



T.C.

**BURSA ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

**TÜRK CEZA HUKUKUNDA KİŞİSEL VERİLERİN
KORUNMASINA YÖNELİK SUÇLAR**

(YÜKSEK LİSANS TEZİ)

GİZEM BÜŞRA TİTREK

BURSA - 2020



T.C.

**BURSA ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

**TÜRK CEZA HUKUKUNDA KİŞİSEL VERİLERİN
KORUNMASINA YÖNELİK SUÇLAR**

(YÜKSEK LİSANS TEZİ)

GİZEM BÜŞRA TİTREK

Danışman:

DOÇ. DR. ZEYNEL TEMEL KANGAL

BURSA - 2020

T. C.

BURSA ULUDAĞ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

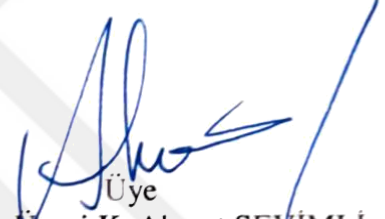
.....Kamu Hukuku..... Anabilim / Ana sanat
Dalı, Ceza ve Ceza Muhakemesi Hukuku Bilim Dalı'nda
70180.0002 numaralı Güzen Başra T. İREK
.....'nın

hazırladığı "Türk Ceza Hukukunda Kişisel Verilerin Korunmasına Yönelik
Sualler" konulu Yüksek Lisans (Yüksek Lisans / ~~Doktora~~ /
Sanatta Yeterlik Tezi / Çalışması) ile ilgili tez savunma sınavı, 22.01.2020 günü
13.10. - 14.10. saatleri arasında yapılmış, sorulan sorulara alınan cevaplar sonunda
adayın tezinin/çalışmasının başarılı (başarılı / ~~başarısız~~) olduğuna
oybirliği (oybirliği / ~~oy çokluğu~~) ile karar verilmiştir.



Üye (Tez Danışmanı ve Sınav
Komisyonu
Başkanı)

Doç. Dr. Zeynel T. KANGAL
Bursa Uludağ Üniversitesi



Üye
Dr. Öğr. Üyesi K. Ahmet SEVİMLİ
Bursa Uludağ Üniversitesi



Üye
Dr. Öğr. Üyesi Asuman AYTEKİN İNCEOĞLU
İstanbul Bilgi Üniversitesi

22.01.2020



SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS/DOKTORA İNTİHAL YAZILIM RAPORU

BURSA ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

.....K.A.M.Y. HUKUKU..... ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 07/01/2020

Tez Başlığı / Konusu: Türk Ceza Hukukunda Kişisel Verilerin Korunmasına
Yönelik Sorular

Yukarıda başlığı gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 136..... sayfalık kısmına ilişkin, 07/01/2020 tarihinde şahsım tarafından Turnitin..... adlı intihal tespit programından (Turnitin)* aşağıda belirtilen filtrelemeler uygulanarak alınmış olan özgünlük raporuna göre, tezimin benzerlik oranı %20'tür.

Uygulanan filtrelemeler:

- 1- Kaynakça hariç
- 2- Alıntılar hariç/dahil
- 3- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Özgünlük Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza

07.01.2020

Adı Soyadı: Gizem Başca TITREK

Öğrenci No: 701680002

Anabilim Dalı: Kamu Hukuku

Programı: Tezli Yüksek Lisans

Statüsü: Y.Lisans ~~Doktora~~

Danışman
(Adı, Soyad, Tarih)

Doç. Dr. Zeynel T. Kangal
07.01.2020 ZT/

* Turnitin programına Bursa Uludağ Üniversitesi Kütüphane web sayfasından ulaşılabilir

Yemin Metni

Yüksek Lisans tezi olarak sunduğum “Türk Ceza Hukukunda Kişisel Verilerin Kayıtına Yönelik Suçlar” başlıklı çalışmanın bilimsel araştırma, yazma ve etik kurallarına uygun olarak tarafımdan yazıldığına ve tezde yapılan bütün alıntılarının kaynaklarının usulüne uygun olarak gösterildiğine, tezimde intihal ürünü cümle veya paragraflar bulunmadığına şerefim üzerine yemin ederim.

Tarih ve İmza

07.01.2020

Adı Soyadı: Gizem Büsra TIREK

Öğrenci No: 701650002

Anabilim Dalı: Kamu Hukuku

Programı: Tezli Yüksek Lisans

Statüsü: Yüksek Lisans Doktora

ÖZET

Yazar Adı ve Soyadı: Gizem Büşra TİTREK

Üniversite: Bursa Uludağ Üniversitesi

Enstitü: Sosyal Bilimler Enstitüsü

Anabilim Dalı: Kamu Hukuku Anabilim Dalı

Tezin Niteliği: Yüksek Lisans Tezi

Sayfa Sayısı: XI + 136

Mezuniyet Tarihi:/...../2020

Tez Danışmanı: Doç. Dr. Zeynel Temel KANGAL

TÜRK CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK SUÇLAR

Günümüzde bilgi ve iletişim teknolojileri alanında yaşanan gelişmeler sonucunda, kişilere ait bilgilerin kaydedilmesi, yayılması gibi işlemler, çok daha kolay ve hızlı işlemler haline gelmiştir. Bu durum da kişisel verilerin korunması gerekliliğini ortaya çıkarmıştır. Uluslararası alanda uzun yıllardır kişisel verilerin korunması konusunda tartışmalar ve çalışmalar mevcuttur.

Kişisel verilerin korunması hakkı, pek çok hukuki düzenlemede ayrı bir hak olarak yer almayı özel hayatın gizliliği hakkı kapsamında korunmuştur. Ancak teknolojiye yaşanan gelişmelerle birlikte kişisel verilerin korunması hakkının önemi artmış, bu hak temel hak ve özgürlüklerden biri olarak sayılmıştır. Temel hak ve özgürlükler içinde yer alması sebebiyle de bu hakkın korumasına yönelik önlemler alınması daha da önemli hale gelmiştir.

Uluslararası alanda çeşitli hukuki metinlerle koruma altına alınan kişisel veriler, ülkemizde de çeşitli hukuki düzenlemeler ile korunmaktadır. Mevzuatımıza 2016 yılında dahil olan 6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin korunması alanındaki ana kaynaktır. Bu kanun, kişisel verilere ilişkin suçlar bakımından 5237 sayılı Türk Ceza Kanunu'na atıf yapmıştır.

Bu çalışmada kişisel verilerin korunması konusu incelenmiş olmakla beraber, çalışmamızın asıl amacı Türk Ceza Hukuku'nda kişisel verilerin korunmasına yönelik inceleme yapmak olduğundan, özellikle Türk Ceza Kanunu'nda düzenlenen suçlar ile kişisel verilere sağlanan koruma konusunda detaylı inceleme ve açıklamalara yer verilmiştir.

Anahtar Sözcükler:

Kişisel veri, kişisel verilerin korunması, özel hayatın gizliliği, Türk Ceza Kanunu, Kişisel Verilerin Korunması Kanunu.

ABSTRACT

Name and Surname: Gizem Büşra TİTREK

University: Uludag University

Institution: Social Science Institution

Field: Public Law

Degree Awarded: Master

Page Number: XI + 136

Degree Date:/...../2020

Supervisor: Assoc. Prof. Dr. Zeynel Temel KANGAL

TURKISH CRIMINAL LAW ON PROTECTION OF PERSONAL DATA IN CRIMES

Nowadays, as a result of developments in information and communication technologies, processes such as collection and distribution of personal data have become much simpler and faster. This situation revealed the necessity of protection of personal data. There have been international discussions and studies on the protection of personal data for many years.

The right to protection of personal data is not included in many legal arrangements as a separate right and is protected under the right to privacy of personal life. However, with the advances in technology, importance of the right to the protection of personal data has increased and this right has been considered as one of the fundamental rights and freedoms. As it is included in the fundamental rights and freedoms, it has become even more important to take measures to protect this right.

Personal data, which is protected by various legal texts in the international field, is also protected by various legal regulations in our country. 6698 numbered Law on the Protection of Personal Data, which was included in our legislation in 2016, is the main source on the subject of protection of personal data. This law refers to 5237 numbered Turkish Criminal Code in respect of crimes related to personal data.

Even though the protection of personal data has been examined in this study, since the main purpose of our study is to examine the protection of personal data in Turkish Criminal Code, detailed investigations and explanations on the protection of personal data are provided.

Keywords:

Personal data, protection of personal data, privacy, Turkish Criminal Code, Law on the Protection of Personal Data.

İÇİNDEKİLER

ÖZET	iv
ABSTRACT	v
İÇİNDEKİLER.....	vi
KISALTMALAR.....	xi
GİRİŞ	1

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE KORUNMASI

I. KİŞİSEL VERİ KAVRAMI	3
A. Kişi.....	3
B. Veri	4
C. Kişisel Veri.....	4
1. Kişi ile ilgili bir bilginin bulunması.....	5
2. Kişinin gerçek kişi olması	7
3. Kişinin kimliği belirli veya belirlenebilir olması.....	9
D. Hassas Veri.....	10
E. Diğer Kavramlar	11
II. KİŞİSEL VERİLERİN HUKUKİ NİTELİĞİ.....	14
A. Kamu Hukuku Açısından.....	14
B. Özel Hukuk Açısından.....	15
III. KİŞİSEL VERİLERİN KORUNMASI.....	18
A. Kişisel Verilerin Korunması Gerekliliği.....	18
B. Kişisel Verilerin Korunmasına İlişkin İlkeler	19
C. Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri.....	22
1. Özel nitelikli olmayan kişisel verilerin işlenmesinde hukuka uygunluk nedenleri	22

2. Özel nitelikli kişisel verilerin işlenmesinde hukuka uygunluk nedenleri	26
--	----

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ VE KORUNMASINA YÖNELİK DÜZENLEMELER VE UYGULAMA

I. KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ	29
II. KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK DÜZENLEMELER.....	30
A. Uluslararası Düzenlemeler.....	30
B. Çeşitli Devletlerde Kişisel Verilerin Korunması.....	35
1. Almanya	35
2. Fransa	36
3. İngiltere	37
4. İsviçre.....	38
5. Amerika Birleşik Devletleri	39
III. TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI	40
A. Anayasa.....	41
B. Türk Medeni Kanunu Ve Borçlar Kanunu.....	43
C. İş Kanunu	45
D. Ceza Muhakemesi Kanunu	45
E. Kişisel Verilerin Korunması Kanunu.....	47
IV. UYGULAMADA KİŞİSEL VERİLERİN KORUNMASI	53

ÜÇÜNCÜ BÖLÜM

TÜRK CEZA HUKUKU KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI

I. GENEL BİLGİLER.....	63
II. KİŞİSEL VERİLERİN KAYDEDİLMESİ SUÇU (TCK m. 135).....	64
A. Genel Olarak	64

B. Korunan Hukuksal Değer.....	65
C. Suçun Unsurları.....	65
1. Tipiklik.....	66
a. Suç tipinin genel özellikleri	66
b. Suçun maddi unsurları.....	67
(1) Fail	67
(2) Mağdur	68
(3) Suçun konusu.....	69
(4) Hareket	71
(5) Nitelikli unsurlar	73
c. Suçun manevi unsuru.....	74
2. Hukuka aykırılık unsuru.....	76
D. Kusur.....	80
E. Suçun Özel Görünüm Şekilleri.....	82
1. Teşebbüs.....	82
2. İştirak	82
3. İçtima	83
F. Yaptırım.....	84
G. Muhakemeye İlişkin Kurallar.....	85
III. VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME SUÇU (TCK m. 136)	86
A. Genel Olarak	86
B. Korunan Hukuksal Değer.....	87
C. Suçun Unsurları.....	88
1. Tipiklik.....	88
a. Suç tipinin genel özellikleri	88

b. Suçun maddi unsurları.....	90
(1) Fail	90
(2) Mağdur	91
(3) Suçun konusu.....	91
(4) Hareket	93
(5) Nitelikli unsurlar	97
c. Suçun manevi unsuru.....	98
2. Hukuka aykırılık unsuru.....	99
D. Kusur.....	101
E. Suçun Özel Görünüm Şekilleri.....	103
1. Teşebbüs.....	103
2. İştirak	103
3. İçtima	104
F. Yaptırım.....	107
G. Muhakemeye İlişkin Kurallar.....	108
IV. VERİLERİ YOK ETMEME SUÇU (TCK m. 138)	108
A. Genel Olarak	108
B. Korunan Hukuksal Değer.....	110
C. Suçun Unsurları	111
1. Tipiklik.....	111
a. Suç tipinin genel özellikleri	111
b. Suçun maddi unsurları.....	112
(1) Fail	112
(2) Mağdur	113
(3) Suçun konusu.....	114
(4) Hareket	114

(5) Nitelikli unsurlar.....	118
c. Suçun manevi unsuru.....	119
2. Hukuka aykırılık unsuru.....	120
D. Kusur.....	120
E. Suçun Özel Görünüm Şekilleri.....	121
1. Teşebbüs.....	121
2. İştirak	121
3. İçtima	122
F. Yaptırım.....	122
G. Muhakemeye İlişkin Kurallar.....	123
SONUÇ	125
KAYNAKLAR.....	129

KISALTMALAR

Kısaltma	Bibliyografik Bilgi
a.g.e.	Adı geçen eser
a.g.m.	Adı geçen makale
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AK	Avrupa Konseyi
APEC	Asia-Pacific Economic Cooperation
AÜHFD	Ankara Üniversitesi Hukuk Fakültesi Dergisi
AYM	Anayasa Mahkemesi
BM	Birleşmiş Milletler
B. No	Başvuru Numarası
C.	Cilt
CD.	Ceza Dairesi
CGK	Ceza Genel Kurulu
E.	Esas numarası
ed.	Editör
EÜHFD	Erzincan Üniversitesi Hukuk Fakültesi Dergisi
GVKT	Genel Veri Koruma Tüzüğü
HGK	Hukuk Genel Kurulu
İÜHFM	İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
K.	Karar sayısı
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
m.	Madde
OECD	Organisation for Economic Co-operation and Development
PVSK	2559 sayılı Polis Vazife ve Salahiyet Kanunu
RG.	Resmi Gazete
s.	Sayfa
S.	Sayı
ss.	Sayfa aralığı
sy.	Sayı
TBK	Türk Borçlar Kanunu
TBMM	Türkiye Büyük Millet Meclisi
TCK	Türk Ceza Kanunu
TDK	Türk Dil Kurumu
TMK	Türk Medeni Kanunu
vb.	ve bunun gibi
vd.	ve devamı
Y.	Yıl

GİRİŞ

Kişisel verilerin korunması, kişilerin yaşamlarını özgürce sürdürebilmeleri, takip edilme korkusuyla baskı altına alınmamaları ve kendilerini geliştirebilmeleri için çok önemlidir. Bilişim teknolojilerinde yaşanan gelişmelerle birlikte önemi artan kişisel verilerin korunması kavramı; tarih boyunca da gizliliğin korunması, bilgilerin korunması şeklinde ortaya çıkmış ve her zaman önemli bir konu olmuştur.

Kişisel verilerin hukuka uygun olarak toplanması bile, gerektiğinde yok edilmediği takdirde kişinin hakkını ihlal ederken, kötü niyetli olarak toplanması, dağıtılması kişiler için çok daha büyük tehlike arz etmektedir. Bilişim teknolojilerinin bu kadar gelişmemiş olduğu tarihlerde, veriler dosyalarda, kağıt üzerine yazılı olarak toplanmaktaydı. Bu şekilde kişilere ilişkin bilgileri kaydetmek, kağıt ve dosya yığınları arasından bu bilgilere erişmek çok zahmetli olacağından, bilgiler bugün olduğu kadar tehlike altında değildi. Bugün ise kişilerin rızaları ile verdikleri bilgilerin rızaları olmaksızın satılması; bilgisayar virüsleri, bilgisayar sistemlerine izinsiz giriş gibi yöntemlerle bu verilerin hukuka aykırı şekilde elde edilmesi ve tek bir tuşa basılarak yine hukuka aykırı bir şekilde dağıtılabilmesi mümkündür.

Bu faaliyetler günümüzde ekonomik kaygılarla da yapıldığından, kişilerin, bilgilerinin haberleri ve izinleri olmaksızın işlenmesinden korunması çok büyük önem arz etmektedir. Bilgilerin satılmasının yanında ortaya çıkacak bir diğer olumsuzluk ise devlet tarafından, vatandaşlarına ilişkin toplanan bilgilerin, kişilerin aleyhine kullanılabilmesi ihtimalidir. Bu ve bunun gibi daha pek çok riskin ortaya çıkabilecek olması sebebiyle kişisel veriler ile ilgili yapılacak her türlü işlemin sınırlarının belirlenmesi, bu konuda önlemlerin alınması oldukça önemlidir.

Kişisel verilerin korunmasının bu kadar önemli olması sebebiyle gerek uluslararası düzenlemelerle gerekse de her ülkenin kendi ulusal mevzuatıyla, kişisel verilerin korunmasına yönelik adımlar atılmaktadır. Diğer ülkelerde ve uluslararası platformda oldukça uzun yıllardır bu konuda çalışmalar ve düzenlemeler yapılmaktadır. Ülkemiz, bu konudaki çalışmalara yeni yeni başlamış olsa da başta 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu olmak üzere, mevzuatımızdaki pek çok düzenlemede kişisel verilerin korunmasına ilişkin hükümler yer almaktadır.

Bu tez çalışması ile kişisel verilerin korunması konusu ceza hukuku kapsamında incelenecektir. Bunun için ise öncelikle, kişisel veri ve kişisel verilerin korunması hakkında kavramlar açıklanacak, daha sonra bu konuda kısa bir tarihi bilgi verilerek kişisel verilerin korunması konusunda yapılan hukuki düzenlemelerden söz edilecek; son olarak da Türk Ceza Kanunu'nda kişisel verilerin korunmasına yönelik düzenlenmiş olan suçlar incelenecektir.

Buna yönelik olarak da birinci bölümde, çalışmanın devamında kullanılacak kavramların anlaşılabilir olmasını sağlamak amacıyla başta kişi, veri, kişisel veri ve hassas veri olmak üzere kavramlar tanımlanacaktır. Bu kavramlara açıklık getirilmesinin ardından ise kişisel verilerin hukuki niteliği ve kişisel verilerin korunması konusunda incelemelere yer verilecektir.

Tez çalışmasının ikinci bölümünde ise öncelikle kişisel verilerin korunması hakkının tarihsel gelişimine kısaca değinilecek, daha sonra ise bu alandaki hukuksal düzenlemeler incelenecektir. Öncelikli olarak, kişisel verilerin korunmasına yönelik uluslararası düzenlemeler incelenecek, ardından farklı ülkelerin ulusal mevzuatlarında kişisel verilerin korunması konusuna değinilecek, son olarak da ülkemizde Anayasa ve Kişisel Verilerin Korunması Kanunu başta olmak üzere çeşitli kanunlarda yer alan kişisel verilerin korunmasına yönelik hükümler incelenecektir. Bu bölümde en son olarak ise kişisel verilerin korunmasına yönelik uygulamalara yer verilecek, bu bağlamda çeşitli kararlarla kişisel verilerin korunmasının nasıl gerçekleştiği daha somut olarak anlatılmış olacaktır.

Çalışmanın son bölümü olan üçüncü bölümde ise Türk ceza hukuku kapsamında kişisel verilerin korunması konusu işlenecek, buna yönelik olarak da Türk Ceza Kanunu'nda yer alan "kişisel verilerin kaydedilmesi", "verileri hukuka aykırı olarak verme veya ele geçirme" ve "verileri yok etmeme" suçları konusunda detaylı incelemeler yapılacaktır.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE KORUNMASI

I. KİŞİSEL VERİ KAVRAMI

Kişisel verilerin korunması hususuna ilişkin olarak gerek ulusal düzenlemelerde gerekse uluslararası düzenlemelerde pek çok kavram geçmektedir. Ülkemiz için yeni sayılabilecek bir alan olduğundan kullanılan kavramların anlamları tam olarak bilinmemektedir. Bu sebeple bu bölümde, ilerleyen bölümlerde de kullanılacak olan ve konu ile ilgili temel kavramlar açıklanacaktır.

A. KİŞİ

Kişi kavramı, günlük hayatımızda kullandığımız şekliyle Türk Dil Kurumu tarafından “*Kadın veya erkeğe verilen genel ad, şahıs, zat, nefer*”¹ olarak tanımlanmıştır. Hukuki olarak ise kişiyi “*kendilerine hukukun hak ve borç sahipliği yetkisini tanıdığı varlıklar...*” şeklinde tanımlayabiliriz². Buna göre hukuki olarak kişi, haklara ve borçlara sahip olabilen varlıklardır³.

Hukuki anlamda kişiler iki başlık altında incelenmektedir. Bunlar; gerçek kişiler ve tüzel kişilerdir.

Gerçek kişi; insanlardır, fiziki bir varlığı, bilinci ve iradesi olup irade beyanı ile hukuki sonuç doğurabilen varlıklardır⁴. Türk Medeni Kanunu’nun 28. maddesine göre; “*kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümlle sona erer.*”

¹Türk Dil Kurumu Güncel Türkçe Sözlük, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c483384d72341.45647739 (23.01.2019)

² Ejder Yılmaz, “Kişi”, (Öğrenciler İçin) *Hukuk Sözlüğü*, 4. b., Ankara: Yetkin Yayınları, 2012, s. 425.

³ Jale G. Akipek, Turgut Akıntürk, Derya Ateş Karaman, *Türk Medeni Hukuku, Başlangıç Hükümleri – Kişiler Hukuku*, 9.b., İstanbul: Beta Yayınevi, 2012, s. 229; Mehmet Ayan, Nurşen Ayan, *Kişiler Hukuku*, 8. b, Ankara: Seçkin Yayıncılık, 2016, s. 29; Şaban Kayıhan, Mustafa Ünlütepe, *Medeni Hukuk Bilgisi*, 4. b, Ankara: Seçkin Yayıncılık, 2017, s. 155.

⁴ Engin Dinç, *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye’nin Durumu*, (Yüksek Lisans Tezi), Diyarbakır: Dicle Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 14.

Tüzel kişi ise sosyal hayatın yarattığı zorunluluklar sebebiyle ortaya çıkan, gerçek kişiler gibi fiziki bir varlıkları olmayan insan veya mal topluluklarıdır. Tüzel kişiler de tıpkı gerçek kişiler gibi haklara ve borçlara sahip olabilirler, ehliyetleri vardır⁵.

Gerçek ve tüzel kişi ayrımının kişisel verilerin korunması konusundaki önemi bu korumadan yararlanabilecek kişilerin belirlenmesi noktasında önem arz etmektedir. Bu konu hakkında detaylı açıklama ilerleyen bölümlerde yapılacaktır.

B. VERİ

Veri kelimesi TDK tarafından farklı şekillerde tanımlanmıştır. Ancak çalışmamız ile daha yakından ilgisi bulunan tanımları “*Bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done*”, “*bilgi, data*” şeklindedir⁶.

Bilgi, veri ve enformasyonun farklı anlamlara gelen kavramlar oldukları genel kabul görmüş bir görüştür. Ancak bunların aralarındaki ilişki konusunda tartışma söz konusudur. Bununla birlikte kısaca; çeşitli işlemler sonucunda verinin enformasyona, enformasyonun da bilgiye dönüştüğünü ifade edebiliriz⁷.

Veri ve veri ile ilişkili kavramların tanımı bilişim teknolojileri ile ilgili çok fazla teknik bilgi barındırmaktadır. Bu kavramların tanımları, tam olarak ne anlama geldikleri bilişim teknolojileri bakımından oldukça önemlidir⁸; ancak kişisel verilerin korunması konusu açısından baktığımızda bu kavramları ayırt etmeye çalışmak yersiz bir karışıklığa sebep olacağından veri, enformasyon ve bilgi kavramları aynı anlamda kullanılacaktır.

C. KİŞİSEL VERİ

Kişisel verinin tanımına geçmeden önce yukarıda verilen kişi kavramına dair açıklamalar ışığında kişisel kavramını tanımlamak gerekmektedir. Kişisel kelimesi “*Kişi*

⁵ Akipek, Akıntürk, Ateş Karaman, a.g.e., s. 499-500; Ayan, Ayan, a.g.e., s. 201; Kayıhan, Ünlütepe, a.g.e., s. 211.

⁶ Türk Dil Kurumu Güncel Türkçe Sözlük, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c49b8a99754b3.76834606, (24.01.2019)

⁷ Elif Küzeci, *Kişisel Verilerin Korunması*, 2. b., Ankara: Turhan Kitabevi Yayınları, 2018, s. 10.

⁸ a.g.e., s. 12.

ile ilgili, kişiye ilişkin, kişinin kendi malı olan, şahsi, zati” şeklinde tanımlanabilir⁹. Buna göre en sade şekliyle kişisel veriyi kişi ile ilgili olan bilgiler olarak tanımlamak mümkündür.

6698 sayılı Kişisel Verilerin Korunması Kanunu “Tanımlar” başlıklı 3. maddesinde kişisel veri kavramının tanımına da yer vermiştir. Buna göre kişisel veri; “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” şeklinde tanımlanmıştır. Kişisel veri ulusal ve uluslararası düzenlemelerin bir kısmında¹⁰ da bu şekilde tanımlanmıştır.

Bu tanımdan yola çıkarak, kişisel veriden bahsedebilmemiz için öncelikle bir kişi ile ilgili bir bilginin bulunması gerektiği açıktır. Bunun dışında, bu kişinin bir gerçek kişi olması ve bunun yanında, bu kişinin kimliği belirli veya belirlenebilir olması da gerekmektedir. Bu unsurların bir arada olduğu durumlarda kişisel verinin varlığından söz etmek mümkün olacaktır.

1. Kişi ile İlgili Bir Bilginin Bulunması

Kişisel veri kavramının pek çok ulusal ve uluslararası düzenlemede, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” ifadesi ile tanımlandığını yukarıda belirtmiştik. Bu tanımdan yola çıkarak veriyi en basit haliyle “her türlü bilgi” olarak ele almamız mümkündür. Söz konusu her türlü bilgi kavramının kapsamı ise oldukça geniştir. Kişinin özel ve aile hayatı, ekonomik, sosyal ve iş ilişkileri gibi bilgiler kişisel veri kapsamında yer almaktadır. Kişinin şifreleri gibi gizli bilgileri ya da fiziksel

⁹ Türk Dil Kurumu Güncel Türkçe Sözlük, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c49e6ea97dc16.28761191

¹⁰ 95/46/EC sayılı ve 24 Ekim 1995 tarihli Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki Avrupa Birliği Konseyi ve Avrupa Parlamentosu Direktifi'nin 2/a maddesinde kişisel veri, “belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgiler” şeklinde tanımlanmıştır. Direktif metni için bakınız: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (23.04.2019); aynı tanım 95/46/EC sayılı direktifi ilga eden 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 4. maddesinde de bulunmaktadır. Tüzük metni için bakınız: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>, (22.07.2019).

5237 sayılı Türk Ceza Kanunu'nun 135. madde gerekçesinde ise “gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir” ifadesi yer almaktadır. Gerekçe metninin tamamı için bakınız: www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc (23.04.2019).

özellikleri gibi herkesçe bilinmesi mümkün olan, gizli olmayan bilgileri de kişisel veri kapsamındadır. Bilginin öznel ya da nesnel olması da kişisel veri olması konusunda etkili değildir. Kişinin saç rengi ya da mesleği gibi nesnel bilgilerin yanında, yardımsever ya da azimli olması gibi kişiden kişiye değişebilecek düşünceler de kişisel veri olarak değerlendirilir. Bilginin kağıt üzerinde ya da bilgisayarda saklanması, görüntü, ses, yazı niteliğine sahip olması da kişisel veri olması noktasında önemli değildir, tamamı kişisel veri kapsamındadır¹¹.

Kişi hakkındaki doğru bilgiler gibi yanlış bilgiler de kişisel veri kapsamındadır. Bu konuda mevzuatta yalnızca gerçek verilerin korunması gerektiği yönünde bir düzenlemeye yer verilmemiştir. Ayrıca gerek Anayasa'da (m. 20/3) gerekse Kişisel Verilerin Korunması Kanunu'nda (m. 11/1-d) kişinin hakkındaki yanlış bilgilerin düzeltilmesini isteme hakkı olduğu belirtilmiş, dolayısıyla kişilerin, kendileri hakkındaki yanlış bilgiler sebebiyle zarar görmeleri de engellenmiştir. Yanlış bilgilerin de kişisel veri kapsamında değerlendirilmesi, kişilerin menfaatlerinin tam anlamıyla korunabilmesine olanak sağlayan bir durumdur; çünkü gerçek bilgilerden yanlış bilgiler insanları daha zor durumda bırakabilmekte ve dolayısıyla daha zarar verici olabilmektedir¹².

Değişik özelliklere sahip olabilen bu verilerin ortak özelliği kişi ile ilgili olmasıdır. Söz konusu veriler içerik, amaç ya da sonuç yönünden kişi ile ilgili olabilmektedir¹³.

Verinin içerik bakımından kişi ile ilgili olması onun kişi hakkında bir bilgi olduğu anlamına gelmektedir. Bir kişinin okul bilgileri, iş bilgileri ya da özgeçmişi kişi hakkında bilgiler olduğundan içerik bakımından kişisel veriyi oluşturmaktadır. Bazı durumlarda ise veriler doğrudan kişi hakkında olmasa bile amaç ya da sonuç yönünden kişi ile ilgili bir bilgi ortaya çıkabilmektedir. Kişiye ilişkin bir bilgi elde etmek amacıyla veri toplanması durumunda ise amaç yönünden kişi ile ilgili bilgiden söz etmek mümkündür. Bir fabrikada bulunan bir makinenin faaliyetine ilişkin veriler makine ile ilgili olarak değil de, onu kullanan işçinin çalışma performansını ölçmek amacıyla kullanılıyorsa burada

¹¹ Hüseyin Can Aksoy, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, 1. b., Ankara: Çakmak Yayınevi, 2010, s. 13-16.

¹² Hale Akdağ, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, 1. b., Ankara: Adalet Yayınevi, 2013, s. 10-13.

¹³ Aksoy, a.g.e., s. 28.

amaç yönünden kişi ile ilgili bir veri söz konusu olacaktır. Asıl amacın doğrudan kişiye ilişkin veri toplamak olmadığı durumlarda toplanan veri sonuç olarak bir kişiyi de etkiliyorsa bu durumda da kişi ile ilgili bilgi bulunmaktadır denilebilir. Örneğin iyi hizmet ve yakıt tasarrufu sağlanması amacıyla kurulan taksilerin lokasyonlarının uydudan izlenmesi ve en yakın taksinin müşteriye almasını sağlayan bir sistem ile toplanan veriler taksi şoförü hakkında değil araç hakkındadır, sistemin kullanılmasındaki amaç da şoförün çalışmasıyla ilgili bilgi toplamak değil uygun güzergahları belirlemektir. Ancak sonuç olarak bu sistem şoförlerin çalışma performansının takip edilmesine, hız limitlerine uyulup uyulmadığının, uygun güzergahın kullanılıp kullanılmadığının ya da şoförün aracını durdurup dinleniyor olup olmadığının tespitine olanak sağlamaktadır. Bu durumda da sonuç bakımından kişi ile ilgili bir verinin söz konusu olduğu açıktır. Dolayısıyla toplanan ya da kullanılan veri doğrudan kişi hakkında olmasa bile kişisel veriden bahsetme olanağı bulunan durumlar söz konusu olabilmektedir¹⁴.

2. Kişinin Gerçek Kişi Olması

Kişisel verilerin korunmasına yönelik düzenlemelerin kişi bakımından kapsamının belirlenmesi ve uygulamaların buna göre yapılması gerekmektedir. Genel görüşe göre korunması gereken veriler gerçek kişilere ait veriler olsa da, tüzel kişilerin de bu korumadan yararlanması gerekip gerekmediği konusunda tartışmalar mevcuttur.

Mülga 95/46/EC sayılı Direktif'te, "108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" Başlıklı Avrupa Konseyi Sözleşmesinde¹⁵ ve 6698 sayılı KVKK'da kişisel veri tanımlanırken "gerçek kişiye ilişkin her türlü bilgi" şeklinde bir tanım yapılmıştır. Söz konusu düzenlemeler açıkça gerçek kişiden söz ettiğine göre korumanın gerçek kişinin verilerine ilişkin olması gerektiği açıktır. Ancak bunun yanında 108 sayılı Avrupa Konseyi Sözleşmesi'nin 3. maddesinin 2. fıkrasının b bendi isteyen devletlerin bu kapsama tüzel kişileri de almasına imkan sağlamaktadır. Avusturya, Danimarka, Lüksemburg ve İsviçre Veri Koruma Kanunları

¹⁴ Article 29 Data Protection Working Party, *Opinion 4/2007 On The Concept Of Personal Data*, <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf>, (31.05.2019), s.11; Aksoy, a.g.e., s. 28-30.

¹⁵ Sözleşme için bakınız: http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktaraflioz/ak/turkce/108_tur.pdf (01.06.2019).

gerçek kişilerin yanında tüzel kişileri de koruma kapsamına almaktadır¹⁶. 2018 yılında yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğü ise yalnızca gerçek kişilerin verilerinin korunmasına yönelik olarak düzenlenmiştir¹⁷.

KVKK'nın 1. maddesinde bu kanunun amacının, kişilerin temel hak ve özgürlüklerinin korunması olduğu belirtilmektedir. Korunacak hak ve özgürlüklerin başında ise özel hayatın gizliliği olduğu kanunda açıkça ifade edilmektedir. Bu durum göz önüne alındığında koruma kapsamına tüzel kişileri almak bu amaca uygun olmayacağı gibi, gerçek kişilere yönelik korumanın zayıflamasına da sebep olabilecektir¹⁸. Her ne kadar tüzel kişilerin kişilik hakları dolayısıyla kişisel verilerinin korunması gerektiği yönünde görüşler¹⁹ mevcut olsa da, kanımızca kişisel verilerin korunması hakkı insan hakları kapsamındadır ve bu sebeple tüzel kişilerin bu haktan yararlanması mümkün olmayacaktır.

Bizim de katıldığımız bir görüşe göre ise, özel hayat yalnızca gerçek kişilere ait bir alan olduğundan tüzel kişiler bakımından ancak ticari sırların korunması mümkün olabilecektir²⁰. TCK'ya baktığımızda kişisel verilerin korunmasına ilişkin suçlar “Özel hayata ve hayatın gizli alanına karşı suçlar” bölümünde düzenlenmektedir. Tüzel kişiler bakımından özel hayat gibi bir alanın söz konusu olması mümkün değildir, ancak ticari sır kavramı mümkün olabilecektir. Kanun koyucu tüzel kişiler için mümkün olan ticari sır kavramını kişisel veri kavramından ayırmış ve “Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması suçu”nu TCK 239. maddede ekonomi, sanayi ve ticarete ilişkin suçlar bölümünde ele almıştır. Tüzel kişiler için korunması gereken ticari sırların farklı bir bölümde düzenlenmiş olması kişisel verilerin korunmasının yalnızca gerçek kişilere tanınan bir hak olduğu görüşümüzü destekler niteliktedir.

¹⁶ Oğuz Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 1. b., İstanbul: Beta Yayınevi, 2008, s. 122; Nafiye Yücedağ, “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”, *İÜHFİM*, C. LXXV, S. 2 (2017), s. 766.

¹⁷ Tüzük metni için bakınız: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN> (10.06.2019).

¹⁸ Küzeci, a.g.e., s. 325.

¹⁹ Doruk Gönen, *Tüzel Kişilerde Kişilik Hakkı ve Korunması*, 1. b., İstanbul: On İki Levha Yayıncılık, 2011, s. 43.

²⁰ Durmuş Tezcan, “Bilgisayar Karşısında Özel Hayatın Korunması”, *Anayasa Yargısı Dergisi*, C.8 (1991), s. 389.

Ancak tüzel kişiler hakkındaki veriler, belirli ya da belirlenebilir bir gerçek kişi hakkında ise, bir gerçek kişiyi belirli ya da belirlenebilir kılıyorsa bu durumda bu veriler hakkında da kişisel verilerin korunması gerekliliği ortaya çıkacaktır²¹.

3. Kişinin Kimliği Belirli veya Belirlenebilir Olması

Gerek ulusal gerekse uluslararası pek çok düzenlemede kişisel veri ile ilgili olarak, “kimliği belirli ya da belirlenebilir kişi”ye ait olma ifadesi yer almaktadır.

Kişinin kimliğinin belirli olması; isim, kimlik numarası gibi bilgilerle, herhangi bir işleme gerek duyulmadan kişinin kimliğinin ortaya çıkarılması anlamına gelmektedir. Kişinin kimliğinin belirlenebilir olması ise kişinin doğrudan tespit edilemeyip, elde edilmiş başka bilgilerin de kullanılmasıyla kişinin tespit edilmesi olarak tanımlanabilir²².

KVKK'nın 3. maddesinin gerekçesinde ise, bir kişinin belirli veya belirlenebilir olması, “*mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesi*”²³ olarak ifade edilmiştir. Gerekçede “sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veri” olarak sayılmıştır.

AB'nin 95/46/EC sayılı direktifinde belirlenebilir kişi “*Özellikle bir kimlik numarası referans alınarak doğrudan ya da dolaylı belirlenebilen ya da fiziksel, psikolojik, akli, ekonomik, kültürel veya sosyal kimliğine özgü bir veya birden çok faktörle tanımlanabilen kişi*”²⁴ şeklinde tanımlanmıştır. GVKK'de ise belirlenebilir kişi, “*isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak belirlenebilen gerçek bir kişi*” olarak tanımlanmıştır.

²¹ Şimşek, a.g.e., s. 123.

²² Şimşek, a.g.e., s. 122; Korkmaz, a.g.e., s. 37.

²³ Kişisel Verileri Koruma Kurumu, *Madde ve Gerekçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü*, s. 9, <https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu> (13.06.2019).

²⁴ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

Kişinin belirlenebilir olup olmadığı konusu somut olaya göre değerlendirilmesi gereken bir durumdur. Örneğin çok yaygın bir isme sahip kişinin yalnızca isminden belirlenebilmesi mümkün değilken, bir dersi alan kişiler içinden kişinin ismi ile belirlenmesi mümkün olabilecektir. Burada ilk durum için kişisel verinin varlığından söz etmek olanaksızken ikinci durumda kişisel verinin varlığı söz konusudur²⁵. Bu duruma benzer şekilde, elindeki veriyi kullanarak bir kişiyi ortaya çıkarma imkanına sahip olanlar bakımından kişisel veri sayılan bilgiler, kişiyi ortaya çıkarma imkanına sahip olmayanlar için kişisel veri niteliğini haiz olmayacaktır²⁶. Kişinin bu imkana sahip olup olmadığı hususu değerlendirilirken, henüz bu imkana sahip olmasa da, sahip olma ihtimali bulunup bulunmadığının da değerlendirilmesi gerektiği kanısındayız. Eğer böyle bir ihtimal söz konusu ise kişisel veriler bakımından bir tehlike ortaya çıkacağından, bu durumda da kişisel verinin varlığından söz etmek gerekecektir.

D. HASSAS VERİ

Hassas veriler, kişisel verilerin daha fazla korunması gereken alanını oluşturur. Kişilerin ırkı ve etnik kökeni, ten rengi, siyasi görüşleri, dini ve felsefi inançları, sendika üyelikleri, sağlık ve cinsel yaşamı ve mahkumiyetlerini içeren bilgiler diğer bilgilere göre daha özel nitelikte olduklarından hassas veri olarak adlandırılırlar. Yürürlükte olan GVKT ve mülga 95/46/EC sayılı Veri Koruma Direktifinde de bu verilerin neler olduğu sayılmış ve işlenmeleri yasaklanmıştır. Ancak bazı istisnai durumlarda işlenmelerine izin verilebileceği de belirtilmiştir. Hassas veriler kavramının içerisine ne tür verilerin gireceği hemen hemen her ülkede benzer olsa da, ülkelere göre farklı uygulamalar da söz konusu olabilmektedir. Örneğin, Polonya’da genetik bilgiler ve bağımlılıklar, Çek Cumhuriyeti’nde biyometrik bilgiler, Estonya’da engellilik durumu, Finlandiya’da sosyal yardımlar hassas veri kapsamında yer alan bilgilerdendir²⁷.

KVKK ise hassas veri kavramı yerine “özel nitelikli kişisel veri” kavramını tercih etmiş ve 6. maddede; “*kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini,*

²⁵ Melike Köse Aysun, *Kişisel Verilerin Kaydedilmesi Suçu (TCK m.135)*, 1. b., Ankara: Seçkin Yayıncılık, 2018, s. 34.

²⁶ Aksoy, a.g.e., s. 27.

²⁷ Cemil Kaya, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, *İÜHFİM*, C. LXIX, S.1 – 2 (2011), s. 318-319.

mezhebi veya diđer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliđi, sađlıđı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veri”ler olarak sayılmıştır. Bu verilerin, kişilerin açık rızası olmadan işlenmesi ise yasaklanmıştır.

TCK 135. maddede ise *“kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sađlık durumlarına veya sendikal bağlantılarına ilişkin”* bilgiler hassas veri kapsamına alınmış; bu veriler bakımından verilecek ceza artırılarak hassas verilerin korunmasının daha etkin olması sađlanmıştır.

KVKK’da da kişisel verilerin, kişilerin açık rızası olmaksızın işlenebileceđi haller 6. maddede sayılmıştır. Buna göre; maddede sayılan *“sađlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sađlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sađlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sađlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüđü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir”*.

E. DİĐER KAVRAMLAR

Kişisel verilerin korunması ile ilgili temel kavramların yanında konu ile ilişkili ya da konunun anlaşılmasını sađlayacak birtakım kavramlar bulunmaktadır. Bu kavramların da açıklanması çalışmamızın ilerleyen bölümlerinin daha anlaşılabilir olmasını sađlayacaktır.

Öncelikle bir önceki bölümde hassas veri kavramının tanımlanmasının ardından, *“anonim veri”* kavramını da açıklamak yerinde olacaktır. KVKK’nın 3. maddesinde anonim hâle getirme *“kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliđi belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi”* olarak tanımlanmıştır. Buna göre, istatistik ya da araştırma gibi amaçlarla kaydedilen, ancak *“kimliđi belirli ya da belirlenebilir bir kişi”* ile ilişkilendirilmesi mümkün olamayacak bir hale getirilen bilgilere anonim veri denilmektedir. Bu verilerin

herhangi bir kişi ile ilişkilendirilmesi mümkün olmadığından kişisel veri olarak değerlendirilmesi ve koruma altına alınması söz konusu değildir²⁸.

Kişisel verilerin korunmasının amacı, verilerin işlenmesinde kişilerin haklarının korunması olduğuna göre veri işlenmesi de açıklamamız gereken kavramlar arasında yer almaktadır. Kişisel verilerin işlenmesi kavramı KVKK m. 3'te "*kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*" olarak ifade edilmiştir. Aynı maddenin gerekçesinde ise kişisel verilerin işlenmesi kısaca, "*kişisel verilerin işlenmesi, verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlem türleri*" ifadesiyle tanımlanmıştır.

KVKK'ya göre veri işleyen, "*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi*", ilgili kişi, "*kişisel verisi işlenen gerçek kişiyi*", veri sorumlusu, "*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi*" ifade etmektedir.

Kişisel verilerin korunması ile ilgili inceleyeceğimiz son kavram ise unutulma hakkıdır. Unutulma hakkı; kişilerin, internette bulunan kişisel verilerinin arama sonuçlarında isimleriyle bağlantılı olmamasını, internet ortamında kendileri ile ilgili bilgilerin yok edilmesini talep etme hakkı olarak tanımlanmaktadır²⁹. Unutulma hakkının kapsamının internette yer alan verilere ilişkin olduğu yönündeki tanımlamalara karşılık, bu kapsamın daha geniş yorumlanması gerektiği, dijital ortamda yer alan verilerin yanında yer almayan veriler için de unutulma hakkının tanınması gerektiği yönünde

²⁸ Uğur Ersoy, *Bir İnsan Hakları Kavramı Olarak "Kişisel Verilerin Korunması"*, (Yüksek Lisans Tezi), Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2009, s. 17.

²⁹ Can Yavuz, *İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı*, 2. b., Ankara: Seçkin Yayıncılık, 2018, s. 45; Aydın Akgül, "Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" ve AB Adalet Divanı'nın "Google Kararı"", *Türkiye Barolar Birliği Dergisi*, S.116 (2015), s. 34.

görüşler mevcuttur³⁰. Kişilerin geçmişlerinde olan ve silinmesini isteyecekleri veriler, yalnızca dijital ortamda değil, kağıt üzerinde de bulunabilir. Unutulma hakkı, kişisel verilerle dolayısıyla özel hayatın gizliliği hakkı ile ilişkili bir hak olduğundan, bu hakkın yalnızca dijital ortam ile sınırlandırılmaması, dijital olmayan ortamlar için de tanınması gerektiği görüşüne katılmaktayız.

Unutulma hakkı GVKT'nin 17. maddesinde düzenlenmiştir. Ülkemizdeki hukuki düzenlemelerde “unutulma hakkı” ifadesi açıkça yer almasa da, kişilere ait verilerin silinmesine ilişkin hükümler yer almaktadır. Anayasa m. 20/3'te herkesin kendisi ile ilgili kişisel verilerin silinmesini talep etme hakkı olduğu belirtilmiştir. Aynı şekilde KVKK m. 7'de veri sahibinin talebiyle, kişisel verilerin silinebileceği, yok edilebileceği ya da anonim hale getirilebileceği düzenlenmiştir. Unutulma hakkı, ülkemizdeki yargı kararlarında da tanınmış bir haktır³¹.

