu Dergisi, C. 83, S. 3, 2009, s. 1197-1214.

ŞİMŞEK, Oğuz : Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008.

TAHMAZOĞLU

ÜZELTÜRK, Sultan : Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği, Legal Hukuk Dergisi, S. 93, 2010, s. 3151-3156.

TANDOĞAN, Haluk : Türk Mes'uliyet Hukuku, 1961 yılı Birinci Baskıdan Tıpkı Baskı, İstanbul 2010.

TAŞTAN, Furkan Güven : Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 2. Baskı, İstanbul 2017.

TEZCAN, Durmuş : Bilgisayar Karşısında Özel Hayatın Korunması, Anayasa Yargısı Dergisi, C. 8, 1991, s. 285-292.

UNCULAR, Selin : Kişisel Verilerin Korunması Kanunu ve AB Genel Veri Koruma Tüzüğü Kapsamında İş İlişkisinde İşçinin Kişisel Verilerin Korunması, 2. Baskı, Ankara 2018.

ÜNVER, Yener : Kişisel Verilerin Korunması, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, S. 1, 2008, 163-196.

VELİDEDEOĞLU,

H. Veldet : Türk Medenî Hukuku, 3. Baskı, İstanbul 1963.

YILMAZ, Sabire Sanem : Tıp Alanında Kişisel Verilerin Açıklanması Suçu, Terazi Hukuk Dergisi, C. 11, S. 119, 2016, s. 272-283.

YÜCEDAĞ, Nafiye : Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 75, S. 2, 2017, s. 765-790.

ZEVKLİLER, Aydın /

ACABEY, M. Acabey /

GÖKYAYLA, K. Emre : Medenî Hukuk, Giriş, Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku, 5. Baskı, İzmir 1997.

ZEYBEK ÜNSAL, Çağrı : Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri ile Uyumluluğu ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi, Hacettepe Hukuk Fakültesi Dergisi, C. 3, S. 1, 2013, s. 99-124.

ZORLU, Süheyla : İnternet Yoluyla Kişilik Hakkının İhlâli ve Korunması, (Yayınlanmamış Yüksek Lisans Tezi), Konya 2010.