

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

AVRUPA BİRLİĞİ VE TÜRK HUKUKUNDA
KİŞİSEL VERİLERİN KORUNMASI

Fatma Nur YILDIRIM

Danışman
Doç. Dr. Damla GÜRPINAR

İZMİR - 2019

YÜKSEK LİSANS
TEZ ONAY SAYFASI

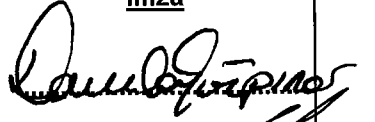
Üniversite : Dokuz Eylül Üniversitesi
Enstitü : Sosyal Bilimler Enstitüsü
Adı ve Soyadı : FATMA NUR YILDIRIM
Öğrenci No : 2014800691
Tez Başlığı : Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması

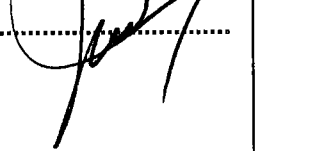
Savunma Tarihi : 25/10/2019
Danışmanı : Doç.Dr. Damla GÜRPINAR

JÜRİ ÜYELERİ

<u>Ünvanı, Adı, Soyadı</u>	<u>Üniversitesi</u>
Doç.Dr. Damla GÜRPINAR	- Dokuz Eylül Üniversitesi
Doç.Dr.Lale Burcu ÖNÜT	- Dokuz Eylül Üniversitesi
Doç.Dr.Burcu DÖNMEZ	- Yaşar Üniversitesi

İmza


.....

.....


FATMA NUR YILDIRIM tarafından hazırlanmış ve sunulmuş olan bu tez savunmada başarılı bulunarak oy birliği (✓) / oy çokluğu () ile kabul edilmiştir.

Doç. Dr. Erkan GÖKSU
Müdür V.

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum “Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması” adlı çalışmanın, tarafımdan, akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

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

Fatma Nur YILDIRIM



ÖZET

Yüksek Lisans Tezi

Avrupa Birlięi ve Türk Hukukunda Kişisel Verilerin Korunması

Fatma Nur YILDIRIM

Dokuz Eylül Üniversitesi

Sosyal Bilimler Enstitüsü

Kamu Hukuku Anabilim Dalı

Avrupa Birlięi Hukuku Programı

Bu çalışmamızda çağımızda Avrupa Birlięi ve Türk Hukuk sistemi içerisinde özel hayatın ve aile hayatının korunması hakkında bağımsız bir hak olarak kabul gören kişisel verilerin korunması hakkı incelenmiştir. Kişisel veri kavramının tanımı yapıldıktan sonra kişisel verilerin korunması ihtiyacı ve kişisel verilerin korunması hukukuna dair temel ilkeler irdelenmiş, daha sonra kişisel verilerin korunması hukukunun tarihsel sürecine değinilmiş, son olarak Avrupa Birlięi ve Türk Hukukunda yer alan yasaldüzenlemeler çerçevesinde kişisel verilerin korunması hukuku incelenmiştir. Çalışmada yöntem olarak kişisel verilerin korunması hakkına dair Avrupa Birlięi Veri Koruma Tüzüğü ile 6698 sayılı Kişisel Verilerin Korunması Kanunu arasındaki benzerlikler ve farklılıklar tespit edilerek, Türk Hukuk sistemi içerisinde 5237 sayılı Türk Ceza Kanunu, 4721 sayılı Türk Medeni Kanunu ve 6098 sayılı Türk Borçlar Kanunu'nda kişisel verileri koruma altına alan hükümler açıklanmıştır.

Anahtar Kelimeler: Kişisel Veri, Hassas Veri, Kişisel Verilerin Korunması, Veri Güvenlięi, Avrupa Birlięi Veri Koruma Tüzüğü, 6698 sayılı Kişisel Verilerin Korunması Kanunu.

ABSTRACT

Master's Thesis

Protection of Personal Data in EU and Turkish Law

Fatma Nur YILDIRIM

Dokuz Eylul University

Graduate School of Social Sciences

Department of Public Law

European Union Law Program

In this study, we examined the right of protection of personal data which regarded as a different right from the protection of private life and family life, in the context of EU and Turkish law. Firstly, we defined the concept of personal data, after that we addressed the need for protection of personal data and basic principles of personal data protection law. Later, historical process of personal data protection law is mentioned. Finally, the personal data protection law is examined in the frame of EU and Turkish regulations. The similarities and differences between EU General Data Protection Regulation and Turkish Personal Data Protection Law No: 6698 is compared. Personal data protection provisions in Turkish Criminal Code No: 5237, Turkish Civil Code No: 4721 and Turkish Obligations Code No: 6098 are explained.

Keywords: Personal Data, Sensitive Data, Personal Data Protection, Security of Data, EU General Data Protection Regulation, Turkish Personal Data Protection Law No. 6698.

**AVRUPA BİRLİĞİ VE TÜRK HUKUKUNDA
KİŞİSEL VERİLERİN KORUNMASI**

İÇİNDEKİLER

TEZ ONAY SAYFASI	ii
YEMİN METNİ	iii
ÖZET	iv
ABSTRACT	v
İÇİNDEKİLER	vi
KISALTMALAR	xii
GİRİŞ	1

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASI HAKKI

I.KİŞİSEL VERİ	3
A. Kişisel Verinin Tanımı	3
B. Kişisel Verinin Unsurları	4
1. Bilgi	4
2. Kimliği Belirli veya Belirlenebilir Kişi	6
3. İlişkin Olma	7
C. Hassas Kişisel Veri	8
II.KİŞİSEL VERİLERİN KORUNMASI	11
A. Kişisel Verilerin Korunması İhtiyacı	11
B. Kişisel Verilerin Korunması Hakkının Hukuki Niteliği	12
1. Mülkiyet Hakkı	12
2. Fikri Mülkiyet Hakkı Görüşü	13
3. Kişilik Hakkı Görüşü	14
III. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN İLKELER	16
A. Verilerin Hukuka ve Dürüstlük Kuralına Uygun İşlenmesi İlkesi	17

B. Belirli, Açık ve Meşru Amaç İçin Toplama İlkesi	19
C. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması İlkesi	20
D. Doğru ve Gerekliğinde Güncel Olarak Tutulma İlkesi	20
E. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme İlkesi	21
F. Veri Güvenliği İlkesi	22
G. Kişisel Verilerin İşlenmesi Sırasında İlgili Kişinin Bilgilendirilmesi İlkesi	26
IV. İLGİLİ KİŞİNİN HAKLARI	28
A. Erişim Hakkı	28
B. Düzeltme Hakkı	31
C. Unutulma Hakkı	32
D. İtiraz Hakkı	32
E. İşleme Faaliyetinin Kısıtlanması Hakkı	34

İKİNCİ BÖLÜM

TARİHSEL SÜREÇ İÇERİSİNDE

KİŞİSEL VERİLERİN KORUNMASI HUKUKU

I. TARİHSEL SÜREÇ	35
II. ULUSLARARASI KURUMLAR BÜNYESİNDE YAPILAN DÜZENLEMELER	36
A. OECD (Ekonomik İşbirliği ve Kalkınma Örgütü)	36
B. Birleşmiş Milletler	38
1. İnsan Hakları Evrensel Beyannamesi	38
2. Birleşmiş Milletler Medeni ve Siyasal Haklara İlişkin Uluslararası Sözleşme	38
3. Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler	39
C. Avrupa Konseyi	40
1. 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi	41

2. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek: Denetleyici Makamlar ve Sınırışan Veri Akışına İlişkin Protokol	44
3. Avrupa İnsan Hakları Sözleşmesi	44
D. Avrupa Birliği	46
1. 95/46/AT Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi	47
a. Amacı ve Kapsamı	48
b. Temel Kavramlar	48
c. Temel İlkeler	50
d. İlgili Kişinin Hakları	51
e. Bağımsız Denetleme Makamı ve Veri Koruma Grubu	53
2. Avrupa Birliği Temel Haklar Şartı	53
3. Avrupa Parlamentosu ve Konseyi 2002/58/AT Sayılı Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Yönergesi	54
4. 2006/24/AT Sayılı İletişim Trafik Verilerinin Saklanması Yönergesi	54
5. 2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)	54

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNDA TÜRKİYE MEVZUATI

I.6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU	61
A. Kanunun Gerekçesi, Amacı ve Kapsamı	61
1. Kanunun Gerekçesi	61
2. Kanunun Amacı	62
3. Kanunun Kapsamı	63
B. Temel Kavramlar	63
1. Kişisel Veri ve Kişisel Verilerin İşlenmesi	63
a. Kişisel Veri	63
b. Kişisel Verinin İşlenmesi	65
2. Açık Rıza	66

3. Anonim Hale Getirme	68
4. Veri Kayıt Sistemi	69
5. Veri Sorumlusu ve Veri İşleyen	69
C. Kişisel Verilerin İşlenmesine İlişkin Genel İlkeler	71
D. Kişisel Verilerin İşlenme Şartları	72
1. Genel Olarak Kişisel Verilerin İşlenme Şartları	73
2. Özel Nitelikli Kişisel Verilerin İşlenme Şartları	74
E. Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi	75
F. Kişisel Verilerin Aktarılması	77
G. Veri Sorumlusuna Başvuru, Kurula Şikâyet ve Veri Sorumluları Sicili	81
1. Veri Sorumlusuna Başvuru	81
2. Kişisel Verileri Koruma Kurulu'na Şikâyet Yolu İle Yapılan Başvuru	82
3. Kişisel Verileri Koruma Kurulu Tarafından Yapılan İncelemenin Usul ve Esasları	82
4. Veri Sorumluları Sicili	83
H. Kişisel Verileri Koruma Kurumu ve Teşkilatı	85
1. Kişisel Verileri Koruma Kurumu	85
2. Kişisel Verileri Koruma Kurulu	86
a. Kurulun Görev ve Yetkileri	87
b. Kurulun Çalışma Esasları	88
İ. Yaptırım	89
1. Suçlar	89
2. Kabahatler	90
3. Tazminat	91
J. İstisnalar	91
II. 5237 SAYILI TÜRK CEZA KANUNUNDA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN SUÇLAR	93
A. Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)	94
1. Suç Tipi Hakkında Genel Bilgiler	94
2. Suçla Korunan Hukuki Değer	95
3. Suçun Unsurları	96
a. Tipikliği Maddi Unsurları	96

(1) Fail	96
(2) Mağdur	97
(3) Suçun Konusu	97
(4) Hareket (Eylem, Fiil)	101
b. Tipikliğin Manevi Unsurları	102
c. Suçun Hukuka Aykırılık Unsuru	103
4. Suçun Nitelikli Hali	104
5. Suçun Neticesi Sebebiyle Ağırlaşmış Hali	105
6. Teşebbüs	106
7. İştirak	106
8. İçtima	106
9. Yaptırım ve Kovuşturma Usulü	110
B. Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (TCK m. 136)	110
1. Suç Tipi Hakkında Genel Bilgiler	110
2. Suçla Korunan Hukuki Değer	111
3. Suçun Unsurları	111
a. Tipikliği Maddi Unsurları	111
(1) Fail	111
(2) Mağdur	112
(3) Suçun Konusu	112
(4) Hareket (Eylem, Fiil)	113
b. Tipikliğin Manevi Unsurları	115
c. Suçun Hukuka Aykırılık Unsuru	116
4. Suçun Nitelikli Hali	116
5. Suçun Neticesi Sebebiyle Ağırlaşmış Hali	117
6. Teşebbüs	117
7. İştirak	117
8. İçtima	118
9. Yaptırım ve Kovuşturma Usulü	119
C. Verileri Yok Etmeme Suçu (TCK m. 138)	120
1. Suç Tipi Hakkında Genel Bilgiler	120

2. Suçla Korunan Hukuki Değer	121
3. Suçun Unsurları	121
a. Tipikliği Maddi Unsurları	121
(1) Fail	121
(2) Mağdur	122
(3) Suçun Konusu	122
(4) Hareket (Eylem, Fiil)	122
b. Tipikliğin Manevi Unsurları	124
c. Suçun Hukuka Aykırılık Unsuru	124
4. Suçun Nitelikli Hali	125
5. Suçun Neticesi Sebebiyle Ağırlaşmış Hali	126
6. Teşebbüs	126
7. İştirak	126
8. İçtima	127
9. Yaptırım ve Kovuşturma Usulü	127
III. KİŞİSEL VERİLERİN 4721 SAYILI TÜRK MEDENİ KANUNU VE 6098 SAYILI TÜRK BORÇLAR KANUNU KAPSAMINDA KORUNMASI	128
SONUÇ	130
KAYNAKÇA	132

KISALTMALAR

ABAD	Avrupa Birliđi Adalet Divanı
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AT	Avrupa Topluluđu
ATAD	Avrupa Topluluđu Adalet Divanı
AÜHFD	Ankara Üniversitesi Hukuk Fakóltesi Dergisi
AYM	Anayasa Mahkemesi
bkz.	Bakınız
BM	Birleşmiş Milletler
BM Rehber İlkeleri	Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler
C.	Cilt
CMK	Ceza Muhakemesi Kanunu
Çev.	Çeviren
dn	dipnot
GVKT	Genel Veri Koruma Tüzüđu
İÜHFM	İstanbul Üniversitesi Hukuk Fakóltesi Mecmuası
K.	Karar Sayısı
KVK İmha Yön.	Kişisel Verilerin Silinmesi, Yok edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik
KVK Kurulu	Kişisel Verileri Koruma Kurulu
KVK Kurumu	Kişisel Verileri Koruma Kurumu
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
m.	madde
OECD	Ekonomik İşbirliđi ve Kalkınma Teşkilatı
OECD Rehber İlkeleri	Özel Yaşamın Korunmasına ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler
R.G.	Resmi Gazete
S.	Sayı
s.	sayfa

T.	Tarih
TAAD	Türkiye Adalet Akademisi Dergisi
TBBD	Türkiye Barolar Birliği Dergisi
TBK	6098 sayılı Türk Borçları Kanunu
TCK	5237 sayılı Türk Ceza Kanunu
TMK	4721 sayılı Türk Medeni Kanunu
Tüzük	Genel Veri Koruma Tüzüğü
vd.	ve devamı
YCGK	Yargıtay Ceza Genel Kurulu
Yönerge	Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi
108 Nolu Sözleşme	Kişisel Verilerin Otomatik İşleme Tabi Tutulmasında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi

GİRİŞ

Kişisel veri, belirli veya belirlenebilir bir kişiye ait tüm bilgilerdir. Endüstri 4.0 olarak adlandırılan sanayi devriminin dördüncü jenerasyonunu yaşadığımız ve hatta endüstri 5.0'a adım attığımız bu dönemde yapay zeka, nesnelerin interneti, robot teknolojileri, yeni nesil yazılım sistemleri, büyük veri, akıllı sistemler hayatımızın her alanına etki etmektedir. Bilim ve teknolojiadaki hızlı ve sınırsız gelişim, pek çok faydasının yanında kişisel verilerin istismar edilme riskini de her geçen gün daha da arttırmaktadır. Çağımızda temel hak ve özgürlüklerden özel hayatın ve aile hayatının korunması hakkından bağımsız olarak kabul gören kişisel verilerin korunması hakkı, Avrupa'da 1970'li yıllardan beri tartışılmaktadır. Uzun yıllar süren çalışmaların sonucunda 25 Mayıs 2018 tarihinde yürürlüğe giren Avrupa Birliği Veri Koruma Tüzüğü ile kişisel verilerin küresel düzeyde korunması amaçlanmıştır.

Ülkemizde ise 2010 yılı Anayasa değişikliği ile kişisel verilerin korunması hakkı, Anayasa ile koruma altına alınmıştır. Ardından 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu ile konuya olan ilgi daha da artmıştır. Kanun'un yapım sürecinde özellikle 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ile 95/46/AT Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiki Yönergesi olmak üzere uluslararası belgeler göz önüne alınarak kişisel verilerin korunması amaçlanmıştır.

Bu çalışmanın amacı da, kişisel verilerin korunmasına dair Avrupa Birliği ve Türk Hukuku'ndaki düzenlemeleri değerlendirmektir. Bu amaçla özellikle Avrupa Birliği Veri Koruma Tüzüğü ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun karşılaştırılması yoluyla her iki düzenlemenin incelenmesine önem verilmiştir. Konuyla ilgili kişisel verilerin korunması hukukunun temel belgeleri ve ilkeleri incelenmiş, Avrupa Birliği Veri Koruma Tüzüğü ile 6698 sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde kişisel verileri koruma altına alan yasal düzenlemelere değinilmiştir.

Çalışmamızın ilk bölümünde kişisel veri ve hassas kişisel veri kavramı açıklanarak, kişisel verilerin korunması ihtiyacı ele alınmıştır. Ayrıca kişisel verilerin

korunması hakkının hukuki niteliğine ilişkin öđretideki tartıřmalar deęerlendirilmiř ve son olarak kiřisel verilerin korunması hukukunun temel ilkeleri belirlenmiřtir.

İkinci bölümde, Avrupa’da tarihsel süreç ierisinde kiřisel verilerin korunması hukukunun geliřimi uluslararası kurumlar bünyesinde yapılan düzenlemelerle birlikte incelenmiřtir.

Üüncü ve son bölümde ise kiřisel verilerin korunması hukukunda Türkiye mevzuatı, 6698 sayılı Kiřisel Verilerin Korunması Kanunu, 5237 sayılı Türk Ceza Kanunu, 4721 sayılı Türk Medeni Kanunu ile 6098 sayılı Türk Borlar Kanunu çerevesinde ele alınmıřtır.



BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE KİŞİSEL VERİLERİN KORUNMASI HAKKI

I. KİŞİSEL VERİ

A. Kişisel Verinin Tanımı

Ulusal ve uluslararası metinlerde benzer şekilde tanımlandığı üzere kişisel veri, belirli veya belirlenebilir nitelikteki bir kişiye ilişkin tüm bilgilerdir. Kişisel veri bir anlamda bireyin kimliğini ortaya çıkaran, bireyi belirli veya belirlenebilir kılan bilgileri ifade etmektedir¹. Kişisel veri tanımından yola çıkarak kişisel verileri, kişisel olmayan verilerden ayırabilmek için temel üç ölçütün değerlendirilmesi gerekmektedir. Aşağıda detaylandıracağımız bu üç ölçüt; bilgi, kimliği belirli veya belirlenebilir kişi, bilginin kimliği belirli veya belirlenebilir kişiye ilişkin olmasıdır.

En basit hali ile yeni tanıştığımız bir kişinin bize aktardığı hatta aktarmasa dahi gözlemlerimiz sonucunda edindiğimiz bilgiler o kişinin kişisel verileridir. Hangi verilerin kişisel veri olduğu sayısal olarak sınırlandırılmasa da kişiyi belirli veya belirlenebilir kılan; kişinin adı, soyadı, yaşı, fiziksel özellikleri, kimlik bilgileri, telefon numarası, adresi, medeni durumu, mesleği, kanaatleri, özgeçmişi, eğitim durumu, sosyo- ekonomik durumu, sağlık bilgileri, banka bilgileri, elektronik posta adresi, ses ve görüntüsü gibi bilgileri kişisel verileridir². Bu noktada kişisel verileri belirlerken eldeki bilginin kişiyi belirli veya belirlenebilir kılacak nitelikte olmasına dikkat edilmelidir.

Kişisel verilerin korunmasına ilişkin mevzuatımız Avrupa'daki konuyla ilgili düzenlemeler esas alınarak oluşturulmuştur. OECD "Kişisel Verilerin Sınıraşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri"nde, 108 No'lu "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi"nde, 95/46/AT sayılı "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa

¹Aydın Akgül, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, Beta Yayınları, İstanbul, 2014, s. 8.

² Akgül, s. 8; Anayasa Mahkemesi 12.11.2015 tarihli 2015/32 E. 2015/102 sayılı kararı için bkz. RG, 2 Aralık 2015, S. 29550.

Konseyi Direktifi”nde ve Genel Veri Koruma Tüzüğü’nde birbiri ile benzer şekilde kişisel veri, kimliği belirli veya belirlenebilir kişiye ilişkin tüm bilgiler şeklinde tanımlanmıştır³. Avrupa’daki sayılan düzenlemeler ışığında 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu’nda da kişisel veri kavramı “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak açıklanmıştır.

B. Kişisel Verinin Unsurları

1. Bilgi

Uluslararası düzenlemelerde ve 6698 sayılı Kişisel Verilerin Korunması Kanunu’nda kişiye ait “her türlü bilgi” koruma altına alınmıştır.

Kişisel veri tanımı bakımından bilgi unsurunun ne ifade ettiğini açıklamadan önce doktrinde birbiri yerine geçecek şekilde kullanılmasının tartışmalara yol açması sebebiyle “veri” ve “bilgi” kavramlarına değinmekte fayda olacaktır. Veri, “bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi”⁴yi; bilgi ise “ anlamlı bir biçime sokularak, kullanıcısına güncel ve olası kararların alınmasında yardımcı olan veri”⁵yi ifade

³ Kişisel veri tanımına dair uluslararası düzenlemeler şöyledir: (a) OECD Rehber İlkelerinde “kimliği bilinen veya bulunabilecek olan bir şahsa (veri sahibi) ait her türlü bilgi”,(b) 108 No’lu Sözleşme’nin 2. maddesinde “kimliği belirli veya belirlenebilir bir gerçek kişi (“ilgili kişi”) hakkındaki tüm bilgiler”, (c) AB Veri Koruma Yönergesi’nin 2. maddesinde“fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilir kişi;tespit edilmiş veya tespit edilebilir gerçek kişiye (“veri öznese”) ilişkin herhangi bir bilgi”, (d) Genel Veri Koruma Tüzüğü’nün 4. maddesinde “kimliği bilinen veya bulunabilecek olan gerçek kişiler (“veri sahibi”) hakkındaki her türlü bilgiyi ifade eder; kimliği bilinen veya bulunabilecek olan bir gerçek kişi, özellikle adı, kimlik numarası, konumu verileri, internet üzerinden (online) kimlik belirleyici unsurlar gibi kimlik belirleyici unsurlara ya da o gerçek kişinin fizikseli fizyolojik, genetik, akılsal, ekonomik, kültürel veya sosyal kimliğine özel bir veya birden fazla faktör vasıtasıyla doğrudan veya dolaylı olarak kimliği tespit edilebilecek olan bir gerçek kişi” olarak tanımlanmıştır. Bora Gemicioğlu, Zeynephan Gemicioğlu, Mine Yağcı ve Alara Yılmaz, **Kişisel Verilerin Korunması Mevzuatı Uluslararası Düzenlemeler ve İçtihatlar**, Onikilevha Yayınları, İstanbul, 2019, s. 265.

⁴ Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, Hukuk Akademisi, İstanbul, 2019, s. 6.

⁵ Elif Küzeci, **Kişisel Verilerin Korunması**, Turhan Kitabevi, Ankara, 2019, s. 11.

etmektedir. Bu bağlamda, verinin kişi tarafından anlaşılmış hali bilgi olacaktır⁶. Bütün veriler bilgi olarak kabul edilebilirken bütün bilgiler veri olarak kabul edilemeyecektir⁷. Her iki kavram esasen farklı anlamlara gelse de günümüzde 6698 sayılı Kişisel Verilerin Korunması Kanunu ve uluslararası metinlerde bu iki kavram birbiri yerine geçecek şekilde kullanılmaktadır. Anlamsal farklılıklarını kabul etmekle birlikte çalışmamızda kişisel verilerin korunması hukuku irdelendiğinden bu iki kavramın birbiri yerine kullanıldığını belirtmek isteriz.

Kişisel verilerin korunması hukuku anlamında kişiye ait tüm bilgiler kişisel veri olarak kabul edilmektedir. Sınırlı ve açık bir kapsam belirlenemediğinden “tüm bilgiler” ifadesinin geniş şekilde yorumlanması hak ihlallerinin önüne geçebilmek adına yerinde olacaktır. 6698 sayılı Kişisel Verilerin Korunması Kanunu’nda yer alan tanımdan kanun koyucunun da geniş şekilde yorumlama iradesinin varlığı anlaşılmaktadır. Sayılan unsurları sağlayana verilerin kişisel veri olarak kabul edilmesi gerekecektir.

Kişiye ilişkin öznel veya nesnel bilgiler, doğruluğu kanıtlanmamış hatta yanlış bilgiler, önemsiz bilgiler dahi somut olayın özelliğine göre kişisel veri olarak kabul edilebilecektir⁸. Kişinin yaşı, kilosu, boyu, sağlık durumu, genetik bilgileri gibi nesnel verileri ile kişi hakkında yapılan güzel- çirkin, zengin- fakir gibi öznel değerlendirmeler de kişisel veri sayılabilecektir. Yine bir kişinin nüfusa kayıtlı adının herkesçe farklı bilinmesine rağmen o kişiyi belirlemek için yanlış olan ad kullanılabiliyorsa bu bilgi de kişisel veridir⁹.

Bir verinin kişisel veri olarak kabul edilebilmesi için bu bilginin ilgili kişi tarafından gizli tutulmuş olması gerekli değildir. Kişinin kendisi tarafından alenileştirdiği ya da herkes tarafından kolayca ulaşılabilen bilgileri de kişisel veridir¹⁰. Kişinin elektronik posta şifresi gibi gizli bilgileri yanında sosyal paylaşım sitelerinde paylaşmış olduğu bilgileri, fotoğrafları, yazıları da kişisel veri kapsamında yer almaktadır.

⁶ Furkan Güven Taştan, **Türk Sözleşmeler Hukukunda Kişisel Verilerin Korunması**, Onikilevha Yayıncılık, İstanbul, 2007, s. 40.

⁷ Akgül, s. 10.

⁸ Dülger, s. 8; Taştan, s. 41; Akgül, s. 12; Mehmet Hanifi Bayram, **Avrupa Birliği ve İnternet Hukuku**, Seçkin Yayınları, Ankara, 2011, s. 23.

⁹ Dülger, s. 9.

¹⁰ Dülger, s.10; Taştan, s. 40.

Kişiye ait bilgiler kâğıt üzerinde, bilgisayarda, kamera, ses veya görüntü kayıt araçlarında; yazılı, fotoğrafik, akustik veya sayısal biçimde tutuluyor olabilir¹¹. Farklı bir şekilde veya yerde bulunuyor olması kişisel veri olma niteliğini etkilemeyecektir.

2. Kimliği Belirli veya Belirlenebilir Kişi

Kişisel verilerin korunması hakkı gerçek kişiye ait bilgilerin korunması isteği ve ihtiyacı sonucunda doğmuştur. Çoğu veri koruma yasası ve ulusal mevzuatımızda gerçek kişiye ait bilgiler koruma altına alınmıştır¹².

6698 sayılı Kişisel Verilerin Korunması Kanun’unda açıkça gerçek kişilere ait verilerin Kanun kapsamında korunacağı öngörülmüştür. Ancak bu noktada tartışmalı olan husus; tüzel kişiye ait verilerin bir gerçek kişi ile ilişkilendirilebilir nitelikte olması halinde kişisel veri olarak korunup korunmayacağıdır. Tüzel kişiye ait verilerin korunmayacağını savunan görüşe göre; tüzel kişiye ait veriler ancak ticari sır kapsamında korunacaktır¹³. Aksini savunan görüşe göre; tüzel kişiye ait veri ile gerçek kişi belirli veya belirlenebilir hale geliyorsa bu verinin kişisel veri olarak korunması gerekir¹⁴. Bu bağlamda tüzel kişiye has ticaret unvanı, MERSİS/vergi kimlik numarası tek başına kişisel veri değildir. Ancak bir veritabanında şirketin ticaret unvanı ve adresinin yanında şirket çalışanlarının da ismi yer alıyorsa gerçek

¹¹ Dülger, s. 9.

¹² Bunun yanında gerçek kişilere ait verilerin yanı sıra tüzel kişilere ait veriler Avrupa Birliği’nin 2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin Direktif ile koruma altına alınmıştır. Hukukumuzda da 24 Temmuz 2012 tarihli Resmi Gazete’de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik ile 2002/58/EC Yönergesi’ne benzer bir koruma öngörülmüştür. Taştan, s. 31.

¹³ Durmuş Tezcan, **Bilgisayar Karşısında Özel Hayatın Korunması**, Anayasa Yargısı, 1991, C.8, 385-395, s.389 (Çiğdem Aygözer Öngün, **Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, Beta Yayınları, İstanbul, 2019, s. 10 Naklen); Taştan, kar amacı güden tüzel kişiler ile kar amacı gütmeyen tüzel kişileri ikiye ayırarak; kar amacı gütmeyen tüzel kişilere ait verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ile olmasa da genel koruma yollarıyla korunması gerektiğini savunmaktadır. Taştan, s. 33.

¹⁴ Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Yetkin Yayınları, Ankara, 2004, s. 35 dn 53’ deki yazar; Dülger, s. 10; Akgül, s.15; Ersan Şen, **Kişisel Verilerin Korunması Kanunu Tasarısı’nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi**, İstanbul Barosu Dergisi 2009, C. 83, S.3, 1197-1214, s. 1201.

kişinin işyeri ve işyeri adresi belirli hale geldiğinden bu veriler kişisel veri olarak kabul edilecektir¹⁵.

Kişisel verilerin korunması hakkı bireyin kişilik hakkının bir sonucu olduğundan tüzel kişiler bu hakkın sujesi olamayacaklardır¹⁶. Kanaatimizce tüzel kişiye ait gibi gözükse de esasen gerçek kişinin hakları koruma altına alındığından; tüzel kişilerin sadece gerçek kişiler ile ilişkilendirilebilen bilgilerinin korunması gerekmektedir.

Eldeki bilginin, kişisel veri sayılabilmesi için bir gerçek kişiyi belirli veya belirlenebilir kılması gerekir. Belirli olma, kişinin parmak izi, kimlik numarası gibi makul vasıtalar ile doğrudan tespit edilebilir olmasıdır¹⁷. AB Veri Koruma Yönergesi'nde Kişisel Verilerin Korunması Kanunu'ndan farklı olarak "belirlenebilir" kavramına açıklık getirilmiştir. Buna göre belirlenebilirlik; doğrudan veya dolaylı olarak özellikle bir kimlik numarası veya kişinin fiziksel, psikolojik, ruhsal, ekonomik, kültürel veya sosyal kimliğine bir veya birden fazla spesifik faktör ile ilişkilendirilebilmesi suretiyle kişinin belirlenebilir hale gelmesini sağlayan tüm haller olarak açıklanmıştır¹⁸. Kişinin belirli veya belirlenebilir olması her somut olayın özelliğine göre karar verilmesi gereken bir unsurdur. Örneğin bir topluluk içerisinde kırmızı arabaya sahip biri için arabasının rengi kişiyi belirli kılabilirken; kişinin kırmızı arabasının olması Türkiye'de yaşayanlar açısından kişiyi belirlenebilir kılmayacaktır. Benzer şekilde bilgisayar IP adresleri ile bilgisayarın birden çok kişi tarafından kullanıldığı durumlarda kişi doğrudan tespit edilemese de belirlenebilir hale gelmektedir¹⁹.

3. İlişkin Olma

Kişisel verileri koruma hukuku anlamında bir bilgiden söz edebilmek için bilginin, kişiyi belirli veya belirlenebilir kılarak o kişiye ilişkin olması zorunlu bir

¹⁵Armağan Ebru Bozkurt Yüksel, **Bulut Bilişimde Kişisel Verilerin Korunması (Personal Data Protection in Cloud Computing)**, Yetkin Yayınları, Ankara, 2016, s. 89.

¹⁶Şimşek, s. 123.

¹⁷Taştan, s. 37; Şimşek, s. 122; Aygözer Öngün, s. 12.

¹⁸Küzeci, s. 315; Başalp, s. 33; Akgül, s. 16.

¹⁹Aygözer Öngün, s. 12.

unsurdur²⁰. Bilgi ile kişinin belirlenemediği veya belirlenebilecek bir hale gelmediği durumlarda bu bilginin toplanması, işlenmesi veya saklanması işlemi kişisel verilerin korunması hukukunun kapsamında değerlendirilemeyecektir. Bu bağlamda anonim veriler veya sonradan anonimleştirilen veriler kişiyi belirli veya belirlenebilir kılmadığından kişisel veri olarak kabul edilemeyecektir.

C. Hassas Kişisel Veri

Kişisel verilerin korunmasına ilişkin ulusal ve uluslararası mevzuatta bazı veriler özel olarak koruma altına alınmıştır. “Hassas veri”, “özel nitelikli veri”, “özel koruma gerektiren veri”²¹ olarak adlandırılan bu veriler kişinin temel hak ve özgürlükleri ile mahremiyetine daha yakın türde verilerdir. Bu verilerin hukuka aykırı olarak toplanması, işlenmesi, ifşa edilmesi halinde kişinin ayrımcılığa maruz kalması veya zarar görmesi riski daha fazladır.

6698 sayılı Kişisel Verilerin Korunması Kanunu’nda hangi verilerin özel nitelikli kişisel veriler olduğu sınırlı olarak sayılmıştır. Kanun’un 6. maddesine göre, “kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik²² ve genetik verileri” özel nitelikli kişisel veridir. Hukukumuzda başta AB Veri Koruma Yönergesi ve GVKT olmak üzere Avrupa Birliği Hukuku düzenlemelerinden farklı olarak kılık, kıyafet, dernek ve vakıf üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler özel nitelikli veri kabul edilmektedir²³. AB Veri Koruma Yönergesinin

²⁰ Dülger, s. 10.

²¹ Hüseyin Can Aksoy, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Çakmak Yayınevi, Ankara, 2010, s. 30.

²² Biyometrik yöntemler, parmak izi tarama, yüz tanıma, el geometrisi tanıma, iris tanıma, imza tanıma, ses tanıma gibi ölçülebilir bireysel ve fiziksel özellikler aracılığıyla gerçekleştirilen ve otomatik olarak doğrulanabilen kimlik denetleme teknikleridir. Cüneyd Er, **Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı: Parmak İzi, Göz ve DNA Tarama Gibi Teknolojik Kimlik Denetleme Usullerinin Hukuki Statüsü**, Yetkin Yayınları, Ankara, 2007, s. 24; Akgül, s. 9.

²³ AB Veri Koruma Yönergesi m.8’de “ Üye Devletler, sağlık durumuna veya cinsel yaşama ilişkin verilerin işlenmesini ve sendika üyeliğini, dini veya felsefi inançları, siyasi görüşleri, ırk veya etnik kökeni açıklayan kişisel verilerin işlenmesini yasaklayacaktır.” ; GVKT m. 9’da “ ırk veya etnik kökeni, siyasi görüşleri, dini veya felsefi inançları veya sendika üyeliklerini ortaya çıkaran kişisel verilerin işlenmesi ile genetik verilerin ve biyometrik verilerin gerçek bir kişiyi sadece ona mahsus olarak bulabilmek amacıyla ve sağlık hakkındaki verilerin ya da bir gerçek kişinin cinsel hayatı veya cinsel tercihleri hakkındaki verilerin işlenmesi yasaktır.” hükümlerine yer verilerek bazı veriler özel

yürürlükte olduğu dönemde bazı verilerin özel düzenlemelerle korunması konusunda fikir birliği bulunsa da Avrupa Birliğine üye devletlerce hassas veri kapsamında koruma altına alınan veri kategorilerinde farklılıklar mevcuttur²⁴.

Kural olarak hassas verilerin işlenmesi yasaktır. Ancak ulusal ve uluslararası düzenlemelerde kesin işlem yasağına ilişkin bazı istisnai durumlar öngörülmüştür. 6698 sayılı Kişisel Verilerin Korunması Kanun’unda öngörülen istisnai hallere çalışmamızın üçüncü bölümünde değinileceğinden bu başlık altında sadece GVKT kapsamında yer alan istisnalara yer verilecektir.

GVKT ile AB Veri Koruma Yönergesi’ne benzer şekilde özel nitelikli kişisel verilerin işlenmesi yasağına getirilen istisnai durumlar şunlardır (m.9)²⁵:

- a) Birlik veya Üye Devlet hukuku çerçevesinde özel kategorideki kişisel verilerin işlenme yasağının veri sahibi tarafından kaldırılamayacağına ilişkin bir hüküm sağlanması haricinde, veri sahibinin belirtilen bir veya daha fazla sayıda amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık bir şekilde rıza göstermesi²⁶,

olarak koruma altına alınmıştır. Mehmet Bedii Kaya, Furkan Güven Taştan, **Kişisel Veri Koruma Hukuku Mevzuat & İhtihat**, Onikilevha Yayınları, İstanbul, 2018, s. 286; Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 344; GVKT m. 10’ da “ Madde 6 (1)’e dayalı olarak mahkumiyet kararları ile ceza gerektiren suçlara veya alakalı güvenlik önlemlerine ilişkin kişisel verilerin işlenmesi, sadece resmi yetkili kontrolü altında ya da veri sahibinin temel hak ve menfaatini korumak için uygun önlemler öngören Avrupa Birliği veya Üye Devlet kanunu kapsamında işleme faaliyetine izin verilirse gerçekleştirilebilir. Mahkumiyet kararları hakkındaki her türlü kapsamlı sicil kayıtları, resmi yetkililer tarafından tutulur.” denilerek her ne mahkumiyet kararları ile ceza gerektiren suçlara veya alakalı güvenlik önlemlerine ilişkin kişisel veriler özel veri kategorisinde sayılmasa da bu verilerin işlenmeleri özel olarak koruma altına alınmıştır.

²⁴ “genetik bilgilere (Polonya, İzlanda, Estonya ve Bulgaristan), biyometrik bilgilere (Slovenya, Slovakya, Çek Cumhuriyeti), ten rengine (İzlanda), milli kökenine (Çek Cumhuriyeti ve Slovenya), siyasi partilere veya hareketlere (Slovakya), dernek üyeliğine (İtalya), özür durumuna (Estonya), bağımlılıklara (Polonya), alkol, tıbbi ilaç ve uyuşturucu kullanımına (İzlanda), cinsel yaşama ve cinsel davranışlara (İzlanda), cinsel tercihlere ve cinsel yaşama (Finlandiya), sosyal görüşlere (Finlandiya), sağlık, hastalık veya handikap (özür) durumuna ve tedavi ve diğer benzer tedbirlere (Finlandiya), sosyal refah ihtiyaçlarına e alman yararlanmalarına, destek ve diğer sosyal refah yardımlarına (Finlandiya), fiziksel ve zihinsel sağlık ve duruma (İngiltere), işlenilen ya da işlendiği iddia edilen suçlara (İngiltere), işlenilen ya da işlendiği iddia edilen suçlar için yürütülen kovuşturmalara, bu kovuşturmaların sonlandırılmasına ve bu kovuşturmalar sonucunda bir mahkeme tarafından verilen mahkumiyetlere (İngiltere) ilişkin veriler de veri koruma kanunlarında hassas veri olarak kabul edilmiştir.” Cemil Kaya, **Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi**, İÜHFİM, C. 69, S1-2, Prof. Dr. İl Han Özay’a Armağan, 2011, 317-334, s. 319; Akgül, s. 22, Ayözger Öngen, s. 21.

²⁵ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 344; Aygözer Öngün, s. 25.

²⁶ AB Veri Koruma Yönergesi’ne benzer şekilde Üye Devletlerce, veri sahibinin açık rızasının bulunduğu hallerde dahi hassas verilerin işlenmesi yasaklanabilir.

- b) Birlik veya üye devlet hukuku çerçevesinde ya da üye devlet hukuku uyarınca yapılan ve veri sahibinin temel hakları ve menfaatlerine yönelik uygun güvencelerin sağlandığı bir toplu sözleşme çerçevesinde izin verildiği sürece veri sorumlusunun veya veri sahibinin iş, sosyal güvenlik ve sosyal koruma hukuku alanındaki yükümlülüklerini gerçekleştirilmesi ve spesifik haklarının kullanılması amacıyla işleme faaliyetinin gerekmesi,
- c) Veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde, veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olması²⁷,
- d) İşleme faaliyetinin, politik, felsefi, dini veya sendika amacıyla hareket eden bir vakıf, birlik veya kar amacı gütmeyen başka bir örgüt tarafından uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında işlemenin ve yalnızca örgütün üyeleri veya eski üyeleri ya da amaçlarıyla bağlantılı olarak kendisi ile düzenli olarak temas halinde bulunan kişilerle ilgili olması ve kişisel verilerin veri sahiplerinin rızası olmaksızın söz konusu örgüt dışında açıklanmaması koşuluyla gerçekleştirilmesi²⁸,
- e) İşleme faaliyetinin veri sahibi tarafından açık bir biçimde kamuya açıklanan kişisel verilerle ilgili olması,
- f) Yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ettiğinde işleme faaliyetinin gerekli olması,
- g) Gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler sağlayan Birlik veya Üye Devlet hukukuna dayalı olarak kayda değer ölçüde kamu yararı adına nedenlerden ötürü işleme faaliyetinin gerekmesi,

²⁷ Veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde, kendisinin veya başka bir gerçek kişinin hayati menfaatlerini korumak amacıyla açık rızasının varlığı kabul edilir olması hukukumuz bakımından da geçerli olacaktır. Ancak veri sahibinin böyle bir durumda bulunmasaydı dahi rıza göstereceği hallerde açık rızasının var olduğu kabul edilmelidir. Veri sahibinin rızasını verebileceği andan itibaren somut rızasının alınması gerekir. Aksi halde veri sahibinin açık rızası bulunmadığından yapılan işlem hukuka aykırı olacaktır. Hayrunnisa Özdemir, **Elektronik Haberleşme Sektöründe Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin Yayınları, Ankara, 2009, s. 128.

²⁸ Ölüme bağlı tasarruf ile kurulan vakıf ve dernekler kapsam dışındadır. Ayözger Öngün, s. 28.

- h) Birlik ya da Üye Devlet kanunları veya sağlık uzmanı ile yapılan sözleşme uyarınca ve gizlilik yükümlülüğüne tabi kişilerce önleyici veya tedavi amaçlı tıbbın, çalışanın çalışma kapasitesinin değerlendirilmesi, sağlık, sosyal hizmet veya tedavi sunmak ya da bu hizmetlerin yönetilmesi için gerekli olması,
- i) Özellikle mesleki gizlilik olmak üzere veri sahibinin hakları ve menfaatlerine ilişkin güvence sağlanmasına uygun ve spesifik tedbirler sağlayan Birlik veya Üye Devlet hukukuna dayalı olarak, sağlığa yönelik ciddi sınır ötesi tehditlere karşı koruma sağlanması veya sağlık hizmetleri ve tıbbi ürünler ya da tıbbi cihazlara ilişkin yüksek kalite ve emniyet standartları sağlanması gibi kamu sağlığı alanında kamu yararına yönelik olarak işleme faaliyetinin gerekmesi,
- j) Gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınmasına uygun ve spesifik güvenceler sağlayan Birlik veya Üye Devlet kanunlarına dayalı olarak, kamu yararına yönelik arşivleme, bilimsel veya tarihi araştırma amacı ya da istatistiki amaçlar doğrultusunda işleme faaliyetinin gerekmesi.

GVKT ile Üye Devletlerin kişisel veri koruma kanunları yürürlükten kalksa da Tüzüğün 9. maddesinde Üye Devletlerin genetik, biyometrik veya sağlık ile ilgili veriler ile alakalı sınırlamalar da dâhil olmak üzere ek koşullar uygulamaya devam edebileceği ya da ek koşullar getirebileceği öngörülmüştür²⁹.

II. KİŞİSEL VERİLERİN KORUNMASI

A. Kişisel Verilerin Korunması İhtiyacı

Endüstri 4.0 olarak adlandırılan sanayi devriminin dördüncü jenerasyonunu yaşadığımız ve hatta endüstri 5.0'a adım attığımız bu dönemde yapay zeka³⁰, nesnelerin interneti, öğrenen makine ve robotlar, yeni nesil yazılım sistemleri, büyük

²⁹ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 345; Aygözer Öngün, s. 33.

³⁰ “Doğal sistemlerin yapabildiği (zekice olsun veya olmasın) her bilişsel etkinliği (gerekirse bedenleri olan) yapay sistemlere, daha da yüksek başarımlı düzeylerinde nasıl yaptırabileceğimizi inceleyen bilim dalı” olarak tanımlanmaktadır. Cem Say, **50 Soruda Yapay Zeka**, 7 Renk Yayıncılık, İstanbul, 2019, s. 83.

veri³¹, akıllı sistemler hayatımızın her alanına etki etmektedir. Bilim ve teknolojiadaki hızlı ve sınırsız gelişim, pek çok faydasının yanında verilerimizin istismar edilme riskini de her geçen gün daha da arttırmaktadır. Gerek kamu kurumları gerekse özel kuruluşlar tarafından farklı sebeplerle saniyeden bile kısa sürede verilerimiz toplanmakta, depolanmakta ve sınır ötesi aktarılmaktadır. Verilerimizin yetkisiz kişiler tarafından elde edilmesi, kullanılması, ifşa edilmesi gibi hukuka aykırı eylemlere konu edilmesi temel hak ve özgürlüklerimizin ihlaline sebep olmaktadır. Günümüzde kişisel veriler, ekonomik anlamda bir değer olarak tartışılmaktadır. Makul bir dengenin kurulması ve olumsuzlukların önlenmesi ancak kişisel verilerin korunması bilincinin oluşması ve bu alanda etkin bir denetim mekanizmasını öngören yasal düzenlemelerin yapılması ile mümkündür. Kişisel verilerin korunması alanında Avrupa'daki düzenlemeler çok daha eski olsa da ülkemizde de son yıllarda bu alandaki çalışmalar hız kazanmıştır.