³⁰ Eren Sözüer, *Unutulma Hakkı, İnsan Hakları Hukuku Perspektifinden Bir İnceleme*, 1. b, İstanbul: On İki Levha Yayıncılık, 2017, s. 23; Zeynel T. Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, 1. b, İstanbul: On İki Levha Yayıncılık, 2019, s. 3; Akgül, a.g.m., s. 36.

³¹ Yargıtay Hukuk Genel Kurulu 2015 tarihli bir kararında unutulma hakkını kabul etmekle birlikte bu hakkın yalnızca dijital ortamdaki veriler ile sınırlı kalmaması, geniş yorumlanması gerektiğini ifade etmiştir: “Ayrıca şunun da ifade edilmesi gereklidir ki; unutulma hakkı tanımlarına bakıldığında her ne kadar dijital veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiği açıktır. // Davacı, geçmişte yaşadığı kötü bir olayın toplum hafızasından silinmesini istemektedir. Unutulma hakkı ile geçmişindeki yaşanan talihsiz bir olayın unutulmasıyla geleceğini serbestçe şekillendirmek, diğer bir deyişle hayatında, yeni bir sayfa açma olanağı istemektedir. Kaldı ki, davacı da yargılama sırasında verdiği dilekçelerinde bu istem üzerinde ısrarla durmuştur. Davacı unutulma hakkı ile özel hayatına ilişkin kişisel verilerinin üçüncü kişiler tarafından bilinmemesini, aradan geçen süre nedeniyle toplum hafızasından silinmesini istemektedir. // Bu bağlamda değerlendirildiğinde; 4 yıl önce gerçekleşen bir olayın mağduru olan kişinin adının açık bir şekilde yazılarak kitapta yer alması halinde unutulma hakkının bunun sonucunda da davacının özel hayatının gizliliğinin ihlal edildiği kabul edilmelidir. Avrupa Birliği Adalet Divanı'nın Google Kararı'nda açıkladığı gibi ilgili verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi şeklinde, üstün bir kamu yararını ortaya koyan özel sebepler bulunmadığına göre bilimsel esere alınan kararda kişisel veriler açık bir şekilde yer almamalıdır. // Görüşmeler sırasında azınlıkta kalan üyeler mahkeme kararlarında yer alan isimlerin rumuzlanmasına gerek olmadığını, yargılamanın istisnalar haricinde açık bir şekilde yapıldığını hükmün alenen tefhim edildiğini, bu nedenle özel hayatın gizliliğinin ihlal edilmediğini savunmuşlar ise bu görüş sorunun mahkeme kararlarında isimlerin rumuzlanmadan yer alması değil, kararların kitaba alınması sırasında rumuzlanması gerekmediği sorunu olduğu gerekçesi ile kurul çoğunluğu tarafından kabul edilmemiştir. // O halde davacının isminin rumuzlanmadan kitapta yer almasının unutulma hakkını ve bunun neticesinde özel hayatın gizliliğini ihlal ettiği dikkate alındığında davacı lehine manevi tazminat koşullarının gerçekleştiğinin kabulü zorunludur”. (HGK, 17.6.2015, E. 2014/4-56, K. 2015/1679, www.kazanci.com, (29.11.2019)).

Anayasa Mahkemesi de 2016 tarihli bireysel başvuru kararında unutulma hakkını tanımıştır: “Unutulma hakkı Anayasa'mızda açıkça düzenlenmemiştir. Bununla birlikte Anayasa'nın “Devletin temel amaç ve ödevleri” başlığı altında düzenlenen 5. maddesinde “insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak” ifadesi ile devlete pozitif bir yükümlülük yüklenmiştir. Bu yükümlülük bağlamında Anayasa'nın 17. maddesinde düzenlenen kişinin manevi bütünlüğü bağlamında

II. KİŞİSEL VERİLERİN HUKUKİ NİTELİĞİ

Kişisel verilerin hukuki niteliğinin ne olduğu konusuna ilişkin görüşler, bu hakkın hangi menfaat ve hukuki varlık ile ilgili olduğu noktasında farklılaşmaktadır. Bu görüşleri özel hukuk açısından ve kamu hukuku açısından incelememiz mümkündür.

A. KAMU HUKUKU AÇISINDAN

Kişisel verilerin hukuki niteliğine ilişkin görüş farklılıkları; kişisel verilerin, korunmasının ekonomik bir hak mı, yani kişisel verinin, tasarrufta bulunulabilecek bir mal olarak mı görülmesi gerektiği ya da kişilerin doğuştan sahip olduğu bir hak, yani insan hakkı mı olduğu konusunda ayrılmaktadır³². ABD’de kişisel verilerin korunmasının ekonomik bir hak olduğuna dair görüş yaygınken, Avrupa’da ise insan hakkı olduğu yönündeki görüş daha fazla desteklenmektedir³³. İnsan hakları, kişilerin yalnızca insan olmaları sebebi ile doğuştan sahip olduğu, vazgeçilemez, devredilemez ve dokunulamaz haklardır. Bu haklar birçok uluslararası belgede ve pek çok ülkenin anayasasında koruma altına alınmıştır. Kişisel verilerin korunması hakkının da, insan hakları içerisinde yer alan

şeref ve itibarının korunması hakkı ve Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı ile birlikte düşünüldüğünde, devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek "yeni bir sayfa açma" olanağı verme hususunda bir sorumluluğu olduğu açıktır. Özellikle kişisel verilerin korunması hakkı kapsamında kişisel verilerin silinmesini talep edebilme hakkı, kişilerin geçmişlerinde yaşadıkları olumsuzlukların unutulmasına imkân tanımayı kapsamaktadır. Dolayısıyla Anayasa'da açıkça düzenlenmeyen unutulma hakkı, İnternet vasıtasıyla ulaşılması kolay olan ve dijital hafızada bulunan haberlere erişiminin engellenmesi için Anayasa'nın 5., 17. ve 20. maddelerinin doğal bir sonucu olarak karşımıza çıkmaktadır. Diğer taraftan unutulma hakkının kabul edilmemesi, İnternet vasıtasıyla kolayca ulaşılabilir ve uzun süre muhafaza edilebilir kişisel veriler nedeniyle başkaları tarafından kişiler hakkında ön yargı oluşturabilmesi nedeniyle manevi varlığının geliştirilmesi için gerekli onurlu bir yaşam sürdürmesine ve manevi bağımsızlığına müdahaleyi sürekli kalmaktadır. // Anayasa Mahkemesinin ifade ve basın özgürlükleri ile şeref ve itibarın korunması hakkı arasındaki dengelemeye ilişkin kararlarında Anayasa'nın 17. maddesinin birinci fıkrası temelinde değerlendirme yaptığı gözetilerek unutulma hakkına ilişkin iddiaların İnternet ortamındaki haberlerin kişisel veriler ile arasındaki ilişki dikkate alınarak Anayasa'nın 17. maddesinin birinci fıkrası kapsamında inceleme yapılması gerekmektedir". (AYM, 03.03.2016, N.B.B., B. No: 2013/5653, RG. 24.08.2016, sy: 29811).

Yargıtay ve Anayasa Mahkemesi'nin unutulma hakkına yer verdiği diğer karar örnekleri için bakınız: AYM, 15.03.2018, C.K., B. No: 2014/19685, RG. 17.05.2018, sy: 30424; Yargıtay 19. CD., 05.06.2017 E. 2016/15510, K. 2017/5325).

³² Küzeci, a.g.e., s. 62.

³³ a.g.e., s. 63-69.

“özel hayatın gizliliği hakkı” kapsamında olduğu dolayısıyla insan hakkı olduğu yönünde görüşler mevcuttur³⁴.

B. ÖZEL HUKUK AÇISINDAN

Özel hukuk açısından; kişisel verilerin korunmasının özünün kişilik hakkı, mülkiyet hakkı ve fikri mülkiyet hakkı olduğu yönünde üç temel görüş ortaya çıkmaktadır³⁵.

Kişisel verilerin kişilik hakkı kapsamında olduğunu savunan görüşe göre, kişisel veriler; kişilik haklarından olan özel hayat ile ilişkili bir kavram olduğundan, kişilik hakkı kapsamında yer almaktadır³⁶. Kişilik hakkı; kişilerin, maddi ve manevi bütünlüğüne, menfaat ve ilişkilerine karşı oluşacak saldırılardan kaçınılmasını diğer kişilerden isteme yetkisi verir³⁷. Kişilik hakkını, maddi değil manevi değeri olan; kişilerin hayat, vücut bütünlüğü, şeref ve haysiyet, isim, özel hayat gibi değerleri üzerindeki hakkı şeklinde tanımlamak mümkündür³⁸. Kişilik hakları mutlak ve kişiye sıkı sıkıya bağlı haklardır. TMK'nın 24. maddesinde “*Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir*” denilerek genel mahiyette bir kişilik hakkı tanımlanmıştır³⁹. Kamu hukuku kapsamında yer alan insan hakları kavramının özel hukuktaki yansıması kişilik hakları olarak ortaya çıkmaktadır⁴⁰. Kişilik hakkı Medeni Kanun (TMK m. 23-25) ve Borçlar Kanunu'nda (TBK m. 58) düzenlenen bir hak olsa da, yalnızca özel hukuk alanında var olan bir hak değildir. Özel hukukun yanında kişilik hakkı, anayasal korumaya (Anayasa m. 17) da sahip bir haktır. Bu sebeple kişilik hakkı anayasal niteliğe sahip, temel bir insan hakkıdır⁴¹.

³⁴ Doğan Kılınç, “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, *AÜHFD*, C.61, S.3 (2012), s. 1097-1098.

³⁵ Aksoy, a.g.e., s. 37.

³⁶ Kılınç, a.g.m., s. 1099.

³⁷ Akipek, Akıntürk, Ateş Karaman, a.g.e., s. 341.

³⁸ Ayan, Ayan, a.g.e., s. 85; Kayıhan, Ünlütepe, a.g.e., s. 189-190; Zafer Zeytin, Ömer Ergün, *Türk Medeni Hukuku*, 4. b, Ankara: Seçkin Yayıncılık, 2018, s. 87-88.

³⁹ Akipek, Akıntürk, Ateş Karaman, a.g.e., s. 345.

⁴⁰ Haluk Tandoğan, “Şahsiyetin Akit Dışı İhlallere Karşı Korunmasının İşleyiş Tarzı ve Basın Yoluyla Olan İhlallere Karşı Özel Hayatın Korunması”, *Ankara Hukuk Fakültesi Dergisi*, C.20, S.1 (1963), s. 15.

⁴¹ Şimşek, a.g.e., s. 132; Ayan, Ayan, a.g.e., s. 89.

95/46/EC sayılı Direktif'in amacı özellikle özel hayatın gizliliği⁴² başta olmak üzere kişilerin temel hak ve özgürlüklerinin korunması olarak belirtilmiştir⁴³. GVKT'nin amacı da benzer şekilde “gerçek kişilerin temel hakları ve özgürlükleri ve özellikle, kişisel verilerin korunması hakkının korunması” olarak belirtilmiştir. KVKK'nın amacı da bu düzenlemeler ile paralel şekilde “...*başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak...*” olarak ifade edilmiştir. Dolayısıyla söz konusu düzenlemelerin, bu görüşü temel aldığı söylemek mümkün olabilecektir.

Kişisel verilerin mülkiyet hakkı kapsamında olduğunu savunan görüş ise, kişisel verilerin hukuki niteliği konusundaki diğer bir görüştür. Bu görüşe göre, herkesin, kendisine ait kişisel verilerin sahibi olduğu ve bu verilerin nasıl kullanılacağını kontrol edebileceği kabul edilmektedir⁴⁴. Kişisel verilerin mülkiyet hakkına dayandırılması sonucunda, kişilerin bir bedel karşılığında verilerinin kullanılmasında anlaşmalar yapabileme imkanı bulacağı, bu yolla da şirketlerin toplamaları bir maliyet getireceğinden, toplanacak veriler konusunda daha titiz davranılacağı, her bilginin toplanmayacağı için de özel hayatın gizliliğinin daha etkili şekilde korunmuş olacağı savunulmaktadır⁴⁵.

Kişisel verilerin, kişilik hakkının bir parçası olduğunu düşünerek mülkiyet hakkı görüşüne karşı çıkanlar, veriler üzerinde mülkiyet hakkı olduğunun kabul edilmesi durumunda, kişilik haklarının ihlal edilmesi sonucunun doğacağını savunmaktadırlar. Mülkiyet hakkı görüşünü savunanlar ise bunun aksine, veriler üzerinde mülkiyet hakkı tanınması durumunda kişilerin, veri işleyenlerce sömürülmesinin önüne geçilebileceğini, bilgilerinin ne amaçla kullanılacağını kontrol edebilme imkanına sahip olabileceklerini, böylece özel hayatlarının ihlal edildiği endişesini yaşamayacaklarını savunmaktadırlar⁴⁶.

Kişisel veriler üzerinde mülkiyet hakkı tanınmasının verilerin gizliliği ve dolayısıyla kişilerin özel hayatları bakımından olumsuz sonuçlar doğmasına sebep olabileceği yönünde pek çok eleştiri mevcuttur. Veriler üzerinde mülkiyet hakkı tanınması durumunda, verileri satın alan kişi bunlar üzerinde tasarruf edebilecek, istediği

⁴² “Privacy” kelimesi kimi çevirilerde mahremiyet şeklinde ifade edilmişse de, mahremiyet özel hayatın gizliliğinden daha dar bir alanı kapsadığından İngilizce karşılığı “intimacy” kelimesi olduğundan çalışmamızda “privacy” deyimini özel hayatın gizliliği olarak ifade edilecektir. Benzer görüş ve detaylı açıklama için bakınız: Küzeci, a.g.e., s. 14-15.

⁴³ Aksoy, a.g.e., s. 47.

⁴⁴ Aksoy, a.g.e., s. 57.

⁴⁵ Küzeci, a.g.e., s. 64.

⁴⁶ Aksoy, a.g.e., s. 59.

gibi kullanabilecek ve satabilecektir. Bu durum da verilerin gizliliğinin ortadan kalkmasına, kişilerin verileri üzerindeki hakimiyetlerini kaybetmesine sebep olacaktır⁴⁷.

Kişisel verilerin hukuki niteliği hususundaki son görüş ise fikri mülkiyet hakkı görüşüdür. Bu görüş de mülkiyet hakkı gibi ABD’de savunulan bir görüştür. Bu görüşü destekleyenlere göre, fikri mülkiyet hakkı ile kişisel verilerin korunması arasında, bilgilerin korunması ve dağılımının kontrol edilmesi konusunda bir amaç benzerliği mevcuttur⁴⁸.

Hem kişisel veriler hem de fikri mülkiyet açısından kişiye ait olan, ancak kontrolünün kaybedilmesi mümkün olan bir değer mevcuttur. Fikri mülkiyet hakkında, eser sahibine tanınan eseri umuma arz yetkisi ve eserde değişiklik yapılmasını yasaklama yetkisinin kişisel veriler açısından da geçerli olacağı, kişisel veri sahibinin de bu yetkileri kullanarak verilerini koruyabileceği savunulmaktadır. Bu görüşe getirilen eleştirilerden birine göre; fikri mülkiyet hakkı, kişinin fikri ürünlerinin korunması için öngörölmüş bir haktır. Ancak kişisel veriler, fikri ürün değildir. Bunun yanında mülkiyet hakkı görüşüne getirilen eleştirilerin bir kısmı bu görüş için de geçerli olmaktadır⁴⁹.

Bu görüşlerin tamamında eleştirilen, eksik bulunan konular olduğundan hiçbiri kişisel verilerin hukuki niteliğini saptamada yeterli görülmemektedir. Bu sebeple kişisel verilerin hukuki niteliğinin enformasyonel self determinasyon hakkı olduğu savunulmaktadır. Bu hak ise kişilik hakkının bir görünümü olarak ortaya çıkmaktadır ve kişilerin, kendilerine ilişkin verilerden hangilerinin, kimler tarafından ve hangi koşullarda kullanılabilceğine karar verme hakkına sahip olması olarak tanımlanmaktadır⁵⁰.

Kişisel verilerin kişilik hakkı kapsamında olması durumunda, daha etkin korunma imkanı bulacağı kanaatindeyiz. Bunun yanında, kişilerin; kendilerine ilişkin verilerin, kimler tarafından, ne amaçla kullanıldığı gibi hususları bilme hakkına sahip olmaları, bu durumu kontrol edebilmeleri de gizlilik endişesi yaşamamaları bakımından önemlidir. Bu sebeple, kişisel verilerin hukuki niteliğinin, özel hukukta kişilik hakkının bir

⁴⁷ Küzeci, a.g.e., s. 66.

⁴⁸ Pamela Samuelson, “Privacy As Intellectual Property?”, *Stanford Law Review*, C.52, S.5 (2000), s. 1134.

⁴⁹ Küzeci, a.g.e., s. 66-67; Aksoy, a.g.e., s. 60-61; Samuelson, a.g.m., s. 1141-1148.

⁵⁰ Paul Schwartz, “The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination”, *American Journal of Comparative Law*, C.37, S.4 (1989), s. 689-690.

görünümü olarak ortaya çıkan enformasyonel self determinasyon hakkı olduğu yönündeki görüşe katılmaktayız. Veri sahibi kişilerin, bu veriler üzerindeki hakimiyetlerini korumaları bu durumda mümkün olabilecektir.

III. KİŞİSEL VERİLERİN KORUNMASI

Kişisel veriler gerek ulusal gerekse uluslararası pek çok düzenleme ile korunmaktadır. Bu düzenlemeler kişisel verilerin korunmasını sağlamak amacıyla işlenmeleri ile ilgili birtakım ilkeler belirlemiştir ve ancak bu ilkelere uyulması şartı ile kişisel veriler işlenebilmektedir. Kişisel verilerin korunmasına ilişkin bu ilkelerin yanında, bu korumaya neden ihtiyaç duyulduğu, kişisel verilerin neden geniş çapta korunan bir değer olduğu ve bu korumanın sınırsız olup olmadığı konularının açıklanması gerekmektedir.

A. KİŞİSEL VERİLERİN KORUNMASI GEREKLİLİĞİ

Kişilerin temel hak ve özgürlükleri gerek ulusal gerekse uluslararası çeşitli düzenlemeler ile koruma altına alınmıştır. Kişisel verilerin korunması hakkı da bu kapsamda değerlendirilebilecektir. Çünkü bu koruma ile veriler değil, veri öznesinin kişiliği korunmaktadır. Günümüz şartlarında bilginin değeri oldukça fazladır. Demokratik toplumlarda kişilerin temel haklarının, mahremiyetlerinin korunması kural olsa da, devletler vatandaşlarının güvenliğini sağlamak ve ihtiyaçlarını gidermek amacıyla birtakım verileri toplamaktadır. Devletler dışında özel hukuk tüzel kişileri de müşterilerine sağladıkları hizmetlerin kalitesinin kontrol edebilmek ve müşterileri hakkında bilgi sahibi olabilmek için kişisel verileri toplamaktadırlar. Bunun yanında kişisel verilerin üçüncü kişilere satılması bu kuruluşlar açısından gelir getirici bir faaliyet olmaktadır⁵¹.

Kişisel verilerin çok büyük önem arz ettiği bu ortamda verilerin korunması; veri sahiplerinin kişiliklerini geliştirebilmesi, verileri üzerinde söz hakkına sahip olabilmesi ve temel hak ve özgürlüklerin, dolayısıyla veri sahiplerinin korunması açısından

⁵¹ Aksoy, a.g.e., s. 78; Metin Çokmutlu, *Türk Ceza Hukukunda Kişisel Verilerin Korunması*, (Doktora Tezi), Kocaeli: Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, 2014, s. 38-39.

önemlidir. Bu korumanın olmadığı durumda kişilerin bütün bilgileri ve özel hayatları kontrol dışı bir şekilde şeffaf hale gelecektir. Bu da insan hakları ve onuru ile bağdaşmayan durumların oluşmasına sebep olabilecektir⁵². Bu sebeple kişilerin kendi verileri üzerinde söz sahibi olabilmesi, verilerin hukuka aykırı işlenmesinin önüne geçilerek koruma sağlanması son derece önemli bir gereksinimdir. Söz konusu koruma ise yalnızca bilgisayar ortamında otomatik işleme durumunda değil, el ile yapılan dosyalar ile verilerin toplanması konusunda da geçerli olacaktır.

Kişisel verilerin korunması hakkı her ne kadar kişiler için çok önemli bir gereklilik olsa da, bu koruma sınırsız değildir. Özellikle devletler tarafından vatandaşlara sunulan hizmetler ya da güvenlik gibi sebeplerle kişisel verilerin işlenmesi söz konusu olabilmektedir. Ancak bu işleme kişinin açık rızasına dayanmalıdır. Açık rızanın olmadığı durumlarda ise önemli bir kamusal yarar ve verilerin işlenmesine olanak sağlayan yasal temel bulunmalıdır. Ancak bu yasa Anayasa ile düzenlenen temel hakların sınırlandırılmasına ilişkin kurallara da uygun olmak zorundadır. Anayasaya uygun yasal bir düzenleme ya da kişinin açık rızasının bulunmadığı durumlarda bu hakkın sınırlandırılması dolayısıyla kişisel verilerin işlenmesi hukuka aykırı olacaktır⁵³.

B. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN İLKELER

Kişisel verilerin işlenmesi deyiminin tanımını yukarıda yapmıştık. Bu tanım dışında kişisel verilere ilişkin her türlü fiil kişisel verileri işlemek olarak değerlendirilebilir. Kişisel verilerin işlenmemesi asıl olmakla beraber birtakım ilkelere uymak şartı ile kişisel verilerin işlenmesi mümkündür⁵⁴.

Bu ilkeler GVKT'nin 5. maddesinde, “hukuka uygunluk, dürüstlük ve şeffaflık, amacın sınırlandırılması, verilerin en az seviyeye indirilmesi, doğruluk, saklama süresinin sınırlanması, bütünlük ve gizlilik, hesap verilebilirlik” olarak sayılmıştır. Mülga 95/46/EC sayılı Direktif'in 6. maddesinde de GVKT'den birtakım farklılıklar olsa da, benzer ilkeler sayılmıştır. Bunlar; “hukuka ve dürüstlük kurallarına uygun işleme, belirli,

⁵² Şimşek, a.g.e., s. 111-114.

⁵³ Şimşek, a.g.e., s. 127.

⁵⁴ Erbil Beytar, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 2. b., İstanbul: On İki Levha Yayıncılık, 2018, s. 61; Akdağ, a.g.e., s. 71.

açık ve meşru amaçlar için toplanma, toplanma ve/veya bunu izleyen işleme amaçları bakımından yeterli ve onlarla ilgili olma ve aşırı olmama, doğru ve eğer gerekli ise güncel olma, ilgili kişinin teşhis edilmesine olanak sağlayacak şekilde, kişisel verilerin toplandığı ya da daha sonra işlendiği amaçlar için gerekli olandan daha uzun süre tutulmama” olarak belirtilmiştir. KVKK’nın 4. maddesinde de kişisel verilerin işlenmesinde uyulması gereken genel ilkeler sayılmıştır. Direktif’e benzer şekilde; “hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” şeklinde ilkeler belirlenmiştir.

Hukuka ve dürüstlük kuralına uygunluk, pek çok düzenlemede yer alan ve diğer ilkelerin de kaynağını oluşturan ilkedir⁵⁵. Buna göre kişisel verilerin işlenmesi kapsamında değerlendirilen her türlü işlemin hukuka ve dürüstlük kurallarına uygun olarak gerçekleştirilmesi gerekmektedir. Yani kişisel verilerin toplanması aşamasından, işlenmesi ve silinmesi, yok edilmesi veya anonim hale getirilmesi aşamasına kadar her işlem bu ilkeye uygun olmak zorundadır⁵⁶. Buradaki hukuka uygunluk kavramı, detaylı açıklamaya ihtiyaç duymayacak bir kavramdır. İşlemlerin her türlü hukuki düzenlemeye uygun olarak yapılması gerektiğini ifade etmektedir⁵⁷. Dürüstlük kuralı ise, toplumun çoğunluğu tarafından benimsenen ve uygulanan; doğruluk, dürüstlük, ilişkilerde dikkat, özen ve güven esaslarına dayanan bir davranış şekli olarak tanımlanabilir⁵⁸. Konumuz açısından dürüstlük kuralına uygun olmayı ise veri sahiplerinin çıkarlarının ve beklentilerinin dikkate alınması şeklinde ifade edebiliriz⁵⁹. Bu durumda kişisel verilerin hukuki temele dayanmaksızın ve kanunda öngörülen amaca aykırı olarak kaydedilmesi ve işlenmesinin dürüstlük kuralına aykırı olacağını söyleyebiliriz⁶⁰.

Bir diğer ilke ise, verilerin belirli, açık ve meşru amaçlar için toplanmasıdır. Bu ilkenin uygulanabilmesi için öncelikle hukuki düzenlemelerde, verilerin toplanma ve

⁵⁵ Küzeci, a.g.e., s. 206.

⁵⁶ Sefer Oğuz, “Kişisel Verilerin Korunması Hukukunun Genel İlkeleri”, *Bilgi Ekonomisi ve Yönetimi Dergisi*, C.13, S.2 (2018), s. 132.

⁵⁷ Akdağ, a.g.e., s. 71.

⁵⁸ Akipek, Akıntürk, Ateş Karaman, a.g.e., s. 167.

⁵⁹ Lee A. Bygrave, *Data Protection Law, Approaching Its Rationale, Logic and Limits*, Hollanda: Kluwer Law International, 2002, s. 58’den aktaran Küzeci, a.g.e., s. 207.

⁶⁰ Şimşek, a.g.e., s. 85.

işlenme amacının tam ve açık olarak belirlenip tanımlanması gerekmektedir⁶¹. Veriler toplanırken; ilgili kişiler amaç konusunda bilgilendirilmeli, veri toplama bu amaca uygun olarak gerçekleştirilmeli ve veriler toplandıktan sonra da farklı bir amaçla kullanılmamalıdır⁶². Verilerin işlenmesinde amacın belirli ve açık olmasının yanında meşru olması da gerekmektedir. 95/46/EC sayılı Direktifin 7. maddesinde sayılan durumlardan birinin varlığı amacın meşru olduğunun kabulü için aranmaktadır. Buna göre; “ilgili kişinin açık bir şekilde rıza göstermesi, bir sözleşme yapmadan önce ilgili kişinin talebi üzerine önlem almak için ya da kişinin taraf olduğu bir sözleşmenin ifası için gerekli olması, veri sorumlusunun hukuki sorumluluğunu yerine getirmesi için işlemenin gerekli olması, ilgili kişinin yaşamsal menfaatlerinin korunması için işlemenin gerekli olması, işlemenin kamu yararının bulunduğu görevin yerine getirilmesi ya da veri sorumlusunun veya verilerin açıklandığı üçüncü kişinin resmi yetkisini kullanması için gerekli olması, Direktif’in 1/1. maddesi uyarınca koruma gerektiren veri öznesinin temel hak ve özgürlükleriyle ilgili menfaatleri çığnemesi haricinde, verilerin açıklandığı üçüncü şahısların ya da veri sorumlusunun meşru menfaatlerinden kaynaklanan amaçlar için gerekli olması” şartlardan herhangi birinin varlığı halinde, verinin işlenmesi meşru olarak kabul edilecektir.

Toplanma ve/veya bunu izleyen işleme amaçları bakımından yeterli ve onlarla ilgili olma ve aşırı olmama ise kişisel verilerin işlenmesi ile ilgili bir diğer ilkedir. Bu ilkeye göre ilk olarak veri sorumlusu, amacına ulaşabilmesi için kişisel verilere ihtiyaç duyup duymadığını belirlemelidir. Eğer kişisel verilerin kullanılması mutlaka gerekli değilse kullanılmaması tercih edilmelidir. Ancak kişisel verilerin kullanılmasının zorunlu olduğu durumlar söz konusu ise de mümkün olan en az miktarda verinin kullanılması gerekmektedir⁶³.

Bir diğer ilke, verilerin doğru ve gerekli ise güncel olmasıdır. Buna göre veri özneleri, kendilerine ait verilerin doğru olmasını talep etme ve gerektiğinde doğruluğunu kontrol etme hakkına sahiptir. Ayrıca verilerin doğru olmaması durumunda veri öznesi

⁶¹ a.g.e., s. 84.

⁶² Kılınç, a.g.m., s. 1110; Küzeci, a.g.e., s. 209.

⁶³ Küzeci, a.g.e., s. 214.

söz konusu verilerin düzeltilmesini ya da imha edilmesini talep edebilir⁶⁴. Bu ilkeye göre verilerin doğru olarak tutulmasının yanında gerekiyorsa güncellenmesi de gerekmektedir.

Son ilke ise verilerin gereğinden uzun süre tutulmamasıdır. Kişisel verilerin işlenmesi ile amaç arasındaki ilişki son bulduğunda verilerin silinmesi ya da anonimleştirilmesi yoluna gidilmesi gerekmektedir. Amacın gerçekleşmesi için kişisel verilere ihtiyaç duyulduğunda verilerin tutulması hukuka uygunken, amaç ile kişisel verilerin arasındaki ilişki sona erdiğinde verilerin tutulması hukuka aykırı hale gelecektir⁶⁵.

C. KİŞİSEL VERİLERİN İŞLENMESİNDE HUKUKA UYGUNLUK NEDENLERİ

1. Özel Nitelikli Olmayan Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri

Kural olarak kişisel verilerin işlenmesi yasak olsa da, hukuki metinlerde bu işlemenin belirli koşullar altında yapılması durumunda, hukuka uygun hale geleceğine ilişkin düzenlemeler mevcuttur. Kişisel verilerin işlenme şartları KVKK'nın 5. maddesinde sayılmıştır. Aynı şekilde GVKT'nin 6. maddesinde de işlemenin hukuka uygunluk şartları yer almaktadır.

GVKT'de hukuka uygunluk nedenleri, “veri sahibinin rızası, veri sahibinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için gerekli olması, veri sorumlusunun yasal yükümlülüğünü yerine getirebilmesi için gerekli olması, veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı için gerekli olması, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması için gerekli olması, özellikle veri sahibinin çocuk olması halinde veri

⁶⁴ Hayrunnisa Özdemir, “Haberleşmenin Gizliliği ve Kişisel Veriler”, *EÜHFD*, C. XIII, S. 1-2 (2009), s. 296.

⁶⁵ Küzeci, a.g.e., s. 221-222; Nurullah Tekin, “Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi”, *Uyuşmazlık Mahkemesi Dergisi*, S.4 (2014), s. 232.

sahibinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir kontrolör veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması” olarak sayılmıştır.

KVKK m. 5’te ise bu şartlar, “ilgili kişinin açık rızasının varlığı, kanunlarda açıkça öngörülmesi, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” şeklinde, “kişisel verilerin işleme şartları” başlığı altında sayılmıştır.

Açık rıza, KVKK m. 3’te “*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*” olarak tanımlanmıştır. Bu tanımdan yola çıkarak “ilgili kişinin açık rızası”ndan söz edilebilmesi için üç şartın arandığı söylenebilir. Bu şartlar, “rızanın belirli bir konuya ilişkin olması, rızanın bilgilendirmeye dayanması, rızanın özgür iradeyle açıklanması”dır⁶⁶. Veri sorumlusu, açık rızayı hangi konu ile ilgili olarak istediğini ve hangi verilerin işleneceğini açıkça belirtmelidir. Belirli bir konuya ilişkin açık rıza alındıktan sonra farklı bir veri işleme amacının ortaya çıkması durumunda, daha önce alınan rıza bu durumu kapsamadığından, bu durum için ayrıca rıza alınması gerekecektir. Hangi konuda veri işleneceği ve hangi verilerin işleneceğinin belirtilmesi, alınan rızanın açık rıza niteliği taşıması için yeterli değildir. Bunun dışında ayrıca kişinin bilgilendirilmesi de gerekmektedir. Bu bilgilendirme; kişinin rızası sonucu oluşacak durum, verilerin nasıl kullanılacağı gibi verilerin işlenmesi ile ilgili her konuda, açık ve ilgili kişinin anlayabileceği şekilde yapılmalıdır. Rıza alınacak konu bildirildikten ve bunun hakkında bilgilendirme yapıldıktan sonra, verilerin işlenmesi konusunda kişinin

⁶⁶ Kişisel Verileri Koruma Kurumu, *Açık Rıza*, s. 3, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf>, (25.11.2019).

açık rızasının olduğundan söz edilebilmesi için, bu rıza beyanının özgür irade ile açıklanması gerekmektedir. Açık rızanın varlığı için cebir, tehdit, hata ya da hile gibi iradeyi sakatlayan sebeplerin bulunmaması gerekmektedir. Ayrıca bir mal veya hizmetten yararlanmanın ön şartı olarak veri işlenmesine izin verilmesi gibi bir şartın bulunduğu durumda da, açık rızanın varlığından söz etmek mümkün olmayacaktır. Çünkü böyle bir durumda kişi mal veya hizmetten yararlanmak amacıyla, kendisini rıza vermeye zorunlu hissedeceğinden, özgür iradede bahsedilemeyecektir⁶⁷.

Kişisel verilerin işlenmesinin hukuka uygun sayılabilmesini sağlayan bir diğer koşul ise, “kanunlarda açıkça öngörülmesi”dir. 2559 sayılı Polis Vazife ve Salâhiyet Kanunu, 5352 sayılı Adli Sicil Kanunu, Ceza Muhakemesi Kanunu, İş Kanunu gibi pek çok kanunda kişisel verilerin işlenmesine ilişkin hükümler yer almaktadır. Bu hükümler sebebiyle kişisel verilerin işlenmesi durumunda hukuka aykırılık söz konusu olmayacaktır.

“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” durumunda da veri işleme hukuka uygun olacaktır. Bu durumda veri sahibinin ya da üçüncü bir kişinin hayati menfaati, sağlığı ya da beden bütünlüğüne ilişkin menfaatin korunması için veri işlemenin şart olması gerekmektedir. Bunun yanında veri sahibinin rızasını açıklayamayacak durumda bulunması, örneğin bilincini kaybetmiş olması, ya da rızasına hukuken geçerlilik tanınmıyor olması gerekmektedir⁶⁸.

“Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” durumunda da verilerin işlenmesi hukuka uygun olacaktır. Örneğin bir kira sözleşmesi sebebiyle kiracının, kiraya veren kişinin hesap numarasını kaydetmesi hukuka uygundur.

“Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için veri işlemenin zorunlu olması” da KVKK’da sayılan hukuka uygunluk nedenlerindedir. Örneğin bir şirketin, çalışanına vereceği maaş için medeni durumu, kaç çocuk sahibi olduğu gibi verileri işlemesi gerekecektir. Burada şirket hukuki yükümlülüğünü yerine

⁶⁷ a.g.e., s. 4-6.

⁶⁸ Yücedağ, a.g.m., s. 776-777.

getirmek amacıyla veri işleme faaliyetinde bulunduğundan, bu verilerin işlenmesi hukuka aykırı değildir⁶⁹.

Kişisel verinin, “veri sahibi tarafından alenileştirilmiş olması” durumunda korunması gereken bir hukuki yararın varlığından söz edilemeyecektir. Bu sebeple ilgili kişi tarafından, herkesçe bilinebilir hale getirilen verilerin işlenmesi hukuka uygun bir işleme olacaktır. Ancak bunun için alenileştirmenin, kişinin iradesi ile yapılmış olması ve verilerin alenileştirme amacı dışında kullanılmaması gerekmektedir. Örneğin, iş için telefon numarasını internet sitesinde paylaşan kişinin numarasının, iş dışında, reklam amacı ile işlenmesi, alenileştirme amacına uygun olmadığından hukuka aykırı olacaktır⁷⁰.

“Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması” da bir diğer hukuka uygunluk sebebidir. Bir sözleşmenin bitiminden itibaren, dava zamanaşımı süresinin sonuna kadar gerekli belgelerin saklanması bu duruma örnek oluşturmaktadır ve bu sebeple hukuka uygundur⁷¹.

Son olarak “ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” durumu da KVKK’da yer alan hukuka uygunluk sebeplerinden birisidir. Bu hukuka uygunluk sebebinden yararlanılabilmesi için, veri sorumlusunun, kişisel verilerin işlenmesini gerektirecek meşru bir menfaatinin olmasının yanında, bu menfaatin veri işlenmesini gerektirecek derecede önemli olması da gerekmektedir. Meşru bir menfaatin bulunması da tek başına yeterli değildir. Bu menfaatin elde edilebilmesi için veri işlenmesi dolayısıyla, veri sahibinin temel hak ve özgürlükleri arasında denge kurulmalı ve bunlara zarar verilmemelidir⁷².

⁶⁹ Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, s. 10, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8c90423f-97ea-4d81-a7c1-ace74295c2b8.pdf>, (25.11.2019)

⁷⁰ a.g.e., s. 11.

⁷¹ a.g.e., s. 12; Yücedağ, a.g.e., s. 782.

⁷² Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, s. 13-17; Yücedağ, a.g.e., s. 783-785.

2. Özel Nitelikli Kişisel Verilerin İşlenmesinde Hukuka uygunluk Nedenleri

Diğer kişisel verilerden daha özel korumaya ihtiyaç duyan hassas kişisel verilerin işlenmesi de kural olarak yasak olmakla beraber, belirli şartlara bağlı olarak işlenmeleri hukuka uygun işleme sayılmaktadır. GVKT'nin 9. maddesinde bu şartlar 95/46/EC sayılı Direktife göre daha geniş şekilde; “veri sahibinin rızası; veri sorumlusunun veya veri sahibinin istihdam ve sosyal güvenlik ve sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve belirli haklarının kullanılması amacıyla işleme faaliyetinin gerekmesi; 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 olması; işleme faaliyetinin bir vakıf, birlik veya kar amacı gütmeyen başka bir organ tarafından siyasi, felsefi, dini veya sendika amacıyla uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında işlemenin ve yalnızca organın 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 organ dışında açıklanmaması koşuluyla gerçekleştirilmesi; işleme faaliyetinin veri sahibi tarafından açık bir biçimde kamuya açıklanan kişisel verilerle ilgili olması, yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ettiğinde, işleme faaliyetinin gerekmesi; 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 AB veya üye devlet hukukuna dayalı olarak kayda değer ölçüde kamu yararı adına nedenlerden ötürü işleme faaliyetinin gerekmesi; koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, AB ya da üye devlet hukukuna dayalı olarak veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi açısından işleme faaliyetinin gerekli olması; özellikle mesleki gizlilik olmak üzere veri sahibinin hakları ve özgürlüklerine ilişkin güvence sağlanmasına uygun ve spesifik

tedbirler sağlayan AB 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 halk sağlığı alanında kamu yararına yönelik olarak işleme faaliyetinin gerekmesi; gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyetinin gerekmesi” olarak sayılmıştır⁷³. Mahkumiyet kararları ve ceza gerektiren suçlarla ilgili kişisel verilerin işleme şartları ise GVKT m. 10’da “Mahkumiyet kararları ve ceza gerektiren suçlara ilişkin ya da ilgili güvenlik tedbirlerine ilişkin kişisel verilerin 6(1) maddesine dayalı olarak işlenmesi, ancak resmi merciin denetimi altında veya veri sahiplerinin hakları ve özgürlüklerine uygun güvenceler sağlayan Birlik veya üye devlet hukuku çerçevesinde işleme faaliyetine onay verildiğinde gerçekleştirilir. Mahkumiyet kararlarına ilişkin kapsamlı herhangi bir sicil yalnızca resmi merciin denetimi altında tutulur” şeklinde düzenlenmiştir.

KVKK’da ise özel nitelikli kişisel verilerin işlenmesinin hukuka uygun olacağı haller 6. maddede, “ilgili kişinin açık rızası; sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler için ancak kanunlarda öngörülmüş olması; sağlık ve cinsel hayata ilişkin kişisel veriler için 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 işlenmesi” olarak sayılmıştır.

KVKK’ya göre ilgili kişinin açık rızasının bulunması durumunda başka bir şart aranmadan özel nitelikli kişisel verilerin işlenmesi hukuka uygun olacaktır. Açık rızanın bulunmadığı durumlarda ise; KVKK m. 6/1’de sınırlı olarak sayılan verilerden, sağlık ve cinsel hayat dışında kalan verilerin işlenebilmesi, yalnızca kanun hükümlerinde öngörülmüş olması şartıyla mümkün olabilecektir. Sağlık ve cinsel hayata ilişkin veriler ise yalnızca “kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım

⁷³ Onur Doğan Yörük, (AB) 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Kişisel Verilerin Korunması, (Yüksek Lisans Tezi), İzmir: İzmir Ekonomi Üniversitesi Lisansüstü Eğitim Enstitüsü, 2019, s. 69-71.

hizmetlerinin yürütülmesi, sađlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla”, sır saklama yükümlülüđü altında bulunan kişiler ya da yetkili kurum veya kuruluşlar tarafından işlenebilecektir.

Gerek hassas kişisel veriler için gerekse diđer kişisel veriler için sayılan hukuka uygunluk nedenleri, verilerin işlenmesinin hukuka uygun olduğunun kabulü için gerekli şartlardır. Ancak bu şartların varlığının yanında, işleminin hukuka uygunluđundan bahsedebilmemiz için yukarıda sayılan ilkelere de uyulması gerekmektedir. Hukuka uygunluk şartlarının sađlandığı ancak sayılan ilkelere uyulmadığı bir durumda, işleminin hukuka uygun olduğundan söz etmek mümkün olmayacaktır⁷⁴.



⁷⁴ K. Ahmet Sevimli, “Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419”, *Sicil İş Hukuku Dergisi*, Y.6, S.24 (2011), s. 128.

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ VE KORUNMASINA YÖNELİK DÜZENLEMELER VE UYGULAMA

I. KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ

Tarih boyunca kişilerin gizliliği, mahremiyeti ve bilgilerin korunması önem verilen bir konu olmuştur. Bugünkü anlamda kişisel verilerin korunması kavramı, verilerin otomatik işlenmesi ile ortaya çıkmış olsa da tarihte hekim, din adamı, avukat ve bankacı gibi meslek mensuplarının sır saklama ve buna benzer yükümlülüklerinin olması kişisel verilerin korunması kavramının temellerinin günümüzden çok daha öncesine dayandığını göstermektedir⁷⁵.

1960'lardan itibaren bilişim teknolojilerinin gelişmesi ile birlikte kişisel verilerin depolanması ve toplanması daha kolay hale gelmiş ve bunun sonucu olarak da korunması gereksinimi ortaya çıkmıştır. Dünyada ilk veri koruma kanunu ise 1970 yılında Almanya'nın Hessen Eyaleti'nde çıkarılmıştır. Bundan sonra 1973'te İsveç'te verilerin korunmasına dair kanun, 1974'te ise ABD'de özel alanın korunmasına ilişkin kanun kabul edilmiştir. Bu dönemde Kanada, Fransa, Danimarka, Norveç ve İsviçre de bu alanda hukuki düzenlemeler yapmışlardır⁷⁶.

Ayrıca bu dönemde kişisel verilerin korunması hakkı, insan hakları kapsamında değerlendirilmeye başlanmıştır. 1948 tarihli "İnsan Hakları Evrensel Bildirgesi" ve 1950 tarihli "Avrupa İnsan Hakları Sözleşmesi"nin kişisel verilerin korunması hususuna ilişkin ilk uluslararası düzenlemeler olduğu söylenebilirse de, her iki düzenleme de kişisel verilerin korunmasına yönelik olarak doğrudan hükümler içermemektedir. Kişisel veriler bu düzenlemelerle doğrudan korunma imkanına sahip olmasa da, "özel hayatın gizliliği

⁷⁵ Küzeci, a.g.e., s. 107; Şimşek, a.g.e., s. 5.

⁷⁶ Şimşek, a.g.e., s. 9-11.

hakki” kapsamında dolaylı bir koruma söz konusu olmaktadır. Daha sonrasında ise 1980 tarihinde “OECD Rehber İlkeleri” kabul edilmiş, 1981 yılında ise “108 sayılı Avrupa Konseyi Sözleşmesi” imzaya açılmıştır. 1995 yılında Avrupa Birliği tarafından hazırlanan “95/46/EC sayılı Avrupa Birliği Direktifi” ise kişisel verilerin korunması alanındaki en büyük gelişmelerden birisi olarak değerlendirilmişse de, 25 Mayıs 2018 tarihinde yürürlüğe giren “2016/679 sayılı Genel Veri Koruma Tüzüğü” bu direktifi ilga etmiş ve kişisel verilerin daha etkin olarak korunmasının sağlanması için yeni düzenlemeler getirmiştir⁷⁷.

II. KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK DÜZENLEMELER

Kişisel verilerin korunması ile ilgili yukarıda kısaca değinilmiş olan gerek uluslararası düzenlemeler gerekse de ulusların kendi düzenlemeleri hakkında daha detaylı açıklamalara bu başlık altında yer verilecektir.

A. ULUSLARARASI DÜZENLEMELER

Kişisel verilerin korunması ile ilgili uluslararası düzenlemelerin başlıcaları şunlardır; Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler, Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler, Avrupa İnsan Hakları Sözleşmesi, 108 Sayılı Avrupa Konseyi Sözleşmesi, 95/46/EC Sayılı Kişisel Verilerin Korunması Direktifi, 2016/679 Sayılı Genel Veri Koruma Tüzüğü ve Özel Yaşamın Gizliliği Çerçeve Belgesi.

