

2018

KAMU HUKUKU ABD

GAZİANTEP ÜNİVERSİTESİ

YÜKSEK LİSANS TEZİ

KADER SARIUSTA

T.C.
GAZİANTEP ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANA BİLİM DALI

KİŞİSEL VERİLERİN CEZA HUKUKU YOLUYLA KORUNMASI

YÜKSEK LİSANS TEZİ
KADER SARIUSTA

GAZİANTEP
TEMMUZ 2018

T.C.
GAZİANTEP ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANA BİLİM DALI

**KİŞİSEL VERİLERİN
CEZA HUKUKU YOLUYLA KORUNMASI**

YÜKSEK LİSANS TEZİ

KADER SARIUSTA

Tez Danışmanı: Dr. Öğr. Üyesi Ahmet BOZDAĞ

GAZİANTEP
TEMMUZ 2018

T.C.
UNIVERSITY OF GAZİANTEP
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF PUBLIC LAW

**PERSONAL DATA PROTECTION THROUGH
CRIMINAL LAW**

MASTER'S THESIS

KADER SARIUSTA

Supervisor: Ass. Prof. Dr. Ahmet BOZDAĞ

GAZİANTEP
JULY 2018

T.C.
GAZİANTEP ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANA BİLİM DALI

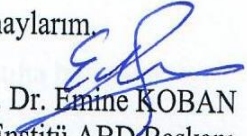
Kişisel Verilerin Ceza Hukuku Yoluyla Korunması
Kader SARIUSTA

Tez Savunma Tarihi: 02.07.2018

Sosyal Bilimler Enstitüsü Onayı


Doç. Dr. Zekiye ANTAKYALIOĞLU
SBE Müdürü

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.


Doç. Dr. Emine KOBAN
Enstitü ABD Başkanı

Bu tez tarafımca (tarafımızca) okunmuş, kapsamı ve niteliği açısından bir Yüksek Lisans tezi olarak kabul edilmiştir.


Dr. Öğr. Üyesi Ahmet BOZDAĞ
Tez Danışmanı

Bu tez tarafımızca okunmuş, kapsam ve niteliği açısından bir Yüksek Lisans tezi olarak oybirliği/oyçokluğu ile kabul edilmiştir.

Jüri Üyeleri:
(Unvanı, Adı ve SOYADI)

Dr. Öğr. Üyesi Ahmet BOZDAĞ

Doç. Dr. Emine KOBAN

Doç. Dr. Mehmet Emin ALŞAHİN

İmzası





ETİK BEYAN

Gaziantep Üniversitesi Sosyal Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Kader SARIUSTA

ÖZ

KİŞİSEL VERİLERİN CEZA HUKUKU YOLUYLA KORUNMASI

SARIUSTA, Kader

Yüksek Lisans Tezi, Kamu Hukuku ABD

Tez Danışmanı: Dr. Öğr. Üyesi Ahmet BOZDAĞ

Temmuz 2018

Kişisel veri kavramı en genel anlamda; kimliği belirli veya belirlenebilir gerçek bir kişiye ilişkin her türlü bilgi olarak tanımlanmaktadır. Bu anlamda kişinin fiziki görüntüsü, karakteri, ekonomik veya sağlık durumuna ilişkin bilgileri kişisel veri olarak kabul edilmektedir. Toplumsal yaşamda, bu bilgiler hem kamusal hem de özel sektörler tarafından çeşitli sebeplerle işlenebilmektedir. Kişisel verilerin hukuka uygun işlenmesine ilişkin esas ve usuller 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda düzenlenmiştir. Bu esas ve usullere aykırı olarak kişisel verilerin işlenmesi; veri sorumluları ve işleyicilerinin, idari veya cezai sorumluluğunu gündeme getirecektir.

5237 sayılı TCK'nın 135., 136. ve 138. maddelerinde korunması gereken hukuksal bir yarar olarak, kişinin özel yaşamı ve mahremiyeti dahilinde kişisel verileri kabul edilmiştir. Kişisel verilerin hukuka aykırı olarak kaydedilmesi, ele geçirilmesi, yayılması ve yok edilmemesi Kanun'un suç olarak düzenlendiği eylemlerdir. Böylelikle ceza hukuku yoluyla kişilerin, kişisel verilerinin korunması hakkı güvence altına alınmıştır. Bu çalışmanın temel amacı da, ceza hukukumuzun sağlamış olduğu bu korunmanın daha üst bir düzeye taşınmasını sağlayacak akademik faydanın gerçekleştirilmesidir. Bu doğrultuda çalışmada kişisel verilerin korunmasını konu edinen hem uluslararası hem de ulusal güncel metinlerden faydalanılarak, uygulamada verimlilik toplumsal yaşamda ise farkındalık yaratılmaya çalışılmıştır.

Anahtar kelimeler: Kişisel Veri, Veri Koruması, Kişisel Verilerin Korunması, Bilgilerin Geleceğini Belirleme, TCK'da Kişisel Verilerin Korunması, 6698 sayılı Kanun.



ABSTRACT

PERSONAL DATA PROTECTION THROUGH CRIMINAL LAW

SARIUSTA, Kader

M. A. Thesis, Department of Public Law

Supervisor: Ass. Prof. Dr. Ahmet BOZDAĞ

July 2018

Personal data is defined as any information related to an identified or identifiable natural person. In this respect, physical or characterical appearance, information concerning economic or health conditions are accepted as personal data. This information could be processed for various purposes by both private and public sectors. The main principles and the procedures about lawfulness of processing personal data have been regulated in Law no. 6698. In the case of a personal data breach, the controller and the processor will be responsible both criminally and administratively.

Personal data protection in the concept of private life and privacy has been accepted as a judicial interest to be protected in No. 5237 Turkish Criminal Law and sanctions listed under No.135., 136., 138. Processing of personal data as recording, collection, dissemination and not erasing unlawfully are criminal deeds regulated in Law no. 5237. In this way, the personal data have been protected by criminal law. The main purpose of this paper is to contribute the academical studies of personal data protection in criminal law. Accordingly the study conceived to efficiency in practice and awareness in social life by means of international and national actual documents about personal data protection.

Key words: Personal Data, Data Protection, Personal Data Protection, Informational Self-Determination, Personal Data Protection in TCK, Law No. 6698.