B. Kişisel Verilerin Korunması Hakkının Hukuki Niteliği

Kişisel verilerin korunması hakkının tek başına bir hak olup olmadığı tartışmasının dışında başka birçok hak ile ilişkili olması sebebiyle hakkın varlığının kaynağı konusunda farklı görüşler mevcuttur. Kişisel verilerin korunması ile neyin amaçlandığına verilen cevapların farklılığından kaynaklanan bu görüşler: kişilik hakkı görüşü, mülkiyet hakkı görüşü ve fikri mülkiyet hakkı görüşüdür³².

1. Mülkiyet Hakkı

Özellikle Amerikan hukukunda ileri sürülen bu görüşe göre: kişi, kişiliğinin ürünü olan verilerinin sahibidir ve mülkiyet hakkı kapsamında bu verileri üzerinde

³¹ “Geleneksel ya da klasik veri işleme yöntemleri ile değerlendirilemeyecek kadar çok hacimli, oldukça kompleks, hızlı değişebilen ve çok zayıf yapılandırılmış büyük miktardaki veri” olarak ifade edilmektedir. Metin Turan, **Bilişim Hukuku**, Seçkin Yayınları, Ankara, 2017, s. 211. Büyük veri, çevremizde sürekli üretilen sınırı ve kapsamı tam olarak belirlenemeyen kişisel veriler de dahil olmak üzere her türlü veriyi bünyesinde barındıran geniş bir kavramdır. Büyük veri uygulamaları kapsamında hızlı ve sınırsız veri işlem faaliyetleri sebebiyle kişisel verilerin korunmasının önemi her geçen gün artmaktadır. Şehriban İpek Aşıkoğlu, **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, Onikilevha Yayınları, İstanbul, 2018, s. 20.

³² Aksoy, s. 37; Taştan, s. 54.

tasarrufta bulunabilir³³. Mülkiyet hakkı, hak sahibine başka bir kimsenin yardımına gerek duymaksızın sahip olduğu şey üzerinde kullanma, yararlanma ve tasarrufta bulunma yetkisi verir³⁴. Bu yaklaşımda bilginin ekonomik değeri öne çıkarılmakta ve bilgi, serbest piyasa ekonomisinde alınıp satılabilen kiralanan bir ticari değer olarak kabul edilmektedir.

Bu görüşü savunan yazarlar, bilginin bir ticari değer olarak kullanılmasıyla; (i) ilgili kişinin verilerinin maliki kabul edileceğinden malike tanınan geniş yasal korumadan yararlanabileceğini, (ii) doğrudan dava açma ve zararın giderilmesini talep hakkının tanınmış olacağını, (iii) kişilerin verilerinin kullanılmasının karşılığını alabileceğini, (iv) şirketler bakımından verilerin toplanması ve kullanılması için bir maddi külfet oluşacağından özel hayatın daha güçlü bir şekilde korunacağını ileri sürmektedir³⁵. Karşı görüşteki yazarlara göre kişisel verilerin bu şekilde kullanımıyla; (i) kişilik hakkının ihlal edileceği, (ii) verilerin, devretme amacının dışında kullandığının tespiti çoğu zaman mümkün olmayacağı, (iii) mülkiyet hakkının devri ile mülkiyet hakkını kazanan teşebbüslerin artık bu veriler üzerinde dilediği gibi tasarruf imkânı kazanacağı, (iv) yapılacak pazarlıkta eşit koşulların sağlanamayacağı ve ilgili kişinin verileri üzerinde denetimi yeniden sağlamasına olanak bulunmadığı ileri sürülmektedir³⁶.

2. Fikri Mülkiyet Hakkı Görüşü

Mülkiyet hakkı görüşünü savunan yazarlara benzer şekilde fikri mülkiyet hakkı görüşünü savunan yazarlar da kişisel verilerin korunması ile bilgi ekonomisine katılımı sağlamayı amaçlamaktadır³⁷.

Fikri mülkiyet hakkı kapsamında eser sahibinin bir parçası, ürünü olarak kabul edilen eserin değiştirilmemesini ve doğruluğunun korunmasını isteme, eserin nasıl, ne şekilde ve ne isimle paylaşılacağını belirleme, “eseri umuma arz yetkisi” ve “eserde değişiklik yapılmasını yasaklama yetkisi” gibi birtakım manevi hakları

³³ Taştan, s. 55 dn.161’deki yazarlar; Küzeci, s. 60 dn 184’deki tartışmaya ilişkin açıklamalar.

³⁴ Mehmet Ayan, **Eşya Hukuku I Zilyetlik ve Tapu Sicili**, Seçkin, Ankara, Ekim 2016, s. 35.

³⁵ Küzeci, s. 61; Taştan, s. 55.

³⁶ Aksoy, s. 58; Küzeci, s. 61.

³⁷ Taştan, s. 55 dn 175’deki yazarlar; Elif Mendos Kuşkonmaz, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması** (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul, 2013, s. 22 dn 62’deki yazarlar.

bulunmaktadır³⁸. Bu görüşü savunan yazarlara göre veri sahibinin de verileri üzerinde fikri mülkiyet hukukundaki manevi haklara benzer hakları bulunmaktadır. Veri sahibi, verilerinin değiştirilmemesini, doğruluğunun korunmasını, verilerinin nasıl, ne şekilde ve kimlerle paylaşılacağını belirleme ve hatta verilerinin unutulmasını isteme hakkına sahiptir³⁹. Bu görüşü eleştirenlere göre fikri mülkiyet kapsamındaki eser kişinin bilinçli çabasının bir sonucu olarak ortaya çıkmakta iken kişisel veri kişinin varoluşunun bir sonucudur⁴⁰. Fikri mülkiyet hakkının amaçlarından birisi fikri ve sınaî mülkiyetin korunarak teşviki ile eserin ticari getirilerinin korunması amaçlanmaktadır⁴¹. Ancak kişisel verilerin korunması hakkı ile kişisel verilerin işlenmesinin teşviki ve ticari getiri sağlaması amaçlanmamaktadır.

3. Kişilik Hakkı Görüşü

Kişisel verilerin hukuki niteliğini mülkiyet hakkı ve fikri mülkiyet hakkına dayandıran ekonomik hak görüşünün dışında özellikle Kıta Avrupası hukukunda hâkim olan bir diğer görüş ise kişisel verilerin korunması hakkının kişilik hakkı olduğudur⁴². Kişilik hakkı, kişinin doğuştan sahip olduğu haklarının korunmasını ve herkes tarafından tanınmasını isteme hakkıdır⁴³. Literatürde yapılan hiçbir tanım kişilik hakkının sınırlarını somut olarak belirlemeye yetmemektedir. Somut olay içerisinde görünce tanıdığımız ancak tanımını ve sınırlarını tam ve kesin olarak belirleyemediğimi bu hakkın; soyut ve kültüre, dünya görüşüne, zamana göre şekillenebilen bir hak olduğunu söylemek mümkündür⁴⁴.

³⁸ Ünal Tekinalp, **Fikri Mülkiyet Hukuku**, Vedat Yayıncılık, İstanbul, 2012, s. 160; Aksoy, s. 60; Dülger, s. 45; Kuşkonmaz, s. 22.

³⁹ Kuşkonmaz, s. 23.

⁴⁰ Taştan, s. 58 dn 178'deki yazarlar.

⁴¹ Taştan, s. 58; Aksoy, s. 67.

⁴² Küzeci, s. 65; Dülger, s. 45; Aksoy, s. 47; Aygözer Öngün, s. 15.

⁴³ Bilge Öztan, **Medeni Hukuk'un Temel Kavramları**, Turhan Kitapevi Yayınları, Ankara, 2010, s. 274; Jale G. Akıntürk, Turgut Akıntürk ve Derya Ateş Karaman, **Türk Medeni Hukuku Birinci Cilt Başlangıç Hükümleri Kişiler Hukuku**, Beta Yayınları, İstanbul, 2012, s. 343; Kemal Oğuzman/Nami Barlas, **Medeni Hukuk Giriş, Kaynaklar, Temel Kavramlar**, Vedat Yayıncılık, İstanbul, 2008, s. 50; Kemal Oğuzman, Özer Seliçi, Saibe Oktay-Özdemir, **Kişiler Hukuku (Gerçek ve Tüzel Kişiler)**, Filiz Kitabevi, İstanbul, 2010, s. 1; Şaban Kayıhan, Mustafa Ünlütepe, **Medeni Hukuk Bilgisi**, Seçkin Yayıncılık, Ankara, 2017, s. 189; Zafer Zeytin, Ömer Ergün, **Türk Medeni Hukuku**, Seçkin Yayıncılık, Ankara, 2018, s. 42.

⁴⁴ Akıntürk, Akıntürk ve Karaman, s. 343; Öztan, s. 274.

Bu yaklaşıma göre kişisel verilerin korunması hakkı; insan onuru, kişiliğin serbestçe geliştirilmesi hakkı, özel yaşamın gizliliği hakkı, düşünce özgürlüğü, bilim özgürlüğü, bilgi edinme hakkı, haberleşmenin gizliliği gibi diğer pek çok temel hak ve özgürlükler ile iç içe geçmiş durumdadır⁴⁵. Bu bağlamda kişinin bedeni ve maddi bütünlüğünden, menfaatlerinden, ilişkilerinden kaynaklanan pek çok verisi kişisel veri olarak kabul edilecektir.

Kişisel veriler ilk olarak özel yaşamın gizliliği hakkı kapsamında korunmaya başlanmıştır. Birleşmiş Milletler Evrensel İnsan Hakları Beyannamesi, Birleşmiş Milletler Bireysel ve Siyasal Haklar Şartı, Avrupa İnsan Hakları Sözleşmesi gibi insan haklarını konu alan pek çok uluslararası düzenlemede özel yaşamın gizliliği hakkına yer verilmektedir.

Kişisel verilerin korunması hakkının özel yaşamın gizliliği hakkından bağımsız bir hak olarak tartışılmaya başlanmasında 1983 yılında Federal Almanya Anayasa Mahkemesi'nin "Nüfus Sayım Kararı"nın etkisi büyüktür⁴⁶. Mahkeme, 1983 yılında yapılması planlanan nüfus sayımına ilişkin yasayla yurttaşların adları, adresleri, medeni durumları gibi nüfus sayımıyla ilgili sayılabilecek bilgilerinin yanında gelir kaynakları, çalışma saatleri, eğitim durumları gibi bilgilerinin de toplanmasının mümkün kılınmasını bireyin "insan onuru ve bireysel özerklik temelinde kişisel verilerin geleceğini belirleme hakkı" ile bağdaşmayacağını kabul etmiştir⁴⁷. Kararda kişisel verilerin korunması hakkının, özellikle özel hayatın gizliliği hakkı başta olmak üzere kişilik hakkından tamamen ayrı olmasa da kişilik hakkının özel görünüm şekli olduğuna işaret edilmiştir.

Özel yaşamın sınırlarının çizilememesi özel yaşamı tanımlamayı da zorlaştırmaktadır. Özel yaşamın kapsamı hakkında ileri sürülen görüşleri SÖZÜER, "yalnız bırakılma hakkı, kişiye sınırlı ulaşım, yakınlık ve kişisel bilgileri kontrol hakkı" olarak dört başlık altında toplamıştır⁴⁸. Benzer şekilde ARASLI iç içe geçmiş üç çember oluşturarak "genel yaşam alanı" olarak adlandırdığı dış çemberde kişinin herkesle paylaşabildiği bilgilerine, "kişinin özel yaşam alanı" olarak adlandırdığı

⁴⁵ Küzeci, s. 66.

⁴⁶ Küzeci, s. 66; Dülger, s. 49; Taştan, s. 67.

⁴⁷ Elif Küzeci, **İstatiki Birimler ve Bilgilerin Geleceğini Belirleme Hakkı**, İnsan Hakları Yıllığı, C. 32, 2014, 53-75, s. 56; Taştan, s. 59.

⁴⁸ Eren Sözüer, **Unutulma Hakkı İnsan Hakları Hukuku Perspektifinden Bir İnceleme**, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Ekim 2017, s. 51.

daha dar ikinci çemberde kişinin belirli kimselerle ve belirli ölçüde paylaştığı bilgilerine, “sır alanı” olarak adlandırdığı en küçük üçüncü çemberde ise kişinin kimseyle paylaşmak istemediği özel yaşam içerisinde değerlendirdiği bilgilerine yer vererek konuya açıklık getirmiştir⁴⁹.

Kişisel verilerin korunması hakkı özünü özel yaşamın gizliliği hakkına dair ilkeler oluştursa birbirinden farklı kavramlardır. Kişisel veri, belirli veya belirlenebilir bir kişiye ait tüm bilgilerdir. Daha önce açıkladığımız üzere bir bilginin kişisel veri olarak kabul edilebilmesi için doğru veya kişiyi doğrudan tanımlanabilir kılması ya da kişinin sır alanında kalan bir bilgi olması gerekli değildir. Özel yaşamın gizliliği hakkı ile kişinin özel alanı, sır alanı içerisinde kalan bilgilerin korunması amaçlanmaktadır. Kişisel veri olarak kabul ettiğimiz tüm bilgilerin özel yaşamın gizliliği hakkı kapsamında korunması gerektiği kabul edildiğinde kişinin kendi isteğiyle ya da isteği dışında açıklanan bilgileri gizliliğini yitireceğinden koruma altına alınamayacaktır⁵⁰.

Küreselleşme ve teknolojiadaki hızlı gelişim ile kişisel veriler ekonomik bir değer kazanarak veriler sınırsız bir şekilde toplanan, özellikle ekonomik kazanç elde etmek için kullanılan ve devredilen ticari değer haline gelmiştir. Bilgileri sınırsız bir şekilde toplanılmaya, kullanılmaya ve devredilmeye başlayan birey için özel yaşamın gizliliği hakkı kapsamında getirilen korumalar yetersiz kalmaya başlamıştır. Bu nedenle her ne kadar temelde ortak birçok değeri koruma altına almış olsalar da kişisel verilerin korunması hakkının bağımsız bir hak olarak kabul edilmesi gerekmektedir.

III.KİŞİSEL VERİLERİNİŞLENMESİNE İLİŞKİN İLKELER

Kişisel verilerin korunması hukukuna dair tüm düzenlemelerde veri işlem faaliyetlerinin tüm aşamalarında uyulması gereken temel ilkelere yer verilmiştir. Her ilke birbiriyle ilişkili ve birbirini tamamlar niteliktedir.

AB Veri Koruma Yönergesi ile 108 No’lu Sözleşme’de benzer şekilde yer verilen temel ilkelere göre kişisel veriler: (i) hukuka ve dürüstlük kurallarına uygun

⁴⁹ Oya Araslı, **Özel Yaşamın Gizliliği Hakkı ve T.C Anayasasında Düzenlenişi**(Yayınlanmamış Doçentlik Tezi), Ankara, 1979, s. 4 (Küzeci, s.69 Naklen).

⁵⁰ Aksoy, s. 63; Taştan, s. 65; Aygözer Öngün, s. 16.

işlenmeli, (ii) belirli, açık ve meşru amaçlar için kaydedilmeli ve bu amaçlara uygun şekilde kullanılmalı, (iii) kaydedilme amaçlarına uygun ve yeterli işlenmeli, (iv) doğru ve gerektiğinde güncel olmalı, (v) kaydedilme amaçlar için makul olan süre boyunca tutulmalıdır⁵¹. Hukukumuzda da anılan uluslararası düzenlemeler dikkate alınarak 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde şu ilkelere yer verilmiştir:

“ (1) Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir

(2) Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.”

GVKT ile bu konuda daha yeni ve kapsamlı ilkeler öngörülmüştür. Tüzük'ün 5. maddesinde yer alan bu ilkeler: (i) hukuka uygunluk, adalet ve şeffaflık, (ii) amaca uygunluk, (iii) doğruluk, (iv) saklama süresinin kısıtlanması, (v) bütünlük ve gizlilik, (vi) hesap verilebilirliktir⁵². Bu başlık altında yapacağımız açıklamalarda özellikle GVKT ve 6698 sayılı Kişisel Verilerin Korunması Kanunu esas alınacaktır.

A. Verilerin Hukuka ve Dürüstlük Kuralına Uygun İşlenmesi İlkesi

Kişisel verilerin korunması hukukunun temel ilkelerinin kaynağı sayılabilecek ilk ilke kişisel verilerin hukuka ve dürüstlük kuralına uygun olarak işlenmesi ilkesidir⁵³.

Verilerin hukuka uygun işlenmesi, verilerin özel olarak hukuk normlarına uygun olarak işlenmesini değil aynı zamanda evrensel hukuk ilkelerine de uygun

⁵¹ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 294.

⁵² Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 341.

⁵³ İbrahim Korkmaz, **Kişisel Verilerin Korunması Kanunu Hakkında Değerlendirme**, Türkiye Barolar Birliği Dergisi, D.2016, S.124, 81-152, s. 100; Taştan, s. 48; Sır saklama yükümlülüğünün, telif hakkının ihlal edilmemesi gibi diğer kanunlardan doğan yükümlülüklerle uygun şekilde verilerin işlenmesi gerekecektir. Taştan, s. 49.

olarak işlenmesi gerekliliğini ifade etmektedir. Kişisel verilerin toplanmasından itibaren veriler üzerindeki kaydetme, saklama, kullanma, engelleme, silme, yok etme gibi her türlü uygulamada evrensel hukuk ilkelerine ve hukuk normlarına uygun davranılması gerekmektedir⁵⁴.

Hukukumuz bakımında dürüstlük kuralına uygun olma Türk Medeni Kanunu'nun 2. maddesi ile düzenlenen dürüstlük kuralına riayet edilmesidir. Maddeye göre "Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır. Bir hakkın açıkça kötüye kullanılmasını hukuk düzeni korumaz.". Dürüstlük kuralının sınırları ve içeriğinin sayılması mümkün olmadığından somut olayın özelliklerine göre orta zekâlı, normal, makul bir kimseden beklenen davranışa göre değerlendirme yapılmalıdır⁵⁵.

Kişisel verilerin korunması hukuku açısından dürüstlük kuralı; ilgili kişinin çıkarlarını ve makul beklentilerini koruyarak kişinin öngöremeyeceği şekilde hareket etmemek, veri işleme faaliyetinin açıklığını, belirliliğini ve şeffaflığını sağlamak, kanun ve yasal düzenlemelere dayanan meşru bir amaç için en az miktarda işlenen verileri toplanma amacını aşacak şekilde ve toplanma amacı dışında kullanmamak, amacın sona ermesi durumunda verileri silmek, yok etmek, anonim hale getirmek gibi davranışlarda bulunmayı gerektirir⁵⁶.

Kişisel verilerin korunması hukukuna dair sayacağımız diğer ilkeler verilerin hukuka ve dürüstlük kuralına uygun işlenmesi ilkesinin somutlaşmış halidir. Dolayısıyla diğer ilkelere uygun davranılması halinde veriler hukuka ve dürüstlük kuralına uygun işlenmemiş olacaktır.

Genel Veri Koruma Tüzüğü kişisel verilerin hukuka ve dürüstlük kuralına uygun işlenmesinin yanında adil ve şeffaf işleme ilkesine de yer vermiştir⁵⁷. Şeffaflık ilkesi gereğince ilgili kişinin; veri sorumlusunun kimliği, veri işleme süreci, faaliyetleri ve amaçları, haklarını nasıl kullanacağı hakkında bilgilendirilmesi

⁵⁴ Özdemir, s. 137.

⁵⁵ Öztan, s. 173.

⁵⁶ Dülger, 111; Küzeci, s. 201; Akgül, s. 126; Başalp, s. 37; Özdemir, s. 138.

⁵⁷ "Kişisel veriler: (a) hukuka ve hakkaniyete uygun olarak ve ilgili kişiyle bağlantılı olarak şeffaf bir şekilde işlenmelidir ('hukuka uygunluk, hakkaniyet ve şeffaflık')". Hüseyin Murat Develioğlu, **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, Onikilevha Yayınları, İstanbul, 2017, s. 180.

gerekmektedir⁵⁸. Veri üzerinde yapılan işlemin hukuka ve dürüstlük kuralına uygun olup olmadığının değerlendirilmesi işlemin şeffaflığı ile kolaylaşmış olacaktır⁵⁹.

B. Belirli, Açık ve Meşru Amaç İçin Toplama İlkesi

Kişisel verilerin belirli, açık ve meşru amaçlar için işlenmesi ilkesi veri sorumlusunun veri işleme amacını açık ve kesin olarak belirleyerek ortaya koyması ve amacın meşru olması zorunluluğunu ifade etmektedir (Kişisel Verilerin Korunması Kanunu Madde Gerekçeleri). Bu bağlamda kişisel veriler “bir gün lazım olur” düşüncesiyle işlenemez⁶⁰.

İlkenin ilk kriteri belirli ve açık bir amacın olmasıdır. Kişisel veriler ancak veri sorumlusu tarafından belirtilen açık, belirli ve meşru amaçlar doğrultusunda işlenebilecektir. Amanın gerçekleşmesi için veriler üzerinde daha fazla işlem yapılmasının gerektiği durumlarda öncelikle belirlenen ilk amaç ile uyumlu olup olmadığı değerlendirilmelidir⁶¹. Belirlenen amaç, ilgili kişi tarafından anlaşılır açıklıkta olmalıdır. Benzer şekilde veri sorumlusunun amacının değişmesi halinde, ilgili kişinin belirlenen yeni amaca rıza göstermesinin makul olmadığı durumlarda veri sorumlusu tarafından yeniden rıza alınması gerekmektedir⁶².

Amanın meşru olması ise; verilerin amacının yasal bir dayanağının bulunması, veri sorumlusu tarafından toplanan verilerin, veri sorumlusunun yapmış olduğu iş veya sunmuş olduğu hizmet ile bağlantılı ve bu amaç için gerekli olmasıdır (Kişisel Verilerin Korunması Kanunu Madde Gerekçeleri).

⁵⁸ Dülger, s. 115; Küzeci, s. 202.

⁵⁹ Dülger, s. 82; Özdemir, s. 137.

⁶⁰ Küzeci, s. 203.

⁶¹ Dülger, s. 118; Küzeci, s. 41. Benzer şekilde GVKT 5. maddesi uyarınca kişisel veriler “kamu yararı için arşivleme amacıyla, bilimsel veya tarihi araştırma amacıyla veya istatistiksel amaçlarıyla işlenecekleri zaman, ilgili kişilerin hak ve özgürlüklerini koruma üzere bu Tüzük tarafından aranan uygun teknik ve organizasyonel tedbirlerin alınmasına bağlı olarak daha uzun süre depolanabilir (‘sınırlı süre saklama’).” Develioğlu, s. 181.

⁶² Taştan, s. 51.

C. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması İlkesi

Kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ilkesi; belirlenen amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenilmesinden kaçınılması gerekliliğini ifade etmektedir⁶³.

Veri sorumlusu, işleme amacına ulaşmak için asgari, zorunlu miktarda veriyi toplamalı ve işlemeli, aşırıya kaçmamalıdır. “Veri ekonomisi” veya “verilerin asgari seviyeye indirilmesi ilkesi” olarak da adlandırılan bu yöntem ile ilgili kişinin en az miktarda verisi risk altında olacaktır⁶⁴. Bunun için veri sorumlusu öncelikle hangi amaç için verileri topladığını ve işlediğini belirlemeli ardından bu amacı gerçekleştirmek için gerçekten hangi kişisel verilere ihtiyacı olduğu sorusuna cevap vermelidir⁶⁵.

Belirli, açık ve meşru amaç doğrultusunda toplanan kişisel veriler bu amaçla sınırlı olarak işleme tabi tutulmalıdırlar. Sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik veri işlenebilmesi halinde, işlemeye ilk kez başlıyor gibi kişisel verilerin işleme şartlarından birinin gerçekleşip gerçekleşmediği değerlendirilmelidir⁶⁶.

D. Doğru ve Gerekliğinde Güncel Olarak Tutulma İlkesi

Kişisel verilerin doğru ve gerektiğinde güncel tutulması ilkesi, veri üzerindeki faaliyetlerin doğru ve gerektiğinde güncel olan veriler ile gerçekleştirilmesidir. Doğru olmayan yanlış verilerin işlenmesi ilgili kişinin temel hakları zedelenerek zarara uğramasına yol açacaktır.

⁶³ İşlenen verilerin işleme amacı ile bağlantılı olması gerekmektedir. Örneğin bir hazır giyim mağazasının, müşterilerinin kimlik ve iletişim bilgilerini işlemesi, işleme amacı ile bağlantılı iken; müşterilerin kan gruplarını işlemesi verilerin işleme amacına uygun kabul edilemeyecektir. Kişisel Verilerin Korunması Kanunu Madde Gerekçeleri, s.8; Korkmaz, s. 103 (Değerlendirme); Özdemir, s. 141.

⁶⁴ Akgül, s. 133; Küzeci, s. 208; Şimşek, s. 85.

⁶⁵ Avrupa İnsan Hakları Mahkemesi, Z./Finlandiya kararında başvurucunun tıbbi kayıtlarının detaylarını içeren mahkeme kararının 10 yıl sonra kamuya açık hale gelmesiyle başvurucunun kişilik haklarının ihlal edildiği, mahkeme kararının kamuya açıklanmasında haklı bir gerekçe bulunmadığı ve bu durumun orantılılık ilkesine aykırı olduğu gerekçesiyle Sözleşme’nin 8. maddesine aykırılık kararı vermiştir. Özdemir, s. 143; Kilkelly, s. 69; Türkiye Cumhuriyeti Adalet Bakanlığı İnsan Hakları Dairesi Başkanlığı, AIHM Kararları Tematik Bilgi Notları, s. 20.

⁶⁶ Dülger, s. 126; Özdemir, s. 142.

Bu ilke ile esasen hem ilgili kişiye hem de veri sorumlusu açısından birtakım yükümlülükler getirmektedir. İlgili kişi açısından verilerini doğru bir şekilde vermesi beklenmektedir. Aynı zamanda veri sorumlusunun sürekli verilerin güncelliğini araştırması hakkaniyete uygun düşmeyeceğinden verilerindeki değişikliği veri sorumlusuna iletmeli verilerinin güncelliğini korumalıdır⁶⁷. Veri sorumlusu ise doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin silinmesini veya düzeltilmesinin sağlanmak, ilgili makul tüm adımları atmakla yükümlüdür⁶⁸.

E. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme İlkesi

Kişisel verilerin ilgili mevzuatta bir süre öngörülmüş ise bu süre kadar; ilgili mevzuatta bir süre öngörülmemiş ise işlenme amaçları için gerekli olan makul süre kadar muhafaza edilmeleri gerekmektedir⁶⁹. İşlenen verilerin ileride kullanılma ihtimali olsa da işlenme amacı için makul olan süreden daha uzun saklanması yasaktır. Bu nedenle veri sorumlusu, işlemenin her aşamasını ve amacını belirleyerek verilerin saklanması için makul olan süreyi belirlemelidir.

Kişisel verilerin işlenme amacına ulaşılması, işlenme amacının ortadan kalkması ya da veri sorumlusunun amaca ulaşmak için muhafaza ettiği verilerin gerekli olmadığının veya fazla olduğunun farkına varması durumunda artık veri sorumlusunun verileri ortadan kaldırması ya da anonimleştirmesi gerekmektedir⁷⁰.

Kural olarak veri sorumluları öncelikle Kanun ile öngörülen süreleri dikkate almakla yükümlüdür. Bunun dışında Kişisel Verileri Koruma Kurulu'nun sektörlere

⁶⁷ Küzeci, s. 214; Örneğin; bir aboneliğe ilişkin internet üzerinde doldurulan formlar ile daha önce işlenen verilerin güncellenmesi veya e-posta ile güncel bilgilerin veri sorumlusuna aktarılması. Taştan, s. 50; Şimşek, s. 84; Akgül, s. 132; Başalp, s. 39; Özdemir, s. 144.

⁶⁸ 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 11. maddesinde ilgili kişinin "kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme" hakkı düzenlenmiştir. Benzer şekilde GVKT 5. maddesinde "Kişisel veriler: (d) doğru ve gereken hallerde, güncel şekilde bulundurulmalı; işlendikleri amaçlar göz önünde bulundurularak, yanlış olan kişisel verilerin gecikmeden silinmesini veya düzeltilmesini sağlamak için tüm makul adımlar atılmalıdır ('doğruluk')" doğru ve gerektiğinde güncel tutulma ilkesine yer verilmiştir. Dülger, verilerin doğruluğunun ve güncelliğinin sağlanabilmesi için belirli periyotlarla ve araçlarla verilerin doğruluğunu ve güncelliğini denetleyen bir yöntem oluşturulması gerektiğine değinmiştir. Bizce de verilerin doğruluğunun ve güncelliğinin denetlenebileceği bir yöntemin oluşturulması veri ihalelerinin önlenmesi bakımından yerinde bir tedbir olacaktır. Dülger, s. 134.

⁶⁹ Şimşek, s. 84; Akgül, s. 131; Özdemir, s. 138.

⁷⁰ Küzeci, s. 215; Taştan, s. 52.

göre kişisel verilerin işlenme sürelerine ilişkin ilke kararı almaları da mümkündür⁷¹. Kanun ile veya ilke kararları ile sürenin öngörülmediği durumlarda veri sorumluları ancak kişisel verilerin işlenme amaçları için gerekli olan süre boyunca kişisel verileri muhafaza edebilecektir. 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 16. maddesinde veri sorumlularının, veri sorumluları siciline kayıt başvurusunda kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi bildirmeleri gerekmektedir.

Avrupa İnsan Hakları Mahkemesi kararlarında da verilerin belirsiz süre muhafaza edilmesi Sözleşme’nin 8. maddesine aykırılık olarak kabul edilmiştir. M.M/Birleşik Krallık kararında başvuranın, oğlunun boşanmasının ardından Avustralya’ya gitmesini engellemek amacıyla bebek olan erkek torununu alarak bir gün ortadan kaybolması sonrasında verilen uyarı cezasının ilk başta başvuranın sicilinde beş yıl durması planlanmış iken; değişen politika gereği ömür boyu saklanmasına karar verilmesinin Avrupa İnsan Hakları Sözleşmesi’nin 8. maddesine aykırı olduğuna karar vermiştir⁷². Yine S. ve Marper/Birleşik Krallık kararında başvuranlardan alınan parmak izlerinin, hücre örneklerinin ve DNA profillerinin haklarında beraat ve düşme kararı verilmesine rağmen belirsiz bir süre boyunca saklanmasını Sözleşme’nin 8. maddesinin ihlali olarak değerlendirmiştir⁷³.

F. Veri Güvenliği İlkesi

Kişisel verilerin korunması hukuku açısından verilerin güvenliği ilkesi son derece önemlidir. Veri güvenliği ilkesi, kişisel verilerin korunması amacıyla gerekli olan tüm tedbirlerin alınmasını ifade eder⁷⁴.

6698 sayılı Kişisel Verilerin Korunması Kanun’un “veri güvenliğine ilişkin yükümlülükler” başlıklı 12. maddesine göre veri sorumlusu varsa veri işleyen, kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli

⁷¹ Taştan, s. 52.

⁷² Küzeci, s. 216; Türkiye Cumhuriyeti Adalet Bakanlığı İnsan Hakları Dairesi Başkanlığı, AİHM Kararları Tematik Bilgi Notları, s. 16.

⁷³ Küzeci, s. 216; Türkiye Cumhuriyeti Adalet Bakanlığı İnsan Hakları Dairesi Başkanlığı, AİHM Kararları Tematik Bilgi Notları, s. 13; Sedat Erdem Aydın, **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, İstanbul Ceza Hukuku ve Kriminoloji Arşivi, Onikilevha Yayınları, İstanbul, 2015, s. 38.

⁷⁴ Taştan, s. 74; Şimşek, s. 95; Akgül, s. 134.

teknik ve idari tedbirleri almak zorundadır. Kanun veri sorumluları ile veri işleyenin, öğrendikleri kişisel verileri, Kanun hükümlerine aykırı olarak başkasına açıklamasını ve işleme amacı dışında kullanmasını da veri güvenliği kapsamında değerlendirmiştir. Bu sorumlulukları görevden ayrılmalarından sonra da devam eder. Ayrıca veri sorumlusu, kendi kurum veya kuruluşunda, 6698 sayılı Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirmeli ve Kurul gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan etmelidir.

KVKK Kurulu'nun 31 Ocak 2018 tarihli 2018/10 sayılı Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler ile ilgili ilke kararında özel nitelikli kişisel verilerin işlenmesinde veri sorumluları tarafından alınması gereken önlemler belirlenmiştir. Buna göre⁷⁵:

“1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,

2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,

a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,

b) Gizlilik sözleşmelerinin yapılması,

c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,

ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,

d) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,

3- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise

a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

⁷⁵ www.kvkk.gov.tr.

- b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
- c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
- ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,

4- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise

- a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,
- b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,

5- Özel nitelikli kişisel veriler aktarılacaksa

- a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,
- b) Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,
- c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımının gerçekleştirilmesi,
- ç) Verilerin kağıt 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.

6- Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır.”

Kişisel verilerin korunması hukukuna ilişkin metinlerin tamamında veri güvenliğine dair düzenlemelere yer verilmiştir⁷⁶. GVKT ile veri sorumlusu veya veri işleyen tarafından, tekniğin durumu, uygulama maliyetleri ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılık ve önemde riskleri dikkate alarak, risk açısından uygun bir güvenlik seviyesi sağlamak üzere teknik ve idari tedbirlerin alınması gerekmektedir (GVKT m.32)⁷⁷. GVTK m. 32’ye göre uygulanabilecek bazı güvenlik tedbirleri şunlardır: (i) takma ad kullanımı ve kişisel verilerin şifrelenmesi, (ii) veri işleme sistem ve hizmetlerinin sürekli gizliliğini, bütünlüğünü, kullanılabilirliğini ve esnekliğini sağlanması, (iii) fiziksel veya teknik bir olayın olduğu durumlarda kişisel verilerin kullanılabilirliğini ve kişisel verilere erişimi vakitlice geri kazanabilme kapasitesinin sağlanması, (iv) işleme faaliyetinin güvenliliğini sağlamak için öngörülen teknik ve düzenlemeye ilişkin önlemlerin etkinliğini düzenli olarak test etmek, ölçmek ve değerlendirmek⁷⁸. Ayrıca uygun güvenlik seviyesi değerlendirilirken, iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı olarak imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişim başta olmak üzere özellikle işleme faaliyetinin yol açtığı riskler göz önünde bulundurulması gerektiğine işaret edilmiştir (GVKT m.32/2)⁷⁹.

Sonuç olarak kişisel verilerin korunmasının sağlanabilmesi için öncelikle veri güvenliğine ilişkin bilincin oluşturularak bu anlamda gerekli tüm önlemlerin alınması gerekmektedir.

⁷⁶ İlgili düzenlemeler için bkz. Küzeci, s. 254.

⁷⁷ Develioğlu, s. 213.

⁷⁸ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 360.

⁷⁹ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 360.

G. Kişisel Verilerin İşlenmesi Sırasında İlgili Kişinin Bilgilendirilmesi İlkesi

İlgili kişinin haklarını etkin şekilde kullanabilmesi için verilerinin işlenmesi hakkında bilgilendirilmesi gerekmektedir.

İlgili kişinin bilgilendirilmesi ilkesi Kişisel Verilerin Korunması Kanunu’nun 10. maddesinde AB Veri Koruma Yönergesi ‘ne uygun olarak veri sorumlusunun ilgili kişiyi aydınlatma yükümlülüğü kapsamında düzenlenmiştir. Maddeye göre kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi, Kanun’un 11. maddesinde sayılan diğer hakları konusunda bilgi vermekle yükümlüdür (KVKK m.10).

İdarenin en temel ilkelerinden biri olan idarenin şeffaflığı ilkesinin bir gereği olarak ilgili kişiye bilgi verilmesi bireyin haklarını etkin şekilde kullanabilmesini sağlanacaktır⁸⁰.

10 Mart 2018 tarihli 30356 sayılı Resmi Gazetede “Kişisel Verilerin Koruma Kurulu tarafından Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ” yayımlanmış ve aynı gün yürürlüğe girmiştir. Tebliğin 4. maddesinde Kanunun 10. maddesi gereği veri sorumlusu veya yetkilendirdiği kişiler tarafından ilgili kişiye bilgi verilmesinin zorunlu olduğu, yapılacak bilgilendirmenin ise asgari olarak yine Kanunun 10. maddesinde belirtilen konuları içermesi gerektiği düzenlenmiştir.

Tebliğin 5. maddesinde veri sorumlusu ya da yetkilendirdiği kişi tarafından sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle aydınlatma yükümlülüğünün yerine getirilmesi esnasında uyulacak usul ve esaslar ayrıntılı olarak belirtilmiştir. Sayılan usul ve esaslara göre:

- a) İlgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir.

⁸⁰ Küzeci, s. 217.

- b) Kişisel veri işleme amacı değiştiğinde, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmelidir.
- c) Veri sorumlusunun farklı birimlerinde kişisel veriler farklı amaçlarla işleniyorsa aydınlatma yükümlülüğü her bir birim nezdinde ayrıca yerine getirilmelidir.
- d) Sicile kayıt yükümlülüğünün bulunması durumunda, aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilecek bilgiler Sicile açıklanan bilgilerle uyumlu olmalıdır.
- e) Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir. Ayrıca aydınlatma yükümlülüğünü yerine getirdiğini veri sorumlusu ispat edecektir.
- f) Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir. Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadelerle yer verilmeden anlaşılır, açık ve sade bir dil kullanılmalıdır. Gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadelerden kaçınılmalıdır. Bildirimde eksik, ilgili kişileri yanıltabilecek ve yanlış olan bilgilere yer verilmemelidir. Ayrıca kişisel verilerin, tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerden hangisiyle elde edildiği açık bir şekilde belirtilmelidir.
- g) Aydınlatma yükümlülüğü kapsamında, kişisel verilerin aktarılma amacı ve aktarılacak alıcı grupları belirtilmelidir.

Kişisel verilerin ilgili kişiden elde edilmemesi halinde de aydınlatma yükümlülüğünün yerine getirilmesi gerekir. Tebliğin 6. maddesinde kişisel verilerin ilgili kişiden elde edilmemesi halinde veri sorumlusu veya yetkilendirdiği kişi tarafından; “a) kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde, b) kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında, c) kişisel verilerin aktarılacak olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada, ilgili kişiyi aydınlatma yükümlülüğünün yerine getirilmesi gerekir.”

GVKT 14. maddesinde şeffaflık temel bir ilke olarak öngörülmüştür.⁸¹ Bir çocuğa yönelik her türlü bilgi başta olmak üzere işleme faaliyetine ilişkin her türlü bildirimin öz, şeffaf, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanarak veri sahibine bildirilmesi gerekmektedir (m.12). Bilgilendirme yazılı olarak veya uygun olduğu hallerde elektronik yollar da dâhil olmak üzere diğer yollarla sağlanacaktır. Bilgilendirmenin ilgili kişi tarafından talep edilmesi durumunda ilgili kişinin kimliğinin diğer yollarla doğrulanması koşuluyla, bilgilendirme sözlü olarak yapılabilecektir. Ayrıca veri sorumlusunun kimliğinin yanında veri koruma görevlisinin de kimliğine yer verilmesi gibi düzenlemelerle bilgilendirme kapsamının genişletilerek ilgili kişinin haklarının güçlendirilmiştir⁸².

Aydınlatma yükümlülüğünün bir diğer görünümü hesap verilebilirlik ilkesidir. GVKT gereğince hesap verilebilirlik ilkesi, veri sorumlusunun veri işleme faaliyetinin her aşamasında GVKT 5. maddesinde sayılan kişisel verilerin işlenmesine ilişkin hukuka uygunluk, adalet ve şeffaflık, amacın sınırlandırılması, verilerin en az seviyeye indirilmesi, doğruluk, saklama süresinin sınırlandırılması, bütünlük ve gizlilik ilkelerine uygun davranmak ve uygun davrandığını gösterebilmesi gerekliliğini ifade etmektedir⁸³.

IV. İLGİLİ KİŞİNİN HAKLARI

A. Erişim Hakkı

Bireyin, verileri üzerinde hâkimiyet sağlayabilmesi, verilerini koruyabilmesi ve verilerinin geleceğini belirleyebilmesi için öncelikle verilerinin kim tarafından, ne zaman, hangi amaçla, hangi verilerini işlediğini bilmesi gerekir⁸⁴.

OECD Rehber İlkelerine göre ilgili kişinin kendisi hakkında veriler toplanıp toplanmadığını, toplanmış ise hangi verilerinin toplandığını: ücretsiz veya makul bir ücret karşılığında, makul bir sürede, kendisinin anlayabileceği bir şekilde öğrenme

⁸¹ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 346.

⁸² Küzeci, s. 219.

⁸³ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 341.

⁸⁴ Şimşek, s. 90.

hakkı ve verilerinin silinmesini, düzeltilmesini, tamamlanmasını, değiştirilmesini talep etme hakkı bulunmaktadır⁸⁵.

AB Yönergesinin 12. maddesinde konuyla ilgili Üye Devletler tarafından aşırı gecikme veya masraf olmaksızın ve makul aralıklarla, sınırlama olmaksızın ilgili kişinin: (i) verilerin işlenip işlenmeyeceğine ilişkin onay ve en azından, verilerin açıklandığı alıcı kategorileri veya alıcıları ve ilgili verilerin kategorileri, işleme amaçları, (ii) işlenmekte olan bilginin kaynakları ve işleme tabi tutulan verilerin anlaşılır biçimde iletilmesini, (iii) otomatik kararlar durumunda, kendisine ilişkin verilerin otomatik işlenmesiyle ilgili temel bilgiye erişim hakkına sahip olduğu belirtilmiştir. Ayrıca Yönerge'ye göre ilgili kişinin verinin eksik veya yanlış olması yüzünden, Yönerge hükümlerine uymayan işlemede, verilerin engellenmesi veya silinmesi, uygun olarak düzeltilmesini; bunun imkânsız olması veya orantısız çabayı gerektirmesi haricinde her türlü düzeltme, silme veya engellenmenin verilerin açıklandığı üçüncü şahıslara bildirilmesini isteme hakkı vardır (Yönerge m. 12).

Kişisel verilerin korunmasına ilişkin AK Sözleşmesi'nde (8. madde), BM Rehber İlkeleri'nde de (4. İlke) erişim hakkına benzer şekilde yer verilmiştir⁸⁶. 6698 sayılı Kanun'da erişim hakkı ilgili kişinin erişim hakkına sahip olduğu bilgiler ayrıntılı olarak yer verilerek koruma altına alınmıştır. Kanun'un 11. maddesine göre:

“ (1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

a) Kişisel veri işlenip işlenmediğini öğrenme,

b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

c) Kişisel verilerin işleme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,

e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

⁸⁵ Şimşek, s. 90.

⁸⁶ Küzeci, s. 220.

f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.”

GVKT ile ilgili kişi erişim hakkı kapsamında aşağıdaki hakları kullanabilecek ve aşağıdaki bilgileri talep etme hakkına sahiptir (m.15)⁸⁷:

- a) İşleme faaliyetinin amaçları ve ilgili kişisel veri kategorileri,
- b) Kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri,
- c) Mümkün olması halinde, kişisel verilerin saklanması açısından öngörülen süre veya bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler,
- d) Kişisel verilerin veri sahibinden elde edilmemesi halinde bu verilerin kaynaklarına ilişkin mevcut bilgiler,
- e) İşleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları.

Ayrıca erişim hakkı kapsamında kişisel verilerin düzeltilmesi veya silinmesini veya söz konusu verilerin işlenmesinin kısıtlanmasını talep etme veya söz konusu işleme faaliyetine itiraz etme hakkına, denetim makamına şikâyetle bulunma hakkına ilişkin bilgi de talep edebilecektir (GVKT m. 15).

GVKT ile yeni bir hak daha kabul edilmiştir. “Veri taşınabilirliği hakkı” olarak adlandırılan bu hak ile veri sahibinin kendisi ile ilgili olarak veri sorumlusuna sağlamış olduğu kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma ve veri sorumlusunun herhangi bir engellemesi olmaksızın bu verileri başka bir kontrolöre iletme olanağını sağlamaktadır (GVKT m. 20)⁸⁸.