Ekonomik İş Birliği ve Kalkınma Teşkilatı (OECD), 14 Aralık 1960’ta kurulmuştur. Çeşitli sosyal, ekonomik ve çevresel zorluklara çözümler bulmak, daha iyi yaşam standartları yaratmak, istihdam yaratmak, ekonomiyi iyileştirmek gibi amaçlarla kurulmuş bir örgüttür⁷⁸. Kişisel verilerin korunması konusunda ilk adımı atan OECD,

⁷⁷ Köse Aysun, a.g.e., s. 60; Küzeci, a.g.e., s. 200; Korkmaz, a.g.e., s. 73-74.

⁷⁸ <https://www.oecd.org/about/>, (21.07.2019).

1980 yılında “Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler”i⁷⁹ kabul etmiştir.

Bu Rehber İlkeler’de otomatik veri işleme sistemlerinin gelişmesiyle birlikte çok büyük miktardaki verinin oldukça kısa sürede sınır ötesine iletilmesinin mümkün olduğu belirtilmektedir. Bu sebeple de kişisel verilerin hukuka aykırı şekilde kaydedilmesi, depolanması ya da bunların kötüye kullanılmasının insan haklarına aykırı olduğu belirtilerek veri transferleri konusunda birtakım sınırlamalara gidilmesi gerektiği ifade edilmiştir. Rehber İlkeler ile uyulması gereken 8 temel ilke sayılmıştır. “Kişisel veri toplanması ve işlenmesinin sınırlı olması ve ülkelere bağlılığı, kişisel verilerin kaliteli olması ilkesi, amaca bağlılık ilkesi, verilerin korunması için gereken önlemlerin alınması gerektiği ilkesi, açıklık ilkesi, bireysel katılım ilkesi ve sorumluluk ilkesi” sayılan ilkelerdir. Ancak bu ilkelerin, üye devletler için herhangi bir bağlayıcılığı bulunmamaktadır, yalnızca yol gösterici bir rehber niteliğindedir⁸⁰.

Uluslararası barış ve güvenliğin sağlanması ve toplumsal, sosyal, kültürel ve ekonomik nitelikteki sorunların çözümü için 24 Ekim 1945’te BM şartının yürürlüğe girmesi ile Birleşmiş Milletler Örgütü resmen kurulmuştur⁸¹. BM, gerek 10 Aralık 1948 tarihli “BM İnsan Hakları Evrensel Beyanname”i⁸² ile gerekse de “BM Medeni ve Siyasal Haklar Sözleşmesi”⁸³ ile kişilerin özel yaşamlarının gizliliğini koruma altına almıştır. Ancak bu genel kapsamlı belgeler dışında, bilişim teknolojilerinin gelişmesi sonucunda kişilerin haklarının ihlal edilmesinin önüne geçilebilmesi amacıyla, 14 Aralık 1990 yılında Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler⁸⁴ BM Genel Kurulu tarafından kabul edilmiştir. Belgenin adından da anlaşılacağı üzere söz konusu ilkeler bilgisayarda işlenen kişisel verileri korumaya yöneliktir. Bu belgede de OECD rehber ilkelerinde olduğu gibi ülkelerin uyması gereken birtakım ilkelere yer

⁷⁹2013 yılında güncellenmiş metin için bakınız: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, (21.07.2019).

⁸⁰ Ersoy, a.g.e., s. 52-55.

⁸¹ <https://www.un.org/en/sections/history/history-united-nations/index.html>, (21.07.2019); Birleşmiş Milletler Şartı için bakınız: <https://www.un.org/en/charter-united-nations/index.html>, (21.07.2019).

⁸²Türkçe metin için bakınız: <https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf>, (21.07.2019).

⁸³Türkçe metin için bakınız: <https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/53-73.pdf>, (21.07.2019).

⁸⁴ İngilizce metin için bakınız: Guidelines for the Regulation of Computerized Personnel Data Files, <https://undocs.org/en/A/RES/45/95>, <https://www.refworld.org/pdfid/3ddcafaac.pdf>, (21.07.2019).

verilmiştir. Bu ilkeler; “yasallık ve dürüstlük, doğruluk, amacın belirli olması, ilgili kişilerin erişim hakkı, ayrımcılıktan kaçınma, istisna koyma yetkisi, güvenlik, denetim ve yaptırım ve sınır ötesi veri aktarımıdır”⁸⁵. BM Rehber İlkeleri, denetim ile görevli bir organ kurulmasını öngören ilk uluslararası belgedir ve bu sebeple bazı uluslararası belgelerden daha ileri bir belge olduğunu söylemek mümkündür⁸⁶.

Kişisel verilerin korunması alanında düzenlemeler yapan bir diğer örgüt ise Avrupa Konseyi’dir. AK, 5 Mayıs 1949’da kurulan, üye ülkelerin siyasi ve ekonomik ilerlemelerini sağlamayı ve ekonomik, sosyal, kültürel, bilimsel, yasal ve idari konularda birlikte hareket edilerek, temel insan hakları ve özgürlüklerinin geliştirilmesini amaçlayan bir topluluktur⁸⁷. İnsan hakları ve temel özgürlükleri koruma amacı dolayısıyla da Avrupa Konseyi 4 Kasım 1950 tarihinde “Avrupa İnsan Hakları Sözleşmesi”ni kabul etmiştir⁸⁸. AİHS ile kişisel verilerin korunması konusunda özel bir düzenleme öngörülmemiştir, ancak Sözleşme’nin 8. maddesi ile “özel hayatın gizliliği hakkı” koruma altına alınmıştır⁸⁹. Avrupa İnsan Hakları Mahkemesi içtihatlarıyla özel hayat kapsamına kişisel verilerin de girdiği kabul edilmiş, bu madde ile kişisel verilerin de korunması mümkün olmuştur⁹⁰. Ancak verilerin daha etkin şekilde korunabilmesi amacıyla AK 1973 ve 1974 yıllarında Tavsiye Kararları kabul etmiş, sonrasında da 28 Ocak 1981 yılında “108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi”ni⁹¹ imzaya açmıştır. 1 Ekim 1985 tarihinde de söz konusu Sözleşme yürürlüğe girmiştir. Bu belge kişisel verilerin korunmasına

⁸⁵ Ersoy, a.g.e., s. 62-63; Korkmaz, a.g.e., s. 140-142.

⁸⁶ Küzeci, a.g.e., s. 126-127.

⁸⁷ AK Statüsü’nün Türkçe metni için bakınız: http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktarafli-soz/ak/turkce/001_tur.pdf, (21.07.2019).

⁸⁸ Türkçe metin için bakınız: <https://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf>, (22.07.2019).

⁸⁹ AİHS m.8: “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.”

⁹⁰ Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler*,

<https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20ALANINDA%20ULUSLARARASI%20VE%20ULUSAL%20D%C3%9CZENLEMELER.pdf>, s. 5-6, (22.07.2019).

⁹¹ Türkçe metni için bakınız: <https://www2.tbmm.gov.tr/d26/1/1-0320.pdf>, (22.07.2019).

ilişkin olarak hukuki bağlayıcılığa sahip ilk belge olması sebebiyle önemlidir⁹². Bu Sözleşme ile, “gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayata saygı hakkını güvence altına almak” amaçlanmıştır (m. 1). Sözleşme’nin 5. maddesine göre işlemeye konu olan kişisel veriler; “adil biçimde ve yasal yoldan elde edilir ve işlenir, belli ve meşru amaçlar için kaydedilir ve bu amaçlara aykırı şekilde kullanılamaz, kaydedilme amaçlarına göre uygun ve yerinde olur ve aşırı olmaz, doğru bilgileri yansıtır ve gerektiğinde güncellenir, kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde ilgili kişilerin kimliklerini belirlemeye imkan veren bir biçimde saklanır.”

Avrupa Birliği de kişisel verilerin korunması konusunda düzenleme yapan topluluklardan biridir. Barışı, özgürlüğü, güvenliği ve adaleti sağlayarak vatandaşların refahını artırmak gibi amaçlarla kurulan AB, insanlık onuru, özgürlük, demokrasi, eşitlik, hukukun üstünlüğü ve insan hakları kavramlarını vazgeçilmez değerler olarak gören bir oluşumdur⁹³. Kişisel verilerin korunması konusu AB’de diğer ülkelere göre çok daha fazla önem verilen bir konudur. Bu sebeple de başta AB Temel Haklar Şartı ve Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafikine İlişkin 95/46/EC sayılı Avrupa Parlamentosu ve Konseyi Direktifi olmak üzere bu konuda pek çok düzenleme yapılmıştır⁹⁴. AB Temel Haklar Şartı’nın 8. maddesi kişisel verilerin korunmasına yönelik olarak yapılmıştır. Maddeye göre; “Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir.”⁹⁵. 24 Ekim 1995 tarih ve 95/46/EC sayılı Direktif’in amacı ise üye devletler arasındaki veri akışı konusunda kısıtlamaları kaldırmak ve üye devletlerin vatandaşı olan gerçek kişilerin temel hak ve özgürlüklerinin korunması ve

⁹² Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler*, s. 4; Kılınç, a.g.e., s. 1112-1113; Eda Manav, “İş İlişkisinde İşçinin Kişisel Verilerinin Korunması”, *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, C. XIX, S.2 (2015), s. 101-102.

⁹³ https://europa.eu/european-union/about-eu/eu-in-brief_en, (22.07.2019).

⁹⁴ Korkmaz, a.g.e., s. 181.

⁹⁵ Türkçe metin için bakınız: <https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708#>, (23.07.2019).

kişisel verilerin işlenmesi konusunda özel hayatlarına saygı duyulmasının sağlanmasıdır⁹⁶. Bu direktif ile beraber, bunu kabul eden her üye devletin mevcut mevzuatını direktifteki ilkelere uygun olarak düzenlemesi ya da bu konuda yeni hukuki düzenlemeler yapma yoluna gitmesi gerekmektedir⁹⁷. Bu direktifin devamında AB; 1997 yılında “97/66/EG sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi”ni, 2002 yılında “2002/58/EC sayılı Özel Hayatın Korunması ve Elektronik İletişim Direktifi”ni, 2006 yılında ise “2006/24/EC sayılı Direktif”i çıkartmıştır⁹⁸.

95/46/EC sayılı Direktif’in zamanla beklenen etkiyi göstermemesi ve üye devletler arasında istenen uyumun sağlanamaması sonucunda 2010 yılından sonra AB’de veri koruma reformu düşüncesi ortaya çıkmıştır. Bu düşüncenin sonucu olarak da 95/46/EC sayılı Direktif’i ilga eden “2016/679 sayılı Genel Veri Koruma Tüzüğü” kabul edilmiş ve bu Tüzük 25 Mayıs 2018’de yürürlüğe girmiştir⁹⁹. Tüzük, üye devletler bakımından bağlayıcıdır ve uygulanması için iç hukuka aktarılmasına da gerek bulunmamaktadır. Bu tüzük ile veri öznesi olan kişilerin daha etkin şekilde korunabilmesi amacıyla, veri sorumlularına ve veri kontrolörlerine yüklenen sorumluluklar arttırılmıştır¹⁰⁰.

Çalışmamızda bahsedeceğimiz, kişisel verilerin korunması alanında düzenleme yapan son örgüt ise Asya-Pasifik Ekonomik İş birliği (APEC)’dir. APEC, Asya-Pasifik bölgesinde sürdürülebilir ekonomik büyümeyi ve refahı desteklemek başta olmak üzere serbest ticaret ve yatırımları savunarak, bölgesel ekonomik entegrasyonu teşvik ederek ve hızlandırarak, ekonomik ve teknik işbirliğini teşvik ederek, insan güvenliğini artırarak ve olumlu ve sürdürülebilir bir iş ortamı sağlayarak dinamik ve uyumlu bir Asya-Pasifik topluluğu kurma amaçlarıyla 1989 yılında kurulmuştur¹⁰¹. APEC, 2005 yılında özel hayatın gizliliğinin korunması amacı ile Özel Yaşamın Gizliliği Çerçeve Belgesi¹⁰²,ni

⁹⁶ İngilizce metin için bakınız: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en>, (22.07.2019)

⁹⁷ Tekin, a.g.m., s. 226.

⁹⁸ Alaattin Bük, *Bilişim Alanında Kişisel Verilerin Korunması*, 1. b., Ankara: Seçkin Yayıncılık, 2018, s. 71-72.

⁹⁹ Köse Aysun, a.g.e., s. 60; Küzeci, a.g.e., s. 200.

¹⁰⁰ Köse Aysun, a.g.e., s. 62.

¹⁰¹ <https://www.apec.org/About-Us/About-APEC/Mission-Statement>, (22.07.2019).

¹⁰² İngilizce metin için bakınız: <https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework>, (22.07.2019).

kabul etmiştir. OECD Rehber İlkeleri ışığında düzenlenen bu belgede verilerin korunmasında hakim olan ilkeler ve sınır ötesi veri akışının kuralları başlıklı iki bölüm bulunmaktadır. 2013 yılında OECD Rehber İlkelerinin güncellenmesi ve kişisel verilerin korunması ile ilgili yeni kavramların ortaya çıkması ile 2015 yılında Özel Yaşamın Gizliliği Çerçeve Belgesinde de güncelleme yoluna gidilmiştir¹⁰³.

B. ÇEŞİTLİ DEVLETLERDE KİŞİSEL VERİLERİN KORUNMASI

Uluslararası düzenlemelerin yanında, kişisel verilerin korunması amacıyla ülkeler de yasal düzenlemeler yapmaktadır. Bu başlık altında; Almanya, Fransa, İsviçre, İngiltere ve Amerika Birleşik Devletleri'nde kişisel verilerin korunmasına yönelik düzenlemeler hakkında bilgi verilecektir.

1. Almanya

Alman Anayasası'nda¹⁰⁴ kişisel verilerin korunması hakkına özel olarak yer verilmemiştir. Ancak bu hak Anayasa'da bulunan genel kişilik hakkı kapsamında korunmaktadır. Anayasa'da özel bir hüküm bulunmasa da kişisel verilerin korunması konusunda ilk yasal düzenlemenin 1970 tarihli Almanya'nın Hessen Eyaleti'nde kabul edilen veri koruma kanunu olması bu konuya önem verildiğini açık bir şekilde göstermektedir. Bu veri koruma kanunu ile, bilişim sistemleriyle tapu kayıtlarına erişim sağlanabilmesi sonucunda, verilerin toplanması ve depolanmasına ilişkin usul ve esasları belirlemek amaçlanmıştır¹⁰⁵.

1977 yılında ise ülke genelinde verilerin korunması amacıyla Federal Veri Koruma Kanunu yürürlüğe girmiş ve bu kanun 1990, 1994, 1997, 2002 ve 2016 yıllarında değişikliğe uğramıştır¹⁰⁶. 30 Haziran 2017 tarihinde ise 2016/679 sayılı Tüzük'e ve

¹⁰³ Güncellenmiş İngilizce metin için bakınız: [https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-\(2015\)](https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)), (22.07.2019).

¹⁰⁴ Türkçe metin için bakınız: <http://www.adalet.gov.tr/duyurular/2011/eylul/anayasalar/ulkeana/pdf/08-ALMANYA%20209-276.pdf>, (02.08.2019).

¹⁰⁵ Köse Aysun, a.g.e., s. 71; Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanununa Duyulan İhtiyaç*, s. 1, <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/8e39e0a1-6ec4-4179-a5d3-bbd8e78dce31.pdf> (31.07.2019).

¹⁰⁶ Korkmaz, a.g.e., s. 224.

2016/680 sayılı Direktif'e¹⁰⁷ uyum sağlanması amacıyla, DSAnpUG-EU isimli bir kanun yürürlüğe girmiştir¹⁰⁸. Bu Kanun ile Federal Veri Koruma Kanunu revize edilmiştir¹⁰⁹. 2016/679 sayılı Tüzük'ün 25 Mayıs 2018 tarihinde yürürlüğe girmesinin ardından, Federal Veri Koruma Kanunu, Tüzük ile birlikte uygulanmaktadır¹¹⁰. Veri Koruma Kanunu'nun yanında Telekomünikasyon Kanunu ve Telekomünikasyon Alanında Verilerin Korunması Yönetmeliği de kişisel verilerin korunması konusundaki mevzuatlardır¹¹¹.

Bu kanunlar dışında Alman Ceza Kanunu¹¹² ve Alman Ceza Muhakemesi Kanunu¹¹³ da kişisel verilerin korunmasına yönelik birçok maddeye yer vermiştir¹¹⁴.

2. Fransa

Fransa'da anayasal seviyede özel hayatın gizliliği ve kişisel verilerin korunması hakkı düzenlenmemiştir. Ancak Fransız Anayasa Mahkemesi'nin 1994 tarihli kararında özel hayatın gizliliği hakkının Anayasa'da¹¹⁵ örtülü olarak bulunduğu kabul edilmiştir. Kanun seviyesinde kişisel verilerin korunmasına yönelik ilk düzenleme ise 1978 tarihli Bilgi Teknolojisi, Veri Dosyaları ve Bireysel Özgürlükler Kanunu¹¹⁶ olmuştur. Bilişim yoluyla kişisel verilerin toplanmasını ve depolanmasını düzenleyen bu kanun ile bağımsız, hiçbir makamdan emir almayan Fransız Veri Koruma Komisyonu kurulmuştur.

¹⁰⁷ 27 Nisan 2016 tarihli ve 2016/680 sayılı, Konsey'in 2008/977/JHA Çerçeve Kararını yürürlükten kaldıran, yetkili makamlar tarafından suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi amacıyla işlenen kişisel verilere ilişkin gerçek kişilerin korunmasına ve bu tür verilerin serbest dolaşımına dair Direktif.

¹⁰⁸ İngilizce metin için bakınız: https://www.bvdnet.de/wp-content/uploads/2017/08/BMI_%C3%9Cbersetzung_DSAnpUG-EU_mit_BDSG-neu.pdf, (18.08.2019).

¹⁰⁹ İngilizce metin için bakınız: https://www.gesetze-im-internet.de/englisch_bdsge/englisch_bdsge.pdf, (18.08.2019).

¹¹⁰ Köse Aysun, a.g.e., s. 72-73.

¹¹¹ Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, s. 71.

¹¹² İngilizce metin için bakınız: <https://germanlawarchive.iuscomp.org/?p=752>, (02.08.2019).

¹¹³ İngilizce metin için bakınız: <https://germanlawarchive.iuscomp.org/?p=754>, (02.08.2019).

¹¹⁴ Nil Melek Gültekin, *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*, (Yüksek Lisans Tezi), İstanbul: Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, 2012, s. 49-51.

¹¹⁵ Türkçe metin için bakınız: <http://www.adalet.gov.tr/duyurular/2011/eylul/anayasalar/ulkeana/pdf/07-FRANSA%20169-208.pdf>, (02.08.2019).

¹¹⁶ Fransızca metin için bakınız: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20080609>, (02.08.2019).

95/46/EC sayılı Direktif'in iç hukuka etkili bir şekilde aktarılabilmesi için 2004 tarihli Kişisel Verilerin İşlenmesinde İlgili Kişilerin Korunması Kanunu kabul edilmiştir¹¹⁷.

Kişisel verilerin korunmasına yönelik suçlar ise ayrı bir kanun ile değil, Fransız Ceza Kanunu¹¹⁸ ile düzenlenmiştir¹¹⁹. Bu kanun ile, kişiye ait bilgilerin, kanunda öngörülen formaliteler yerine getirilmeden taksirle bile olsa otomatik olarak işlenmesi, izin alınmadan hırsızca, sessizce veri toplanması veya gerçek bir kişiye ait verilerin onun hukuken geçerli itirazına rağmen işlenmesi ve sağlık alanında araştırma amacıyla kişiye ilişkin verilerin, hak sahibine haklarını hatırlatmadan otomatik olarak işlenmesi gibi fiiller suç olarak sayılmıştır. Bahsedilen suçlar dışında kişisel verilere yönelik farklı suçlar da bu kanun ile detaylı olarak düzenlenmiştir¹²⁰.

3. İngiltere

Yazılı bir anayasası bulunmayan İngiltere'de kişisel verilerin korunması hakkı özel bir statüye sahip değildi. Ancak AİHS'nin iç hukukta uygulanması ile kişisel verilerin korunması hakkı, özel hayata ve aile hayatına saygı hakkı kapsamında gelişmiş bir korumaya sahip olmuştur¹²¹.

1984'te İngiltere'de ilk veri koruma kanunu yürürlüğe girmiştir. Ancak bu kanun kişilerin mahremiyet hakkına ve bu hakkın nasıl kullanılacağına ilişkin açık hükümlere yer vermemiş olması sebebi ile kişisel verilerin korunması konusunda yeterli olmamıştır¹²². Bunun üzerine daha yeterli koruma sağlanması amacıyla 1998 tarihinde Veri Koruma Kanunu¹²³ kabul edilmiştir.

¹¹⁷ Korkmaz, a.g.e., s. 217; Ahmet Boz, *Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri*, (Yüksek Lisans Tezi), Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2014, s. 87.

¹¹⁸ Fransızca için bakınız: <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719>, (02.08.2019).

¹¹⁹ Boz, a.g.e., s. 87.

¹²⁰ Çokmutlu, a.g.e., s. 114-115.

¹²¹ Douwe Korff, *EC Study on Implementation of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49)*, *Comparative Summary of National Laws*, Cambridge: Human Rights Centre University of Essex, 2002, s. 8-9.

¹²² Dilek Yüksel Civelek, *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*, (Uzmanlık Tezi), Ankara: Bilgi Toplumu Dairesi Başkanlığı, 2011, s. 87.

¹²³ İngilizce için bakınız: http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf, (02.08.2019).

1998 tarihli Veri Koruma Kanunu ise İngiltere’de en kapsamlı şekilde kişisel verilerin korunmasını ele alan düzenlemedir. Bunun yanında 2016 tarihinde AB’den ayrılma kararı alan İngiltere AB ile süren ekonomik ilişkilerinin aksamaması için 2016/679 sayılı Tüzük ile benzer koruma sağlayan bir Veri Koruma Kanunu hazırlamış ve bu kanun 2018 yılında yürürlüğe girmiştir¹²⁴. Bu kanun ile; kasten ya da taksirle kişisel verileri ele geçirme, ifşa etme, başkalarına verme, kişinin izni olmadan saklama ve anonim hale getirilmiş verilerin tekrar kişi ile bağlantılı hale getirilmesi durumlarının cezalandırılacağı belirtilmiştir¹²⁵.

4. İsviçre

İsviçre Federal Anayasa’sının¹²⁶ 13. maddesinde kişilerin kendileri ile ilgili kişisel verilerin kötüye kullanılmasından korunma hakkı olduğu ifade edilmiştir. Anayasa’nın yanında İsviçre Medeni Kanunu¹²⁷ ve İsviçre Ceza Kanunu’nda¹²⁸ da kişisel verilerin korunmasına yönelik düzenlemeler yer almaktadır¹²⁹.

Bu kanunlar dışında İsviçre’de verilerin korunmasına yönelik ilk düzenleme 1976 tarihli Anayasal Veri Koruma Yönetmeliği’dir. Verilerin Korunmasına İlişkin Federal Kanun¹³⁰ ise 1993 yılında yürürlüğe girmiştir. Bu kanun hem gerçek hem de tüzel kişileri koruma altına almıştır. Kanun, 2008 yılında değiştirilerek 95/46/EC sayılı Direktif ile paralel koruma sağlayacak hale getirilmiştir¹³¹.

¹²⁴ İngilizce metin için bakınız: <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>, (02.08.2019).

¹²⁵ Köse Aysun, a.g.e., s. 74-75.

¹²⁶ İngilizce metin için bakınız: <https://www.admin.ch/opc/en/classified-compilation/19995395/201809230000/101.pdf>, (02.08.2019).

¹²⁷ İngilizce metin için bakınız: <https://www.admin.ch/opc/en/classified-compilation/19070042/201901010000/210.pdf>, (02.08.2019).

¹²⁸ İngilizce metin için bakınız: <https://www.admin.ch/opc/en/classified-compilation/19370083/index.html>, (02.08.2019).

¹²⁹ Gültekin, a.g.e., s. 44.

¹³⁰ İngilizce metin için bakınız: <https://www.admin.ch/opc/en/classified-compilation/19920153/201903010000/235.1.pdf>, (02.08.2019).

¹³¹ Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, s. 75; Gültekin, a.g.e., s.46-47.

5. Amerika Birleşik Devletleri

Amerika Birleşik Devletleri’nde özel olarak kişisel verilerin korunmasına yönelik bir kanun bulunmamaktadır. ABD Anayasası’nda ise temel hakların korunmasına yönelik olarak birtakım hükümler yer alsa da, kişisel verilerin korunması konusunda doğrudan hükümler yer almadığından, bu konuda ancak dolaylı bir koruma söz konusu olacaktır. Ancak bu korumanın kapsamı da devletin vatandaşlara karşı eylemleri ile sınırlıdır. Anayasa’nın köleliği yasaklayan 13. değişiklik maddesi dışında, kişilerin birbirlerine karşı eylemleri ile ilgili anayasal bir koruma söz konusu değildir¹³².

ABD’de federal düzeyde kişisel veriler ile ilgili koruma sağlayan ilk kanun Özel Hayatın Gizliliği Kanunu olarak ifade edebileceğimiz 1974 tarihli “*The Privacy Act of 1974*¹³³” adlı kanundur. Bu kanun, federal kuruluşlar tarafından elde edilen, depolanan, yayınlanan ve kullanılan kişisel verilerin korunması ile ilgilidir. Ancak verilerin özel sektörde işlenmesi durumunda bu kanunun uygulanması mümkün olmadığı gibi ABD vatandaşı olmayan kişiler bakımından da bu kanunun uygulanması söz konusu değildir. Bu Kanun ile düzenlenen haklar; kişilerin kendisi hakkındaki verileri görebilme hakkı, kişilerin kendileri ile ilgili verilerin düzeltilmesini isteme hakkı ve kişisel verilerin işlenmesi sırasında kişinin saldırılara karşı korunma hakkı olarak özetlenebilir¹³⁴.

Bu kanun dışında 1936 yılında haberleşme özgürlüğünü koruma altına alan bir kanun, 1984 yılında Kablolü Haberleşme Kanunu çıkarılmıştır. Bunların yanında mali bilgilerin korunmasına yönelik 1978 tarihli Mali Gizlilik Kanunu olan *Financial Privacy Act*¹³⁵, 1991 tarihli telekomünikasyon alanında kişisel verilerin korunmasına yönelik Telefon Müşterilerini Koruma Kanunu olan *Telephone Consumer Protection Act*¹³⁶, uluslararası veri transferlerinin kontrolünü sağlamak amacıyla 1996 yılında çıkarılan İletişim Ahlak Yasası olan *Communications Decency Act*¹³⁷, 1998 tarihli Çocukların Çevrimiçi Korunması Yasası olarak ifade edebileceğimiz *Child Online Protection Act*¹³⁸

¹³² İkbâl Gür, *Kişisel Verilerin Korunması Hususunda AB ile ABD arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları*, (Yüksek Lisans Tezi), Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2009, s. 65.

¹³³ İngilizce metin için bakınız: <https://www.justice.gov/opcl/privacy-act-1974>, (02.08.2019).

¹³⁴ Armağan Ebru Bozkurt Yüksel, *Bulut Bilişimde Kişisel Verilerin Korunması (Personal Data Protection in Cloud Computing)*, 1. b., Ankara: Yetkin Yayınları, 2016, s. 58; Korkmaz, a.g.e., s. 241.

¹³⁵ İngilizce metin için bakınız: <https://www.law.cornell.edu/uscode/text/12/chapter-35>, (02.08.2019).

¹³⁶ İngilizce metin için bakınız: <https://www.law.cornell.edu/uscode/text/47/227>, (02.08.2019).

¹³⁷ İngilizce metin için bakınız: <https://www.law.cornell.edu/uscode/text/47/230>, (02.08.2019).

¹³⁸ İngilizce metin için bakınız: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>, (02.08.2019).

isimli kanunlar da kişisel verilerin özel sektörde korunması amacıyla çıkarılan kanunlardan bir kısmına örnek oluşturmaktadır¹³⁹.

Yukarıda örnekleri verilen kanunlardan da görülebileceği üzere ABD’de kişisel verilerin korunması ile ilgili olarak tek bir kanun yerine belirli sanayi dalları ya da belirli konuları ele alan ayrı kanunlar mevcuttur. Bu da kişisel verilerin korunması konusunda bir standart olmaması dolayısıyla farklı uygulamalara sebep olabilecektir¹⁴⁰.

III. TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

Uluslararası belgeler ve yabancı ülkelerin mevzuatlarında kişisel verilerin korunması konusunda yer alan düzenlemelerin ardından ülkemizde yer alan düzenlemeleri de incelemek gerekmektedir. Kişisel verilerin korunması konusunda başta Anayasa olmak üzere Türk Ceza Kanunu, Türk Medeni Kanunu, Borçlar Kanunu ve İş Kanunu gibi kanunlarda çeşitli hükümler yer almaktadır. Bu kanunların yanında kişisel verilerin korunması konusuna özel olarak Kişisel Verilerin Korunması Kanunu da mevzuatımızda yer almaktadır.

Son yıllarda ülkemizde kişisel verilerin korunması hakkı önem kazanmış ve bu konuda çeşitli düzenlemeler yapılmıştır. Anayasa’da yer alan kişisel verilerin korunması hakkı 2010 yılındaki referandum ile getirilmiş, Kişisel Verilerin Korunması Kanunu ise 2016 yılında kabul edilmiştir.

Yukarıda saydığımız, mevzuatımızda yer alan ve kişisel verilerin korunması konusunda düzenlemelere yer veren kanunlar bu başlık altında genel hatlarıyla incelenecektir. Ancak Türk Ceza Kanunu’nda kişisel verilerin korunmasına yönelik olarak düzenlenen suçlar ilerleyen bölümlerde çok daha detaylı şekilde inceleneceğinden bu başlık altında TCK’daki düzenlemelere yer verilmeyecektir.

¹³⁹ Ersoy, a.g.e., s.80; Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, s. 73.

¹⁴⁰ Gür, a.g.e., s. 86.

A. ANAYASA

2010 yılı öncesinde Anayasa’da kişisel verilerin korunması hakkı konusunda açık hüküm bulunmazken Anayasa’nın “Devletin temel amaç ve görevleri” başlıklı 5., “Kişinin dokunulmazlığı, maddi ve manevi varlığı” başlıklı 17., “Özel hayatın gizliliği” başlıklı 20., “Konut dokunulmazlığı” başlıklı 21., “Haberleşme hürriyeti” başlıklı 22., “Din ve vicdan hürriyeti” başlıklı 24., “Düşünce ve kanaat hürriyeti” başlıklı 25. ve “Düşünceyi açıklama ve yayma hürriyeti” başlıklı 26. maddelerinde yer alan düzenlemeler bu hakkın temeli olarak görülmektedir¹⁴¹.

Bu maddeler dışında Anayasa’nın Başlangıç bölümünün 6. paragrafında yer alan “*Her Türk vatandaşının bu Anayasadaki temel hak ve hürriyetlerden eşitlik ve sosyal adalet gereklerince yararlanarak milli kültür, medeniyet ve hukuk düzeni içinde onurlu bir hayat sürdürme ve maddi ve manevi varlığını bu yönde geliştirme hak ve yetkisine doğuştan sahip olduğu*” ifadesinin de kişisel verilerin korunması konusunda güvence getirdiği ifade edilmektedir¹⁴².

Kişisel verilere ilişkin bir düzenleme 2010 yılı öncesinde Anayasa metninde yer almasa bile, yukarıda görülebileceği üzere bu hak pek çok maddeden kaynaklanmakta ve kişisel veriler dolaylı olarak korunma imkanı bulmaktaydı. Ancak gelişen teknoloji ile kişisel verilerin korunmasının büyük bir gereklilik haline geldiği günümüzde, bu hakkı başka hakların içerisinde değil de, ayrı bir hak olarak değerlendirip gereken korumanın bu hakka özgü düzenlemeler ile sağlanmasının çok daha doğru bir yaklaşım olduğunu düşünmekteyiz¹⁴³.

Anayasa’nın bazı maddelerinde 2010 yılında “5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun” ile değişiklikler yapılmıştır. Yapılan değişikliklerden birisi de “Özel hayatın gizliliği” başlıklı 20. maddeye “*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*

¹⁴¹ Türkay Henkoğlu, *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, 1. b., Ankara: Yetkin Yayınları, 2015, s. 72.; Korkmaz, a.g.e., s. 270; Kılınç, a.g.m., s. 1131.

¹⁴² Bük, a.g.e., s. 75.

¹⁴³ Küzeci, a.g.e., s. 288.

kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.” ifadesini içeren 3. fıkranın eklenmesidir.

20. maddeye bu fıkranın eklenmesi ile, kişisel verilerin korunması hakkı farklı maddeler kapsamında, dolaylı olarak değil, doğrudan anayasal güvenceye kavuşmuştur. İlgili fıkrada kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla belirleneceği düzenlendiği halde, 2016 yılı öncesinde kişisel verilerin korunması konusunda bir kanunun yürürlükte olmaması, Anayasa’nın bu maddesinin uygulanması konusunda önemli bir eksiklik olarak görülmüştür¹⁴⁴.

Kişisel verilerin korunması ile ilgili olarak Anayasa’da görülen bir diğer eksiklik ise kişisel verilerin işlenmesini denetleyecek bağımsız bir organ öngörmemiş olmasıdır. Ancak bu düzenlemenin Anayasa ile yapılmaması kanun ile de yapılamayacağı anlamına gelmediğinden bu eksiklik kanunla giderilebilecek bir husustur¹⁴⁵. Nitekim bu eksiklik kanunla giderilmiş ve 6698 sayılı KVKK ile bu şekilde bir denetim otoritesi öngörülmüştür.

Anayasa’nın 20/3. maddesi ile ilgili olarak eleştirilen bir diğer konu ise kişilerin, kendisine ilişkin kişisel verilerin korunmasını “isteme” hakkına sahip olduğunu belirtmesidir. Hakkın “isteme” şeklinde düzenlenmiş olması 20. maddenin diğer fıkraları ile benzerlik¹⁴⁶ gösterse de, temel hak ve özgürlüklerin korunması mantığı ile ters düşen bir durum söz konusudur. Madde metnine bakıldığında, kişisel verilerin korunabilmesi için kişinin bu yönde bir isteğinin bulunması gerektiği yönünde bir anlam çıkarılabilmektedir. Bu sebeple böyle bir düzenlemenin temel hakların korunması açısından doğru olmadığı kanısındayız¹⁴⁷. Ayrıca ilgili fıkrada kişisel verilerin, “ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla” işlenebileceği belirtilmiştir. Yalnızca kanunla ya da kişinin rızasına bağlı olarak hakkın sınırlandırılabilmesinin belirtilmiş olması temel hak ve özgürlüklerin korunmasına ilişkin temel prensiplere bakıldığı zaman doğru görülmemektedir. Anayasa’nın 13. maddesinde “*Temel hak ve*

¹⁴⁴ Henkoğlu, a.g.e., s. 72.

¹⁴⁵ Küzeci, a.g.e., s. 290-291.

¹⁴⁶ 20. maddede özel hayatın gizliliği ve aile hayatına saygı gösterilmesini isteme hakkı şeklinde düzenleme de mevcuttur. Yani “isteme” şeklindeki düzenleme maddenin genel düzenlemesine uyum göstermektedir.

¹⁴⁷ Selen Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, 2. b., Ankara: Seçkin Yayıncılık, 2018, s. 84; Küzeci, a.g.e., s. 291.

hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.” şeklinde bir düzenleme yer almaktadır. Buna göre bu hakkın sınırlandırılmasının kanunlara bırakılmaması, Anayasa’da sınırlama sebebinin belirtilmesi; bu sınırlama sebeplerine bağlı olarak da kanun ile sınırlama getirilmesi, hakkın sınırlandırılabilmesi için kanuna sınırsız bir alan bırakılmaması bu hakkın etkin şekilde korunabilmesi açısından daha doğru bir düzenleme olurdu¹⁴⁸.

Kişisel verilerin korunması hakkı ile ilgili olarak Anayasa’da incelenmesi gereken son madde “Milletlerarası andlaşmaları uygun bulma” başlıklı 90. maddedir. Bu maddede yer alan “*Usulüne göre yürürlüğe konulmuş Milletlerarası andlaşmalar kanun hükmündedir. Bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz. (Ek cümle: 7/5/2004-5170/7 md.) Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma hükümleri esas alınır.*” hükmüne göre kişisel verilerin korunması ile ilgili olarak AİHS başta olmak üzere bu konudaki diğer milletlerarası anlaşmalar, kanunlar gibi göz önüne alınarak uygulanacaktır. Kanunlar ile anlaşmalar arasında çatışma çıkması durumunda ise bu konudaki anlaşmalar öncelikli olarak uygulanacaktır.

B. TÜRK MEDENİ KANUNU VE BORÇLAR KANUNU

4721 sayılı Türk Medeni Kanunu ve 6098 sayılı Türk Borçlar Kanunu’nda kişilik haklarının korunmasına ilişkin genel düzenlemeler çerçevesinde kişisel verilere de koruma sağlamak mümkündür¹⁴⁹. Kişiliğin korunmasına yönelik düzenlemeler ise TMK’nın 23, 24 ve 25. maddelerinde ve TBK’nın 58. maddesinde yer almaktadır.

23. madde “*Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez. Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlâka aykırı olarak sınırlayamaz. Yazılı rıza üzerine insan kökenli biyolojik maddelerin alınması, aşılması ve nakli mümkündür. Ancak, biyolojik Madde verme borcu altına girmiş olandan edimini*

¹⁴⁸ Küzeci, a.g.e., s. 291.

¹⁴⁹ Küzeci, a.g.e., s. 378.

yerine getirmesi istenemez; maddî ve manevî tazminat isteminde bulunulamaz.” şeklindeki düzenleme ile kişiliğin vazgeçme ve aşırı sınırlamaya karşı korunmasını amaçlamaktadır.

Kişilik hakkına karşı saldırılarda “*Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.*” şeklindeki 24. madde ile temel ilke belirlenmiştir. 25. maddede yer alan “*Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir. Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir. Davacının, maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır. Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; mirasbırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez. Davacı, kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yeri mahkemesinde dava açabilir.*” şeklindeki düzenleme ile de kişilik hakkına saldırı olması durumunda başvurulabilecek dava yolları sayılmıştır.

Ayrıca kişilik hakları hukuka aykırı olarak saldırıya uğrayan kişinin, TBK’nın “*Kişilik hakkının zedelenmesi*” başlıklı 58. maddesinde yer alan “*Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir. Hâkim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir.*” şeklindeki düzenlemeye göre manevi tazminat talep etme hakkı da bulunmaktadır¹⁵⁰. Bunun dışında TBK m. 419’da yer alan “*İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. Özel kanun hükümleri saklıdır.*” şeklindeki düzenleme ile de işçinin kişisel verilerinin korunması sağlanmaktadır.

¹⁵⁰ Gültekin, a.g.e., s. 70.

Bu düzenlemeler ile kişisel verilerin korunması mümkün olsa da yalnızca genel hükümler çerçevesinde kişisel verilerin yeterli şekilde korunması mümkün değildir. Bu alana özgü kuralları içeren özel bir kanunun varlığı yeterli ve etkili bir koruma için bir gerekliliktir¹⁵¹. Bu sebeple de kişisel verilere karşı saldırılarda Kişisel Verilerin Korunması Kanunu'nun da uygulanması etkin bir korumanın sağlanabilmesi için oldukça önemlidir.

C. İŞ KANUNU

4857 sayılı İş Kanunu'nun "İşçi özlük dosyası" başlıklı 75. maddesinde "*İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır. İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür.*" denilerek işverene; işçilerin kişisel verilerini içeren özlük dosyası tutma yükümlülüğü getirilmekle beraber, elde ettiği verileri dürüstlük kuralları ve hukuka uygun olarak kullanma yükümlülüğü de getirilmiştir.

Ancak işverenin hukuka aykırı hareket etmesi durumunda nasıl bir yaptırım uygulanacağı belirtilmemiştir. Ayrıca bu madde yalnızca işçinin çalıştığı süreyi değil, işçi-işveren ilişkisinin sona ermesinden sonraki süreyi de kapsamaktadır. Yani işçi işten ayrılrsa bile işveren edindiği bilgileri hukuka aykırı olarak kullanmama yükümlülüğü altında olacaktır¹⁵².

D. CEZA MUHALEMESİ KANUNU

5271 sayılı Ceza Muhakemesi Kanunu'nun 75 vd. maddelerinde beden muayenesi, vücuttan örnek alınması, moleküler genetik incelemeler ve fiziki kimliğin tespitine ilişkin düzenlemeler yer almaktadır. Bu düzenlemelere göre kişilerden alınacak

¹⁵¹ Kılınc, a.g.m., s. 1132.

¹⁵² Gültekin, a.g.e., s. 71.

örnekler ve toplanacak bilgiler kişisel veri niteliğinde olduğundan kişisel verilerin korunması açısından büyük önem taşımaktadır¹⁵³.

CMK m. 80 “(1) 75, 76 ve 78 inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez.

(2) Bu bilgiler, kovuşturmayaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir.” şeklinde düzenlenmiştir. Buna göre “Şüpheli veya sanığın beden muayenesi ve vücudundan örnek alınması” başlıklı 75. madde, “Diğer kişilerin beden muayenesi ve vücuttan örnek alınması” başlıklı 76. madde ve “Moleküler genetik incelemeler” başlıklı 78. madde hükümlerine göre alınan örneklerin incelenmesi sonucu elde edilen bulgular kişisel veridir. Bu bilgiler kişisel veri niteliğine haiz olduğundan gizliliğinin sağlanabilmesi için gerekli tedbirler de bu maddede düzenlenmiştir. 81. maddede yer alan “Fizik kimliğin tespiti” başlıklı “(1) Üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın, kimliğinin teşhisi için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konulur.

(2) Kovuşturmayaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde söz konusu kayıtlar Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus tutanağa geçirilir.” şeklindeki düzenleme de kişisel verilerin işlenmesi ile ilgili olduğundan konumuz bakımından önemlidir.

Ceza Muhakemesi Kanunu’nun 134 vd. maddelerinde ise bilgisayar ortamında verilerin kopyalanması, “telekomünikasyon yoluyla yapılan iletişimin denetlenmesi” ve “teknik araçlarla izleme” ve bu işlemlerin denetlenmesine ilişkin düzenlemeler yer

¹⁵³ Bük, a.g.e., s. 86.

almaktadır. Günümüzde teknolojik gelişmelerin ve telekomünikasyon yolu ile iletişimin oldukça yaygınlaşp geliştiđi göz önüne alındığında, “Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma” başlıklı 134., “İletişimin tespiti, dinlenmesi ve kayda alınması” başlıklı 135. ve “Teknik araçlarla izleme” başlıklı 140. maddelerin değerinin oldukça fazla olduğunu söylemek mümkündür¹⁵⁴.

Ayrıca “Duruşmada anlatılması zorunlu belge ve tutanaklar” başlıklı 209. maddenin 2. fıkrasında yer alan “*Sanığa veya mağdura ait kişisel verilerin yer aldığı belgelerin, açıkça istemeleri halinde, kapalı oturumda anlatılmasına mahkemece karar verilebilir.*” şeklindeki düzenleme ile sanığın veya mağdurun talebi halinde dava ile ilgisi bulunmayanların, bu kişilerin kişisel verilerini öğrenmesi engellenmiştir¹⁵⁵.

E. KİŞİSEL VERİLERİN KORUNMASI KANUNU

6698 sayılı Kişisel Verilerin Korunması Kanunu 26 Aralık 2014 tarihinde tasarı olarak TBMM Başkanlığı’na sunulmuş, 24 Mart 2016 tarihinde ise kanunlaşmıştır. Bu kanun 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir. Aslında Türkiye’de bu alanda bir kanun yapma çalışmaları 1989 yılında başlamış, kanun tasarısı hazırlamak amacıyla ilk komisyon 1995 yılında kurulmuş, ancak komisyon çalışmalarını sonuçlandıramamıştır. Daha sonra 2000 yılında bir komisyon daha oluşturulmuş, 3 yıllık çalışma ile de bir kanun tasarısı hazırlanmış, ancak tasarı kanunlaşmamıştır. 2008 ve 2014 yıllarında da bu konu ile ilgili kanun tasarısı hazırlanıp TBMM’ye sunulmuş, ancak yasama döneminin sona ermesi sebebi ile tasarılar kanunlaşmamış, kişisel verilerin korunması konusunda bir kanunun yürürlüğe girmesi 2016 yılına kadar gerçekleşmemiştir¹⁵⁶.

Başta Anayasa olmak üzere kişisel verilerin korunması hakkının çeşitli kanunlar ile güvenceye alındığı mevzuatımızda; kişisel verilerin işlenmesi, sınırlanması ve bu işlemleri denetleyecek bir organın oluşturulması noktasında detaylı düzenlemeler getiren

¹⁵⁴ Kılınç, a.g.m., s. 1134-1135.

¹⁵⁵ Çokmutlu, a.g.e., s. 165.

¹⁵⁶ Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler*, s. 15; Küzenci, a.g.e., s. 311.

özel bir kanunun yürürlükte olması son derece önemlidir. Bunun yanında ülkemizin AB üyesi olabilmesi konusunda da bu kanunun önemi büyüktür¹⁵⁷.