İÇİNDEKİLER

ÖZ.....	i
ABSTRACT	iii
İÇİNDEKİLER	v
SEMBOLLER VE KISALTMALAR.....	xi
GİRİŞ	1

BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASININ KAVRAMSAL ÇERÇEVESİ, TEMEL İLKELERİ VE ULUSLARARASI DÜZENLEMELER

I. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL KAVRAMLAR..	5
A. Kişisel Veri Kavramı	5
1. Genel Olarak Kişisel Veri Kavramı ve Unsurları.....	6
a. Veri Kavramı ve İçeriği.....	7
b. Kişi ve Kişiselliğin Kapsamı	8
c. Kimliğin Belirli veya Belirlenebilir Olması	11
d. Kişiyeye İlişkin Olma	13
2. Özel Nitelikli Kişisel Veri (Hassas Veri).....	14
B. Kişisel Verilerin Korunması Kavramı, Gerekliiliği ve Tarihsel Süreçte Gelişimi	18
1. Kişisel Verilerin Korunması Kavramı ve Kapsamı	18
2. Kişisel Verilerin Korunmasının Tarihi Gelişimi ve Bilgi Toplumu	20
3. Kişisel Verilerin Korunması Gerekliiliği	21
C. Kişisel Verilerin İşlenmesi Kavramı ve İşlemenin Kapsamı	23
1. Genel Olarak Veri İşleme Kavramı	25
2. Veri İşlemenin Kapsamı	26
a. Verilerin Anonim Olarak İşlenmesi	28
b. Verilerin Takma Adlaştırılması	29
II. KİŞİSEL VERİ KORUMASININ TEMEL İLKELERİ.....	30
A. Veri Korumanın Esasına Dair İlkeler	31
1. Veri Güvenliiliği ve Mahremiyeti	31

2. Hassas Verilerin İşlenmesi ve Özellikli Olarak Korunması	32
B. Verinin İşlenme Usulüne Dair İlkeler	34
1. Hukuka ve Dürüstlük Kurallarına Uygunluk	34
a. Açık Rızanın Kapsamında Verilerin İşlenmesi	35
b. Tarafı Olunan Bir Sözleşmenin İcrası veya İfası Kapsamında Verilerin İşlenmesi	39
c. Yasal Zorunluluklara Mutabık Kişisel Verilerin İşlenmesi.....	39
d. Veri Öznesinin veya Başka Bir Gerçek Kişinin Yüksek Menfaatleri Gereği Verilerin İşlenmesi	40
e. Kamu Yararı veya Resmi Yetkinin Kullanılması Gereğiyle Verilerin İşlenmesi	40
f. Veri Sorumlusu veya Üçüncü Kişilerin Gözettiği Meşru Menfaatler Gereği Verilerin İşlenmesi	40
2. Amaçla Bağlılık	41
3. Ölçülülük	42
4. Doğruluk ve Güncellik	43
C. Veri Sahibi Kişinin Haklarına İlişkin İlkeler	44
1. Bilgi Edinme Hakkı	45
2. Erişim Hakkı.....	47
3. Düzeltme Hakkı.....	48
4. Unutulma Hakkı	49
5. İşlemenin Sınırlandırılması Hakkı.....	52
6. Verilerin Taşınması Hakkı	53
7. İtiraz ve İrade Sergileyebilme Hakkı	54
III. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ULUSLARARASI DÜZENLEMELER	56
A. OECD Düzenlemelerinde Kişisel Verilerin Korunması.....	57
B. Birleşmiş Milletler Temel Metinlerinde Kişisel Verilerin Korunması	58
C. Avrupa Konseyi Düzenlemelerinde Kişisel Verilerin Korunması	59

1. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında/Karşısında Gerçek Kişilerin Korunmasına İlişkin Sözleşme	61
2. AİHS 8. Madde Kapsamında Koruma.....	63
D. Avrupa Birliği Dahilinde Kişisel Verilerin Korunması.....	65
1. Avrupa Birliği Temel Haklar Şartı	66
2. 95/46/AT Sayılı Avrupa Birliği Veri Koruma Direktifi	68
3. 2002/58/AT Sayılı Özel Yaşamın ve Elektronik İletişimin Korunması Direktifi.....	70
4. 2016/680 Kişisel Verilerin Cezai Prosedür Gereği İşlenmesi Karşısında Gerçek Kişilerin Korunması Direktifi	71
5. 2016/679 Sayılı Avrupa Birliği Veri Koruma Regülasyonu.....	72

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN ULUSAL DÜZENLEMELER VE CEZA HUKUKU ÖZELİNDE KORUNMASI

I. GENEL OLARAK.....	78
II. TEMEL ULUSAL DÜZENLEMELERDE KİŞİSEL VERİLER.....	81
A. Anayasa’ da Kişisel Verilerin Korunması	81
B. Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Veriler	88
1. Kanun’un Kapsamı ve Uygulama Alanı	91
2. Kişisel Verileri Koruma Kurumu	94
C. Diğer Temel Ulusal Metinlerle Kişisel Verilerin Korunması	99
III. TÜRK CEZA MEVZUATINDA KİŞİSEL VERİLERİN KORUNMASI	103
A. Ceza Muhakemesi Kanunu’nun Kişisel Verilere İlişkin Hükümleri.....	105
B. Türk Ceza Kanunu’nda Kişisel Verilere İlişkin Suçlar	111
1. Genel Olarak	111
2. Kişisel Verilerin Kaydedilmesi Suçu.....	114
a. Genel Olarak	114
b. Suçla Korunan Hukuksal Yarar	116
c. Suçun Unsurları	117
i. Maddi Unsurlar	117