⁸⁷ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 349.

⁸⁸ Dülger, s. 160; Küzeci, s. 223; Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 352.

B. Düzeltme Hakkı

Veri sahibi, bilgi alma ve erişim hakkının doğal bir sonucu olarak kendisi ile ilgili tam veya doğru olmayan kişisel verilerinin gereksiz gecikmeye mahal verilmeksizin düzeltilmesini, silinmesini, tamamlanmasını veya engellenmesini talep etme hakkına sahiptir⁸⁹. Veri sahibi, veri sorumlusu tarafından bilgilendirilmemiş olsa dahi başka bir yolla öğrendiği eksik veya doğru olmayan verilerinin düzeltilmesini, silinmesini, tamamlanmasını veya engellenmesini talep edebilir.

Düzeltme hakkı, kişisel verilerin eksik, yanlış veya ilgili düzenlemelere aykırı işlendiği ya da doğruluğunu ve güncelliğini yitirdiği durumlarda veri sahibi tarafından kullanılabilecek bir haktır⁹⁰. GVKT16. maddesinde düzeltme hakkı, tamamlama hakkı ile birlikte “Veri sahibi, kendisine ilişkin doğru olmayan kişisel verilerin fazla gecikmeden düzeltilmesini ver sorumlusundan isteme hakkına haizdir. İşleme amaçları da gözetilmek suretiyle veri sahibi, ek beyan temin etme yolu da dâhil olmak üzere eksik kişisel verilerini tamamlattırma hakkını haizdir.” olarak düzenlenmiştir⁹¹. Verilerin düzeltilmesini isteme hakkı, yanlış olan verilerinin düzeltilmesinin yanında eksik olan verilerin tamamlanmasını da isteme hakkını içermektedir⁹². Veri sahibinin verilerinin düzeltilmesini veya tamamlanmasını talep etmesi üzerine veri sorumlusu, veri sahibinin talebinde yer alıp almadığına bakmaksızın durumun imkânsız veya ölçüsüz bir çabayı gerektirmediği hallerde her türlü düzeltme veya silme işlemi ya da işleme faaliyetini, kısıtlama işlemini kişisel verilerin açıklandığı her alıcıya bildirmekle yükümlüdür (GVKT m.19)⁹³.

Engelleme hakkı, kişisel verilerin doğruluğunun tartışmalı olduğu durumlarda verilerin doğruluğu veya yanlışlığı belirleninceye kadar bu verilerin işlenmemesi amacına yönelik önlem niteliğinde bir haktır⁹⁴.

⁸⁹ Şimşek, s. 92; Akgül, s. 143.

⁹⁰ Şimşek, s. 93; Akgül, s. 143; Aygözer Öngün, s. 155.

⁹¹ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 350.

⁹² Başalp, s. 50.

⁹³ Dülger, s. 163; Gemicioğlu/ Gemicioğlu/ Yağcı/ Yılmaz, s. 350.

⁹⁴ Şimşek, s. 93; Akgül, s. 144; GVKT’ nün 18. maddesinde veri faaliyetinin kısıtlanması hakkı kapsamında “Veri sahibi, aşağıdaki durumlarda veri sorumlusundan işleme faaliyetinin kısıtlanmasını talep etme hakkını haizdir: (a) veri sahibinin kişisel verilerin doğruluğuna itiraz etmesi halinde veri sorumlusuna kişisel verilerin doğruluğunu teyit etme fırsatı tanıyan bir süre için” denilerek engelleme hakkına yer verilmiştir. Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 351.

C. Unutulma Hakkı

Unutulma hakkı, “bireyin geçmişte hukuka uygun olarak yayılmış ve doğru nitelikteki bilgilerinin zamanın geçmesine bağlı olarak erişimden kaldırılmasını ya da gündeme getirilmemesini” talep etme hakkıdır⁹⁵. Bilişim teknolojilerinin sebep olduğu sorunlara karşı tartışılmaya başlanan unutulma hakkı, bir bakıma insan onuru ve bireyin “kişisel veriler üzerinde tam kontrol sahibi olma hakkı”nın bir görünümüdür⁹⁶.

Avrupa Birliği Adalet Divanı’nın 13 Mayıs 2014 tarihli Google- İspanya Kararı “unutulma hakkı”nın çıkış noktası olarak kabul edilmektedir⁹⁷. Daha sonra GVKT ile “unutulma hakkı” silme hakkı ile ilişkilendirilerek tanınmıştır. GVKT 17. maddesine göre veri sorumluları şu hallerde kişisel verileri gecikmeksizin silmekle yükümlüdür: (i) kişisel verilerin toplanma amacının gerçekleşmesi veya daha fazla tutulmasına ihtiyaç duyulmaması, (ii) veri sahibinin rızasını geri alması veya veri sahibinin işlemeye itiraz etmesi, (iii) kişisel verilerin kanuna aykırı işlenmiş olması, (iv) veri sorumlusunun tabi olduğu Avrupa Birliği ya da Üye Devlet kanunlarında yer alan düzenlemeler gereği kişisel verileri silmekle yükümlü olması, (v) kişisel verilerin bilgi toplumlarına hizmet sunulması amacıyla toplanmış olması.

D. İtiraz Hakkı

Veri sahibi, veri işleme faaliyetinin her aşamasında hukuka aykırı eylemlere karşı kamusal görevlerin yerine getirilmesi veya haklı çıkarların korunması amacıyla zaman sınırlaması olmaksızın itiraz etme hakkına sahiptir.⁹⁸ Belirli durumlarda kişisel verilerin işlenmesine itiraz hakkı ilk defa AB Veri Koruma Yönergesi’nin 14. maddesi ile tanınmıştır⁹⁹. İtiraz hakkı, bireyin temel hak ve özgürlüklerinin

⁹⁵ Sözüer, s. 7.

⁹⁶ Dülger, s. 167; Sözüer, s. 13; Yavuz, s. 44.

⁹⁷ Akıncı, s. 1; Kararın esasen unutulma hakkı tanımadığına ilişkin eleştirilere yönelik açıklamalar için bkz. Sözüer, s. 128; Yavuz, s. 75.

⁹⁸ Şimşek, 94; Akgül, s. 145.

⁹⁹ Küzeci, s. 228; Akgül, s. 145; Yönerge’nin 14. maddesi şöyledir: “Üye Devletler aşağıdaki hakları veri öznesine vereceklerdir: a. En azından madde 7 (e) ve (f)’de atıfta bulunulan durumlarda, ulusal mevzuat tarafından aksinin belirtilmesi haricinde, kendisine dair verilerin işlenmesinde, özel durumuna ilişkin zorlayıcı kanuni gerekçelere her zaman itiraz etmek. Geçerli bir itiraz

korunması, verileri üzerindeki hâkimiyetinin tam olarak sağlanması açısından oldukça önemli bir haktır.

6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 11. maddesinde veri sahibine veri sorumlusuna başvurarak kendisiyle ilgili “işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına” itiraz etme hakkı tanınmıştır.

GVKT ile 6698 sayılı Kanun’a benzer şekilde genel itiraz hakkının yanında kişisel verilerin doğrudan pazarlama amacıyla işlenmesi halinde itiraz etme hakkına ayrıca yer verilmiştir (GVKT m. 21). Tüzük’e göre genel itiraz hakkının söz konusu olduğu durumlarda veri sorumlusu veri sahibinin çıkar, hak ve özgürlüklerine ağır basan meşru gerekçeler göstermesi halinde kişisel verileri işleyebilecektir (GVKT m. 21/1). Ancak kişisel verilerin doğrudan pazarlama amacıyla işlenmesine itiraz etme hakkı mutlak olup; veri sorumlusu meşru gerekçelere dayanamaz ve artık bu kişisel verileri işlemeye devam edemez (GVKT m. 21/2)¹⁰⁰. GVKT ile ayrıca profil çıkarma da dahil olmak üzere verilerinin sadece otomatik işlenmesine dayalı kendisini önemli derecede etkileyen ya da hukuksal bağlayıcılığı olan otomatik bireysel kararlara itiraz hakkı da düzenlenmiştir (GVKT m. 22)¹⁰¹.

olduğunda, denetleyici tarafından başlatılan işleme, artık bu verileri kapsamayabilir; b. Denetleyicinin doğrudan pazarlama amaçları için işlenmesini öngördüğü, kendisine ait kişisel verilerin işlenmesine ücretsiz ve istek üzerine itiraz etme (hakkı) veya kişisel veriler üçüncü şahıslara ilk kez ifşa edilmeden veya doğrudan pazarlama amaçları için üçüncü şahıslar adına kullanılmadan önce bilgilendirilme (hakkı) ve bu tür ifşalara veya kullanımlara ücretsiz itiraz hakkının açık şekilde sunulması; Üye Devletler, (b)’nin ilk paragrafında atıfta bulunulan hakkın varlığından veri öznelerinin haberdar olmasını temin etmek için gerekli tedbirleri alacaklardır.”Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 322.

¹⁰⁰ Develioğlu, s. 97; Dülger, s. 165.

¹⁰¹ Dülger, s. 175; GVKT m. 22’de yer verilen hakkın kapsamına profil çıkarma da dahil edilmiştir. GVKT 4. maddesinde profil çıkarma, “özellikle bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, cinsel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumunu veya hareketleri ile ilgili hususları analiz etmek veya tahmin etmek gibi söz konusu gerçek kişinin bazı kişisel özelliklerini değerlendirmek için kişisel verilerin kullanılmasından ibaret olan her türlü otomatik imkanlar ile kişisel veri işleme” faaliyeti olarak tanımlanmıştır. Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 338.

E. İşleme Faaliyetinin Kısıtlanması Hakkı

GVKT ile veri sahibine, belirli durumlarda veri işleminin kısıtlanmasını talep etme hakkı tanınmıştır. Aşağıdaki durumlardan birinin geçerli olması halinde, veri sahibinin işleme faaliyetinin kısıtlanmasını talep etme hakkı bulunur (m.18)¹⁰²:

- a) Kişisel verilerin doğruluğuna veri sahibi tarafından itiraz edilmesi halinde, kontrolörün kişisel verilerin doğruluğunu teyit etmesini sağlayan bir süre boyunca,
- b) İşleme faaliyetinin yasa dışı olması ve veri sahibinin kişisel verilerin silinmesine itiraz etmesi ve bunun yerine verilerin kullanımının kısıtlanmasını talep etmesi,
- c) Veri sorumlusunun işleme amaçlarına yönelik olarak artık kişisel verilere ihtiyaç duymaması, ancak veri sahibinin yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması amacıyla söz konusu verilere ihtiyaç duyması,
- d) Veri sahibinin itiraz etmesi üzerine veri sorumlusunun meşru gerekçelerinin veri sahibinin meşru gerekçelerine ağır basıp basmadığı doğrulanana kadar süre boyunca.

¹⁰² Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 351.

İKİNCİ BÖLÜM

TARİHSEL SÜREÇ İÇERİSİNDE

KİŞİSEL VERİLERİN KORUNMASI HUKUKU

I. TARİHSEL SÜREÇ

Kişiye ait bilgiler, doğuştan gelen merak duygusunun dışında sosyolojik, siyasal ve hukuksal sebeplerden dolayı bir ya da birden fazla kişi ve örgüt tarafından bilinmek istenmiştir. Tarihsel süreçte veri koruma isteği bireyin, devletin gözetim ve denetim isteğine duyduğu kaygı sonucunda oluşmuştur. Koloniler halinde yaşayan insanlar birbirleri hakkında her şeyi bilirken; 18. yüzyıla gelindiğinde Sanayi Devrimi ile birlikte şehirlere göç eden insanlar bireysel alanlarını oluşturmaya başlamıştır. Bireyin kendi alanını belirlemesi ve onu koruma isteği özel hayat ve özel hayatın gizliliği hakkına ilişkin tartışmaları başlatmıştır.

Feodalitenin ve kilisenin etkisinin sona ermesinin ardından geleneksel devlet anlayışından modern devlet anlayışına geçilmiştir. POGGI, modern devleti “aralarında eşgüdüm sağlanmış çok sayıda görevin hizmetindeki tek bir merkezden gelen bilgiyle harekete geçen ve o merkezce yönetilen bir makina” olarak betimlemektedir¹⁰³. Devlet, tek bir merkezden güçlü ve istikrarlı bir yönetimin sağlayabilmek için bireylerin bilgilerini gözetim araçları toplamaya ve kullanmaya başlamıştır. George Orwell’in “1984”¹⁰⁴ adlı romanında “Büyük Birader” imgesi ile ortaya koyduğu totaliter rejimin, kişinin hayatında aldığı yer ve aynı zamanda kişilerin hayatında yarattığı etkileri daha net bir şekilde ortaya koymaktadır. George Orwell’indistopyasında devlet; yurttaşları evlerindeki televizyonlar aracılığıyla gözetlemekte, düşüncelerini yönlendirebilmekte ve her türlü bilgiyi elinde tutarak bilgiyi istediği şekilde değiştirebilmektedir. Bugün için bireyin bilgilerine sınırsız erişim sadece devlet tekeline değildir. Bilişim teknolojilerinin gelişimi ile ulusal ve uluslararası birçok veri toplayıcısı gün içerisinde biz farkında olmadan bilgilerimize erişmekte ve bu bilgilerimizi paylaşmaktadır. Özel teşebbüsler kişilere ait veriler

¹⁰³ Gianfranco Poggi, **Modern Devletin Gelişimi Sosyolojik Bir Yaklaşım**, çev. Şule Kurt, Binnaz toprak, İstanbul Bilgi Üniversitesi Yayınları, 2. Baskı, İstanbul 2002, s.119 (Dülger, s. 37 Naklen).

¹⁰⁴ George Orwell, **Bin Dokuz Yüz Seksek Dört**, çev. Nuran Akgören, Can Yayınları, 2001.

sayesinde kazanç sağlamaktadır. Bilim ve teknolojiadaki ilerleme karşısında bireyin kişisel verilerini korunma ihtiyacı artmıştır.

II. ULUSLARARASI KURUMLAR BÜNYESİNDE YAPILAN DÜZENLEMELER

A. OECD Ekonomik İşbirliği ve Kalkınma Örgütü

Ekonomik İşbirliği ve Kalkınma Teşkilatı kısaca OECD, İkinci Dünya Savaşı sonrasında Avrupa Ekonomi İşbirliği Teşkilatı'nın (OEEC) işlevini tamamlaması ardından 14 Aralık 1960 tarihinde; ekonomik büyümeyi ve hayat standardını yükseltecek, uluslararası standartlara uygun dünya ticaretinin büyüyen dünya ekonomisinin gelişmesini sağlayacak, örgüte üye olmayan devletlerde ekonomik kalkınmayı sağlayacak yöntemler geliştirmek amacıyla kurulmuştur¹⁰⁵.

Küresel ekonominin kalkınmasına ve gelişmesine katkı sağlayacak pek çok ekonomik, sosyal, hukuksal ve siyasal faaliyete imza atan örgütün 1980 yılında kabul etmiş olduğu “Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler (Guidelines on The Protection of Privacy and Transborder Flows of Personal Data)” kişisel verilerin korunması hakkını birebir ele alan ilk belge niteliğini taşımaktadır¹⁰⁶. Üye Devletler açısından tavsiye niteliğinde olan bu ilkeler ile güvenlik kültürünün oluşması için mevcut politika ve düzenlemelerde işbirliği yapılması amaçlanmıştır¹⁰⁷.

OECD Rehber İlkelerinde kişisel veri, devamında gelecek pek çok uluslararası düzenlemede olduğu “kimliği bilinen veya bulunabilecek olan bir şahsa (veri sahibi) ait her türlü bilgi” olarak tanımlanmıştır¹⁰⁸. Kişisel verilerin korunmasına ilişkin standartların oluşturulmasında ve üye devletlerce oluşturulacak politikalarda esas alınması tavsiye edilen temel ilkeler şunlardır:¹⁰⁹

¹⁰⁵ Türkiye Cumhuriyeti Dış İşleri Bakanlığı, İktisadi İşbirliği ve Gelişme Teşkilatı (OECD), www.mfa.gov.tr, (10.10.2019).

¹⁰⁶ Dülger, s. 50.

¹⁰⁷ Küzeci, s. 114.

¹⁰⁸ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 267.

¹⁰⁹ Dülger, s. 51; Küzeci, s. 114; Şimşek, s. 15; Taştan, s. 12; Ayözger Öngün, s. 68; Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 268.

- a) Veri toplamanın sınırlı olması ilkesi: Kişisel verilerin, veri sahibinin rızası ve bilgisi dâhilinde hukuka uygun sebeplerle ve araçlarla sınırlı toplanmasını,
- b) Verilerin belirli bir niteliği karşılaması (veri kalitesi) ilkesi: Kişisel verilerin kullanılacakları amaçla ilgili doğru, tam ve güncel olması gerektiğini,
- c) Amacın özgülük ilkesi: Kişisel verilerin belirli bir amaç için ve bu amaçla sınırlı olarak toplanması gerektiğini,
- d) Kullanımının sınırlı olması ilkesi: Veri sahibinin rızası ve kanunun verdiği yetki istisna olmak kaydıyla; toplanan kişisel verilerin toplanma amacı dışında bulundurulamayacak, kullanılamayacak ve ifşa edilemeyecek olmasını,
- e) Güvenlik Önlemleri İlkesi: Toplanan kişisel verilerin kaybedilme, yetkisiz kişilerce erişilme, değiştirilme, kullanılma, ifşa edilme gibi tehlikelere karşı güvenlik önlemleri ile korunması gerektiğini,
- f) Açıklık İlkesi: Kişisel verilerle ilgili işlemler, uygulamalar ve politikalarının aleni olması gerektiğini,
- g) Bireyin katılımı ilkesi: Veri sahibinin; (i) veri sorumlusunun kendisi ile bilgiye sahip olup olmadığı konusunda bilgi alma, (ii) kendisiyle ilgili verileri makul bir süre içerisinde, fahiş olmayan bir ücret karşılığında, makul bir şekilde ve kolayla anlaşılabileceği araçlarla kendisine iletilmesini, (iii) bilgi alma ve irtibata geçme hakkı kapsamında yapmış olduğu başvurunun reddedilmesi halinde itiraz etme hakkını, (iv) itirazının kabul edilmesi durumunda verisinin silinmesini, düzeltilmesini, değiştirilmesini veya tamamlanmasını isteme hakkını,
- h) Hesap verilebilirlik ilkesi: Veri sorumlusunun yukarıda anılı ilkelere uymaktan sorumlu tutulmasını ifade eder.

OECD Rehber İlkeleri, 2013 yılında temel ilkeler korunarak yasal gizlilik politikaları ve veri sızıntılarını bildirme yükümlülüğü gibi yeni düzenlemeler eklenerek güncellenmiştir¹¹⁰. Örgüt tarafından ayrıca 1985 yılında sınır ötesi veri akışlarına, 1998 yılında küresel ağlarda mahremiyetin korunmasına ilişkin iki ayrı bildiri daha kabul edilmiştir¹¹¹.

¹¹⁰ Küzeci, s. 117.

¹¹¹ Dilek Yüksel Civelek, **Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi** (Uzmanlık Tezi), 2011, s. 62; Ayözger Öngün, s. 69.

B. Birleşmiş Milletler

İkinci Dünya Savaşından galip çıkan devletler, savaşın yıkıcı etkilerinin giderilmesi, uluslararası barış ve güvenliğin sağlanması ve korunması, savaşların tekrarlanmaması amacıyla galip çıkan devletler 24 Ekim 1945 tarihinde Birleşmiş Milletler Örgütü'nü (BM) kurmuşlardır¹¹². Örgütün kurucu antlaşması olan Birleşmiş Milletler Şartı'nda örgütün temel amaçlarından birinin de insan haklarına ve temel özgürlüklere olan saygının geliştirilmesi ve bu konuda uluslararası işbirliğinin sağlanması olduğu açıklanmıştır¹¹³.

1. İnsan Hakları Evrensel Beyannamesi

Temel hak ve özgürlüklerin tanınması ve korunmasına dair atılan en önemli adım Birleşmiş Milletler tarafından 10 Aralık 1948 tarihinde kabul edilen “İnsan Hakları Evrensel Beyannamesi”dir. Beyanname'nin 12. maddesi “Hiç kimsenin özel hayatını, ailesi, meskeni veya yazışması hususunda keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz kalmaz. Herkesin bu karışma ve tecavüzlere karşı kanun yolu ile korunmağa hakkı vardır” şeklinde düzenlenmiş olup özel hayatın gizliliğine vurgu yapılmıştır¹¹⁴.

2. Birleşmiş Milletler Medeni ve Siyasal Haklara İlişkin Uluslararası Sözleşme

İnsan Hakları Evrensel Beyannamesi'ne benzer şekilde 23 Mart 1976 tarihinde yürürlüğe giren “Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme”sinin 17. maddesinde “Hiç kimsenin özel hayatına, ailesine, evine ya da haberleşmesine keyfi ya da yasadışı olarak müdahale edilemez; hiç kimsenin şeref ve itibarına yasal olmayan tecavüzlerde bulunulamaz. Herkesin, bu gibi müdahalelere

¹¹² Türkiye Cumhuriyeti Dış İşleri Bakanlığı, Birleşmiş Milletler Teşkilatı ve Türkiye, www.mfa.gov.tr, (10.10.2019).

¹¹³ Birleşmiş Milletler Antlaşması, R.G 24.08.1945 S. 6092; Mehmet Semih Gemalmaz, **Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş**, Beta Yayınları, İstanbul, 2001, s. 312.

¹¹⁴ İnsan Hakları Evrensel Beyannamesi, R.G 27.05.1949 S. 7217; Enver Bozkurt, **Türkiye'nin Uluslararası Hukuk Mevzuatı**, Asil Yayınları, Ankara, 2011, s. 412; Gemalmaz, s. 317.

ya da tecavüzlere karşı yasalarca korunma hakkı vardır”denilmekle özel hayatın gizliliği koruma altına alınmıştır¹¹⁵.

Birleşmiş Milletler İnsan Hakları Komitesi’nin 1988 tarihli oturumunda Sözleşme’nin 17. maddesine getirdiği açıklamadan kişisel verilerin korunması hakkını özel hayatın gizliliği hakkı kapsamında değerlendirdiği anlaşılmaktadır¹¹⁶. Yorumda bugün için kişisel verilerin korunması hakkı bağlamında kabul gören pek çok ilkeye yer verildiği dikkat çekmektedir.

Ülkemizde de Danıştay 10. Dairesi’nin 08.06.2015 tarihli 2014/3950 E. 2015/2774 K. sayılı¹¹⁷ kamu çalışanlarının faaliyet yürüttüğü servislerde uygulanan kameralı takip sistemine ve Danıştay İdari Dava Daireleri Kurulu’nun 09.12.2015 tarihli 2014/2242 E. 2015/4991 K. sayılı¹¹⁸ parmak izi tarama sistemiyle mesai kontrol uygulamasına ilişkin kararında Birleşmiş Milletler Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşmesi dikkate alınmıştır¹¹⁹.

3. Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler

BM tarafından kişisel verilerin korunması hakkını özel hayatın gizliliği kapsamından bağımsız olarak ele alan ilk düzenleme Birleşmiş Milletler Genel

¹¹⁵ Türkiye, Sözleşmeyi 4868 sayılı Kanun ile onaylamıştır; Bozkurt, s. 561.

¹¹⁶ “Tüm insanların toplum içerisinde yaşamalarının sonucu olarak, özel hayatın gizliliğinin korunması kaçınılmaz şekilde görecelidir. Ancak, Sözleşme’den anlaşıldığı üzere yetkili kamu otoriteleri, bilinmesi toplumun çıkarlarının korunması açısından gerekli olan, bireyin özel hayatıyla ilgili bir bilgiyi öğrenme talebinde bulunabilmelidir... Bu nedenle Komite, Devletlerin raporlarında özel hayata meşru müdahalelere dair kanun ve düzenlemeleri belirtmelerini önermektedir. Kamu otoritelerinin, özel kişi veya kurumların bilgisayarlarda, veri bankalarında veya benzeri cihazlarda kişisel bilgileri toplaması veya saklaması hukuki düzenlemeye tâbi olmalıdır. Devletler, bir kimsenin özel hayatına dair bilgilerin hukuken bu bilgilere sahip olma ve kullanma yetkisine sahip olmayanların eline geçmesini ve bu bilgilerin Sözleşme’nin amaçlarına aykırılık teşkil edecek şekilde kullanılmasını engellemek için etkili tedbirler almalıdır. Özel hayatın gizliliğinin en etkili şekilde korunabilmesi için, her birey kişisel dosyalarda veya veri tabanlarında kendisiyle ilgili bilgiler saklanmışsa bu bilgilerin ne tür bilgiler olduğunu ve ne amaçla saklandığını öğrenme hakkına sahiptir. Ayrıca, her birey hangi kamu otoritelerinin, özel kişilerin veya kurumların bu dosyaları kontrol altında tuttuğunu veya tutabileceğini öğrenebilmelidir. Söz konusu dosyaların, yanlış kişisel bilgilere yer vermesi halinde veya bu bilgilerin hukuka aykırı şekilde toplanması veya kullanılması halinde her birey düzeltme veya bilgilerin ortadan kaldırılmasını talep etme hakkına sahiptir.” Mehmet Semih Gemalmaz, **Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş**, 6. Baskı, Legal, 2007, s. 434 (Küzeci, s. 118 Naklen).

¹¹⁷ www.kazanci.com.tr.

¹¹⁸ Karar metni için bkz. Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 531.

¹¹⁹ Dölger, s. 52.

Kurulu tarafından 14 Aralık 1990 tarihinde yayınlanan “Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler”dir.¹²⁰ Düzenlemede ayrıca Rehber İlkelerin uygulanmasını denetleyecek bir organın kurulması gerektiğine işaret edilmektedir¹²¹. Üye ülkelerin iç hukuk düzenlemelerinde uymaları gereken ilkeler şunlardır¹²²:

- a) Kanuna uygunluk ve adalet ilkesi,
- b) Doğruluk ilkesi,
- c) Amaç belirtme ilkesi,
- d) İlgili kişinin erişimi ilkesi,
- e) Ayrımcılık yasağı ilkesi,
- f) İstisna yapma yetkisi,
- g) Güvenlik ilkesi,
- h) Denetim ve yaptırım ilkesi,
- i) Sınır ötesi veri akışı ilkesi
- j) Uygulama alanı.

C. Avrupa Konseyi

Avrupa Konseyi (AK), İkinci Dünya Savaşı’nın bitmesiyle maddi ve manevi kayıplar yaşayan Avrupa’da insan hakları, hukukun üstünlüğü, demokrasi ilkelerine bağlı kalarak ekonomik, sosyal, kültürel, bilimsel, yasal ve idari alanda üye ülkeler arasında sıkı ve ayrılmaz bir birlik kurmak amacıyla 5 Mayıs 1949 tarihinde kurulmuştur¹²³. Türkiye’nin kurucu üyesi sayıldığı örgütün, kurucu antlaşması 5 Mayıs 1949 tarihinde imzalanarak 3 Ağustos 1949 tarihinde yürürlüğe giren “Avrupa Konseyi Statüsü”dür¹²⁴.

Avrupa Konseyi Statüsü’nün 1. maddesinin (a) bendinde Avrupa Konseyi’nin amacının “üyeleri arasında, ortak mirasları olan ülkü ve ilkeleri korumak ve yaymak ve siyasi, ekonomik ilerlemelerini sağlamak amacıyla daha sıkı bir birlik

¹²⁰ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 303; Küzeci, s. 119.

¹²¹ Küzeci, s.120; Şimşek, s. 16; Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 305.

¹²² Dülger, s. 53; Şimşek, s. 16; Taştan, s. 12; Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s.304.

¹²³ Gemalmaz, s. 364.

¹²⁴ Avrupa Konseyinin Kurulması Hakkında İmzalanmış Olan Statünün Onanmasına Dair Kanun, RG, 17Aralık 1949, s. 7382; Türkiye Cumhuriyeti Dış İşleri Bakanlığı, Avrupa Konseyi, www.mfa.gov.tr, (10.10.2019); Bozkurt, s. 698.

yaratmak”olduğu bildirilmiştir. AK üyesi Devletler, Statü’nün 3. maddesi uyarınca, hukukun üstünlüğünü ve kendi yetkisi altında bulunan herkesin insan haklarından ve temel özgürlüklerden yararlanmasını sağlamakla yükümlüdür. Konsey’in bu amaç doğrultusunda atmış olduğu en büyük adım “Avrupa İnsan Hakları Sözleşmesi”nin kabulüdür. Bunun yanı sıra 1981 tarihli “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi”, 1966 tarihli “Biyotıp ve İnsan Hakları Sözleşmesi (Biyotetik Sözleşmesi)”, “Siber Suç Sözleşmesi (Bilgisayar Suçluluğuna İlişkin 185 No’lu Sözleşme veya Budapeşte Sözleşmesi)”diğer önemli düzenlemelerdir¹²⁵.

1. 108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde Strazburg’da imzaya açılarak 1 Ekim 1985 tarihinde yürürlüğe giren 108 No’lu sözleşme olarak da bilinen “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi” kişisel verilerin korunması hukuku alanında bağlayıcılığı olan ilk sözleşme özelliğini taşımaktadır¹²⁶. Sözleşme, Türkiye tarafından 1981 yılında imzalamıştır¹²⁷.

Sözleşmenin amacı; sözleşmeye taraf devlette uyruğu ve ikametgâhı ne olursa olsun gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel yaşama saygı hakkını güvence altına almaktır (m.1). Sözleşme, Konsey üyesi olmayan devletlerin de katılımına açıktır (m.23). Taraf devletler, sözleşme ile koruma altına alınan kişisel verilerin korunması amacıyla kendi iç hukukunda gerekli önlemleri en geç Sözleşme’nin kendisi bakımından yürürlüğe girdiği tarihte almakla yükümlüdür (m.4).

¹²⁵ Şimşek, s. 19.

¹²⁶ Dülger, s. 54; Taştan, s. 14; Sözleşme için bkz. Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 291.

¹²⁷ 17 Mart 2016 tarihinde 29656 sayılı Resmi Gazetede yayımlanan onay kanunu ile yürürlüğe girmiştir.

Sözleşme’de kişisel verilerin korunması hukuku alanına ilişkin temel kavramlara ve ilkelere açıklık getirmiştir. Sözleşmeye göre (m.2)¹²⁸;

“Bu sözleşmenin amaçları bakımından:

a) ”Kişisel veriler”: kimliği belirli veya belirlenebilir bir gerçek kişi (“ilgili kişi”) hakkındaki tüm bilgileri ifade eder;

b) “Otomatik veri dosyası”, otomatik işleme konu olan bilgilerin tümünü ifade eder;

c) “Otomatik işlem”, tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılr.

d) “Dosya yöneticisi”, otomatik veri dosyasının amacının ne olacağı, hangi kişisel veri kategorilerinin kaydedilmesi gerektiği ve bunlara hangi işlemlerin uygulanacağı hakkında karar verebilecek olan gerçek veya tüzel kişi, kamu kurumunu, birimi veya ulusal kanunlara göre yetkili olan diğer kuruluşları ifade eder.”

Otomatik işleme tabi tutulan kişisel verilere ilişkin temel ilkeler göre kişisel veriler (m.5):

- a) Adil ve yasal yollarla elde edilmeli ve işleme tabi tutulmalı,
- b) Bir amaca uygun olarak kaydedilmeli ve amaca uygun olarak kullanılmalı,
- c) Kaydedilme amaçlarına göre aşırı olmamalıdır,
- d) Doğru bilgileri yansıtmalı ve gerektiğinde güncellenmeli,
- e) İlgili kişilerin kimliklerini belirlemeye imkân verecek şekilde ve kaydedilme amaçları için gerekli süreyi aşmayacak sürede saklanmalıdır.

Sözleşmede kişisel verilerin kategorilere ayrılarak; bireyin ırksal kökenine, siyasal düşüncesine, din veya diğer inançları ortaya koyan kişisel verileri ile sağlık veya cinsel hayatına, ceza mahkûmiyetlere dair verilerinin hassas veri olduğu kabul edilmiştir (m.6).

Hassas verilerin özel olarak koruma altına alınmış iç hukukta uygun güvenceler sağlanmadıkça otomatik işleme tabi tutulamayacakları öngörülmüştür. Sözleşmeye Taraf Devletler otomatik işleme tabi tutulan verilerin güvenliğini

¹²⁸ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 292.

sağlanmak için kişisel verilerin kazaen veya izinsiz olarak imhasına veya bunların izinsiz olarak elde edilmesine, değiştirilmesine veya dağıtılmasına karşı güvenlik önlemlerini almakla yükümlüdür (m.7). Bununla birlikte ilgili kişilere birtakım ek güvenceler de sağlanmıştır. Buna göre herkesin (i) kendisine ait verilerin toplanma amacını, veri sorumlusunun kimliğini, ikametini ve kurumunu bilmeye, (ii) makul bir süre içerisinde, makul bir ücret karşılığında, makul bir şekilde ve kolayla anlaşılabileceği araçlarla kendisine ait verilerin işlenip işlenmediğini öğrenmeye, (iii) gerekli hallerde verilerin silinmesini, düzeltilmesini, tamamlanmasını veya değiştirilmesini istemeye, (iv) talepleri yerine getirilmezse yasal yollara başvurmaya hakkı vardır (m.8).

Sözleşmede, öngörülen hakların kullanılmasına Taraf Devletlerin kanunlarında öngörülmüş ve ancak demokratik bir toplulukta gerekli bir tedbir olarak, devletin güvenliğinin korunması, kamu güvenliği, devletin menfaatleri, suçun önlenmesi ve ilgili kişinin veya 3. kişinin hak ve özgürlüklerinin korunması amacıyla istisnalar getirilebileceği öngörülmüştür (m.9).

Sözleşmede otomatik işleme konu olan veya otomatik işleme konu olmak üzere toplanmış olan kişisel verilerin sınır ötesi transferine yer verilmiştir. Kural olarak Taraf Devletlerin her biri özel yaşamın korunması amacıyla kendi egemenlik alanındaki verileri Sözleşmeye taraf diğer devletlere vermeyi yasaklayamaz ve özel bir izne tabi tutamaz (m.12). Ancak bu kurala getirilen iki istisnai durum: (i) taraf devletin iç hukukunda belli kişisel veri veya otomatik kişisel veri dosyası kategorileri için verilerin veya dosyaların doğasından kaynaklanan özel düzenlemeler bulunması, transfer edilecek diğer taraf devletin iç hukukunda ise eşdeğer bir korumanın bulunmaması, (ii) taraf devletin ülkesinden yapılacak transferin diğer taraf devletin mevzuatında yer alan boşluklardan yararlanılarak taraf olmayan bir devletin ülkesine yapılmasını engellemek istenmesidir (m.12/3).

Taraf Devletlerin belirleyeceği bir asil temsilci bir de temsilci vekilinden oluşacak Danışma Komitesi kurulması öngörülmüştür (m.18). Sözleşmeye taraf olmayan Avrupa Konseyi üyesi devletlere de Komitede bir gözlemci tarafından temsil edilme hakkı tanınmıştır. Danışma Komitesinin görevleri ise şöyledir: (i) sözleşmenin uygulanmasını kolaylaştırmak veya iyileştirmek amacıyla önerilerde bulunmak, (ii) sözleşmede değişiklik yapılmasına dair önerilerde bulunmak ve

kendisine sunulan tüm öneriler hakkında görüş bildirmek, (iii) taraflardan gelecek talep üzerine Sözleşme'nin uygulanması ile ilgili sorular hakkında görüş bildirmektir (m.19).

Görüldüğü üzere 108 No'lu Sözleşmesi ile kişisel verileri koruma bilinci oluşturularak kişisel verilerin hem Avrupa Konseyine üye devletler hem de üye olmasa da Sözleşme'ye taraf devletlerce korunması amaçlanmaktadır.

2. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek: Denetleyici Makamlar ve Sınırışan Veri Akışına İlişkin Protokol

108 No'lu Sözleşme'ye ek bir düzenleme niteliğinde olan protokol Sözleşmedeki eksikliklerin giderilmesi için düzenlenmiştir. 181 No'lu Ek Protokol ile veri işleme faaliyetlerini denetleyecek bağımsız bir organ belirlenmesi gerektiği öngörülmüştür¹²⁹. Bu yolla Taraf Devletler, Sözleşme ve Protokolde belirtilen ilkeleri uygulamaya koymak ve denetlemekle yükümlü bir veya birden fazla organ belirleme yükümlülüğü altına girmiştir.

3. Avrupa İnsan Hakları Sözleşmesi

BM İnsan Hakları Evrensel Beyannamesinde anılan hakların her yerde tanınmasını ve fiilen uygulanmasını sağlamak amacıyla 4 Kasım 1950 tarihinde “İnsan Haklarını ve Ana Hürriyetlerini Korumaya Dair Sözleşmesi (Avrupa İnsan Hakları Sözleşmesi)” kabul edilmiştir¹³⁰. Türkiye, Sözleşmeyi 4 Kasım 1954 tarihinde imzalamıştır¹³¹. Sözleşme'de kişisel verilerin korunması hakkı bağımsız bir hak olarak düzenlenmemiştir. Ancak Sözleşme'nin 8. maddesinde özü itibarıyla kişisel verilerin korunması hakkını kapsayan “özel hayatın ve aile hayatının korunması hakkı”na yer verilmiştir. Sözleşme'nin 8. maddesi şöyledir;

¹²⁹ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 333; Türkiye Büyük Millet Meclisi, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınırışan Veri Akışına İlişkin Protokolün Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı (1/692) ve Dışişleri Komisyonu Raporu, www.tbmm.gov.tr, (10.10.2019), s. 9.

¹³⁰ Bozkurt, s. 429.

¹³¹ 10 Mart 1954 tarihinde 6366 sayılı “İnsan Haklarını ve Ana Hürriyetleri Koruma Sözleşmesi ve buna Ek Protokolün Tasdiki Hakkında Kanun” kabul edilmiştir. RG, 19 Mart 1954, Sayı 8662.

“ 1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.”

Avrupa İnsan Hakları Mahkemesi, Sözleşme’nin 8. maddesini geniş yorumlayarak kişisel verilerin korunması hakkına dair temel ilkeleri koruma altına almıştır. Mahkeme Stjerna/Finlandiya kararı ve Guillot/Fransa kararında kişinin soyadının; kişinin kimliğini ve ailesini belirli kılacağından özel hayatın ve aile hayatının korunması hakkı kapsamında değerlendirilmesi gerektiğine karar vermiştir¹³². S. ve Marper/Birleşik Krallık kararında başvuranlardan alınan parmak izlerine, kök hücrelerine ve DNA profillerine ilişkin verilerinin saklanması özel yaşamın korunması hakkına orantısız müdahale teşkil ettiğini belirterek Sözleşme’nin 8. maddesinin ihlal edildiğine karar vermiştir¹³³.

Sözleşmenin 8. maddesinin 2. fıkrasına göre özel hayatın ve aile hayatının korunması hakkına kamu makamlarınca yapılacak müdahalenin ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda mümkün olduğu belirtilmiştir. AİHM içtihatlarında da özel hayatın ve aile hayatının korunması hakkı ile zorlayıcı toplumsal ihtiyaç ve kamu makamlarınca yapılacak müdahale arasında makul bir dengenin bulunmasının zorunlu olduğu vurgulanmaktadır. Mahkeme Leander/İsveç kararında; hakkında güvenlik soruşturması yapıldıktan sonra işine son verilmesi üzerine bilgi edinme hakkı kapsamında hakkında sakıncalı bulunan bilgileri öğrenme talebinin reddinin,

¹³² Ursula Kilkelly, **Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı Avrupa İnsan Hakları Sözleşmesi’nin 8. Maddesi’nin Uygulanmasına İlişkin Kılavuz**, İnsan Hakları Kitapları No.1, Türkiye Cumhuriyeti Adalet Bakanlığı İnsan Hakları Dairesi Başkanlığı, www.inhak.gov.tr, (10.10.2019), s. 22.

¹³³ Türkiye Cumhuriyeti Adalet Bakanlığı İnsan Hakları Dairesi Başkanlığı, AİHM Kararları Tematik Bilgi Notları, www.inhak.gov.tr, (10.10.2019), s. 13.

ulusal güvenlik sebebiyle Sözleşme'nin 8. maddesine aykırılık teşkil etmeyeceği yönünde karar vermiştir¹³⁴.

D. Avrupa Birliği

Avrupa'nın bütünleşmesi fikri eski dönemlerden beri var olsa da özellikle İkinci Dünya Savaşı'nın yıkıcı sonuçlarına karşı; barışın yeniden sağlanması, Avrupa devletlerinin güvence altına alınması, ekonomik kalkınma ve bütünleşme, refahın teşvik edilmesi, insan hakları ve temel özgürlüklerin güvence altına alınması amacıyla 1992 yılında Maastricht Antlaşması'yla (Avrupa Birliği Antlaşması) Avrupa Birliği kurulmuştur¹³⁵. Birliğin kurulma sürecini hazırlayan diğer antlaşmalar: 9 Mayıs 1950 tarihinde Fransız Hükümeti tarafından açıklanan Schuman Planı sonrası 18 Nisan 1951 tarihinde "Avrupa Kömür Çelik Topluluğu'nu Kuran Antlaşma (AKÇT Antlaşması)", 25 Mart 1957 tarihinde "Avrupa Ekonomik Topluluğu'nu Kuran Antlaşma (AET Antlaşması)" ve "Avrupa Atom Enerjisi Topluluğu'nu Kuran Antlaşma (AAET Antlaşması)"dır¹³⁶. Süreç içerisinde kurucu antlaşmaları değiştiren antlaşmalar ise: Avrupa Tek Senedi (1987), Amsterdam Antlaşması (1999), Nice Antlaşması (2003), Lizbon Antlaşması (2009)¹³⁷.

Avrupa Birliği ile Avrupa Devletleri'nin ekonomik, sosyal, siyasal ve hukuki bütünleşmesi amaçlanmıştır. Ekonomik, sosyal ve siyasal bütünleşmenin sağlanabilmesi ve ortak iç pazarın işleyebilmesi için ulusal hukukların birbirine yakınlaştırılması gerekmektedir¹³⁸.

Birlik Hukuku kuralları hiyerarşik bir üstünlük teşkil etmeksizin üye devlet bakımından doğrudan uygulanabilir nitelikte ve ulusal hukuk kuralları karşısında

¹³⁴ Cavidan Soykan, **İnsan Hakları Merkezi Çalışma Metinleri -III Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı: Özel Hayatın Gizliliği X İfade Özgürlüğü**, Ankara Üniversitesi Siyasal Bilimler Fakültesi İnsan Hakları Merkezi, Ankara, 2006, www.ihmpolitics.org, (10.10.2019), s. 6; Aydın, s. 67.

¹³⁵ Hacı Can, **Avrupa Birliği Hukuku**, Sürat Üniversitesi Yayınları, 2013, s. 13; Dülger, s. 57.

¹³⁶ Can, s. 12; Türkiye Cumhuriyeti Dış İşleri Bakanlığı Avrupa Birliği Başkanlığı, Avrupa Birliği'nin Kurucu Antlaşmaları, www.ab.gov.tr, (10.10.2019).

¹³⁷ Mehmet Hanifi Bayram, **Avrupa Birliği Hukuku Dersleri**, Seçkin Yayınları, Ankara, 2018, s. 148.

¹³⁸ Lale Burcu Önüt, **Avrupa Birliği Hukukunun Üye Devletlerde Uygulanması**, Seçkin Yayınları, Ankara, 2017, s. 143.

önceliklidir¹³⁹. Birlik Hukukunun kaynakları: birincil mevzuat olarak adlandırılan kurucu antlaşmalar, sözleşme hukuku olarak adlandırılan uluslararası antlaşmalar, ATAD tarafından kurucu andlaşmaların açık, kesin ve koşulsuz olması şartıyla doğrudan etkiye sahip olabileceği kabul edilmiştir¹⁴⁰.

Birlik Hukuku kaynakları arasında yer alan tüzükler doğaları gereği üye devletler tarafından ek bir düzenlemeye ihtiyaç duymaksızın doğrudan uygulanabilir ve bütünüyle bağlayıcıdır¹⁴¹. Buna karşın yönergelerin uygulanabilmesi üye devletlerin süresi içerisinde yönergedeki hususları iç hukuklarına aktarmasına ve konuya ilişkin yasal düzenlemeler yapmasına bağlıdır¹⁴². Üye devletler Birlik Hukukundan kaynaklanan yükümlülükleri yerine getirmek amacıyla gerekli düzenlemeleri yapmak ve önlemleri almakla yükümlüdür.