6698 sayılı Kanun'un genel gerekçesinde bu kanunun neden gerekli olduğu net bir şekilde açıklanmıştır. Genel gerekçede yer alan bazı ifadeler şu şekildedir:

"...Günümüzde bu veriler, gerek özel sektör ve gerekse kamu sektörü tarafından bilişim sistemleri üzerinden otomatik yollarla sıkça kullanılmaktadır. Bu bilgilerin kullanılması bireyler ile mal ve hizmet sunanlar bakımından bazı kolaylıklar veya avantajlar sağlasa da, bu durum söz konusu bilgilerin istismar edilme riskini de beraberinde getirmektedir. Bu verilerin yetkisiz kişiler tarafından elde edilmesi, kullanılması ve ifşa edilmesi gerek taraf olduğumuz sözleşmeler ve gerekse Anayasamızda koruma altına alınan temel hakların ihlali olarak karşımıza çıkmaktadır. Bu iki menfaat arasında makul bir dengenin oluşturulması gerekmektedir..."

...Çağımızda insan haklarının korunması bilincinin gelişmesine paralel olarak, kişisel verilerin korunmasının da önemi her geçen gün artmaktadır. Bu nedenle günümüzde gelişmiş ülkelerde kişisel verilerin korunması alanında detaylı kanuni düzenlemelerin uygulanmakta olduğu görülmektedir..."

...Buna karşın ülkemizde, kişisel verilerin korunmasına ilişkin alanı bütüncül olarak düzenleyen bir kanun bulunmamakta, bu konuya ilişkin hükümler farklı kanunlarda yer almaktadır. Ayrıca ülkemizde kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurum da bulunmamaktadır. Bunun bir sonucu olarak, halen kişisel veriler yeterli düzenleme ve denetime tabi olmaksızın, birçok kişi veya kurum tarafından kullanılabilen ve bu durum bazı hak ihlallerinin yaşanmasına sebep olabilmektedir.

Ülkemizde kişisel verilerin korunmasını sağlayacak bir kanunun yürürlüğe girmesini gerektiren değişik sebepler bulunmaktadır. Öncelikle, 5237 sayılı Türk Ceza Kanununun 135 ve devamı maddelerinde, kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiilleri suç olarak düzenlenmiş ve yaptırımı bağlanmıştır. Bununla birlikte, kişisel verilerin işlenmesine yönelik özel bir kanunun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı, ne zaman hukuka uygun olduğunun belirlenmesinde tereddütlerin yaşandığı görülmektedir.

Öte yandan 12 Eylül 2010 tarihinde yapılan halkoylaması sonucu kabul edilen 5982 sayılı Kanunla Anayasanın 20 nci maddesinde yapılan düzenlemeyle, kişisel verilerin korunması temel bir insan hakkı olarak güvence altına alınmış ve detayların kanunla düzenlenmesi öngörülmüştür.

Yine ülkemizle ilgili olarak devam etmekte olan Avrupa Birliği tam üyelik sürecinde, müzakere fasıllarından dördü, doğrudan kişisel verilerle ilgilidir. Bu fasıllarla ilgili sürecin ilerleyebilmesi için ülkemizde kişisel verilerin korunmasına ilişkin temel bir kanunun yürürlüğe girmesi gerekmektedir. Avrupa Birliğinin Türkiye ile ilgili olarak hazırladığı ilerleme raporlarında Türkiye'de veri koruma alanındaki kanuni boşluğa işaret edilmektedir.

Ülkemizde kişisel verilerin korunmasına ilişkin kanuni bir düzenleme olmaması sebebiyle, polis birimleri arasında etkin bir işbirliğini hayata geçiren EUROPOL

¹⁵⁷ Korkmaz, a.g.e., s. 277.

ile ülkemiz güvenlik birimleri arasında operasyonel işbirliği anlaşması yapılamamakta ve elektronik bilgi değişimi gerçekleştirilememektedir.

Benzer şekilde, sınır aşan suçlarla ilgili değişik ülkelerin yargı mercilerinin ortak operasyonlar yapabilmesi amacıyla oluşturulan EURO JUST ile çok sayıda sınır aşan suçun işlendiği geçiş güzergahında bulunan ülkemiz arasında bu suçlarla mücadeleye yönelik işbirliği yapılamamaktadır.

Sağlık kuruluşlarında hastalara ilişkin çok sayıda özel nitelikli veri tutulmakta olup, bu verilerin tutulmasına ilişkin kanuni dayanağın olmayışı, verilerin güvenliğinin sağlanmasına yönelik yeterli önlemlerin alınmaması ve yetkisiz kişilerce bu nitelikteki bilgilerin ifşa edilmesi, Avrupa İnsan Hakları Mahkemesince özel hayatın gizliliğine müdahale olarak nitelendirilmekte ve ihlal kararları verilebilmektedir...

...Kişisel verilerin korunması konusu ekonomik alanla da yakından ilgilidir. Zira yabancı sermayenin ülkemizde yatırım yapması ve başka ülkelerdeki yatırımları ile ülkemizdeki yatırımlarını etkin bir şekilde yönetebilmesi için ihtiyaç duyduğu veri aktarımı, ülkemizde kanuni düzenleme olmaması sebebiyle gerçekleştirilememekte ve bu durum yabancı sermayenin ülkemizde yatırım yapması bakımından caydırıcı bir etken olarak değerlendirilmektedir. Yine işadamlarımızın yabancı ülkelerdeki yatırımları ve ortaklıklarıyla ilgili ihtiyaç duydukları veri aktarımında sorunlar yaşanmaktadır...¹⁵⁸

Gerekçe metninde yer alan açıklamaların bir kısmında bizim de yukarıda değindiğimiz hususlara da değinilmiş ve bu kanun ile “*kişisel verilerin çağdaş standartlarda işlenmesi ve koruma altına alınması*”nın amaçlandığı belirtilmiştir.

KVKK'nın “Amaç” başlıklı 1. maddesinde ise Kanun'un amacı “*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 düzenlemektir.*” şeklinde ifade edilmiştir. Bu maddeye bakıldığında Kanun'un amacının öncelikle özel hayatın gizliliği olmak üzere temel hak ve özgürlükleri korumak olduğu açıkça görülmektedir. Ayrıca madde gerekçesinde, günümüzde önem kazanan mahremiyet hakkı ve bilgi güvenliği hakkının korunmasının bu amaç kapsamında değerlendirildiği belirtilmiştir¹⁵⁹. Ancak madde metninde ya da gerekçesinde “*kişisel verilerin korunması hakkı*”ndan bahsedilmemektedir. Kişisel verilerin korunması amacıyla düzenlenen bir kanunun, “*kişisel verilerin korunması hakkı*”nı temel hak olarak tanımlayıp düzenlemesinin etkili bir koruma sağlanması bakımından daha yerinde olacağı kanısındayız¹⁶⁰.

¹⁵⁸ Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>, (06.08.2019), s. 4-5.

¹⁵⁹ Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s. 6.

¹⁶⁰ Küzeci, a.g.e., s. 320; Korkmaz, a.g.e., s. 278.

Kanun'un 2. maddesinde ise kapsam belirtilmektedir. Buna göre "*kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler*" için bu kanun uygulanacaktır. Kanun'un gerekçesinde de belirtildiği gibi, uygulama konusunda özel sektör ve kamu sektörü açısından bir ayırım yapılmamıştır, öngörülen düzenlemeler her iki sektör bakımından da uygulanacaktır¹⁶¹.

"Tanımlar" başlıklı 3. maddede ise kanunda kullanılan terimlere ilişkin tanımlamalar yapılmıştır. "Açık rıza", "anonim hâle getirme", "başkan", "ilgili kişi", "kişisel veri", "kişisel verilerin işlenmesi", "kurul", "kurum", "veri işleyen", "veri kayıt sistemi" ve "veri sorumlusu" tanımlaması yapılan terimlerdir.

Kişisel veri kanunda, "*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" şeklinde tanımlanmıştır ve bu tanım ile mevzuatımızda bulunan bir eksiklik giderilmiş, özellikle TCK bakımından kanunilik ve belirlilik ilkesine uyulması sağlanmıştır. TCK m. 135-140 arasında kişisel verilerin korunmasına yönelik olarak düzenlenmiş suçların madde metinlerinde kişisel veri ya da kişisel verinin işlenmesi gibi kavramlara ilişkin bir tanım yapılmamış olması ve bunu tanımlayacak başka bir kanun da bulunmaması sorunlara sebep olmuş ve eleştirilmiştir¹⁶².

İnsan onuru ile bağdaşmayacak işlemler yapılmaması için kişisel verilerin işlenmesi birtakım ilkelere bağlanmıştır. Bu ilkelere uyulmadığı durumda işleme mümkün olmayacak, işleme yapıldığı takdirde ise hukuka aykırı ve kötü niyetli bir işleme olduğu kabul edilecektir. KVKK'nın 4. maddesinde de kişisel verilerin işlenmesi sırasında uyulması gereken ilkeler sayılmıştır. Bu ilkeler; "*hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme*" olarak sayılmıştır.

Kişisel verilerin işlenmesi kural olarak yasaktır. Ancak kişinin açık rızasının olması ya da hukuki düzenlemelerde sayılan şartların varlığı halinde kişisel veriler işlenebilir. Kişinin açık rızası Kanun'un 3. maddesinin gerekçesinde, 95/46/EC sayılı

¹⁶¹ Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s. 6.

¹⁶² Küzeci, a.g.e., s. 320; Korkmaz, a.g.e., s. 280.

Direktifteki tanımı ile “*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*”¹⁶³ şeklinde tanımlanmıştır. Kişinin açık rızası olmayan durumda verilerin işlenebilmesi için ise “*Kanunlarda açıkça öngörülmesi, fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması*” şartlarından birinin gerçekleşmesi gerekmektedir (KVKK m.5/2).

Ancak bu veri işleme şartları 6. maddede sayılan özel nitelikli kişisel verilerin (hassas veri) işlenmesinde geçerli değildir. 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 ve kişinin açık rızası olmadan işlenemez. Ayrıca bu tür verilerin işlenebilmesi için, Kişisel Verileri Koruma Kurulu tarafından belirlenen yeterli önlemlerin alınması da gerekmektedir. Özel nitelikli kişisel verilerin de kişinin rızası aranmaksızın işlenebileceği durumlar sayılmıştır. Buna göre “*sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir*”.

¹⁶³ Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s. 8.

KVKK'nın 7. maddesinde “verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi” hususunda düzenleme yapılmıştır. 8. maddede ise kişisel verilerin aktarımının ancak veri sahibinin açık rızası ile yapılabileceği, ancak hassas veriler için gerekli önlemler de alındıktan sonra 6. maddede sayılan şartların, diğer veriler için ise 5. maddede sayılan şartlardan birinin bulunması durumunda, veri sahibinin rızası aranmaksızın aktarılabilmesi düzenlenmiştir. Bu maddedeki aktarma eylemi ilerleyen bölümlerde inceleyeceğimiz TCK m. 136 kapsamında yer alan “verileri hukuka aykırı olarak verme, yayma veya ele geçirme” suçunu oluşturan verme ve yayma eylemlerini ifade etmektedir. 9. maddede ise verilerin yurt dışına aktarılmasını düzenleyen hükme yer verilmiştir.

Kanun'un 10. maddesi veri sorumlusunun aydınlatma yükümlülüğü konusunda düzenlemelere yer verirken, 11. maddede ise ilgili kişinin hakları yer almaktadır. Kişisel verilerin işlenmesi sırasında kişinin bilgilendirilmesi, kişisel verilerin korunması hakkına yönelik müdahalelerin hukuka uygunluğunu denetlemek ve kişilerin haklarını etkili olarak kullanabilmelerini sağlamak açısından son derece önemlidir¹⁶⁴. Buna göre veri sorumlusu kişisel verileri elde ederken, “veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilmesi, kişisel veri toplamanın yöntemi ve hukuki sebebi, 11. maddede yer alan diğer hakları” konusunda ilgili kişileri bilgilendirmekle yükümlü kılınmıştır (KVKK m. 10). İlgili her kişi ise; “kişisel verilerinin işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse buna ilişkin bilgi talep etme, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme, kişisel verilerin eksik veya yanlış işlenmiş olması durumunda bunların düzeltilmesini isteme, 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, (d) ve (e) bentleri uyarınca yapılan işlemlerin¹⁶⁵, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde

¹⁶⁴ Güray Dağ, *Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması*, (Doktora Tezi), İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2011, s. 121; Küzeci, a.g.e., s. 224.

¹⁶⁵ Bu işlemler, verilerin düzeltilmesi ve silinmesi ya da yok edilmesi talebi uyarınca yapılan işlemlerdir.

zararın giderilmesini talep etme” haklarına sahiptir ve bunları gerçekleştirmek için veri sorumlusuna başvurabilir.

Veri sorumlusunun “veri güvenliğine ilişkin yükümlülükler”i ise 12. maddede sayılmıştır. Kanun’un 13-16. maddelerinden oluşan dördüncü bölüm ise “başvuru, şikayet ve veri sorumluları sicili” konularını düzenlemektedir. 17 ve 18. maddelerde ise “Suçlar ve kabahatler” düzenlenmiştir. Kanun 17. madde ile kişisel verilere ilişkin suçlar için TCK’nın 135-140. maddelerine atıf yapmıştır. Altıncı bölümde bulunan 19-27. maddelerde “Kişisel Verileri Koruma Kurumu ve Teşkilat” yapısına yer verilmiştir.

KVKK’nın uygulanmayacağı durumları düzenleyen “İstisnalar” başlıklı 28. maddeye bakıldığında, düzenlenen istisnaların 95/46/EC sayılı Direktif’e göre oldukça fazla olduğu, dolayısıyla Kanun’un kapsamının, hazırlanmasında örnek alınan Direktif’e göre oldukça daraldığı fark edilmektedir¹⁶⁶.

KVKK, 95/46/EC sayılı Direktif örnek alınarak hazırlanmıştır. Zaten maddeleri de bu Direktif ile paralellik göstermektedir. Ancak Kanun hazırlanırken 2016/679 sayılı GVKT yerine Direktif’in esas alınmış olması bu Kanun’un eleştirilen noktalarından biridir. GVKT’nin teklifi 2012 yılında yayınlanmıştır. Bu nedenle KVKK hazırlanırken 95/46/EC sayılı Direktif yerine bu direktifi 25.05.2018 yılında ilga eden GVKT esas alınabilirdi. Bu haliyle KVKK’nın, yürürlüğe girdiği andan itibaren güncellenmesi gereken hükümler içeren bir kanun olduğu yorumu yapılabilecektir¹⁶⁷.

IV. UYGULAMADA KİŞİSEL VERİLERİN KORUNMASI

Yukarıda kişisel verilerin korunmasına yönelik olarak hazırlanmış gerek ulusal gerekse uluslararası pek çok düzenleme sayılmış ve bunlar hakkında kısaca bilgi verilmiştir. Bu başlık altında sayılan bu düzenlemeler ışığında verilen kararlardan bahsedilerek, bu alanda yapılan düzenlemelerin uygulamada nasıl kullanıldığı, kişisel verilerin pratikte nasıl korunduğu konusunda bir fikir oluşturulması ve konunun verilen örnekler yardımı ile daha anlaşılır hale getirilmesi amaçlanmaktadır.

¹⁶⁶ Köse Aysun, a.g.e., s. 81.

¹⁶⁷ Uncular, a.g.e., s. 98; Köse Aysun, a.g.e., s.80.

Verilerin korunması konusunda oldukça önemli bir yere sahip olan 1983 tarihli Alman Anayasa Mahkemesi kararı, Alman Parlamentosu tarafından 1982 yılında kabul edilen Nüfus Sayım Yasası'nın iptaline ilişkindir. Parlamento tarafından oy birliği ile kabul edilen bu kanun yapılacak nüfus sayımı sırasında vatandaşlarca oldukça detaylı bilgiler verilmesini gerektiren bir anket uygulanmasını öngörmektedir. İsim, adres, medeni durum, gelir durumu, çalışma ve iş bilgileri gibi bilgileri içeren bu anketlerin uzun süre tutulacak olmasının düşünülmesi ve sadece istatistiki amaçlarla değil, ikametgah kayıtlarının karşılaştırılması ve düzeltilmesi için kullanılacak olması vatandaşlarda kişisel verilerinin korunması konusunda endişe yaratmıştır. Kişiler bu anketlerde yer alan bilgilerin tekrar kendileri ile ilişki kurulacak şekilde işlenmesinden kaygı duymuşlardır. Bu sebeple yasaya karşı protestoların yanında hukuki başvurular da yapılmıştır¹⁶⁸.

Alman Anayasa Mahkemesi bu yasayı vatandaşların temel hak ve özgürlükleri konusunda yeterli önlem alınmamış olması sebebi ile iptal etmiştir. Mahkeme kararında kişilerin “bilgilerin geleceğini belirleme hakkı”na sahip olduğunu ve bu hakkın insan onuru ve kişiliği serbestçe geliştirme hakkının bir yansıması olduğunu belirtmiştir. Kişinin karar verme özgürlüğüne sahip olabilmesi için kendisine ait bilgilerden hangilerinin toplandığını, bu bilgilerin ne amaçla ve kimler tarafından kullanıldığını bilmesi gerekmektedir. Özellikle bilgisayar gibi otomatik veri işleme araçlarıyla verilerin işlendiği durumlarda bu durumun daha da büyük önem arz ettiği kanaatinde olan mahkeme toplanan verilerin kişinin kamusal hayata katılımını engelleyebileceğini belirtmiştir. Mahkeme örnek olarak toplantı, gösteri yürüyüşü ya da sivil toplum örgütüne katılan kişinin, bu durumun kaydedildiği düşüncesine sahip olması durumunda, bu haklarından vazgeçebileceğini, bu durumun kişilerin kendilerini özgürce geliştirmelerine engel olabileceğini ve bunun sonucu olarak da demokratik toplumun varlığının tehlikeye girebileceğini belirtmiştir. Mahkeme aynı zamanda bu kararında; devletin demokratik toplum değerlerine zarar vermemek kaydıyla kendisine verilen görevin gereği olması durumunda kayıt tutup, bu kayıtları değerlendirip gerekirse farklı kayıtlar arasında ilişki kurabileceğini, bilgilerin geleceğini belirleme hakkının sınırsız bir hak olmadığını

¹⁶⁸ Elif Küzeci, “İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı”, *İnsan Hakları Yıllığı*, C.32, (2014), s. 55, https://www.academia.edu/37176330/%C4%B0statistik%C3%AE_Birimler_ve_Bilgilerin_Gelece%C4%9Fini_Belirleme_Hakk%C4%B1_Statistical_Units_and_Right_to_Informational_Self-Determination, (07.08.2019).

belirtmiştir. Mahkemenin bu kararına bakıldığında; korunması gereken değer insan onuru ve bireysel özerklik olduğu; bu değerlerin korunması için de özel hayatın gizliliği, kişisel verilerin korunması ve bilgilerin geleceğini belirleme hakkına ihtiyaç olduğu yaklaşımının söz konusu olduğu görülmektedir¹⁶⁹.

Ülkemizde Anayasa Mahkemesi'ne "kanunen verilmemesi gereken kişisel verinin idari makamlara açıklanması ve güvenlik soruşturmasına esas alınması nedeniyle özel hayata saygı hakkının ihlal edildiği iddiası" ile yapılan bireysel başvuru¹⁷⁰ sonucunda Mahkeme başvurunun kabul edilebilir olduğuna ve hak ihlaline karar vermiştir. Başvurucunun on sekiz yaşından küçükken hırsızlık suçu işlediği, yapılan yargılama sonucunda 5 aylık hapis cezası aldığı ve bu cezanın ağır para cezasına çevrilerek ertelendiği belirtilmiştir. Kapalı Ceza İnfaz Kurumlarına sözleşmeli infaz ve koruma memurluğu alımı için sınava katılan başvuru Adli Yargı İlk Derece Mahkemesi Adalet Komisyonu tarafından yapılan yazılı ve sözlü sınavlarda başarılı olmuş ve infaz ve koruma memurluğuna yerleştirilmesi düşünülmüştür. Ancak Komisyon Başkanlığınca yapılan güvenlik soruşturması ve arşiv araştırması sonucunda Emniyet Müdürlüğü tarafından Komisyona, başvuru hakkında hırsızlık suçundan işlem yapıldığının tespit edildiği bildirilmiş ve ilgili karar da gönderilmiştir. Bunun sonucunda Komisyon Başkanlığı tarafından CTE Genel Müdürlüğüne gönderilen yazı ile hırsızlık suçu nedeniyle başvuru devletin memurluğuna atanacaklarda aranan şartları taşımadığı belirtilerek sözleşmeli infaz ve koruma memuru olarak istihdam edilmesinin uygun olmayacağı görüşü bildirilmiştir. Bu bildirimden ardından başvuru hukuki yolları tüketerek Anayasa Mahkemesine bireysel başvuruda bulunmuştur.

Anayasa Mahkemesi bu konuda ilgili hukuk başlığı altında KVKK'nın özel nitelikli kişisel verileri düzenleyen 6. maddesine ve Anayasa'da, kişisel verilerin korunmasını isteme hakkının düzenlendiği 20. maddesine değinmiş ve ceza mahkumiyetinin kişisel veri olduğunu, bu sebeple konunun Anayasa m. 20'de yer alan özel hayata saygı hakkı kapsamında değerlendirilmesi gerektiğini belirtmiştir. Anayasa Mahkemesi'ne göre kamu mercileri tarafından özel yaşamı ile ilgili sorular sorulması dahil bir bireyin özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin alınması,

¹⁶⁹ a.g.m., s. 55-58.

¹⁷⁰ AYM, 27.02.2019, *Fatih Saraman*, B. No: 2014/7256, (RG. 27.03.2019, sy: 30727).

kaydedilmesi, saklanması ve kullanılması özel hayata saygı hakkına müdahale teşkil etmektedir. Bu sebeple de Mahkeme başvuru konusuyla ilgili olarak “*Resmî makamlar tarafından muhafaza edilmekte olan, başvuru hakkında yürütülen ceza yargılamasına dair bilgilerin özel hayata saygı hakkı anlamında kişisel nitelikli veriler olduğu açıktır. Söz konusu kişisel verinin kamu kurumlarıyla paylaşılması ve güvenlik soruşturmasında kullanılmasının Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkına bir müdahale oluşturduğu sonucuna varılmıştır.*” şeklinde görüşünü ifade etmiştir. Anayasa uyarınca temel hak ve özgürlüklere sınırlama getirilebilmesi için, bunun kanunda belirtilmiş olması ve kişisel verilerin korunması hakkının sınırlanmasının da ancak kanun ile olabileceği kararda belirtilmiştir. Mahkeme kararda yer alan

“Bununla birlikte temel hak ve hürriyetlerin sınırlandırılmasına ilişkin kanunların şeklen var olması yeterli değildir. Kanunilik ölçütü aynı zamanda maddi bir içeriği de gerektirmekte olup bu noktada kanunun niteliği önem kazanmaktadır. Kanunla sınırlama ölçütü sınırlamanın erişilebilirliğini, öngörülebilirliğini ve kesinliğini ifade etmekte; böylece uygulayıcının keyfi davranışlarının önüne geçtiği gibi kişinin hukuku bilmesine de yardımcı olmakta; bu yönüyle hukuk güvenliği teminatı sağlamaktadır.

Kanunun bu gerekliliklere uygun olduğunun söylenebilmesi için yeterince ulaşılabilir olması, vatandaşların belirli bir olaya uygulanabilir nitelikteki hukuk kurallarının varlığı hakkında yeterli bilgiye sahip olabilmesi, ayrıca ilgili normun keyfiliğe karşı uygun bir koruma sağlaması, yetkili makamlara verilen yetkinin genişliğini ve icra edilme biçimlerini yeterli bir netlikte tanımlaması gerekmektedir.

Hukukun kendisi -beraberinde getireceği idari pratiğin dışında- söz konusu işlemin meşru amacım da gözönünde tutarak keyfi müdahalelere karşı bireyi korumak için yetkili makamlara bırakılan takdir yetkisinin kapsamını yeterince açık bir şekilde göstermelidir. Hukuk sistemi vatandaşlara, kamu makamlarına hangi koşullarda ve hangi sınırlar içinde müdahalelerde bulunma yetkisi verdiğini yeterince açık ifadelerle gösterecek nitelikte olmalı ve bu bağlamda ilgili müdahalenin muhataplarının müdahaleye zemin hazırlayan koşullar ile müdahalenin sonuçları açısından bir öngörüde bulunabilmeleri imkânı tanınmalıdır.

Bununla birlikte her ihtimale çözüm getiremeyecek olan yasal mevzuatın sağladığı koruma seviyesi büyük ölçüde ilgili metnin düzenlediği alan ve içeriğiyle birlikte muhataplarının niteliği ve sayısı ile yakından bağlantılıdır. Bu nedenle kuralın karmaşık olması ya da belirli ölçülerde soyutluk içermesi ve buna bağlı olarak hukuki yardım ile tam olarak anlaşılabilir hâle gelmesi tek başına hukukten öngörülebilirlik ilkesine aykırı görülemez. Bu kapsamda hak ya da özgürlüğe müdahale eden kural belirli ölçülerdeki takdir alanını elbette uygulayıcıya bırakabilir. Fakat bu takdir alanının sınırlarının da yeterli açıklıkta belirlenmesi ve kuralın asgari bir kesinlik içermesi zaruridir.

Bu kapsamda ilgili kanuni düzenlemenin söz konusu sınırlamaya ilişkin temel çerçeveyi ortaya koymakla birlikte özellikle uygulama koşulları ve usule ilişkin ayrıntıları düzenleyici işlemlere bırakması mümkündür. Ancak bu ihtimalde de söz konusu düzenleyici işlemin yine muhataplarınca ulaşılabılır olması ve içeriği hakkında ilgilileri yeterince aydınlatacak nitelik ve açıklıkta olması gerekmektedir.”

şeklindeki açıklaması ile temel hak ve özgürlükleri sınırlandıracak kanunlarda bulunması gereken şartları da saymıştır.

Olayla ilgili olarak, 5352 sayılı Kanun'un 10. maddesinde “Onsekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir.” hükmünün bulunduğu, buna göre kişi, suç işlediği sırada on sekiz yaşından küçükse, bu suça ilişkin kayıtların idari makamlara bildirilmesinin hukuken mümkün olmadığı, kanunda yer alan hükme açıkça aykırı şekilde işlem yapıldığı dikkate alınarak “özel hayata saygı hakkına yönelik müdahalenin kanuni dayanaktan yoksun olduğu” belirtilmiş ve Anayasa'nın 20. maddesinde koruma altına alınan “özel hayata saygı hakkı”nın ihlal edildiğine karar verilmiştir. Bu karar kişisel verilerin korunması hakkı ve diğer haklar bakımından uyulması gereken sınırlama şartlarının belirtilmesi ve devlet kurumlarında işe başlayacak kişiler hakkında uygulanan güvenlik soruşturmasında dahi kişisel verilere sınırsız erişim sağlanmasının mümkün olmadığını, bu durumun hukuka aykırılıklar teşkil edebileceğini göstermesi açısından önemli bir karardır.

Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlayıp kişisel verilerle ilgili hak ihlali oluştuğunu ileri sürenlerin şikâyetlerini karara bağlayıp, gerekli incelemeler yapmak ve önlemler almak gibi görevleri olan ve bağımsız bir merci olan Kişisel Verileri Koruma Kurulu da kişisel verilerin korunması için şikâyetleri karara bağlamaktadır. Kurula yapılan bir başvuruda “İlgili kişi şahsına ait cep telefonunun açık rızası olmaksızın bir yatırım ve menkul değerler şirketi tarafından bilgilendirme/reklam amaçlı aranması üzerine veri sorumlusuna yaptığı başvuruya yeterli yanıt alamaması nedeniyle Kişisel Verileri Koruma Kuruluna” şikâyette bulunmuştur¹⁷¹. Yapılan inceleme ile “şikâyetçinin müşterisi olduğu personelin daha önce başka bir yatırım şirketinde çalıştığı, bu şirketin faaliyetlerine son verilip kapatılmasının ardından 2017 yılında bahse

¹⁷¹ Kişisel Verileri Koruma Kurulu Kararı, Karar Tarihi: 08/07/2019, Karar No:2019/204, [https://www.kvkk.gov.tr/Icerik/5517/2019-204,\(07.08.2019\)](https://www.kvkk.gov.tr/Icerik/5517/2019-204,(07.08.2019)).

konu personelin yine aynı alanda faaliyet gösteren veri sorumlusu şirkette çalışmaya başladığı, dolayısıyla şikayetçinin telefon numarası bilgisine bu şekilde vakıf olunduğu ve sonrasında veri sorumlusunun bir personeli tarafından ilgili kişinin reklam ve bilgilendirme amacıyla arandığı” belirtilmiştir. Kurul olayı kişisel verilerin işleme şartlarının düzenlendiği KVKK m. 5 kapsamında değerlendirmiştir. Buna göre verilen karar şu şekildedir:

“• Şikayete konu başvuru, veri işleme şartları açısından değerlendirildiğinde Şirketin Şikayetçinin telefon numarasını işlemesinin 6698 sayılı Kanunun 5 inci maddesinde sayılan şartlardan herhangi birine dayanmaması nedeniyle Şirketin hukuka aykırı bir veri işleme faaliyetinde bulunduğu sonucuna ulaşıldığından, Kanunun 12 nci maddesinin (1) numaralı fıkrasının (a) bendine aykırı hareket etmesi nedeniyle Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi gereğince Şirket hakkında 75.000 TL idari para cezası uygulanmasına,

• Şirketin beyanlarında yer alan; Şikayetçinin Şirketin bir pazarlama personelinin başka bir şirkette çalışırken müşterisi olması nedeniyle, bu personelin yeni işyeri olan Şirkete bu verileri aktardığına ilişkin iddialarına ilişkin olarak; Şikayetçinin Türk Ceza Kanununun 136 ncı maddesi hakkında bilgilendirilmesine,

• Şikayetçinin Şirketi muhatap başvurusunda yer alan kişisel verilerinin kimlerden ne şekilde elde edildiğine dair bilgi talebine Şirketçe cevap verilmemiş olması nedeniyle Şirketin Kanuna uyum konusunda gerekli hassasiyeti ve özeni göstermesi yönünde uyarılmasına ve söz konusu hususlarda Şirketin Kurumu muhatap yazısında belirtildiği şekliyle Şikayetçiye bilgi vermesi yönünde talimatlandırılmasına karar verilmiştir.”

Özellikle ülkemizde kısa mesaj ve telefonla arama yoluyla reklam faaliyetlerinin oldukça yaygın olduğu ve bu sebeple kişilerin telefon numarası ve diğer bilgilerinin üçüncü kişilere aktarıldığı göz önüne alındığında, kişisel verilerin hukuka uygun olmayan şekilde işlenmesi durumunda karşılaşılabilecek sonuçları göstermesi ve caydırıcılık sağlanarak kişisel verilerin etkili şekilde korunması bakımından bu karar oldukça önemlidir¹⁷².

¹⁷² Kişisel Verileri Koruma Kurulu'nun reklam amaçlı kısa mesaj gönderen kurumlar hakkında idari para cezası verdiği farklı kararları da mevcuttur: Kişisel Verileri Koruma Kurulu Kararı, Karar Tarihi: 18/09/2019, Karar No: 2019/276, <https://www.kvkk.gov.tr/Icerik/6558/2019-276>, (25.11.2019); Kişisel Verileri Koruma Kurulu Kararı, Karar Tarihi: 31/05/2019, Karar No:2019/162, <https://www.kvkk.gov.tr/Icerik/5495/2019-162>, (25.11.2019).

Kişisel Verileri Koruma Kurulu'na yapılan bir diğer başvuruda¹⁷³ ise, başvuran veri sahibi, sadakat programına kayıtlı olduğu havayolu şirketine kullanıcı adı ile şifresini değiştirme talebinde bulunmuş, şirket bu işlemin yapılabilmesi için kişiden kimliğinin arkalı önlü fotokopisini talep etmiştir. İlgili kişi, kimliğinin fotokopisini şirkete iletmesinin ardından, kimlik görüntülerinin silinmesi ve bu bilgiler üçüncü kişilere aktarıldıysa, söz konusu bilgilerin bu kişilerin kayıtlarından da silinmesi talebinde bulunmuştur. Veri sorumlusu talebe yanıt olarak bu verilerin sistemde tutulmadığını ve üçüncü kişilerle de paylaşılmadığını belirtmiştir. Veri sahibinin Kurul'a başvurusu sonucu Kurul, kimlik üzerinde din ve kan grubu bilgilerinin yer alması sebebiyle hassas verilerin işlenmiş olduğunu, bu işleme faaliyetine ilgili kişinin rızası olmadığı gibi, KVKK'da sayılan işlemeyi hukuka uygun hale getirecek şartların da bulunmadığını, dolayısıyla hukuka aykırı olarak verilerin işlenmiş olduğunu belirtmiştir.

Kurul bunun yanında olayla ilgili, kişisel verilerin işlenmesine ilişkin ilkeler çerçevesinde de bir değerlendirme yapmıştır. Bu değerlendirmede;

“• Arkalı önlü kimlik görüntüsünün işlenmesinin, Kanunun 5 inci ve 6 ncı maddeleri kapsamında kişisel verilerin işleme şartlarına uygun olmayan bir işleme faaliyeti olduğu değerlendirildiğinden, hukuka uygunluk ilkesine aykırı olduğu; öte yandan veri sorumlusunun kimlik görüntüsünün muhafaza edilmesine rağmen kayıt altına alınmadığı yönünde ilgili kişiye cevap vermesinden dolayı şeffaf olmadığı, bu nedenlerle de dürüstlük kuralına aykırı veri işleme faaliyetinde bulunduğu,

• Veri sorumlusunun kimlik görüntülerini işlemesinde hangi hukuki işleme şartına dayandığı hususunun ilgili kişiye verilen cevapta ve kurumumuza intikal eden yazıda belirtilmediği, bu nedenle veri sorumlusunun veri işleme faaliyetinin belirli, açık ve meşru amaçlar için işleme ilkesine aykırı olduğu,

• Kimlik doğrulama işlemi için daha az verinin işlenmesinin mümkün olduğundan hareketle veri sorumlusunun somut olayda işlediği kimlik görüntüsünün işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırı olduğu,

• Veri sorumlusunun kimlik görüntüsünü işlediği gibi, kimlik doğrulama işlemi bittikten sonra bu verileri silmediği, Kurumumuzca bilgi belge talep edilmesi üzerine sildiğini beyan ettiği gerçeğinden yola çıkarak, veri sorumlusunun veri işleme faaliyetinin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesine de aykırı olduğu”

¹⁷³ Kişisel Verileri Koruma Kurulu Kararı, Karar Tarihi: 01/10/2019, Karar No:2019/294, <https://www.kvkk.gov.tr/Icerik/6556/2019-294>, (25.11.2019).

sonucuna varmıştır. Değerlendirmeler sonucunda, hassas verileri ilgili kişinin rızası ya da diğer şartlar olmaksızın işleyen, genel ilkelere (KVKK m. 4) uygun davranmayan ve veri sahibinin haklarına uymayan veri sorumlusu hakkında veri güvenliği ile ilgili yükümlülüklerine uymaması sebebiyle idari para cezası verilmiştir.

Buna benzer şekilde başka bir başvuruda¹⁷⁴ da Kişisel Verileri Koruma Kurulu, KVKK m. 4’te yer alan ilkelere uyulmaması sebebiyle hukuka aykırılık kararı vermiştir. İlgili başvuruda, bir banka personeli; veri sahibinin telefon numarasını, veri sahibinin eşine ulaşmak amacıyla aramıştır. Veri sahibi tarafından bankacılık işlemleri ile ilgili olarak verilmiş olan telefon numarasının, bu işlemlerle ilgisi olmayan bir amaçla kullanılması sebebiyle Kurul, “belirli, açık ve meşru amaçlar için işleme ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkelerine aykırılık olduğuna karar vermiştir.

Bu kararlardan da görülebileceği gibi, kişisel verilerin işlenmesi sırasında, işleminin hukuka uygun kabul edilebilmesi için yalnızca işleme şartlarının (KVKK m.5 ve m. 6) varlığı yeterli değildir. Bu şartlar sağlansa da verilerin işlenmesi sırasında, kişisel verilerin işlenmesine ilişkin ilkelere aykırı bir durumun söz konusu olması işlenmeyi hukuka aykırı hale getirecektir.

AİHM de kişisel verilerin korunmasına ilişkin pek çok karar vermiştir. S. ve Marper/Birleşik Krallık Davası¹⁷⁵ da kişisel verilerin korunmasına ilişkin bir davadır. Başvuranlardan biri şiddet kullanarak hırsızlık yapmaktan diğeri ise birlikte olduğu kişiyi taciz etmekten dolayı suçlanmış ve parmak izleri DNA ve hücre örnekleri alınmıştır. Sonrasında başvuranlardan biri hakkında beraat diğeri hakkında ise kovuşturmaya yer olmadığı kararı verilmiştir. Her iki başvuran da parmak izleri ve DNA örneklerinin yok edilmesini talep etmişler, ancak talepleri polis tarafından kabul edilmemiştir. Yasal yollarda da talepleri reddedilen başvuranlar, herkesin kendine ait bilgilerin özel kalması, iletilmemesi veya izni olmaksızın başkasına verilmemesi hakkına sahip olduğunu belirterek AİHS m. 8’in ihlal edildiği gerekçesiyle AİHM’ye başvurmuşlardır. Hükümet savunmasında “parmak izlerinin, DNA profillerinin ve örneklerin, Verilerin Korunması Kanunu kapsamında, ilgili kişilerin kimliğini belirleyebilecek kişilerin elinde

¹⁷⁴ Kişisel Verileri Koruma Kurulu Kararı, Karar Tarihi: 18.09.2019, Karar No:2019/277, <https://www.kvkk.gov.tr/Icerik/5545/2019-277>, (25.11.2019).

¹⁷⁵ S. ve Marper/Birleşik Krallık Davası, Başvuru No: 30562/04 ve 30566/04, Karar Tarihi: 4 Aralık 2008.

bulunan ‘kişisel nitelikte veriler’ olduklarını” kabul etmiştir. Ancak “sadece, parmak izlerinin, DNA profillerinin ve örneklerin, 1984 Kanunu’nun 64. maddesinde öngörülen amaçlarla sınırlı olarak muhafaza edilmesinin, Sözleşme’nin 8/ 1. maddesinde öngörülen, özel yaşama saygı gösterilmesi hakkı kapsamına girmediği”ni ifade etmiştir. Hükümet, “Bu verilerin alınmalarından farklı olarak, muhafaza edilmelerinin, fiziksel ve psikolojik bütünlüğe saldırı oluşturmadığını ve kişisel gelişime, benzerleriyle ilişki kurma ve geliştirme ve geleceğini belirleme hakkına da aykırı” olmadığını belirtmiştir (Paragraf 63).

Mahkeme de kişilerden alınan örneklerin kişisel veri olduğunu belirtmiştir (Paragraf 68). Mahkeme ayrıca kişinin, “gelecekte, resmi makamların muhafaza ettikleri, özel bilgilerinin nasıl kullanılabilmesine ilişkin kaygılarının meşru olduğunu” belirtmiştir. Genetik ve bilgi teknolojileri alanındaki yeniliklerin artması sebebiyle Mahkeme, “genetik bilgilere dayanan, özel yaşamın unsurlarının, bugün öngörülemez, ileride, yeni yollarla, müdahalelere yol açabileceği ihtimalinin göz ardı” edilemez olduğunu belirtmiştir (Paragraf 71). Mahkeme, “hücre örneklerinin, son derece kişisel nitelikleri dışında, bunların, bir kişiyle ilgili, özellikle de sağlığıyla ilgili, çok hassas bilgiler taşıdıklarını” belirtmiştir. Ayrıca hücre örneklerinin, “hem ilgili kişi için hem de onun aile fertleri için, çok önemli olan, tek bir genetik şifre” içerdiği belirtilmiştir (Paragraf 72). DNA profilleri konusunda Hükümet, “DNA profilinin, tamamen objektif ve çürütülemez olan bilgiler barındıran bir rakamlar serisi ya da barkoddan oluştuğunu ve bir kişinin kimliğinin belirlenmesinin, sadece, veri tabanındaki profillerden biriyle uyum göstermesi halinde mümkün olduğunu” ifade etmiş ve “söz konusu bilgilerin şifreli olmaları sebebiyle, bunları anlaşılabilir hale getirebilmek için, bilgisayar teknolojisine başvurulması gerektiğini ve sadece, kısıtlı sayıdaki kişilerin, bunları yorumlayabileceklerini” belirtmiştir. Mahkeme ise bunların, daha az, kişisel bilgi barındırdıklarını kabul etmiştir (Paragraf 74). Ancak “DNA profillerinin, bireyler arasındaki genetik ilişkilerin tespit edilmesini sağlayacak bir araç” olduğunu ve “bunların muhafaza edilmesinin, bu bireylerin özel hayatına saldırı oluşturduğunu”nu kabul etmiştir (Paragraf 75). Ayrıca, etnik kökene ilişkin çıkarımlar da DNA profilleri aracılığı ile yapılabileceğinden bu verilerin daha hassas ve özel hayata saldırı oluşturabilecek, iyi korunması gereken veriler kategorisine dahil olduğu ifade edilmiştir (Paragraf 76). Görüldüğü gibi verinin kişi ile ilişkilendirilmesi herkes tarafından ve doğrudan

yapılamıyor olsa bile sonucunda ortaya çıkacak bilgi sebebiyle verinin hassas veri kapsamında korunması beklenmektedir. AİHM'nin bazı kararlarında, parmak izlerinin, hücre örnekleri ve DNA profilleri kadar bilgi barındırmadığı, bu nedenle de AİHS'ye aykırılık oluşmadığı belirtilmiştir. Bu sebeple, ilgili olayda da Mahkeme, parmak izlerinin diğer örnekler ile aynı şekilde değerlendirilmemesi gerektiğini kabul etmiştir (Paragraf 78). Ancak söz konusu olayda, parmak izlerinin toplanması, kullanılması ve saklanması konusunda haklı gerekçe bulunup bulunmadığının belirlenmesi gerektiğini belirtmiş, ardından bu bilgilerin saklanmasının özel yaşama saygı gösterilmesi hakkına saldırı niteliğinde olması sebebiyle AİHS m. 8'in ihlal edildiğine karar vermiştir (Paragraf 125-126).



ÜÇÜNCÜ BÖLÜM

TÜRK CEZA HUKUKU KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI

I. GENEL BİLGİLER

Türk Ceza Kanunu'nda kişisel verilerin korunmasına yönelik olarak ikinci kitabında “Kişilere Karşı Suçlar” başlıklı ikinci kısım ve “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı dokuzuncu bölüm altında üç suç tipi düzenlenmiştir. “Kişisel verilerin kaydedilmesi”, “Verileri hukuka aykırı olarak verme veya ele geçirme”, “Verileri yok etmeme” suçları TCK'nın 135, 136 ve 138. maddelerinde düzenlenmiştir. TCK 135 ve 136. maddedeki suçlara ilişkin “Nitelikli haller” TCK m. 137'de, “Şikayet”e ilişkin düzenleme TCK m. 139'da ve “Tüzel kişiler hakkında güvenlik tedbiri uygulanması” TCK m. 140'da düzenlenmiştir.

Kişisel verilerin korunması konusunda cezai düzenlemeler yapılırken ülkeler iki farklı yöntem tercih etmektedir. Birincisi İtalya ve Almanya'da olduğu gibi kişisel verilerin korunmasına yönelik kanunlarda bu konudaki suçlara da yer verilmesi, ikincisi ise Fransa ve ülkemizde olduğu gibi bu tip suçlara ilişkin düzenlemelerin ceza kanunlarında yer almasıdır¹⁷⁶.

Kişisel verilerin korunmasının düzenlendiği TCK maddelerinin kişisel verinin tanımına yer vermemesi, kanunda eksik noktalar olduğu hususunda doktrinde çokça eleştirilmiştir. Doktrinde kanunda kişisel veri tanımı olmaksızın bu maddelerin uygulanmasının kanunilik ilkesine aykırı olacağı görüşünü savunanlar bulunmaktadır¹⁷⁷. Ancak 2016 yılında KVKK'nın yürürlüğe girmesi ile beraber kişisel veri ve kişisel verinin işlenmesi kavramlarının tanımı ile ilgili belirsizlikler ortadan kalkmış, kanuni bir tanıma dayalı olarak TCK maddelerinin uygulanması imkanı doğmuştur.

¹⁷⁶ Elif Mendos Kuşkonmaz, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, (Yüksek Lisans Tezi), İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2013, s. 127-128.

¹⁷⁷ Gültekin, a.g.e., s. 122-124.

KVKK'nın "Suçlar" başlıklı 17. maddesinde bu konudaki suçlar için TCK'ya atıf yapıldığından iki kanunun bu konu bakımından bağlantılı hale geldiği söylenebilir.

II. KİŞİSEL VERİLERİN KAYDEDİLMESİ SUÇU (TCK m. 135)

A. GENEL OLARAK

Kişisel verilerin kaydedilmesi suçu eski 765 sayılı TCK'da yer almamakta olup 5237 sayılı TCK'nın 135. maddesinde "*(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. (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.*" şeklinde düzenlenmiştir. Maddenin temel şeklinin işlenmesi halinde verilecek cezanın alt sınırı daha önce altı ayken 21.2.2014 tarihli ve 6526 sayılı Kanun ile bir yıl şeklinde değiştirilmiştir. İkinci fıkrada yer alan nitelikli hale ilişkin düzenlemede ise daha önce "*yukarıdaki fıkra hükmüne göre cezalandırılır*" şeklinde bir ibare yer alırken, 24.3.2016 tarihli ve 6698 sayılı Kanun ile "*birinci fıkra uyarınca verilecek ceza yarı oranında artırılır*" şeklinde değişiklik yapılmıştır. Bu değişiklik hassas veri niteliğine sahip kişisel verilerin daha özel bir korumaya sahip olması bakımından yerinde olmuştur.