1. Suçun Konusu	117
2. Fail ve Mağdur	122
3. Hareket	124
ii. Manevi Unsur	126
iii. Hukuka Aykırılık Unsuru.....	128
e. Suçun Özel Görünüş Biçimleri	135
i. Teşebbüs.....	135
ii. İştirak	136
iii. İçtima	136
f. Nitelikli Haller.....	142
i. Suçun Konusunun Özel Nitelikli Veri Olması	143
i. Suçun Kamu Görevlisi Tarafından ve Görevinin Sağladığı Kolaylıkla İşlenmesi.....	144
ii. Suçun Belli Bir Meslek ve Sanatı İfa Etmenin Sağladığı Kolaylıkla İşlenmesi.....	146
g. Yaptırım	147
3. Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu .148	
a. Genel Olarak	148
b. Suçla Korunan Hukuksal Yarar	150
c. Suçun Unsurları	151
i. Maddi Unsurlar	151
1. Suçun Konusu	151
2. Fail ve Mağdur	151
3. Hareket	151
ii. Manevi Unsur	157
iii. Hukuka Aykırılık	158
e. Suçun Özel Görünüş Biçimleri	160
i. Teşebbüs.....	160

ii. İştirak	162
iii. İçtima	162
f. Nitelikli Haller	167
g. Yaptırım	168
4. Verilerin Yok Edilmemesi Suçu.....	169
a. Genel Olarak	169
b. Suçla Korunan Hukuksal Yarar	170
c. Suçun Unsurları	171
i. Maddi Unsurlar	171
1. Suçun Konusu	171
2. Fail ve Mağdur	172
3. Hareket	173
ii. Manevi Unsur	176
iii. Hukuka Aykırılık	176
e. Suçun Özel Görünüş Biçimleri	178
i. Teşebbüs	178
ii. İştirak	178
iii. İçtima	179
f. Nitelikli Haller	181
g. Yaptırım	181
SONUÇ	183
KAYNAKÇA.....	187



SEMBOLLER VE KISALTMALAR

Aktaran	: Akt.
Avrupa Birliđi	: AB
Avrupa Birliđi Temel Haklar Şartı	: ABTHŞ
Ankara Üniversitesi Hukuk Fakóltesi Dergisi	: AÜHFD
Avrupa Topluluđu	: AT
Avrupa İnsan Hakları Mahkemesi	: AİHM
Avrupa İnsan Hakları Sözleşmesi	: AİHS
Avrupa Topluluđu Adalet Divanı	: ATAD
Bakınız	: Bkz.
Birleşmiş Milletler	: BM
Ceza Dairesi	: CD.
Ceza Genel Kurulu	: CGK.
Ceza Muhakemesi Kanunu	: CMK
Cilt	: C.
Çeviren	: Çev.
Çok yazarlı eserlerde ilk yazardan sonrakiler	: vd.
Deoksiribo Nükleik Asit	: DNA
Esas	: E.
General Data Protection Regulation	: GDPR.
Hukuk Dairesi	: HD.
Hukuk Genel Kurulu	: HGK.
İdari Dava Dairesi	: İDD.
İstanbul Üniversitesi Hukuk Fakóltesi Mecmuası	: İÜHFM
Karar	: K.
Kişisel Verileri Korunma	: KVK
Kişisel Verileri Koruma Kanunu	: KVKK
Madde	: md.
Milattan Önce	: M.Ö.
Milli İstihbarat Teşkilatı	: MİT
Passenger Name Record	: PNR
Polis Vazife ve Salahiyet Kanunu	: PVSK

Resmi Gazete	: RG
Sayfa	: s.
Sayı	: S.
Ekonomik Kalkınma ve İşbirliği Örgütü	: OECD
Treaty On The Functioning Of The European Union:	TFEU
Türkiye İstatistik Kurumu	: TÜİK
Türk Ceza Kanunu	: TCK
Türk Medeni Kanunu	: TMK
Türkiye Büyük Millet Meclisi	: TBMM
Vergi Usul Kanunu	: VUK
Yüzyıl	: yy.

GİRİŞ

Günümüze kadar birbirinden farklı, pek çok amaç kapsamında ve pek çok alanla ilgili olarak gereksinim duyulmuş olan kişiye ilişkin bilgilerin öğrenilme isteğinin özünde, her şeyden çok kişisel merak duygusu yatmaktadır. Basit bir meraktan yola çıkılarak öğrenilmek istenilen kimliği belirli veya belirlenebilir gerçek bir kişiye ilişkin veriler yani kişisel veriler, bugün itibarıyla ekonomik değere sahip, ticareti yapılan ve para kazanılma amacıyla ihtiyaç duyulan bir eşya olma seviyesine ulaşmıştır. Kişisel verilerin böyle bir nitelik kazanmakla daha ziyade özel kişi ve kuruluşların ilgisini çektiği düşünülse de aslında kamusal kurum ve kuruluşlar da karmaşık bürokratik süreçleri kolaylaştırmak ve kamusal faaliyetleri daha kolay denetleyebilmek için kişilere ait verileri kayıt altına almaktadırlar. Yani aslında hem devlet hem de özel kurum ve kuruluşlar açısından kişisel veriler, her geçen gün daha fazla ihtiyaç duyulan ve depolanan bir cevher olarak değer kazanmaktadır. Kişisel veriler, günümüze kadar ve hatta günümüzde de hukuken farklı şekillerde nitelendirmelere tabi tutulmuşlardır. Kişisel veriler, üzerinde mülkiyet kurulabilecek olan bir eşya, fikri ve sınai bir eser ya da kişiliğimizi oluşturan bir değer veya hak olarak kabul görmüştür. Kişisel verilere ilişkin bu nitelendirmeler, verilerin hukuken hangi şekil ve kapsamda korunması gerektiğine dair sorulara da bir yanıtın bulunmasını sağlayabilecek olduğundan bugüne kadar önem arz etmiştir. Günümüzde kişisel veriler, hem Avrupa Birliği bünyesindeki veri koruma düzenlenmeleri ekseninde hem de ulusal düzenlemelerimizde temel bir kişilik hakkı olarak korunmaktadır. Bu doğrultuda kişisel verilerin korunması hakkı Anayasa'mızın 20. maddesinin 3. fıkrasında; *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* şeklinde düzenlenerek güvence altına alınmıştır. Kişisel verilerin korunması hakkı, aynı zamanda kişilerin özel yaşamının korunmasını konu edinen Anayasa'mızda veya uluslararası metinlerde düzenlenmiş olan temel hak ve özgürlükler kapsamında da

korunmaya çalışılmıştır. Kişisel veriler, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde düzenlenmiş olan özel ve aile hayatına saygı hakkı kapsamında korunması gereken bir değer olarak kabul edilmiş ve AİHM kişisel verilerin korunması hakkına ilişkin olarak önemli içtihatlarla bulunmuştur. Bunun dışında kişisel verilerin korunması hukukunun temel düzenleyici mevzuatı olarak kabul edilen 95/46 sayılı Avrupa Birliği Veri Koruma Direktifi ve bu Direktifi yürürlükten kaldıracak olan 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Regülasyonu, kişisel verilerin uluslararası düzlemde etkin ve uyumlu bir korumaya sahip olabilmesi adına yapılmış önemli çalışmalar arasındadır.