1. 95/46/AT Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi

Birlik içerisinde iç pazarın kurulması, ekonomik ve sosyal entegrasyonun sağlanması; kişisel verilerin üye devletler arasında serbestçe aktarımında zorunlu bir artışa sebep olmuştur. Teknolojinin gelişmesi ile kişisel verilerin aktarımı, işlenmesi kolaylaşmıştır. Birlik bünyesinde Üye Devletler arasında kişisel verilerin sınır ötesi aktarımının önündeki engelleri kaldırmak, üye devletlerin kişisel verilerin korunması hukukuna ilişkin farklı uygulamalarının önüne geçebilmek ve aynı zamanda bireyin kişisel verilerini koruma altına alabilmek için çalışmalar başlamıştır. Bu anlamdaki en önemli düzenlemelerden biri 24 Ekim 1995 tarih 95/46/EC sayılı “Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi”dir. 6698 sayılı Kişisel Verilerin Korunması Kanunu hazırlanırken Yönerge örnek alınmıştır.

25 Mayıs 2018 tarihinden itibaren AB Veri Koruma Yönergesinin yerini Avrupa Birliği Genel Veri Koruma Tüzüğü almıştır.

¹³⁹ Önüt, s. 44.

¹⁴⁰ Konuya ilişkin Atad kararları için bkz. Önüt, s. 167.

¹⁴¹ Küzeci, s. 194; Önüt, s. 170.

¹⁴² Önüt, s. 172.

a. Amacı ve Kapsamı

Yönerge'nin 1. maddesinde amacı şöyle belirlenmiştir: “(1)Bu Direktif’e uygun olarak, Üye Devletler, kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere gerçek kişilerin temel haklarını ve özgürlüklerini koruyacaktır; (2) Üye Devletler, 1 inci paragraf kapsamında sağlanan bağlantılı nedenler için Üye Devletler arasında kişisel verilerin akışını yasaklamayacak ya da engellemeyeceklerdir”¹⁴³. Yönerge'nin bir diğer amacı ise ortak pazarın kurulması ve işleyebilmesi için ülkeler arası veri akışı önündeki engellerin kaldırılması ile temel hakların korunması arasında makul dengenin sağlanmasıdır¹⁴⁴.

Yönerge, gerçek kişiye ait kişisel verilerin kısmen veya tamamen otomatik araçlarla işlenmesi ile bir dosya içerisine kaydedilerek veya kaydedilebilecek verilerin otomatik olmayan yollarla işlenmesi bakımından uygulanacaktır (m.3/1). Yönerge'nin uygulama alanı dışında bırakılan durumlar şunlardır: kişisel verilerin (i) ceza hukuku alanında devlet faaliyetleri, devlet güvenliği, savunma, kamu güvenliği sebebiyle, (ii) Avrupa Birliği Antlaşması'nın V. ve VI. başlıkları kapsamındaki faaliyetler, (iii) Topluluk Hukukunun uygulama alanı dışındaki faaliyetler, (iv) bir gerçek kişi tarafından tamamen kişisel ve eviçi faaliyetler gereğince işlenmiş olmasıdır. (m.3/2).

b. Temel Kavramlar

Yönerge’de, kişisel verilerin korunması hukukuna özgü kavramların tanımlamalarına yer verilmiştir. Yönerge ‘de açıklanan kavramlar ve açıklamaları şöyledir:¹⁴⁵

¹⁴³ 96/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direkti çevirisi için bkz. Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 307.

¹⁴⁴ Ayözger Öngün, s. 79; Murat Uygun, **Avrupa Birliği’nin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması**, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı Avrupa Birliği Hukuku Yayınlanmamış Yüksek Lisans Tezi, Ankara, 2010, s. 36.

¹⁴⁵ Şimşek, s. 43; Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 316.

- a) Kişisel veri: Yönerge’de bir gerçek kişiyi belirli veya belirlenebilir kılan tüm bilgiler kişisel veri olarak kabul edilmiştir. Ayrıca belirlenebilir kişi, “fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi ” olarak açıklanmıştır.
- b) Kişisel verilerin işlenmesi: Yönerge’ye göre kişisel verilerin işlenmesi: otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan silme, tahrip etme, engelleme, toplama, kaydetme, değiştirme veya adaptasyon, birleştirme veya sıralama, sağlama veya dağıtma, iletme, açıklama, değiştirme, danışma, depolama, kurtarma herhangi bir faaliyet veya faaliyet dizisidir. Veri işleme kavramı bakımından verilerin otomatik veya otomatik olmayan araçlarla işlenmesi yönünde bir ayırım yapılmamıştır.
- c) Kişisel veri dosyalama sistemi: Merkezi veya merkezi olmayan ya da işlevsel veya coğrafi tabana yayılmış özel kriterlere göre erişilebilir olan herhangi bir yapılandırılmış kişisel veri dizisidir.
- d) Denetleyici: Denetleyici bir diğer ifade ile veri işlem sorumlusu, tek başına ya da bir başkasıyla kişisel verilerin işlenme amaçlarını ve araçlarını belirleyen gerçek veya tüzel kişi, kamu makamı, devlet dairesi veya her türlü kuruluştur. Veri işlem sorumlusunun kim ve hangi ölçüde olacağı konusunda düzenleme yapma yetkisi Üye Devletlere ve Topluluk Hukuku’na verilmiştir.
- e) İşleyici: İşleyici yani veri işleyen, denetleyicinin talimatı ile denetleyici adına kişisel verileri işleyen gerçek veya tüzel kişiyi, kamu makamı, devlet dairesi veya her türlü kuruluştur. Veri işleyen, sadece veri sorumlusunun talimatı doğrultusunda hareket edecek ve talimatı kapsamında veri toplayabilecektir.
- f) Üçüncü kişi: Veri işlemek için yetkilendirilen işleyici veya denetleyicinin doğrudan yetkisi altındaki kişiler ve işleyici, denetleyici, veri öznesi dışındaki herhangi bir gerçek veya tüzel kişi, kamu makamı, devlet dairesi veya her türlü kuruluştur.
- g) Alıcı: Bir üçüncü kişi olsun ya da olmasın, verilerin açıklandığı gerçek veya tüzel kişi, kamu makamını, devlet dairesini veya diğer her türlü kuruluştur. Özel bir soruşturma kapsamında verileri alan makamlar alıcı olarak kabul edilmemektedir.

- h) Veri öznesinin rızası: Veri öznesinin, özgürce ve bilgilendirme yapıldıktan sonra kişisel verilerinin işlenmesine yönelik irade beyanıdır. Rıza beyanına ilişkin özel bir şekil öngörülmemiştir. Önemli olan veri öznesinin rızasının herkes tarafından kesin bir şekilde anlaşılır olmasıdır. Verilen rıza, somut veri işleme faaliyetine yönelik olmalıdır. Yapılan bilgilendirme, ilgili kişinin hangi kişisel verilerinin, hangi faaliyette, hangi amaç için, ne kadar süre ile kullanılacağı gibi bilgileri içerecek şekilde kapsamlı olmalıdır.

c. Temel İlkeler

Yönerge 'de bireyin temel hak ve özgürlüklerini koruma altına alabilmek için kişisel verilerin işlenmesine ilişkin temel ilkeler belirlenmiştir (m.6). Üye Devletlerin veri işleme faaliyeti sırasında uymaları gereken temel ilkeler:¹⁴⁶

- a) Adil ve yasal işleme: Kişisel verilerin özellikle dürüstlük kuralına ve hukuka uygun bir şekilde adil bir şekilde yasal yollarla işlenmesi gerektiğini ifade etmektedir.
- b) Amaca uygunluk ve amaç ile sınırlılık: Kişisel verilerin belirli, açık ve meşru amaç için toplanması ile bu amaca uygun ve bu amaçla sınırlı olarak işlenmiş olmasıdır.
- c) Orantılılık: Kişisel veriler, toplandığı ve/veya işlendiği amaç için yeterli, bu amaçla olmalıdır.
- d) Doğruluk ve güncellik: Kişisel verilerin doğru ve güncel tutulması gerekir. Verilerin toplanması ve daha sonraki işlemler bakımından verilerin eksik veya yanlış olması halinde silinmesine veya düzeltilmesine ilişkin tüm makul önlemler alınmalıdır.
- e) Süre ile sınırlılık: Veri öznesinin, verilerin toplandığı veya işlendiği amaçlar için makul olan süre boyunca tespit edilebilir olması; diğer bir anlatımla verilerin toplandığı veya işlendiği amaçlar için gerekli olan süreden daha uzun saklanamamasıdır.

Kural olarak kişinin özel kategorideki verisi olarak sayılan sağlık durumuna veya cinsel yaşama, sendika üyeliğine, dini veya felsefi inançlarına, siyasi

¹⁴⁶ Dülger, s. 58; Şimşek, s. 46; Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 318.

görüşlerine, ırk veya etnik kökenine ilişkin verilerinin işlenmesi yasaklanmışsa da; veri öznesinin fiziksel veya yasal olarak rızasını açıklamasının mümkün olmadığı durumlarda hayati menfaatini korumak için gerekli olması, işlemenin kanundan kaynaklanması gibi hallerde işlenebileceği öngörülmüştür (m.8).

Avrupa Birliği Hukukunda yönerge hükümleri Üye Devletlerde doğrudan uygulanamaz¹⁴⁷. Üye Devletler, antlaşmalardan kaynaklanan yükümlülüklerinin yerine getirilmesini sağlamak üzere iç hukuklarında her türlü tedbiri almakla yükümlüdür¹⁴⁸.

d. İlgili Kişinin Hakları

- a) Bilgi edinme hakkı: Veri öznesinin, kendisine ait verilerin işlenip işlenmediğini ve verileri işlenmişse hangi verilerinin veri işleme faaliyetine konu edildiğini öğrenme, özellikle eksik veya yanlış işlenmesi halinde verilerine erişimin engellenmesini, düzeltilmesini veya silinmesini; verilerin engellenmesi, düzeltilmesi veya silinmesi halinde verilerin aktarıldığı üçüncü kişilerin bilgilendirilmesini isteme hakkına sahip olmasıdır (m.12). Veri sorumlusunun bu konuda bilgi verme yükümlülüğü bulunmaktadır (m.10).
- b) Veri sahibinin itiraz hakkı: Veri öznesi, kişisel verilerinin işlenmesine itiraz etme hakkına sahiptir (m.14). Reklam amacıyla kişisel verilerinin işlenmesine doğrudan ve ücretsiz olarak itiraz edebilir¹⁴⁹. Üye Devletler tarafından ilgili kişilere, kişisel verileri üçüncü kişiler tarafından ifşa edilmeden önce veya pazarlama amacıyla üçüncü kişiler tarafından kullanılmadan önce bilgilendirme hakkı ve bu tür ifşa veya kullanımlara ücretsiz itiraz hakkı olduğu hususunda açık bir şekilde bilgi verilmelidir. Üye devletler ilgili kişilerin haklarının bildirilmesini temin etmek için gerekli tedbirleri almakla yükümlüdür.
- c) Otomatik bireysel kararlara tabi olmama hakkı: Bireylerin performans, kredibilite, güvenilirlik, tutum vb. gibi kişisel yönlerini değerlendirmek amacıyla verilerinin otomatik veri işlenmesi karşısında kendisini önemli derecede etkileyen hukuksal

¹⁴⁷ Yönergelerin doğrudan etkiye sahip olabileceğine ilişkin açıklamalar ve ATAD kararları için bkz. Önüt, s. 172.

¹⁴⁸ Önüt, s. 172; Hacı Can, Avrupa Birliği Sözleşme Hukuku, Adalet Yayınları, Ankara, 2015, s. 25.

¹⁴⁹ Şimşek, s. 47.

bağlayıcılık taşıyan ya da haklarını önemli ölçüde etkileyen otomatik bireysel kararlara tabi olmama hakkı vardır (m.15). Öngörülen istisnai durumlar şöyledir: Üye Devletler tarafından, (i) veri öznesinin görüşünü bildirmesine izin veren düzenlemeler gibi meşru menfaatlerini güvenceye alacak uygun tedbirler öngörülmüş olması, (ii) veri öznesi tarafından sözleşmenin kurulması veya yerine getirilmesi sırasında izin verilmesi, (iii) veri öznesinin meşru menfaatlerini güvence altına alan bir yasanın bulunmasıdır.

- d) Yargı yollarına başvurma hakkı: Üye Devletler ilgili kişinin, verilerinin işlenmesine karşı ulusal hukuka göre öngörülen yargısal yollara başvurma hakkını garanti altına almalıdır (m.22). Ayrıca Yönerge'ye göre Üye Devletler, Yönerge uyarınca kabul edilen ulusal hükümlerle aykırı bir işlemenin veya yasadışı bir işleme faaliyetinin sonucu olarak zarara uğrayan kişilerin, uğradığı zarar için denetleyiciden tazminat almaya hak kazanması hakkını koruma altına almalıdır (m.23). Denetleyici, zarara yol açan olayda sorumlu olmadığını kanıtlarsa, kısmen ya da tamamen bu yükümlülüğünden kurtulabilecektir¹⁵⁰.

Üye Devletler, özellikle bir ağ üzerinde kişisel verilerin iletilmesi gerektirdiğinde ve yetkisiz açıklama veya erişim, değiştirme, kazara kayıp veya kazara veya yasa dışı tahribe karşı diğer yasa dışı durumlara ve olası risklere karşı kişisel verileri korumak için gereken uygun teknik ve kurumsal tedbirleri almak veri işleminin güvenliğini garanti almakla yükümlüdür (m.17).

Üye Devletler gerekli önlemlerin alınması halinde verilerin işlenmesine ilişkin temel ilkelere, ilgili kişinin bilgilendirilmesi yükümlülüğüne ve verilerine erişim hakkına, veri işlem faaliyetlerinin aleniliği ilkelerine sınırlamalar ve istisnalar getirebilecektir (m.13). Ulusal güvenlik, ülkenin savunulması, meslekler bakımından etik ihlallerinin engellenmesinin veya suçların önlenmesi, incelenmesi, tespiti ve kovuşturulmasının; parasal, bütçe ve vergilendirme konuları dâhil olmak üzere Avrupa Birliği'nin veya bir Üye Devletin önemli bir ekonomik veya mali menfaatinin, ilgili kişinin ve diğer kişilerin temel hak ve özgürlüklerinin korunmasının gerektirdiği durumlarda sınırlama veya istisnalar getirilebilecektir.

¹⁵⁰ Şimşek, s. 48.

e. Bağımsız Denetleme Makamı ve Veri Koruma Grubu

Yönerge 'ye göre Üye Devletler, Yönerge uyarınca kabul edilen hükümlerin kendi ülkesindeki uygulamasını denetlemekle üzere tam bağımsız bir veya daha fazla kamu makamı belirlemek yükümlüdürler (m.28). Üye Devletler, kısmen veya tamamen otomatik işleme faaliyeti veya tek amaç veya ilgili çeşitli amaçlara hizmet etmek üzere bir dizi faaliyeti yürütmeden önce Yönerge'nin 28. maddesi doğrultusunda belirlenecek denetleme makamına bildirimde bulunacaklardır (m.18).

Ayrıca Yönerge ile Birlik düzeyinde ulusal denetleme makamlarının temsilcilerinden oluşan danışma statüsünde bağımsız bir veri koruma grubu oluşturulmuştur (m.29).

2. Avrupa Birliği Temel Haklar Şartı

Avrupa Birliği Temel Haklar Şartı (ABTŞ), Avrupa Birliği kurumlarının ve üye devletlerin insan haklarına saygı duymasını sağlamak, bireyin temel hak ve özgürlüklerini koruma altına almak ve bireylerin daha önce AB düzenlemeleri ile tanınmamış haklarına yer vererek temel hak ve özgürlüklerini tek bir belgede toplamak amacıyla 7 Aralık 2000 tarihinde kabul edilmiştir¹⁵¹.

ABTŞ ile temel haklar: onur, özgürlükler, eşitlik, dayanışma, yurttaş hakları, adalet olmak üzere altı bölümde incelenmiştir. Temel Haklar Şartı'nda kişisel verilerin korunması hakkı özel hayatın gizliliği hakkından bağımsız olarak düzenlenmiştir. "Kişisel bilgilerin korunması" başlıklı 8. madde şöyledir:

"1. Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.

2. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.

¹⁵¹ Yüksel Metin, **Avrupa Birliği Temel Haklar Şartı**, Ankara Üniversitesi SBF Dergisi, 57-4, s. 46; Küzeci, s. 156; Taştan, s. 16.

3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir.”

Böylelikle kişisel verilerin korunması hakkı, Birlik Hukukunca temel hak ve özgürlükler arasında bağımsız bir hak olarak sayılmıştır.

3. Avrupa Parlamentosu ve Konseyi 2002/58/AT Sayılı Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Yönergesi

95/46/AT Veri Koruma Yönergesi’ni tamamlayıcı mahiyette olan “Avrupa Parlamentosu ve Konseyi Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Direktifi” 12 Temmuz 2002 tarihinde kabul edilmiştir¹⁵². Yönerge’nin amacı “üye ülkelerin, elektronik haberleşme sektöründeki kişisel bilgilerin işlenmesine ilişkin olarak temel hak ve özgürlüklerin, özellikle de gizlilik hakkının eşit ölçüde korunmasını ve Birlik içinde bu tür veriler ile elektronik haberleşme ekipmanı ve hizmetlerinin serbest bir şekilde dolaşmasını sağlamasını gerektiren hükümleri uyumlaştırmak” olarak açıklanmıştır¹⁵³.

4. 2006/24/AT Sayılı İletişim Trafik Verilerinin Saklanması Yönergesi

15 Mart 2016 tarihinde kabul edilen Yönerge ile iletişim hizmetlerinden yararlanan kişilerin iletişimin içeriği haricindeki bilgilerinin ciddi suç şüphesinin varlığı halinde saklanabileceği öngörülmüştür¹⁵⁴.

5. 2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü GDPR

Avrupa Birliği Veri Koruma Yönergesinin yürürlüğe girdiği 90’lı yıllardan itibaren bu alanda oluşan tecrübe, gelişen teknolojiyle veriler üzerindeki faaliyetlerin artması ve değişmesi, çağın gereklerine uyum sağlama ihtiyacı kişisel verilerin korunması alanındaki mevcut düzenlemelerin yeniden ele alınması gerekliliğini

¹⁵² Nurullah Tekin, **Kişisel Verilerin Korunması İle İlgili Türkiye’deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi**, Uyuşmazlık Mahkemesi Dergisi, S. 4, 2014, s. 222-262, s. 285.

¹⁵³ Ayözger Öngün, s. 84.

¹⁵⁴ Dülger, s. 63.

gündeme getirmiştir¹⁵⁵. Dünya genelinde bu değişimi tetikleyen olayların başında Edward Snowden Olayı olarak anılan; 5 Haziran 2013 tarihinde TheGuardian Gazetesi'nde, Amerika Birleşik Devletleri'nin kendi müttefiklerini ve vatandaşlarını dinlediğine ilişkin belgelerin yayınlanması olayı gelmektedir¹⁵⁶. Bir diğer dönüm noktası şüphesiz Avrupa Birliği Adalet Divanı'nın (ATAD) Google-İspanya Kararı'dır¹⁵⁷. Karara konu olay, 5 Mart 2010 tarihinde İspanya vatandaşı olan avukat Mario Costeja Gonzalez, Google Arama Motoruna adını girdiğinde, yüksek tiraja sahip bir günlük gazetenin 19 Ocak ve 9 Mart 1998 tarihli iki sayfasında sosyal güvenlik borçlarının tahsiline ilişkin haciz davaları ile bağlantılı bir gayrimenkul açık arttırma ilanında kendisinden bahsedilmesi üzerine habere ilişkin kısa yolun arama motorundan kaldırılması talebinin reddine ilişkindir. Karar, daha sonra GVKT ile tanınan “unutulma hakkı”nın çıkış noktası olarak kabul edilmektedir¹⁵⁸. Divan ayrıca arama motorlarının AB Veri Koruma Yönergesi'ne göre denetleyici sayılması gerektiğine de karar vermiştir¹⁵⁹.

Yaşanan gelişmeler sonucunda AB Veri Koruma Yönergesi'ne benzer ancak daha kapsamlı düzenlemeler içeren “Genel Veri Koruma Tüzüğü (General Data Protection Regulation)” 14 Nisan 2016 tarihinde Avrupa Parlamentosu tarafından onaylanmıştır. Tüzük, 24 Mayıs 2016 tarihinde yürürlüğe girmişse de uygulanmaya başladığı tarih 25 Mayıs 2018 olarak belirlenmiştir.

Avrupa Birliği'nin İşleyişi Hakkında Kanun'un 288. maddesine göre Avrupa Birliği'nin hukuki kaynaklarından sayılan tüzükler, tüm üye devletler açısından tüm

¹⁵⁵ Ayşe Nur Akıncı, **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, Çalışma Raporu No.6, T.C Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Bilgi Toplumu Dairesi Başkanlığı, Haziran 2017, s. 10; Dülger, s. 64; Taştan, s. 17; Yapılan değişiklikler, bireylerin verileri üzerindeki kontrolünün güçlendirilmesi ve ticari işletmeler açısından hukuki belirliliğin sağlanması amacını taşımaktadır. Sözüer, s. 143.

¹⁵⁶ Akıncı, s. 11; Fatih Sezgin, **Edward Snowden Olayı'nın ABD-Rusya İlişkileri Üzerindeki Etkileri**, Uluslararası Yönetim ve Sosyal Araştırma Dergisi, C.1, S.1, 2014, 24-31, s. 26; Dülger, s. 64.

¹⁵⁷ Akıncı, s. 11; Karar için bkz. T.C Adalet Bakanlığı Avrupa Birliği Genel Müdürlüğü, www.abgm.adalet.gov.tr; Bozkurt Yüksel, s. 133.

¹⁵⁸ Akıncı, s. 1; Kararın esasen unutulma hakkı tanımadığına ilişkin eleştirilere yönelik açıklamalar için bkz. Sözüer, s. 128; Can Yavuz, **İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı**, Seçkin Yayıncılık, Ankara, 2018, s. 75.

¹⁵⁹ Yavuz, s. 89.

kısımlarıyla bağlayıcı ve üye devletlerde doğrudan uygulanabilir niteliktedir¹⁶⁰. Bu bakımdan GVKT ile üye devlet uygulamaları bakımından yeknesaklık sağlanmıştır.

Genel Veri Koruma Tüzüğü ile getirilen temel değişiklikler şöyledir¹⁶¹:

- a) AB Veri Koruma Yönergesi'nden farklı olarak GDPR tüzük olarak mevzuata dâhil edilmiştir. Genel Veri Koruma Tüzüğü üye devletler açısından bağlayıcı ve tüm üye devletlerde doğrudan uygulama alanı bulmaktadır.
- b) Direktif'ten farklı olarak yapılan en büyük değişiklik veri korumasına ilişkin bölgesel kapsamın arttırılmasıdır. Tüzük hükümleri AB dışındaki ülkeler bakımından da uygulama alanı bulmaktadır. AB içerisinde yer alan veri sorumlusu veya veri işleyen AB sınırları dışındaki veri işleme faaliyetleri GDPR kapsamında sayılmıştır. Ayrıca AB vatandaşlarına ait kişisel verilerin AB coğrafi sınırları dışında işlenmesi halinde AB vatandaşları GDPR düzenlemeleri ile getirilen korumalardan yararlanabilecektir.
- c) Rıza, veri sahibinin kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş, spesifik, bilinçli ve açık beyan ya da onay eylemidir. Tüzük ile veri sahibinden alınacak rızanın şartları güçlendirilmiştir. Her bir veri işleme faaliyeti için ayrı ayrı rıza alınması ve veri sorumlularının veri sahibinin rıza göstermiş olduğunu ispatlayabilmeleri öngörülmüştür. Ayrıca çevrimiçi sosyal ağları ya da web tarayıcılarını kullananların gizlilik ayarlarına ilişkin sessiz kalmalarının geçerli bir rıza beyanı olmayacağı öngörülmüştür.
- d) GVKT ile AB Veri Koruma Yönergesinden farklı olarak çocukların rızasına ilişkin hükümler yer almaktadır. Buna göre 16 yaşından küçük çocukların bilgi toplumu hizmetlerinden yararlanması amacıyla verilerinin işlenmesi ancak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verilmesi veya onaylanması halinde mümkündür. Üye devletler, 13 yaştan küçük olmamak kaydıyla daha küçük bir yaş belirleyebilecektir.
- e) AB Veri Koruma Yönergesi'nde veri işleme faaliyetleri sırasında hukuka aykırı eylemlerden sadece veri sorumlusu sorumlu tutulurken; GVKT ile veri sorumlusu ile birlikte veri işleyenlerinde sorumlu olduğu öngörülmüştür.

¹⁶⁰ Can, Sözleşmeler Hukuku, s. 24.

¹⁶¹ Dülger, s. 68; Akıncı, s. 14; Taştan, s. 18; Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 337, Develioğlu, s. 173; Ayözger Öngün, s. 88; Eda Uludere, **AB Genel Veri Koruma Tüzüğü ve Yer Bakımından Uygulanması**, Hukuk Postası 2017, Onikilevha Yayınları, İstanbul, 2018, 305-311, s. 306.

- f) GVKT ile aşağıda sayılan hallerde veri koruma görevlisi belirlenmesi zorunlu kılınmıştır:
- 1) İşleme faaliyetinin, yargı yetkisi çerçevesinde hareket eden mahkemeler hariç, bir kamu kuruluşu veya organı tarafından gerçekleştirilmesi,
 - 2) Veri kontrolörlerinin veya işleyicilerinin temel faaliyet alanlarının ya da amaçlarının, veri sahiplerini sistematik ya da düzenli şekilde izleyerek veri işleme faaliyetini gerçekleştirmesi durumunda,
 - 3) Kontrolör veya işleyicinin temel faaliyetlerinin 9. maddede sayılan özel kategorilerdeki verilerden ve 10. maddede belirtilen mahkûmiyet kararları ve suça ilişkin kişisel verilerin işlenmesinden oluşması durumunda.
- g) GVKT ile daha önce AB Veri Koruma Yönergesi'nde yer almayan, veri ihlallerine karşı önemli idari para cezaları öngörülmüştür. İdari para cezalarının üst sınırı şirketlerin cirolarına oranlanarak belirlenecektir. Somut olayın özelliğine göre idari para cezası kesilip kesilmeyeceğine karar verilirken ve idari para cezası meblağına karar verilirken, aşağıdaki hususların dikkate alınması öngörülmüştür:
- 1) İlgili işleme faaliyetinin mahiyeti, kapsamı veya amacı dikkate alındığında ihlalin mahiyeti, ciddiyeti ve süresinin yanı sıra etkilenen veri sahibi sayısı ve veri sahiplerinin yaşadığı zarar düzeyi,
 - 2) İhlalin kasıtlı olması veya ihmalkârlıktan kaynaklanması,
 - 3) Veri sahiplerinin yaşadığı zararın azaltılması için kontrolör veya işleyici tarafından gerçekleştirilen herhangi bir işlem,
 - 4) 25 ve 32. maddeler uyarınca kendileri tarafından uygulanan teknik ve düzenlemeye ilişkin tedbirler dikkate alındığında, kontrolörün veya işleyicinin sorumluluk derecesi,
 - 5) Kontrolör veya işleyicinin geçmişte konuyla ilgili ihlalleri,
 - 6) İhlalin düzeltilmesi ve ihlalin olası olumsuz etkilerinin azaltılması amacı ile denetim makamı ile gerçekleştirilen işbirliği derecesi,
 - 7) İhlalden etkilenen kişisel veri kategorileri,
 - 8) Kontrolör veya işleyicinin ihlali bildirip bildirmediği ve bildirdiyse ne ölçüde bildirdiği başta olmak üzere, denetim makamının ihlalden haberdar edilme şekli,

- 9) Denetim makamının düzeltme yetkisi kapsamında alınan tedbirlerin ilgili kontrolör veya işleyiciye karşı aynı konu ile ilgili olarak daha önceden alınmış olduğu hallerde, bu tedbirlere uyum,
- 10) 40. madde uyarınca onaylı davranış kurallarına veya 42. madde uyarınca onaylı belgelendirme mekanizmalarına uygun hareket edilmesi,
- 11) İhlal nedeniyle doğrudan veya dolaylı olarak elde edilen maddi menfaatler veya kaçınılan zararlar gibi durumun özellikleri açısından geçerli diğer ağırlaştırıcı veya hafifletici faktörler.
- h) Verilerin transfer edileceği ülkede yeterli düzeyde koruma bulunmaması durumunda veri sahibinin verilerinin paylaşılmasına ilişkin rızası bulunsa da verilerin Birlik dışına aktarımı yasaklanmıştır. AB Veri Koruma Yönergesi'nde yeterli düzeyde koruma şartının denetimi veri sorumlusuna bırakılmışken GVKT ile bu değerlendirmeyi yapma yükümlülüğü veri koruma otoritesine bırakılmıştır.
- i) GVKT ile ilkdefa veri sahibine veri taşınabilirliği hakkı tanınmıştır. Veri taşınabilirliği hakkı, Tüzük ile sayılan hallerde veri sahibinin veri kontrolörüne sağlamış olduğu verilerini yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma ve kontrolörün engellemesi olmaksızın verilerini başka bir kontrolöre iletme hakkıdır. Bu haller şöyle sayılmıştır:
- 1) İşleme faaliyetinin; (i) veri sahibinin, kişisel verilerinin bir ya da daha fazla amaca yönelik olarak işlenmesine onay vermesi, (ii) veri sahibinin taraf olduğu bir sözleşmenin kurulması ya da uygulanması için gerekli olması, (iii) veri sahibinin, özel kategorilerdeki kişisel verilerinin bir veya daha fazla amaca yönelik olarak işlenmesine açık rıza göstermesi halinde gerçekleşmesi,
- 2) İşleme faaliyetinin otomatik yollarla gerçekleştirilmesi.
- j) Veri kontrolörü, veri sahibinin erişim hakkı ve profil çıkarma da dahil olmak üzere otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı ile ilgili bir talebe ilişkin bilgileri herhangi bir gecikmeye mahal vermeksizin ve her halükarda talebin alınmasından itibaren bir ay içerisinde veri sahibine sağlamakla yükümlüdür. Öngörülen bir aylık süre, gerekli durumlarda iki aya kadar uzatılabilir. Kontrolör, bir aylık süre içerisinde süre uzatımıyla birlikte

gecikme sebeplerini veri sahibine bildirir. Talebin elektronik yollarla yapması halinde, veri sahibi tarafından aksi belirtilmedikçe ve mümkün olması durumunda bilgilendirme, elektronik yollarla yapılır. Bilgilendirmeye ilişkin belirli bir sürenin öngörülmesi ile Üye Devletlerin farklı süre uygulamalarının önüne geçilmiştir.

k) Tüzüğe göre kişisel veri ihlali olması ve bu ihlalin veri sahibinin hak ve özgürlükleri açısından risk oluşturması halinde bu riskin kontrolör tarafında gecikmeye mahal vermeksizin ihlalden haberdar olduğu andan itibaren 72 saat içerisinde yetkili denetim makamına bildirilmesi gerekir. Ayrıca kontrolör, kişisel veri ihlalinin gecikmeksizin veri sahibine de iletilecektir. Aşağıda sayılan durumlarda veri sahibine bilgilendirme yapılmasının gerekli olmadığı öngörülmüştür:

- 1) Kontrolör tarafından uygun koruma tedbirlerinin uygulanması,
- 2) Kontrolörün, veri sahibinin hak ve özgürlükleri açısından riskin oluşmasını engelleyecek ek tedbirler alması,
- 3) Bildirimin, ölçüsüz bir çaba gerektirecek olması,
- l) Kontrolör, özellikle yeni teknolojik veri işleme yöntemleri kullanıldığında ve veri işleme faaliyetinin kapsamı, bağlamı, amacı ve niteliği itibarıyla, gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riskin içermesinin muhtemel olduğu durumlarda, işleme faaliyetinden önce, veri koruma etki değerlendirmesi yapacaktır,
- m) Kontrolör, tasarımdan itibaren verilerin korumasına ve gizliliğinin sağlanmasına yönelik tedbirleri almakla yükümlüdür,
- n) Veri silinmesi olarak da bilinen unutulma hakkı: veri sahibinin, verilerinin gecikmeksizin silinmesini talep etme hakkıdır.

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNDA TÜRKİYE MEVZUATI

Hukukumuzda, kişisel veriler ilk defa 6 Şubat 2004 tarihinde 25365 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren “Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik” ile koruma altına alınmıştır¹⁶². Yönetmeliğin ardından 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu’nun 135 ve devamı maddeleri ile kanun düzeyinde koruma sağlanmıştır. Ancak TCK ile kişisel verilere ilişkin temel kavramlara açıklık getirilmemesi ve bu alanda özel bir kanunun bulunmayışı uygulamada tereddütlerin yaşanmasına sebep olmuştur¹⁶³.

2010 yılı Anayasa değişikliğine kadar kişisel verilerin korunması hakkı Anayasa ile koruma altına alınan temel hak ve özgürlüklerin içerisinde bağımsız bir hak olarak yer almamaktadır. Ancak Anayasa’da yer alan, kişinin maddi ve manevi varlığını geliştirme hakkı, özel hayatın gizliliği ve korunması hakkı, haberleşme hürriyeti düşünce ve kanaat hürriyeti, din ve vicdan hürriyeti gibi pek çok temel hak ve özgürlüklerle ilişkilendirilebilmesi sebebiyle Anayasal temelli bir hak olduğunu söylemek mümkündür.

2010 yılı değişikliği ile Anayasa’nın 20. maddesine eklenen “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.” hüküm ile kişisel verilerin korunması hakkı, bağımsız bir hak olarak Anayasa güvenceye kavuşmuştur. Akabinde 7 Nisan 2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun yürürlüğe girmesi bu alanda Avrupa Hukukuna paralel pek çok yasal düzenlemenin önünü açmıştır. Bu

¹⁶² Taştan, s. 23; Yönetmelik 24 Temmuz 2012 tarih ve 28363 sayılı Resmi Gazete ’de yayımlanan “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik” ile yürürlükten kaldırılmıştır.

¹⁶³ Kişisel Verilerin Korunması Kanunu Genel Gerekçe, s. 5; TCK’nın gerekçesinde kişisel veri, “gerçek kişiyle ilgili her türlü bilgi, kişisel veri kabul edilmelidir”denilerek bu konudaki belirsizlik giderilmeye çalışılmışsa da tek başına yeterli olmamıştır.

düzenlemelerin hepsine değinmek mümkün olmasa da çalışmamızın bu bölümünde kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ile ceza hukuku ve medeni hukuk kapsamında korunmasına ilişkin başlıca düzenlemeler aktarılmaya çalışılacaktır.

I. 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU

A. Kanunun Gerekçesi, Amacı ve Kapsamı

1. Kanunun Gerekçesi

Sosyal ve ekonomik hayatın devamı, kamu hizmetlerinin etkin biçimde sunumu için kişisel verilerin işlenmesi kaçınılmaz olmakla birlikte bu verilerin sınırsız biçimde toplanması, yetkisiz kişiler tarafından elde edilmesi, kullanılması ve ifşa edilmesi taraf olduğumuz sözleşmeler ve Anayasa ile koruma altına alınan temel hakların ihlalinin beraberinde getirmiştir. Bu iki menfaat arasındaki dengenin oluşması, özel bir kanun ve etkin bir denetim mekanizmasının bulunmaması sebebiyle toplumda oluşan olumsuz algının ortadan kaldırılabilmesi için kişisel veriler üzerinde gerçekleştirilecek faaliyetlere ilişkin temel ilkelerin belirlenmesi ihtiyacı doğmuştur.

6698 sayılı Kanun'un gerekçesinde kişisel verilerin korunmasını sağlayacak özel bir kanunun yürürlüğe girmesinin sebepleri şöyle sıralanmıştır:

- a) Türk Ceza Kanununun 135 ve devamı maddelerinde, kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiilleri suç olarak düzenlenmiş ve yaptırıma bağlanmışsa da kişisel verilerin korunmasına yönelik özel bir kanunun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı, ne zaman hukuka uygun olduğunun belirlenmesinde yaşanan tereddütler,
- b) Anayasanın 20.maddesinde yapılan düzenlemeyle konuya ilişkin usul ve esasları düzenleyecek bir yasa yapma gerekliliği,
- c) Avrupa Birliği tam üyelik sürecinde, müzakere fasıllarından dördünün doğrudan kişisel verilerle ilgili olması sebebiyle sürecin ilerleyebilmesi için temel bir kanunun yürürlüğe girmesinin gerekliliği,

- d) EUROPOL ve EUROJUST ile işbirliği ve elektronik bilgi değişimi yapılamaması,
- e) Sağlık kuruluşlarında tutulan özel nitelikli verilerin kanuni dayanaktan yoksun olması ve bu konuda Avrupa İnsan Hakları Mahkemesi tarafından verilen ihlal kararları,
- f) Türkiye’de yaşayan yabancılar ile yurtdışında yaşayan Türk vatandaşları bakımından askerlik, vatandaşlık, kimlik ve malvarlığı gibi konularda veri paylaşımında yaşanan sorunlar,
- g) Kişisel verilerin korunması konusunda kanun hazırlanmasının Katılım Ortaklığı Belgesine cevap olarak hazırladığı 2003 Ulusal Programında taahhüt edilmiş olması,
- h) 64. Hükümet 2016 yılı Eylem Planında üç ay içerisinde gerçekleştirilecek reformlar arasında kişisel verilerin korunmasına ilişkin kanuni düzenlemelerin hayata geçirileceğinin yer alması,
- i) Ekonomik alanda yaşanan sorunlar ve kayıplar,
- j) AvrupaKonseyitarafından, tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınırötesi veri akışı ilkelerinin belirlenmesi amacıyla 28 Ocak 1981 tarihinde imzaya açılan ve Türkiye Tarafından imzalanan Kişisel Verilerin Otomatik İşlemeTabiTutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme’nin 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazetede yayımlanarak iç hukuka dâhil edilmesi ile yasal düzenlemelerin yapılmasının gerekliliği,
- k) Başta 24 Ekim 1995 tarihinde “Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafığı Direktifi”nin yürürlüğe girmesi.

Görüldüğü üzere 6698 sayılı Kişisel Verilerin Korunması Kanunu ile uluslararası belgeler, karşılaştırmalı hukuk uygulamaları da dikkate alınarak kişisel verilerin çağdaş standartlarda işlenmesi ve koruma altına alınması amaçlanmıştır.

2. Kanunun Amacı

6698 sayılı Kişisel Verilerin Korunması Kanunu’nun amacı 1. maddede “kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel

hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek”olarak açıklanmıştır.Maddenin gerekçesinde ayrıca kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların belirlenmesi ve özel hayatın gizliliği hakkı ile bilgi güvenliği hakkının korunmasının da Kanun’un amaçlarından olduğu belirtilmiştir.

3. Kanunun Kapsamı

Kişisel Verilerin Korunması Kanunu’nun 2. maddesinde Kanun’un “kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler” hakkında uygulanacağı belirtilmiştir. Gerekçede de belirtildiği üzere Kanunun uygulanması bakımından kamu ve özel sektör ayrımı yapılmadığı gibi verilerin otomatik olarak ya da herhangi bir veri kayıt sisteminin parçası olmak kaydı ile otomatik olmayan yollarla işlenmiş olması da uygulanabilirliği yönünden herhangi bir fark bulunmamaktadır.

Kanun ile sadece gerçek kişilere ait veriler koruma altına alınmıştır. Ancak daha önce de belirttiğimiz üzere tüzel kişiye ait veriler bir gerçek kişi ile ilişkilendirilebiliyorsa bu verilerde kişisel verilerin korunması hakkı kapsamında korunmalıdır¹⁶⁴.

B. Temel Kavramlar

1. Kişisel Veri ve Kişisel Verilerin İşlenmesi

a. Kişisel Veri

6698 sayılı Kişisel Verilerin Korunması Kanunu’nda uluslararası düzenlemelere paralel şekilde kişisel veri, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlamıştır. Kanun’un gerekçesinde de

¹⁶⁴ Dülger, s. 10; Şimşek, s. 123.

açıklandığı üzere kişinin sadece “adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgileri” değil aynı zamanda “fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgileri, isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgileri” de kişisel verileridir. Eldeki verinin, kişisel veri olarak kabul edilebilmesi için daha önce detaylı olarak incelediğimiz (i) bilgi, (ii) kimliği belirli veya belirlenebilir bir gerçek kişi ve (iii) ilişkin olma unsurlarının tamamını barındırması gerekmektedir.

AB Veri Koruma Yönergesi’nin 2. maddesinde kişisel veri, “bir gerçek kişi hakkındaki olabilecek ve onu belirlenebilir kılacak her türlü bilgi” tanımlanmıştır¹⁶⁵. Yönerge’de, Kişisel Verilerin Korunması Kanunu’ndan farklı olarak “belirlenebilir” kavramına da açıklık getirilmiştir. Buna göre belirlenebilirlik; doğrudan veya dolaylı olarak özellikle bir kimlik numarası veya kişinin fiziksel, psikolojik, ruhsal, ekonomik, kültürel veya sosyal kimliğine bir veya birden fazla spesifik faktör ile ilişkilendirilebilmesi suretiyle kişinin belirlenebilir hale gelmesini sağlayan tüm haller olarak açıklanmıştır¹⁶⁶. Genel Veri Koruma Tüzüğü’nde ise Yönerge ile benzer ancak daha kapsamlı bir şekilde kişisel veri, “belirli veya belirlenebilen kişiye (‘ilgili kişi’) ilişkin her türlü bilgi anlamına gelir; belirlenebilir gerçek kişi, bir tanımlayıcıya, örneğin ismine, kimlik numarasına, konum bilgisine, bir çevrimiçi tanımlayıcıya ya da bu kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine ilişkin bir veya birden fazla etkene referans yaparak doğrudan veya dolaylı olarak belirlenebilen kişidir” olarak tanımlanmıştır¹⁶⁷.

Görüldüğü gibi konu ile ilgili uluslararası düzenlemelerde ve Kişisel Verilerin Korunması Kanunu’nda kişisel verilere ilişkin sınırlı sayım yoluna gidilmemiştir. Bu sebeple hangi verinin kişisel veri olarak kabul edileceği somut olayın özelliğine göre değerlendirme yapılarak belirlenecektir.

¹⁶⁵ Başalp, s. 33.

¹⁶⁶ Küzeci, s. 315; Başalp, s. 33.

¹⁶⁷ Develioğlu, s. 175.

b. Kişisel Verinin İşlenmesi

Kişisel verilerin işlenmesi 6698 sayılı Kanunda “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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”olarak tanımlanmıştır. Verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlem türleri bu kapsamda değerlendirilecektir (Kişisel Verilerin Korunması Kanunu Madde Gerekçeleri). Kanunun gerekçesinde de açıklandığı üzere verilerin işlenmesine yönelik işlem türlerine ilişkin yapılan bu sayım örnekleyici bir sayımdır. Sayılı işlem türlerine benzer tüm işlemler kişisel verilerin işlenmesi olarak kabul edilecektir. KVKK ile veri işleme faaliyetinin özel sektör ya da kamu sektörü tarafından gerçekleştirilmesi bakımından bir ayrım da yapılmamıştır.

Kanun, tamamen otomatik veya kısmen otomatik yollarla kişisel verilerin işlenmesini koruma altına almıştır. Verilerin otomatik olarak işlenmesi, kişisel verilerin işlenmesi sırasında bilgisayar ve benzeri bilişim sisteminin kullanılmasıdır¹⁶⁸. Herhangi bir bilişim sistemi dâhil edilmeden elle gerçekleştirilen işlemler ise otomatik olmayan yolları ifade etmektedir. Verilerin otomatik olmayan yollarla işlenmesi Kanun kapsamına alınmamıştır. Otomatik olmayan yollarla yapılacak veri işleminin Kanun kapsamında değerlendirilemeyeceği konusunda yaşanacak bir tereddütte, veri işlenmesinde bir veri kayıt sisteminin var olup olmadığını değerlendirmek yeterli olacaktır. Veri kayıt sistemi, Kanunda “kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi” olarak tanımlanmıştır. Veri kayıt sisteminin elektronik ve ya fiziki ortamda oluşturulması önem arz etmemekte; verilerin belirli kriterlere göre örneğin; ad, soyad veya kimlik numarasına göre ya da kredi borcunu ödeyip ödemediğine göre sınıflandırılarak bir kayıt sisteminin oluşturulması yeterlidir(Kişisel Verilerin Korunması Kanunu Madde Gerekçeleri).Verilerin sınırlı insan müdahalesinin olduğu bir veri kayıt sisteminin parçası olacak şekilde işlendiği durumlar Kanun kapsamında sayılmıştır. Bu

¹⁶⁸ Başalp, s. 30.

bağlamda avukatlık bürolarında avukatların özlük dosyalarının işveren avukatın bilgisayarına işlenmesi otomatik olan yollarla işleme sayılırken; hastanede elle tutulan doğum defteri yeni doğanların doğum tarihi, saati, kilosu, boyu gibi kriterlere göre bir sınıflandırılarak bir veri kayıt sistemine dâhil edildiğinden otomatik olmayan yollarla işleme sayılsa da bir veri kayıt sisteminin içerisine dâhil edildiğinden Kanun kapsamındadır¹⁶⁹.