Maddenin gerekçesinde¹⁷⁸ ise; "Çağımızda kişilerle ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmakta...bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler." şeklinde bir ifade yer almaktadır. Bu durumun kişileri zarara

¹⁷⁸ Ankara HBV Üniversitesi Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, *Türk Ceza Hukuku Mevzuatı – Cilt 1 (Kanunlar)*, 23. b., Ankara: Seçkin Yayıncılık, 2019, s. 340.

uğratacak olması sebebiyle, kişilerin uğrayacağı zararların önüne geçilebilmesi amacıyla kişisel verilerin kaydedilmesi suçu oluşturulmuştur.

TCK m. 135/1’de suçun temel şekline yer verilmiş, ikinci fıkrada ise sayılan hassas veri niteliğine sahip bilgilerin kaydedilmesi durumunda, cezanın artırılmasını gerektiren nitelikli hale yer verilmiştir. TCK’nın 137. maddesinde¹⁷⁹ ise suçu işleyen kişiler bakımından cezanın artırılmasını gerektiren nitelikli hallere yer verilmiştir.

B. KORUNAN HUKUKSAL DEĞER

Kişisel verilerin kaydedilmesi suçu “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı bölümde yer almaktadır. Türk Ceza Kanunu’nun sistematığıne bakıldığında suçla özel hayat koruma altına alınmaya çalışılmıştır. AİHM’nin de kişisel verilere karşı yapılan müdahaleleri, AİHS m. 8’de düzenlenen özel hayata saygı hakkı kapsamında değerlendirdiğine daha önceki bölümlerde değinilmişti.

Anayasa’ya baktığımızda ise kişisel verilerin korunması; kişi hakları ve ödevlerinin düzenlendiği ikinci bölümde “Özel hayatın gizliliği” başlıklı 20. maddede düzenlenmiştir. Özel hayatın gizliliğini düzenleyen maddede yer alsa da tek başına kişisel verilerin korunmasını isteme hakkı şeklinde Anayasa’da yer verilmiştir. Yani bu hakkı, özel hayatın korunması hakkının bir parçası olarak değerlendirmek mümkünse de kişisel verilerin korunması hakkı tek başına bir haktır. Bu sebeple kişisel verilerin kaydedilmesi suçu ile korunmaya çalışılan hukuksal değer de kişisel verilerin korunması hakkıdır¹⁸⁰.

C. SUÇUN UNSURLARI

Bu bölümde tipiklik ve hukuka aykırılık unsuru başlıkları altında kişisel verilerin kaydedilmesi suçunun unsurları incelenecektir.

¹⁷⁹ TCK m. 137 Nitelikli haller: (1) 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.

¹⁸⁰ Handan Yokuş Sevik, *Türk Ceza Hukuku Özel Hükümler*, 1. b., Ankara: Adalet Yayınevi, 2018, s. 242-243.

1. Tipiklik

Tipiklik başlığı altında, suç tipinin genel özelliklerinden bahsedildikten sonra suçun maddi ve manevi unsurları konusunda açıklamalara yer verilecektir.

a. Suç tipinin genel özellikleri

Kişisel verilerin kaydedilmesi suçu yukarıda da belirtildiği gibi TCK m. 135'te iki fıkra olarak düzenlenmiştir. Birinci fıkrada “*Hukuka aykırı olarak kişisel verileri kaydeden kimseye*” verilecek cezadan bahsedilmiştir. İkinci fıkrada ise “*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*” artırılmış ceza verilmesi ile ilgili düzenleme yapılmıştır. Ayrıca TCK m. 137'de sayılan kişilerce ve belirtilen yollarla bu suçun işlenmesi durumunda da verilecek cezanın artırılması gerektiği konusunda bir düzenleme yer almaktadır.

Söz konusu suç bir tehlike suçudur, hareketin yapılması ile suç oluşmuş olur, ayrıca bir zararın meydana gelmesi gerekmemektedir. Yani verilerin kaydedilmesinden sonra silinmesi sebebiyle ya da başka bir sebeple verilere ulaşılamamış olması suçun oluşmasına engel değildir¹⁸¹. Ayrıca bu suçun cezalandırılabilmesi için, kanun maddesinde hareketin somut bir tehlikeye sebep olabilecek niteliği olması gerektiği belirtilmediğinden soyut tehlike suçudur¹⁸².

Kişisel verilerin kaydedilmesi suçunun oluşması için gereken hareketin kaydetme olduğu kanunda belirtilmiştir. Kaydetme fiili dışında bir fiil ile kişisel verilerin kaydedilmesi suçunun oluşması mümkün olmadığından bu suç bağlı hareketli suç niteliğine sahiptir¹⁸³.

Sırf hareket suçudur. Hareketin tamamlanmasıyla suç oluşur, ayrıca bir neticenin oluşması aranmaz¹⁸⁴.

¹⁸¹ Yokuş Sevük, a.g.e., s. 244.

¹⁸² Veli Özer Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, 13. b., Ankara: Seçkin Yayıncılık, 2018, s. 588.

¹⁸³ a.g.e., s. 587. Serbest hareketli suç olduğu yönündeki görüş için bakınız: Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 6. b., Ankara: Seçkin Yayıncılık, 2015, s. 680.

¹⁸⁴ Şeyma Sert, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, 1. b., Ankara: Seçkin Yayıncılık, 2019, s. 105; Akdağ, a.g.e., s. 97.

Verilerin hukuka aykırı şekilde kaydedildiği anda suç tamamlanmış olacağından, tipik hareketin belirli bir süre icrasına devam edilmesi zorunlu olmadığından ani suç niteliğini taşımaktadır¹⁸⁵.

Suçun özelliğine ilişkin belirtilmesi gereken son husus ise icrai hareketle işlenen bir suç olduğudur. Suçun işlenebilmesi için verilerin kaydedilmesi gerektiğinden ihmali olarak işlenmesi mümkün değildir¹⁸⁶.

b. Suçun maddi unsurları

Kişisel verilerin kaydedilmesi suçunun maddi unsurları; fail, mağdur, suçun konusu, hareket ve nitelikli unsurlardan oluşmaktadır. Bu suç bakımından sayılan her bir unsur konusunda değerlendirme yapılarak suç tipi detaylı olarak incelenecektir.

(1) Fail

TCK m. 135’te suçu işleyen kişi bakımından “hukuka aykırı olarak kişisel verileri kaydeden kimse”den bahsedilmiş, bunun dışında farklı bir özellik ise aranmamıştır. Bu durumda herkes bu suçun faili olabilecektir. Herkesin fail olması mümkün olmakla beraber; KVKK’nın uygulanması kapsamında bu suçun oluşması durumunda, KVKK kapsamında verilerin işlenmesi konusunda yetkili kişiler veri sorumlusu ve veri işleyen olduğundan genellikle bu kişilerin fail olması durumu ortaya çıkacaktır. KVKK’da veri işleyen, “*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*” olarak ifade edilmiştir (KVKK m. 3/1-ğ). Veri sorumlusu ise “*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*” şeklinde tanımlanmıştır (KVKK m. 3/1-ı).

Suçun faili yalnızca gerçek kişiler olabilir. TCK m. 20/2’ye göre tüzel kişilerin fail olması mümkün değildir. Tüzel kişinin faaliyeti sonucu kişisel verilerin kaydedilmesi suçunun işlenmesi durumunda ise, bu fiili gerçekleştiren gerçek kişinin fail olması

¹⁸⁵ Özbek, a.g.e., s. 587-588; Korkmaz, a.g.e., s. 330.

¹⁸⁶ Özbek, a.g.e.; Korkmaz, a.g.e.

mümkündür. Tüzel kişiler hakkında ancak TCK m. 60'da yer alan güvenlik tedbirleri uygulanabilir¹⁸⁷.

Suçun failinin kamu görevlisi ya da belirli bir meslek ve sanatı yapan kimse olması durumunda ise TCK m. 137'ye göre verilecek cezanın artırılması gerekecektir. Suçun temel şeklinin faili herkes olabilirken, nitelikli halin oluşması için maddede sayılan kişiler tarafından suçun işlenmesi aradığından kişisel verilerin kaydedilmesi suçu görünüşte özgü suçtur¹⁸⁸.

(2) Mağdur

Kanunda kişisel verilerin kaydedilmesi suçunun mağduru için özel bir düzenleme yapılmadığından herkes bu suçun mağduru olabilir.

Ancak hem gerçek hem tüzel kişilerin bu suçun mağduru olup olamayacağı hususuna da değinmek gerekmektedir. Gerçek kişiler bakımından tereddüt oluşturacak bir durum yoktur ve her gerçek kişi bu suçun mağduru olabilir. Tüzel kişilerin, kişisel verilerin kaydedilmesi suçunun mağduru olabilmesi noktasında ise görüş ayrılıkları mevcuttur. Kanunda bir ayırım yapılmamış olması sebebiyle bu suçun mağdurunun hem gerçek hem de tüzel kişi olabileceğini savunan görüşler¹⁸⁹ mevcuttur. Ancak KVKK m. 3'te ilgili kişi, kişisel verisi işlenen "gerçek kişi" olarak tanımlanmıştır. Ayrıca TCK m. 135'in gerekçesinde de kişisel veri, "gerçek kişiyle ilgili her türlü bilgi" olarak tanımlanmıştır¹⁹⁰. Bunların yanında TCK m. 135/2'de "kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına ve sendikal bağlantılarına ilişkin" veriler ile ilgili düzenlemeye yer verildiğini ve bu sayılan bilgilere ancak gerçek kişilerin sahip olabileceğini göz önüne aldığımızda, bu

¹⁸⁷ Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 61.

¹⁸⁸ İzzet Özgenç, *Türk Ceza Hukuku Genel Hükümler*, 14. b., Ankara: Seçkin Yayıncılık, 2018, s. 206.

¹⁸⁹ Doğan Soyaslan, *Ceza Hukuku Özel Hükümler*, 8. b., Ankara: Yetkin Yayınları, 2010, s. 346; Dülger, a.g.e., s. 677.

¹⁹⁰ Ankara HBV Üniversitesi Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, a.g.e., s. 340.

suçun mağdurunun yalnızca gerçek kişiler olabileceği kanısına varmaktayız¹⁹¹. Tüzel kişilerin ise suçtan zarar gören olması mümkündür¹⁹².

(3) Suçun konusu

Kişisel verilerin kaydedilmesi suçunun gerekçesinde suçun konusunun “kişisel veriler” olduğu belirtilmiş ve devamında “kişiye ait her türlü bilgi”nin kişisel veri olduğu söylenerek kişisel veri tanımlanmıştır¹⁹³. KVKK’da ise kişisel veri için “*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” tanımı yapılmıştır. Kişisel veri kavramı ile ilgili detaylı açıklama önceki bölümlerde yapıldığından bu bölümde yalnızca hangi verilerin kişisel veri kapsamında değerlendirildiği konusunda açıklamalara yer verilecektir. KVKK’nın 3. maddesinin gerekçesinde “isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler” kişisel verilere örnek olarak sayılmıştır. Yargıtay’ın kişisel verinin kapsamı ile ilgili olarak

“...nüfus bilgileri (TC kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA’sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği; ancak, herkes tarafından bilinen veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgilerin, yasal anlamda "kişisel veri" kapsamında değerlendirilemeyeceği, aksinin kabulü halinde; maddenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçların doğacağı, bu nedenle, bir kişisel bilginin, yasal anlamda "kişisel veri" kabul edilip edilmeyeceğine karar verilirken, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması, sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerektiği; öte yandan, bir özel hayat görüntüsü ya da sesinin, "kişisel veri" olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına dair görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere

¹⁹¹ Korkmaz, a.g.e., s. 338.

¹⁹² Sedat Erdem Aydın, *AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu*, 1. b., İstanbul: On İki Levha Yayıncılık, 2015, s. 131; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 62.

¹⁹³ Ankara HBV Üniversitesi Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, a.g.e., s. 340.

*sabitlenmesi 5237 Sayılı 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 5237 Sayılı TCK'nın 134/2. maddesinde özel hayatın gizliliğini ihlal suçu kapsamında düzenlendiğinden, kişinin özel hayatına dair görüntüsü, fotoğrafı ya da sesinin, yasal anlamda, 5237 Sayılı TCK'nın 136/1. maddesi kapsamında kişisel veri olarak değerlendirilemeyeceği...*¹⁹⁴

şeklinde bir kararı mevcuttur. Buna göre Yargıtay, kişinin özel hayatına ilişkin görüntü ve sesinin kişisel veri olduğunu kabul etmekle beraber bunların kaydedilmesi ve içeriğini öğrenme yetkisi bulunmayan kişilere ifşa edilmesi durumunda TCK m. 135 kapsamında olmadığını, TCK m. 134 kapsamında özel hayatın gizliliğini ihlal suçunun oluştuğunu belirtmiştir. “Özel hayatın gizliliğini ihlal” suçunun düzenlendiği 134. maddenin gerekçesinde “*gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının saptanması ve kaydedilmesi cezalandırılmaktadır*” ifadesi bulunmaktadır. Madde gerekçesine bakıldığı zaman Yargıtay’ın kararının yerinde olduğu anlaşılmaktadır. Ancak yine de her durumda kişinin ses ve görüntüsünün TCK m. 135 dışında olacağını söylemek doğru olmayacaktır. Kişinin ses ve görüntüsünün yalnızca özel hayata ilişkin olarak kaydedilmesi durumunda özel hayatın gizliliğini ihlal suçu oluştuğu kabul edilse de, kişinin özel hayatının dışında bu bilgilerin kaydediliyor olması durumunda olayın TCK m. 135 kapsamında değerlendirilmesinin daha doğru olacağı kanaatindeyiz¹⁹⁵.

Anılan kararda ve kişisel verinin tanımına ilişkin önceki bölümlerdeki açıklamalarımızda, kişisel verinin kapsamının çok geniş olduğu; mezun olunan okul, kişinin saç rengi gibi kişiye ait her verinin kişisel veri olduğu belirtilmiştir. Bu kadar geniş bir kavramın, sınırlandırılmadan, bu kapsama nelerin gireceği belirtilmeden TCK kapsamına dahil edilmesi, kanunun çok geniş bir alanda uygulanmasına sebebiyet verebilecek bir durumdur. Belirtilen kararda Yargıtay, somut olayın gereklerine göre verinin, kişisel veri olup olmadığının tespitinin yapılması gerektiğini ifade etmiş olsa da,

¹⁹⁴ 12. CD., 02.10.2012, E. 2012/20543, K. 2012/20422, www.kazanci.com, (28.11.2019)

¹⁹⁵ Korkmaz, a.g.e., s. 343; Yokuş Sevik, a.g.e., s. 243-244; Köse Aysun, a.g.e., s. 126.

bu farklı uygulamaların ortaya çıkmasına, maddenin kapsamının çok geniş bir şekilde uygulanmasına kesin olarak bir engel değildir¹⁹⁶.

Kişisel verilerin kapsamının çok geniş olması ve maddede bir sınırlamanın yer almaması sebebiyle kişilerin, aslında suç kapsamına girmesi gerekmeyen, kişisel verilerin korunması hakkının ağır ihlalini oluşturmayacak bir verinin kaydedilmesi sebebiyle de ceza alması mümkün olabilecektir. Bu durum ceza hukukuna son çare (ultima ratio) olarak başvurulması ilkesi ile bağdaşmamaktadır.

Bu gibi olumsuzlukların yaşanmaması için, TCK kapsamında kişisel verinin tanımına yer verilmesi, hangi verilerin bu kapsama girebileceği ya da hangi verilerin bu kapsama giremeyeceği gibi hususların daha açık şekilde ilgili maddede belirtilmesi daha yerinde olurdu. Bu şekilde bir düzenlemenin, uygulama açısından kolaylık sağlayacağı gibi belirlilik ilkesine de daha uygun olacağı kanaatindeyiz. Ayrıca yukarıda belirtildiği gibi, kişisel verilerin korunması hakkının ağır ihlaline sebep olmayacak nitelikteki kişisel verilerin kaydedilmesi durumunda idari yaptırımların uygulanması, daha ağır ihaller bakımından ise ceza hukukuna başvurulması, ultima ratio ilkesine uygunluk bakımından da daha yerinde bir düzenleme olacaktır¹⁹⁷.

Maddenin ikinci fıkrası için suçun konusu ise kişilerin, “siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin” kişisel verileridir.

(4) Hareket

Kişisel verilerin kaydedilmesi suçunun hareket unsurunu “kaydetmek” fiili oluşturmaktadır. Kaydetmek TDK’da “*Yazmak, bazı önemli noktaları tespit etmek; herhangi bir şeyi bir yere mal etmek, bir şeyin tarih, numara veya adını bir deftere geçirmek; hatırlamak için yazmak, not etmek; belirtmek, söylemek; sesi veya resmi manyetik bant üzerine geçirmek; elektronik veya sayısal araçlarda bilgiyi korumaya*

¹⁹⁶ Köksal Bayraktar, “Kişisel Verilerin Kaydedilmesi, Verilmesi, Ele Geçirilmesi ve Yok Edilmemesi”, *Özel Ceza Hukuku, Cilt III: Hürriyete, Şeref, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar (TCK m. 106-140)*, Köksal Bayraktar vd., İstanbul: On İki Levha Yayıncılık, 2018, s. 637.

¹⁹⁷ Kangal, a.g.e., s. 177.

almak.” ifadeleri ile tanımlanmıştır¹⁹⁸. KVKK ya da TCK’da kişisel verilerin kaydedilmesi ifadesinin tanımı yapılmamıştır. Ancak KVKK m. 3’te kişisel verilerin işlenmesi kavramının, kişisel verilerin kaydedilmesini de kapsayan bir işlem olduğu belirtilmiştir. İlgili düzenlemede “*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*” (KVKK m. 3/1-e) ifadeleriyle kişisel verilerin işlenmesi tanımlanmıştır. Bu tanımdan yola çıkarak KVKK kapsamında kişisel verilerin kaydedilmesinden bahsedilebilmesi için verilerin, “tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla” kaydedilmesi gerektiğini söyleyebiliriz. Ancak TCK m. 135’in kapsamı bu kadar dar değildir. Bir veri kayıt sisteminin parçası olmasa da otomatik olmayan yollarla kaydedilen kişisel veriler de, bu madde kapsamında suç oluşturacaktır¹⁹⁹. Bu durumda TCK m. 135 açısından kaydetmek fiilini kişisel verilerin herhangi bir yöntemle, daha sonra kullanmak amacıyla hazır edilmesi, depolanması şeklinde tanımlayabiliriz. Kaydetme fiili kağıt üzerine kaydetme olabileceği gibi elektronik ortama kaydetme şeklinde de olabilir²⁰⁰. Doktrinde verilerin ezberlenmesinin ya da kağıt üzerine yazılmasının kaydetmek olarak kabul edilemeyeceğini savunan görüş de mevcuttur²⁰¹. Bu görüşün, verilerin ezberlenmesi suretiyle kaydedilmesinin bu kapsamda olmadığı yönündeki fikrine katılmaktayız. Ancak kağıt üzerine yazılan bilginin daha sonra da kullanılabilmesi mümkün olduğundan bunun TCK m. 135 kapsamında kaydetmek fiilini oluşturacağı kanaatindeyiz. Nitekim söz konusu maddenin gerekçesinde de “kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayrım” yapılmadığı belirtilmiştir²⁰².

¹⁹⁸ <http://sozluk.gov.tr/>, (08.08.2019).

¹⁹⁹ Kangal, a.g.e., s. 65.

²⁰⁰ Yokuş Sevik, a.g.e., s. 244.

²⁰¹ Özbek vd., a.g.e., s. 587.

²⁰² Ankara HBV Üniversitesi Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, a.g.e., s. 340.

(5) Nitelikli unsurlar

Maddenin ikinci fıkrasında özel nitelikli kişisel verilerin kaydedilmesi durumunda cezanın artırılacağı düzenlenmiştir. Kişilerin “siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına” ilişkin verilerin kaydedilmesi suçun nitelikli halini oluşturur ve bu durumda suçun temel haline göre verilecek ceza yarı oranında artırılacaktır.

KVKK m. 6/1’de “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 mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri” özel nitelikli veri olarak sayıldığı halde TCK’da bu kadar kapsamlı bir düzenleme yapılmamıştır. Bu sebeple KVKK’da sayılıp TCK’da sayılmamış olan özel nitelikli kişisel veriler bakımından TCK m. 135/2’nin uygulanması mümkün olmayacaktır²⁰³.

Bu sebeple TCK m. 135/2’de yer almayan ancak hassas veri niteliğine sahip olan bu veriler, TCK kapsamında hassas verilere sağlanan korumadan yararlanamayacaktır. Örneğin biyometrik ve genetik veriler, TCK kapsamında hassas veri sayılmadığından bu verilerin kaydedilmesi durumunda faile ağırlaştırılmış ceza verilemeyecektir. Hassas verilerin daha özel korumayı gerektiren veri çeşidi olmasına rağmen, bu verilerin bir kısmına ceza kanunu tarafından gereken korumanın sağlanamaması kişilerin mağduriyetlerine sebep olabilecek bir durumdur. Bu sebeple de, TCK kapsamındaki hassas verilerin KVKK ile uyumlu olacak şekilde yeniden düzenlenmesinin daha uygun olacağı kanaatindeyiz²⁰⁴.

Kişisel verilerin kaydedilmesi suçu bakımından nitelikli unsurlar yalnızca TCK m. 135’te yer almamaktadır. “Nitelikli haller” başlıklı TCK m. 137 de bu suç bakımından uygulanacak nitelikli unsurları düzenlemiştir. “Suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle” işlenmesi maddede sayılan nitelikli hallerden biridir. TCK m. 6’da kamu görevlisi, “*kamusal faaliyetin yürütülmesine atama*

²⁰³ Korkmaz, a.g.e., s. 284; Özbek vd., a.g.e., s. 592.

²⁰⁴ Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 68; Sinem Göçmen Uyarer, *Kişisel Verilerin Korunması*, 1. b., Ankara: Seçkin Yayıncılık, 2019, s. 175-176.

veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi” olarak tanımlanmıştır. Ancak maddeye bakıldığında kamu görevlisi olmasının nitelikli halin oluşması için tek başına yeterli olmadığı görülecektir. Kişinin kamu görevlisi olmasının yanında suçu görevinin verdiği yetkiyi kötüye kullanmak suretiyle işlemiş olması da gerekmektedir. Yetkinin kötüye kullanılması arandığına göre kamu görevlisinin bu konuda bir yetkisinin olması gerektiği de açıktır²⁰⁵. Ancak bu halin oluştuğundan bahsedilebilmesi için suçun, kamu görevlisinin görevi sırasında işlenmiş olması şart değildir. Kişinin kamu görevlisi olması ve bu görevini kötüye kullanarak suç işlemiş olması yeterlidir²⁰⁶.

TCK m. 137’de yer alan diğer nitelikli hal ise bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle suçun işlenmesidir. Meslek, sözlükte “*Belli bir eğitim ile kazanılan, sistemli bilgi ve becerilere dayalı, insanlara yararlı mal üretmek, hizmet vermek ve karşılığında para kazanmak için yapılan, kuralları belirlenmiş iş, uğraş, öğretimi, dizge, çığır, okul, ekol*” şeklinde tanımlanmıştır. Sanat ise “*Bir duygu, tasarı, güzellik vb.nin anlatımında kullanılan yöntemlerin tamamı veya bu anlatım sonucunda ortaya çıkan üstün yaratıcılık, bir şey yapmada gösterilen ustalık, bir meslekte uyulması gereken kuralların tümü, zanaat*” şeklinde tanımlara sahiptir²⁰⁷.

Kanun belli bir meslek veya sanattan bahsetmiş, ama hangi meslek ya da sanat olduğunu belirtmemiştir. Bu durumda kişisel verilerin kaydedilmesi konusunda kolaylık sağlama imkanı bulunan her meslek ve sanat bu maddenin kapsamında değerlendirilebilir. Örneğin hastanelerde ya da bankalarda çalışan kişiler, kişisel verilere erişim kolaylıkları olması sebebiyle bu kanun kapsamına girebilecek meslek gruplarındandır²⁰⁸.

c. Suçun manevi unsuru

Bu suçun manevi unsuru kasttır. Kanun koyucu suçun işlenmesi için özel bir amaç ve saik aramadığından doğrudan kasta tabi bir suçtur. Failin, kişisel verileri kaydetme

²⁰⁵ Mustafa Artuç, *Kişilere Karşı Suçlar*, 2. b., Ankara: Adalet Yayınevi, 2018, s. 1633.

²⁰⁶ Özbek vd., a.g.e., s. 589.

²⁰⁷ <http://sozluk.gov.tr/>

²⁰⁸ Özbek vd., a.g.e., s. 591.

faaliyetini bilerek ve isteyerek gerçekleştirmesi suçun oluşması için aranmaktadır. Bunun yanında, kanunda “hukuka aykırı olarak” ifadesinin yer aldığı durumlarda, hukuka aykırılığa özellikle işaret edildiği, bunun tipikliğe ait bir unsur olduğu, bu sebeple failin, fiilin hukuka aykırı olduğunu bilmesi gerektiği ve bu tür suçların ancak doğrudan kastla işlenebileceği, olası kastın mümkün olmayacağı yönünde görüşler mevcuttur²⁰⁹. Bizim de katıldığımız bir başka görüşe göre ise, hukuka aykırılık ifadesi suçun maddi unsurlarından birini nitelendiriyorsa, bu durumda hukuka aykırılık tipikliğe dahil bir unsurdur ve bu durumda suçun işlenmesi ancak doğrudan kastla mümkün olabilecektir. Örneğin, TCK m. 244/4’te “*kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlama*” ifadesi yer almaktadır. Burada “haksız” kelimesi “çıkara sağlama” fiiline ilişkin bir özellik olduğundan, failin haksız olarak çıkar sağladığını bilmesi gerekmektedir. Dolayısıyla bu suç ancak doğrudan kastla işlenebilecektir. Ancak hukuka aykırılık ifadesi, suçun genel değerlendirmesi ile ilgiliyse, bunun tipiklik ve kastla ilgili olmadığı, kanun koyucunun, hakimi bir hukuka uygunluk nedeninin varlığı konusunda uyarmak amacıyla kanuna eklenmiş bir ifade olduğu görüşü savunulmaktadır²¹⁰. Bu durumda hukuka aykırılık konusunda doğrudan kastla hareket etme şartı aranmayacağından bu tip suçlar olası kastla da işlenebilecektir. Öyleyse TCK m. 135’te yer alan “*hukuka aykırı olarak*” ifadesi, suçun genel değerlendirmesine ilişkin olduğundan, kişisel verilerin kaydedilmesi suçunun olası kastla işlenmesi de mümkündür.

TCK m. 22’ye göre “taksirle işlenen fiiller, kanunun açıkça belirttiği hallerde” cezalandırılabilir. Suçlarda taksir istisnai bir haldir ve kanunda suçun taksirli halinin cezalandırılabilirliğine ilişkin düzenleme olması gerekmektedir. Bu suçun taksirli hali kanunda düzenlenmediğinden, taksir ile işlenmesi söz konusu olmayacaktır.

TCK m. 30/1’e göre “*Fiilin icrası sırasında suçun kanuni tanımındaki maddi unsurları bilmeyen bir kimse, kasten hareket etmiş olmaz. Bu hata dolayısıyla taksirli sorumluluk hali saklıdır*”. Bu durumda kişisel verilerin kaydedilmesi sırasında maddi hataya düşülmesi durumunda kasttan söz etmek mümkün olmayacaktır. Bu suçun taksirli

²⁰⁹ Mehmet Emin Artuk, Ahmet Gökçen, Ahmet Caner Yenidünya, *Ceza Hukuku Genel Hükümler*, 7. b., Ankara: Adalet Yayınevi, 2013, s. 372-373; Veli Özer Özbek vd., *Türk Ceza Hukuku Genel Hükümler*, 9. b., Ankara: Seçkin Yayıncılık, 2018 s. 278; Özgenç, a.g.e., s. 312.

²¹⁰ Mahmut Koca, İlhan Üzülmöz, *Türk Ceza Hukuku Genel Hükümler*, 11. b., Ankara: Seçkin Yayıncılık, 2018, s. 268-269; Neslihan Göktürk, “Suçun Yasal Tanımında Yer Alan “Hukuka Aykırılık” İfadesinin İcra Ettiği Fonksiyon”, *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, C. 7, S. 1 (2016), s. 427-428.

hali de kanunda düzenlenmediğinden fail kişisel verilerin kaydedilmesi suçundan sorumlu olmayacaktır. Örneğin, kişi kendi verilerini kaydettiğini düşünürken başkasına ait verileri kaydederse, suçun maddi unsurlarında hata meydana geldiğinden kişinin kastı ortadan kalkacaktır²¹¹.

Kişinin hatasının kastını kaldırdığından söz edilebilmesi için bu hataya düşmeseydi fiilinin suç oluşturmayacağı kabulü gereklidir. Yani kişinin hatası olmasaydı da fiil suç oluşturacaksa bu durumda hatanın kastı kaldırdığından söz edilemeyecek ve fail işlediği suç dolayısıyla sorumlu olacaktır. Örneğin fail A'nın kişisel verilerini kaydetmek isterken hatası sebebiyle B'nin kişisel verilerini kaydederse mağdurun kimliğinde hataya düşmesi sebebiyle cezai sorumluluğunda bir değişiklik olmayacaktır²¹².

Fail suçun nitelikli unsurlarında da hataya düşebilir. Böyle bir hataya düşmesi durumunda hatasından yararlanır (TCK m. 30/2). Kişisel verilerin kaydedilmesi suçunu işleyen fail TCK m. 135/2 kapsamında olmayan bir veriyi kaydettiğini düşünürken hata ile TCK m. 135/2'de sayılan ve nitelikli hali oluşturan verilerden birini kaydederse hatasından yararlanacaktır. Yani kaydettiği verilerin TCK m. 135/2 kapsamında olduğunu bilmiyorsa faile suçun nitelikli halinden değil temel halinden ceza verilecektir²¹³.

2. Hukuka Aykırılık Unsuru

Yukarıda, madde metninde yer alan “hukuka aykırı olarak” ifadesinin işlevinden bahsetmiştik. Bu açıklamalara göre, TCK m. 135'te yer alan bu ifadenin tipiklik ile ilgili olmadığını belirtmiştik. Hukuka aykırı olarak ifadesi, suçun hukuka aykırılık unsuru ile ilişkilendirilebilir. Burada kanun koyucu, olayda bir hukuka uygunluk nedeni olabileceği konusunda hakimi uyarmak amacıyla bu ifadeye yer vermiştir. Bu durumda tipikliğin

²¹¹ İzzet Özgenç, İlhan Üzülmez, *Ceza Genel Hukuku*, 2. b., Ankara: Seçkin Yayıncılık, 2019, s.104; Artuk, Gökçen, Yenidünya, a.g.e., s. 522; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 71.

²¹² Özgenç, Üzülmez, a.g.e., s. 104-105; Artuk, Gökçen, Yenidünya, a.g.e., s. 523; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 72.

²¹³ Özgenç, Üzülmez, a.g.e., s. 105; Artuk, Gökçen, Yenidünya, a.g.e., s. 524-525; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 72.

gerçekleşmesi hukuka aykırılık konusunda bir karine oluşturmayacak ve hakim olayda bir hukuka uygunluk nedeni bulunup bulunmadığını araştıracaktır²¹⁴.

Kişisel verilerin kaydedilmesi suçu bakımından söz konusu olabilecek hukuka uygunluk nedenlerinden biri kanun hükmünü yerine getirmedir. TCK m. 24/1’de bu durum, “*kanunun hükmünü yerine getiren kimseye ceza verilmez*” şeklinde ifade edilmiştir. KVKK m. 5/2-a’da da kanunlarda açıkça öngörülen durumlarda kişisel verilerin işlenmesinin mümkün olduğu belirtilmiştir. Hassas verilere ilişkin olarak ise; sağlık ve cinsel hayat dışındaki kişisel verilerin, kanunlarda öngörülmesi halinde işlenebileceği belirtilmiştir (KVKK m. 6/3).

Mevzuatımızda yer alan pek çok kanunda kişisel verilerin işlenmesi ya da kaydedilmesi ile ilgili düzenlemeler yer almaktadır. Bu kanunlara uygun olarak kişisel verilerin kaydedilmesi durumunda fiil hukuka uygun hale gelecek ve suç oluşmayacaktır. Örneğin CMK’nın “Şüpheli veya sanığın beden muayenesi ve vücudundan örnek alınması” başlıklı 75. maddesi şüpheli veya sanığa ait kişisel verilerin kaydedilmesine olanak sağlamaktadır. Ancak bu kanunla öngörülen bir işlem olması sebebiyle bu kapsamda kişisel verilerin kaydedilmesi hukuka uygun olacaktır. 2559 sayılı Polis Vazife ve Salahiyet Kanunu’nda yer alan kişilerin parmak izi ve fotoğraflarının kaydedileceğine ilişkin hüküm (PVSK m. 5), Adli Sicil Kanunu’nda yer alan kişilere ait adli sicil bilgilerinin kayıt altında tutulacağına ilişkin hüküm (Adli Sicil Kanunu m. 2) de bu hususa örnek oluşturmaktadır²¹⁵.

Kişisel verilerin kaydedilmesi suçu için, meşru savunmanın (TCK m. 25/1) hukuka uygunluk nedeni olarak uygulanmasının mümkün olup olmadığı konusunda görüş ayrılığı mevcuttur. Meşru savunmanın mümkün olabileceği yönündeki görüşe göre, kişinin kendisine ya da bir başkasına yönelik; tehdit, hakaret ya da şantaj gibi bir saldırı gerçekleşmekte ya da gerçekleşmesi muhakkak ise, saldırganın kişisel verilerinin kaydedilmesi durumu meşru savunma kapsamında değerlendirilmelidir²¹⁶. Diğer görüşe göre ise, bu tip suçlar ani hareketli suçlar olduğundan, herhangi bir savunma hareketi ile

²¹⁴ Göktürk, a.g.m., s. 432.

²¹⁵ Sert, a.g.e, s. 117-118; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 74.

²¹⁶ Yavuz Erdoğan, “Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi (Madde 135, 136, 137, 138), *Erciyes Üniversitesi Hukuk Fakültesi Dergisi*, C.VIII, S.2 (2013), s.599.

bu suçlardan kaçınmak mümkün değildir. İlgili suçların oluşması için gereken hareketler yapıldığı anda suç tamamlanacağından, meşru savunma için aranan mevcut saldırı şartı da gerçekleşmemiş olacaktır. Ayrıca yetkili makamlara delil olarak sunulması amacıyla kişisel verilerin kaydedilmesi, saldırıya karşı bir savunma hareketi olarak da görülmemektedir. Bu noktada ilgili görüşe biz de katılmaktayız. Nitekim, saldırganın fotoğrafı çekilerek ya da benzeri şekilde gerçekleştirilecek kişisel verilerin kaydedilmesi fiili, saldırıdan kurtulmayı sağlayacak nitelikte olmadığı gibi, saldırıdan kurtulma amacından çok delil elde etme amacını taşımaktadır. Bu sebeple, kişisel verilerin kaydedilmesi suçu bakımından, meşru savunma halinin uygulanmasının mümkün olabileceği bir durumun oluşması tarafımızca olasılık dışı görülüyor olsa da, kanunda yer alan şartların sağlanması durumunda, bu suç için de meşru savunma halinin uygulama alanı bulması mümkün olabilecektir²¹⁷.

Hakkın kullanılması da bu suç için hukuka uygunluk nedeni oluşturabilecektir. TCK m. 26/1’de “*hakkını kullanan kimseye ceza verilmez*” denilerek bu hukuka uygunluk hali düzenlenmiştir. KVKK m. 5/2-e’de de “*bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması*” durumunda kişisel verilerin işlenmesinin hukuka uygun olacağı düzenlenmiştir. Örneğin, basının haber verme hakkı kapsamında gazetecilik mesleğinin icrası sırasında kişisel verileri kaydeden kişilerin ya da tıbbi müdahale için gerekli olması sebebiyle kişilere ait verileri kaydeden hekimlerin fiilleri hakkın kullanılması kapsamında değerlendirilebileceğinden suç oluşturmayacaktır²¹⁸.

TCK m. 26/2’de ilgilinin rızası ile ilgili “*kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez*” ifadesi yer almaktadır²¹⁹. Aynı şekilde KVKK m. 5/1’de

²¹⁷ Mustafa Özen, “Kişisel Verilerin Kaydedilmesi, Verilmesi veya Ele Geçirilmesi ve Yok Edilmemesi Suçları (TCK m. 136, 137, 138)”, *Kamu Hukuku Arşivi*, C.12, S.1 (2009), s. 17; Köse Aysun, a.g.e., s. 164; Aydın, a.g.e., s. 159; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 75.

²¹⁸ Sert, a.g.e., s. 118; Artuk, Gökçen, *Yenidünya*, a.g.e., s. 413-417.

²¹⁹ “*Sanık ... ile hakkındaki hükmün açıklanması geri bırakılan sanık ...'e ait ortak işyerinde, üçüncü kişilere ait çok sayıda nüfus cüzdanı fotokopisinin hukuka aykırı olarak saklandığı iddiasıyla ilgili olarak mahkemece kişisel verilerin hukuka aykırı olarak kaydedilmesi suçundan sanık ... hakkında mahkumiyet hükmü kurulmuş ise de; TCK'nın 135. maddesinde düzenlenen “Kişisel Verilerin Kaydedilmesi” suçunun konusunu oluşturan kişisel veri kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya 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, belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesi gerektiği gözetildiğinde; üçüncü kişilere ait nüfus cüzdanı*”

kişisel verilerin “ilgili kişinin açık rızası olmaksızın” işlenemeyeceği belirtilmiş, KVKK m. 6/2’de ise “özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın” işlenmesinin yasak olduğu ifade edilmiştir. Benzer şekilde TCK m. 135’in gerekçesinde de “kişinin rızası ile kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı” ifade edilmiştir²²⁰. Bu durumda kişinin rızasının bu suç için hukuka uygunluk nedeni oluşturacağı açıktır. Ancak rızanın “açık rıza” olması önem taşımaktadır.

Açık rıza KVKK’da tanımlanmıştır. Buna göre “*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*” (KVKK m. 3/1-a) açık rızadır. Açık rıza ve şartlarına ilişkin detaylı açıklamaya önceki bölümlerde yer verildiğinden bu bölümde detaylı açıklamaya yer verilmeyecek, açık rızaya ilişkin kısa açıklamalarla yetinilecektir.

Kanundaki tanımdan da anlaşılacağı gibi, veri sahibinin rızasının açık rıza olduğunun kabulü için; “rızanın belirli bir konuya ilişkin verilmesi”, “rızanın bilgilendirmeye dayalı olması” ve “rızanın özgür iradeyle açıklanmış olması” gerekmektedir. Sayılan üç şartın dışında, rızanın yazılı şekilde alınması zorunlu değildir. Elektronik ortam ve çağrı merkezi gibi yöntemlerle de açık rıza alınması mümkündür. Açık rızanın alındığı konusunda ispat yükü veri sorumlusundadır²²¹.

Bunun yanında kişisel verilerin kaydedilmesi suçu açısından varsayılan rıza da hukuka uygunluk nedeni olarak ortaya çıkabilecektir. KVKK m. 5/2’ye göre “*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*” durumunda kişisel veriler işlenebilecektir ve bu sebeple bu fiil dolayısıyla faile ceza verilmeyecektir. Bu durumda, verileri işlenen kişinin bir rıza açıklaması bulunmaması sebebiyle, kanunda yer alan bir suç işlenmektedir. Ancak burada, veri sahibine sorulsaydı bu duruma rıza göstereceği kabul

fotokopilerinin, bu kişilerin rızaları dışında hukuka aykırı olarak ele geçirilip sanığın işyerinde bulundurulduğuna dair bir iddia bulunmadığı gibi, nüfus cüzdanı sahiplerinin ifadelerinde kendi rızaları ile birtakım hukuki işlemler nedeniyle nüfus cüzdanlarını verdiklerini beyan etmeleri karşısında sanık...’in, unsurları oluşmayan hukuka aykırı olarak kişisel verileri kaydetmek suçundan beraati yerine mahkumiyetine karar verilmesi...” (5. CD., 21.06.2018, E. 2014/10479, K. 2018/4622, www.kazanci.com, (29.11.2019)).

²²⁰ Ankara HBV Üniversitesi Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, a.g.e., s. 340.

²²¹ Kişisel Verileri Koruma Kurumu, *Açık Rıza*, s. 1-3.

edilmekte ve kişisel verilerin kaydedilmesi fiili hukuka uygun hale gelmektedir²²². Ancak bu durum KVKK'nın 6. maddesinde sayılmadığından, özel nitelikli kişisel verileri açısından söz konusu olmayacaktır²²³.

KVKK m. 5/2'deki kişisel verilerin işlenmesinin hukuka uygun olacağı durumlar sayılmıştır. Sayılan bu koşulların bulunması durumunda veri sahibinin açık rızası olmasa da verilerin işlenmesi hukuka uygun hale gelecektir. Bu durumlara ilişkin detaylı açıklama da önceki bölümlerde yer aldığından, tekrara düşmemek adına burada detaylı açıklama yapılmayacaktır. Ancak bu haller özel nitelikli kişisel veriler için geçerli değildir. Özel nitelikli kişisel verilerin kişinin açık rızası olmadan da hukuka uygun olarak işlenebilmesi için gereken şartlar KVKK 6. maddede sayılmıştır. Buna göre, “sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir” denilerek hassas kişisel verilerin işlenmesinin hukuka uygun olacağı durumlar sayılmıştır. Kişisel verilerin işlenmesi kavramının kapsamına yukarıdaki bölümlerde değinmiştik. Buna göre kişisel verilerin kaydedilmesi de işlenmesi kapsamında yer aldığından kanunda sayılan hallerde kişisel verilerin kaydedilmesi de hukuka uygun olacaktır.

D. KUSUR

TCK m. 135'te yer alan “hukuka aykırı olarak” ifadesi haksızlık yanılığı konusu açısından önemlidir. Haksızlık yanılığı, kusurluluğu etkileyen bir hata halidir. Fail, kişisel verileri kaydederken, bu fiilin hukuka aykırı olduğu konusunda kesinlikle bilgi sahibi olmalıdır. Failin bu konuda bir şüpheye sahip olması onun haksızlık yanılığı içinde olmasına sebep olacaktır. Bu durumda da fail kusurlu sayılamayacaktır²²⁴.

²²² Zeynel T. Kangal, “Ceza Hukukunda Varsayılan Rıza”, *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, C. XV, S. 4 (2011), s. 224.

²²³ Korkmaz, a.g.e., s. 358.

²²⁴ Göktürk, a.g.m., s. 432-433.

Yetkili amirin emrini ifa (TCK m. 24/2) kişisel verilerin kaydedilmesi suçu bakımından kusurluluğu kaldıran bir sebep olarak ortaya çıkabilecektir. Ancak kusurun olmadığı kabulü için; “emrin yetkili bir merci tarafından verilmesi (TCK m. 24/2), görev dolayısıyla yerine getirilmesi zorunlu bir görev olması (TCK m. 24/2) ve konusu suç teşkil etmeyen bir emir olması (TCK m. 24/3)” gerekmektedir. Bu şartlar altında verilen emir gereğince kişisel verileri kaydeden kişiye ceza verilmeyecektir.

TCK m. 25/2’de zorunluluk hali düzenlenmiştir. Bu düzenleme, “*gerek kendisine gerek başkasına ait bir hakka yönelik olup, bilerek neden olmadığı ve başka suretle korunmak olanağı bulunmayan ağır ve muhakkak bir tehlikeden kurtulmak veya başkasını kurtarmak zorunluluğu ile ve tehlikenin ağırlığı ile konu ve kullanılan vasıta arasında orantı bulunmak koşulu ile işlenen fiillerden dolayı faile ceza verilmez*” şeklindedir. Buna göre, maddede belirtilen şartlar altında kişi, kendisinin ya da üçüncü bir kişinin hakkını korumak amacıyla kişisel verileri kaydedebilecektir. Ancak bu durumda kişinin kusursuz sayılabilmesi için; korunmak istenen hukuksal yararın, kişisel verileri koruma hakkından daha üstün ya da eşit öneme sahip bir yarar olması gerekmektedir²²⁵.

Bunun dışında kişi, kurtulma imkanı bulunmayan cebir ve şiddet ya da ağır tehdit altında kişisel verileri kaydetme suçunu işlerse, kişiye ceza verilmez. Bu durumda TCK m. 28’e göre cebir ya da tehdidi kullanan kişi dolaylı fail olarak sorumlu olur.

Kendisine karşı yapılan haksız fiilin etkisi altında, bu fiili gerçekleştiren kişiye karşı bu suçu işleyen fail hakkında verilecek ceza, TCK m. 29’a göre haksız tahrik altında bu suçu işlemiş olduğundan, indirilecektir.

Bunlar dışında, şartlarının varlığı halinde, kusurluluğu etkileyen diğer haller olan; yaş küçüklüğü, akıl hastalığı, sağır dilsizlik ve alkol ve uyuşturucu madde etkisinde olma halleri konusundaki genel hükümler, bu suç için de uygulanabilecektir.