Üzerinde yaşamakta olduğumuz topraklarda da günümüzden yaklaşık 2 yy. öncesinde Osmanlı Devleti zamanında, Elazığ'ın Palu ilçesinde yapılan askeri amaçlı bir nüfus sayımında; bir köyde kaç hane olduğu, hangi hanede kaç kişinin yaşadığı, hanedeki kişilerin yaşı ve fiziksel özellikleri ve aile bireyleri arasındaki alt-üst soy ilişkisine ilişkin bilgiler gibi kişisel veriler kayıt altına alınmıştı. Bu ve benzeri sebeplerle tarihimizin en eski zamanlarından beri işlemekte olduğumuz kişisel verilerin, korunması için ülkemizde de son yıllarda önemli çalışmalar yapılmıştır. Kişisel verilerin korunmasını, hem hukuki hem de adli olarak güvence altına almak üzere pek çok mevzuatımızda çeşitli hükümler yer almaktayken, 2016 yılı itibarıyla münhasıran kişisel verilerin korunmasının temel esas ve usullerini düzenleyen veri koruma mevzuatı da hukukumuza girmiştir. 765 sayılı TCK'da doğrudan kişisel verilere karşı işlenen suçları cezalandıran bir hüküm bulunmazken, 5237 sayılı Türk Ceza Mevzuatı ve reform çalışmaları kapsamında kişisel verilerin korunması, mukayeseli hukukun konuya gösterdiği öneme paralel şekilde, cezai olarak güvence altına alınmıştır. Bu çalışmamızın temel amacı da, modern toplum araçları ve teknolojinin kaçınılmaz tehdidi altında olan verilerini ve mahremiyetini korumaya çalışan bireylere, Türk ceza hukukumuzun ne şekilde bir korunma öngördüğünün, sağlanan korumanın yeterli olup olmadığının, eksik veya çelişkili noktalarının neler olduğunun tespit edilerek çözüm önerileri getirilmesidir.

İki bölümden oluşan bu çalışmamızda, kişisel verilerin korunmasına dair temel kavramlara ve temel uluslararası düzenlemelere ilk bölümde temas edilmiş olup, ayrıca bu düzenlemeler ekseninde veri koruma hukukunun temel ilkeleri de açıklanmıştır. Özellikle 25.05.2018 tarihinden itibaren uygulanmaya konulmuş bulunan 2016/679 sayılı Avrupa Birliği Veri Koruma Regülasyonu düzenlemesi ve

gerekçesi doğrultusunda yapılan bu açıklamalarla, çalışmamıza kişisel verilerin korunması alanında güncellik kazandırılmaya çalışılmıştır. Kişisel verilerin ceza hukuku yoluyla korunması amacına hizmet eden, TCK'nın dokuzuncu bölümünde düzenlenmiş olan kişisel verilerin hukuka aykırı olarak işlenmesi, verilmesi, yayılması, ele geçirilmesi ve yok edilmemesi suçları suç inceleme metoduna uygun olarak çalışmamızın ikinci bölümünde incelenmiştir. Bu bölümde ayrıca temel ulusal mevzuatlarımız ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun kişisel verilerin korunmasına ilişkin düzenlemelerine de yer verilmiştir. Çalışmamızda, ulaşılabilen tüm ulusal ve uluslararası literatür, güncel düzenleme ve uygulamaların taranması metodu kullanılarak konunun ayrıntılı kavranabilmesi sağlanmaya çalışılmıştır.



BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASININ KAVRAMSAL ÇERÇEVESİ, TEMEL İLKELERİ VE ULUSLARARASI DÜZENLEMELER

I. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL KAVRAMLAR

A. Kişisel Veri Kavramı

Kişisel veri kavramının, verilerin korunması alanında üretilmiş olan pek çok uluslararası veya ulusal metinde belli bir istikamette tanımlaması yapılmıştır. Bu tanımlamaların uluslararası düzeyde yeknesaklığını sağlamak amacıyla oluşturulan ancak bu amacı tam olarak sağlayamamış ilk uluslararası düzenleme olarak 1980 yılında OECD tarafından yayınlanmış kişisel verilerin korunması hususunda rehber ilkeleri içeren metne göre; kişisel veri, “tanımlanmış/belirlenmiş veya tanımlanabilir/belirlenebilir olan bireyle ilişkili her türlü bilgi” şeklinde tanımlanmıştır.¹ Bu tanımlanma şekliyle kişisel veri kavramı genel itibarıyla üç temel unsurun birleşmesiyle bir araya gelmiştir denilebilir. Öncelikle kişisel bir veriden bahsolunabilmesi için elimizde bir veri bulunması gerekir. Dahası bu verinin bir kişiye ilişkin olması² ve kişiyi belirli veya belirlenebilir kılma özelliğinin bulunması gerekir.³

¹ OECD Kişisel Verilerin Sınır Aşan Transferi ve Mahremiyetin Korunması Rehber İlkeleri md. 1. Tam metin için bakınız. <http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm>. (12.12.2017). Bundan sonra “OECD Rehber İlkeleri” olarak anılacaktır.

² “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin” 2002/58 Sayılı Avrupa Konseyi Direktifi gibi bazı uluslararası düzenlemelerde veri öznesinin gerçek kişi veya tüzel kişi olması arasında bir fark bulunmadığı kabul edilmektedir.

³ Veri Çalışma Grubu’nun 4/2007 Sayılı Kişisel Veri Kavramı Hakkında Görüşü (Opinion 4/2007 On The Concept Of Personal Data, Article 29 Data Protection Working Party), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (12.12.2017).