GVKT ile de veriler üzerinde gerçekleştirilen işlemler sınırlı olarak sayılmamış ve kişisel verilerin işlenmesi “otomatik vasıtalarla olsun veya olmasın, kişisel veriler veya kişisel veri setleri üzerinde elde etme, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, erişme, başvurma, kullanma, yayınlamak, yaymak veya diğer şekilde ulaştırılabilir hale getirmek suretiyle ifşa etme, sıralama veya birleştirme, sınırlama, silme veya imha etme gibi faaliyet veya faaliyet setleri”olarak tanımlanmıştır¹⁷⁰. AB Veri KorumaYönergesi’nde olduğu gibi GVKT de kişisel veriler üzerinde gerçekleştirilen her türlü otomatik işlem halinde uygulanacaktır. Kişisel verilerin otomatik olmayan yollarla işlenmesi halinde ancak bir sınıflandırma yapılarak erişimin kolaylaşması sağlanmış ise Tüzük kapsamında sayılacaktır¹⁷¹. Bu bakımdan hem 6698 sayılı Kişisel Verilerin Korunması Kanunu hem de AB Veri Koruma Yönergesi ve Genel Veri Koruma Tüzüğü birbiri ile uyumlu düzenlemeler içermektedir.

2. Açık Rıza

6698 sayılı Kanunda açık rıza AB Yönergesi ile uyumlu olarak “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza” olarak tanımlanmıştır. Kanunun gerekçesinde de açıklandığı üzere açık rıza “açık rıza ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı” olarak anlaşılmalıdır. Kanun gereğince kişisel veriler ve özel nitelikli kişisel veriler açık rıza olmaksızın işlenemeyecek ve aktarılamayacaktır.

¹⁶⁹ Taştan, s. 47.

¹⁷⁰ Develioğlu, s. 176.

¹⁷¹ Başalp, s. 33.

İlgili kişinin açık rızası, verilerin işlenmesine meşruluk katar¹⁷². GVKT ile ilgili kişiye istediği zaman rızasını geri çekme hakkı tanınmıştır (m.7). İlgili kişi söz konusu işleme rıza göstermeden önce rızasını geri çekme hakkı olduğu konusunda bilgilendirilmelidir. Rızanın geri çekilmesi, rızaya dayalı olarak gerçekleştirilen işlemlerin hukuka uygunluğunu etkilemeyecektir.

KVKK'nın temel aldığı AB Yönergesinde rıza; özgürce ve bilgilendirme yapıldıktan sonra kendisine dair kişisel verilerin işlenmesi için kabul ettiğini gösterir işaret olarak tanımlanmıştır. GVKT ile rıza daha kapsamlı olarak düzenlenmiştir. Buna göre rıza “bir beyan veya olumlayıcı eylem şeklinde kendisiyle ilgili kişisel verilerin işlenmesine mutabık kaldığını ortaya koyan, ilgili kişinin isteklerinin özgürce verilmiş, konuya özel, bilgilendirilmiş ve belirsizlik içermeyen bir göstergesi anlamına gelir”¹⁷³. Hem Kanun hem de GVTK ve AB Yönergesinde geçerli bir rıza beyanında aşağıda sayılan unsurların birlikte var olması gerekmektedir (GVKT m. 7):¹⁷⁴

- a) Rıza beyanı, tereddüte yer bırakmayacak şekilde kesin ve açık olmalıdır. İlgili kişi verileri üzerinde gerçekleştirilecek faaliyetlere açık ve kesin bir irade açıklaması ile rıza gösterebilir. Rıza yazılı veya sözlü olarak açıklayabileceği gibi davranış biçimleri ile de gösterebilir. Önemli olan rıza beyanı konusunda tereddüttün yaşanmamasıdır.
- b) İlgili kişi özgür iradesi ile rıza göstermelidir. İlgili kişinin özgür iradesini sakatlayan hata, hile ve ikrah dışında ilgili kişinin karşı tarafa karşı güçsüz, bağımlı olduğu durumlarda da özgür iradesinin olup olmadığı irdelenmelidir. Örneğin, işçi- işveren ilişkisinde işverenin işçinin kişisel verileri üzerindeki faaliyetlerinde işçinin özgür iradesi çoğu zaman mümkün olmayacaktır. İşçinin işini kaybetme korkusu yüzünden rıza göstermesi mümkündür. Bu sebeple işçi- işveren ilişkisinde olduğu gibi güçsüz olan tarafa bazı ek güvencelerin sağlanması gereklidir. Ayrıca bir hizmetin sağlanması da dâhil olmak üzere bir sözleşmenin ifasının söz konusu sözleşmenin ifası için gerekmeyen kişisel verilerin işlenmesine yönelik bir rızaya bağlanması durumunda azami özen gösterilmelidir.

¹⁷² Korkmaz, s. 96 (Değerlendirme); Şimşek, s. 106; Kuşkonmaz s.101, Küzeci, s. 231.

¹⁷³ Develioğlu, s. 177.

¹⁷⁴ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 343.

- c) İlgili kişinin kişisel verileri üzerinde gerçekleştirilecek faaliyetler konusunda bilgilendirilmesi gerekir. Aydınlatma yükümlüğü kapsamında ilgili kişinin hangi verileri üzerinde hangi faaliyetlerin kimler tarafından gerçekleştirileceği ve hatta verileri üzerinde ileride gerçekleşmesi muhtemel faaliyetler konusunda kapsamlı bir şekilde aydınlatılması ve bunun sonucunda rızasının alınmış olması gerekir. Veri sorumlusu rıza talebini diğer hususlardan açık bir şekilde ayırt edilebilecek bir şekilde, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanılarak sunulmalıdır.
- d) İlgili kişinin vermiş olduğu rıza somut olaya ilişkin olmalıdır. İlgili kişinin her türlü veri işleme faaliyetine rıza göstermesi geçerli bir rıza olmayacaktır.

AB Veri Koruma Yönergesinde sadece hassas verilerin işlenmesi bakımından açık rıza koşulu aranırken Tüzük ile hassas veri ayrımı yapılmaksızın kişisel verilerin işlenmesi bakımından açık rıza aranmaktadır.

3. Anonim Hale Getirme

6698 sayılı Kanunda anonim hale getirme “kişisel verilerin, başka verilerle eşleştirerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi”olarak tanımlanmıştır. Kişisel verilerin anonim hale getirilmesine ilişkin usul ve esaslar 28.10.2017 tarihli “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik” ile düzenleme altına alınmıştır. Yönetmeliğe göre kişisel verilerin anonim hale getirilmesi için; kişisel verinin veri sorumlusu, alıcı ya da alıcı grupları tarafından geri döndürülmesi ve kişisel verinin başka verilerle eşleştirilmesi yoluyla dahi kimliği belirli veya belirlenebilir kişinin bir gerçek kişi ile ilişkilendirilemez hale getirilmesi gerekir (m.10). Kişisel verilerin anonim hale getirilmesi de bir imha işlemi olduğundan veri uygun teknik ve yöntemler ile anonim hale getirildiği andan itibaren kişisel veri olmaktan çıkacaktır.

4. Veri Kayıt Sistemi

Veri kayıt sistemi Kanunda “kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi” olarak tanımlanmıştır. Veri kayıt sisteminden söz edebilmek için verilerin belirli kriterlere göre örneğin; ad, soyad veya kimlik numarasına göre ya da kredi borcunu ödeyip ödemediğine göre sınıflandırılarak bir kayıt sisteminin oluşturulması yeterli olup; sistemin elektronik ve ya fiziki ortamda oluşturulması önem arz etmemektedir (Kişisel Verilerin Korunması Kanunu Madde Gerekçeleri).

Genel Veri Koruma Tüzüğü’nde veri kayıt sistemi “dosyalama sistemi” olarak adlandırılmış ve “işlevsel veya coğrafi bir temelde merkezi, ademi-merkezi veya dağınık olarak spesifik kriterlere göre erişilebilen yapılandırılmış herhangi bir kişisel veri dizisi” olarak tanımlanmıştır (m.4). Kişisel verilerin 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 işlem hem KVKK hem de GVKT kapsamındadır.

5. Veri Sorumlusu ve Veri İşleyen

6698 sayılı Kişisel Verilerin Korunması Kanunu’nda veri sorumlusu, “kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi” olarak tanımlanmıştır. Veri sorumlusu gerçek kişi olabileceği gibi, kamu kurumları, şirketler, dernekler veya vakıflar gibi tüzel kişi de olabilir. Kişisel verileri işleme konusundaki yükümlülükler ve yaptırımlar bakımından tüzel kişiler de gerçek kişiler gibi sorumlu olacaktır¹⁷⁵. Veri sorumlusunun kim olduğuna ilişkin yaşanan bir tereddütte; kişisel verilerin işlenmesi ve işlenme amacı, işlenecek kişisel veri türleri, işlenen kişisel verilerin hangi amaçlarla kullanılacağı, hangi kişilerin kişisel

¹⁷⁵ “Örneğin inşaat alanında faaliyet gösteren bir anonim şirket uhdesinde tutulan kişisel veriler bakımından veri sorumlusu, söz konusu şirkettir.” Taştan, s. 70.

verilerinin işleneceği, kişisel verilerin paylaşılıp paylaşılmayacağı, paylaşılacaksa kimlerle paylaşılacağı, ne kadar süreyle saklanacağı, ilgili kişilerin erişim hakkı ve diğer haklarının uygulanıp uygulanmayacağı gibi hususlara kimin karar verdiği dikkate alınarak veri sorumlusu tespit edilebilecektir¹⁷⁶.

Genel Veri Koruma Tüzüğü'nde veri sorumlusu, "kişisel verilerin işlenmesinin amaçlarını ve vasıtalarını tek başına veya başkalarıyla birlikte belirleyen gerçek veya tüzel kişi, kamu kurumu veya diğer bir kamu kuruluşu" olarak tanımlanmıştır¹⁷⁷. Buna göre veri sorumlusu, işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, işleme faaliyetinin Tüzük uyarınca gerçekleştirilmesini sağlamak ve bu şekilde gerçekleştirildiğini gösterebilmek için uygun teknik ve düzenlemeye ilişkin tedbirler uygulamak, tedbirler gözden geçirmek ve gerektiğinde güncellemekle yükümlüdür (GVKT m. 24)¹⁷⁸.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nda veri işleyen, "veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" olarak tanımlanmıştır. Herhangi bir gerçek veya tüzel kişinin hem veri sorumlusu hem de veri işleyen olabilmesi mümkündür¹⁷⁹. Veri işleyen, veri sorumlusunun çalışanı olabileceği gibi veri sorumlusunun hizmet satın almak suretiyle belirlediği ayrı bir gerçek veya tüzel kişi de olabilir¹⁸⁰.

Veri sorumlusunun veri işleyen kişiyle yapacağı bir sözleşmeyle; kişisel verilerin toplanması için kullanılacak bilgi teknoloji sistemleri ile metotların belirlenmesi, kişisel verilerin hangi yöntemle saklanacağı veya aktarılacağı, verilerin korunmasına yönelik alınacak güvenlik önlemlerinin detayları, kişisel verilerin saklanmasına ilişkin sürelerin doğru uygulanabilmesi için kullanılacak metot, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesine ilişkin yöntemler gibi

¹⁷⁶ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununu Hakkında Sıkça Sorulan Sorular, s. 3; Dülger, s. 21.

¹⁷⁷ Develioğlu, s. 176.

¹⁷⁸ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 355.

¹⁷⁹ Örneğin, bir muhasebe şirketi, kendi personeliyle ilgili tuttuğu verilere ilişkin olarak veri sorumlusu; müşterisi olan şirketlerle ilgili tuttuğu verilere ilişkin olarak veri işleyen olarak kabul edilecektir. Kişisel Verilerin Korunması Kanunu Madde Gerekçeleri, s. 7.

¹⁸⁰ Veri işleyenin, veri sorumlusunun çalışanı olması halinde, ilgili kişiler veri sorumlusuna karşı Türk Borçlar Kanunu'nun 66. maddesi gereğince adam çalıştıranın sorumluluğu kapsamında da başvurma imkânına sahip olacaktır. Taştan, s. 72.

hususlarda karar alma yetkisini veri işleyene bırakması mümkündür¹⁸¹. Ancak böyle bir durumda da veri sorumlusunun yasal yükümlülükleri devam etmektedir¹⁸².

C. Kişisel Verilerin İşlenmesine İlişkin Genel İlkeler

Kişisel verilerin korunması hukukunun ulusal ve uluslararası tüm kaynaklarında kişisel veriler üzerinde gerçekleştirilen her türlü faaliyete ilişkin temel ilkeler belirlenmiştir. Ulusal mevzuatımız bakımından kişisel veriler ancak Kişisel Verilerin Korunması Kanunu'ndave diğer kanunlarda öngörülen usul ve esaslar çerçevesinde işlenebilecektir. Bu konu çalışmamızın üçüncü bölümünde ele alındığından tekrara düşmemek adına sadece temel ilkelere değinilmekle yetinilecektir.

Kanun'un 4. maddesinde kişisel verilerin işlenmesi sırasında uyulması gereken zorunlu temel ilkeler şöyle sıralanmıştır:

- a) Hukuka ve dürüstlük kurallarına uygun olma,
- b) Doğru ve gerektiğinde güncel olma,
- c) Belirli, açık ve meşru amaçlar için işlenme,
- d) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
- e) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Söz konusu ilkeler Kişisel Verileri Koruma Kurul'u kararlarına da konu olmuştur. Kişisel Verileri Koruma Kurulu'nun önüne gelen karara konu olayda¹⁸³ veri sorumlusu, ilgili kişi olan müşterisinin talebi üzerine gerçekleştirdiği işlemde, müşterisinden işlemin gerçekleşmesi için gerekli olmayan kişisel verileri içeren bir belge istemiştir. Kurul, bu belgenin istenilmesinin ilgili mevzuatta yer almaması ve ulaşılmak istenen amaç ile bağdaşmaması sebebiyle; veri sorumlusunun bu talebinin, Kanunun 4. Maddesinde yer alan hukuka ve dürüstlük kurallarına uygun olma ve belirli, açık ve meşru amaçlar için işleme ilkesine aykırılık teşkil ettiğine karar vermiştir. Kişisel veri güvenliğini sağlamaya yönelik gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında Kanunun 18. maddesi uyarınca idari yaptırım

¹⁸¹ Kişisel Verileri Koruma Kurumu, Veri Sorumlusu ve Veri İşleyen, s. 3.

¹⁸² Dülger, s. 21; Kişisel veri işleme sözleşmesi ile ilgili açıklamalar için bkz. Taştan, s. 118.

¹⁸³ www.kvkk.gov.tr; Dülger, s. 212.

uygulanması öngörülmüştür. Kurul bir başka kararında¹⁸⁴ tabi olduğu mevzuat uyarınca işlediği kişisel verileri 10 yıl boyunca muhafaza etmesi zorunluluğu bulunduğundan veri sorumlusunun, hâlihazırda aktif olmayan müşterisi olan ilgili kişinin kişisel verilerinin silinmesi hususundan talebini yerine getirmemesi üzerine aktif olmayan müşterilerin kişisel verilerinin, Kanunun 4 üncü maddesinde yer verilen genel ilkelere uygun olarak saklama amacı dışında işlenmemesi gerektiği yönünde veri sorumlusunun talimatlandırılmasına karar vermiştir.

Kurul tarafından verilen en çarpıcı karar, kişisel verilerin mahkemelere dahi gereğinden fazla aktarılmasının veri minimizasyonu ilkesine aykırılık teşkil etmesidir. Kurul, önüne gelen olayda¹⁸⁵ mahkemenin, veri sorumlusundan, ilgili kişi hakkında bazı kişisel verilerin talep edilmesi üzerine veri sorumlusunun gereğinden fazla kişisel veri aktarımında bulunmasını Kanunun 4 üncü maddesinde yer alan işlendikleri, amaçla bağlantılı, sınırlı ve ölçülü olma ilkesinin ihlali olarak kabul etmiştir. Kurul, kişisel verilerin güvenliğini sağlayamayan veri sorumlusu hakkında Kanunun 18. maddesi uyarınca idari yaptırım uygulanmasına karar vermiştir.

Konunun hassasiyeti sebebiyle veri sorumlusunun sorumluluğunun doğmaması için kişisel veriler üzerinde gerçekleştirdiği her türlü faaliyette öncelikle temel ilkelere dikkat etmesi gerekmektedir.

D. Kişisel Verilerin İşlenme Şartları

Kanun ile kişisel verilerin işlenmesi için bazı şartlar öngörülmüştür. Kanun ile sayılan şartların gerçekleşmesi halinde kişisel verilerin işlenmesi hukuka uygun hale gelmektedir¹⁸⁶. Kişisel verilerin işlenme şartları bakımından ikili ayrıma gidilerek özel nitelikli kişisel verilerin işlenmesi uluslararası düzenlemelere paralel şekilde daha farklı şartlara bağlanmıştır.

¹⁸⁴ www.kvkk.gov.tr; Dülger, s. 213.

¹⁸⁵ www.kvkk.gov.tr; Dülger, s. 212.

¹⁸⁶ Dülger, s. 214.

1. Genel Olarak Kişisel Verilerin İşlenme Şartları

Kanun'un 5. maddesinde kişisel verilerin işlenme şartları düzenlenmiştir. Buna göre kural olarak kişisel verilerin ilgili kişinin açık rızası bulunmaksızın işlenmesi yasaktır. Ancak Kanunda öngörülen istisnai hallerde ilgili kişinin açık rızası olmaksızın işlenebilmesi mümkündür.

Kanunun gerekçesinde ilgili kişinin açık rızası ile ilgili AB Veri Koruma Yönergesi'ne atıf yapılarak; rıza, ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı olarak açıklanmıştır. Doktrinde ilgili kişinin rızası konusunda farklı görüşler bulunmaktadır. Bu görüşlerden ilki, ilgili kişi kişisel verilerinin işlenmesine rıza göstererek, kişisel verilerin korunmasını hakkını bizzat kullanmaktadır¹⁸⁷. İkinci görüşe göre ise, ilgili kişi kişisel verilerinin işlenmesine rıza göstererek kişisel verilerinin korunması hakkından vazgeçmektedir. Biz bu görüşlerden ilkinde katılmaktayız. Birey, kişisel verilerinin işlenmesine rıza göstermesi ile verilerinin korunması hakkından vazgeçmemektedir¹⁸⁸. Bireyin verdiği rıza sadece o işlemle sınırlı olarak verilmiş bir rızadır. Veri sorumlusu işlediği verileri amacına ulaşması için kullanacak ve daha sonra bu verileri silecek veya anonim hale getirecektir. Her ne kadar ilgili kişinin verileri rızası işlenmişse de veri koruması devam edecektir.

İlgili kişinin rızası aranmaksızın kişisel verilerinin işlenmesinin mümkün olduğu haller Kanun'da sınırlı olarak sayılmıştır. Bu haller;

- a) Kanunlarda açıkça öngörülmesi,
- b) 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,
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- d) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

¹⁸⁷ Şimşek, s. 108 dn 508'deki yazarlar; Korkmaz, s. 96 (Değerlendirme).

¹⁸⁸ Şimşek, s. 108 dn 509'daki yazarlar.

- e) İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- g) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Kişisel verilerin işlenmesi Genel Veri Koruma Tüzüğü'nün 6. Maddesinde benzer şartlara bağlanmıştır. Buna göre sayılan durumlardan en az birinin geçerli olması halinde veri işleme faaliyeti hukuka uygun olacaktır.

2. Özel Nitelikli Kişisel Verilerin İşlenme Şartları

Kişisel verilerin korunmasına ilişkin ulusal ve uluslararası mevzuatta bazı verilerin hukuka aykırı olarak işlenmesi halinde ilgili kişinin temel hak ve özgürlüklerinin daha fazla zarar görme tehlikesi sebebiyle bazı kişisel veriler “hassas veri”, “özel nitelikli veri”, “özel koruma gerektiren veri”¹⁸⁹ olarak kabul edilmiş ve daha sıkı koruma altına alınmıştır. 6698 sayılı Kanun’a göre “ kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri”özel nitelikli kişisel veridir. Özel nitelikli veriler sınırlı olarak sayılmış olup genişletilmesi mümkün değildir. GVKT ile de bireyin “ırk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile biyometrik verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verileri” özel nitelikli kişisel verileri olarak sayılmıştır.

Kanun’un 6. maddesinin 3. fıkrasına özel nitelikli kişisel verilerin işlenme yasağının istisnaları bir bakıma hukuka uygunluk sebepleri sıralanmıştır. Özel nitelikli verilerin başkaları tarafından öğrenilmesi durumunda ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte olmaları nedeniyle işlenmeleri öncelikle ilgilinin açık rızasına bağlıdır (Kişisel Verilerin Korunması Kanunu Madde Gereçekleri). Açık rızaya ilişkin daha önce

¹⁸⁹ Aksoy, s. 30.

yapmış olduğumuz açıklamalar özel nitelikli kişisel verilerin işlenmesi bakımından da geçerlidir.

Özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenebileceği haller şöyledir:

- a) Sağlık ve cinsel veriler dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir.
- b) Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel veriler ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

Sağlık ve cinsel hayata ilişkin kişisel veriler ayrı olarak düzenlenmiş ve ancak sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlarca işlenebileceği öngörülmüştür. Kanun’da ayrıca özel nitelikli kişisel verilerin işlenmesinde Kurul tarafından belirlenen yeterli önlemlerin alınması şartına da yer verilmiştir.

E. Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi

6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili diğer kanun hükümlerine uygun olarak işlenmesine rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler, resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinecek, yok edilecek veya anonim hale getirilecektir (KVKK m. 7). Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesine ilişkin usul ve esaslar 28.10.2017 tarihli “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik” ile düzenleme altına alınmıştır.

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesidir (Yönetmelik m.8). Buna göre veriler, kayıtlı oldukları evrak, dosya, CD, disket, hard disk gibi araçlardan geri dönüştürülemeyecek şekilde imha edilecektir (Kişisel Verilerin Korunması Kanunu Madde Gerekçeleri). Anayasa’nın özel hayatın gizliliğini düzenleyen 20. maddesinin

3. fıkrasında bireyin, kişisel verilerinin korunmasını isteme hakkının bir parçası olarak kişisel verilerinin silinmesini isteme hakkına da sahip olduğunu düzenlemektedir.

Kişisel verilerin yok edilmesi ise; kişisel verilerin, ilgili kullanıcılar dâhil hiç kimse tarafından, hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir (Yönetmelik m. 10). Yok edilme işlemi gereğince verilerin kaydedildiği evrak, dosya, CD, disket, hard disk gibi veri saklamaya elverişli materyallerin imha edilmesi gerekmektedir. Verileri yok etmeme, Türk Ceza Kanunu'nun 138. maddesinde suç olarak düzenlenerek yaptırıma bağlanmıştır.

Son olarak anonim hale getirme daha önce açıkladığımız üzere kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Anonimleştirme sürecinde yapılan işlemlerle belirlenebilir bir kişi ile verinin arasındaki bağ kopartılarak kişinin kimliği tespit edilemez hale geldiğinden, anonim hale getirilen veriler kişisel veri olmaktan çıkacaktır.

Kişisel Verilerin Korunması Kanunu 7. maddesinde verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklı tutulmuştur. Kanun'un gerekçesinde verilen örnekte olduğu gibi Adli Sicil Kanunu'nda verilerin silinmesini veya yok edilmesini düzenleyen hükümler 6698 sayılı Kanun'a göre öncelikli olarak uygulanacaktır.

Kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin resen silinmesi, yok edilmesi veya anonim hale getirmesine ilişkin süreler ile ilgili kişinin talep etmesi durumunda silme ve yok etme süreleri birbirinden farklıdır. Buna göre:

- a) Kişisel verilerin resen silinmesi, yok edilmesi veya anonim hale getirmesine ilişkin süreler Yönetmeliğin 11. maddesinde düzenlenmiştir. Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması halinde belirlenen süreleri kısaltabilir. Veri sorumlusu tarafından kişisel veri saklama ve imha politikası hazırlamış olma yükümlülüğüne göre yapılan ayırimda:
 - 1) Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri silmek, yok

etmek veya anonim hale getirmekle yükümlüdür. Periyodik imhanın gerçekleştirileceği zaman aralığı, veri sorumlusu tarafından kişisel veri saklama ve imha politikası ile belirlenecektir. Her halde bu süre altı ayı geçemez.

- 2) Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu ise, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri silmek, yok etmek veya anonim hale getirmekle yükümlüdür.
- b) İlgili kişinin kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirmesi için veri sorumlusuna başvurması halinde veri sorumlusunun ilgili kişinin talebini yerine getirmesi için öngörülen süreler Yönetmeliğin 12. maddesinde yer almaktadır. Kişisel verileri işleme şartlarının tamamı ortadan kalkıp kalkmadığına göre yapılan ayırmada:
 - 1) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir. Ayrıca talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirmek ve üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin etmekle yükümlüdür.
 - 2) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, veri sorumlusunca ilgili kişinin talebi gerekçesi açıklanarak reddedilebilir. Ret cevabının en geç otuz gün içinde ilgili kişiye yazılı olarak ya da elektronik ortamda bildirilmesi gerekir.

F. Kişisel Verilerin Aktarılması

Kişisel verilerin aktarılması yani her türlü el değiştirmesi esasen kişisel verilerin işlenme türlerindendir¹⁹⁰. Kural olarak kişisel veriler ilgili kişinin rızası olmaksızın yurt içinde veya yurt dışına aktarılması yasaktır. Ancak ilgili kişinin açık rızası dışında bu yasağın bazı istisnaları bulunmaktadır. Kanun'un 8. maddesinde yer verilen istisnalar şöyledir:

¹⁹⁰ Küzeci, s. 354; Aygözer Öngün, s. 199.

- a) Kanun'un 5. maddesinin ikinci fıkrasında sayılan haller: (i) kanunlarda açıkça öngörülmesi, (ii) 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, (iii) bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, (iv) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, (v) ilgili kişinin kendisi tarafından alenileştirilmiş olması, (vi) bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, (vii) ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.
- b) Özel nitelikli kişisel veriler bakımından Kanun'un 6. maddesinin üçüncü fıkrasında sayılan haller: (i) kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf veya sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleri, biyometrik ve genetik verileri kanunlarda öngörülen hallerde, (ii) Sağlık ve cinsel hayata ilişkin veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası olmaksızın aktarılabilir.

Kişisel verilerin yurt dışına aktarılması da öncelikle ilgilinin açık rızasına bağlıdır. İlgilinin açık rızası aranmaksızın; (i) kişisel verilerin aktarılacağı yabancı ülkede yeterli korumanın bulunması, (ii) yeterli korunmanın bulunmaması halinde Türkiye'deki ve yabancı ülkedeki veri sorumluları tarafından yeterli korumanın yazılı olarak taahhüt edildiği ve Kişisel Verileri Koruma Kurulu'nun izninin bulunması kaydıyla Kanun'un 5. maddesinin ikinci fıkrasında ve 6. maddesinin üçüncü fıkrasında sayılan şartlardan birinin varlığı halinde kişisel verilerin yurt dışına aktarılması mümkündür (KVKK m. 9). Kurul, yabancı ülkede yeterli koruma bulunup bulunmadığına ve yeterli korumanın bulunmaması durumunda izin verilip verilmeyeceğine; (i) Türkiye'nin taraf olduğu uluslararası sözleşmeleri, (ii) kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık

durumunu, (iii) her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işleme amaç ve süresini, (iv) kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını, (v) kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verecektir.

Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda kişisel veriler, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir. Bu hükmün gerekçesi ise şöyle açıklanmıştır: “Kişisel verilerin yurt dışına aktarılması bazı durumlarda ülkemizin veya ilgili kişilerin menfaatlerine ciddi şekilde zarar verebilmektedir. Bu durumun engellenmesi amacıyla, ülkenin veya ilgili kişinin menfaatlerinin ciddi zarar göreceği durumlarda Dışişleri Bakanlığı ya da ilgili kamu kurum veya kuruluşlarının bu hususta görüşü alınarak kurulun izin vermesinden sonra verilerin yurt dışına aktarılması amaçlanmaktadır. Bununla birlikte, uluslararası sözleşme hükümleri saklı tutulmaktadır. Uluslararası sözleşme hükümleri bulunması hâlinde kişilerin menfaatlerinin ciddi şekilde zarar görmesi nazara alınmayacaktır”¹⁹¹.

Kanun'un 9. maddesinin son hükmünde diğer kanunlarda yer alan hükümler saklı tutulmuştur. Madde gerekçesinde 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun, uluslararası bilgi değişimi konusunda Malî Suçları Araştırma Kurulu Başkanına yetki veren 12. ve 19. maddeleri öncelikli olarak uygulanması örnek olarak gösterilmiştir.

Genel Veri Koruma Tüzüğü ile kişisel verilerin aktarımı iki şekilde mümkün kılınmıştır. İlki Avrupa Birliği Komisyonu'nun uygunluk kararı, ikincisi uygunluk kararı olmasa dahi Tüzükte öngörülen istisnai durumlardan birinin varlığı. Uygunluk kararı Avrupa Birliği Komisyonu'nun, aktarım yapılacak üçüncü ülke, ülke içerisindeki bir bölge veya sektörlerin veya uluslararası kuruluşun yeterli korumayı sağladığı yönündeki kararıdır (GVKT m. 45). Komisyon, koruma düzeyinin yeterliliğini değerlendirirken aşağıda sayılan hususları dikkate alacaktır: (i) hukukun üstünlüğü, insan haklarına ve temel özgürlüklere saygı, kamu güvenliği, savunması, ulusal güvenlik ve ceza hukuku ile kamu idarelerinin kişisel verilere erişimi

¹⁹¹ Küzeci, s. 356; TBMM Tutanak Dergisi, 26. Dönem 1. Yasama Yılı, 59. Birleşim, 8. Oturum, 22 Mart 2016, s. 66.

hakkındakiler de dâhil hem genel hem de sektöre özel ilgili mevzuat ile bu mevzuatın uygulamaya konuluşu, o ülkede veya uluslararası kuruluşta toplanan kişisel verilerin başka üçüncü ülkelere veya uluslararası kuruluşlara transit aktarımı da dâhil veri koruma kuralları, mesleki kurallar ve güvenlik önlemleri, içtihat hukukunun yanı sıra etkin ve uygulanabilir veri sahibi hakları ve kişisel verileri aktarılmakta olan veri sahipleri için etkin idari ve yargısal telafi imkânları, (ii) üçüncü ülkede ya da uluslararası kuruluşun tabi olduğu, yeterli uygulama yetkileri de dahil veri koruma kurallarına uyulmasını sağlama ve uygulama yetkisine sahip, veri sahiplerine haklarını kullanmakta yardımcı olma ve yol gösterme ve Üye Devletlerin denetçi makamları ile işbirliği yapma sorumluluklarına sahip bir veya birden fazla bağımsız denetçi makamının bulunması ve etkin bir şekilde işlemesi, (iii) özellikle kişisel verilerin korunmasına ilgili üçüncü ülke veya uluslararası kuruluşun üstlendiği uluslararası taahhütler veya hukuken bağlayıcı antlaşma veya belgelerden ya da çok taraflı ya da bölgesel sistemlere katılmasından kaynaklanan diğer yükümlülükler (GVKT m. 45/2)¹⁹².

Verilerin aktarımı konusunda Genel Veri Koruma Tüzüğü, AB Veri Koruma Yönergesi'ne oranla daha kapsamlı düzenlemeler içermektedir. Bunda AB Veri Koruma Yönergesinin yürürlüğe girmesinden bu yana veri koruma konusunda oluşan tecrübe ve teknolojinin gelişimi ile hukuka aykırı aktarımların artması etkili olmuştur.

Uygunluk kararı bulunmasa dahi verilerin üçüncü ülke veya kuruluşa aktarımının mümkün olduğu istisnai haller ise şunlardır: (i) veri sahibinin aktarımın riskleri konusunda bilgilendirilmesinden sonra alınana açık rızası, (ii) aktarımın bir sözleşmenin ifası ya da veri sahibinin talebi üzerine alınan sözleşme öncesi önlemlerin uygulanmaya konulabilmesi için gerekli olması, (iii) veri sahibinin menfaati için akdedilen bir sözleşmenin tamamlanabilmesi veya ifası için gerekli hallerde, (iv) kamu menfaatine ilişkin önemli sebepler için gerekli hallerde, (v) aktarımın yasal taleplerde bulunma, bunların uygulanması veya savunması için gerekli olması halinde, (vi) veri sahibinin fiziksel veya yasal olarak rıza verebilecek durumda olmadığı zamanlarda veri sahibinin veya diğer kişilerin hayati çıkarlarını korunmak için, (vii) Avrupa Birliği veya Üye Devlet hukukuna göre kamuya bilgi

¹⁹² Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 371; Develioğlu, s. 74.

verme amacıyla oluşturulan ve gerek kamu genelinin gerekse meşru çıkarı olduğunu gösterebilen herhangi bir kişinin danışabilmesi için açık tutulan bir sicilden yapılması durumudur(GVKT m. 49)¹⁹³.

G. Veri Sorumlusuna Başvuru, Kurula Şik yet ve Veri Sorumluları Sicili

1. Veri Sorumlusuna Başvuru

Kişisel Verilerin Korunması Kanunu'nun 13. maddesinde veri sorumlusuna başvuru yolunu düzenlemektedir. İlgili kişiler, Kanunun uygulanması ile ilgili taleplerini öncelikle veri sorumlusuna iletmek zorundadırlar. Kanun'un 14. maddesinde açıkça 13. madde uyarınca başvuru yolu tüketilmeden şikâyet yoluna başvurulamayacağı düzenlenmiştir. İlgili kişilerin, taleplerini veri sorumlusuna yazılı olarak ya da uygulamada oluşacak ihtiyaca göre Kurulun belirleyeceği diğer yöntemlerle iletebilmeleri mümkündür.

İlgili kişinin talebini alan veri sorumlusu, başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve herhalde en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifiedeki ücret talep edebilir. Veri sorumlusu talebi inceledikten sonra kabul veya gerekçesini açıklayarak reddetmesi ve cevabını ilgili kişiye yazılı veya elektronik ortamda bildirmesi gerekmektedir¹⁹⁴. Veri sorumlusu talebi kabul etmesi halinde, gereğini yerine getirmesi gerekmektedir. İlgili kişinin başvurusu veri sorumlusunun hatasından kaynaklanıyorsa, veri sorumlusu başvuru için aldığı ücreti iade etmek zorundadır.

¹⁹³ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 375.

¹⁹⁴ Gerekçede veri sorumlusu tarafından yapılan "bildirim" ayrıca açıklanmıştır. Veri sorumlusunun 7201 sayılı Tebligat Kanununa tabi olması halinde yapacağı bildirim bu Kanun hükümlerine göre resmi tebligat yoluyla yapılacaktır. Ancak veri sorumlusu, gerçek kişi veya özel hukuk tüzel kişisi olup 7201 sayılı Tebligat Kanununa tabi olmaması halinde yapacakları bildirim bir ispat sorunu olup gerektiğinde yargı mercilerince ele alınacaktır.

2. Kişisel Verileri Koruma Kurulu'na Şikâyet Yolu İle Yapılan Başvuru

Kişisel Verilerin Korunması Kanunu'nun 14. maddesinde ilgili kişi tarafından Kanun'un 13. maddesi uyarınca yapmış olduğu başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hallerinde Kişisel Verileri Koruma Kuruluna başvuru yolu düzenlenmiştir. İlgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyetle bulunabilir.

Maddenin ikinci fıkrasında Kanun'un 13. maddesi uyarınca veri sorumlusuna başvuru yolu tüketilmeden şikâyet yoluna başvurulamayacağı düzenlenmiştir. Başvuru yolunun zorunlu olması, şikâyet yoluna gitmenin ise ihtiyari olması, uyuşmazlıkların öncelikle veri sorumlusu ile ilgili kişi arasında çözülerek Kurulun yoğun bir iş yüküyle karşı karşıya kalmasının önlenmesi amaçlanmaktadır (Kişisel Verilerin Korunması Kanunu Madde Gereçekçeleri). Başvurusu zımnen veya açıkça reddedilen ilgili kişinin bir yandan masrafsız ve daha hızlı sonuç alınması mümkün olan şikâyet yoluna gidebilmesi, diğer yandan Maddenin son fıkrasına göre tazminat hakları saklı tutulduğundan veri sorumlusunun hukuki statüsüne göre adli ya da idari yargı yoluna gidebilmesi mümkün olacaktır.

3. Kişisel Verileri Koruma Kurulu Tarafından Yapılan İncelemenin Usul ve Esasları

Kişisel Verilerin Korunması Kanunu'nun 15. maddesinde Kişisel Verileri Koruma Kurulu tarafından yapılan incelemenin usul ve esasları düzenlenmektedir. Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi halinde resen, görev alanına giren konularda gerekli incelemeyi yapar. Kurul'a yapılacak ihbar ve şikâyetlerin 1 Kasım 1984 tarihli ve 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6. maddesinde belirtilen şartları taşıması gerekmektedir.¹⁹⁵ Kurul'un resen genel inceleme yetki ve görevi bulunmamakta olup, yapılacak inceleme şikâyet veya resen

¹⁹⁵ 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6. maddesinde Türkiye Büyük Millet Meclisine veya yetkili makamlara verilen veya gönderilen dilekçelerde; dilekçenin belli bir konuyu ihtiva etmesi, yargı mercilerinin görevine giren konularla ilgili olmaması, dilekçe sahibinin adı soyadı ve imzası ile iş veya ikametgâh adresinin bulunması gerekir. Bu şartları sağlamayan dilekçeler incelenmez.

öğrenilen şikâyet konusuna bağlıdır. Veri sorumluları devlet sırrı niteliğindeki bilgi ve belgeler hariç, talep edilen bilgi ve belgeleri, Kurula on beş gün içerisinde göndermek veya gerektiğinde yerinde inceleme yapılmasına imkân sağlamakla yükümlüdür.

Kurulun şikâyet üzerine yapacağı inceleme sonunda cevap vermesi öngörülmekte olup; şikâyet tarihinden itibaren altmış gün içerisinde cevap verilmezse talep reddedilmiş sayılacaktır. Altmış günlük sürenin sonunda ilgili kişinin idari yargıda dava açma süresi başlar. Kurulun resen yapacağı incelemeler yönünden herhangi bir süre öngörülmemiştir.

Şikâyet üzerine veya resen yapılan inceleme sonucunda Kanun hükümlerinin ihlal edildiği sonucuna varılması halinde tespit edilen hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek kararı ilgililere tebliğ eder. Bu kararın, tebliğden itibaren gecikmeksizin ve en geç otuz gün içerisinde yerine getirilmesi gerekmektedir. İlgililer, Kurulca verilen kararlara karşı idare mahkemelerinde dava açabilirler (Kişisel Verilerin Korunması Kanunu Madde Gerekçeleri). Yine şikâyet üzerine veya resen yapılan inceleme sonucunda, kanuna aykırı uygulamanın yaygın olduğunun tespit edilmesi halinde Kurul bu konuda ilke kararı alarak bu kararı yayımlar.

Kişisel Verilerin Korunması Kanunu'nun 15. Maddesinin son fıkrasında Kurula, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık şartlarının birlikte gerçekleşmesi halinde, nihai karardan önce veri işlenmesinin veya verinin yurtdışına aktarılmasının durdurulmasına karar verme yetkisi de tanınmıştır.

4. Veri Sorumluları Sicili

Kişisel Verilerin Korunması Kanunu'nun 16. maddesinde veri sorumlularının kaydedilmesi amacıyla Kişisel Verileri Koruma Kurulu'nun gözetiminde Başkanlık tarafından kamuya açık olarak tutulan Veri Sorumluları Sicilidüzenlenmektedir. Kişisel verileri işleyen gerçek ve tüzel kişiler veri işlemeye başlamadan önce Sicile kaydolmak zorundadır. Kurul, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi belirlenecek

objektif kriterler göz önüne alınmak suretiyle kayıt zorunluluğuna istisnalar getirilebilecektir¹⁹⁶.

Kanun'un 16. maddesinin üçüncü fıkrasında Veri Sorumluları Siciline kayıt başvurusu için yapılacak bildirimin içeriği düzenlenmiştir. Buna göre yapılacak bildirimin; (i) veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgilerini, (ii) kişisel verilerin hangi amaçla işleneceğini, (iii) veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamaları, (iv) kişisel verilerin aktarılabileceği alıcı veya alıcı gruplarını, (v) yabancı ülkelere aktarımı öngörülen kişisel verileri, (vi) kişisel veri güvenliğine ilişkin alınan tedbirleri, (vii) kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi¹⁹⁷ içermesi gerekir¹⁹⁸. Anılan bilgilerde değişiklik olması halinde meydana gelen değişikliklerin derhal

¹⁹⁶ 30286 sayılı Veri Sorumluları Sicili Hakkında Yönetmeliğin 8. maddesi gereğince “Kayıt yükümlülüğü altında bulunmayan, sonradan kayıt yükümlüsü haline gelen veri sorumluları, yükümlülük altına girmelerini müteakip otuz gün içerisinde Sicile kaydolurlar. Kayıt yükümlülüğü altında bulunan veri sorumluları, herhangi bir fiili, teknik ya da hukuki imkânsızlık nedeniyle kayıt yükümlülüklerinin yerine getirilememesi halinde, bu imkânsızlığın ortaya çıktığı tarihten itibaren en geç 7 iş günü içerisinde Kuruma yazılı olarak başvurmak ve gerekçesini belirtmek şartıyla, kayıt yükümlülüklerini yerine getirmek için Kurumdan ek süre talep edebilirler. Kurum, bir defaya mahsus olmak ve her halde otuz günü geçmemek üzere ek süre verebilir.”.

¹⁹⁷ Kişisel verilerin mevzuatta öngörülen veya işlendikleri amaç için gerekli olan azami muhafaza edilme süresi hakkında Sicile açıklanacak bilgilerin veri kategorileri ile eşleştirilerek bildirilmesi gerekir. Veri sorumlusu tarafından Sicile bildirilen veri kategorilerinin işleme amaçları ve bu amaçlara dayalı olarak işlenmeleri için gerekli olan azami muhafaza edilme süreleri ile mevzuatta öngörülen süreler farklı olabilir. Bu durumda mevzuatta azami muhafaza edilme süresi öngörülmüşse öngörülen bu süre yoksa bunlardan en uzun süre esas alınarak bu veri kategorisi için Sicile bildirim yapılır. Kişisel verilerin işlendikleri amaç için gerekli olan azami muhafaza edilme süresi belirlenirken; ilgili veri kategorisinin işlenme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre, ilgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre, ilgili veri kategorisinin işlenme amacına bağlı olarak veri sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre, ilgili veri kategorisinin işlenme amacına bağlı olarak saklanmasıyla yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre, belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı, veri sorumlusunun hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre, veri sorumlusu tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi dikkate alınır (30286 sayılı Veri Sorumluları Sicili Hakkında Yönetmelik m.9/4). Veri sorumluları ayrıca kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin belirlenmesi, bu sürelerin kişisel veri işleme envanterinde belirtilen bilgilerle uyumu ve azami sürenin aşılp aşılmadığının takibi için kişisel veri saklama ve imha politikası hazırlayarak, bu politikanın uygulanmasını temin ederler (30286 sayılı Veri Sorumluları Sicili Hakkında Yönetmelik m.9/5).

¹⁹⁸ Veri sorumluları tarafından kişisel verilerin hangi amaçla işleneceği, veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar, kişisel verilerin aktarılabileceği alıcı veya alıcı gruplar, yabancı ülkelere aktarımı öngörülen kişisel veriler, Kanunun 12. maddesinde belirtilen hususları kapsayacak şekilde kişisel veri güvenliğine ilişkin alınan tedbirler VERBİS üzerinden Sicile iletilir (30286 sayılı Veri Sorumluları Sicili Hakkında Yönetmelik m.9).

Başkanlığa bildirilmesi öngörülmüştür. Maddenin son fıkrasında Veri Sorumluları Siciline ilişkin diğer usul ve esaslar yönetmelikle düzenleneceği öngörülmüştür. 30286 sayılı 30 Mart 2017 tarihli Resmi Gazetede yayımlanarak “Veri Sorumluları Sicili Hakkında Yönetmelik” yayımlanarak 01 Ocak 2018 tarihinde yürürlüğe girmiştir.