²²⁵ Zeynel T. Kangal, *Ceza Hukukunda Zorunluluk Durumu*, 1. b., Ankara: Seçkin Yayıncılık, 2010, s. 30; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 76.

E. SUÇUN ÖZEL GÖRÜNÜM ŞEKİLLERİ

1. Teşebbüs

Kişisel verilerin kaydedilmesi suçu sırf hareket suçudur ve kaydetme hareketinin yapılması ile suç oluşur. Bu suç bakımından teşebbüs ancak icra hareketlerinin bölünebildiği durumda söz konusu olabilecektir. Örneğin fail, mağdura ait kişisel verileri kaydedecekken bir sebeple bu işlemi gerçekleştirememesi durumunda suç teşebbüs aşamasında kalmış olacaktır²²⁶.

Kişisel veriler ele geçirildiği halde kaydedilememişse, bu durumda TCK m. 136'da yer alan kişisel verileri hukuka aykırı olarak ele geçirme suçu oluşacağından, burada teşebbüsten söz etmek mümkün olmayacaktır²²⁷.

2. İştirak

Kişisel verilerin kaydedilmesi suçu iştirak açısından herhangi bir özellik göstermemektedir. TCK'da iştirak ile ilgili 34-41. maddelerde düzenlenen genel hükümler bu suç bakımından da uygulanacaktır.

TCK m. 137 hükmü gereğince, bu maddede sayılan kişilerin suça iştirak etmesi halinde ise bu kişiler bakımından ceza artırılabilecektir²²⁸. TCK m. 137'de aranan niteliğe sahip kişi ile birlikte, bu niteliğe sahip olmayan bir kişinin suçu birlikte işlemesi durumunda ise, nitelikli hal yalnızca aranan niteliğe sahip kişi bakımından uygulanacaktır. Aranan özelliklere sahip olmayan kişi ise suçun temel şeklinden fail olarak cezalandırılacaktır²²⁹.

²²⁶ Yokuş Sevik, a.g.e., s. 248.

²²⁷ Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 595.

²²⁸ Kuşkonmaz, a.g.e., s. 148.

²²⁹ Berrin Akbulut, "Bağlılık Kuralı", *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, C. XIV, S. 1 (2010), s. 186; Mahmut Koca, İlhan Üzülmöz, "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, C. 21, Özel Sayı (2019), s. 90.

3. İçtima

Kişisel verilerin kaydedilmesi suçu, bir suç işleme kararı kapsamında aynı kişiye karşı birden fazla kez işlenebilir. Bu durumda TCK m.43'te yer alan zincirleme suç hükümleri uygulanacak ve ceza, dörtte birinden dörtte üçüne kadar artırılacaktır. Bunun yanında fail birden fazla kişiye ait kişisel verileri tek bir fiille de kaydedebilir. Bu durumda aynı neviden fikri içtima söz konusu olacak ve ceza zincirleme suç hükümlerine göre belirlenecektir.

TCK m. 133'te yer alan "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçunda "kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi"den bahsedilmektedir. Bu suç işlenirken konuşmaların kaydedilmesiyle beraber kişisel verilerin de kaydedilmesi durumunda, kişisel veri kavramı "kimliği belirli ya da belirlenebilir kişiye ilişkin her türlü veri"yi kapsarken, TCK m. 133'te her türlü verinin değil, kişiler arasındaki aleni olmayan konuşmaların kaydedilmesinden söz edildiğinden, TCK m. 133'te yer alan düzenleme, kişisel verilerin kaydedilmesi suçuna göre özel norm olduğundan, TCK m. 133 hükmü uygulanacaktır.

"Haberleşmenin gizliliğini ihlal" başlıklı TCK m. 132'de ise "gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle" ifadesi yer almaktadır. Belirtilen suç işlenirken, kişisel veri niteliğine sahip verilerin de kaydedilmesi durumunda, yukarıdaki açıklamalar ışığında, TCK m. 132 yalnızca haberleşme içeriklerini kapsadığından, özel normdur. Bu sebeple bu durumda TCK m. 132 uygulama alanı bulacaktır.

Farklı neviden fikri içtima da bu suç için söz konusu olabilecektir. TCK m. 134'te yer alan "özel hayatın gizliliğini ihlal" suçu işlenirken, kişinin özel hayatı dışında kalan kişisel verilerinin kaydedilmesi durumunda, farklı neviden fikri içtima hükümleri uygulanacaktır. TCK m. 244'te yer alan "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" suçu işlenirken de kişisel veri niteliğine sahip bilgilerin kaydedilmesi durumunda da farklı neviden fikri içtima ortaya çıkacaktır.

TCK m. 239'da yer alan "ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması" suçu ile kişisel verilerin kaydedilmesi suçu arasında da fikri içtima uygulanabilecektir. Müşteri sırrı niteliğindeki kişisel veriyi herkesin

erişebileceği bir internet sitesine kaydeden fail aynı hareketle hem bir kişisel veriyi kaydetmiş hem de müşteri sırrı niteliğindeki bilgiyi ifşa etmiş olduğundan TCK m. 239 ve TCK m. 135 arasında farklı neviden fikri içtima hükümleri uygulanacaktır.

Ayrıca şartlarının olması durumunda TCK m. 136'da yer alan "kişisel verileri hukuka aykırı olarak verme veya ele geçirme" suçu ile 135. madde arasında da farklı neviden fikri içtima hükümlerinin uygulanması da mümkündür. Bu durumda TCK m. 44'e göre, fail, en ağır cezayı gerektiren suçtan dolayı cezalandırılacaktır²³⁰.

Kişisel verilerin kaydedilmesi suçu için gerçek içtimanın uygulanabilmesi de mümkündür. Kişinin cebir veya tehdit yoluyla kişisel verileri kaydetmeye mecbur bırakılması durumunda, cebir (TCK m. 108) veya tehdit (TCK m. 106) uygulayan kişi hem bu suçlardan hem de kişisel verilerin kaydedilmesi suçundan ayrı ayrı cezalandırılacaktır²³¹.

F. YAPTIRIM

Kişisel verilerin kaydedilmesi suçu için kanun hapis cezası öngörmüştür. Suçun temel şekli olan hukuka aykırı olarak kişisel verilerin kaydedilmesi durumunda suçu işleyen kişiye "bir yıldan üç yıla kadar hapis cezası" verilecektir. İkinci fıkrada yer alan özel nitelikli verilerin kaydedilmesi durumunda ise suçun nitelikli hali oluşacak ve verilecek ceza suçun temel haline göre yarı oranında artırılabilecektir. Ayrıca 137. maddeye göre, "kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle" ya da "belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" suçun işlenmesi durumunda verilecek ceza yarı oranında artırılabilecektir.

Suç için bir yıldan üç yıla kadar hapis cezası öngörüldüğünden hapis cezasının ertelenmesi ya da sanık hakkında hükmün açıklanmasının geri bırakılması mümkün olabilecektir. TCK m. 51 uyarınca, maddede aranan şartların varlığı halinde, "işlediği suçtan dolayı iki yıl veya daha az süreyle hapis cezasına mahkûm edilen kişinin cezası ertelenebilir". Aynı şekilde CMK m. 231'e göre kişiye verilen ceza "iki yıl veya daha az süreli hapis veya adli para cezası ise; mahkemece, hükmün açıklanmasının geri

²³⁰ Korkmaz, a.g.e., s. 366-369.

²³¹ Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 86.

bırakılmasına karar verilebilir”. Bu kararın verilebilmesi için aynı maddede sayılan şartların da varlığı aranacaktır.

Kasten işledikleri suç dolayısıyla hapis cezasına mahkûm edilen kişilerin belli haklardan yoksun bırakılmaları da söz konusudur. Bu suç dolayısıyla kişiye hapis cezası verilmesi durumunda, kişi hakkında TCK m. 53’te yer alan hak yoksunlukları uygulanacaktır.

TCK’nın 140. maddesinde ise tüzel kişilere yönelik yaptırıma ilişkin düzenleme yer almaktadır. Maddeye göre bu suçun “işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur”. Tüzel kişiler hakkında güvenlik tedbirlerine ilişkin düzenleme ise TCK m. 60’ta yer almaktadır.

Suç, 5 yıldan fazla cezayı gerektirmediği için TCK m. 66/1’e göre dava zamanaşımı sekiz yıldır. TCK m. 68/1’e göre ceza zamanaşımı ise on yıldır.

G. MUHAKEMEYE İLİŞKİN KURALLAR

TCK m. 139’da “*Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikayete bağlıdır.*” hükmü yer almaktadır. Madde metninden anlaşılacağı gibi bu suçun soruşturma ve kovuşturulması şikayete bağlı olmadığından, resen yapılacaktır²³². Ayrıca suçun kamu görevlisi tarafından görevi dolayısıyla işlenmesi halinde 4483 sayılı “Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun”a göre soruşturma yapılabilmesi için yetkili makamdan izin alınması gerekmektedir.

CMK m. 253’te uzlaştırma hükümlerinin uygulanacağı suçlar sayılmıştır. Kişisel verilerin kaydedilmesi suçu için, gerek şikayete tabi olmaması gerekse de maddede sayılan diğer suçlar arasında yer almaması sebebiyle uzlaştırma yoluna gidilemeyecektir.

Suç için öngörülen cezanın üst sınırı göz önüne alındığında, 5235 sayılı “Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun”un 11. maddesine göre görevli mahkeme asliye ceza

²³² Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 596.

mahkemeleridir²³³. Yetkili mahkeme ise CMK m. 12/1'e göre belirlenecektir. Buna göre; "Davaya bakmak yetkisi, suçun işlendiği yer mahkemesine aittir". Suçun işlendiği yer belirlenemiyorsa CMK m. 13'te yer alan özel yetki kuralları uygulama alanı bulacaktır.

III. VERİLERİ HUKUKA AYKIRI OLARAK VERME VEYA ELE GEÇİRME SUÇU (TCK m. 136)

A. GENEL OLARAK

Verileri hukuka aykırı olarak verme veya ele geçirme suçu da 765 sayılı eski Türk Ceza Kanunu'nda düzenlenmemiş olup 5237 sayılı TCK'nın 136. maddesinde "(1) *Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır. (2) Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.*" şeklinde düzenlenmiştir. Madde ile öngörülen cezanın alt sınırı daha önce bir yılken, 21.2.2014 tarihli ve 6526 sayılı kanunun 4. maddesi ile iki yıl şeklinde değiştirilmiştir. Nitelikli hale ilişkin ikinci fıkra ise, çok kısa bir süre önce, 17.10.2019 tarihli ve 7188 sayılı Kanunun 17. maddesi ile TCK m. 136'ya dahil edilmiştir.

Maddenin gerekçesinde "*Bu madde hükmü ile, hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır.*"²³⁴ şeklinde bir ifade yer almaktadır. Görüldüğü gibi bu suçun oluşması bakımından kişisel verilerin hukuka uygun kaydedilmiş olup olmamasının önemi yoktur.

Günümüzde gelişen teknoloji ile kişilerin gerek kurum kuruluşlarla paylaştıkları bilgiler gerekse de elektronik ortamlarda kullandıkları bilgiler başkaları ile paylaşılabilen ve satılabilmektedir. Artık günümüzde kişiler, çok basit işlemleri yapabilmek için bile kişisel verilerini vermek zorunda kalabilmektedir. Bu durumda da

²³³ a.g.e.

²³⁴ Ankara HBV Üniversitesi Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, a.g.e., s. 341.

bu verilerin üçüncü kişiler ile paylaşılmasının önlenmesi büyük önem arz etmektedir. Kişisel veriler, üçüncü kişilerle paylaşılmasa bile teknolojik gelişmelerle paralel olarak bu verilerin ele geçirilebilmesi riski de artmıştır. Bu madde, bu gibi olumsuz fiillerin cezalandırılması amacıyla düzenlenmiştir²³⁵. Bu madde ile düzenlenen suçun bazı ülkelerdeki kimlik hırsızlığı fiiline karşılık geldiği de söylenebilir²³⁶.

Madde başlığında “kişisel veriler” yerine “veriler” ifadesine yer verilmiş olması ise bu madde ile ilgili eleştirilen bir husustur. Veri kavramının kapsadığı alan kişisel veri kavramından çok daha fazladır. Maddede ise, veri olarak ifade edilen kavramla kastedilenin aslında kişisel veri olduğu çok açıktır. Bu sebeple maddenin başlığında yalnızca veri değil, kişisel veri ifadesinin yer alması gerektiği yönündeki eleştirilere katılmaktayız²³⁷.

Madde başlığı konusunda bir diğer eleştiri ise, başlıkta “yayma” ibaresine yer verilmemesi konusundadır. Gerçekten de madde içeriği verme, yayma veya ele geçirme şeklindeyken başlıkta yalnızca verme veya ele geçirme ifadesinin yer alması uygun bir düzenleme olmamıştır²³⁸.

TCK m. 136/1’de suçun temel şekline yer verilmiş, ikinci fıkrada ise CMK m. 236/5-6 kapsamında kaydedilen beyan ve görüntülerin verilmesi, yayılması ya da ele geçirilmesi durumunda, cezanın artırılmasını gerektiren nitelikli hale yer verilmiştir. TCK’nın 137. maddesinde ise, TCK m. 135’te olduğu gibi, suçu işleyen kişiler bakımından cezanın artırılmasını gerektiren nitelikli hallere yer verilmiştir.

B. KORUNAN HUKUKSAL DEĞER

Bu suç ile korunan hukuksal değer kişisel verilerin kaydedilmesi ile aynı şekilde Anayasa’nın 20. maddesi ile güvence altına alınmış olan kişisel verilerin korunması hakkıdır. Kişisel verilerin korunması hakkı özel hayatın gizliliği hakkının kapsamında bir hak olduğu için genel olarak özel hayatın gizliliği hakkının korunduğu söylenebilirse de düzenleme ile asıl korunmak istenen hukuksal değer kişisel verilerin korunması

²³⁵ Gültekin, a.g.e., s. 160-161.

²³⁶ Dülger, a.g.e., s. 704.

²³⁷ Çokmutlu, a.g.e., s. 214.

²³⁸ Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 598.

hakkıdır²³⁹. Konu ile ilgili daha detaylı açıklama kişisel verilerin kaydedilmesi başlığı altında yapıldığından tekrara düşmemek adına bu bölümde detaylı açıklamaya yer verilmeyecektir.

C. SUÇUN UNSURLARI

Bu bölümde tipiklik ve hukuka aykırılık unsuru başlıkları altında verileri hukuka aykırı olarak verme veya ele geçirme suçunun unsurları incelenecektir.

1. Tipiklik

Tipiklik başlığı altında, kişisel verilerin kaydedilmesi başlığında olduğu gibi, suç tipinin genel özelliklerinden bahsedildikten sonra suçun maddi ve manevi unsurları konusunda açıklamalara yer verilecektir.

a. Suç tipinin genel özellikleri

Verileri hukuka aykırı olarak verme veya ele geçirme suçu TCK m. 136'da iki fıkra halinde düzenlenmiştir. Birinci fıkra da “*kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren*” kişiye verilecek ceza düzenlenmiştir. İkinci fıkra da ise “*Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda*” verilecek cezanın artırılacağına ilişkin düzenlemeye yer verilmiştir. Ayrıca kişisel verilerin kaydedilmesi suçu ile aynı şekilde, TCK m. 137'de düzenlenen suçun işlenmesi durumunda cezanın artırılmasına sebep olacak nitelikli haller bu suç için de söz konusudur.

Suçun oluşabilmesi için vermek, yaymak ya da ele geçirmek eylemlerinden birinin yapılması gerekli ve yeterli olduğundan suç seçimlik hareketli suçtur. Seçimlik

²³⁹ Yokuş Sevik, a.g.e., s. 249. “TCK'nun 136. maddesinde tıpkı 135. maddesinde olduğu gibi korunan hukuki değer genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özelde ise kişisel verilerdir.” (CGK, 17.06.2014, E. 2012/12-1510, K. 2014/331, www.kazanci.com, (28.11.2019)).

hareketlerden birinin gerçekleştirilmesi durumunda suç oluşmuş olacağından, bu suç sırf hareket suçu niteliğini taşımaktadır²⁴⁰.

Verileri hukuka aykırı olarak verme veya ele geçirme suçu ani suç niteliğine sahiptir. Özellikle suç verilerin ele geçirilmesi suretiyle işlendiğinde, ele geçirme dışında ayrıca bir süre depolama gibi bir şart aranmamaktadır. Ancak yayma fiili açısından mütemadi suç özelliği taşıması da mümkün olabilecektir. Örneğin bir kişi, fotoğrafının internet sitesinde paylaşılması konusunda bir başkasına rıza gösterdiğinde, kişinin rızası olduğu için suç oluşmayacaktır. Ancak daha sonra fikrini değiştirip fotoğrafın kaldırılmasını istemesi durumunda fotoğraf kaldırılmazsa, kaldırmayan kişi bu suç işlemiş olacaktır. Ancak bu durumda suç tamamlandığı halde kaldırılmadığı süre boyunca bitmiş olmayacaktır. Bu durumda da ani değil, mütemadi suç söz konusu olacaktır²⁴¹.

Yargıtay'ın bu doğrultuda

“Sanığın, bir karede mağdurun kendisini yanağından öptüğü, diğerlerinde kendisine sarıldığı ve her ikisinin üzerlerinde günlük kıyafetleri bulunduğu halde yan yana poz vererek çektikleri fotoğraflarını, mağdurun bilgisi dahilinde facebook hesabında yayımladıktan sonra, söz konusu fotoğrafları, mağdurla ayrılmasına ve mağdur tarafından kaldırılması istenilmesine rağmen yayımlamaya devam ettiği olayda;

İddiaya konu sanıkla mağdur arasındaki ilişkinin varlığını ve boyutunu gösteren fotoğrafların, daha önce mağdurun rızasına uygun olarak facebook adlı sosyal paylaşım sitesinde yayımlanmış olması karşısında, bu fotoğraflar, mağdurun özel yaşam alanına ilişkin ve özel hayatının gizliliğini ihlal edecek nitelikte görüntüler olarak kabul edilemeyeceğinden, sanığın, mağdura ait kişisel veri niteliğindeki fotoğrafları, mağdurun rızasına aykırı şekilde yayımlamaya devam etmesi biçiminde sübut bulan eyleminden dolayı TCK'nun 136/1. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet kararı verilmesi gerektiği”²⁴²

şeklinde bir kararı mevcuttur.

Suçun tamamlanması için maddede sayılan hareketlerden birinin gerçekleşmesi yeterli olup, ayrıca bir zarar doğması gerekmediğinden bir tehlike suçudur. Bunun yanında maddede hareketin somut bir tehlikeye sebep olması aranmadığından soyut tehlike suçudur²⁴³.

²⁴⁰ Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 598.

²⁴¹ Gültekin, a.g.e., s. 164.

²⁴² 12. CD., 13.09.2017, E. 2017/150, K. 2017/6231, www.kazanci.com, (29.11.2019).

²⁴³ Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 598.

Son olarak suç için maddede sayılan hareketlere bakıldığında suçun icrai bir hareketle işlenebilen suç olduğu görülmektedir. Ancak yaymak fiili konusunda yukarıda verilen örnek göz önüne alındığında, fotoğrafın kaldırılmaması ile suç işlenmiş olduğundan yayma fiili bakımından ihmali olarak da bu suçun işlenmesinin mümkün olduğu söylenebilir.

b. Suçun maddi unsurları

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi unsurları; fail, mağdur, suçun konusu, hareket ve nitelikli unsurlardan oluşmaktadır. Bu suç bakımından sayılan her bir unsur konusunda değerlendirme yapılarak suç tipi detaylı olarak incelenecektir.

(1) Fail

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun düzenlendiği maddede “*Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren*” kişiden söz edilmiştir. Fail için ayrıca bir özellik belirtilmediğinden, herkes bu suçun faili olabilecektir. Herkesin fail olması mümkün olmakla beraber; KVKK’nın uygulanması kapsamında bu suçun oluşması durumunda, KVKK kapsamında verilerin işlenmesi konusunda yetkili kişiler veri sorumlusu ve veri işleyen olduğundan bu kişiler fail olarak karşımıza çıkacaktır.

Suçun faili yalnızca gerçek kişiler olabilecektir. TCK m. 20/2 gereğince tüzel kişilerin fail olması mümkün değildir. Tüzel kişinin faaliyeti sonucu kişisel verilerin kaydedilmesi suçunun işlenmesi durumunda ise, bu fiili gerçekleştiren gerçek kişinin fail olması mümkündür. Tüzel kişiler hakkında ancak TCK m. 60’da yer alan güvenlik tedbirleri uygulanabilir²⁴⁴.

Ancak nitelikli hal konusunda TCK m. 137’de failin kamu görevlisi ya da belirli bir meslek ve sanatı yapan kimse olması aranmıştır. Bu durumda bu tanıma uymayan kişilerin suçu işlemesi nitelikli hal oluşturmayacaktır. Bir önceki suç tipinde de

²⁴⁴ Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 61.

değindiği gibi, suçun temel halinin herkes tarafından işlenebildiği ancak nitelikli halinin yalnızca kanunda sayılan kişilerce işlenebildiği suçlardan olması sebebiyle, bu suç da görünüşte özgü suçtur.

(2) Mağdur

Kanunda suçun mağduru için de özel bir düzenleme yer almadığından, herkes bu suçun mağduru olabilir. Ancak kişisel verilerin kaydedilmesi suçunda detaylı olarak açıklandığı üzere, tüzel kişiler suçun mağduru olamayacak, yalnızca gerçek kişiler suçun mağduru olabilecektir. Tüzel kişilerin ise suçtan zarar gören olabilmeleri mümkündür.

(3) Suçun konusu

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun konusunu “kişisel veriler” oluşturmaktadır. Kişisel verinin tanımı detaylı olarak geçmiş bölümlerde verildiğinden burada tekrar detaylı açıklamaya yer verilmeyecektir. Suç ile ilgili bir Yargıtay kararında ise bu suçun maddi konusunu oluşturan kişisel veri kavramı,

“...Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan “kişisel veri” kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir. Herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler de, yasal anlamda “kişisel veri” olarak kabul edilmekte ise de, anılan maddenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçların doğmaması için, maddenin uygulamasında, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması, olayda herhangi bir hukuk dalı tarafından kabul edilebilecek bir hukuka uygunluk nedeni veya bu kapsamda nazara alınabilecek bir hususun bulunup bulunmadığının saptanması ve sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerekir...”²⁴⁵

²⁴⁵ 12. CD., 07.02.2018, E. 2016/6071, K. 2018/1183, www.kazanci.com, (29.11.2019).

ifadeleriyle açıklanmıştır. Görüldüğü gibi kişisel veri, “kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilgi”dir. Ancak kişisel verinin kapsamı çok geniş olduğundan Yargıtay, suçun kapsamının amaçlanandan fazla genişlememesi, her eylemin suç oluşturmaması için somut olayın özelliklerine göre değerlendirme yapılması gerektiğini belirtmiştir. Örneğin yukarıdaki kararda, mağdur isminin rızası dışında sanığın internet sitesinde yer aldığını, bu sebeple verileri hukuka aykırı olarak verme veya ele geçirme suçunun işlendiğini iddia etmiştir. Mahkeme kararında, iki ismi olan mağdurun ilk ismi ile soyisminin sanığa ait internet sitesinin künyesinde yayın koordinatörü başlığı altında gösterilmiş olsa da bu ismin tamamen hayali olarak sanık tarafından oluşturulmuş olabileceği gibi, mağdurla aynı isim ve soyisime sahip başka kişiler de olabileceği gerekçesi ile somut olayda, bu bilgilerin kişisel veri niteliğine sahip olmadığını ve ilgili suçun oluşmadığını belirtmiştir. Görüldüğü gibi, kişinin adı ve soyadı kişisel veri niteliğinde bilgi olsa da, somut olayın özelliğine göre kişisel veri olarak değerlendirilmemesi de mümkün olabilmektedir. Bu sebeple kişisel verinin varlığı konusunda her olayın özellikleri incelenerek karar verilmesi yerinde bir karardır. Ancak burada, kişisel verilerin kaydedilmesi suçunun incelenmesi sırasında yapılan eleştirimizi yinelememiz gerekmektedir. Yargıtay, somut olayın gereklerine göre verinin, kişisel veri olup olmadığının tespitinin yapılması gerektiğini ifade etmiş olsa da, bu farklı uygulamaların ortaya çıkmasına, maddenin kapsamının çok geniş bir şekilde uygulanmasına kesin olarak bir engel değildir. Bu sebeple daha önce de belirttiğimiz gibi, TCK kapsamında kişisel verinin tanımına yer verilmesi, hangi verilerin bu kapsama girebileceği ya da hangi verilerin bu kapsama giremeyeceği gibi hususların daha açık şekilde ilgili maddede belirtilmesi daha uygun olurdu.

Herkesçe bilinen ya da kolaylıkla bilinmesi mümkün olabilecek durumda olan yani aleni veriler bu suç kapsamında cezalandırılmayacaktır²⁴⁶.

²⁴⁶ Nizamettin Aydın, “Tıp Ceza Hukukunda Verileri Hukuka Aykırı Olarak Verme ve Ele Geçirme Suçu (TCK m. 136.)”, *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, C. 21, S. 2 (2013), s. 17.

TCK m. 136/2 için suçun konusunu ise, “Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler” oluşturmaktadır.

(4) Hareket

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun gerçekleşmesi için kanunda yer alan vermek, yaymak ya da ele geçirmek fiillerinden birinin gerçekleştirilmesi yeterlidir²⁴⁷. Sayılan hareketlerin tamamının ya da iki tanesinin yapılması durumunda da birden fazla suç oluşmayacak, tek suç oluşacaktır²⁴⁸. Ancak bu durumda, TCK m. 61’e göre faile verilecek cezanın üst sınıra yaklaşması olasılığı ortaya çıkacaktır²⁴⁹.

Vermek sözcüğü, sözlükte “*üzerinde, elinde veya yakınında olan bir şeyi birisine eriştirmek, iletmek*” şeklinde tanımlanmıştır. Yaymak sözcüğü için ise sözlükte, “*birçok*

²⁴⁷ Maddede yer alan seçimlik hareketler Yargıtay tarafından şu şekilde tanımlanmıştır: “TCK'nun 136. maddesinde korunan hukuki değer genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özelde ise kişisel verilerdir. Bu düzenlemeler ile tüm kişisel veriler koruma altına alındığından kişisel verilerin mutlaka gizli olması zorunlu değildir. Gizli olmayan ve herkes tarafından bilinen kişisel veriler de hukuka aykırı eylemlere karşı korunmalıdır. Zira kişisel verilerin korunmasına ilişkin suçlarda korunan hukuki değer "sır" olmayıp, verinin ilgilisi olan kişinin kişilik haklarıdır. (Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, Seçkin Yayınevi, Ankara, 2014, 4. bası, s.579, 588-593) TCK'nun 136. maddesindeki "verileri hukuka aykırı olarak verme veya ele geçirme" suçu, seçimlik hareketli bir suç olarak düzenlenmiştir. Hukuka aykırı olarak kişisel verilerin başkasına verilmesi, kişisel verilerin yayılması ve kişisel verilerin ele geçirilmesi şeklindeki seçimlik hareketlerin birinin gerçekleştirilmesiyle suç işlenmiş olacaktır. "Kişisel verileri bir başkasına verme" seçimlik hareketinde, maddede geçen "başkası" gerçek bir kişi olabileceği gibi tüzel kişi de olabilecek, veriler bu kişilere elden, posta ya da internet üzerinden elektronik posta ile vb. şekillerde verilebilecektir. Türk Dil Kurumu Büyük Türkçe Sözlüğünde "vermek"; "üzerinde, elinde veya yakınında olan bir şeyi birisine eriştirmek, iletmek, düşünce veya bilgi anlatan şeyleri başkalarına iletmek, bildirmek" şeklinde açıklanmıştır. Bu seçimlik harekette verilerin hukuka uygun ya da aykırı yöntemle elde edilmiş olmasının önemi bulunmamakta olup, önemli olan husus verme eyleminin hukuka aykırı olmasıdır. "Kişisel verileri yayma" seçimlik hareketi de çeşitli şekillerde gerçekleştirilebilecektir. İnternet üzerindeki bir web sitesinde kişisel verileri yayınlamak, birçok kişiye elektronik posta ile ya da telefonda kısa mesajla göndermek, yazılı ya da görsel medyada yayınlamak gibi... Türk Dil Kurumu Büyük Türkçe Sözlüğünde "yaymak"; "birçok kimseye duyurmak, çevreye dağılmasına sebep olmak" olarak açıklanmıştır. "Kişisel verilerin ele geçirilmesi" seçimlik hareketi ise; kişisel verilerin kayıtlı olduğu belgelerin alınması ya da kayıtlı olduğu bilişim sisteminden ele geçirilmesi vb... şekillerde gerçekleştirilebilecektir. Ele geçirme fiili, başkasının hakimiyeti altında bulunan bir kişisel verinin, failin hakimiyeti altına girmesi ile gerçekleşmiş olacaktır.” (CGK, 04.07.2017, E. 2017/829, K. 2017/363, www.kazanci.com, (29.11.2019)).

²⁴⁸ Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 598.

²⁴⁹ Rezzan İtişgen, “Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu”, *Türkiye Adalet Akademisi Dergisi*, S. 23 (2015), s. 187; Kader Sarıusta, *Kişisel Verilerin Ceza Hukuku Yoluyla Korunması*, (Yüksek Lisans Tezi), Gaziantep: Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü, 2018, s. 152.

kimseye duyurmak” olarak tanımlanmıştır²⁵⁰. Kelimelerin anlamlarına bakıldığında, verme fiili bir şeyin, bir kişiye iletilmesiyle, yayma fiilinde birden fazla kişiye iletilmesi durumu ortaya çıkmaktadır. Bu durumda “yayma”nın kapsamının “verme”ye göre daha geniş olduğu söylenebilir²⁵¹. Verme fiili, bir kişiye bilgilerin yazılı olduğu kağıt vermek, elektronik posta göndermek gibi çok çeşitli şekillerde yapılabilir. Yaymak fiilinin oluşabilmesi için ise bilgilerin daha çok kişiye ulaşmasına imkan verecek yollarla paylaşılması gerekmektedir. Örneğin bilgilerin bir internet sitesine konulması durumunda bu bilgiye çok fazla kişinin erişmesi mümkün olduğundan vermek değil, yaymak fiili söz konusu olacaktır²⁵². Doktrinde bu suçun bir araç kullanılmadan, kulaktan kulağa aktarılma şeklinde gerçekleşmeyeceği, bu durumda TCK m. 133/3 ya da TCK m. 134/1’in söz konusu olabileceği yönünde görüşler vardır²⁵³. Ancak kanunda suçun oluşabilmesi için bilginin bir araç ile verilmesi gerektiği yönünde bir ifade olmadığı gibi sözlü bilgi aktarımının bu kapsamda değerlendirilmemesi durumunda kişilerin ciddi mağduriyetleri oluşabileceğinden, bu tür bilgi aktarımlarının da TCK m. 136 kapsamında değerlendirilmesi gerektiği kanısındayız²⁵⁴. Verilerin, öğrenilmesine imkan sağlanacak şekilde verilmesi ya da yayılması suçun işlenmesi için yeterlidir. Ayrıca birileri tarafından öğrenilmesi ya da algılanması gerekmemektedir. Birileri tarafından öğrenilmemiş olsa bile, bir internet sitesinde kişisel verilerin paylaşılması ile bu suç işlenmiş olacaktır²⁵⁵.

²⁵⁰ <http://sozluk.gov.tr/>

²⁵¹ Artuç, a.g.e., s. 1647.

²⁵² İtişgen, a.g.m., s. 188.

²⁵³ Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 598. “...TCK'nın 136/1. maddesinin, “Bu madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır.” şeklindeki gerekçesinden de anlaşılacağı üzere, kişisel verilerin, “verildiği”, “yayıldığı” veya “ele geçirildiği”nin kabul edilebilmesi için, kişisel verilerin kaydedilmiş halde bulunması, kaydedilmiş haliyle başkalarına verilmesi, yayılması ya da ele geçirilmesi gerekir. Kişisel verilerin kaydedilmeden önce öğrenilmesi, hafızada tutulan kişisel verilerin başkalarına açıklanması, kişisel verilere salt duyu organları aracılığıyla vakıf olunması, ancak TCK'nın 134/1. maddesinin 1. cümlesinde düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilebilir. Bu açıklamalar ışığında incelenen dosyada, elektronik mühendisi olan sanığın, teknik servis elemanı olarak çalıştığı sırada, T. Ö. Tıp Merkezi psikiyatri anabilim dalında tedavi gören mağdure hemşirenin, C. adli bilgi sisteminde bulunan muayene bilgilerini okuyup, hastane çalışanlarına, mağdurenin intihar girişiminde bulunduğunu anlattığı olayda, // Dairemizin değişen görüşüne göre; Mağdurenin kişisel verilerini, kaydedilmiş haliyle ele geçirip, bu haliyle başkalarına verdiğine veya yaydığına dair hakkında bir delil bulunmayan sanığın, mağdurenin özel yaşam alanındaki sağlık bilgilerini okuyup, içeriğini öğrendiği mağdureye ait kişisel verileri başkalarına açıklaması eyleminin, TCK'nın 134/1-1. maddesinde tanımlanan özel hayatın gizliliğini ihlal suçunu oluşturacağı gözetilmeden, suç vasfında yanlıya düşülerek, sanık hakkında, verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet kararı verilmesi, kanuna aykırı olup...” (12. CD., 27.10.2014, E. 2014/3107, K. 2014/20959, www.kazanci.com, (29.11.2019)).

²⁵⁴ İtişgen, a.g.m, s. 188.; Akdağ, a.g.e., s. 130.

²⁵⁵ Akdağ, a.g.e., s. 130-131.

Kişisel verileri vermek ya da yaymak fiillerinin gerçekleştirilebilmesi için failin bu veriye sahip olması gerektiği açıktır. Ancak yukarıda da değinildiği gibi, bu suç açısından, failin elinde bulundurduğu verinin hukuka aykırı ya da uygun olarak kaydedilmiş olması önem arz etmemektedir. Kamu ya da özel hukuk tüzel kişilerince hukuka uygun olarak saklanan verilerin verilmesi ya da yayılması durumunda da bu suçun oluşacağı açıktır. Ancak kişisel veriler hukuka aykırı olarak kaydedildikten sonra bu suçu da işleyen fail, hem TCK m.135 hem de TCK m. 136'dan sorumlu olacak bu iki madde arasında gerçek içtima hükümleri uygulanacaktır²⁵⁶.

Verilen ya da yayılan kişisel verinin, kamuya açık alanda çekilmiş bir görüntü olması da bu suçun işlenmesine engel değildir. Kamuya açık alanda çekilen bir görüntüyü veren veya yayan kimse de, bu suçu işlemiş olacaktır. Çünkü kişisel veri kavramı yalnızca özel hayat alanını kapsamamakta, kişiye ilişkin her türlü bilgiyi ifade etmektedir²⁵⁷.

Ele geçirmek fiilinin sözlük tanımı “*sahibi olmak*” şeklindedir. Kişinin, normalde ulaşması mümkün olmayan bilgileri çeşitli yollarla elde etmesi durumunda ele geçirme hareketinin gerçekleşeceğini söyleyebiliriz²⁵⁸. Bu hareket, bilgilerin yazılı olduğu kağıt

²⁵⁶ Artuç, a.g.e., s. 1648; Çokmutlu, a.g.e., s. 219.

²⁵⁷ Yargıtay'ın da bu konu ile ilgili bir kararı mevcuttur: “TCK'nın 135 ve 136. maddelerindeki kişisel verilerin korunmasına dair düzenlemelerde sadece sır niteliğinde kişisel verilerin korunacağına dair bir hükmün bulunmaması ve aksine 135. maddenin gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesi, yayılması ve ele geçirilmesi fiilleri TCK'nın 136. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturur. Bu sebeple herkes tarafından bilinen ve/veya kolaylıkla ulaşılabilecek ve bilinmesi mümkün olan kişisel bilgiler de, yasal anlamda “kişisel veri” olarak kabul edilmektedir... sanığın, bir dönem internet üzerinden tanışıp arkadaş olduğu katılanın daha önce kendi facebook hesabında paylaştığı resimleri, katılan ile tartışmaları sebebiyle katılan adına açtığı sahte facebook hesabından katılanın rızası dışında yayınladığı iddia edilen olayda, katılanın gündelik kıyafetler ile kamuya açık alanda çekilmiş ve kişisel veri niteliğindeki resimlerini daha önce kendi facebook hesabında yayınlamasının bu resimlerin kişisel veri olma özelliğini değiştirmeyeceği gibi üçüncü kişilere katılanın rızası dışında yayınlama hakkı da tanımayacağı gözetilmeden sanık hakkında verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyetine karar verilmesi gerekirken...” (12. CD., 14.02.2018, E. 2017/2960, K. 2018/1541, www.kazanci.com, (28.11.2019)). “Dosya kapsamına göre; sanığın, katılan adına açtığı sahte facebook hesabından katılana ait iletişim bilgilerini resimleri paylaştığı iddia ve kabul edilen olayda, sanığın savunmasına göre suça konu resimlerin daha önce katılan tarafından facebook hesabında yayınlanması nedeniyle başkalarının görmesini ve bilmesini istemeyeceği özel yaşam alanına ilişkin bir görüntü olarak kabul edilemeyeceğinden, katılanın kişisel veri niteliğindeki resmini, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle facebook adlı sosyal paylaşım sitesinde yayınlayan sanığın eyleminin, TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden, suç vasfında yanılığa düşülerek, yasal ve yeterli olmayan gerekçelerle sanık hakkında TCK'nın 134/2. madde ve fıkrasında düzenlenen özel hayatın gizliliğini ihlal suçundan mahkumiyet kararı verilmesi...” (12. CD., 19.06.2019, E. 2018/8331, K. 2019/7459, www.kazanci.com, (01.12.2019)).

²⁵⁸ Akdağ, a.g.e., s. 135.

ya da belgelerin alınması ile gerçekleşeceği gibi, elektronik ortamda çeşitli yöntemlerle bilgilerin elde edilmesi yoluyla da gerçekleştirilebilir²⁵⁹.

Failin ele geçirdiği verinin hukuka uygun ya da hukuka aykırı olarak muhafaza edilmesi önemli değildir. Hukuka uygun olarak kaydedilmiş bir verinin fail tarafından ele geçirilmesi bu suçu oluşturduğu gibi; hukuka aykırı kaydedilmiş bir verinin ele geçirilmesi durumunda da bu suç oluşacaktır²⁶⁰.

Ele geçirme fiilinin kimi zaman kaydetme fiilini de kapsamına alması mümkündür. Bu durum kişisel verilerin kaydedilmesi suçu ile verilerin ele geçirilmesi suçu arasında ayırım yapılmasını zorunlu kılmaktadır. Bu konu ile ilgili olarak doktrinde, kişisel verilerin kaydedilmesi suçu için ayrı bir düzenleme bulunması sebebiyle, kaydetme dışında kalan fiillerin ele geçirme olarak değerlendirilmesi gerektiği belirtilmektedir²⁶¹. Yargıtay da bazı kararlarında ele geçirme fiilinin kaydedilmiş olan veriler için söz konusu olabileceğini belirtmiştir. Ancak kaydedilme fiili ve ele geçirme fiilinin birbiri yerine kullanılma ihtimalinin bulunması sebebiyle²⁶², belirlilik ilkesine de uygunluğun sağlanması açısından, bu kavramlardan ne anlaşılması gerektiğinin kanun metninde belirtilmesi yerinde olurdu²⁶³.

Failin, kişisel verileri ele geçirme kastı olmadan, kişiye ait telefonun çalınması durumu söz konusu olduğunda ise TCK m. 136 kapsamında suç oluşmayacağı, bu fiilin hırsızlık suçu kapsamında (TCK m. 141) değerlendirilmesi gerektiği kanısındayız²⁶⁴.

²⁵⁹ Kuşkonmaz, a.g.e., s. 154.

²⁶⁰ Murat Volkan Dülger, “Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması”, *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, C. 3, S. 6 (2016), s. 132.

²⁶¹ Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 598

²⁶² “Diğer sanıklarla kart kopyalamak üzere anlaşılıp karşılığında menfaat elde ettiği anlaşılan sanığın eyleminin, çalıştığı restoranta gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmekten ibaret olduğu diğer sanıkların sahte kart üretmek ve bu kartları kullanmak suçlarına iştirak ettiğine dair dosya kapsamında delil bulunmadığı anlaşılmakla, eyleminin TCK.nun 136. maddesinde düzenlenen birden fazla kişiye ait kişisel verileri hukuka aykırı olarak ele geçirme suçunu oluşturduğu gözetilmeden...” (8. CD., 31.01.2018, E. 2017/15706, K. 2018/866, www.kazanci.com, (28.11.2019)).

²⁶³ Ayrıca kişisel verileri ele geçirme fiilinin, kişisel verilerin kaydedilmesi fiiline göre daha az haksızlığa sebep olacağı, kişisel verilerin kaydedilmesi suçunun ele geçirme fiilinin oluşturacağı haksızlığı kapsamının mümkün olduğu ve ele geçirme hareketi sonrasında verilerin kaydedilmesi, verilmesi ya da yayılması sonucu ortaya çıkmadığı sürece ele geçirmenin cezalandırmayı gerektirmeyen bir hazırlık hareketi olarak değerlendirilmesi gerektiği, bu sebeple de ele geçirme fiilinin TCK m. 136 kapsamından çıkarılması gerektiği yönündeki görüş için bakınız: Koca, Üzülmüş, “Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)”, s.80.

²⁶⁴ İtişgen, a.g.m., s. 189.

(5) Nitelikli unsurlar

TCK m. 136/2'de “Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.” düzenlemesi yer almaktadır. CMK m. 236/5 ve m. 236/6 hükmü gereğince kayda alınmış olan beyan ve görüntülerin hukuka aykırı olarak verilmesi, yayılması ya da ele geçirilmesi durumunda suçun nitelikli hali ortaya çıkacak ve verilecek ceza artırılabilecektir.

CMK m. 236/5 “Türk Ceza Kanununun 103 üncü maddesinin ikinci fıkrasında düzenlenen suçlardan mağdur olan çocukların soruşturma evresindeki beyanları, bunlara yönelik hizmet veren merkezlerde Cumhuriyet savcısının nezaretinde uzmanlar aracılığıyla alınır. Mağdur çocuğun beyan ve görüntüleri kayda alınır. Kovuşturma evresinde ise ancak, maddi gerçeğin ortaya çıkarılması açısından mağdur çocuğun beyanının alınması veya başkaca bir işlem yapılmasında zorunluluk bulunması hâlinde bu işlem, mahkeme veya görevlendireceği naip hâkim tarafından bu merkezlerde uzmanlar aracılığıyla yerine getirilir. Mağdur çocuk yargı çevresi ve mülkî sınırlara bakılmaksızın en yakın merkeze götürülmek suretiyle bu fıkroda belirtilen işlemler yerine getirilir.” şeklinde düzenlenmiştir. CMK m. 236/6'da ise “Türk Ceza Kanununun 102 nci maddesinin ikinci fıkrasında düzenlenen suçlardan mağdur olanların soruşturma evresindeki beyanları bakımından da beşinci fıkra hükmü uygulanır. Ancak, beyan ve görüntülerin kayda alınmasında mağdurun rızası aranır.” hükmü yer almaktadır.

Çocukların cinsel istismarı suçunun vücuda organ veya sair bir cisim sokulması şeklindeki nitelikli hali (TCK m. 103/2) dolayısıyla mağdur olan çocuğun, soruşturma ve kovuşturma evreleri sırasında kayda alınan beyan ve görüntülerinin korunmasına kanun koyucu tarafından önem verilmiş ve bu verilere karşı TCK m. 136 kapsamında işlenecek suçlar bakımından daha özel bir koruma getirilmiştir. Aynı durum, cinsel saldırı suçunun vücuda organ veya sair bir cisim sokulması şeklindeki nitelikli hali (TCK m. 102/2) dolayısıyla mağdur olan kişinin, soruşturma evresinde kayda alınan beyan ve görüntüleri için de öngörülmüştür. Ancak CMK m. 236/6'da mağdurun beyan ve görüntülerinin kayda alınmasının rızaya bağlı olduğu belirtilmiştir. TCK m. 136/2'de ise kayda alınan beyan ve görüntülerden bahsedildiği için bu beyan ve görüntülerin kayda alınmaması durumunda nitelikli hal oluşturacak verinin ortaya çıkmayacağı da açıktır. CMK m.

236//5'te ise herhangi bir rıza şartı aranmamış, çocuğun beyan ve görüntülerinin kayda alınacağı belirtilmiştir.

TCK m. 137 de bu suç için uygulanacak nitelikli haldir. Öyleyse suçun, “kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle” ya da “belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle” işlenmesi durumunda nitelikli hal söz konusu olacak ve ceza artırılabacaktır. TCK m. 137'de yer alan düzenleme ile ilgili detaylı açıklama bir önceki suçun incelenmesi sırasında yapıldığından bu bölümde detaylı açıklamaya yer verilmeyecektir.

c. Suçun manevi unsuru

Kanun koyucu suçun işlenmesi için özel bir amaç ve saik aramadığından verileri hukuka aykırı olarak verme veya ele geçirme suçu doğrudan kasta tabi bir suçtur. Failin kişisel verileri bilerek ve isteyerek vermesi, yayması ya da ele geçirmesi suçun oluşması için gereklidir²⁶⁵. Kişisel verilerin kaydedilmesi suçu için, maddede yer alan hukuka aykırılık ifadesinin kastın ve tipikliğin unsuru olmadığı açıklaması bu suç için de geçerlidir. TCK m. 136'da yer alan “hukuka aykırı olarak” ifadesi de suçun genel değerlendirmesine ilişkin olduğundan, bu suçun olası kastla işlenmesi mümkündür. Kanunda bu suçun taksirle işlenebileceğine dair bir düzenleme yer almadığından, taksirle işlenmesi de mümkün değildir.