*95/46/AT Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi'nin*⁴ kişisel verileri “belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi” şeklinde tanımlayan 2/a. ve *95/46/EC Sayılı Direktifi Yürürlükten Kaldıran, Kişisel Verilerin İşlenmesi ve Verilerin Serbest Dolaşımı Karşısında Gerçek Kişilerin Korunmasına İlişkin Genel Veri Koruma Regülasyonu'nun*⁵ 4/1. maddeleri ekseninde bir tanımlamaya 6698 Sayılı *Kişisel Verilerin Korunması Kanunu*⁶ “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” şeklinde yer vermiştir.

1. Genel Olarak Kişisel Veri Kavramı ve Unsurları

Kişisel veri kavramına ilişkin yapılan tanımlamaların ortak noktalarından hareketle bir analizde bulunursak kişisel veri kavramının temel unsurlarını; veri/bilgi, kimliğin belirli veya belirlenebilir olması ve bilginin kişiselleştirilmiş, gerçek bir kişiyle ilişkilendirilebilir olması olarak sıralayabiliriz.⁷ Bu doğrultuda doğrudan veya dolaylı olarak bir kişi ile ilişkilendirilerek kişinin kimliğini belirli kılan veya kılabilen olan bilgiler; kimlik, etnik köken, fiziksel özellikler, sağlık, öğrenim, ikamet, emniyet, kredi kartı, istihdam durumuna ilişkin bilgiler; başkaları ile gerçekleştirilen haberleşmeler; kişisel düşünce ve inançlar; alışveriş alışkanlıklarına ilişkin bilgiler kişisel veri olarak nitelendirilebilir.⁸ Bu örneklendirmelerin kapsamı teknoloji ve kişilik tespiti çalışmalarının gelişimine paralel olarak her geçen gün artmaktadır. Örneğin günümüz teknolojisi bize kişilerin DNA analizinden, parmak

⁴ Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi'nin tam metni için bakınız. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN> (16.11.2017). Bundan sonra “Direktif” olarak anılacaktır.

⁵ GDPR (General Data Protection Regulation) şeklinde kısaltılan düzenlemeye çalışmamız kapsamında da bundan “Regülasyon” olarak yer verilecektir. Tam metin için bkz. <http://eur-lex.europa.eu>

⁶ 6698 sayılı 24.03.2016 tarihli Kişisel Verilerin Korunması Kanunu'nun tam metni için bakınız. <http://www.mevzuat.gov.tr>. Bundan sonra “Ulusal Veri Koruma Mevzuatı” olarak anılacaktır.

⁷ Veri Çalışma Grubu'nun 4/2007 Sayılı Kişisel Veri Kavramı Hakkında Görüşü (Opinion 4/2007 On The Concept Of Personal Data, Article 29 Data Protection Working Party) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (12.12.2017).; AKSOY, Hüseyin Can, *Kişisel Verilerin Korunması*, Ankara, Çakmak Yayınevi, 2010, s. 13.

⁸ AKSOY, *Kişisel Verilerin Korunması*, s. 1.; BAŞALP, Nilgün, *Kişisel Verilerin Korunması ve Saklanması*, Ankara, Yetkin Yayınları, 2004, s. 33.

izinden ⁹, ses renginden ¹⁰ veya diğer biyometrik verilerinden kim olduğunu belirleyebilme imkanı yaratmaktadır. Dolayısıyla bundan 10 yıl öncesinde kişisel veri olarak yada veri olarak sahip olmadığımız bu bilgiler günümüzde kişisel veri kabul edilmekte ve korunmaya çalışılmaktadır.

a. Veri Kavramı ve İçeriği

Veri, Türk Dil Kurumu Bilişim Terimleri Sözlüğü'nde “olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi” şeklinde tanımlanmıştır. ¹¹ Daha genel anlamda veri; işlenebilen veya transfer edilebilen dijital formdaki bilgi veya bilgi çıktısıdır. ¹² Türkçe karşılığı bilgi ya da enformasyon olarak kabul edilen “information” ve “knowledge” kavramları da uluslararası hukuksal literatürde veriye karşılık olarak kullanılabilmektedir. ¹³ Ancak anlam itibarıyla farklı şeyleri ifade eden bu kavramların tümünün veriye karşılık olarak ulusal veya uluslararası literatürde kullanılmakta olmasının ¹⁴ yerinde ve doğru bir kullanım olduğunu söylememiz mümkün değildir. Bunun yanı sıra veri koruma hukuku bakımından bilgi, veri ve enformasyon kavramlarına ilişkin böylesi bir ayrımın üstüne fazlaca düşmek gereksiz görülmektedir. ¹⁵

Bir verinin kişisel veri olarak kabul edilebilmesinde içerik açısından aranan tek kriterin kimliği belirli veya belirlenebilir bir kişiyle ilişkilendirilebilmek olması dolayısıyla, bu kavramın kapsamı oldukça geniştir. Bilginin; öznel yada nesnel olması,

⁹ Mesaiye devamlılık tespitinde çalışanların parmak izi tarama yönteminin tercih edilmiş olmasının yanında, bu yöntemin ilgili mevzuatın mesai tespitine ilişkin benimsemiş olduğu sistemler arasında yer almaması ve parmak izi yöntemi ile çalışanların “kişisel verilerinin korunması” ve “özel hayatın gizliliği” Anayasa'nın 20. maddesinde koruma altına alınmış olan temel haklarının yasal bir dayanağı bulunmaksızın sınırlandırılmasına ilişkin dava konusu işlemin Anayasal ilkelere ve hukuka uyarlığının bulunmadığı Danıştay tarafından tespit edilmiştir. Danıştay 5. İDD., E: 2013/5342, K: 2013/9525. <http://www.hukukturk.com> (11.01.2018).

¹⁰ AİHM, P.G. ve J.H. & Birleşik Krallık Davası, Başvuru Numarası: 44787/98, Karar Tarihi: 25.01.2001, <https://hudoc.echr.coe.int> (7.01.2018).

¹¹ Türk Dil Kurumu Bilgisayar Terimleri Karşılıklar Klavuzu'na göre; veri İngilizce “data” kavramına karşılık olarak kullanılmaktadır. <http://www.tdk.gov.tr> (24.02.2018).

¹² Merriam Webster Sözlüğü, <https://www.merriam-webster.com/dictionary/data> (24.02.2018).

¹³ HENKOĞLU, Tülay, *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, Ankara, Yetkin Yayınları, 2015, s. 28.

¹⁴ KORKMAZ, İbrahim, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, Ankara, Seçkin Yayıncılık, 2017, s. 29.