H. Kişisel Verileri Koruma Kurumu ve Teşkilatı

1. Kişisel Verileri Koruma Kurumu

Bireyin temel haklarının etkin bir şekilde korunabilmesi için veri işlem faaliyetlerinin her aşamasında temel ilkelere ve kurallara uyulup uyulmadığının bağımsız veri koruma otoriteleritarafından denetlenmesi gerekir¹⁹⁹. Bireyin haklarının güvence altına alınabilmesi için bağımsız bir makamın varlığı son derece önemlidir. Bu anlamda Genel Veri Koruma Tüzüğü ile Avrupa Veri Koruma Kurumu kurulmuştur. Avrupa Veri Koruma Kurumu, bağımsız bir kurum olup; başta GVKT’nın yeknesak bir şekilde uygulanması, uyumsuzlukların çözülmesi ve denetim makamları arasında koordinasyonun sağlanması gibi pek çok konuda görevlidir (GVKT m. 70)²⁰⁰. Ülkemizde bu görev Kişisel Verileri Koruma Kurumu tarafından yerine getirilmektedir.

Kişisel Verilerin Korunması Kanunu’nun 19. maddesinde Kanun’un verdiği görevleri yerine getirmek amacıyla idari ve mali özerkliğe sahip, kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumu’nun kuruluşu düzenlenmektedir. Kurum Cumhurbaşkanının görevlendireceği bakan ile ilişkilidir²⁰¹. Kurumun merkezi Ankara’dır. Kurum, Kurul ve Başkanlıktan oluşmakta olup; Kurumun karar organı Kuruldur.

Kanunu’nun 20. maddesinde Kişisel Verilerin Koruma Kurumu’nun görevleri sayılmıştır. Maddeye göre Kurumun görevleri; (i) uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirmek ve önerilerde bulunmak, (ii) araştırma ve

¹⁹⁹ Şimşek, s. 102.

²⁰⁰ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 390.

²⁰¹ Kurum Başbakanlık ile ilişkili iken 2 Temmuz 2018 tarihli ve 703 sayılı KHK’nin 163. maddesiyle Cumhurbaşkanının görevlendireceği bakan ile ilişkilendirilmiştir.

incelemeler yapmak veya yaptırmak, (iii) ihtiyaç duyulması hâlinde görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak, (iv) uluslararası gelişmeleri izlemek ve değerlendirmek, uluslararası kuruluşlarla iş birliği yapmak, toplantılara katılmak, (v) yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna sunmak, (vi) kanunlarla verilen diğer görevleri yerine getirmektir.

2. Kişisel Verileri Koruma Kurulu

Kişisel Verileri Koruma Kurumu'nun karar organı olan Kişisel Verileri Koruma Kurulu, Kanunla ve diğer mevzuatla verilen görev ve yetkileribağımsız olarak yerine getirmekle ve kendisine verilen yetkileri kullanmakla yükümlüdür (KVKK m. 21). Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi Kurul'a emir, talimat, tavsiye veremeyeceği gibi telkinde de bulunamayacaktır.

Kurul, 9 üyeden oluşmakta olup; beş üyesi Türkiye Büyük Millet Meclisi, dört üyesi Cumhurbaşkanı tarafından seçilecektir (KVKK m. 21/2)²⁰². Kurula üyelik şartları ise şöyledir (KVKK m. 21/3): (i) Kurumun görev alanındaki konularda bilgi ve deneyim sahibi olmak, (ii) 657 sayılı Devlet Memurları Kanununun 48. maddesinde belirtilen nitelikleri taşımak, (iii) herhangi bir siyasi parti üyesi olmamak, (iv) en az dört yıllık lisans düzeyinde yükseköğrenim görmüş olmaktır. Kurul üyelerinin görev süresi dört yıl olup, süresi biten üyeler tekrar seçilebilir. Kural olarak Kurul üyelerinin görev süreleri bitmeden görevlerine son verilemez. Ancak üyelerin (i) seçilmek için gereken şartları taşımadıklarının sonradan anlaşılması, (ii) görevleriyle ilgili olarak işledikleri suçlardan dolayı haklarında verilen mahkûmiyet kararının kesinleşmesi, (iii) görevlerini yerine getiremeyeceklerinin sağlık kurulu raporuyla kesin olarak tespit edilmesi, (iv) görevlerine izinsiz, mazeretsiz ve kesintisiz olarak on beş gün ya da bir yılda toplam

²⁰² Kurul'un 9 üyesinin ikisi Cumhurbaşkanı, ikisi Bakanlar Kurulu ve beşi Türkiye Büyük Millet Meclisi tarafından seçilmekte iken 2 Temmuz 2018 tarihli ve 703 sayılı KHK'nın 163. maddesiyle yapılan değişiklik neticesinde artık Bakanlar Kurulu tarafından seçilen iki üyenin de Cumhurbaşkanı tarafından seçilecektir.

otuz gün süreyle devam etmediklerinin tespit edilmesi, (v) bir ay içinde izinsiz ve mazeretsiz olarak toplam üç, bir yıl içinde toplam on Kurul toplantısına katılmadıklarının tespit edilmesihisinde Kurul kararıyla üyelikleri sona erdirilir. Görev süresi dolmadan herhangi bir sebeple görevi sona eren üyenin yerine seçilen kişi, yerine seçildiği üyenin kalan süresini tamamlayacaktır. Kurul üyeliğine seçilenlerin önceki görevleri ile olan ilişkileri kesilir. Seçilen üyeler Yargıtay Birinci Başkanlık Kurulu huzurunda yemin ederler.

Kurul üyeleri aksi özel bir kanunla düzenlenmedikçe, Kuruldaki resmî görevlerinin dışında resmî veya özel hiçbir görev alamaz, dernek, vakıf, kooperatif ve benzeri yerlerde yöneticilik yapamaz, ticaretle uğraşamaz, serbest meslek faaliyetinde bulunamaz, hakemlik ve bilirkişilik yapamazlar. Ancak görevlerini aksatmayacak şekilde bilimsel amaçlı yayın yapabilir, ders ve konferans verebilir ve bunlardan doğacak telif hakları ile ders ve konferans ücretlerini alabilirler.

Kurul üyeleri hakkında yapılacak disiplin soruşturması ve kovuşturması 657 sayılı Devlet Memurları Kanunu hükümlerine göre yapılır. Üyelerin görevleri sebebiyle işledikleri iddia edilen suçlara ilişkin soruşturmalar 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanuna göre yapılır ve soruşturma izni Cumhurbaşkanı tarafından verilir.

a. Kurulun Görev ve Yetkileri

Kişisel Verileri Koruma Kanunu'nun 22. maddesinde Kurulu'nun görev ve yetkileri düzenlenmektedir. Buna göre Kurul'un görev ve yetkileri şunlardır:

- a) Kişisel verilerin temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak,
- b) Kişisel verileri ihlal edilenlerin şikâyetlerini karara bağlamak,
- c) Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak.
- d) Özel nitelikli kişisel verilerin işlenmesi için gerekli olan önlemleri belirlemek,
- e) Veri Sorumluları Sicilinin tutulmasını sağlamak,

- f) Kurulun görev alanına, Kurumun işleyişine, veri güvenliğine ilişkin yükümlülüklerin belirlenmesine ve veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlemler yapmak,
- g) Kişisel Verilerin Korunması Kanunu'nda öngörülen idari yaptırımlara karar vermek,
- h) Kişisel verilere ilişkin hüküm içeren diğer kurum ve kuruluşlarca hazırlanan mevzuat taslakları hakkında görüş bildirmek,
- i) Kurumun stratejik planını karara bağlamak, amaç ve hedeflerini belirlemek ve bunlara uygun bütçe teklifini görüşüp karara bağlamak,
- j) Kurumun hizmet kalite standartlarını ve performans kriterlerini belirlemek,
- k) Kurumun performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında hazırlanan rapor taslaklarını onaylamak ve yayımlamak.
- l) Taşınmaz alımı, satımı ve kiralınması konularındaki önerileri görüşüp karara bağlamak,
- m) Kanunlarla verilen diğer görevleri yerine getirmektir.

16 Kasım 2017 tarihli 30242 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren “Kişisel Verileri Koruma Kurulu Çalışma Usul Ve Esaslarına Dair Yönetmelik” ile Kurul’un birtakım ek görevler yüklenmiştir. Bunlar; (i) üniversiteler ve ilgili diğer yurt içi ve yurt dışı kurum ve kuruluşlarla işbirliği ve koordinasyon çalışmaları yürütmek, (ii) ücret tarifeleri ile ilgili çalışmalar yapmak, (iii) kişisel verilerin korunması konusunda kurum ve kuruluşları bilgilendirmek, kamuoyuna yönelik farkındalık faaliyetleri gerçekleştirmek, (iv) kişisel verilerin korunması ile ilgili yurt içi ve yurt dışı projeler yapmak ve yaptırmak, (v) kişisel verilerin korunması, işlenmesi ve güvenliği ile ilgili sektörel uygulama esaslarını belirlemek ve akreditasyon, sertifikasyon, eğitim ile rehberlik konularında usul ve esasları belirlemek, (vi) yurt dışına veri aktarılabilmesi için yeterli korumaya sahip olan ve olmayan ülkeleri belirleyip ilan etmektir.

b. Kurulun Çalışma Esasları

Kişisel Verilerin Korunması Kanunu’nun 23. maddesinde Kurul’un çalışma usul ve esasları düzenlenmiş olup; ayrıca usul ve esaslar ile Kurul kararlarının yazımı

ile diğer başkaca hususların yönetmelik ile belirleneceği öngörülmüştür. Kanun 23. maddesinde belirlenen çalışma esasları şöyledir:

- a) Kurulun toplantı günlerini ve gündemini Başkan belirler. Başkan gereken hâllerde Kurulu olağanüstü toplantıya çağırabilir. Aksi kararlaştırılmadıkça, Kurul toplantılarındaki görüşmeler gizlidir
- b) Kurul, başkan dâhil en az altı üye ile toplanır ve üye tam sayısının salt çoğunluğuyla karar alır. Kurul üyeleri çekimser oy kullanamaz. Kurul üyeleri; kendilerini, üçüncü dereceye kadar kan ve ikinci dereceye kadar kayın hısımlarını, evlatlıklarını ve aralarındaki evlilik bağı kalkmış olsa bile eşlerini ilgilendiren konularla ilgili toplantı ve oylamaya katılamaz.
- c) Kurul üyeleri çalışmaları sırasında ilgililere ve üçüncü kişilere ait öğrendikleri sırları bu konuda kanunen yetkili kılınan mercilerden başkasına açıklayamazlar ve kendi yararlarına kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.
- d) Kurulda görüşülen işler tutanağa bağlanır. Kararlar ve varsa karşı oy gerekçeleri karar tarihinden itibaren en geç on beş gün içinde yazılır. Kurul, gerekli gördüğü kararları kamuoyuna duyurur.

İ. Yaptırım

1. Suçlar

Kişisel verilere ilişkin suçlar bakımından Kanun'un 17. maddesinde 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140. madde hükümlerine atıf yapılmıştır. TCK'nın atıf yapılan maddelerinde kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme, yayma veya ele geçirme ile verileri yok etmeme suç olarak düzenlenmiştir. Ceza hukukuna hâkim olan "suç ve cezaların kanuniliği" ve "kıyas yasağı" ilkesi gereğince TCK ile suç sayılan eylemler haricinde veriler üzerinde gerçekleştirilen hukuka aykırı faaliyetlerin TCK'nın 135 ve devamı hükümleri kapsamında değerlendirilerek cezalandırılması mümkün değildir²⁰³. Konuya ilişkin

²⁰³ Küzeci, s. 380.

incelemelerimizi çalışmamızın 5237 sayılı Türk Ceza Kanunu'nda kişisel verilerin korunmasına ilişkin suçlar başlığı altında ayrıntılı olarak aktaracağız.

2. Kabahatler

Kişisel Verilerin Korunması Kanunu'nun 18. maddesinde Kanun ile öngörülen yükümlülüklerle aykırı davranılması halinde uygulanacak idari yaptırımlar düzenlenmiştir. Buna göre;

“Bu Kanunun;

a) 10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar,

b) 12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar,

c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar,

ç) 16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar, idari para cezası verilir.

(2)Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır.

(3) Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir.”

İdari yaptırımlara Kurul tarafından karar verilecektir. Verilen yaptırım kararlarına karşı idari yargı yolu açıktır.

İdari para cezalarının alt ve üst sınırları arasındaki genişliğe Kanun'un gerekçesinde,“Kabahatler karşılığında öngörülen idari para cezalarının alt ve üst sınırları arasındaki makas bilinçli olarak geniş tutulmuştur. Kurul karar verirken kabahatler hususunda genel kanun niteliğinde olan 30/3/2005 tarihli ve 5326 sayılı

Kabahatler Kanununun 17 nci maddesinin ikinci fıkrasında belirtildiği üzere kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumunu dikkate alacaktır. Bu şekilde düzenleme yapılmak suretiyle, söz konusu kabahatlerin çok farklı ekonomik güce sahip gerçek veya tüzel kişiler hakkında uygulanacak olması nedeniyle yaptırım uygulanmasında hakkaniyeti sağlamak amaçlanmıştır. Buna göre örneğin, küçük bir şehirde faaliyet gösteren bir aile şirketiyle ülke çapında faaliyet gösteren bir holdingin Kanun hükümlerini ihlal etmesi durumunda belirlenecek idari para cezalarının miktarı söz konusu şirketlerin ekonomik durumlarına göre farklı olacaktır.” şeklinde açıklama getirilmiştir.

3. Tazminat

Kişisel veriler üzerinde hukuka aykırı eylemler ilgili kişinin maddi ve manevi zararına sebep olabilir. İlgili kişinin maddi ve manevi zararının giderilmesini talep etme²⁰⁴ ve zararının tazmini için tazminat talep etme hakkı²⁰⁵ Kanun ile koruma altına alınmıştır. Konuya ilişkin incelemelerimizi çalışmamızın Kişisel Verilerin 4721 Sayılı Türk Medeni Kanunu ve 6098 Sayılı Türk Borçlar Kanunu Kapsamında Korunması başlığı altında ayrıntılı olarak aktaracağız.

. İstisnalar

Kişisel Verilerin Korunması Kanunu’nun 28. maddesinde Kanun’un kapsamı dışında kalan haller düzenlenmiştir. Kanun’un tamamen kapsamı dışında bırakılan haller şöyledir KVKK m.28/1 :

- a Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülöklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi,
- b Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi,

²⁰⁴ KVKK m.11 “Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir”; Küzeci, s. 373.

²⁰⁵ KVKK m.14 “Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır”; Küzeci, s. 373.

- c) Sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi,
- d) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik yürütülen önleyici, koruyucu ve istihbarî faaliyetler kapsamında işlenmesi,
- e) Soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.

Kanun'un 28. maddesinin 2. fıkrasında ise Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10. maddenin, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11. maddenin ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16. maddenin uygulanmayacağı haller düzenlenmiştir. Kanun'un kısmen uygulanmayacağı durumlar şunlardır:

- a) Kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması,
- b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi,
- c) Kişisel veri işleminin kanunun verdiği yetkiye dayanarak 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,
- d) Kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

GVKT ile de veri sorumlusu veya işleyicisinin tabi olduğu Birlik veya üye devlet hukukunun bir yasama tedbiri vasıtasıyla; temel haklar ve özgürlüklerin özüne saygı göstermesi ve demokratik bir toplumda gerekli ve orantılı olması koşuluyla ilgili kişinin haklarının kısıtlanabileceği durumlar sınırlı olarak sayılmıştır (GVKT m. 23). Buna göre²⁰⁶:

- a) Milli güvenlik, savunma, kamu güvenliği ile kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesinin söz konusu olduğu durumlar,

²⁰⁶ Gemicioğlu, Gemicioğlu, Yağcı ve Yılmaz, s. 354.

- b) Başta Birliğin veya bir üye devletin önemli bir ekonomik veya mali çıkarına olmak üzere parasal hususlar ile bütçe ve vergilendirmeye ilişkin hususlar, halk sağlığı ve sosyal güvenlik de dâhil Birlik ya da bir üye devletin genel kamu yararına yönelik diğer önemli hedeflerin sağlanmasına yönelik olarak,
- c) Yargı bağımsızlığının ve adli süreçlerin korunması amacıyla,
- d) Düzenlenmiş mesleklere ilişkin etik kurallarının ihlalinin önlenmesi, soruşturulması, tespiti ve kovuşturulması amacıyla,
- e) Resmi yetkinin kullanımı ile bağlantılı bir izleme, denetleme veya düzenleme işlevinin sağlanması ya da veri sahibinin veya başkalarının haklarının ve özgürlüklerinin korunması amacıyla,
- f) Medeni hukuktan kaynaklanan taleplere ilişkin kararların icrası söz konusu olduğunda ilgili kişinin hakları kısıtlanabilir.

Özellikle bir yasama tedbiri söz konusu olduğunda ilgili kısıtlamanın: işlemenin veya işleme kategorilerinin amaçları, kişisel veri kategorileri, getirilen kısıtlamaların kapsamı, kötüye kullanım veya yasa dışı yollarla erişim veya aktarımın engellenmesine yönelik güvenceler, kontrolör veya kontrolör kategorilerinin belirlenmesi, işleme veya işleme kategorilerinin mahiyeti, kapsamı ve amaçları dikkate alınarak saklama süreleri ve uygulanabilir güvenceler, veri sahiplerinin hakları ve özgürlüklerine yönelik riskler, kısıtlama amacına halel getirmemesi durumunda, veri sahiplerinin kısıtlamayla ilgili bilgi sahibi olma hakkını içermesi gerekir (GVKT m. 23/2).

II. 5237 SAYILI TÜRK CEZA KANUNUNDA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN SUÇLAR

765 sayılı Türk Ceza Kanunu'nda özel hayatın ve kişisel verilerin korunmasına ilişkin suç tiplerine yer verilmemiştir. Ancak başta 765 sayılı Kanun'un beşinci faslında "sırrın masuniyeti aleyhine cürümler" başlığı altında düzenlemeler olmak üzere Kanun'un çeşitli maddelerinde özel hayatın korunması ile bağlantılı düzenlemeler yer almaktadır²⁰⁷. Özel hayatın ve kişisel verilerin korunmasına dair suç tipleri ilk olarak 5237 sayılı Türk Ceza Kanunu'nun özel hükümlerin

²⁰⁷ Güçlü Akyürek, **Özel Hayatın Gizliliğinin İhlal Suçu**, Seçkin Yayınları, Ankara, 2013, s. 190.

düzenlendiği ikinci kitabının ikinci kısmının “özel hayata ve özel hayatın gizli alanlarına karşı suçlar” başlıklı dokuzuncu bölümünde yer almaktadır²⁰⁸. Bu bölüm altında yer alan 135. maddede “kişisel verilerin kaydedilmesi” suçu, 136. maddede “verileri hukuka aykırı olarak verme veya ele geçirme” suçu, 137. maddede nitelikli haller, 138. maddede “verileri yok etmeme” suçu, 140. maddede tüzel kişilere uygulanacak güvenlik tedbirleri yer almaktadır. Esasen kişisel verilerin korunmasına dair TCK kapsamında yer alan bu suçlar, kişisel verilerin korunması hukukuna dair temel ilkelerin ceza hukukuna yansımalarıdır²⁰⁹. TCK’nın 135 ve 136. maddelerinin özellikle dürüst ve hukuka uygun toplama ve işleme, amaçla bağlılık ilkesinin; 138. maddenin ise amaçla bağlılık ilkesi ile unutulma hakkının²¹⁰ özel bir görünümü niteliğindedir²¹¹.

Çalışmamızın bu bölümünde 5237 sayılı Türk Ceza Kanunu’nun 135 vd. maddelerinde yer alan “kişisel verilerin kaydedilmesi”, “verilerin hukuka aykırı olarak verme veya ele geçirme” ve “verileri yok etmeme” suçu incelenecektir.

A. Kişisel Verilerin Kaydedilmesi Suçu TCK m. 135

1. Suç Tipi Hakkında Genel Bilgiler

5237 sayılı TCK’nın 135. maddesinin 1. fıkrasında hukuka aykırı olarak kişisel verilerin kaydedilmesi eylemi suç olarak düzenlenmiştir. Maddenin 2. fıkrasında hukuka aykırı olarak kaydedilen kişisel verinin; kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması suçun nitelikli hali olarak düzenlenmiştir.

“(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

²⁰⁸ Durmuş Tezcan, Mustafa Ruhan Erdem ve Murat Önok, **Teorik ve Pratik Ceza Özel Hukuku**, Seçkin Yayınları, Ankara, 2018, s.641; Akyürek, s. 189.

²⁰⁹ Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları**, Adalet Yayınevi, 2008, s. 205; Alaattin Bük, **Bilişim Alanında Kişisel Verilerin Korunması**, Seçkin Yayınları, Ankara, 2018, s. 100.

²¹⁰ Metin Turan, **Karşılaştırmalı Hukukta Kişisel Verilerin Korunması**, Seçkin Yayınları, Ankara, 2019, s. 101.

²¹¹ Ketizmen, s. 206.

(2)Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.”²¹².

Maddenin gerekçesinde de belirtildiği üzere çağımızda bazı kurum ve kuruluşlar tarafından kişilere ait veriler kaydedilip muhafaza altına alınmaktadır. Örneğin hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alış verişi yapılan mağazaların müşterilerine ilişkin kayıtlar kaydedilmekte ve kullanılmaktadır. Bu bilgilerin ilgilinin rızası olmaksızın kullanılması, kaydedilme amacı dışında kullanılması veya herhangi bir üçüncü kişilerin eline geçerek hukuka aykırı olarak kullanılmasından dolayı veri sahibi kişiler zarara uğrayabileceklerinden kişisel verilerin hukuka aykırı olarak kayda alınması suç olarak düzenlenmiştir (Türk Ceza Kanunu Madde Gerekçeleri). Maddenin gerekçesinde ayrıca kişisel verilerin kaydedilmesi suçunun tanımı ile Avrupa Konseyi tarafından hazırlanan Türkiye’nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu “Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme”ye uyum sağlandığı ve ilgili hükümlerine geçerlilik tanınmış olduğu belirtilmiştir.

2. Suçla Korunan Hukuki Değer

Kanun’un sistematüğinden de anlaşıldığı üzere suçla korunan hukuki değer genel olarak özel hayat ve özel hayatın gizli alanları²¹³, özel olarak kişisel verilerdir²¹⁴.

²¹² 24 Mart 2016 tarihli ve 6698 sayılı Kanunun 30. maddesiyle, bu fıkra da yer alan “kişilerin” ibaresi “kişisel verinin, kişilerin” şeklinde; “bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır” ibaresi “olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır” şeklinde değiştirilmiştir.

²¹³ Zeki Hafizoğulları ve Muharrem Özen, **Türk Ceza Hukuku Özel Hükümler, Kişilere Karşı Suçlar**, U S-A Yayıncılık, Ankara, 2016, s. 286; Ali Karagölmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Seçkin Yayınları, 5. Baskı, Ankara, 2014, s. 446; Gökhan Taneri/ve Gani Kamışlı, **Kişilere Karşı İşlenen Suçlar**, Seçkin Yayınları, Ankara, 2018, s. 740; Ali arlar, **Türk Ceza Kanunu Şerhi**, C.2, Bilge Yayınevi, Ankara, 2015, s. 1549; Veli Özer Özbek, Mehmet Nihat Kanbur, Koray Doğan, Pınar Bacaksız ve İlker Tepe, **Türk Ceza Hukuku Özel Hükümler**, Seçkin Yayınları, Ankara, 2018, s. 582; Şeyma Sert, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Seçkin Yayınları, Ankara, 2019, s.101; Kuşkonmaz, s. 133; Hasan Tahsin Gökcan, **Tıbbi Müdahaleden Doğan Hukuki ve Cezai Sorumluluk**, Seçkin Yayınları, Ankara, 2017, s. 809.

Kişisel verilerin korunması hakkı 2010 Anayasa değişikliği ile anayasa ile koruma altına alınan temel hak ve özgürlükler arasında bağımsız bir hak olarak güvence altına alınmıştır. Kişisel verilerin korunması hakkının Anayasa’da yer alan, özel hayatın gizliliği ve korunması hakkı, haberleşme hürriyeti, düşünce ve kanaat hürriyeti, din ve vicdan hürriyeti gibi pek çok temel hak ve özgürlüklerle ilişkilendirilebilmesi sebebiyle bu suç ile başta özel hayatın ve özel hayatın gizli alanlarının korunması hakkı olmak üzere kişilik hakkı²¹⁵ gibi diğer pek çok hak koruma altına alınmaktadır.

3. Suçun Unsurları

a. Tipikliği Maddi Unsurları

1 Fail

TCK’nın 135. maddesine göre suçun faili kişisel verileri hukuka aykırı olarak kaydeden kişidir. Madde metninde fail bakımından “kişisel verileri kaydeden kimse” ibaresi kullanıldığından suçun faili herkes olabilir²¹⁶. Ancak TCK’nın 20. maddesine göre suçun faili tüzel kişiler olamayacaksa da TCK m.140 gereğince haklarında güvenlik tedbirleri uygulanır²¹⁷. Failin kamu görevlisi olması ve görevinin verdiği yetkiyi kötüye kullanmak suretiyle bu suçu işlenmesi halinde TCK m. 137 gereğince verilecek ceza yarı oranında arttırılacaktır. Yine aynı maddede failin belirli bir meslek veya sanatın sağladığı kolaylıktan yararlanan kişi olması halinde yine cezanın yarı oranında arttırılacağı öngörülmüştür.

²¹⁴ Tezcan, Erdem ve Önok, s.643; Doğan Soyaslan, **Ceza Hukuku Özel Hükümler**, 11. Baskı, Yetkin Yayınları, Ankara, 2016, s. 349; Dülger, s. 310; Sacit Yılmaz, **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Adalet Yayınevi, Ankara, 2016, s. 258.

²¹⁵Bük, s.102; Soyaslan, s. 349; Handan Yokuş Sevük, **Kişisel Verilerin Açıklanması**, Türkiye Barolar Birliği, Tıp Ceza Hukukunun Güncel Sorunları, V. Türk Alman Tıp Hukuku Sempozyumu, Ankara, 2008, 782-811, s.794; Hamide Zafer, **Özel Hayat ve Özel Hayatın Gizli Alanının Ceza Hukukuyla Korunması TCK m.132-134**, Beta Yayınları, İstanbul, 2010, s. 23.

²¹⁶ Hafizoğulları ve Özen, s. 286; Yılmaz, s. 257; Parlar, s. 1549; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 587; Korkmaz, s. 398; Soyaslan, s. 350; Sert, s. 106.

²¹⁷ Hafizoğulları ve Özen, s. 287; Soyaslan, s. 350; Sert, s. 106.

2 Mağdur

Suçun mağduru konusunda da maddede herhangi bir özellik belirtilmemiştir. Bu sebeple suçun mağduru herkes olabilir²¹⁸. Kanunun gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edildiğine değinilmiştir. Yine KVKK ile sadece gerçek kişilerin kişisel verileri olabileceğini, tüzel kişiye ait verilerin ancak bir gerçek kişi ile ilgisinin bulunması halinde korunabileceğini çalışmamızın birinci bölümünde açıklamıştık. Bu nedenle suçun mağduru tüzel kişiler olamayacaktır. TCK'nın Kişisel Verilerin Korunması Kanunu ile ilişkisi dikkate alındığında doktrinde suçun mağdurunun hem gerçek kişiler hem de tüzel kişiler olabileceği yönündeki görüşe katılmıyoruz²¹⁹. Tüzel kişiler ancak suçtan zarar gören olabilecektir²²⁰.

3 Suçun Konusu

Suçun hukuki konusu kişisel verilerdir. 5237 sayılı TCK'nın 135. maddesinin gerekçesinde gerçek kişilere ilişkin her türlü bilgi kişisel veri olarak kabul edilmektedir. Bu noktada Kanun'da açıkça kişisel verinin tanımlanmamış olması sebebiyle doktrinde kişisel veriden ne anlaşılması gerektiği, suçla sadece kişinin özel hayatı ve özel hayatının gizli alanlarına dâhil olan herkes tarafından bilinmeyen ve bilinmesini istemediği verilerinin mi yoksa çalışmamızın birinci bölümünde de açıkladığımız üzere kişiyi belirli veya belirlenebilir kılan her türlü bilginin mi koruma altına alındığı yönündeki görüş farklılıklarına ve Yargıtay kararlarına değinmekte fayda olacaktır.

Öncelikle 765 sayılı Türk Ceza Kanunu'nun yürürlükte olduğu dönem bakımından özel hayata ve özel hayatın gizli alanlarına karşı suçlar Kanunu'nda özel olarak düzenlenmemiştir. Bu dönemde daha önce de bahsettiğimiz üzere başta “sırrın masuniyeti aleyhine cürümler” başlığı altında başta haberleşmenin gizliliğini ihlal suçu olmak üzere kanunun çeşitli bölümlerinde “halkı rahatsız etmeme kabahati”

²¹⁸ Hafızoğulları ve Özen, s. 287; Dülger, s. 314; Parlar, s. 1549; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 587.

²¹⁹ Suçun mağdurunun hem gerçek hem de tüzel kişiler olabileceği yönündeki görüş için bkz. Soyaslan, s. 350; Yılmaz, s.257.

²²⁰ Dülger, s. 314; Sert, s. 107; Aydın, s. 131.

gibi toplumsal huzurun korunmasına yönelik düzenlemeler yer almaktaydı²²¹. 5237 sayılı Türk Ceza Kanunu’nu ile “özel hayata ve özel hayatın gizli alanlarına karşı suçlar” başlığı altında kişisel verilerin korunmasına dair suç tipleri düzenlenmiştir. Doktrindeki bir görüş kanunun sistematigi ve hükmün getiriliş amacı ele alınarak suçun konusunu oluşturan kişisel verilerin, kişinin herkes tarafından bilinmeyen ve bilinmesini istemediği, sır niteliğine haiz kişisel verilerle sınırlı olduğu yönündedir²²². Yargıtay 12. Ceza Dairesi’nin 30.03.2016 tarihli 2015/4349 E. 2016/5349 sayılı kararına konu olan olayda; sanık, sahte facebook profili oluşturarak ilgi duyduğu katılana arkadaşlık isteği göndererek bir süre yazıştıktan sonra katılan, sanığın kullandığı profilin sahte hesap olduğunu anlayarak sanığı arkadaşlıktan çıkarmış, sonrasında sanık kullandığı sahte profile hesabına katılanın facebook hesabından elde ettiği, katılanın arkadaş listesinde yer almayan kişilerce de görülebilen fotoğrafını koymuştur²²³. Yerel Mahkeme sanığa isnat edilen eylemde TCK’nın 135. maddesindeki kişisel verilerin kaydedilmesi suçu oluşmadığından sanık hakkında beraat kararı vermiş ve Yerel Mahkeme kararı Yargıtay 12. Ceza Dairesi’nin anılı esaslı kararı ile onanmıştır. Kararda TCK’nın 135 ve 136. maddelerinde düzenlenen suçların konusunu oluşturan kişisel veri kavramından, kişinin yetkisiz üçüncü kişilerin bilgisine sunmadığı, ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen, kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği vurgulanmıştır.

Doktrinde bizim de katıldığımız bir diğer görüşe göre kişisel verilerin korunmasına dair suçların Kanun’un özel hayata ve özel hayatın gizli alanına karşı suçlar başlığı altında yer alması kişinin sadece özel hayatına dair gizli tuttuğu, herkes tarafından bilinmesini istemediği, sır olarak sakladığı verilerinin koruma kapsamına

²²¹ Akyürek, s. 190; Alper Yaser Efil, **Özel Hayatın Gizliliğinin İhlali Suçu**, (Yayınlanmamış Yüksek Lisans Tezi), Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir, 2018, s. 66.

²²² Fatih Selami Mahmutoglu, **Sır Saklama Yükümlülüğü Kapsamında Hastaya Ait Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Yayma Suçu**, fsmahmutoglu.av.tr, s.2; Hakan Hakeri, **Tıp Hukuku**, Seçkin Yayınları, Ankara, 2018, s. 1104; Sevük, s. 796; Zeki Hafızogulları ve Muharrem Özen, **Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar**, Ankara Barosu Dergisi, Yıl:67, Sayı: 4, 2009, 9-22, s. 9; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 586.

²²³ www.yargitay.gov.tr.

alındığı şeklinde değerlendirilmemelidir²²⁴. Çalışmamızın birinci bölümünde de değindiğimiz üzere kişiye ait verilerin kişisel veri olarak kabul edilebilmesi için bu verinin ilgili kişi tarafından gizli tutulmuş olması gerekli değildir. Kişinin kendisi tarafından alenileştirdiği ya da herkes tarafından kolayca öğrenilebilen verileri de kişisel veri olarak kabul edilmektedir. Nitekim 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun henüz yürürlüğe girmedığı dönemde de Yargıtay Ceza Genel Kurulu’nun 17.06.2014 tarihli 2012/1510 E. 2014/331 sayılı kararında da bu hususa açıklık getirilmiştir²²⁵. Karara konu olayda; Katılanın 'S..N..' isimli gazetede yazdığı köşe yazısı için verdiği resim, sanık tarafından M.Bilişim Hizmetlerine ait 'www.i..l.net' isimli sosyal ağ platformu olarak hizmet veren sitede 'belkiba' rumuzuyla yayınlanmış, evli ve iki çocuklu olan katılan için bekar, aradığı cinsiyet erkek 24-29 yaşlarında, aradığı ilişki arkadaşlık ve sitede sorulan birçok soruya cevap şeklinde aradığı kişide bulunmasını istediği özellikler yazılmıştır. Yargıtay Ceza Genel Kurulu verdiği kararda, Türk Ceza Kanunu açısından kişisel verilerin korunmasına ilişkin düzenlemelerde sadece sır niteliğinde kişisel verilerin korunacağına ilişkin bir hükmün bulunmaması ve aksine 135. Maddenin gerekçesinde kişisel verilerin gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin TCK’nın kişisel verilerin korunmasına dair düzenlenen suçların konusu olabileceğine yer vermiştir²²⁶.

Türk Ceza Kanunu’nda yer alan kişisel verilerin korunmasına dair hükümlerin 6698 sayılı Kişisel Verilerin Korunması Kanunu’ndan önce yürürlüğe girmiş ve uygulanıyor olması, Türk Ceza Kanunu’nda kişisel verilerin tanımlanmamış olması iki kanun arasında uyumsuzluklara, Türk Ceza Kanunu’nun uygulanması bakımından farklılıklara sebep olmaktadır. Anayasa Mahkemesi’nin 12.11.2015 T. 2015/32 E. 2015/102 sayılı kararında her ne kadar ceza mevzuatında “kişisel veri” ile ilgili bir tanım ve sınırlama yapılmamışsa da kavramın teknolojik gelişmelere bağlı olarak çok farklı şekillerde ortaya çıkabileceğinden bu kapsama giren tüm verilerin önceden öngörülmesi ve tek tek sayılmasının mümkün olmadığı,

²²⁴ Dülger, s. 312.

²²⁵ www.yargitay.gov.tr.

²²⁶ Aynı yöndeki kararlar için bkz. Yargıtay 12. Ceza Dairesi 26.12.2017 T. 2016/9756 E. 2017/10938 K., Yargıtay 12. Ceza Dairesi 13.09.2017 T. 2016/6247 E. 2017/6230 K., Yargıtay 12. Ceza Dairesi 12.04.2017 T. 2015/13248 E. 2017/3108 K.

ulusal ve uluslararası mevzuat çerçevesinde ve yargı kararları neticesinde kavramın belirli veya kimliği belirlenebilir olmak kaydıyla bir kişiye ilişkin tüm bilgiler olarak kabul edildiği, tüm bu hususlar dikkate alındığında kavramın belirsizliğinden söz edilemeyeceği açıkça ortaya konulmuştur²²⁷. Ancak her iki kanun arasındaki uyumsuzluk özel nitelikli kişisel verilerin korunması bakımından da sorun teşkil etmektedir. TCK'nın 135. maddesinin ikinci fıkrasında “*Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır*” hükmüne yer verilerek kişilerin siyasi, felsefi, dini görüşleri, ırki kökenleri, ahlaki eğilimleri, cinsel yaşamları, sağlık durumları ile sendikal bağlantılarının kaydedilmesi daha ağır cezayı gerektirecek şekilde düzenlenmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde yer verilen özel nitelikli kişisel verilerden kişinin etnik kökenine, mezhebine veya diğer inançlarına, kılık ve kıyafetine, dernek veya vakıf üyeliğine, ceza mahkûmiyetine ve güvenlik tedbirleriyle ilgili verilerine, biyometrik ve genetik verilerine yer verilmemiştir. KVKK ile özel olarak koruma altına alınan bu veri kategorilerine de TCK'nın 135. maddesinin ikinci fıkrasında yer verilmesi her iki kanunun birbiri ile uyumlu olması ve özel nitelikli verilerin niteliği itibarıyla daha çok korunmaya ihtiyaç duyması bakımından yerinde olacaktır.

Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesinden önce yaşanan belirsizlikler uluslararası sözleşmelerde yer verilen tanımlar, doktrin, CMK hükümleri ve mahkeme kararları ile giderilmeye çalışılmıştır²²⁸. Ancak KVKK'nın yürürlüğe girmesi ile birçok tereddüt giderilmişse de iki kanunun birlikte işlerliği önündeki yorum farklılıklarının ortadan kalkması ve konunun hassasiyeti gereği bir an önce Türk Ceza Kanunu'nun 6698 sayılı Kişisel Verilerin Korunması Kanunu ile uyumlu hale getirilmesi gerekmektedir.

²²⁷ www.anayasa.gov.tr; Sert, s. 143.

²²⁸ Küzeci, s. 405; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 557; Dülger, s.312.

4 Hareket Eylem, Fiil

Suçun maddi unsurunu oluşturan hareket, kişisel verilerin hukuka aykırı olarak kaydedilmesidir. Kaydetmek, “yazmak, bazı önemli noktaları tespit etmek”, “sesi veya resmi manyetik bant üzerine geçirmek”, “elektronik veya sayısal araçlarda bilgiyi korumaya almak” olarak tanımlanmaktadır²²⁹. Kişisel verilerin kaydedilmesi, verilerin tekrar kullanılmasını, kaydedilmesini, saklanmasını sağlamak amacıyla verilerin bir araç vasıtasıyla veya araç kullanmaksızın bir yere yazılması, aktarılması, çizilmesi, işaretlenmesidir²³⁰. TCK’nın 135. maddesinin gerekçesinde açıkça belirtilmiş olması ve madde metninde de aksi belirtilmediğinden kişisel verilerin hukuka aykırı olarak kâğıt üzerinde veya bilgisayar ortamında kayda alınması arasında bir ayrım bulunmamaktadır²³¹.

Kişisel verilerin kaydedilmesi suçu, failin kişisel verileri kaydetmesi ile icrai bir hareketin varlığını gerektirdiğinden icrai bir suçtur, ihmali bir hareketle işlenemez²³².

Kişisel verilerin kaydedilmesi ile suç tamamlanmaktadır. Kaydetme fiilinin bir süre devam etmesi veya verilerin failin elinde bir süre durması gerekmediğinden, bu suç ani bir suçtur²³³. Suçun tamamlanması için herhangi bir neticenin gerçekleşmesi beklenmez. Bu nedenle kişisel verilerin kaydedilmesi suçu sırf hareket suçudur²³⁴. Yine suçun oluşması için kanuni tipte bir zarar meydana gelmesi aranmamaktadır. Bu nedenle soyut tehlike suçudur²³⁵.

²²⁹ www.tdk.gov.tr.

²³⁰ Hafızoğulları ve Özen, s. 288; Aydın, s. 131; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 587; Sert, s. 102.

²³¹ İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayınları, Ankara, 2019, s. 393; Akdağ, s. 100; Dülger, s. 317; Sert, s. 102; Kişisel verilerin kâğıt üzerine yazılmasının TCK madde 135 anlamında “kaydetmek” olarak değerlendirilemeyeceği yönündeki görüş için bkz. Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 587.

²³² Hafızoğulları ve Özen, s. 288; Sert, s. 104.

²³³ Akdağ, s. 97; Bük, s.150; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 588.

²³⁴ Sert, s. 105.

²³⁵ Dülger, s. 318; Karagülmez, s. 448; Bük, s. 150.

Suçu oluşturan hareketler kanunda özellikle belirtilmemiştir. Her ne şekilde olursa olsun kişisel verilerin kaydedilmesi ile suç oluşacağından, bu suç serbest hareketli bir suçtur²³⁶.

b. Tipikliğin Manevi Unsurları

Kişisel verilerin kaydedilmesi suçunda fail, kaydettiği verilerin kişisel veri olduğunu bilerek ve isteyerek bu eylemi gerçekleştirmesi gerektiğinden; bu suç kasten işlenebilen bir suçtur²³⁷. Failin kastının, kaydettiği verinin kişisel veri olduğunu bilmesi ve isteyerek bu eylemi gerçekleştirmesinin yanında, fiilin hukuka aykırı olduğunu da bilmesi gerekmektedir²³⁸. Kanuni tipte, failin amacına önem verilmediğinden, fiili bilinçli ve iradi olması yeterli görüldüğünden bu suç genel kast ile işlenebilir²³⁹.

Kanun'un gerekçesinde de belirtildiği üzere kural olarak kasten işlenebilen suçlar, olası kastla da işlenebilir²⁴⁰. Ancak Yargıtay Ceza Genel Kurulu'nun 12.11.2013 tarihli 2013/14-511 E. 2013/449 sayılı kararında 5237 sayılı TCK'nın bazı suç tanımlarında "hukuka aykırı olarak", "hukuka aykırı başka bir davranışla", "hukuka aykırı diğer davranışlarla", "hukuka aykırı yolla", "hukuka aykırı yollarla" gibi ifadelerle yer verildiğine, bu ifadelerin geçtiği suçlarda failin, işlediği fiilin hukuka aykırı olduğunu bilmesi, yani bu konuda doğrudan kastla hareket etmesi gerektiğine işaret edilmiştir²⁴¹. Kişisel verilerin kaydedilmesi suçu bakımından maddenin birinci fıkrasında ve ikinci fıkrasında belirtilen kişinin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin verilerine

²³⁶ Dülger, s. 317; Akdağ, s. 97; Sert, s. 104; Parlar, s. 1551; Hareketin önemine göre yapılan ayırmada hareketin şeklinin kanunda belirtilmiş olduğu bu sebeple suçun bağlı hareketli bir suç olduğu yönündeki aksi görüş için bkz. Özbek Kanbur, Doğan, Bacaksız ve Tepe, s. 587.

²³⁷ Karagülmez, s. 448; Akdağ, s. 105; Sert, s. 111; Korkmaz, s. 406.

²³⁸ Karagülmez, s. 448; Failin, izinsiz olarak mağdurun bilgisayarına girmek suretiyle bilgisayardaki verilere ulaşması ve bilgisayarın IP adresini öğrenmesi; kişisel verileri elde ederek kayıt altına alma yönünde kastının olmaması ve mağdurun kişisel verilerini bilgisayar ortamında veya kâğıt üzerinde kayda almamış olması sebebiyle TCK'nın 135. maddesinin ihlali sayılamayacaktır. Ersan Şen/Yasemin Yurttaş, **Bilgisayar Programları Karşısında Özel Hayatın Korunması**, Terazi Hukuk Dergisi, Y. 5, 2010, 29-44, s. 42.

²³⁹ Timur Demirbaş, **Ceza Hukuku Genel Hükümleri**, Seçkin Yayınları, Ankara, 2018, s. 387; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 595.

²⁴⁰ İzzet Özgenç, **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayınları, Ankara, 2017, s.242; Demirbaş, s. 379.

²⁴¹ www.yargitay.gov.tr; Özgenç, s. 301.

ilişkin olarak ayrıca hukuka aykırılık unsuruna yer verilmiştir. Bu bağlamda kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin olması haricinde suç olası kast ile işlenemeyecektir²⁴².