Verileri verme, yayma veya ele geçirme suçunda da fail, kastını kaldıran bir hataya düşmesi durumunda bu hatasından yararlanacaktır. TCK m. 30/1'e göre “*Fiilin icrası sırasında suçun kanuni tanımındaki maddi unsurları bilmeyen bir kimse, kasten hareket etmiş olmaz. Bu hata dolayısıyla taksirli sorumluluk hali saklıdır*”. Bu durumda kişi kendi verilerini başkasına verdiğini düşünürken başka bir kişiye ait verileri vermişse,

²⁶⁵ “*Sanığın, dayısının oğlu olan mağdurun bilgisi ve rızası dışında, mağdurun nüfus cüzdanının fotokopisi ile başvuru yapıp, mağdur adına düzenlenen telefon abonelik sözleşmesini imzalayarak, sahte GSM hattı çıkartmaktan ibaret eyleminde, mağdurun nüfus cüzdanının fotokopisini hukuka aykırı olarak ele geçirdiği iddiasıyla hakkında dava açılmamış olan sanığın kastının, mağdura ait kişisel verileri yaymak değil, bu verileri içeren nüfus cüzdanının fotokopisini ilgili GSM firmasına vererek, sahte telefon hattı çıkartmak olduğu ve eylemin bu haliye özel belgede sahtecilik suçunu oluşturduğu, verileri hukuka aykırı olarak verme veya ele geçirme suçunun yasal unsurlarının oluşmadığı gözetilmeden, yazılı şekilde, özel belgede sahtecilik ve verileri hukuka aykırı olarak verme veya ele geçirme suçlarından iki ayrı mahkumiyet hükmü kurulmasında isabet görülmemiş olup...*” (12. CD., 02.06.2014, E. 2014/10839, K. 2014/13375, www.kazanci.com, (01.12.2019)).

suçun maddi unsurlarında hata meydana geldiğinden kişinin kastı ortadan kalkacaktır. Bu suçun taksirli hali de cezalandırılmadığından kişiye ceza verilmeyecektir²⁶⁶.

Kişinin hatasının kastını kaldırdığından söz edilebilmesi için bu hataya düşmeseydi fiilinin suç oluşturmayacağı kabul edilmelidir. Yani kişinin hatası olmasaydı da fiil suç oluşturacaksa bu durumda hata kastı kaldırmayacağından fail işlediği suç dolayısıyla sorumlu olacaktır. Örneğin fail A'nın kişisel verilerini vermek, yaymak ya da ele geçirmek isterken hatası sebebiyle B'nin kişisel verilerini vermiş, yaymış ya da ele geçirmişse mağdurun kimliğinde hataya düşmesi sebebiyle cezai sorumluluğunda bir değişiklik olmayacaktır²⁶⁷.

Fail suçun nitelikli unsurlarında da hataya düşebilir. Böyle bir hataya düşmesi durumunda hatasından yararlanacaktır (TCK m. 30/2). Bir kişiye ait verileri veren, yayan ya da ele geçiren fail bu fiili ile CMK m. 236/5-6'ya göre kaydedilmiş verileri vermiş, yaymış ya da ele geçirmişse ancak verilerin bu kapsamda olmadığı düşüncesiyle hareket etmişse, suçun nitelikli halinde hataya düşmesi sebebiyle cezası suçun temel halinden verilecektir.²⁶⁸

2. Hukuka Aykırılık Unsuru

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun düzenlemesinde “hukuka aykırı olarak” ifadesine yer verilmiş olmasının sebebi, hakimin, bu suç ile ilgili hukuka uygunluk nedeni olabileceği yönünde uyarılmasının amaçlanmasıdır. Bu durumda TCK m. 135 ile aynı şekilde, tipikliğin gerçekleşmesi ile hukuka aykırılık konusunda bir karine oluşmayacak ve hakim olayda bir hukuka uygunluk nedeni bulunup bulunmadığını araştıracaktır²⁶⁹.

Bu suç bakımından, genel hükümler çerçevesinde hukuka uygunluk nedenlerinin uygulanması mümkündür. Ayrıca KVKK m. 5 ve özel nitelikli veriler için, KVKK m.

²⁶⁶ Özgenç, Üzülmez, a.g.e., s.104; Artuk, Gökçen, Yenidünya, a.g.e., s. 522; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 122.

²⁶⁷ Özgenç, Üzülmez, a.g.e., s. 104-105; Artuk, Gökçen, Yenidünya, a.g.e., s. 523; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 122.

²⁶⁸ Özgenç, Üzülmez, a.g.e., s. 105; Artuk, Gökçen, Yenidünya, a.g.e., s. 524-525; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 122.

²⁶⁹ Göktürk, a.g.e., s. 432.

6’da sayılan şartların varlığı halinde verilerin verilmesi, yayılması ve ele geçirilmesi hukuka aykırı olmayacaktır.

Kanun hükmünü yerine getirme (TCK m. 24/1) bu suç için uygulanabilecek bir hukuka uygunluk nedenidir. Bir kanun hükmüne dayanarak hareketi gerçekleştiren kişinin fiili hukuka uygun olacağından, bu kişiye ceza verilmeyecektir. KVKK m. 8 ve KVKK m. 9’da kişisel verilerin aktarılmasının hukuka uygun olacağı şartlar için, KVKK m. 5/2 ve m. 6/3’e atıf yapılmıştır. Kanunlarda hüküm bulunması da bu şartlar içinde yer almaktadır. Dolayısıyla bu hukuka uygunluk nedeni KVKK tarafından da öngörülmüştür.

TCK m. 278-280 kapsamında, işlenen bir suçun bildirilmesi sırasında kişisel veri niteliğinde bilgilerin de verilmesi durumu, TCK m. 24/1 kapsamında hukuka uygunluk nedeni olacağından suç oluşmayacaktır. Aynı şekilde TCK m. 53 ve Adli Sicil Kanunu m. 7 kapsamında kişisel verilerin verilmesi, kanuni dayanağı sebebiyle hukuka uygun olacaktır²⁷⁰.

Meşru savunmanın (TCK m. 25/1) bu suç için hukuka uygunluk sebebi olmasının mümkün olup olmadığı konusundaki görüşümüz, kişisel verilerin kaydedilmesi suçunda söz edilen sebeplerden dolayı uygulama imkanının olmadığı yönündedir. Ancak tarafımızca olasılık dışı görülüyor olsa da, meşru savunma şartlarının tam olarak sağlandığı bir durumda TCK m. 25/1’in uygulanması mümkün olabilecektir.

Hakkın kullanılması (TCK m. 26/1) da bu suç için hukuka uygunluk nedeni oluşturabilecektir. Basının haber verme hakkı bu duruma örnek olarak verilebilecek bir haktır. Ancak bu hakkın kullanılmasının hukuka uygun kabul edilebilmesi için; “gerçeklik, güncellik, kamu yararı, konu ile ifade arasında düşünsel bağlılık” şartlarının gerçekleşmiş olması aranacaktır²⁷¹.

İlgilinin rızası (TCK m. 26/2) bu suç bakımından uygulama alanı bulabilecek hukuka uygunluk nedenlerinden bir diğeridir. Veri sahibinin rızasının olduğu durumlarda, kişisel verilerin verilmesi, yayılması ya da ele geçirilmesi hukuka uygun hale gelecektir. Kişisel verilerin aktarılmasını (KVKK m. 8) ve kişisel verilerin yurt dışına aktarılmasını

²⁷⁰ Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 123-124.

²⁷¹ Bayraktar, a.g.e., s. 649; İtişgen, a.g.m., s. 192; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 126.

(KVKK m. 9) düzenleyen KVKK hükümlerinde de, veri sahibinin açık rızası ile kişisel verilerin aktarılmasının mümkün olduğu belirtilmiştir.

KVKK m. 5/2’de yer alan, *“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 durumunda kişisel veriler işlenebilecektir ve bu sebeple bu fiil dolayısıyla faile ceza verilmeyecektir”* düzenlemesine göre varsayılan rıza da verileri hukuka aykırı olarak verme veya ele geçirme suçu için hukuka uygunluk nedeni olabilecektir. Ancak KVKK m. 5’te yer alan bu hukuka uygunluk nedeni, KVKK m. 6’da sayılmadığından, özel nitelikli kişisel verileri açısından söz konusu olmayacaktır²⁷².

KVKK m. 8’de kişisel verilerin, KVKK m. 5/2’de yer alan şartlardan birinin bulunması halinde, özel nitelikli kişisel verilerin ise gerekli önlemlerin alınması şartıyla KVKK m. 6/3’teki şartlardan birinin varlığında, veri sahibinin açık rızası olmaksızın aktarılabilmesi hükmü yer almaktadır. Kişisel verilerin, veri sahibinin açık rızası olmaksızın yurt dışına aktarılmasının hukuka uygun olması için ise KVKK m. 9’da ek şartlar getirilmiştir. Buna göre, *“Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede; Yeterli korumanın bulunması, yeterli korumanın bulunmaması durumunda Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir”*. Bu şartların sağlanması durumunda kişisel verilerin, veri sahibinin rızası olmaksızın yurt dışına aktarılması da hukuka uygun olacaktır.

D. KUSUR

Kusurluluğu etkileyen bir hata hali olan haksızlık yanığı, verileri hukuka aykırı olarak verme veya ele geçirme suçu bakımından önemlidir. TCK m. 136’da “hukuka aykırı olarak” ifadesi yer aldığından, bu suçun failinin, işlediği fiilin hukuka aykırılığı konusunda kesin bilgi sahibi olması gerekmektedir. Failde, bu konu hakkında bir şüphe

²⁷² Korkmaz, a.g.e., s. 358.

oluşması durumunda, failin haksızlık yanılığı içinde olduğu ve kusurlu olmadığı kabul edilecektir²⁷³.

Yetkili amirin emrini ifa (TCK m. 24/2) TCK m. 136 bakımından da kusurluluğu kaldıran bir sebep olarak ortaya çıkabilecektir. Ancak kusurun olmadığı kabulü için; “emrin yetkili bir merci tarafından verilmesi (TCK m. 24/2), görev dolayısıyla yerine getirilmesi zorunlu bir görev olması (TCK m. 24/2) ve konusu suç teşkil etmeyen bir emir olması (TCK m. 24/3)” gerekmektedir. Bu şartlar altında verilen emir gereğince TCK m. 136 kapsamındaki hareketlerden birini gerçekleştiren kişiye ceza verilmeyecektir.

Kendi hakkına ya da bir başkasının hakkına yönelik bir saldırı ya da tehlike bulunması durumunda, bu durumdan korunmanın başka yolu olmaması halinde bu suçun işlenmesi durumunda kişiye ceza verilmeyecektir (TCK m. 25). Örneğin kaybolan bir kişinin bulunması amacıyla, o kişinin telefon ya da kredi kartı bilgileri gibi bilgilerinin elde edilmesi durumunda zorunluluk hali söz konusu olacağından bu verileri ele geçiren kişiye ceza verilmeyecektir²⁷⁴.

Kişinin kurtulma imkanı bulunmadığı cebir ve şiddet ya da ağır tehdit altında bu suçu işlemesi durumunda, kişiye ceza verilmeyecek ve TCK m. 28’e göre cebir ya da tehdidi kullanan kişi dolaylı fail olarak sorumlu olacaktır.

Haksız tahrik altında verileri hukuka aykırı olarak verme veya ele geçirme suçunun işlenmesi durumunda ise TCK m. 29’a göre kişiye verilecek ceza indirilecektir.

Bunlar dışında, şartlarının varlığı halinde, kusurluluğu etkileyen diğer haller olan; yaş küçüklüğü, akıl hastalığı, sağır dilsizlik ve alkol ve uyuşturucu madde etkisinde olma halleri konusundaki genel hükümler, bu suç için uygulanabilecektir.

²⁷³ Göktürk, a.g.m., s. 432-433.

²⁷⁴ Sert, a.g.e., s. 127.

E. SUÇUN ÖZEL GÖRÜNÜM ŞEKİLLERİ

1. Teşebbüs

Verileri hukuka aykırı olarak verme veya ele geçirme suçu sırf hareket suçu olduğundan ancak icra hareketlerinin bölünebildiği durumlarda teşebbüs mümkün olacaktır. Örneğin fail, kişisel verileri başkasına elektronik posta ile göndermek isterken elinde olmayan herhangi bir sebepten gönderemezse ya da posta ile gönderirken postada kaybolursa kişisel verileri verme fiili gerçekleşmemiş olacaktır ve suç teşebbüs aşamasında kalacaktır²⁷⁵.

Ele geçirme hareketi için de teşebbüs mümkün olacaktır. Örneğin fail içinde kişisel verilerin bulunduğu bir kasayı açmaya çalışırken hareketini tamamlayamaz ve verilere ulaşamazsa suç teşebbüs aşamasında kalır. Bilişim sistemleri aracılığıyla kişisel verilerin ele geçirilmesi durumunda da failin elinde olmayan sebeplerle hareket yarıda kalırsa suç teşebbüs aşamasında kalır. Fail bilişim sistemlerine girmek suretiyle kişisel verileri ele geçirmeye çalışırken sisteme girdikten sonra kendi isteğiyle hareketten, verileri ele geçirmekten vazgeçerse, TCK m. 36'da yer alan gönüllü vazgeçme hükümleri uygulanacaktır. Bu durumda bilişim sistemlerine girme hareketi tamamlandığından ve bu hareket TCK m. 243 kapsamında bir suç oluşturduğundan fail, bu suçtan sorumlu olacaktır. Ancak verinin içeriğinin öğrenilmesinden itibaren suç tamamlanmış olacağından teşebbüs ya da gönüllü vazgeçme hükümlerinin uygulanması söz konusu olmayacaktır²⁷⁶.

2. İştirak

Verileri hukuka aykırı olarak verme veya ele geçirme suçu, iştirak bakımından bir özellik göstermemekte, iştirak halinde genel hükümlerin uygulanması gerekmektedir.

TCK m. 137'de düzenlenen nitelikli hal sebebiyle, bu maddede belirtilen kişilerin suça iştirak etmesi durumunda, bu kişiler bakımından cezanın artırılması gerekecektir²⁷⁷.

²⁷⁵ Akdağ, a.g.e.,

²⁷⁶ Akdağ, a.g.e., s. 140.

²⁷⁷ Kuşkonmaz, a.g.e., s. 157.

Nitelikli haller için gereken sığata sahip olan kiřiyle birlikte, bu sıfatlardan herhangi birine sahip olmayan kiřinin birlikte suç iřlemesi durumunda, gerekli sığata sahip olmayan kiřiye nitelikli halden ceza verilemeyecektir. Ancak bu kiři suçun temel hali bakımından fail olarak sorumlu olacaktır²⁷⁸.

3. İçtima

Bu suçun bir suç iřleme kararı kapsamında aynı kiřiye karřı birden fazla kez iřlenmesi durumunda zincirleme suç hükümleri uygulanabilecektir. Bu durumda “bir cezaya hükmedilir. Ancak bu ceza, dörtte birinden dörtte üçüne kadar artırılır” (TCK m. 43/1). Ayrıca tek bir hareketle birden fazla kiřiye ait verinin verilmesi, yayılması ya da ele geçirilmesi durumunda aynı neviden fikri içtima söz konusu olacak ve ceza zincirleme suç hükümlerine göre belirlenecektir. Bu durumda da verilecek ceza dörtte birinden dörtte üçüne kadar artırılacaktır.

Farklı neviden fikri içtima da bu suç için söz konusu olabilecektir. Örneğın kişisel verilerin herkes tarafından ulaşılabilir bir internet sitesine kaydedilmesi durumunda hem TCK m.135 hem de TCK m.136 kapsamında suç oluşacaktır ve fikri içtima hükmü uyarınca daha ağır cezayı gerektiren TCK m. 136 hükmü uygulanacaktır²⁷⁹. Ancak önce kişisel veriler kaydedilip daha sonra da yayılır ya da verirse bu durumda iki ayrı hareket söz konusu olacak, iki ayrı suç oluşacak ve gerçek içtima hükümlerinin uygulanması gerekecektir²⁸⁰.

Kişisel verilerin verilmesi ya da yayılması fiilinin aynı zamanda TCK m. 125’te yer alan “hakaret” suçunu oluşturması da verilebilecek bir örnektir. Bu durumda da aynı hareketle birden fazla suç iřlendiğinden farklı neviden fikri içtima söz konusu olacaktır²⁸¹.

TCK m. 239 kapsamında müşteri sırrı olan bilgilerin verilmesi ya da ifřa edilmesi sırasında kişisel veri niteliğindeki bilgiler de veriliyorsa TCK m. 136 ile m. 239 arasında farklı neviden fikri içtima hükümlerinin uygulanması gerekecektir.

²⁷⁸ Akbulut, a.g.m., s. 186.

²⁷⁹ Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 600.

²⁸⁰ Kuřkonmaz, a.g.e., s. 149.

²⁸¹ Yokuř Sevük, a.g.e., s. 257.

TCK m. 244/2’de bir bilişim sistemine veri yerleştiren ya da veriyi başka bir yere gönderen kişinin cezalandırılacağına ilişkin düzenleme yer almaktadır. Kişisel verilerin verilmesi ya da yayılması fiilinin, bilişim sistemindeki veriyi başka bir yere göndermesi fiiliyle gerçekleştirilmesi durumunda TCK m. 136 ve m. 244/2 arasında farklı neviden fikri içtima ortaya çıkacaktır²⁸².

TCK m. 134/2’de yer alan “özel hayatın gizliliğini ihlal” suçu kapsamında kişinin özel hayatına ilişkin görüntü veya seslerinin ifşası sırasında, kişinin özel hayatı dışında kalan kişisel verilerin de yayılması, verilmesi ya da ele geçirilmesi durumunda, farklı neviden fikri içtima hükümleri uygulanacaktır.

TCK m. 132/2’de “kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse” ifadesi yer almaktadır. Bu suç işlenirken haberleşme içeriklerinin ifşa edilmesiyle birlikte kişisel verilerin de verilmesi ya da yayılması durumunda, kişisel veri, kavramı “kimliği belirli ya da belirlenebilir kişiye ilişkin her türlü veri”yi kapsarken, TCK m. 132’de her türlü veriden değil, kişiler arasındaki haberleşme içeriklerinden söz edildiğinden, TCK m. 132’de yer alan düzenleme, kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçuna göre özel norm olduğundan, TCK m. 132 hükmü uygulanacaktır.

TCK m. 133/3’te ise “kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi”den bahsedilmektedir. Bu suç işlenirken kişisel veri niteliğine sahip verilerin de verilmesi ya da yayılması durumunda, yukarıdaki açıklamalara göre, TCK m. 133 yalnızca kişiler arasındaki aleni olmayan konuşmaları kapsadığından, özel normdur ve TCK m. 133 hükmü uygulanır.

5464 sayılı Banka Kartları ve Kredi Kartları Kanunu’nun 23. maddesinin 1. fıkrasında “*Üye işyerleri, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına açıklayamaz, saklayamaz ve kopyalayamaz. Üye işyerleri, kart bilgilerini üye işyeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamaz, satamaz, satın alamaz ve takas edemez. Üye işyeri anlaşması yapan kuruluşlar, bu fıkranın uygulanmasını gözetmekle*

²⁸² Sert, a.g.e., s. 150.

yükümlüdür.” hükmü yer almaktadır. Bu hükme aykırılık durumunda kişisel verilerin verilmesi, yayılması ya da ele geçirilmesi durumu söz konusu olacak olsa da, kart ve kart hamili ile ilgili bilgileri düzenleyen bu madde kişisel verilere ilişkin olarak düzenlenen TCK m. 136’ya göre daha özel bir alanı düzenlediğinden özel normdur. Bu durumda, bu kapsamda bir suçun işlenmesi halinde ceza, TCK m. 136 hükmüne göre değil, Banka Kartları ve Kredi Kartları Kanunu m. 39’a göre verilecektir²⁸³.

TCK m. 245/1’de “Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.” hükmü yer almaktadır. Başkasına ait banka ya da kredi kartının ele geçirilmesi bu suçun bir unsuru olduğundan bileşik suç söz konusu olacaktır. TCK m. 42 gereğince bileşik suç söz konusu olduğunda suç tek fiil ile işlenmiş sayılacak ve bu suçlar arasında içtima hükümleri uygulanmayacaktır. Bu sebeple TCK m. 245/1 kapsamında kendisine yarar sağlayan kimse bu maddeden dolayı cezalandırılacak, TCK m. 136’dan ayrıca ceza almayacaktır²⁸⁴.

Verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunun birden fazla fiille işlenmesi durumunda gerçek içtima hükümleri uygulanacak ve fiil sayısı kadar suç oluştuğu kabul edilecektir²⁸⁵. Fail bir kişiye cebir uygulayarak o kişinin kişisel verilerini ele geçirmişse hem cebir (TCK m. 108) hem de verileri hukuka aykırı olarak ele geçirme suçundan cezalandırılacaktır.

TCK m. 243’te bilişim sistemine girme suçu düzenlenmiştir. Bu suç ile TCK m. 136 arasında gerçek içtima hükümlerinin uygulanması mümkündür. Örneğin fail, kişisel verileri ele geçirmek için önce hukuka aykırı olarak bilişim sistemlerine girer, daha sonra

²⁸³ Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 142.

²⁸⁴ a.g.e., s. 143. “Dosya kapsamına göre, sanık hakkında katılanlar ... ve ...’a karşı kişisel verileri hukuka aykırı ele geçirmek suçlarından kurulan hükümlerde, ele geçirilen katılanlara ait kart bilgilerini kullanarak alışveriş yapmak eylemlerinin küll halinde, mağdur sayısınca TCK’nın 245/1. maddesindeki suçu oluşturacağı gözetilmeden, aynı Kanun’un 136. maddesi uyarınca ayrıca mahkumiyet hükmü kurulmasında isabet görülmemiş olup...” (12. CD., 07.02.2018, E. 2017/11578, K. 2018/ 1164, www.kazanci.com, (28.11.2019)).

²⁸⁵ “Suça konu fotoğrafların toplu halde değil ayrı ayrı çekilip yayımlanması karşısında, sanığa yüklenen suçların mağdur sayısınca oluşacağı gözetilmeden...” (4. CD., 24.01.2013, E. 2011/11771, K. 2013/1376, www.kazanci.com, (28.11.2019)).

da burada bulunan kişisel verileri ele geçirirse her iki suçtan da ayrı ayrı ceza verilmesi gerekecektir.

F. YAPTIRIM

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun temel şekli için, “iki yıldan dört yıla kadar hapis cezası” öngörülmüştür. CMK m.236/5-6’ya göre kaydedilen verilerin bu suça konu olması durumunda ise verilecek ceza bir kat artırılacaktır. Ayrıca TCK m. 137 düzenlemesi uyarınca suçun, “kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle” işlenmesi durumunda verilecek ceza yarı oranında artırılacaktır.

Bu suç dolayısıyla kişiye hapis cezası verilmesi durumunda, kişi hakkında TCK m. 53’te yer alan hak yoksunlukları uygulanacaktır.

Sanığa verilecek cezanın iki yıl veya daha az olması durumunda, şartlarının sağlanması halinde, hapis cezasının ertelenmesi ya da hükmün açıklanmasının geri bırakılması mümkün olabilecektir.

TCK’nın 140. maddesinde ise bu suçun işlenmesi dolayısıyla hukuka aykırı yarar sağlayan tüzel kişilere yönelik yaptırıma ilişkin düzenleme yer almaktadır. Maddeye göre bu suçun işlenmesi dolayısıyla tüzel kişiler hakkında, TCK 60. maddede yer alan bunlara özgü güvenlik tedbirlerine hükmolunacaktır²⁸⁶.

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun temel hali için verilecek hapis cezası beş yıldan fazla olmadığından TCK m. 66/1 uyarınca dava zamanaşımı sekiz yıldır. TCK m. 68/1 uyarınca ceza zamanaşımı ise on yıldır. TCK m. 137 ya da TCK m. 136/2’de yer alan nitelikli hal kapsamında suç işlenmesi durumunda ise verilecek cezanın üst sınırı beş yıldan fazla olacağından dava zamanaşımı on beş yıl olacaktır. Bu durumda ceza zamanaşımı verilecek cezaya göre değişecektir. Beş yıl ve daha az ceza verilmesi durumunda ceza zamanaşımı on yıl olacakken, cezanın beş yılı aşması durumunda yirmi yıl olacaktır.

²⁸⁶ Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 718.

G. MUHAKEMEYE İLİŞKİN KURALLAR

TCK m. 139 hükmü uyarınca, verileri hukuka aykırı olarak verme veya ele geçirme suçunun soruşturması ve kovuşturması şikayete tabi değildir. Bu durumda soruşturma Cumhuriyet Savcılığı tarafından resen yapılacaktır. Kamu görevlileri bakımından, görevleri dolayısıyla suç işlemeleri durumunda 4483 sayılı Kanun gereğince soruşturma yapılabilmesi için yetkili makamdan izin alınması gerekmektedir.

CMK m. 253'te uzlaştırma hükümlerinin uygulanacağı suçlar sayılmıştır. Buna göre uzlaştırma hükümlerinin uygulanabilmesi için, suçun şikayete tabi olması ya da bu maddede sayılan suçlardan olması gerekmektedir. Verileri hukuka aykırı olarak verme veya ele geçirme suçu için, şikayete tabi olmaması ve maddede sayılan diğer suçlar arasında da yer almaması sebebiyle uzlaştırma hükümleri uygulanamayacaktır.

Suç için belirlenen cezanın üst sınırı göz önüne alındığında, 5235 sayılı Kanun'a göre görevli mahkeme asliye ceza mahkemesidir²⁸⁷. Yetkili mahkeme ise CMK m. 12/1'e göre bu suç bakımından suçun işlendiği yer mahkemesidir. Bu yerin belirlenememesi durumunda ise CMK m. 13'te yer alan özel yetki kuralları uygulama alanı bulacaktır.

IV. VERİLERİ YOK ETMEME SUÇU (TCK m. 138)

A. GENEL OLARAK

Verileri yok etmeme suçu da çalışmamızda yer alan diğer iki suç tipi gibi 765 sayılı eski Türk Ceza Kanunu'nda yer almayan bir suç tipidir. 5237 sayılı TCK'nın 138. maddesinde düzenlenen suç tipinin kanun metni “(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.” şeklindedir. Maddenin önceki halinde birinci fıkrada düzenlenen ceza altı aydan bir yıla kadar hapisken, 21.2.2014 tarihli ve 6526 sayılı Kanun ile bir yıldan iki yıla kadar hapis şeklinde

²⁸⁷ Yokuş Sevük, a.g.e., s. 258.

değiştirilmiştir. Ayrıca bu değişiklik ile daha önce maddede yer almayan ikinci fıkra hükmü de maddeye eklenmiştir.

Maddenin gerekçesine göre, hukuka uygun olarak kaydedilen kişisel verilerin kanunlarda belirlenen süre geçtiği halde yok edilmemesi, bir suç olarak düzenlenmiştir²⁸⁸. Kişiler yaşamları süresince çeşitli sebeplerle kişisel verilerini çeşitli kişilere vermektedirler. Bu durumda verilerin toplanması, kaydedilmesi hukuka uygun olsa da süresiz olarak muhafaza edilmeleri kişilerde güvensizlik hissi yaratabilmekte, özel hayata müdahale oluşturabilmektedir. Bu suç tipiyle, bu olumsuzlukların engellenmesi amaçlanmış, verilerin gereken süre dışında sistemde tutulması durumunda, bunu gerçekleştirenlerin cezalandırılmasına imkan verilmiştir²⁸⁹.

TCK m. 136’da olduğu gibi bu maddenin başlığında da “kişisel veri” kavramı yerine yalnızca “veri” kavramı kullanılmıştır. Bu madde ile korunmak istenenin her türlü veri değil, kişisel veriler olduğu açıktır ve madde gerekçesinden de anlaşılmaktadır. Ancak veri kavramı, kişisel veriye göre çok daha geniş bilgi türlerini kapsadığından, maddenin başlığının “kişisel verileri yok etmeme” şeklinde düzenlenmiş olması çok daha uygun olurdu.

Doktrinde bizim de katıldığımız bir görüş, bu maddenin kişisel verilerin korunmasına ilişkin ilkelerden olan sınırlı süre muhafaza ilkesini karşıladığını belirtmektedir. Ancak bu ilkenin amacı; kişisel verilerin işleme amacının gerektirdiği süre kadar muhafaza edilmesini sağlamakken, verileri yok etmeme suçunun oluşması için geçmesi gereken süre kanunlarda aranan sürelerdir. Yani kişisel verilerin işleme amacı için gereken süre çok kısa da olsa kanunlarda belirlenen süre daha uzunsa, bu uzun süre boyunca verileri yok etmeme suçu oluşmayacaktır. Bu durum kişisel verilerin korunmasına yönelik ilkelere uygun olmadığından, TCK m. 138’in kişisel verilerin korunması hukuku dikkate alınarak düzenlenmesinin daha yerinde olacağı kanaatindeyiz²⁹⁰.

Ayrıca konu ile ilgili olarak KVKK’nın “Suçlar” başlıklı 17. maddesinin ikinci fıkrasında “*Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen*

²⁸⁸ Ankara HBV Üniversitesi Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, s. 342.

²⁸⁹ Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 718-719; Korkmaz, a.g.e., 423.

²⁹⁰ Küzeci, a.g.e., s. 408; Göçmen Uyarer, a.g.e., s. 227.

veya anonim hâle getirmeyenler 5237 sayılı Kanununun 138 inci maddesine göre cezalandırılır.” şeklinde bir düzenleme bulunmaktadır. Buna göre KVKK'nın “Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi” başlıklı 7. maddesinde yer alan hükümlere aykırılık halinde de TCK m. 138 uygulanacaktır.

B. KORUNAN HUKUKSAL DEĞER

Suç ile kamu idaresinin güvenliği ve işleyişinin korunduğu yönünde görüşler²⁹¹ mevcut olsa da, bu suç tipi ile korunan hukuksal değer, incelenen diğer suç tipleri ile aynı şekilde, kişisel verilerin korunması hakkı olduğu kanaatindeyiz. Bir diğer görüşe göre ise bu suç ile kişisel verilerin korunma hakkı yanında unutulma hakkı da korunmaktadır²⁹². Yargıtay Hukuk Genel Kurulu'nun bir kararında unutulma hakkı konusunda şu açıklamalar yapılmıştır:

“...unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır.

Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlenmesini isteme hakkı olarak ifade edilebilir.

Bu hak bir yandan kişiye “geçmişini kontrol etme”, “belirli hususların geçmişinden silinmesini ve hatırlanmamayı isteme hakkı” sağladığı gibi, diğer yandan muhataplarına kişi hakkındaki bir kısım bilgilerin üçüncü kişilerin kullanmamasını veya üçüncü kişilerin hatırlanmamasına yönelik önlemleri alma yükümlülüğü yükler. Bu hakkın; bireylerin fotoğraf, internet günlüğü gibi kendileri hakkındaki içerikleri silmek için üçüncü şahısları zorlamayı içermesinin yanında geçmişteki cezalarına ilişkin bilgilerin veya haklarında olumsuz yorumlara neden olabilecek bilgi ve fotoğraflarının kaldırılmasını isteme hakkını tanıdığı kabul edilmektedir. Diğer taraftan bu hak, bireyin geçmişindeki belirli yönlerinin mümkün olmayacak biçimde hatırlanmaması için önlemler alınmasını gerektirmektedir.”²⁹³

²⁹¹ Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 719; Soyaslan, a.g.e., s. 350.

²⁹² Yokuş Sevük, a.g.e., s. 258.

²⁹³ HGK, 17.06.2015, E. 2014/4-56, K. 2015/1679, www.kazanci.com, (01.12.2019).

Bu açıklamalar göz önüne alındığında kişisel verilerin yok edilmesi ile unutulma hakkının bağlantılı olduğu görülmektedir. Bu sebeple unutulma hakkının da kişisel verilerin korunması hakkı ile birlikte, bu suç ile korunan hukuksal değer olduğu yönündeki görüşe katılmaktayız.

C. SUÇUN UNSURLARI

Bu bölümde tipiklik ve hukuka aykırılık unsuru başlıkları altında kişisel verilerin kaydedilmesi suçunun unsurları incelenecektir.

1. Tipiklik

Tipiklik başlığı altında, suç tipinin genel özelliklerinden bahsedildikten sonra verileri yok etmeme suçunun maddi ve manevi unsurları konusunda açıklamalara yer verilecektir.

a. Suç tipinin genel özellikleri

Verileri yok etmeme suçunu düzenleyen 138. maddenin birinci fıkrasında “*Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde*” uygulanacak cezaya yer verilmiştir. İkinci fıkrasında ise “*Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde*” artırılarak ceza verilmesi gerektiğine ilişkin düzenleme bulunmaktadır.

Verileri sistem içinde yok etmekle yükümlü olanların görevlerini yerine getirmeyip, bu işlemi yapmamaları halinde suç olduğundan bu suç, ihmali hareket ile işlenebilen bir suçtur. Verileri yok etmeme suçu gerçek ihmali suçtur²⁹⁴. Suç kişisel verilerin yok edilmemesi ile gerçekleşecek olup ayrıca bir netice aranmadığından sırf hareket suçu niteliğine sahiptir. Suçun tamamlanması için, bir zarar doğmasa bile, yükümlülüğe aykırı şekilde verilerin yok edilmemesi yeterli olduğundan bir tehlike

²⁹⁴ Akdağ, a.g.e., s. 146; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 156.

suçudur. Ayrıca hareketin somut bir tehlikeye sebep olması da kanunda aranmadığından soyut tehlike suçudur²⁹⁵. Verileri yok etmeme suçu mütemadi bir suçtur. Kanunlarda belirlenen sürenin geçmesiyle verileri yok etmeme suçu tamamlanır. Ancak suç, verileri yok etmekle yükümlü kişiler görevlerini yerine getirene kadar devam eder, bu görev yerine getirildiğinde ise sona erer²⁹⁶.

b. Suçun maddi unsurları

Verileri yok etmeme suçunun maddi unsurları; fail, mağdur, suçun konusu, hareket ve nitelikli unsurlardan oluşmaktadır. Bu suç bakımından sayılan her bir unsur konusunda değerlendirme yapılarak suç tipi detaylı olarak incelenecektir.

(1) Fail

Fail olabilmek için, bu suçu işleyen kişinin verileri sistem içinde yok etmekle yükümlü olması gerekmektedir. Öyleyse kanun, fail için özel bir nitelik aramaktadır. Bu nedenle bu suç özgü suçtur. Özgü suç olması sebebiyle herkes bu suçun faili olamayacaktır. Kişinin kamu görevlisi olup olmaması bu suç bakımından bir özellik arz etmez²⁹⁷.

KVKK m. 7’de; “*kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir*” ifadesi yer almaktadır. Buna göre KVKK m. 17/2’de yer alan suçun faili veri sorumlusu olacaktır²⁹⁸. Veri sorumlusu KVKK’nın 3. maddesinde “*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*” olarak tanımlanmıştır. Veri Sorumluları Sicili Hakkında Yönetmelik’in 11. maddesinin 1. fıkrasında ise veri sorumlusu ile ilgili olarak “*Tüzel kişilerde veri sorumlusu tüzel kişiliğin kendisidir. Türkiye’de yerleşik olan tüzel kişilerin Kanun kapsamındaki veri sorumlusu yükümlülükleri, ilgili mevzuat hükümlerine göre tüzel*

²⁹⁵ Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 603; Yokuş Sevik, a.g.e., s. 260.

²⁹⁶ Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 725; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 157.

²⁹⁷ Yokuş Sevik, a.g.e., s. 259

²⁹⁸ Korkmaz, a.g.e., s. 431.

kişiliği temsil ve ilzama yetkili organ veya ilgili mevzuatta belirtilen kişi veya kişiler marifetiyle yerine getirilir. Tüzel kişiliği temsile yetkili organ, Kanunun uygulanması bakımından yerine getirilecek yükümlülükler ile ilgili olarak bir veya birden fazla kişiyi görevlendirebilir. Bu görevlendirme Kanun hükümleri uyarınca tüzel kişiliğin sorumluluğunu ortadan kaldırmaz.” düzenlemesine yer verilmiştir. Bu düzenlemelere göre, veri sorumlusu gerçek kişiyse, fail bu kişi olacaktır. Ancak veri sorumlusunun tüzel kişi olması durumunda, veri sorumlusunun yükümlülüklerini yerine getirmekle görevlendirilecek kişi veya kişiler bu suç bakımından fail olacaktır. Ancak veri sorumlusunun görevlendirdiği gerçek kişinin fail olması veri sorumlusunun sorumluluğunu ortadan kaldırmayacaktır. Bu durumda tüzel kişiye ceza verilemeyeceğinden veri sorumlusu fail olamayacaksa da, hakkında güvenlik tedbiri uygulanması mümkün olabilecektir (TCK m. 20).

(2) Mağdur

Verileri yok etmeme suçunun mağdurunun kim olduğu konusunda da suçla korunan hukuksal değer konusunda yaşanan görüş ayrılığı söz konusudur. Suçla korunan hukuksal değer kamuya idaresine duyulan güven olduğu görüşünü savunanlara göre, suçun mağduru kamudur. Buna göre kişisel verileri yok edilmeyen kişi ise bu suç bakımından mağdur değil, suçtan zarar gören olabilir²⁹⁹. Ancak bizim de katıldığımız görüşe göre bu suçun mağduru, sistemde kişisel verileri kayıtlı olan gerçek kişilerdir³⁰⁰. Tüzel kişiler bu suç bakımından da mağdur olamayacak, ancak suçtan zarar gören olabileceklerdir.

KVKK m. 17/2 açısından mağdur ise, kişisel verilerinin işlenmesini gerektiren sebepler ortadan kalkmasına rağmen, verileri yok edilmemiş, silinmemiş ya da anonim hale getirilmemiş kişidir.

²⁹⁹ Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 720; Soyaslan, a.g.e., s. 350.

³⁰⁰ Yokuş Sevük, a.g.e., s. 259; Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 602; Artuç, a.g.e., s. 1686.

(3) Suçun konusu

Verileri yok etmeme suçunun konusu, sistemde kayıtlı bulunan “kişisel veriler”dir. Ancak madde gerekçesinde de görüleceği üzere bu kişisel verilerin hukuka uygun olarak kaydedilmiş olmaları gerekmektedir³⁰¹. Yok edilmesi gereken kişisel veriler ile ilgili, kanunlarda bir sürenin öngörülmesi olması gerektiği ve bu verileri silmekle görevli kişilerin bulunduğu göz önüne alındığında, bu maddenin hukuka aykırı olarak kaydedilmiş veriler için değil, yalnızca hukuka uygun olarak kaydedilmiş kişisel veriler için uygulama alanı bulacağı açıktır.

Ayrıca düzenlemede sistemde kayıtlı bulunan veriden bahsedilmektedir. Burada geçen “sistem”in otomatik ya da otomatik olmayan her türlü veri kayıt sistemi olarak anlaşılması gerektiği kanaatindeyiz. Veri kayıt sistemi ise KVKK’da “*kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi*” olarak tanımlanmıştır (KVKK m. 3/1-h). Suçun ikinci fıkrasında yer alan nitelikli hal bakımından suçun konusu ise, “Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri”dir. KVKK m. 17/2 açısından ise suçun konusu kanun hükümlerine uygun olarak işlenmiş kişisel verilerdir.

(4) Hareket

Kanunların belirlediği süre geçtiği halde verileri sistem içinde yok etmekle görevli olanların bu görevlerini yerine getirmemesi, bu suçun hareket unsurunu oluşturmaktadır. KVKK m. 17/2 açısından hareket ise, kanun hükümlerine uygun olarak işlenmiş kişisel verilerin, işlenmesini gerektiren sebeplerin ortadan kalktığı halde resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmemesi, yok edilmemesi veya anonim hâle getirilmemesidir.

TCK m. 138 kapsamında suçun oluşması için kanunların belirlediği sürelerin geçmiş olması ve failin verileri yok etmekle görevli olması gerekmektedir. Burada sözü edilen kanun hem maddi hem de şekli anlamda kanundur. Yani bu bir kanun olabileceği gibi, bir yönetmelik de olabilecektir³⁰².

³⁰¹ Yokuş Sevük, a.g.e., s. 259.

³⁰² Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 602.

Maddede bahsedilen, kanunlarca belirlenmiş sürenin 7 gün ya da 2 ay gibi somut bir süre olması mümkündür. Ancak bu şekilde somut bir süre belirlenmemiş de olabilir. Kanunda somut bir süre yerine bir kararın verilmesi durumunda yok edilmesi gerektiğine ilişkin hüküm de yer alabilir. Böyle ifadeler de süre kavramının içinde değerlendirilecek ve kanunda belirtilen durum gerçekleştiğinde verilerin silinmesi gerekecektir³⁰³.

Suçun oluşması için aranan bir diğer şart failin verileri yok etmekle görevli olmasıdır. Bu hususun failin görev alanına girip girmediği kanun ya da yönetmeliklerde yazılı olabileceği gibi, veri işleyen kurumun işleyişinden, iş bölümünden de anlaşılabilir³⁰⁴.

28 Ekim 2018 tarih ve 30224 sayılı Resmi Gazete’de yayınlanan “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik”in 9. maddesinde kişisel verilerin yok edilmesinin tanımı yapılmıştır. Buna göre kişisel verilerin yok edilmesi, “*kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.*”. KVKK m. 7’nin gerekçesinde ise verilerin yok edilmesi “*Verilerin yok edilmesi ise, bilgilerin tekrar geri getirilemeyecek ve kullanılmayacak şekilde, verilerin kaydedildiği evrak, dosya, CD, disket, hard disk gibi veri saklamaya elverişli materyallerin imha edilmesini ifade etmektedir*” şeklinde tanımlanmıştır. Kişisel verilerin geri getirilemez hale getirilmesi; veriler bilişim sistemindeyse bu bilgilerin geri getirilemeyecek şekilde tamamen silinmesi ya da kağıt üzerindelerse belgenin yakılması şeklinde gerçekleşebilir³⁰⁵. Verilerin silinmesi için kanunda belirlenen süre geçtikten sonra ancak yetkili makamlar verilerin yok edilmediğini öğrenmeden önce, verilerin yok edilmesi halinde bile fail bu suçtan sorumlu olacaktır. Çünkü veriler sonradan yok edilmiş olsalar da kanunda belirlenen süre içinde yok edilmemiş olacaktır³⁰⁶.

KVKK m. 17/2’ye göre kişisel verilerin silinmemesi ya da anonim hale getirilmemesi de, TCK m. 138 kapsamında ceza verilmesini gerektiren bir suç olduğundan, verilerin silinmesi ve anonim hale getirilmesi fiillerinin de açıklanması gerekmektedir. “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi

³⁰³ a.g.e.

³⁰⁴ Akdağ, a.g.e., s. 147.

³⁰⁵ Korkmaz, a.g.e., s. 429.

³⁰⁶ Artuç, a.g.e., s. 1689.

Hakkında Yönetmelik”in 8. maddesinde kişisel verilerin silinmesi “*kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi*” olarak tanımlanmıştır. Görüldüğü gibi, kişisel verilerin yok edilmesi durumunda verilerin, hiç kimse tarafından hiçbir şekilde erişilemez ve geri getirilemez duruma getirilmesi söz konusu iken, kişisel verilerin silinmesi durumunda yalnızca ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz hale getirme söz konusudur. Burada sözü edilen ilgili kullanıcılar ise aynı Yönetmelik’in 4. maddesinde “*verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler*” şeklinde tanımlanmıştır.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’in 10. maddesinde, kişisel verilerin anonim hale getirilmesi; “*kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi*” olarak tanımlanmıştır. Kişisel verilerin anonim hale getirilmiş olduğunun kabulü için gerekenler aynı maddenin ikinci fıkrasında, “*Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.*” şeklinde ifade edilmiştir.

KVKK’da “*kişisel verilerin İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi*” ilkesine yer verilmiştir (KVKK m. 4/1-d). Bu “*işlendikleri amaç için gerekli olan süre*” ifadesi ile ilgili olarak ise Veri Sorumluları Sicili Hakkında Yönetmelik’in ilgili hükümlerinin incelenmesi gerekmektedir. Yönetmelik m. 9/5’te “*Veri sorumluları, kişisel verilerin işlendikleri amaç için gerekli olan azami sürenin belirlenmesi, bu sürelerin kişisel veri işleme envanterinde belirtilen bilgilerle uyumu ve azami sürenin aşılmamasının takibi için kişisel veri saklama ve imha politikası hazırlayarak, bu politikanın uygulanmasını temin ederler.*” ifadelerine yer verilmiştir. Buna göre Veri Sorumluları Sicili’ne kayıt olma yükümlülüğü altında bulunan veri sorumluları, kanunlarda süre bulunmaması durumunda; işledikleri kişisel verilerin işlenme amaçları için gereken süreyi belirleyerek, kişisel veri saklama ve imha politikası hazırlayacaklardır. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale

Getirilmesi Hakkında Yönetmelik m. 11/1'e göre "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 siler, yok eder veya anonim hale getirir". Periyodik imhanın gerçekleştirileceği zaman aralığı ise veri sorumlusunca "kişisel veri saklama ve imha politikasında" belirlenecek ancak bu süre altı ayı geçemeyecektir (Yönetmelik m. 11/2). Bu saklama ve imha politikasını hazırlamakla yükümlü olmayan veri sorumlusu ise "kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde kişisel verileri siler, yok eder veya anonim hale getirir" (Yönetmelik m. 11/3). Bu düzenlemelere bakıldığında; kişisel verilerin yok edilmesi, silinmesi ya da anonim hale getirilmesi işlemlerinden hangisinin uygulanacağı kararının veri sorumlusunun tasarrufunda olduğu anlaşılmaktadır.