¹⁵ KÜZECİ, Elif, *Kişisel Verilerin Korunması*, (Yayımlanmamış doktora tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü Ankara, 2010, s. 11.

gerçek veya uydurma olması, açık veya gizli olması¹⁶ kişisel veri olarak kabul edilmesi bakımından fark yaratmamaktadır. Bu doğrultuda veri öznesine, hakkında toplanmış olan doğruluk değeri bulunmayan kişisel verilerin düzeltilmesi veya silinmesini talep etme hakkı tanınmış olması da gerçek dışı bilgilerin kişisel verileri olarak işlenebileceğini göstermektedir.¹⁷ Bunun yanında verilerin hangi şekil veya biçimde olduğunun ve hangi vasıtalarla oluşturulduğunun da kişisel veri kavramı kapsamına dahil edilebilmesi açısından önemi yoktur.¹⁸ Bir kişiyi belirli veya belirlenebilir kılan verinin alfabetik, sayısal, grafiksel, fotografik veya akustik biçimde olabilmesi mümkündür.¹⁹

b. Kişi ve Kişiselliğin Kapsamı

“Kişi” ve “kişisel” kavramları Türk Dil Kurumu Sözlüğünde “şahıs, zat, nefer”, “kişi ile ilgili, kişiye ilişkin, şahsi” tanımlamalarının karşılığı olarak yer almaktadır.²⁰ Hukukta kişi; haklara ve borçlara sahip olabilen, gerçek ve tüzel kişi olarak sınıflandırılan varlıklara verilen addır.²¹ Kişi hukuk tarafından kendisine hak veya borç sahibi olabilme yetisi tanınmış varlıktır.²²

Kişisel verilerin korunması hukuku bakımından da veri öznesi kişi olarak kimlerin kabul edilebileceği ve koruma kapsamında olduğunun tespiti önem taşımaktadır. Dolayısıyla verinin gerçek kişi veya tüzel kişiye, ölüye veya cenine ait

¹⁶ Örneğin; kişinin cinsel tercihi ve kredi kartı şifresi gizli bilgiler kişisel veri olduğu gibi, kişinin fiziksel özellikleri, arabasının rengi gibi herkesçe rahatlıkla ulaşılacak şekilde aleni bilgiler de kişisel veri kapsamına girmektedir. Ayrıca bilginin gizli veya açık olup olmamasının kişisel veri sayılmasında etkili olmadığına ilişkin olarak bkz. AKSOY, *Kişisel Verilerin Korunması*, s. 14.; KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 27.; Köşe yazarı olan katılanın, kendi sayfasında kullandığı ve kendisi tarafından alenileştirilmiş olan resminin bir arkadaşlık sitesinde kullanılması halinde de kişinin kimliğini belirlenebilir kılan fotoğrafının kişisel veri olduğu, kişisel verilerin gizli olmayan veya herkes tarafından bilinen veriler olabilmesinin de mümkün olduğuna ilişkin bkz. Yargıtay CGK, E: 2012/12-1510, K: 2014/331,T: 17.06.2014 www.kazanci.com (04.01.2018).

¹⁷ Regülasyon md. 5/d.

¹⁸ Direktif md. 33. “Komisyon, bilgi çağında ilerlemenin seviyesi bakımından ve bilgi teknolojilerinin gelişimi hesaba katılarak gerekliliği ispatlanmış her türlü uygun öneriyi kabul etmeli ve gerçek kişilere ilişkin ses veya görüntü verilerinin işlenmesinde bu Direktif’in uygulanması özellikle sorgulanmalıdır.”

¹⁹ Veri Çalışma Grubu’nun 4/2007 Sayılı Kişisel Veri Kavramı Hakkında Görüşü (Opinion 4/2007 On The Concept Of Personal Data, Article 29 Data Protection Working Party); AKSOY, *Kişisel Verilerin Korunması*, s. 13. ; KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 26.

²⁰ Türk Dil Kurumu Güncel Türkçe Sözlük, <http://www.tdk.gov.tr> (04.02.2018).

²¹ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 32.

²² G. AKİPEK, *Jale vd., Türk Medeni Hukuku Başlangıç Hüükümleri(Kişiler Hukuku)*, İstanbul, Beta Basım, 10. B., 2013, s. 230.

olması durumu, bu başlık altında tartışılması gereken konulardandır. Kişisel verilerin korumasına ilişkin uluslararası metinlerin genelinde yalnızca gerçek kişilerin veri öznesi olarak korunması gerektiği kabul edilmiştir. Ancak bu durum devletlerin, ulusal düzenlemelerde tüzel kişilere ilişkin verileri de koruma kapsamına alan genişletici düzenleme yapabilme takdirini ortadan kaldırmamaktadır. OECD Rehber İlkeleri kişisel verileri tanımlarken kişiye ilişkin her türlü bilgiden bahsetmiş olup bu kişilerin tam anlamıyla tüzel kişileri de kapsam dışında bıraktığı veya yalnızca gerçek kişileri ifade ettiği vurgulanmış değildir. Bunun yerine üye devletlerin tüzel kişilere ait kişisel verileri de ulusal düzenlemelerle, gerçek kişilere ilişkin verilerin korunması yöntemlerine benzer şekilde koruyabileceği ve koruma kapsamının sınırlarını kişi grupları, organizasyonlar, işbirlikleri ve benzer organlar için belirleme inisiyatiflerinin bulunduğu kabul edilmiştir.²³ 2002/58 Sayılı Elektronik Haberleşme Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Direktifi de elektronik haberleşme sektörüne ilişkin olarak işlenen hem gerçek hem tüzel kişilere ilişkin bilgilerin kişisel veri kabul edilebileceğini düzenlemiştir. Genel Veri Koruma Regülasyonu ve Direktif, milliyeti veya ikametgahı ne olursa olsun verileri işleme konusu yapılan her gerçek kişi hakkındaki veri işlemenin sağladıkları koruma kapsamında olduğunu hüküm altına almış ve tüzel kişiler bu korumanın dışında bırakılmıştır.²⁴ 6698 Sayılı Kişisel Verilerin Korunması Kanunu da kapsamını; yalnızca gerçek kişilere ait kişisel verileri koruma altına alacak şekilde belirlemiştir.²⁵ Ulusal doktrinimizde de aynı doğrultuda; kişisel verilerin korunması düşüncesi temelinde özel yaşama ilişkin bir koruma anlayışı bulunmakta olduğu ve ancak gerçek kişilerin özel yaşamlarının mevcudiyetinden bahsedilebileceği,²⁶ tüzel kişilerin ise ticari gizliliğinin korunabileceği düşüncesiyle yalnızca gerçek kişilere ilişkin kişisel verilerin korunması gereği kabul edilmektedir.²⁷ Bunun yanı sıra tüzel kişiye ilişkin

²³ OECD Rehber İlkeleri Açıklayıcı Memorandum md. 33.-19.