TCK'nın 22. maddesi gereği taksirle işlenen fiiller, kanunun açıkça belirttiği hallerde cezalandırılır. Kişisel verilerin kaydedilmesi suçunun taksirle işlenebileceği Kanunda öngörülmediğin suçun taksirle işlenmesi mümkün değildir²⁴³.

c. Suçun Hukuka Aykırılık Unsuru

Suçun oluşabilmesi için, eylemin hukuka aykırı olması gerekmektedir²⁴⁴. Diğer bir deyişle kural olarak tipe uygun olan eylem, herhangi bir hukuka uygunluk sebebinin bulunmaması halinde, aynı zamanda hukuka da aykırı olacaktır²⁴⁵. Kişisel verilerin kaydedilmesi suçu bakımından TCK'nın 135. maddesinin birinci fıkrasında ve ikinci fıkrasında belirtilen kişinin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin verilerine ilişkin olarak ayrıca hukuka aykırılık unsuruna yer verilmiştir. Madde metninde ayrıca hukuka aykırılık unsuruna yer verilmesi bakımından öğretide farklı görüşler mevcuttur. Bu görüşlerden ilki, madde metninde ayrıca “hukuka aykırılık” ibaresine yer verilmiş olması; “özel hukuka aykırılık” olarak adlandırılmakta ve bu durumda failin eyleminin tipe uygun olması eylemin hukuka aykırı olarak kabul edilebilmesi için yeterli görmemekte, ayrıca failin hukuka aykırı olarak hareket edip etmediğinin de araştırılması ve ispat edilmesi gerektiğini savunmaktadır²⁴⁶. İkinci bir görüş; bu tür ibarelerin gereksiz yere kullanıldığını; kanun koyucunun, hâkimleri, somut olayda hukuka uygunluk nedenlerinin bulunup bulunmadığı konusunda özellikle durması gerektiği yönündeki bir uyarısı olduğunu savunmaktadır²⁴⁷. Biz bu görüşlerden ilkinde katılmaktayız. Suç tanımlarında “hukuka aykırı olarak”, “hukuka aykırı başka bir davranışla”, “hukuka aykırı diğer davranışlarla”, “hukuka aykırı yolla”, “hukuka aykırı yollarla” gibi ifadelerle yer verildiği hallerde hukuka aykırılık, tipikliğin bir

²⁴² Sert, s. 112; Aksi yöndeki görüş için bkz.Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 595.

²⁴³ Dülger, s. 321; Korkmaz, s. 406.

²⁴⁴ Kayıhan İçel, Füsün Sokullu Akıncı, İzzet Özgenç, Adem Sözüer, Fatih s. Mahmutoglu ve Yener Ünver, **Suç Teorisi**, Beta Yayınları, 2000, s. 92.

²⁴⁵ İçel, Sokullu Akıncı, Özgenç, Sözüer, Mahmutoglu ve Ünver, s. 92.

²⁴⁶ Zafer, s. 110;Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 592; Bük, s. 161; Kuşkonmaz, s. 143.

²⁴⁷ Dülger, s. 321; Hakeri, s. 1125.

unsuru haline gelmektedir. Nitekim Yargıtay 12. Ceza Dairesi'nin 26.12.2017 tarihli 2016/9759 E. 2017/10938 sayılı kararında da somut olay bakımından sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun ayrıca tespitini aramaktadır²⁴⁸.

Suçun hukuka uygunluk nedenlerinden ilki kişinin rızasının bulunmasıdır²⁴⁹. Maddenin gerekçesinde kişinin rızasının bulunması, verilerin kayda alınmasının kanundan kaynaklandığı hallerde söz konusu suçun oluşmayacağı açıklanmıştır. Rızanın şekli konusunda bir düzenleme bulunmamakla birlikte suç bakımından rızanın hukuka uygunluk sebebi olarak kabul edilebilmesi için kişinin "açık rıza" beyanında bulunması gerekir²⁵⁰. Ayrıca bir hakkın kullanılması ya da bir kanun hükmünün yerine getirilmesi sırasında kişisel verilerin kayda alınması suç teşkil etmez²⁵¹. Kişisel Verilerin Korunması Kanunu'ndan kaynaklanan hukuka uygunluk sebeplerinin de değerlendirilmesi gerekmektedir.

4. Suçun Nitelikli Hali

TCK'nın 137. maddesinde özel hayata ve hayatın gizli alanlarına karşı suçlar bölümünde yer alan suçların cezayı arttırıcı nitelikli halleri öngörülmüştür. Maddeye göre:

"Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi halinde, verilecek ceza yarı oranında artırılır."

Suçun nitelikli hallerinden ilki suçun failinin kamu görevlisi olmasıdır. TCK anlamında kamu görevlisi; kamusal faaliyetin yürütülmesine atama veya seçilme

²⁴⁸ www.yargitay.gov.tr; Aynı yönde kararlar için bkz. Yargıtay 12. Ceza Dairesi 21.12.2016 T. 2015/10737 E. 2016/ 13557 K., Yargıtay 12. Ceza Dairesi 14.12.2016 T. 2016/9332 E. 2016/ 13355 K.

²⁴⁹ Bük, s. 151; İşletmelerin, çalışanın rızasına dayalı işyeri uzantılı e-postalarının denetlenmesi hem özel hayatın gizliliğinin ihlal suçu bakımından hem de kişisel verilerin kaydedilmesi suçu bakımından hukuka uygunluk nedeni sayılacaktır. Durmuş Tezcan, **Özel Hayatın Gizliliğini İhlal ve Kişisel Verilerin Kaydedilmesi Suçu İle İlgili Bazı Gözlemler**, İÜHFM, C. LXXI, s. 1, 2013, s. 1159-1164, s. 1164.

²⁵⁰ Akdağ, s. 116; Bük, s. 151; Korkmaz, s. 412.

²⁵¹ Parlar, s. 1551; Sert, s. 115; Korkmaz, s. 413.

yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişidir (TCK m.6). Ancak 135. maddenin lafzından da anlaşılacağı üzere suçun kamu görevlisinin görevinin verdiği yetkiyi kötüye kullanmak suretiyle işlenmiş olması gerekir.

Madde ile düzenlenen bir diğer nitelikli hal suçun belirli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmiş olmasıdır. Failin mesleği konusunda bir belirleme yapılmamıştır. Bu bakımdan örneğin doktorların hastaların verilerine, banka çalışanının müşteriilerinin verilerine kolaylıkla erişmesi ve hukuka aykırı olarak verileri kaydetmesi mümkündür²⁵².

TCK'nın 137. maddesinde belirtilen nitelikli hallerin dışında 135. maddenin 2. fıkrasında sayılan özel nitelikli verilerin hukuka aykırı olarak kaydedilmesi halinde 135. maddenin 1. fıkrasına göre verilecek ceza yarı oranında arttırılacağı öngörülmüştür. Madde ile kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin verileri özel olarak koruma altına alınmıştır. Sayılan veri kategorilerinden anlaşılacağı üzere bu veriler KVKK ile tanımlanan özel nitelikli hassas verilerdir. Ancak iki Kanun arasında özel nitelikli veri kategorileri arasında farklılık bulunduğundan uygulamada yaşanacak tereddütlerin giderilmesi için bu konuda bir uyumlaştırma çalışmasına ihtiyaç duyulmaktadır.

5. Suçun Neticesi Sebebiyle Ağırlaşmış Hali

Neticesi sebebiyle ağırlaşmış suçlar, failin eyleminin daha ağır bir neticeye sebep vermesi durumunda faile verilecek cezanın arttırılması gereken suçlardır²⁵³. Kişisel verilerin kaydedilmesi suçunun neticesi sebebiyle ağırlaşmış hali Kanunda düzenlenmemiştir.

²⁵² Sert, s. 111.

²⁵³ Demirbaş, s. 405.

6. Teşebbüs

Kişisel verilerin kaydedilmesi suçu, kişisel verilerin kaydedilmesi ile tamamlanır. Bu bakımdan fail, suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamaz ise veya elinde olmayan nedenlerle kişisel verileri kaydetme neticesinin gerçekleşmemesi halinde teşebbüsten dolayı sorumlu tutulur²⁵⁴. Ancak failin kişisel verileri kaydetmek için hazırlık hareketleri cezalandırılmaz²⁵⁵.

7. İştirak

TCK'nın 37 ve devamı maddelerinde yer alan suça iştirak hükümleri kişisel verilerin kaydedilmesi suçu bakımından da uygulanacaktır. Suça iştirak edenlerin kamu görevlisi olması ya da bir meslek veya sanat sahibi olması halinde haklarında verilecek ceza TCK m.137 gereğince arttırılacaktır.

8. İçtima

Kişisel verilerin kaydedilmesi suçunu içtima yönünden Kanun'un sistematigi dikkate alınarak zincirleme suç, aynı neviden fikri içtima ve farklı neviden fikri içtima hükümleri yönünden değerlendirmekte fayda olacaktır.

TCK'nın 43. maddesinde birinci fıkrasında zincirleme suç bakımından “Bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda, bir cezaya hükmedilir. Ancak bu ceza, dörtte birinden dörtte üçüne kadar artırılır.” hükmüne yer verilmiştir. Kişisel verilerin kaydedilmesi suçunun failinin de bir suç işleme kararının icrası kapsamında değişik zamanlarda bir kişiye karşı birden fazla işlenmesi durumunda TCK'nın 43. maddesi gereği zincirleme suç hükümleri uygulanacaktır. Fail hakkında tek bir cezaya hükmedilecekse de verilecek ceza, dörtte birinden dörtte üçüne kadar arttırılacaktır.

²⁵⁴ Dülger, s. 344; Kuşkonmaz, s. 147.

²⁵⁵ Hafızogulları ve Özen, s. 288.

Failin tek bir hareketle birden fazla kişinin kişisel verilerini kaydetmesi durumunda aynı neviden fikri içtima hükümleri uygulanacaktır²⁵⁶. TCK'nın 43/2 maddesinin uygulanacağı bu halde fail hakkında tek bir cezaya hükmedilecekse de verilecek ceza, dörtte birinden dörtte üçüne kadar arttırılacaktır.

İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi hakkında TCK'nın 44. maddesi gereğince farklı neviden içtima hükümleri uygulanacaktır. Fail, en ağır cezayı gerektiren suçtan dolayı cezalandırılacaktır. Kişisel verilerin kaydedilmesi suçunun düzenlendiği bölüm bakımından TCK'nın 132. maddesinde yer alan “haberleşmenin gizliliğini ihlal”, 133. maddesinde yer alan “kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması”, 134. maddesinde yer alan “özel hayatın gizliliğini ihlal”, 136. maddesinde yer alan “verileri hukuka aykırı olarak verme veya ele geçirme” suçlar ile 243. maddesinde yer alan “bilgi sistemine girme”, 244. maddesinde yer alan “sistemi engelleme, bozma, verileri yok etme veya değiştirme” suçu bakımından içtima problemi ortaya çıkabilecektir.

TCK'nın 132/1 maddesi “Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.” şeklinde düzenlenmiştir. Kişisel arasındaki haberleşmenin gizliliğinin haberleşme içeriklerinin kayda alınması suretiyle işlenmesi sırasında kaydedilen haberleşme içeriklerinin arasında kişisel verilerin de bulunması halinde hem 132. madde hem de 135. madde dolayısıyla cezai sorumluluğu doğacaktır. Bu durumda fail hakkında farklı neviden fikri içtima hükümleri uygulanarak, en ağır cezayı gerektiren suçtan cezalandırılması gerekir²⁵⁷.

TCK'nın 133/1 fıkrasında kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleme veya bunları bir ses alma cihazı ile kaydetme suç olarak düzenlenmiştir. Failin aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın ses alma cihazı ile kaydetmesi esnasında kişisel verilerin de kayda alması halinde kişisel verilerin kaydedilmesi suçu bakımından da sorumluluğu doğacaktır. Yine 133/2 maddesi

²⁵⁶ Zincirleme suç hükümlerinin uygulanamayacağı, kişi sayısınca suç oluşacağı yönündeki görüş için bkz. Nil Melek Gültekin, **Kişisel Verilerin Ceza Hukuku Yönünden Korunması** (Yayınlanmamış Yüksek Lisans Tezi), Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2012, s. 151'deki 438. dn. yazarlar; Sert, s. 129.

²⁵⁷ Gültekin, s. 152; Sert, s. 130.

gereğince katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi de aynı zamanda kişisel verilerin kaydedilmesi suçunu işlemiş olacaktır. Her iki halde de farklı neviden fikri içtima hükümleri uygulama alanı bulacaktır²⁵⁸.

TCK'nın 134/1 maddesi “Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.” şeklinde düzenlenmiştir. Özel hayatın gizliliğinin, görüntü veya seslerin kayda alınması suretiyle işlenmesi durumunda fail hakkında kişisel verilerin kaydedilmesi suçuna ilişkin hükümlerin mi özel hayatın gizliliğini ihlal suçuna ilişkin hükümlerin mi uygulanacağı yönünde yaşanacak tereddütte; kanımızca her ne kadar ses ve görüntü de kişisel veri kabul edilecekse de korunan hukuki değer irdelendiğinde kişisel verilerin kaydedilmesi suçunun değil, özel hayatın gizliliğini ihlal suçunun olduğu kabul edilmelidir²⁵⁹.

²⁵⁸ Gültekin, s. 152; Sert, s. 130.

²⁵⁹ Parlar, s. 1551; Gültekin, s. 154; Dülger, s. 345; Yargıtay kararlarında da benzer hususa açıklık getirilmiştir. Yargıtay 12. Ceza Dairesi 11.9.2012 T. 2012/17703 E. 2012/18222 K. “Bir özel hayat görüntüsü ya da sesinin, “kişisel veri” olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi eyleminin, 5237 sayılı TCK'nın 134/1. maddesinin 2. cümlesinde tanımlanan özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilmesi gerektiği, kişinin özel hayatına ilişkin görüntü, fotoğraf ya da sesin, 5237 sayılı TCK'nın 135. maddesi kapsamında kişisel veri olarak kabul edilemeyeceği iddiaya konu olayda, mağdurenin çıplak vaziyetteki görüntü ve fotoğraflarının kaydedilmesinden ibaret eylemin, “Kişisel verilerin kaydedilmesi” suçunu oluşturmayacağı, çekimin, mağdurenin bilgisi ve rızası kapsamında gerçekleşmesi nedeniyle, özel hayatın gizliliğini ihlal suçunun da oluşmadığı anlaşıldığından, yapılan yargılama sonucunda, sanığa yüklenen suçun yasal unsurlarının oluşmadığı gerekçeleri gösterilerek mahkemece kabul ve takdir kılınmış olduğundan, katılan vekili ile C.Savcısının sanığa atılı suçun sabit olduğuna ilişkin ve yerinde görülmeyen tüm temyiz itirazlarının reddiyle, 5271 sayılı CMK'nın 223/9. maddesi de nazara alınarak, hükmün isteme uygun olarak ONANMASINA” karar verilmiştir. Aynı yöndeki bir başka kararında “bir özel hayat görüntüsü ya da sesinin, “kişisel veri” olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi TCK'nın 134/1. maddesinin 2. cümlesinde; rızası dışında ifşa edilmesi; yani, yayılması, açığa vurulması, afişe edilmesi, ilan edilmesi, kamuoyuna duyurulması, aleniyet kazandırılması, özetle; içeriğini öğrenme yetkisi bulunmayan kişi veya kişilerin bilgisine sunulması TCK'nın 134/2. maddesinde özel hayatın gizliliğini ihlal suçu kapsamında düzenlendiğinden, kişinin özel hayatına ilişkin görüntüsü, fotoğrafı ya da sesi, yasal anlamda, TCK'nın 135. maddesi kapsamında kişisel veri olarak değerlendirilemez.” şeklinde hüküm kurulmuştur. Yargıtay 12. Ceza Dairesi 17.02.2014 T. 2013/9669 E. 2014/3760 K. Daha yeni tarihli bir diğer kararında “Sanıkların, mağdurla arkadaşlık kurdukları ve mağdurun, internet ortamından rızası ile gönderdiği çıplak fotoğraflarını flash diske kaydedip, babası ...'e vermek suretiyle ifşa ettiklerinin iddia edildiği olayda; mağdurun, cinsel ve fiziksel mahremiyetine ilişkin çıplak görüntüleri kişisel veri kapsamında değerlendirilemeyeceğinden, eylemin, kişisel verilerin kaydedilmesi suçunu değil, TCK'nın 134/1. maddesinin 2. cümlesi ve 134/2.

TCK'nın 136. maddesinde kişisel verileri hukuka aykırı olarak verme veya ele geçirme suç olarak düzenlenmiştir. Kişisel verilerin ele geçirilmesi, verilerin hukuka aykırı olarak kaydedilmesi suretiyle gerçekleştirilmişse fail hakkında gerçek içtima hükümleri uygulanarak hem TCK'nın 135. maddesi hem de TCK'nın 136. maddesi gereğince ayrı ayrı ceza verilmesi gerekmektedir²⁶⁰.

TCK'nın 122. maddesinde dil, ırk, milliyet, renk, cinsiyet, engellilik, siyasi düşünce, felsefi inanç, din veya mezhep farklılığından kaynaklanan nefret nedeniyle bir kişinin maddede sayılan haklarını engellemek suç olarak düzenlenmiştir. TCK'nın 135/2 maddesi gereği kaydedilen bilgilerin aynı zamanda TCK'nın 122. maddesi gereği “nefret ve ayrımcılık” suçunu oluşturması halinde gerçek içtima hükümleri uygulanarak hem TCK'nın 135. maddesi hem de TCK'nın 122. maddesi gereğince ayrı ayrı ceza verilmesi gerekmektedir²⁶¹.

TCK'nın 243. maddesinde bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme veya orada kalmaya devam etme suç olarak düzenlenmiştir. Failin, kaydetmek istediği kişisel verilerin bir bilişim sisteminde kayıtlı olması durumunda failin önce bilişim sistemine girmesi daha sonra kişisel verileri kaydetmesi gerekecektir. Bu durumda doktrinde bir kısım yazarlarca failin, kişisel verileri kaydetmek için bilişim sistemine girme zorunluluğundan hareketle kişisel verilerin kaydedilmesi suçunun geçitli suç olduğunu savunulmaktaysa da; biz kişisel verilerin kaydedilmesi için mutlaka bir bilişim sistemine girme zorunluluğunun olmaması ve her iki düzenleme ile farklı hukuki değerlerin koruma altına alınmış olması sebebiyle gerçek içtima hükümlerinin uygulanarak failin her iki suç nedeniyle ayrı ayrı cezalandırılması gerektiği yönündeki diğer görüşe katılmaktayız²⁶².

TCK'nın 244/2 maddesinde “sisteme veri yerleştirme” ifadesiyle sistemin maliki veya ilgisinden izin almaksızın sisteme veri kaydedilmesi, yüklenilmesi veya eklenmesi kastedilmektedir²⁶³. Bir başka deyişle sisteme veri yerleştirme ile 135.

maddesine uyan özel hayatın gizliliğini ihlal suçlarını oluşturacağı” yönünde değerlendirme yapılmıştır. Yargıtay 12. Ceza Dairesi 19.01.2015 T. 2014/11530 E. 2015/584 K.; Parlar, s. 1551

²⁶⁰ Bük, s. 137; Parlar, s. 1551; İtişgen, s. 197.

²⁶¹ Parlar, s.1551.

²⁶² Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, Seçkin Yayınları, Ankara, 2018, s. 299; Sert, s. 132; Aksi yöndeki görüş için bkz. Gültekin, s. 154.

²⁶³ Ali Parlar, **Türk Ceza Hukukunda Bilişim Suçları**, Bilge Yayınevi, Ankara, 2015, s. 43.

madde anlamında kişisel verilerin kaydedilmesi aynı anlama gelmektedir²⁶⁴. 135. maddede düzenlenen suçun konusunu ancak kişisel veriler olabileceken 244. maddede düzenlenen suçun konusu her türlü veri olabilir. Yine 135. madde anlamında kişisel verilerin kaydedilmesi bakımından daha önce de açıkladığımız üzere kişisel verilerin hukuka aykırı olarak bilişim sistemi dışında da bir yere kaydedilmiş olması halinde de suç oluşacaktır. Ancak 244. madde verilerin sadece bir bilişim sistemine yerleştirilmesi durumunda uygulama alanı bulacaktır. Bu nedenle somut olayın özelliğine göre her iki madde arasında özel norm- genel norm ilişkisinin araştırılması gerekmektedir²⁶⁵.

9. Yaptırım ve Kovuşturma Usulü

Kişisel verileri hukuka aykırı olarak kaydeden kişi bir yıldan üç yıla kadar hapis cezası ile cezalandırılacaktır. Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda verilecek ceza yarı oranında artırılır.

TCK'nın 139. maddesinde belirtildiği üzere suçun soruşturulması veya kovuşturması şikâyetle bağlı değildir. 5235 sayılı Kanun gereğince davaya bakmakla görevli mahkeme Asliye Ceza Mahkemesidir.

Bu suç bakımından dava zamanaşımı süresi TCK'nın 66/1 maddesi gereğince sekiz yıl olarak öngörülmüştür. Ceza zamanaşımı süresi ise TCK'nın 68/1 maddesi gereğince on yıldır.

B. Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu TCK m. 136

1. Suç Tipi Hakkında Genel Bilgiler

²⁶⁴ Dülger, s. 344; Sert, s. 133.

²⁶⁵ Dülger, s. 344; Aydın, s. 164.

TCK'nın 136. maddesinde “kişisel verileri hukuka aykırı olarak verme veya ele geçirme” suçu “Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.” şeklinde düzenlenmiştir. Maddenin gerekçesinde kişisel verilerin hukuka uygun olarak kaydedilmiş olsun veya olmasın, hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç tipi olarak tanımlandığı açıklanmıştır. Bu itibarla kişisel veriler hukuka uygun olarak kaydedilmiş olsa dahi kaydedilen verileri hukuka aykırı olarak başkasına veren, yayan veya ele geçiren kişi hakkında 136. madde hükümleri uygulama alanı bulacaktır.

2. Suçla Korunan Hukuki Değer

Suçla korunan hukuki değer Kanun'un 135. maddesinde olduğu gibi genel olarak özel hayat ve özel hayatın gizli alanları²⁶⁶, özel olarak kişisel verilerdir²⁶⁷. Tekrara düşmemek adına kişisel verilerin kaydedilmesi suçu bakımından suçla korunan hukuki değer başlığı altında yapmış olduğumuz ayrıntılı açıklamalara bakılmalıdır.

3. Suçun Unsurları

a. Tipikliği Maddi Unsurları

1 Fail

TCK'nın 136. maddesine göre suçun faili, kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişidir. Madde metninde fail bakımından “kimse” ibaresi kullanıldığından suçun faili herkes olabilir²⁶⁸. Ancak TCK'nın 20. maddesine göre suçun faili tüzel kişiler olamayacaksa da TCK m.140

²⁶⁶ Karagülmez, s. 451; Parlar, s. 1554; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 596.

²⁶⁷ Soyaslan, s. 353; Dülger, s.346; Yargıtay Ceza Genel Kurulu'nun 04.07.2017 T. 2017/829 E. 2017/363 K. (www.yargitay.gov.tr).

²⁶⁸ Hafızoğulları ve Özen, s. 289; Yılmaz, s.268; Dülger, s. 347; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 597.

gereğince haklarında güvenlik tedbirleri uygulanır²⁶⁹. Failin kamu görevlisi olması ve görevinin verdiği yetkiyi kötüye kullanmak suretiyle bu suç işlenmesi halinde TCK madde 137 gereğince verilecek ceza yarı oranında arttırılacaktır. Yine aynı maddede failin belirli bir meslek veya sanatın sağladığı kolaylıktan yararlanan kişi olması halinde yine cezanın yarı oranında arttırılması öngörülmüştür.

2 Mağdur

TCK'nın 136. maddesinde düzenlenen suç bakımından, suçun mağduru konusunda maddede herhangi bir özellik belirtilmemiştir. Bu sebeple kişisel verileri hukuka aykırı olarak bir başkasına verilen, yayılan veya ele geçirilen herkes suçun mağduru olabilir²⁷⁰. Tüzel kişilerin suçun mağduru olup olamayacağına ilişkin madde gerekçesinde bir açıklama bulunmamaktadır. Ancak daha önce de belirttiğimiz gibi TCK'nın gerekçesinde yer verilen kişisel veriye ilişkin tanım ile KVKK birlikte değerlendirildiğinde bu suç bakımından da tüzel kişiler ancak suçtan zarar gören olabilecektir²⁷¹.

3 Suçun Konusu

Suçun konusunu kişisel veriler oluşturmaktadır²⁷². Kişisel verilerin kaydedilmesi suçunun konusuna ilişkin yapmış olduğumuz açıklamalar bu suç bakımından da geçerlidir. TCK'nın 136. maddesinin; ceza mevzuatında kişisel verilerle ilgili bir tanım ve sınırlandırma yapılmaması, suçta ve cezada kanunilik ve belirlilik ilkelerine ve Anayasa'nın 38. maddesine aykırı olduğu ileri sürülerek iptaline karar verilmesi istenmişse de daha önce ayrıntılı olarak incelemiş olduğumuz Anayasa Mahkemesi 12.11.2015 T. 2015/32 E. 2015/102 sayılı kararı ile yapılan itirazın reddine karar verilmiştir.

²⁶⁹ Hafızoğulları ve Özen, s. 289; Soyaslan, s. 353; Sert, s. 141.

²⁷⁰ Hafızoğulları ve Özen, s. 290; Dülger, s. 347; Parlar, s. 1555; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 597.

²⁷¹ Hafızoğulları ve Özen, s. 290; Sert, s. 141.

²⁷² Dülger, s.347; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s.596; Yargıtay 12. Ceza Dairesi 06.04.2016 T. 2016/2168 E. 2016/5860 K. (www.yargitay.gov.tr); Suçun konusunun kişisel verilerin korunmasına ilişkin ferdi- kamusal yarar olduğuna ilişkin görüş için bkz. Hafızoğulları ve Özen, s. 290.

4 Hareket Eylem, Fiil

Suçun maddi unsurunu oluşturan hareket, kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirmediir. Suç seçimlik hareketli bir suçtur²⁷³. Kanun ile belirlenen seçimlik hareketler; kişisel verileri hukuka aykırı olarak bir başkasına verme, yayma ve ele geçirmediir. Seçimlik hareketlerden birinin, birden fazlasının veya tamamının gerçekleşmesi halinde suç oluşacaktır. Seçimlik hareketlerden birkaçının veya tamamının gerçekleşmesi halinde birden fazla suç işlenmiş olmayacak, tek bir suç işlenmiş olarak kabul edilecektir.

Seçimlik hareketlerden ilki “vermek” eylemi; “Üzerinde, elinde veya yakınında olan bir şeyi birisine eriştirmek, iletmek” anlamına gelmektedir²⁷⁴. Kişisel verilerin verildiği kişi mağdur dışında, gerçek veya tüzel kişi olabilir²⁷⁵. TCK’nın 136. maddesinde ve madde gerekçesinde kişisel verilerin bir başkasına verilmesine ilişkin bir hareket belirlenmediğinden kişisel veriler bir başkasına elden verilebileceği gibi posta ya da internet üzerinden elektronik posta ile vb. şekillerde verilebilecektir²⁷⁶. Failin kişisel verileri bir başkasına verebilmesi için öncelikle verileri elinde bulundurması gerekir²⁷⁷. Doktrinde kişisel verilerin sözlü olarak aktarılmasının verme eylemi sayılıp sayılmayacağı hususu tartışmalıdır. Bu görüşlerden ilki göre suçun seçimlik hareketi bakımından kişisel verilerin verilmesinden söz edebilmek için mutlaka bir vasıtanın olması gerektiği bu bağlamda kişisel verilerin sözlü olarak aktarılmasının verme eylemini oluşturmayacaktır²⁷⁸. Biz

²⁷³ Küzeci, s. 410; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 597; Dülger, s.347.

²⁷⁴ www.tdk.gov.tr; CMK’nın 80/1 maddesine göre Kanun’un 75, 76 ve 78 inci madde hükümlerine göre bir suça ilişkin delil elde etmek amacıyla sanık, şüpheli veya diğer kişilerin vücutlarında iç veya dış beden muayenesi ile vücutlarından kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi alınan örnekler, alınan örnekler üzerinde yapılan moleküler genetik incelemeler sonucunda elde edilen veriler, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez. Bu verilerin hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme TCK’nın 136. maddesi kapsamında suç sayılacaktır.

²⁷⁵ Karagülmez, s. 451; Dülger, s. 351.

²⁷⁶ Yargıtay Ceza Genel Kurulu 04.07.2017 T. 2017/829 E. 2017/363 K.; Kişisel verilerin hukuka aykırı olarak bir başkasına posta yoluyla gönderilmesinin TCK. 136. maddesi gereğince suç teşkil edeceğine dair bkz. Yargıtay 11. Ceza Dairesi’nin 10.07.2017 T. 2015/8796 E. 2017/5266 K (www.yargitay.gov.tr); Karagülmez, s. 451; Dülger, s. 350.

²⁷⁷ Hafizoğulları ve Özen, s. 290.

²⁷⁸ Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s.598; Gökcan, s. 819.

kişisel verilerin sözlü veya yazılı olarak aktarılmasının da verme eylemini oluşturabileceği yönündeki diğer görüşe katılmaktayız²⁷⁹.

TCK'nın 136. maddesinde yer verilen ikinci seçimlik hareket olan “yaymak” eylemi; birçok kimseye duyurmak.” anlamına gelmektedir²⁸⁰. Kişisel verilerin yayılması, kişisel verilerin mektup veya elektronik posta ya da kısa mesaj ile gönderilmesi, internet üzerinde erişilir kılınması, web sitede yayınlanması, bir forumda veya basında açıklanması gibi çeşitli şekillerde gerçekleştirilebilir²⁸¹. “Yaymak” eyleminin tanımından hareketle kişisel verilerin yayılmasından söz edebilmek için verilerin birden çok kişinin bilgisine sunulması şeklinde bir sonuca varılabilecekse de, verilerin bir kişinin dahi bilgisine sunulması suçun oluşması bakımından yeterli olacaktır²⁸².

Son olarak kişisel verilerin ele geçirilmesi; hukuka aykırı olarak kişisel verilerin sahibi olmak, onları elde etmek ve temin etmektir²⁸³. Kişisel verilerin ele geçirilmesi çok farklı şekillerde mümkündür. Yargıtay Ceza Genel Kurulu'nun 04.07.2017 T. 2017/829 E. 2017/363 sayılı kararında başkasının hâkimiyet alanında bulunan kişisel verinin, failin hakimiyeti altına girmesi ile kişisel verilerin ele geçirilmiş olacağı, kişisel verilerin ele geçirilmesinin ise verilerin kayıtlı olduğu belgelerin alınması ya da kayıtlı olduğu bilişim sisteminden ele geçirilmesi gibi çeşitli şekillerde gerçekleştirilebileceği açıklanmıştır²⁸⁴.

Suçun oluşumu bakımından madde hükmünde kaydedilmiş olma şartının aranmaması ve kişisel verilerin kaydedilmesinin Kanun'da ayrı bir suç olarak tanımlanmış olması sebebiyle kişisel verilerin verilmesi, yayılması veya ele geçirilmesinden önce kaydedilmiş olması gerekli değildir²⁸⁵. Ancak kişisel verilerin kaydedilmiş olması zorunlu değil ise de kaydedilme dışında öğrenilmesi, hafızada

²⁷⁹ Sevik, s. 798.

²⁸⁰ www.tdk.gov.tr.

²⁸¹ YCGK 04.07.2017 T. 2017/829 E. 2017/363 K. (www.yargitay.gov.tr); Karagülmez, s. 452; Dülger, s. 352; Soyaslan, s. 353; Sert, s. 139; Elektronik mühendisi olan sanığın, teknik servis elemanı olarak çalıştığı tıp merkezinde Corteks isimli bilgi sistemine psikiyatri anabilim dalında tedavi gören hemşire olan mağdurenin muayene bilgilerini okuyarak hastanede çalışanlara ifşa etmesi eyleminin TCK'nın 136. maddesi kapsamında suç teşkil ettiğine ilişkin bkz. Yargıtay 12 Ceza Dairesi'nin 05.06.2012 T. 2012/13104 E. 2012/14146 K. (www.corpus.com.tr).

²⁸² Dülger, s. 352.

²⁸³ Hafızogulları ve Özen, s. 290; Sert, s. 139.

²⁸⁴ www.yargitay.gov.tr

²⁸⁵ Dülger, s. 348; Kişisel verilerin kaydedilmiş halde bulunması, kaydedilmiş haliyle başkalarına verilmesi, yayılması ya da ele geçirilmesi gerektiği yönündeki aksi görüşler için bkz. Yargıtay 12. Ceza Dairesi 21.12.2016 T. 2015/10737 E. 2016/13557 K. (www.yargitay.gov.tr); Ketizmen, s. 240.

tutulan kişisel verilerin başkalarına açıklanması, kişisel verilere salt duyu organları aracılığıyla vakıf olunması TCK'nın 136. maddesi kapsamında değerlendirilemeyecektir²⁸⁶. Kişisel verilerin verilmesinde, yayılmasından veya ele geçirilmesinden önce kaydedilmiş olması halinde TCK'nın 136. maddesinin gerekçesinde de belirtildiği üzere verilerin hukuka uygun olarak kaydedilip kaydedilmemesinin bir önemi yoktur²⁸⁷. Kişisel verilerin hukuka uygun olarak kaydedilmiş olduğu hallerde de seçimlik hareketlerden birinin gerçekleşmesi halinde suçun meydana gelmesi mümkündür²⁸⁸.

Suç, icrai hareketlerle işlenecektir²⁸⁹. Kişisel verilerin verilmesi, yayılması veya ele geçirilmesi ile suç tamamlanmış olacağından sırf hareket suçudur²⁹⁰. Yine suçun tamamlanması bakımından bir zararın gerçekleşmesi gerekmediğinden bu suç soyut tehlike suçudur²⁹¹.

b. Tipikliğin Manevi Unsurları

Kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi suçu bakımından fail, mağdura ait verilerin kişisel veri olduğunu ve yaptığı eylemin hukuka aykırı olduğunu bilerek ve isteyerek kişisel verileri bir başkasına verme, yayma veya ele geçirme eylemlerinden en az bir tanesini gerçekleştirmesi gerekir²⁹². Dolayısıyla fail, bu eylemleri bilerek ve isteyerek gerçekleştirdiğinden; bu suç kasten işlenebilen bir suçtur²⁹³. Kanuni tipte, failin amacına önem verilmediğinden, fiili bilinçli ve iradi olması yeterli görüldüğünden bu suç genel kast ile işlenebilir²⁹⁴. TCK'nın 22. maddesi gereği taksirle işlenen fiiller, kanunun açıkça belirttiği hallerde cezalandırılır. Verileri hukuka aykırı olarak verme

²⁸⁶ Yargıtay 12. Ceza Dairesi 06.04.2016 T. 2016/2168 E. 2016/5860 K.; Yargıtay 12. Ceza Dairesi 21.12.2016 T. 2015/10737 E. 2016/13557 K.; Dülger, s. 349.

²⁸⁷ Hafızoğulları ve Özen, s. 290; Dülger, s. 353.

²⁸⁸ Dülger, s. 348; Korkmaz, s. 456; Rezzan İtişgen, **Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu**, TADD, Yıl:6, Sayı:23 (Ekim 2015), 179-202, s. 187.

²⁸⁹ Hafızoğulları ve Özen, s. 290; Suçun “yayma” eylemi bakımından ihmali hareketle de işlenebileceği yönündeki görüş için bkz. Gültekin, s. 164; Sert, s. 140.

²⁹⁰ Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 598.

²⁹¹ Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 598; Akdağ, s. 129; Bük, s. 158.

²⁹² Soyaslan, s. 355.

²⁹³ Hafızoğulları ve Özen, s.291; Dülger, s. 354; Gültekin, s. 166.

²⁹⁴ Gültekin, s. 166.

veya ele geçirme suçunun Kanunda taksirle işlenebileceği öngörülmediğin suçun taksirle işlenmesi mümkün değildir²⁹⁵.

TCK'nın 136. maddesinde özel olarak “hukuka aykırılık” unsuru arandığından suç olası kast ile işlenemeyecektir²⁹⁶.

c. Suçun Hukuka Aykırılık Unsuru

TCK'nın 136. maddesi bakımından madde hükmünde özel olarak “hukuka aykırılık” unsuruna yer verilmiştir. Bu hali ile daha önce de açıkladığımız üzere “hukuka aykırılık” tipikliğin bir unsuru haline dönüşmektedir. Dolayısıyla failin eylemlerinin hukuka aykırı olduğunu bildiği ve istediğinin özel olarak araştırılması gerekecektir.²⁹⁷ Nitekim Yargıtay 12. Ceza Dairesi'nin 08.02.2017 T. 2015/12942 E. 2017/874 sayılı kararına konu olayda da sanıkların hukuka aykırılık bilinciyle hareket ettikleri özel olarak değerlendirilmiştir²⁹⁸.

Hukuka uygunluk nedeni olarak ilgilinin rızasının bulunduğu hallerde²⁹⁹, bir hakkın kullanılması ya da kanun hükmünün yerine getirilmesi sırasında kişisel verilerin bir başkasına verilmesi, yayılması veya ele geçirilmesi suç teşkil etmeyecektir³⁰⁰.

4. Suçun Nitelikli Hali

²⁹⁵ Dülger, s.354.

²⁹⁶ Gültekin, s. 166; Aksi yöndeki görüşler için bkz. Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 599; Gökcan, s. 822.

²⁹⁷ Gültekin, s. 167.

²⁹⁸ “katılan ...'ın, işyerinde kendisine tahsis edilen bilgisayarı açıp, daha önce aynı işyerinden çıkarılan bir arkadaşı ile facebook üzerinden mesajlaşırken, facebook hesabını ve bilgisayarı kapatmayı unutup bilgisayarın yanından ayrılmasının ardından gelen mesaj seslerinin gürültüsünden rahatsız olan ve katılan ile aynı işyerinde çalışan sanık ...'ın, bilgisayarı kapatmak istediği esnada, katılan ile arkadaşının birbirlerine gönderdikleri mesajlarda, kendisine, annesine, personel amiri olan diğer sanık ...'e ve bir başka işyeri arkadaşına hakaret içeren ibarelerin yazılı olduğunu gördüğü ve çıktısını aldığı katılana ait facebook mesajlarını personel amiri olan diğer sanık ...'e verdiği, bunun üzerine işten çıkarılan katılan tarafından iş mahkemesinde açılan alacak davasında, söz konusu facebook mesajlarının katılanın tarafı olduğu iş akdinin haklı nedenle fesh edildiğinin kanıtı olarak mahkemeye sunulduğu olayda” sanıklara yüklenen fiillerin kanunda suç olarak tanımlanmamış olması nedeniyle sanıkların CMK'nın 223/2-a maddesi gereğince beraatlerine karar verilmesi gerektiğine karar verilmiştir (www.yargitay.gov.tr); Sert, s. 145.

²⁹⁹ Suçun şikâyeteye bağlı olmaması sebebiyle ilgilinin rızasının fiili hukuka uygun hale getirmeyeceği yönündeki aksi görüş için bkz. Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 599.

³⁰⁰ Dülger, s. 354; Soyaslan, s. 355; Parlar, s. 1555.

Suçun nitelikleri halleri TCK'nın 137. maddesinde öngörülmüştür. Buna göre kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek suçu bakımından; suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, verilecek ceza yarı oranında artırılır.

5. Suçun Neticesi Sebebiyle Ağırlaşmış Hali

TCK'nın 136. maddesinde düzenlenen suç bakımından neticesi sebebiyle ağırlaşmış hali Kanunda suç olarak düzenlenmemiştir.

6. Teşebbüs

TCK'nın 136. maddesi bakımından suçu oluşturan eylemlerin bölünebilmesi halinde suça teşebbüs mümkündür.³⁰¹

7. İştirak

TCK'nın suça iştirak hükümleri “verileri hukuka aykırı olarak verme veya ele geçirme” suçu bakımından da uygulanacaktır. Suça iştirak edenlerin kamu görevlisi olması ya da bir meslek veya sanat sahibi olması halinde haklarında verilecek ceza TCK m.137 gereğince arttırılacaktır³⁰².

³⁰¹ Dülger, s. 356; Gültekin, s. 169; Akdağ, s. 139; Korkmaz, s. 474; Hasan Gerçekler, **Yorumlu Uygulamalı Türk Ceza Kanunu**, C.1, Seçkin Yayınları, Ankara, 2017, s. 1376; Yargıtay, sanığın diğer suç ortaklarıyla birlikte değişik zamanlarda bir bankanın Gaziemir ve Narlıdere'deki ATM cihazlarına yerleştirdikleri düzeneklerle işlem yapmaya gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şiflerini elde etmeye çalışmaktan ibaret eylemlerinin TCK'nın 136. maddesinde düzenlenen kişisel verilerin hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturduğuna karar vermiştir.Yargıtay 8. Ceza Dairesi 31.10.2013 T. 2013/10737 E. 2013/25854 K. (www.legalbank.net).

³⁰² Dülger, s. 356.

8. İçtima

Kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi suçu bakımından, bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı birden fazla işlenmesi durumunda TCK'nın 43. maddesi gereği zincirleme suç hükümleri uygulanacaktır. Fail hakkında tek bir cezaya hükmedilecekse de verilecek ceza, dörtte birinden dörtte üçüne kadar arttırılacaktır.

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun; TCK'nın 132/2 maddesinde düzenlenen kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşası, 132/3 maddesinde düzenlenen kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşası, 133/3 maddesinde düzenlenen kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşası, 134/2 maddesinde düzenlenen kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşası³⁰³, 239/1 maddesinde düzenlenen ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin ifşası ve 244/2 maddesinde düzenlenen bir bilişim sistemindeki verileri başka bir yere gönderme suçu bakımından içtima problemi çıkması halinde fail TCK'nın 44. maddesi gereğince fail en ağır cezayı gerektiren suç bakımından cezalandırılacaktır³⁰⁴.

Bir başka içtima problemi ise TCK'nın 243. maddesi bakımından söz konusu olabilir. Bir bilişim sisteminde kayıtlı olan kişisel verileri ele geçirmek isteyen fail bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girebilecektir. Bu halde somut olayın özelliğine göre 243. maddenin 136. madde bakımından geçit suçu olup olmadığının tespiti gerekecektir. 243. maddede yer alan bilişim sistemine girme

³⁰³ Yargıtay, müşteki ile duygusal boyutta arkadaşlık yapan sanığın, müştekinin başka biriyle nişanlanmasından sonra buna sinirlenerek müştekinin isim, soyisim ve fotoğrafını kullanarak sahte web sitesi oluşturması, bu siteden katılan ile arkadaşlıkları sırasında yaptıkları telefon görüşmelerine ilişkin ses kayıtlarını yayınlamak suretiyle özel hayata ilişkin sesleri ifşa ettiği olayda hem özel hayatın gizliliğinin ihlal suçunun hem de sanığın ikrarıyla TCK'nın 136/1.maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunun sabit olduğuna karar vermiştir. Yargıtay 12. Ceza Dairesi 19.01.2015 T. 2014/16564 E. 2015/598 K. (www.yargitay.gov.tr); TCK'nın 134. maddesinin, 136. maddesi bakımından genel hüküm niteliğinde olduğu, kişisel verinin özel hayatın bir parçası olduğu, kişisel verilerin hukuka aykırı olarak verilmesi, yayılması ele geçirilmesinin aynı zamanda özel hayatın gizliliğini ihlal edeceği bu nedenlerle TCK'nın 136. maddesinin özel norm niteliğinde olduğu ve sadece 136. maddenin uygulanması gerektiği yönündeki görüş için bkz. İtişgen, s. 198.

³⁰⁴ Gültekin, s. 171.

suçu işlenmeden 136. maddedeki suçun işlenmesi mümkün değil ise fail sadece 136. madde gereğince cezalandırılacak; 243. maddenin geçit suçu olmadığı durumda gerçek içtima hükümleri uygulanarak fail her iki suç bakımından ayrı ayrı cezalandırılacaktır³⁰⁵.

TCK'nın 334. maddesinde yetkili makamların kanun ve düzenleyici işlemlere göre açıklanmasını yasakladığı ve niteliği bakımından gizli kalması gereken bilgileri temin etme, 336. maddesinde ise yasaklanan bu bilgileri açıklamak suç olarak düzenlenmiştir. Yasaklanan bu bilgilerin temin edilmesi ve/veya açıklanması durumunda TCK'nın 334, 336 ve 136. maddeleri arasında fikri içtima hükümleri uygulanacaktır³⁰⁶.

TCK'nın 125. maddesinde bir kimsenin onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat etmek veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldırma suç olarak düzenlenmiştir. Failin kişisel verileri açıklaması ile hakaret suçunun da oluşması halinde fikri içtima hükümleri uygulanarak, failin en ağır cezayı gerektiren suçtan cezalandırılması gerekecektir³⁰⁷. Nitekim Yargıtay 12. Ceza Dairesi'nin 08.09.2014 T. 2014/1463 E. 2014/17262 sayılı kararında da sanığın, mağdurlar adına internette bir arkadaşlık sitesinde üyelik işlemleri yapıp, oluşturduğu profil sayfalarında, mağdurların şeref, onur ve saygınlığını rencide edecek nitelikte ibareler ile birlikte kişisel veri niteliğindeki fotoğraflarını ve telefon numaralarını ilgili siteye kaydedip, yayımlaması biçimindeki tek eyleminin kanundaki birden fazla suçları oluşturması nedeniyle TCK'nın 44. maddesinde düzenlenen fikri içtima kuralı uyarınca en ağır cezayı gerektiren suçtan dolayı cezalandırılması gerektiğine karar vermiştir³⁰⁸.