KVKK m. 7'de veri sorumlusunun veriyi re'sen imha etmesinin yanında, veri sahibinin talebiyle imha edilmesine ilişkin olarak da düzenleme yapılmıştır. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 12'de buna ilişkin olarak "(1) İlgili kişi, Kanunun 11 inci ve 13 üncü maddelerine istinaden veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Veri sorumlusu, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanunun 13 üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir." şeklinde düzenlemeye yer verilmiştir. Bu düzenlemeye göre kişinin talebinin reddedilmesi ya da kabul edilmesi fark etmeksizin, veri sahibinin başvurusunun 30 gün içinde sonuçlandırılması zorunludur. Kanun koyucu

ilgili maddenin c bendine işleme şartları ortadan kalkmamışsa gerekçesi açıklanmak suretiyle talebi reddetme imkanı verdiğine göre, bu madde kapsamında veri sorumlusunun talebi tamamen reddetmek yerine gerekçesini açıklayarak talepten farklı bir işlem yapmasının mümkün olabileceğini söylemek de mümkün olacaktır. Örneğin ilgili kişi kişisel verilerinin yok edilmesini isterken veri sorumlusunun, bu talebi reddederek bunun yerine yok etmeme gerekçesini bildirerek veriyi anonim hale getirmekle yetinmesinin de mümkün olabileceği kanaatindeyiz.

(5) Nitelikli unsurlar

Suçun nitelikli hali maddenin ikinci fıkrasında “*Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.*” şeklinde düzenlenmiştir. Buna göre nitelikli halin hangi durumlarda uygulanacağını tespiti için CMK’nın ilgili maddelerini incelemek gerekmektedir.

CMK m. 80’de yer alan “Genetik inceleme sonuçlarının gizliliği” başlıklı maddeye göre, “75, 76 ve 78 inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde”dir ve “kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilir.”.

“Fizik kimliğin tespiti” başlıklı CMK’nın 81. maddesine göre ise, “üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın, kimliğinin tespiti için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup tespitini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınabilir”, bu kayıtlar “kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde” Cumhuriyet savcısının huzurunda derhâl yok edilecektir.

“İletişimin tespiti, dinlenmesi ve kayda alınması” başlıklı CMK135. maddede “Şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda

alınmaz. Kayda alma gerçekleşikten sonra bu durumun anlaşılması hâlinde, alınan kayıtlar derhâl yok edilir.” ifadesi yer almaktadır. “Kararların yerine getirilmesi, iletişim içeriklerinin yok edilmesi” başlıklı CMK 137. maddede ise “135 inci 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 edilerek, durum bir tutanakla tespit edilir.” şeklinde düzenleme yer almaktadır. “Gizli soruşturmacı görevlendirilmesi” başlıklı CMK 139. maddede soruşturmacı görevlendirilmesi yolu ile edinilen kişisel bilgilerin suçla bağlantılı olmayanlarının derhal imha edileceği hükmü yer almaktadır. “Teknik araçlarla izleme” başlıklı CMK 140. maddede de elde edilen delillere, ceza kovuşturması için ihtiyaç duyulmaması durumunda, bu delillerin Cumhuriyet savcısının denetiminde hemen yok edileceği belirtilmiştir.

Sayılan CMK maddelerinde belirtilen süreler içinde kişisel verilerin yok edilmemesi durumunda faile suçun nitelikli halinden ceza verilecektir. Bu konuda değinilmesi gereken bir husus da kanunda derhal yok edilir gibi belirsiz süreler bulunması durumunda sürelerin nasıl belirleneceğidir. Bu durumda, somut olaya göre makul sürede verilerin yok edilmesi aranacaktır; ama bu makul sürenin çok uzun olmaması önemlidir³⁰⁷. Ancak kanunlarda bu gibi belirsiz ifadelerin yer alması sürenin ne zaman geçeceği, suçun ne zaman oluşmuş sayılacağı gibi konularda farklı uygulamalara ve uygulamada keyfiliklere sebep olabilecek bir durumdur.

c. Suçun manevi unsuru

Verileri yok etmeme suçu doğrudan kastla işlenebilen bir suçtur, kanunda özel bir amaç ve saik aranmamıştır. Bu durumda failin suçun tanımında yer alan maddi unsurları bilerek ve isteyerek hareket etmesi yeterlidir³⁰⁸. Bu suç tipinin olası kastla da işlenmesi mümkündür. Ancak kanunda taksire ilişkin düzenleme yer olmadığından, taksirle işlenmesi mümkün değildir³⁰⁹.

³⁰⁷ Artuç, a.g.e., s. 1688.

³⁰⁸ a.g.e., s. 1689.

³⁰⁹ Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 604.

TCK m. 30/1'e göre "*Fiilin icrası sırasında suçun kanuni tanımındaki maddi unsurları bilmeyen bir kimse, kasten hareket etmiş olmaz. Bu hata dolayısıyla taksirli sorumluluk hali saklıdır*". Bu durumda verileri yok etmekle görevli kişi, verilerin kişisel veri olmadığı düşüncesiyle hareket etmiş ve verileri yok etmemişse kastı ortadan kalkacak ve bu suçun taksirli hali de düzenlenmediğinden verileri yok etmeme suçundan sorumlu olmayacaktır³¹⁰.

2. Hukuka Aykırılık Unsuru

Verileri yok etmeme suçu açısından kanunda özel bir hukuka uygunluk nedeni bulunmamaktadır. İncelenen diğer iki suçtan farklı olarak ilgilinin rızası bu suçu hukuka uygun hale getirmeyecektir. Verilerin yok edileceği süreler ile ilgili kanunlarda emredici hükümlerin bulunması sebebiyle, mağdurun rızası olsa bile emredici hükümlere aykırılık söz konusu olacağından, hareketin hukuka uygun hale gelmesi mümkün değildir³¹¹. Ancak KVKK m. 17/2 için ilgilinin rızasının hukuka uygunluk sebebi olarak kabul edilebileceği kanaatindeyiz.

KVKK m. 7/2'de "*kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır*" hükmü yer almaktadır. Bu düzenlemeye göre başka kanunlarda kişisel verilerin imha edilmemesi yönünde bir düzenleme bulunması durumunda veri sorumlusunun, veri sahibinin talebi üzerine ya da re'sen kişisel verileri imha etmemesi suç oluşturmayacaktır.

D. KUSUR

Kusurluluğu kaldıran bir sebep olan zorunluluk halinin uygulanması bu suç için mümkün olabilecektir. Örneğin verileri yok etmekle görevli kişi, verileri yok etmek için gitmesi gereken yere burada yaşanan yoğun şiddet olayları sebebiyle ulaşamıyorsa ve kanunda belirtilen süre geçmeden verileri yok etme imkanına sahip değilse, zorunluluk hali sebebiyle bu kişiye ceza verilmez (TCK m. 25/2).

³¹⁰ Özgenç, Üzülmez, a.g.e., s.104; Artuk, Gökçen, Yenidünya, a.g.e., s. 522; Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 170.

³¹¹ Sert, a.g.e., s. 165; Özbek vd., *Türk Ceza Hukuku Özel Hükümler*, s. 604.

Kurtulma imkanı bulunmayan cebir ve şiddet ya da ağır tehdit altında bu suçu işleyen kişiye de ceza verilmeyecektir. Ancak bu durumda TCK m. 28'e göre cebir ya da tehdidi kullanan kişi dolaylı fail olarak sorumlu olacaktır.

Haksız tahrik halinin varlığı durumunda suçun işlenmesi söz konusu olduğunda ise TCK m. 29'a göre kişiye verilecek ceza indirilecektir.

Sayılan haller dışında, şartlarının varlığı halinde, kusurluluğu etkileyen diğer haller olan; yaş küçüklüğü, akıl hastalığı, sağır dilsizlik ve alkol ve uyuşturucu madde etkisinde olma halleri konusundaki genel hükümler, bu suç için de uygulanabilecektir.

Ayrıca kusurluluğu etkileyen, kaçınılmaz bir haksızlık yanılığası olması durumunda da kişinin kusurlu sayılması mümkün olmayacak ve fiilinden dolayı sorumlu tutulamayacaktır³¹².

E. SUÇUN ÖZEL GÖRÜNÜM ŞEKİLLERİ

1. Teşebbüs

Verileri yok etmeme suçu ihmal suretiyle işlenen bir suç olduğundan bu suça teşebbüs mümkün değildir³¹³.

2. İştirak

Bu suça iştirak mümkündür. Ancak özgü suç niteliğine sahip bir suç olduğundan, verileri yok etmekle görevli olmayan kişiler fail olmayacak; ancak azmettiren ya da yardım eden olarak suça katılabileceklerdir (TCK m. 40/2)³¹⁴. KVKK m. 17'de yer alan suçun failinin veri sorumlusu olması gerektiğinden, bu suç da özgü suçtur ve bu sebeple veri sorumlusu sıfatına sahip olmayan kişiler, azmettiren ya da yardım eden olarak bu suça katılabileceklerdir. Veri sorumlusunun tüzel kişi olması durumunda bu kişinin bilinci, iradesi ve hareket yeteneği olmadığı açıktır³¹⁵. Bu sebeple tüzel kişinin fail olması mümkün olmadığı gibi azmettiren ya da yardım eden olması da mümkün değildir. Bu

³¹² Artuk, Gökçen, Yenidünya, a.g.e., s. 536.

³¹³ Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s.724.

³¹⁴ Yokuş Sevük, a.g.e., s. 261.

³¹⁵ Artuk, Gökçen, Yenidünya, a.g.e., s. 279.

durumda azmettiren ya da yardım eden, veri sorumlusunun yükümlülüklerini yerine getirmekle görevlendirilecek kişi veya kişiler olacaktır. Tüzel kişi veri sorumlusunun suça iştirak etmesi durumunda ise benzer şekilde fail tüzel kişi değil, veri sorumlusunun yükümlülüklerini yerine getirmekle görevlendirilecek gerçek kişi olacaktır.

3. İçtima

Bu suçun bir suç işleme kararının icrası dolayısıyla aynı kişiye karşı birden fazla kez işlenmesi durumunda zincirleme suç hükümleri uygulanabilecek ve verilecek ceza dörtte birinden dörtte üçüne kadar artırılabilecektir. Örneğin, bir kişiye ait ve farklı zamanlarda yok edilmesi gereken birden fazla kişisel verinin yok edilmemesi durumunda, zincirleme suç hükümlerinin uygulanması gerekecektir.

Ayrıca yok edilmesi gereken verilerin birden fazla kişiye ait olması durumunda aynı neviden fikri içtima da mümkün olacaktır ve bu durumda ceza zincirleme suç hükümlerine göre belirlenecektir.

Fail verileri yok etmeyip, bu verileri başkasına verir ya da yayarsa TCK m. 136 ve m. 138 arasında gerçek içtima hükümlerinin uygulanması gerekecektir³¹⁶.

TCK m. 257/2’de yer alan “*kanunda ayrıca suç olarak tanımlanan haller dışında, görevinin gereklerini yapmakta ihmal veya gecikme göstererek, kişilerin mağduriyetine veya kamunun zararına neden olan ya da kişilere haksız bir menfaat sağlayan kamu görevlisi*” ifadesi dolayısıyla bu madde, TCK m. 138 karşısında tali normdur. Bu durumda bir kamu görevlisinin görevi sistem içindeki verileri imha etmekken bu görevini yerine getirmiyorsa asli norm olan TCK m. 138 hükmü uygulanacaktır³¹⁷.

F. YAPTIRIM

Verileri yok etmeme suçu için kanunda “bir yıldan iki yıla kadar hapis cezası” öngörülmüştür. İkinci fıkraya göre “*Suçun konusunun Ceza Muhakemesi Kanunu*

³¹⁶ Artuç, a.g.e., s. 1690.

³¹⁷ Kangal, *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, s. 174.

hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması” durumunda ise “verilecek ceza bir kat artırılır”.

Cezanın alt sınırı bir yıl olduğundan, hapis cezası TCK m. 50’de yer alan seçenek yaptırımlara çevrilebilir. Saniğa verilecek cezanın iki yıl ya da daha az olması durumunda, şartlarının sağlanması halinde, hapis cezasının ertelenmesi ya da hükmün açıklanmasının geri bırakılması da mümkün olabilecektir.

Bu suç dolayısıyla kişiye hapis cezası verilmesi durumunda, kişi hakkında TCK m. 53’te yer alan hak yoksunlukları uygulanacaktır. Ayrıca TCK m. 140 gereğince, bu suçun işlenmesi dolayısıyla hukuka aykırı yarar sağlayan tüzel kişiler bakımından TCK 60. maddede yer alan bunlara özgü güvenlik tedbirlerine hükmolunacaktır.

Verileri yok etmeme suçu için verilecek hapis cezası beş yılı aşmadığından TCK m. 66/1’e göre dava zamanaşımı sekiz yıldır, TCK m. 68/1’e göre ceza zamanaşımı ise on yıldır.

G. MUHAKEMEYE İLİŞKİN KURALLAR

TCK m. 139 hükmü gereğince bu suç için soruşturma ve kovuşturma şikayete bağlı değildir, resen yapılır. Kamu görevlileri bakımından, görevleri dolayısıyla suç işlemleri durumunda 4483 sayılı Kanun gereğince soruşturma yapılabilmesi için yetkili makamdan izin alınması gerekecektir.

CMK m. 253’te uzlaştırma hükümlerinin uygulanacağı suçlar sayılmıştır. Buna göre uzlaştırma hükümlerinin uygulanabilmesi için, suçun şikayete tabi olması ya da maddede sayılan suçlardan olması gerekmektedir. Verileri yok etmeme suçu için, şikayete tabi olmaması ve maddede sayılan diğer suçlar arasında da yer almaması sebebiyle uzlaştırma hükümleri uygulanamayacaktır.

Suç için belirlenen cezanın üst sınırı göz önüne alındığında, 5235 sayılı Kanun uyarınca görevli mahkeme asliye ceza mahkemesidir³¹⁸. Yetkili mahkeme ise CMK m. 12/1 hükmüne göre suçun işlendiği yerde bulunan mahkemedir. Suçun işlendiği yerin

³¹⁸ Yokuş Sevük, a.g.e., s. 258.

belirlenmemesi durumunda ise CMK m. 13'te yer alan özel yetki kuralları uygulanacaktır.



SONUÇ

Kişisel veri, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” şeklinde tanımlanır. Bu durumda, kişisel veriden bahsedebilmemiz için öncelikle bir kişi ile ilgili bir veri bulunmalı, bu kişi bir gerçek kişi olmalı ve bu kişinin kimliği belirli veya belirlenebilir olmalıdır. Hassas veri ise, kişisel verilerin daha fazla korunması gereken alanını oluşturur. Kişilerin “ırkı ve etnik kökeni, ten rengi, siyasi görüşleri, dini ve felsefi inançları, sendika üyelikleri, sağlık ve cinsel yaşamı ve mahkumiyetlerini” içeren bilgiler diğer bilgilere göre daha özel nitelikte olduklarından hassas veri olarak adlandırılırlar.

Günümüzde bilginin değeri oldukça fazladır ve devletler veya özel hukuk tüzel kişileri tarafından bilgi toplama faaliyetleri sıklıkla gerçekleştirilmektedir. Devletler, vatandaşlarının güvenliğini sağlamak ve ihtiyaçlarını gidermek amacıyla birtakım verileri toplamakta, özel hukuk tüzel kişileri ise müşterilerine sağladıkları hizmetlerin kalitesini kontrol edebilmek ve müşterileri hakkında bilgi sahibi olabilmek için kişisel verileri toplamaktadırlar. Bunun yanında ekonomik bir faaliyet olarak bilgilerin üçüncü kişilere satılması da söz konusu olmaktadır. Kişisel verilerin böyle bir öneme sahip olduğu bu ortamda verilerin korunması; veri sahiplerinin kişiliklerini geliştirebilmesi, verileri üzerinde söz hakkına sahip olabilmesi ve temel hak ve özgürlüklerin korunması açısından önemlidir. Kişisel verilerin gerekli şekilde korunmadığı bir ortamda, insan hakları ve onuru ile bağdaşmayan durumların oluşması mümkün olabilecektir. Bu sebeple kişisel verilerin korunması son derece önemli bir gereksinimdir.

Bugünkü anlamda kişisel verilerin korunması kavramı, verilerin otomatik işlenmesi ile ortaya çıkmışsa da tarihte hekim, din adamı, avukat ve bankacı gibi mesleklerin sır saklama yükümlülüklerinin olması kişisel verilerin korunması kavramının temellerinin günümüzden çok daha eski zamanlara dayandığını göstermektedir.

1960’lardan itibaren verilerin depolanması ve toplanmasının daha kolay hale gelmesi ile birlikte, kişisel verilerin korunması gereksinimi ortaya çıkmıştır. Kişisel verilerin korunması amacıyla, uluslararası ve ulusal pek çok düzenleme yapılmıştır. Dünyada ilk veri koruma kanunu örneği ise 1970 yılında Almanya’nın Hessen eyaletinde çıkarılmıştır. Bundan sonra 1973’te İsveç’te verilerin korunmasına dair kanun, 1974’te ise ABD’de özel alanın korunmasına ilişkin kanun kabul edilmiştir. Diğer ülkelerde de kişisel verilerin korunduğu düzenlemeler bulunmaktadır. Uluslararası alanda ise OECD

kişisel verilerin korunması konusunda ilk adımı atmış, 1980 yılında Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler'i kabul etmiştir. OECD dışında Birleşmiş Milletler, Avrupa Konseyi, Avrupa Birliği ve Asya-Pasifik Ekonomik İş Birliği bünyesinde de kişisel verilerin korunmasına ilişkin düzenlemeler yapılmıştır.

Kişilerin temel hak ve özgürlüklerinin korunması konusunda en önemli belgelerden olan Avrupa İnsan Hakları Sözleşmesi, kişisel verilerin korunması hakkına özel olarak yer vermemiş olsa da, bu hak özel hayata ve aile hayatına saygı hakkını düzenleyen 8. madde kapsamında korunmaktadır. Avrupa İnsan Hakları Mahkemesi'nin bu yönde pek çok kararı mevcuttur.

Ülkemizde kişisel verilerin korunması hakkı 2010 yılına kadar anayasal bir korumaya sahip değildi. 2010 yılında yapılan Anayasa değişikliği sonrasında Anayasa'nın 20. maddesine eklenen üçüncü fıkra ile kişisel verilerin korunması hakkı Anayasa'da yer almış ve anayasal korunmaya kavuşmuştur. Anayasa'nın yanında Türk Medeni Kanunu, Ceza Muhakemesi Kanunu, İş Kanunu ve Türk Ceza Kanunu gibi pek çok kanunda ve yönetmelikte kişisel verilerin korunmasına yönelik hükümler yer almaktadır. Bunlar dışında 2016 yılında mevzuatımıza dahil olan 6698 sayılı Kişisel Verilerin Korunması Kanunu bu alandaki büyük bir eksikliği gidermiştir.

Çalışmamızda kişisel verilerin korunması incelenmiş, genel açıklamaların ardından özellikle ceza hukuku kapsamında kişisel verilerin korunması konusunda bir çalışma yapıldığından, Türk Ceza Kanunu'nda düzenlenen suçlar, unsurlarıyla birlikte detaylı olarak açıklanmıştır. Kişisel Verilerin Korunması Kanunu'nun 17. maddesi suçlar bakımından Türk Ceza Kanunu'nun 135-140. maddelerinin uygulanacağını belirtmiştir. Kişisel verilere yönelik suçlar bakımından cezai yaptırım ancak sayılan maddelerin uygulanması ile söz konusu olabileceğinden, Türk Ceza Kanunu'nun 135. maddesinde yer alan "Kişisel verilerin kaydedilmesi" suçu, 136. maddesinde yer alan "Verileri hukuka aykırı olarak verme veya ele geçirme" suçu ve 138. maddesinde yer alan "Verileri yok etmeme" suçu kişisel verilerin korunması açısından önemli düzenlemelerdir.

TCK kapsamında yer alan kişisel verilerin korunmasına yönelik suçlar, önemleri sebebiyle tez çalışmamız boyunca çeşitli açılardan eleştirilmiştir. TCK kapsamında kişisel veri kavramının tanımına yer verilmemiş olması bu eleştirilerimizin başında

gelmektedir. “Belirli veya belirlenebilir bir kişiye ilişkin her türlü veri” tanımının kapsamına girebilecek verilerin çok çeşitli olması, TCK’da kişisel verilerin düzenlendiği suçların çok geniş bir alanda uygulanması anlamına gelmekle beraber belirliliği de ortadan kaldırmaktadır. TCK’nın uygulama alanındaki kişisel veri kavramının sınırlarının çok fazla genişletilerek ceza hukukunun son çare olması ilkesi ile bağdaşmayan bir durumun ortaya çıkmasının da engellenmesi açısından, kişisel verilerin TCK kapsamında tanımının yapılması gerekmektedir.

TCK m. 135/2’de sayılan hassas veriler ile KVKK m. 6/1’de sayılan hassas verilerin aynı olmaması, TCK’nın KVKK’ya göre daha az veriyi hassas veri olarak düzenlemiş olması da eleştirilen bir diğer noktadır. TCK m. 135 hükmünün KVKK’dan çok daha önce getirilmiş olması sebebiyle böyle bir uyumsuzluğun ortaya çıkması normal kabul edilebilirse de, KVKK’nın kabulünden sonra burada sayılan hassas nitelikteki kişisel verilerin de gereken özel korumadan yaralanabilmesi için bu iki düzenlemenin uyumlu hale getirilmesi önemlidir.

TCK m. 136 ve 138 bakımından ortak eleştiri konusu olan husus madde başlıklarıdır. Her iki maddede de kişisel verilere yönelik suçlar düzenleniyor olsa da, madde başlıklarında kişisel veri yerine veri kavramı yer almaktadır. Kanunun uygulanması bakımından bu durum bir sorun oluşturmasa da, her iki maddenin başlığında veri yerine kişisel veri ifadesinin kullanılması daha doğru bir yöntem olacaktır.

TCK m. 135’teki “kaydetme” fiili ile TCK m. 136’daki “ele geçirme” fiilleri kimi zaman iç içe geçebilecek çok yakın anlamlı kavramlardır. Bu iki kavramdan ne anlaşılması gerektiğine kanun maddelerinde yer verilmesinin, uygulama sırasında belirsizliklerin önlenmesi ve yanlış uygulamalar yapılmasının önüne geçilmesi bakımından önemli olduğu kanaatindeyiz.

Verileri yok etmeme suçunun TCK’da düzenlenmesi, kişisel verilerin belirli süre ile tutulması ilkesinin korunması bakımından önemlidir. Ancak bu ilkede kastedilen süre kişisel verilerin işleme amaçları için muhafaza edilmesi gereken süreyi ifade ederken, TCK m. 138’de verilerin yok edilmesi gereken süre kanunlarda belirtilen süreler olarak düzenlenmiştir. Bu durum da işleme amacı için gereken süre geçtiği halde, kanunlarda belirtilen sürelerin geçmemesi halinde kişisel verilerin gereğinden fazla sistemde tutulmasına sebep olabilecektir.

TCK m. 138 ile ilgili bir diđer husus ise kişisel verilerin imhasını düzenleyen kanunların bir kısmında belirli bir sürenin yer almamasıdır. Bu durum suçun ne zaman oluştuđuna karar verilmesi bakımından belirsizliklere sebep olabileceđi gibi, sürenin fazla uzatılması gibi durumlara da sebep olabilecektir. Kişisel verilerin imhası için kanunlarda bulunan sürelerin kesin süre şeklinde belirlenmesi bu gibi sakıncaların ortaya çıkmasını engelleyecektir.

Ceza hukuku ilkelerine uygunluđun tam olarak sağlanabilmesi ve kişisel verilerin korunması hakkının daha etkin şekilde korunabilmesi için Türk Ceza Kanunu'nda deđişiklik yapılmasını gerektiren hususlar mevcut olsa da; kişisel verilerin öncelikle 6698 sayılı Kişisel Verilerin Korunması Kanunu ile, sonrasında ise başta TCK olmak üzere çeşitli kanun ve yönetmelikler ile korunuyor olması ülkemizde kişisel verilerin korunması hakkının gelişmesi açısından oldukça önemlidir. Ülkemizde henüz yeni olan kişisel verilerin korunması hukuku zamanla geliştikçe, Kişisel Verileri Koruma Kurulu ve mahkeme kararları ile birlikte uygulama sırasında ihtiyaçlar fark edildikçe, bu alandaki düzenlemelerin daha etkin uygulanmasının sağlanması için gereken deđişikliklerin yapılacağı kanısındayız.

KAYNAKLAR

- AKBULUT Berrin, “Bağlılık Kuralı”, *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, ed. Vahit Doğan, İlhan Üzülmez, C. XIV, S. 1, Ankara: Gazi Üniversitesi Yayını, 2010, ss. 167-214.
- AKDAĞ Hale, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, 1. b., Ankara: Adalet Yayınevi, 2013.
- AKGÜL Aydın, “Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı””, *Türkiye Barolar Birliği Dergisi*, S.116, Ankara: Türkiye Barolar Birliği Yayını, 2015, ss. 11-38.
- AKİPEK Jale G., AKINTÜRK Turgut, ATEŞ KARAMAN Derya, *Türk Medeni Hukuku, Başlangıç Hükümleri – Kişiler Hukuku*, 9. b., İstanbul: Beta Yayıncılık, 2012.
- AKSOY Hüseyin Can, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, 1. b., Ankara: Çakmak Yayınevi, 2010.
- Ankara HBV Üniversitesi Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, *Türk Ceza Hukuku Mevzuatı – Cilt 1 (Kanunlar)*, 23. b., Ankara: Seçkin Yayıncılık, 2019.
- ARTUÇ Mustafa, *Kişilere Karşı Suçlar*, 2. b., Ankara: Adalet Yayınevi, 2018.
- ARTUK Mehmet Emin, GÖKCEN Ahmet, YENİDÜNYA Ahmet Caner, *Ceza Hukuku Genel Hükümler*, 7. b., Ankara: Adalet Yayınevi, 2013
- AYAN Mehmet, AYAN Nurşen, *Kişiler Hukuku*, 8. b, Ankara: Seçkin Yayıncılık, 2016.
- AYDIN Nizamettin, “Tıp Ceza Hukukunda Verileri Hukuka Aykırı Olarak Verme ve Ele Geçirme Suçu (TCK m. 136.)”, *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, ed. İbrahim Ercan, Ümit Süleyman Üstün, Mustafa Arıkan, C. 21, S. 2, Konya: Selçuk Üniversitesi Yayını, 2013, ss. 7-30.
- AYDIN Sedat Erdem, *AIHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu*, 1. b., İstanbul: On İki Levha Yayıncılık, 2015.
- BAYRAKTAR Köksal, “Kişisel Verilerin Kaydedilmesi, Verilmesi, Ele Geçirilmesi ve Yok Edilmemesi”, *Özel Ceza Hukuku, Cilt III: Hürriyete, Şeref, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar (TCK m. 106-140)*, Köksal Bayraktar vd., İstanbul: On İki Levha Yayıncılık, 2018.
- BEYTAR Erbil, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 2. b., İstanbul: On İki Levha Yayıncılık, 2018.
- BOZ Ahmet, *Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri*, (Yüksek Lisans Tezi), Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2014.

- BOZKURT YÜKSEL Armağan Ebru, *Bulut Bilişimde Kişisel Verilerin Korunması (Personal Data Protection in Cloud Computing)*, 1. b., Ankara: Yetkin Yayınları, 2016.
- BÜK Alaattin, *Bilişim Alanında Kişisel Verilerin Korunması*, 1. b., Ankara: Seçkin Yayıncılık, 2018.
- ÇOKMUTLU Metin, *Türk Ceza Hukukunda Kişisel Verilerin Korunması*, (Doktora Tezi), Kocaeli: Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, 2014.
- DAĞ Güray, *Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması*, (Doktora Tezi), İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2011.
- DİNÇ Engin, *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye'nin Durumu*, (Yüksek Lisans Tezi), Diyarbakır: Dicle Üniversitesi Sosyal Bilimler Enstitüsü, 2006.
- DÜLGER Murat Volkan, *Bilişim Suçları ve İnternet İletişim Hukuku*, 6. b., Ankara: Seçkin Yayıncılık, 2015.
- DÜLGER Murat Volkan, "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, C. 3, S. 6, İstanbul: İstanbul Medipol Üniversitesi Yayını, 2016, ss. 101-167.
- ERDOĞAN Yavuz, "Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi (Madde 135, 136, 137, 138)", *Erciyes Üniversitesi Hukuk Fakültesi Dergisi*, ed. Akın Ünal, Fatih Birtek, Atilla Erkal, C. VIII, S. 2, Doğan Soyaslan Armağanı, Kayseri: Erciyes Üniversitesi Yayını, 2013, ss. 569-632.
- ERSOY Uğur, *Bir İnsan Hakları Kavramı Olarak "Kişisel Verilerin Korunması"*, (Yüksek Lisans Tezi), Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2009.
- GÖÇMEN UYARER Sinem, *Kişisel Verilerin Korunması*, 1. b., Ankara: Seçkin Yayıncılık, 2019.
- GÖKTÜRK Neslihan, "Suçun Yasal Tanımında Yer Alan "Hukuka Aykırılık" İfadesinin İcra Ettiği Fonksiyon", *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, C. 7, S. 1, Malatya: İnönü Üniversitesi Yayını, 2016, ss. 407-450.
- GÖNEN Doruk, *Tüzel Kişilerde Kişilik Hakkı ve Korunması*, 1. b., İstanbul: On İki Levha Yayıncılık, 2011.
- GÜLTEKİN Nil Melek, *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*, (Yüksek Lisans Tezi), İstanbul: Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, 2012.
- GÜR İkbâl, *Kişisel Verilerin Korunması Hususunda AB ile ABD arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları*, (Yüksek Lisans Tezi), Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2009.
- HENKOĞLU Türkay, *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, 1. b., Ankara: Yetkin Yayınları, 2015.

- İTİŞGEN Rezzan, “Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu”, *Türkiye Adalet Akademisi Dergisi*, ed. Aşkın Güven, Fethullah Soyubelli, S. 23, Ankara: Türkiye Adalet Akademisi Yayını, 2015, ss. 179-202.
- KANGAL Zeynel T., *Ceza Hukukunda Zorunluluk Durumu*, 1. b., Ankara: Seçkin Yayıncılık, 2010.
- KANGAL Zeynel T., “Ceza Hukukunda Varsayılan Rıza”, *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, ed. İlhan Üzülmez, Hayrettin Çağlar, C. XV, S. 4, Ankara: Gazi Üniversitesi Yayını, 2011, ss. 223-251.
- KANGAL Zeynel T., *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*, 1. b., İstanbul: On İki Levha Yayıncılık, 2019.
- KAYA Cemil, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, *İÜHFMD*, C. LXIX, S.1 – 2, İstanbul: İstanbul Üniversitesi Yayını, 2011, ss. 317-334.
- KAYIHAN Şaban, ÜNLÜTEPE Mustafa, *Medeni Hukuk Bilgisi*, 4. b., Ankara: Seçkin Yayıncılık, 2017.
- KILINÇ Doğan, “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, *AÜHFMD*, C.61, S.3, Ankara: Ankara Üniversitesi Yayını, 2012, ss. 1089-1169.
- KOCA Mahmut, ÜZÜLMEZ İlhan, *Türk Ceza Hukuku Genel Hükümler*, 11. b., Ankara: Seçkin Yayıncılık, 2018.
- KOCA Mahmut, ÜZÜLMEZ İlhan, “Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)”, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, C. 21, Özel Sayı, Prof. Dr. Durmuş Tezcan’a Armağan, İzmir: Dokuz Eylül Üniversitesi Yayını, 2019, ss. 69-93.
- KORFF Douwe, *EC Study on Implementation of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49), Comparative Summary of National Laws*, Cambridge: Human Rights Centre University of Essex, 2002.
- KORKMAZ İbrahim, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, 1. b., Ankara: Seçkin Yayıncılık, 2017.
- KÖSE AYSUN Melike, *Kişisel Verilerin Kaydedilmesi Suçu (TCK m.135)*, 1. b., Ankara: Seçkin Yayıncılık, 2018.
- KUŞKONMAZ Elif Mendos, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, (Yüksek Lisans Tezi), İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2013.
- KÜZECİ Elif, “İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı”, *İnsan Hakları Yıllığı*, C.32, (2014), s. 53-75, [https://www.academia.edu/37176330/%C4%B0statistik%C3%AE_Birimler_ve_Bilgilerin_Gelece%C4%9Fini_Belirleme_Hakk%C4%B1_Statistical_Units_and_Right_to_Informational_Self-Determination_\(07.08.2019\).](https://www.academia.edu/37176330/%C4%B0statistik%C3%AE_Birimler_ve_Bilgilerin_Gelece%C4%9Fini_Belirleme_Hakk%C4%B1_Statistical_Units_and_Right_to_Informational_Self-Determination_(07.08.2019).)

- KÜZECİ Elif, *Kişisel Verilerin Korunması*, 2. b., Ankara: Turhan Kitabevi Yayınları, 2018.
- MANAV Eda, “İş İlişkisinde İşçinin Kişisel Verilerinin Korunması”, *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, ed. Bülent Yavuz, Abdülkerim Yıldırım, M. Çelebi Can C. XIX, S.2, Ankara: Gazi Üniversitesi Yayını, 2015, ss. 95-136.
- OĞUZ Sefer, “Kişisel Verilerin Korunması Hukukunun Genel İlkeleri”, *Bilgi Ekonomisi ve Yönetimi Dergisi*, ed. İbrahim Güran Yumuşak, C.13, S.2, 2018, ss. 121-138.
- ÖZBEK Veli Özer vd., *Türk Ceza Hukuku Genel Hükümler*, 9. b., Ankara: Seçkin Yayıncılık, 2018.
- ÖZBEK Veli Özer vd., *Türk Ceza Hukuku Özel Hükümler*, 13. b., Ankara: Seçkin Yayıncılık, 2018.
- ÖZDEMİR Hayrunnisa, “Haberleşmenin Gizliliği ve Kişisel Veriler”, *EÜHFD*, C. XIII, S. 1–2, Erzincan: Erzincan Üniversitesi Yayını, 2009, ss. 285-303.
- ÖZDEMİR Hayrunnisa, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, 1. b., Ankara: Seçkin Yayıncılık, 2009.
- ÖZEN Mustafa, “Kişisel Verilerin Kaydedilmesi, Verilmesi veya Ele Geçirilmesi ve Yok Edilmemesi Suçları (TCK m. 136, 137, 138)”, *Kamu Hukuku Arşivi*, C.12, S.1 2009, ss. 13-28.
- ÖZGENÇ İzzet, *Türk Ceza Hukuku Genel Hükümler*, 14. b., Ankara: Seçkin Yayıncılık, 2018.
- ÖZGENÇ İzzet, ÜZÜLMEZ İlhan, *Ceza Genel Hukuku*, 2. b., Ankara: Seçkin Yayıncılık, 2019.
- SAMUELSON Pamela, “Privacy As Intellectual Property?”, *Stanford Law Review*, C.52, S.5, Stanford: Stanford University, 2000, ss. 1125-1173.
- SARIUSTA Kader, *Kişisel Verilerin Ceza Hukuku Yoluyla Korunması*, (Yüksek Lisans Tezi), Gaziantep: Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü, 2018.
- SCHWARTZ Paul, “The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination”, *American Journal of Comparative Law*, C.37, S.4, Oxford: Oxford University Press, 1989, ss. 675-701.
- SERT Şeyma, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, 1. b., Ankara: Seçkin Yayıncılık, 2019.
- SEVİMLİ K. Ahmet, “Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419”, *Sicil İş Hukuku Dergisi*, Y.6, S.24, 2011, ss. 120-139
- SOYASLAN Doğan, *Ceza Hukuku Özel Hükümler*, 8. b., Ankara: Yetkin Yayınları, 2010.
- SÖZÜER Eren, *Unutulma Hakkı, İnsan Hakları Hukuku Perspektifinden Bir İnceleme*, 1. b, İstanbul: On İki Levha Yayıncılık, 2017.

- ŞİMŞEK Oğuz, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 1. b., İstanbul: Beta Yayınevi, 2008.
- TANDOĞAN Haluk, “Şahsiyetin Akit Dışı İhlallere Karşı Korunmasının İşleyiş Tarzı ve Basın Yoluyla Olan İhlallere Karşı Özel Hayatın Korunması”, *Ankara Hukuk Fakültesi Dergisi*, C. 20, S. 1, Ankara: Ankara Üniversitesi Yayını, 1963, ss. 1-36.
- TEKİN Nurullah, “Kişisel Verilerin Korunması ile İlgili Türkiye’deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi”, *Uyuşmazlık Mahkemesi Dergisi*, S.4, Ankara: Uyuşmazlık Mahkemesi, 2014, ss. 222-262.
- TEZCAN Durmuş, “Bilgisayar Karşısında Özel Hayatın Korunması”, *Anayasa Yargısı Dergisi*, C.8, (1991), ss. 385-392.
- UNCULAR Selen, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, 2. b., Ankara: Seçkin Yayıncılık, 2018.
- YAVUZ Can, *İnternet’teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı*, 2. b., Ankara: Seçkin Yayıncılık, 2018.
- YILMAZ Ejder, “Kişi”, *(Öğrenciler İçin) Hukuk Sözlüğü*, 4. b., Ankara: Yetkin Yayınları, 2012.
- YOKUŞ SEVÜK Handan, *Türk Ceza Hukuku Özel Hükümler*, 1. b., Ankara: Adalet Yayınevi, 2018.
- YÖRÜK Onur Doğan, *(AB) 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Kişisel Verilerin Korunması*, (Yüksek Lisans Tezi), İzmir: İzmir Ekonomi Üniversitesi Lisansüstü Eğitim Enstitüsü, 2019.
- YÜCEDAĞ Nafiye, “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”, *İÜHFİM*, C. LXXV, S. 2, İstanbul: İstanbul Üniversitesi Yayını, 2017, ss. 765-790.
- YÜKSEL CİVELEK Dilek, *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*, (Uzmanlık Tezi), Ankara: Bilgi Toplumu Dairesi Başkanlığı, 2011.
- ZEYTİN Zafer, ERGÜN Ömer, *Türk Medeni Hukuku*, 4. b, Ankara: Seçkin Yayıncılık, 2018.

İnternet Kaynakları

- 108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, <https://www2.tbmm.gov.tr/d26/1/1-0320.pdf>, (22.07.2019).
- 108 sayılı Avrupa Konseyi Sözleşmesi, http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktarafli-soz/ak/turkce/108_tur.pdf (01.06.2019).
- 1974 tarihli ABD Özel Hayatın Gizliliği Kanunu, <https://www.justice.gov/opcl/privacy-act-1974>, (02.08.2019).

- 1978 tarihli ABD Mali Gizlilik Kanunu, <https://www.law.cornell.edu/uscode/text/12/chapter-35>, (02.08.2019).
- 1978 tarihli Fransız Bilgi Teknolojisi, Veri Dosyaları ve Bireysel Özgürlükler Kanunu, <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20080609>, (02.08.2019).
- 1980 tarihli Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, (21.07.2019).
- 1996 tarihli ABD İletişim Ahlak Yasası, <https://www.law.cornell.edu/uscode/text/47/230>, (02.08.2019).
- 1998 tarihli ABD Çocukların Çevrimiçi Korunması Yasası, <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>, (02.08.2019).
- 1998 tarihli İngiltere Veri Koruma Kanunu, http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf, (02.08.2019).
- 2018 tarihli İngiltere Veri Koruma Kanunu, <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>, (02.08.2019).
- 95/46/EC sayılı ve 24 Ekim 1995 tarihli Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki Avrupa Birliği Konseyi ve Avrupa Parlamentosu Direktifi, <https://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (23.04.2019).
- ABD Telefon Müşterilerini Koruma Kanunu, <https://www.law.cornell.edu/uscode/text/47/227>, (02.08.2019).
- Alman Ceza Kanunu, <https://germanlawarchive.iuscomp.org/?p=752>, (02.08.2019).
- Alman Ceza Muhakemesi Kanunu, <https://germanlawarchive.iuscomp.org/?p=754>, (02.08.2019).
- Alman Federal Veri Koruma Kanunu, https://www.gesetze-im-internet.de/englisch_bds/englisch_bds.pdf, (18.08.2019).
- Almanya Anayasası, <http://www.adalet.gov.tr/duyurular/2011/eylul/anayasalar/ulkeana/pdf/08-ALMANYA%20209-276.pdf>, (02.08.2019).
- APEC hakkında, <https://www.apec.org/About-Us/About-APEC/Mission-Statement>, (22.07.2019).
- Article 29 Data Protection Working Party, *Opinion 4/2007 On The Concept Of Personal Data*, <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf>, (31.05.2019).

- Avrupa Birliđi Genel Veri Koruma Tüzüğü, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN> (10.06.2019).
- Avrupa Birliđi Genel Veri Koruma Tüzüğü, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>, (22.07.2019).
- Avrupa Birliđi hakkında, https://europa.eu/european-union/about-eu/eu-in-brief_en, (22.07.2019).
- Avrupa Birliđi Temel Haklar Şartı, <https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708#>, (23.07.2019).
- Avrupa İnsan Hakları Sözleşmesi, <https://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf>, (22.07.2019).
- Avrupa Konseyi Statüsü, http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktaraflioz/ak/turkce/001_tur.pdf, (21.07.2019).
- Birleşmiş Milletler Şartı, <https://www.un.org/en/charter-united-nations/index.html>, (21.07.2019).
- Birleşmiş Milletler tarihi, <https://www.un.org/en/sections/history/history-united-nations/index.html>, (21.07.2019).
- BM İnsan Hakları Evrensel Beyanname, <https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf>, (21.07.2019).
- BM Medeni ve Siyasal Haklar Sözleşmesi, <https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/53-73.pdf>, (21.07.2019).
- DSAnpUG-EU isimli Alman Kanunu, https://www.bvdnet.de/wp-content/uploads/2017/08/BMI_%C3%9Cbersetzung_DSAnpUG-EU_mit_BDSG-neu.pdf, (18.08.2019).
- Fransa Anayasası, <http://www.adalet.gov.tr/duyurular/2011/eylul/anayasalar/ulkeana/pdf/07-FRANSA%20169-208.pdf>, (02.08.2019).
- Fransız Ceza Kanunu, <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719>, (02.08.2019).
- Guidelines for the Regulation of Computerized Personnel Data Files, <https://undocs.org/en/A/RES/45/95>, <https://www.refworld.org/pdfid/3ddcafaac.pdf> (21.07.2019).
- İsviçre Ceza Kanunu, <https://www.admin.ch/opc/en/classified-compilation/19370083/index.html>, (.08.2019).

İsviçre Federal Anayasası, <https://www.admin.ch/opc/en/classified-compilation/19995395/201809230000/101.pdf>, (02.08.2019).

İsviçre Medeni Kanunu, <https://www.admin.ch/opc/en/classified-compilation/19070042/201901010000/210.pdf>, (02.08.2019).

İsviçre Verilerin Korunmasına İlişkin Federal Kanunu <https://www.admin.ch/opc/en/classified-compilation/19920153/201903010000/235.1.pdf>, (02.08.2019).

Kişisel Verileri Koruma Kurumu, *Açık Rıza*, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf>, (25.11.2019).

Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin İşlenme Şartları*, s. 10, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8c90423f-97ea-4d81-a7c1-ace74295c2b8.pdf>, (25.11.2019).

Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler*, <https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20ALANINDA%20ULUSLARARASI%20VE%20ULUSAL%20D%C3%9CZENLEMELER.pdf>, (22.07.2019).

Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Korunması Kanununa Duyulan İhtiyaç*, <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/8e39e0a1-6ec4-4179-a5d3-bbd8e78dce31.pdf> (31.07.2019).

Kişisel Verileri Koruma Kurumu, *Madde ve Gereçesi ile Kişisel Verilerin Korunması Kanunu (Bilgi Notu) ve Kişisel Verilerin Korunmasına İlişkin Terimler Sözlüğü*, Ankara: KVKK Yayınları, 2019, <https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gereçesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu> (13.06.2019).

Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>, (06.08.2019).

OECD hakkında, <https://www.oecd.org/about/>, (21.07.2019).

Türk Dil Kurumu Sözlükleri, <http://sozluk.gov.tr/>, (08.08.2019).

Türk Dil Kurumu, Güncel Türkçe Sözlük, http://www.tdk.gov.tr/index.php?option=com_gts&view=gts, (23.01.2019).

Mahkeme Kararları

AİHM kararı, <https://hudoc.echr.coe.int> > tur.

Anayasa Mahkemesi ve Yargıtay Kararları, www.kazanci.com.

Kişisel Verileri Koruma Kurulu Kararı, <https://www.kvkk.gov.tr/Icerik/5406/Kurul-Karar-Ozetleri>.