²⁴ Aynı doğrultuda hem Direktif hem Regülasyon Gerekçe kısımlarında tüzel kişilere ilişkin işlemlerin bu ilgili düzenleme kapsamında sağlanan koruma alanına dahil olmadığı açıkça belirtmiştir.(Direktif Gerekçe md. 24; Regülasyon Gerekçe md. 14.)

²⁵ KVKK md. 2.; “Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.”; 5237 Sayılı Türk Ceza Kanunu’nun kişisel verilerin hukuka aykırı olarak tutulmasını suç olarak düzenlediği 135. maddesi gerekçesinde de suçun konusunu oluşturan kişisel veri kavramı gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır.

²⁶ TEZCAN, Durmuş, “Bilgisayar Karşısında Özel Hayatın Korunması”, Anayasa Yargısı Dergisi, C. XIII, Ankara, 1991, s. 389.

²⁷ KVKK 3/d. fıkrasında kişisel verinin “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlamasından ve 5237 Sayılı TCK’nın kişisel verilerin kaydedilmesi suçunu

tutulan bir veriden yola çıkılarak gerçek kişiye ulaşılabilir ve bu veri gerçek kişinin kimliğini belirleyicilik niteliği taşıyorsa, tüzel kişi hakkındaki bu verinin de kişisel verilere ilişkin koruma dahilinde olacağı kabul edilmektedir.²⁸ Genel olarak; tüzel kişilerin belli amaçlarla sonradan kurulmuş organizasyonlar olması karşısında kişilik hakkı olarak kabul edilen kişisel verilerin korunması hakkının tabi olarak kazanılması gerektiği²⁹, yine kişisel verilerin de dahil olduğu gizli ve özel hayat alanının tüzel kişiler için söz konusu olamayacağı³⁰, dahası tüzel kişilerin sır niteliğindeki ticari bilgilerinin de özel kanunlarla koruma altında olması³¹ gibi gerekçeler tüzel kişiye ilişkin bir kişisel verinin olamayacağı ve kişisel verilere ilişkin koruyucu düzenlemeler ekseninde tüzel kişinin korunması ihtiyacının bulunmadığı kanaatlerinin temellerini oluşturmaktadır.

Verilerin ilişkili olduğu kişinin niteliğine ilişkin üzerinde durulması gereken bir diğer önemli husus ölü ve cenine ilişkin verilerin kişisel veri olarak kabul edilip edilemeyeceğidir. Kişilik, hukuki olarak tam ve sağ doğmakla kazanılırken, ölümle sona ermektedir.³² Bu hukuki prensipten hareketle kimliği belirli veya belirlenebilir gerçek kişi, ancak tam ve sağ doğmakla kişisel verilerinin korunması temel hakkına kavuşacak, ölümle ise bu hakkı ortadan kalkacaktır. Genel Veri Koruma Regülasyonu da gerekçesinde açıkça ölmüş kişilere ilişkin kişisel verilerin koruma kapsamının dışında olduğunu düzenlemiştir.³³ Ancak üye devletlere ölümlere ilişkin kişisel verileri koruma altına alan ulusal düzenlemelerle bu kapsamı genişletebilme inisiyatifi

düzenlemiş olduğu 135. maddesinin gerekçe metninde de “Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir.” şeklindeki düzenlemesinden hareketle diyebiliriz ki ulusal hukukumuz bakımından ancak bir gerçek kişi ile ilişkilendirilebilen verilerin kişisel veri olarak kabul edilmesi gerekmektedir.

²⁸ BAŞALP, *Kişisel Verilerin Korunması ve Saklanması*, s. 35.

²⁹ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 35. Aksi istikamette; “Hükmi şahısların da özel hayatları ve ayrıca gizlilik alanları bulunabilir. Bunlar da korunurlar. Hükmi şahıslar, Medeni Kanunun şahsiyet hakkının korunması hükümlerinden (Medeni Kanun md. 24-25, Borçlar Kanunu md 49) faydalanabilecekleri gibi, temel haklardan (Anayasa haklarından) da gayelerine uygun bulunduğu ölçüde, istifade edebilirler.” İMRE, Zahit, “Şahsiyet Haklarından Şahsın Özel Hayatının ve Gizliliklerinin Korunmasına İlişkin Meseleler”, İÜHF Mecmuası, C. 39, S. 1-4, 1974, s. 157.

³⁰ Özel yaşam özü itibarıyla gerçek kişilere ilişkindir. Tüzel kişilik olarak ticari şirketleri, ticari sır kapsamında ilişkili oldukları verilerin korunması haklarını kullanabileceklerdir. TEZCAN, “Bilgisayar Karşısında Özel Hayatın Korunması”, s. 389.

³¹ Veri öznesinin bir şirket olması durumunda artık bir ticari sırdan bahs olunması gerekmektedir. Bkz. ARSLAN, Çetin, “Avrupa Birliği Hukukunda *Kişisel Verilerin Üçüncü Ülkelere Aktarılması*”, Bahçeşehir Üniversitesi Hukuk Fakültesi Kazancı Hakemli Hukuk Dergisi, S. 79-80, 2011, s. 450.; 6102 sayılı Türk Ticaret Kanunu md. 527; TCK md. 239.

³² G. AKİPEK vd., *Türk Medeni Hukuku Başlangıç Hükümleri (Kişiler Hukuku)*, s. 231.