9. Yaptırım ve Kovuşturma Usulü

³⁰⁵ Dülger, s. 357; Kişisel verilerin elde edilebilmesi için her zaman bilişim sistemine girmenin zorunlu olmaması ve failin bilişim sistemine girme yetkisinin olabileceği de dikkate alınarak TCK'nın 136. maddesi ile 243. maddesi arasında geçit suç ilişkisi bulunmadığı yönündeki görüş için bkz. İtişgen, s. 197; Kişisel verilerin elde edilebilmesi için her zaman bilişim sistemine girmenin zorunlu olmaması ve her iki suç tipi ile farklı değerlerin koruma altına alınarak TCK'nın 136. maddesi ile 243. maddesi arasında geçit suç ilişkisi bulunmadığı yönündeki görüş için bkz. Kuşkonmaz, s. 158.

³⁰⁶ İtişgen, s. 198.

³⁰⁷ Dülger, s. 357; Kuşkonmaz, s. 159.

³⁰⁸ www.yargitay.gov.tr.

Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılacaktır. Suçun faili tüzel kişiler olamayacaksa da TCK m.140 gereğince haklarında güvenlik tedbirleri uygulanır.

TCK'nın 139. maddesinde belirtildiği üzere suçun soruşturulması veya kovuşturması şikâyeteye bağlı değildir. 5235 sayılı Kanun gereğince davaya bakmakla görevli mahkeme Asliye Ceza Mahkemesidir.

Bu suç bakımından dava zamanaşımı süresi TCK'nın 66/1 maddesi gereğince sekiz yıl olarak öngörülmüştür. Ancak TCK'nın 66/3 maddesi gereğince 137. maddenin uygulanacağı durumlarda dava zamanaşımı süresi 66/1 uyarınca on beş yıl olacaktır. Ceza zamanaşımı süresi ise TCK'nın 68/1 maddesi gereğince on yıldır.

C. Verileri Yok Etmeme Suçu TCK m. 138

1. Suç Tipi Hakkında Genel Bilgiler

TCK'nın 138. maddesinde hukuka uygun olarak kaydedilmiş olan kişisel verilerin kanunların belirlediği sürelerin geçmiş olmasına rağmen yok edilmemesi suç olarak düzenlenmiştir. Buna göre:

“(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

(2) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır”.

Düzenleme özü itibarıyla veri koruma hukukuna hâkim temel ilkelerin bir yansımasıdır. Kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekliliğinin önemine daha önceki bölümlerde değinmiştik. Kanunlar ile öngörülen, kişisel verilerin kayıtlı olmasına izin verilen süreler geçmiş olmasına rağmen verileri yok etmeyen kişiler bu hüküm gereği cezalandırılacaktır.

2. Suçla Korunan Hukuki Değer

Suçla korunan hukuki değer genel olarak özel hayat ve özel hayatın gizli alanları³⁰⁹, özel olarak kişisel verilerdir³¹⁰. Suç kapsam itibariyle sadece kamu kurum ve kuruluşları bünyesindeki sistemlerde var olan kişisel veriler ile sınırlı olmayıp aynı zamanda özel kurum ve kuruluşlar bünyesindeki sistemlerde de var olan kişisel verileri de kapsamaktadır³¹¹. Bu bakımdan verileri yok etmekle yükümlü olan kişi bu işi kamu adına yerine getirecek olup, kişisel verilerin yok edilmesi ile bireylerin kamu idaresine olan güvenleri zedeleneceğinden suç ile ayrıca kamu idaresinin güvenilirliği ve işleyişi korunmaktadır³¹².

3. Suçun Unsurları

a. Tipikliği Maddi Unsurları

1 Fail

TCK'nın 13(. maddesine göre suçun faili, verileri sistem içinde yok etmekle görevli olankişilerdir. Suçun faili ancak verileri sistem içinde yok etmekle görevli kişiler olabileceğinden özgü bir suçtur³¹³. Dolayısıyla fail kamu görevlisi olabileceği gibi yasa ile verileri yok etmekle görevlendirilen kamu görevlisi olmayan kişiler de olabilir³¹⁴.

KVKK ile verileri sistem içerisinde yok etme görevi veri sorumlusuna verilmiştir. Veri sorumlusunun tüzel kişi olması halinde belirleyeceği temsilci ya da görevlendireceği kişi veya kişiler suçun faili olabilecektir.

³⁰⁹ arlar, s. 1 6 ; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 601; Hafizoğulları ve Özen, s. 291.

³¹⁰ Dülger, s. 360; Karagülmez, s. 46(; Sert, s. 1 3.

³¹¹ Karagülmez, s. 46(.

³¹² Dülger, s. 360; Karagülmez, s. 46(;Korkmaz, s. 494.

³¹³ Hafizoğulları ve Özen, s. 292; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 601.

³¹⁴ Dülger, s. 361; Hafizoğulları ve Özen, s.292; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 601; Karagülmez, s. 470.

2 Mağdur

Suçun mağduruna ilişkin doktrinde iki görüş bulunmaktadır. Bu görüşlerden ilkinde göre suçun mağduru verileri yok edilmeyen herkesken³¹⁵, bir diğer görüşe göre suç ile kamu idaresine olan güven korunduğundan suçun mağduru toplumu oluşturan bireylerdir ve verileri yok edilmeyen ilgili kişiler suçtan zarar gören kişi olacaktır³¹⁶. Bir bu görüşlerden ilgili kişinin suçun mağduru olduğu görüşüne katılmaktayız. Suçun mağdurunun toplumu oluşturan bireylerin her biri olarak kabul edilmesi halinde, yok edilmeyen kişisel verinin ilgili kişisi olmayan kişilerin suçun mağduru olması sonucunu doğuracaktır. Ancak kişisel veriden söz edebilmek için bir verinin belirli veya belirlenebilir bir kişiye ait olması gerekir. Ayrıca Ceza Kanununun amacı; kişi hak ve özgürlüklerini, kamu düzen ve güvenliğini, hukuk devletini, kamu sağlığını ve çevreyi, toplum barışını korumak, suç işlenmesini önlemektir

3 Suçun Konusu

Suçun konusunu kişisel veriler oluşturmaktadır³¹⁷. Suçun konusuna ilişkin “kişisel verilerin kaydedilmesi” suçu ve “verileri hukuka aykırı olarak verme veya ele geçirme” suçu kapsamında yapmış olduğumuz açıklamalar bu suç tipi bakımından da geçerlidir.

Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde ise verilecek ceza bir kat artırılacaktır.

4 Hareket Eylem, Fiil

Suçun maddi unsurunu oluşturan hareket verilerin yok edilmemesidir. “Yok etmek”, “ortadan kaldırmak, ifna etmek, izale etmek, varlığına son vermek” olarak tanımlanmaktadır³¹⁸. Dolayısıyla kişisel verilerin yok edilmesi de kişisel verilerin,

³¹⁵ Parlar, s.1567; Kuşkonmaz, s. 163.

³¹⁶ Dülger, s. 362; Karagülmez, s. 470.

³¹⁷ Dülger, s. 363.

³¹⁸ www.tdk.gov.tr.

ilgili kullanıcılar dâhil hiç kimse tarafından, hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Bu kapsamda daha önce de açıkladığımız üzere Yok edilme işlemi gereğince verilerin kaydedildiği evrak, dosya, CD, disket, hard disk gibi veri saklamaya elverişli materyallerin imha edilmesi gerekmektedir. Kişisel verilerin yok edilmesi verinin anonim hale getirilmesi ile de mümkündür³¹⁹. Anonimleştirme sürecinde yapılan işlemlerle belirlenebilir bir kişi ile verinin arasındaki bağ kopartılarak kişinin kimliği tespit edilemez hale geldiğinden, anonim hale getirilen veriler kişisel veri olmaktan çıkacaktır.

TCK'nın 13(. maddesine konu suçun işlenebilmesi için Kanun'da sayılan iki şartın birlikte gerçekleşmiş olması gerekir. Bunlar; i verilerin yok edilmesi için öngörülen sürenin geçmiş olması, ii verileri sistem içerisinde yok etmekle yükümlü kişilerin bu yükümlülüklerini yerine getirmemiş olmasıdır. Öğretide bir başka görüş suçun oluşabilmesi için sistem içerisindeki verilerin hukuka uygun olarak kaydedilmiş olması şartını aramaktadır³²⁰. Ancak biz bu görüşe katılmıyoruz.

TCK'nın 13(. maddesi kapsamında kişisel verilerin yok edilmemesi suçunun oluşabilmesi için aranan şartlardan ilki verilerin yok edilmesi için öngörülmüş olan sürenin geçmiş olmasına rağmen verilerin yok edilmemesidir. Madde metninde “kanunların belirlediği sürelerin geçmiş olması” ifadesine yer verilmişse de idarenin düzenleyici işlemleri ile belirlenen sürelerin geçmiş olması halinde de cezai sorumluluğun doğduğu kabul edilmelidir³²¹. Nitekim kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesine ilişkin usul ve esaslar 2(.10.2017 tarihli “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik” ile düzenleme altına alınmıştır. Yönetmelik kapsamında belirlenen süreler de TCK'nın 13(. maddesine konu olabilecektir.

TCK'nın 13(. maddesi kapsamında kişisel verilerin yok edilmemesi suçunun oluşabilmesi için bir diğer şart verileri sistem içerisinde yok etmekle yükümlü kişilerin bu yükümlülüklerini yerine getirmemiş olmasıdır. Suç, ihmali hareketle

³¹⁹ Ketizmen, s. 241.

³²⁰ Parlar, s. 1566.

³²¹ Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 602; Dülger, s. 364; Aksi yöndeki görüş için bkz. Sert, s. 155.

gerçekleştirilir³²². Verilerin sistem içerisinde yok edilmemesi ile suç tamamlanmış olacaktır³²³. Dolayısıyla suçun oluşması için bir zarar meydana gelmesi aranmamaktadır. Bu nedenle soyut tehlike suçudur³²⁴.

b. Tipikliğin Manevi Unsurları

Suç genel kastla işlenebilen bir suçtur. Suçun olası kastla işlenebilmesi mümkün iken; taksirle işlenmesi mümkün değildir³²⁵.

c. Suçun Hukuka Aykırılık Unsuru

Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmemeleri halinde “verileri yok etmeme” suçu oluşacaktır. Yine KVKK’nın 7. maddesinde düzenlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi maddesine aykırı hareket edilmesi halinde de 17.maddesinin 2. Fıkrasına yapılan atıfla, TCK’nın 13(. maddesi uygulanacaktır.

TCK’nın 13(. maddesi bakımından kanunda hukuka uygunluk sebebi öngörülmemiştir³²⁶. Verilerin yok edilmesi kamu düzenine ilişkin olduğundan ilgili kişinin rızası da hukuka uygunluk sebebi olarak kabul edilemeyecektir³²⁷. Kanunların belirlediği süreler geçtikten sonra verileri yok etmekle yükümlü kişi tarafından verilerin yok edilmesi de hukuka uygunluk sebebi olarak değerlendirilemeyecektir³²⁸.

³²² Ketizmen, s. 240; Bük, s. 104; Soyaslan, s. 35(; Hafızogulları ve Özen, s.292; Dülger, s. 367; Parlar, s.1567.

³²³ Soyaslan, s. 35(.

³²⁴ Dülger, s. 366.

³²⁵ Dülger, s.367; Akdağ, s. 14(; Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 604.

³²⁶ Genel hukuka uygunluk nedenlerinin suç bakımından geçerli olacağı yönündeki görüş için bkz. Gerçeker, s. 13(2.

³²⁷ Karagülmez, s. 470;Suç ile iki farklı hukuksal değer korunduğundan suçtan zarar gören ilgili kişinin rızasının hukuka uygunluk sebebi olarak değerlendirilemeyeceği yönündeki görüş için bkz. Dülger, s. 36(;Suçun soruşturması ve kovuşturması şikâyete bağlı olmadığından ilgili kişinin üzerinde tasarrufta bulunamayacağı bu sebeple ilgili kişinin rızasının hukuka uygunluk sebebi olarak kabul edilemeyeceği yönündeki görüş için bkz.Özbek, Kanbur, Doğan, Bacaksız ve Tepe, s. 604; İlgili kişinin rızasının bulunmasının hukuka uygunluk sebebi teşkil edeceği yönündeki aksi görüş için bkz. Gültekin, s. 194.

³²⁸ Kuşkonmaz, s. 166.

4. Suçun Nitelikli Hali

Verileri yok etmeme suçu bakımından suçun nitelikli hali, 21.02.2014 tarih ve 6256 sayılı Yasa'nın 5. maddesi ile TCK'nın 13(. maddesine eklenen ikinci fıkrada düzenlenmiştir. Buna göre suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde ise verilecek ceza bir kat artırılacaktır. Ceza Muhakemesi Kanunu'nun çeşitli maddelerinde konuya ilişkin düzenlemeler bulunmaktadır.

CMK'nın (0. maddesinde, CMK'nın 75, 76 ve 7(inci madde hükümlerine göre alınan örnekler üzerinde yapılan genetik inceleme sonuçlarının, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilmesi gerektiği öngörülmüştür.

CMK'nın (1. maddesinde şüpheli veya sanığın, kimliğinin tespiti için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafının, beden ölçülerinin, parmak ve avuç içi izinin, bedeninde yer almış olup tespitini kolaylaştıracak diğer özelliklerinin, sesi ve görüntülerinin kayda alınabileceği ancak alınan bu kayıtların kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi halinde Cumhuriyet savcısının huzurunda derhâl yok edileceği düzenlenmiştir.

CMK'nın 135. maddesinde aranan diğer şartların sağlanması halinde şüpheli veya sanığın telekomünikasyon yoluyla iletişiminin dinlenebileceği, kayda alınabileceği ve sinyal bilgileri değerlendirilebileceği öngörülmüştür. Kayda alma gerçekleşikten sonra bu durumun anlaşılması hâlinde, alınan kayıtlar derhâl yok edilir. CMK'nın 137/3 maddesi gereğince 135. maddeye göre verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hâkim onayının alınamaması halinde, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilir.

CMK'nın 139. maddesine göre gizli soruşturmacı görevlendirilmesi suretiyle elde edilen kişisel bilgiler, görevlendirildiği ceza soruşturması ve kovuşturması dışında kullanılamaz ve suçla bağlantılı olmayan kişisel bilgiler derhâl yok edilir.

CMK'nın 140. maddesine göre şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir. Maddenin ikinci fıkrasında düzenlendiği üzere teknik araçlarla izlemeye hâkim, gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verir. Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunar ve hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde kayıtlar derhâl imha edilir. Elde edilen delillerin ceza kovuşturması bakımından gerekli olmadığı takdirde Cumhuriyet savcısının gözetiminde derhâl yok edilir.

“Kişisel verilerin kaydedilmesi” suçu ve “verileri hukuka aykırı olarak verme veya ele geçirme” suçu bakımından TCK'nın 137. maddesi ile öngörülen nitelikli haller TCK'nın 13(. maddesi bakımından uygulanamayacaktır.

5. Suçun Neticesi Sebebiyle Ağırlaşmış Hali

TCK'nın 13(. maddesinde düzenlenen suç bakımından neticesi sebebiyle ağırlaşmış hali Kanunda suç olarak düzenlenmemiştir.

6. Teşebbüs

Suç, kanunda belirlenen sürelerin geçmiş olmasına rağmen verilerin yok edilmemesi ile tamamlanacağından ve ihmali surette işlenebileceğinden teşebbüse elverişli değildir³²⁹.

7. İştirak

Suçta iştirak bakımından bir özellik söz konusu olmayıp; suçta iştirak mümkündür. Ancak verileri sistem içerisinde yok etmekle yükümlü olan kişilerce işlenebileceğinden, bu yönde yükümlülüğü bulunmayan kişiler ancak azmettiren veya yardım eden sıfatıyla suçta iştirak edebilecektir³³⁰.

³²⁹ Dülger, s. 36(; Parlar, s. 1567.

³³⁰ Parlar, s. 156(.

8. İçtima

Verileri yok etmeme suçu bakımından, bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı birden fazla işlenmesi durumunda TCK'nın 43. maddesi gereği zincirleme suç hükümleri uygulanacaktır. Fail hakkında tek bir cezaya hükmedilecekse de verilecek ceza, dörtte birinden dörtte üçüne kadar arttırılacaktır. Birden fazla kişiye ait kişisel verilerin bulunduğu bir sistemde failin verileri yok etmemesi durumunda TCK'nın 43/2 maddesi gereğince fail hakkında tek bir cezaya hükmedilecekse de verilecek ceza, dörtte birinden dörtte üçüne kadar arttırılacaktır.

TCK'nın 13(. maddesi bakımından fail sistem içerisindeki verileri yok etmemekle birlikte verileri hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme eylemlerinden birini de gerçekleştirmesi halinde gerçek içtima hükümlerine göre hem TCK'nın 13(. maddesi hem de 136. maddesi bakımından cezalandırılacaktır³³¹.

Doktrinde TCK'nın 13(. maddesinin TCK'nın 257. maddesinde düzenlenen “görevi kötüye kullanma” suçunun özel bir tipini oluşturduğu yönünde bir görüş bulunmaktadır³³². Ancak verileri yok etmekle yükümlü kişinin mutlaka kamu görevlisi olması gerekmediğinden biz doktrindeki bir diğer görüşe katılıyoruz³³³.

9. Yaptırım ve Kovuşturma Usulü

Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olan kişilerin görevlerini yerine getirmemeleri halinde bir yıldan iki yıla kadar hapis cezası ile cezalandırılacaktır. Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde fail hakkında verilecek ceza bir kat artırılır. Suçun faili

³³¹ Parlar, s. 156(; Kuşkonmaz, s. 167.

³³² Ersan Şen, **5237 Sayılı Türk Ceza Kanunu'nda Özel Hayata Karşı Suçlar**”, İstanbul Barosu Dergisi, C. 79, s. 3, 2005, 707-720, s. 719; Gerçekler, s. 13(0.

³³³ Korkmaz, s. 49(; Gültekin, s. 1(2.

tüzel kişiler olamayacaksa da TCK m.140 gereğince haklarında güvenlik tedbirleri uygulanır.

TCK'nın 139. maddesinde belirtildiği üzere suçun soruşturulması veya kovuşturması şikâyeteye bağlı değildir. 5235 sayılı Kanun gereğince davaya bakmakla görevli mahkeme Asliye Ceza Mahkemesidir.

Bu suç bakımından dava zamanaşımı süresi TCK'nın 66/1 maddesi gereğince sekiz yıl olarak öngörülmüştür. Ceza zamanaşımı süresi ise TCK'nın 6(/1 maddesi gereğince on yıldır.

III.KİŞİSEL VERİLERİN 4721 SAYILI TÜRK MEDENİ KANUNU VE 6098 SAYILI TÜRK BORÇLAR KANUNU KAPSAMINDA KORUNMASI

Kişisel verilerin korunması hakkı esasen kişilik hakkının özel bir görünüş biçimidir.Kişilik hakkının kapsamı ve sınırları kesin ve açık bir şekilde belirlenememişse de; bu hak kişiye, başkaları tarafından maddi ve bedeni bütünlüğünün, menfaatlerinin, ilişkilerinin özetle kişiliğinin bütününe oluşturan hukuki menfaatlerinin zedelenmesinden kaçınılmasını isteme yetkisi verir³³⁴. Bu bağlamda kişinin bedeni ve maddi bütünlüğünden, menfaatlerinden, ilişkilerinden kaynaklanan pek çok verisi kişisel veri olarak kabul edilecektir.

Nitekim KVKK'nın 14. maddesinin son fıkrasında kişilik hakları ihlal edilen kişilerin tazminat hakları saklı tutulmuştur. Kanun'un 14. maddesi ile atıfta bulunulan düzenlemeler 4721 sayılı Türk Medeni Kanunu'nun 24. ve 25. maddeleri ile 609(sayılı Türk Borçlar Kanunu'nun 49, 53, 54, 56 ve 5(. maddeleridir³³⁵.

4721 sayılı Kanun'un 24. maddesinde hukuka aykırı olarak kişilik haklarına saldırılan kişinin, hâkimden, saldırılara karşı korunmasını isteyebileceği düzenlenmiştir. Kişilik hakkı zarara uğrayan kişiler zararın giderilmesi için

³³⁴ Jale G. Akıntürk, Turgut Akıntürk ve Derya Ateş Karaman,**Türk Medeni Hukuku Birinci Cilt Başlangıç Hükümleri Kişiler Hukuku**, Beta Yayınevi, s. 343; M. Kemal Oğuzman, Nami Barlas, **Medeni Hukuk Giriş Kaynaklar Temel Kavramlar**, Vedat Kitapçılık, İstanbul, 2012, s. 161; Hasan Petek, **Kişilik Değerlerinin Ölümünden Sonra Korunması**, Yetkin Yayınları, Ankara, 2015, s. 53; Küzeci, s. 3(2; Aksoy, s. (0; Ali Yarayan, **Türk Medeni Hukuku Temel Bilgiler**, Yetkin Yayınları, Ankara, 2013; s. 214; Fatma Tülay Karakaş, **Kişiyeye Sıkı Sıkıya Bağlı Haklar**, Turhan Kitapevi Yayınları, Ankara, 2015, s. 91.

³³⁵ Damla Gürpınar, Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Prof. Dr. Şeref Ertaş'a Armağan, C. 19, Özel Sayı, 2017, 679- 694, s. 6(9; Aksoy, s. (0; Küzeci, s. 3(3.

Kanun'un 25. maddesi gereğince maddi ve manevi tazminat davası açabilir. Her iki davanın da açılabilmesi için somut olayda; (i) saldırganın kasten hukuka aykırı bir eylemde bulunması, (ii) bu eylemi sonucunda zarar meydana gelmesi, (iii) zarara sebep olan eylem ile zarar arasında illiyet bağının olması gerekir³³⁶. Ancak kişisel veriler üzerinde hukuka aykırı faaliyette bulunan kişilerin, sadece kusurlu davranışlarının cezalandırılması her zaman hakkaniyete uygun düşmeyecektir. Kişisel verilerin tam anlamıyla korunabilmesi için hem kusur hemde kusursuz sorumluluk hallerinin somut olayın özelliğine göre kabul edilmesi gerekir³³⁷.

Kişilik hakkının ihlal edilmesine sebep olan eylem aynı zamanda haksız fiil sayılacağından kişinin 609(sayılı Kanun'un 49. maddesi vd hükümlerince de korunması mümkündür.

Kişisel verilerin, kişilik hakkı kapsamında korunabileceği yargı kararlara da konu edilmiştir. Yargıtay Hukuk Genel Kurulu'nun 17.06.2015 tarihli 2014/4-56 E. 2015/1679 sayılı kararında³³⁸ kişilik hakkı ile kişisel verilerin korunması hakkı arasındaki ilişkiye ve unutulma hakkına yer verilmiştir. Karara konu olay; cinsel saldırı suçunun mağduru olan davacının, isminin rumuzlanmadan kitapta yer alması sebebiyle manevi zararının tazmini talebine ilişkindir. Kararda, unutulma hakkı ve bunun sonucu olan kişisel verilerin ve kişilik hakkının korunması ile bilim ve sanat hürriyetinin üzerinde durularak; davacının kişisel verisi olan adının rumuzlanmadan kitapta yer almasının unutulma hakkını ve bunun neticesinde özel hayatın gizliliğini ihlal ettiği kabul edilmiştir.

³³⁶ Akıntürk, Akıntürk ve Karaman, s. 404 vd; Yarayan, s.219; Gamze Turan Başara, **Kişiliğin İthalinden Kaynaklanan Maddi ve Manevi Tazminat Davası İle Haksız Kazancın İadesi**, Turhan Kitapevi, Ankara, 201(, s. 53; Petek, s. 212; Seda Kara Kılıçarslan, **Kişilik Hakkına Saldırıda Üstün Nitelikte Özel ve Kamusal Yarar**, Onikilevha Yayınları, İstanbul, 2015, s. 12.

³³⁷ Gürpınar, s. 690; Aksoy, s. ((.

³³⁸ www.neohukuk.net.

SONUÇ

Günümüzde hızlı ve sınırsız gelişen bilim ve teknoloji karşısında temel hak ve özgürlüklerin korunmasına duyulan ihtiyaç her geçen gün artmaktadır. Teknolojinin hayatımızın ayrılmaz parçası haline gelmesiyle hukuksal sorunlar da değişime uğramıştır. Temel hak ve özgürlüklerin korunması ihtiyacı karşısında teknolojinin sağladığı kolaylıklar arasında makul bir sağlanmaya çalışılması yeni hak ve özgürlük kavramlarının tartışılmasını beraberinde getirmiştir. Bu anlamda yeni temel hak ve özgürlüklerden biri de kişisel verilerin korunması hakkıdır.

Kişisel verilerin korunması hakkı, konuyla ilgili uzun yıllardan beri süregelen tartışmaların ve uyuşmazlıkların sonucunda geç de olsa hem Avrupa'da hem de ülkemizde temel hak ve özgürlükler arasında bağımsız bir hak olarak yerini almıştır.

Kişisel verilerin korunması hakkı; insan onuru, kişiliğin serbestçe geliştirilmesi hakkı, özel yaşamın gizliliği hakkı, düşünce özgürlüğü, bilim özgürlüğü, bilgi edinme hakkı, haberleşmenin gizliliği gibi diğer pek çok temel hak ve özgürlükler ile iç içe geçmiş durumdadır. Bu sebeple kişisel verilerin etkin biçimde korunması ile diğer temel hak ve özgürlüklerin ihlali önlenebilecektir.

Kişisel verilere yönelik etkin bir korunmanın sağlanması öncelikle her bireyde kişisel verilerin korunması bilincinin oluşması ile mümkündür. Bu bilincin oluşabilmesi için hem devlet hem de ulusal ve uluslararası kurum ve kuruluşlar tarafından bilgilendirme çalışmaları yapılmalıdır. Yapılan bilgilendirme çalışmalarında bireye, hakları ve başvurabileceği yasal yolların yanında haklarının ihlal edilmesi halinde bildirimde bulunması gerektiği ve bu bildirimi kime, nasıl, ne şekilde yapacağı da anlatılmalıdır.

Kişisel verilerin tam anlamıyla korunabilmesi için yasal düzenlemelerin bölgesel değil küresel düzeyde korumaya yönelik olması gerekir. Bu anlamda 25 Mayıs 2016 tarihinde yürürlüğe giren Genel Veri Koruma Tüzüğü ile getirilen yenilikler son derece önemlidir. Tüzük hükümleri AB dışındaki ülkeler bakımından da uygulama alanı bulmaktadır. AB içerisinde yer alan veri sorumlusu veya veri işleyenin, AB sınırları dışındaki veri işleme faaliyetleri Tüzük kapsamında sayılmıştır. Ayrıca AB vatandaşlarına ait kişisel verilerin AB coğrafi sınırları dışında işlenmesi halinde, AB vatandaşları Tüzük düzenlemeleri ile getirilen korumalardan

yararlanabilecektir. Ayrıca hesap verilebilirlik, unutulma hakkı, veri taşınabilirliği hakkı, rıza beyanının daha sıkı şartlara bağlanması, veri sorumluları ve veri işleyenlerin sorumluluğuna yönelik değişiklikler, idari para cezalarındaki arttırım gibi yenilikler kişisel verilerin korunması hukukunda yeni bir dönem başlatmıştır.

İlkemizde de kişisel verilerin çağdaş standartlarda işlenmesi ve korunmasını sağlamak amacıyla bir an önce mevcut yasal düzenlemelerin Genel Veri Koruma Tüzüğü ile uyumlu hale getirilmesi gerekmektedir.

Kişisel verilerin korunmasına ilişkin ulusal ve uluslararası düzenlemelerde veri işlemenin meşrulaştırıldığı bazı istisnai durumlar öngörülmüştür. Uygulamada bu istisnai durumların yorumlanması ile kişisel verilerin işlenmesi, hukuka uygun hale getirilmeye çalışılmaktadır. Konunun hassasiyeti sebebiyle yasal düzenlemelerde, istisnai durumların sınırları çizilmelidir.

Kişisel verileri işleyen veri sorumluları ve veri işleyenlerin, veri işleme faaliyeti sırasında temel ilkelere ve yasal düzenlemelere uygun davranıp davranmadığının bağımsız kontrol organları tarafından belirli periyotlarla denetlenmesi gerekir. Kişisel verilerin işlenmesinde, temel ilkelerin uygulanmasına yönelik yöntemler geliştirilerek önleyici bir koruma sağlanmalıdır. Ayrıca caydırıcı olması sebebiyle hukuka aykırı veri işleme faaliyetlerine yönelik idari, cezai ve hukuki yaptırımların ağırlaştırılması gerekmektedir.

Türk Ceza Kanunu'nda yer alan kişisel verilerin korunmasına dair hükümlerin 669(sayılı Kişisel Verilerin Korunması Kanunu'ndan önce yürürlüğe girmiş ve uygulanıyor olması, Türk Ceza Kanunu'nda kişisel verilerin tanımlanmamış olması iki kanun arasında uyumsuzluklara, Türk Ceza Kanunu'nun uygulanması bakımından farklılıklara sebep olmaktadır. Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesi ile birçok tereddüt giderilmişse de iki kanunun birlikte işlerliği önündeki yorum farklılıklarının ortadan kalkması ve konunun hassasiyeti gereği bir an önce Türk Ceza Kanunu'nun 669(sayılı Kişisel Verilerin Korunması Kanunu ile uyumlu hale getirilmesi gerekmektedir.

Son olarak teknolojik gelişmeler yorumlanarak ileriye yönelik uyumsuzluklar tespit edilmeli ve bu konuda da çalışmalar yapılmalıdır

KAYNAKÇA

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

Akgül, Aydın. **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, Beta Yayınları, İstanbul, 2014.

Akıncı, Ayşe Nur. **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, Çalışma Raporu No.6, T.C Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Bilgi Toplumu Dairesi Başkanlığı, Haziran 2017.

Akıntürk, Jale G., Turgut Akıntürk ve Derya Ateş Karaman. **Türk Medeni Hukuku Birinci Cilt Başlangıç Hükümleri Kişiler Hukuku**, Beta, İstanbul, 2012.

Aksoy, Hüseyin Can. **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Çakmak Yayınevi, Ankara, 2010.

Akyürek, Güçlü. **Özel Hayatın Gizliliğinin İhlal Suçu**, 2. Baskı, Seçkin Yayınları, Ankara, 2013.

Araslı, Oya. **Özel Yaşamın Gizliliği Hakkı ve T.C Anayasasında Düzenlenişi** (Yayınlanmamış Doçentlik Tezi), Ankara, 1979.

Aşıkoğlu, Şehriban İpek. **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, Onikilevha Yayınları, İstanbul, 201(.

Ayan, Mehmet. **Eşya Hukuku I Zilyetlik ve Tapu Sicili**, Seçkin Yayıncılık, Ankara, Ekim 2016.

Aydın, Sedat Erdem. **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, İstanbul Ceza Hukuku ve Kriminoloji Arşivi, Onikilevha Yayınları, İstanbul, 2015

Aygözer Öngün, Çiğdem. **Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, Beta Yayınları, İstanbul, 2019.

Turan Başara, Gamze. **Kişiliğin İhalinden Kaynaklanan Maddi ve Manevi Tazminat Davası İle Haksız Kazancın İadesi**, Turhan Kitapevi, Ankara, 201(.

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

Bayram, Mehmet Hanifi. **Avrupa Birliği ve İnternet Hukuku**, Seçkin Yayıncılık, Ankara, 2011.

Bayram, Mehmet Hanifi. **Avrupa Birliği Hukuku Dersleri**, Seçkin Yayınları, Ankara, 201(.

Bozkurt, Enver. **Türkiye'nin Uluslararası Hukuk Mevzuatı**, Asil Yayınları, Ankara, 2011.

Bozkurt Yüksel, Armağan Ebru. **Bulut Bilişimde Kişisel Verilerin Korunması Personal Data Protection in Cloud Computing**, Yetkin Yayınları, Ankara, 2016.

Bük, Alaattin. **Bilişim Alanında Kişisel Verilerin Korunması**, Seçkin Yayınları, Ankara, 201(.

Can, Hacı. **Avrupa Birliği Hukuku**, Sürat Üniversite Yayınları, İstanbul, 2013.

Can, Hacı. **Avrupa Birliği Sözleşme Hukuku**, Adalet Yayınları, Ankara, 2015.

Demirbaş, Timur. **Ceza Hukuku Genel Hükümleri**, Seçkin Yayınları, Ankara, 201(.

Develioğlu, Hüseyin Murat. **6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, Onikilevha Yayınları, İstanbul, 2017.

Dülger, Murat Volkan. **Bilişim Suçları ve İnternet İletişim Hukuku**, Seçkin Yayınları, Ankara, 201(.

Dülger, Murat Volkan. **Kişisel Verilerin Korunması Hukuku**, Hukuk Akademisi, İstanbul, 2019.

Efil, Alper Yaser. **Özel Hayatın Gizliliğinin İhlali Suçu**, (Yayınlanmamış Yüksek Lisans Tezi), Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir, 201(.

Er, Cüneyd. **Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı: Parmak İzi, Göz ve DNA Tarama Gibi Teknolojik Kimlik Denetleme Usullerinin Hukuki Statüsü**, Yetkin Yayınları, Ankara, 2007.

Gemalmaz, Mehmet Semih. **Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş**, Beta Yayınları, İstanbul, 2001.

Gemicioğlu, Bora, Zeynephan Gemicioğlu, Mine Yağcı ve Alara Yılmaz. **Kişisel Verilerin Korunması Mevzuatı Uluslararası Düzenlemeler ve İçtihatlar**, Onikilevha Yayınları, İstanbul, 2019.

Gerçekler, Hasan. **Yorumlu Uygulamalı Türk Ceza Kanunu**, C.1, Seçkin Yayınları, Ankara, 2017.

Gökcan, Hasan Tahsin. **Tıbbi Müdahaleden Doğan Hukuki ve Cezai Sorumluluk**, Seçkin Yayınları, Ankara, 2017.

Gültekin, Nil Melek. **Kişisel Verilerin Ceza Hukuku Yönünden Korunması** (Yayınlanmamış Yüksek Lisans Tezi), Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2012.

Gürpınar, Damla. “Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Prof. Dr. Şeref Ertaş’a Armağan**, Cilt:19, Özel Sayı, İzmir, 2017, 679-694

Hafizoğulları, Zeki ve Muharrem Özen. “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar”, **Ankara Barosu Dergisi**, Yıl: 67, Sayı: 4, 2009, ss. 9-22.

Hafizoğulları, Zeki ve Muharrem Özen. **Türk Ceza Hukuku Özel Hükümler, Kişilere Karşı Suçlar**, U S-A Yayıncılık, Ankara, 2016.

Hakeri, Hakan. **Tıp Hukuku**, 13. Baskı, Seçkin Yayınları, Ankara, 201(.

İtişgen, Rezzan. “Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu”, **TADD**, Yıl: 6, Sayı: 23 (Ekim 2015), ss. 179-202.

Kara Kılıçarslan, Seda. **Kişilik Hakkına Saldırıda Üstün Nitelikte Özel ve Kamusal Yarar**, Onikilevha Yayınları, İstanbul, 2015.

Karakaş, Fatma Tülay. **Kişiyeye Sıkı Sıkıya Bağlı Haklar**, Turhan Kitapevi Yayınları, Ankara, 2015.

Karagülmez, Ali. **Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri**, Seçkin Yayınları, 5. Baskı, Ankara, 2014.

Kaya, Cemil. “Avrupa Birliđi Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: 69, Sayı: 1-2, Prof. Dr. İl Han ÖZAY’a Armağın, 2011, ss. 317-334.

Kaya, Mehmet Bedii ve Furkan Güven Taştan. **Kişisel Veri Koruma Hukuku Mevzuat & İçtihat**, Onikilevha Yayınları, İstanbul, 201(.

Kayıhan, Şaban ve Mustafa Ünlütepe. **Medeni Hukuk Bilgisi**, Seçkin Seçkin Yayıncılık, Ankara, 2017.

Ketizmen, Muammer. **Türk Ceza Hukukunda Bilişim Suçları**, Adalet Yayınevi, 200(.

Kılkelley, Ursula. **Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı Avrupa İnsan Hakları Sözleşmesi’nin 8. Maddesi’nin Uygulanmasına İlişkin Kılavuz**, İnsan Hakları Kitapları No.1, Türkiye Cumhuriyeti Adalet Bakanlığı İnsan Hakları Dairesi Başkanlığı, 2001.

Korkmaz, İbrahim. **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, 2. Baskı, Seçkin Yayınları, Ankara, 2019.

Korkmaz, İbrahim. “Kişisel Verilerin Korunması Kanunu Hakkında Değerlendirme” (Değerlendirme), **Türkiye Barolar Birliđi Dergisi**, Sayı:124, Ankara, 2016 ss.(1-152.

Küzeci, Elif. “İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı”, **İnsan Hakları Yıllığı**, Cilt:32, 2014, ss.53-75.

Küzeci, Elif. **Kişisel Verilerin Korunması**, Turhan Kitabevi, Ankara, 2019.

Mahmutoglu, Fatih Selami. “Sır Saklama Yükümlülüğü Kapsamında Hastaya Ait Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Yayma Suçu”, fsmahmutoglu.av.tr, (11.10.2019).

Mahmutoglu, Fatih S. ve Yener ÜNVER, **Suç Teorisi**, Beta Yayınları, 2000.

Mendos Kuşkonmaz, Elif. **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması** (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013.

Metin, Yüksel. “Avrupa Birliği Temel Haklar Şartı”, **Ankara Üniversitesi SBF Dergisi**, Cilt: 57, Sayı: 4, Ankara, 2002, 35-63.

Oğuzman, Kemal ve Nami Barlas. **Medeni Hukuk Giriş**, Kaynaklar, Temel Kavramlar, Vedat Yayıncılık, İstanbul, 200(.

Oğuzman, Kemal, Özer Seliçi ve Saibe Oktay-Özdemir. **Kişiler Hukuku Gerçek ve Tüzel Kişiler**, Filiz Kitabevi, İstanbul, 2010.

Orwell, George, **Bin Dokuz Yüz Seksek Dört**, çev. Nuran Akgören, Can Yayınları, İstanbul, 2001.

Önüt, Lale Burcu. **Avrupa Birliği Hukukunun Üye Devletlerde Uygulanması**, Seçkin Yayıncılık, Ankara, Eylül 2017.

Özbek Veli Özer, Mehmet Nihat Kanbur, Koray Doğan, Pınar Bacaksız ve İlker Tepe. **Türk Ceza Hukuku Özel Hükümler**, Seçkin Yayınları, Ankara, 201(.

Özdemir, Hayrunnisa. **Elektronik Haberleşme Sektöründe Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin Yayınları, Ankara, 2009.

Özgenç, İzzet. **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayınları, Ankara, 2017.

Özkan, Bilge. **Medeni Hukuk'un Temel Kavramları**, Turhan Kitapevi Yayınları, Ankara, 2010.

Parlar, Ali. **Türk Ceza Hukukunda Bilişim Suçları**, Bilge Yayınevi, Ankara, 2015.

Parlar, Ali. **Türk Ceza Kanunu Şerhi**, C. 2, Bilge Yayınevi, Ankara, 2015.

Petek, Hasan. **Kişilik Değerlerinin Ölümden Sonra Korunması**, Yetkin Yayınları, Ankara, 2015.

Poggi, Gianfranco. **Modern Devletin Gelişimi Sosyolojik Bir Yaklaşım**, çev. Şule Kurt, Binnaz Toprak, İstanbul Bilgi Üniversitesi Yayınları, 2. Baskı, İstanbul 2002.

Say, Cem. **50 Soruda Yapay Zeka**, 7 Renk Yayıncılık, İstanbul, 2019.

Sert, Şeyma. **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, Seçkin Yayınları, Ankara, 2019.

Sezgin, Fatih. “Edward Snowden Olayı’nın ABD-Rusya İlişkileri Üzerindeki Etkileri”, **Uluslararası Yönetim ve Sosyal Araştırma Dergisi**, Cilt: 1, Sayı: 1, 2014, ss. 24-31.

Soyaslan, Doğan. **Ceza Hukuku Özel Hükümler**, 11. Baskı, Yetkin Yayınları, Ankara, 2016.

Soykan, Cavidan. Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı: “Özel Hayatın Gizliliği X İfade Özgürlüğü, İnsan Hakları Merkezi Çalışma Metinleri –III, **Ankara Üniversitesi Siyasal Bilimler Fakültesi İnsan Hakları Merkezi**, Ankara, 2006.

Sözüer, Eren. **Unutulma Hakkı İnsan Hakları Hukuku Perspektifinden Bir İnceleme**, On İki Levha Yayıncılık, 1. Baskı, İstanbul, Ekim 2017.

Şahin, Meral Ekici. **Ceza Hukukunda Rıza**, Onikilevha Yayıncılık, İstanbul, 2012.

Şen, Ersan. “5237 Sayılı Türk Ceza Kanunu’nda “Özel Hayata Karşı Suçlar”, **İstanbul Barosu Dergisi**, C. 79, S. 3, 2005, ss. 707-720.

Şen, Ersan ve Yasemin Yurttaş, Bilgisayar Programları Karşısında Özel Hayatın Korunması, **Terazi Hukuk Dergisi**, Y. 5, S. 42, 2010, ss. 29-44.

Şen, Ersan. “Kişisel Verilerin Korunması Kanunu Tasarısı’nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi”, **İstanbul Barosu Dergisi**, Cilt: (3, Sayı:3, İstanbul, 2009, ss. 1197-1214.

Şimşek, Oğuz. **Anayasa Hukukunda Kişisel Verilerin Korunması**, 1. Baskı, İstanbul, 200(.

Taneri, Gökhan ve Gani Kamışlı. **Kişilere Karşı İşlenen Suçlar**, Seçkin Yayınları, Ankara, 201(.

Taştan, Furkan Güven. **Türk Sözleşmeler Hukukunda Kişisel Verilerin Korunması**, Onikilevha Yayıncılık, İstanbul, 2007.

Tekin, Nurullah. “Kişisel Verilerin Korunması İle İlgili Türkiye’deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi”, **Uyuşmazlık Mahkemesi Dergisi**, Sayı:4, Ankara, 2014, ss. 222-262.

Tekinalp, Ünal. **Fikri Mülkiyet Hukuku**, Vedat Yayıncılık, İstanbul, 2012.

Tezcan, Durmuş. “Özel Hayatın Gizliliğini İhlal ve Kişisel Verilerin Kaydedilmesi Suçu İle İlgili Bazı Gözlemler”, **İÜHFİM**, C. LXXI, S. 1, 2013, ss. 1159-1164.

Tezcan, Durmuş, Mustafa Ruhan Erdem ve Murat Önok, **Teorik ve Pratik Ceza Özel Hukuku**, 16. Baskı, Seçkin Yayınları, Ankara, 201(.

Turan, Metin. **Bilişim Hukuku**, Seçkin Yayınları, Ankara, 2017.

Turan, Metin. **Karşılaştırmalı Hukukta Kişisel Verilerin Korunması**, Seçkin Yayınları, Ankara, 2019.

Uludere, Eda. **AB Genel Veri Koruma Tüzüğü ve Yer Bakımından Uygulanması**, Hukuk Postası 2017, Onikilevha Yayınları, İstanbul, 201(, 305-311.

Uygun, Murat. **Avrupa Birliği’nin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması** (Yayınlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2010.

Yarayan, Ali. **Türk Medeni Hukuku Temel Bilgiler**, Yetkin Yayınları, Ankara, 2013.

Yavuz, Can. **İnternet’teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı**, Seçkin Yayıncılık, Ankara, 201(.

Yılmaz, Sacit. **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Adalet Yayınevi, Ankara, 2016.

Yokuş Sevük, Handan. “Kişisel Verilerin Açıklanması”, **Türkiye Barolar Birliği, Tıp Ceza Hukukunun Güncel Sorunları, V. Türk Alman Tıp Hukuku Sempozyumu**, Ankara, 200(, ss. 7(2-(11.

Yüksel Civelek, Dilek. **Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi Uzmanlık Tezi** , Devlet Planlama Teşkilatı, Nisan 2011.

Zafer, Hamide. **Özel Hayat ve Özel Hayatın Gizli Alanının Ceza Hukukuyla Korunması TCK m.132-134** , Beta Yayınları, İstanbul, 2010.

Zeytin, Zafer ve Ömer Ergün. **Türk Medeni Hukuku**, Seçkin Yayıncılık, Ankara, 2010.