³³ Regülasyon Gerekçe md. 27., 158.

tanınmıştır.³⁴ Bu konu 95/46 Sayılı Direktif'in düzenlemeyi ihmal ettiği bir alan olduğundan bu doğrultuda, bazı ulusal metinlerde doğmamış çocukların veya ölmüş kişilerin verilerinin de belli özel koşullarda korunması hukuki düzenlemelerle güvence altına alınmıştır.³⁵ Bu konuya ilişkin diğer bir yaklaşıma göre de; hayatta olmayan bir kişiye ilişkin kişisel verilerin veri koruma hukuku düzenlemeleri kapsamında korunmaması hayatta olan diğer kişileri etkileyebilecekse veya ölmüş kişiye ilişkin bilgiler hayattaki bir kimseyi referans kılıyorsa bu durumda bu kişileri ait verilerin de kişisel veri olarak kabul edilmesi gerekmektedir.³⁶ Kişinin kendi resmi ve şerefi üzerindeki hakkını güvence altına alan düzenlemelerin aynı zamanda ölünün hatırasını da koruma kapsamına aldığı kabulüne göre de, hastanın ölmüş olması mahremiyetini ve verilerinin korunması ihtiyacını ortadan kaldırmamaktadır.³⁷

c. Kimliğin Belirli veya Belirlenebilir Olması

Veri öznesi olan bir gerçek kişinin kimliğinin belirli veya belirlenebilir olması; doğrudan veya dolaylı olarak, özellikle bir kimlik numarası veya kişinin fiziksel, psikolojik, ruhsal, ekonomik, kültürel veya sosyal kimliğine ilişkin bir veya birden fazla unsurun bir araya getirilmesiyle sağlanabilir.³⁸ Kişinin kimliğinin ismi ile doğrudan belirlenebilmesi mümkün iken, bir telefon numarası, ruhsat numarası, sosyal güvenlik numarası, pasaport numarası veya yaş, meslek, ikametgah gibi kişiyi tanımlayan kılın birden fazla anlamlı kriterin birlikte ele alınmasıyla dolaylı olarak da kimliği belirlenebilir.³⁹ Sayma suretiyle belirtilmiş bu kriterler sınırlandırıcı değil örneklendirme amaçlı olup, bir kişinin kimliğinin belirli veya belirlenebilir hale getirecek her türlü bilginin kişisel veri olması mümkündür. Bu kriterlerin koruma

³⁴ Regülasyon Gerekçe md. 27.

³⁵ Örneğin Kanada Kişisel Kayıtlar mevzuatı; ölmüş kişilerin sağlığında yasaklamış olmamaları koşuluyla ve medikal amaçlarla verilerinin işlenebilmesine izin vermektedir. https://www.icrc.org/eng/assets/files/other/icrc_themissing_072002_en_1.pdf (18.11.2017).

³⁶ Veri Çalışma Grubu'nun 4/2007 Sayılı Kişisel Veri Kavramı Hakkında Görüşü (Opinion 4/2007 On The Concept Of Personal Data, Article 29 Data Protection Working Party); AKSOY, *Kişisel Verilerin Korunması*, s. 21.

³⁷ Veri Çalışma Grubu'nun 4/2007 Sayılı Kişisel Veri Kavramı Hakkında Görüşü (Opinion 4/2007 On The Concept Of Personal Data, Article 29 Data Protection Working Party).

³⁸ GDPR md. 4/1.; Direktif md. 2/a.

³⁹ Veri Çalışma Grubu'nun 4/2007 Sayılı Kişisel Veri Kavramı Hakkında Görüşü (Opinion 4/2007 On The Concept Of Personal Data, Article 29 Data Protection Working Party).

kapsamına göre bir tüzel kişinin kimliğini belirlenebilir kılan bilgilere ilişkin olarak da çoğaltılabilmesi mümkündür.⁴⁰

Kişinin kimliğini belirli veya belirlenebilir kılan veri; yalnızca belli bir unsurdan ya da birlikte değerlendirilmesi gereken bir veya birden fazla unsurdan ibaret olabilir. Bu noktada tartışılması gereken, verinin ilgilinin kimliğini hangi şartlarla belirlenebilir kılacak olduğunun tespitidir. Bir verinin kişinin kimliğini belirlenebilir kılıp kılmadığına ilişkin yapılan değerlendirmede; somut olay, verilerin niteliği ve ortaya çıktığı koşulların en başta göz önünde bulundurulması gerekmektedir.⁴¹ Bunun yanı sıra bir veriden yola çıkılarak yapılan araştırmanın ciddiyeti de sıradan bir araştırmadan öte olmak zorundadır. Dolayısıyla eldeki veri, detaylı ve yoğun bir çaba harcanılarak veri öznesinin kimliğini belirlenebilir kılabilecek nitelikteyse kişisel veri olarak kabul edilecektir. Burada yapılacak araştırmanın sınırını araştırmacının makul olmayan bir maddi yükümlülük altına girmemesi oluşturmaktadır.⁴² Bir verinin eldeki tüm makul vasıtalarla ve ciddiyetle değerlendirilmesi yapılmaksızın veri öznesinin kimliğini belirlenebilir kılmadığı, dolayısıyla kişisel veri olarak kabul edilemeyeceği şeklinde bir çıkarımda bulunmak doğru olmayacaktır. Bunun yanı sıra ulusal veri koruma mevzuatımızın hazırlanma sürecinde yapılan değerlendirmelere göre de; verinin kişinin kimliğini belirlenebilir kılıp kılmadığına ilişkin araştırmaların orantılılık ilkesine riayet edilerek yürütülmesi gerekir. Eldeki veriye dayalı araştırma çok fazla zaman veya çaba gerektirmeden kişiyi belirleyebilmemizi sağlayabiliyorsa, bu verinin kişisel veri olarak kabul edilmesi gerekir.⁴³ Birkaç yıl öncesine kadar yapılan araştırmalarda; teknolojik imkanların yetersizliği dolayısıyla elimizdeki verilerden kişinin kimliğine çok fazla çaba harcayarak ulaşabilmekte veya hiç ulaşamamakta iken günümüz teknolojisi bu durumu olumlu yönde değiştirmiştir. Daha önce veri öznesinin kimliğine ulaştıramayan veya orantısız bir çaba gerektirerek kişiye ulaştıran veriler, günümüz teknolojisiyle yapılan araştırmalarda bizi kolaylıkla verinin

⁴⁰ AKSOY, *Kişisel Verilerin Korunması*, s. 18.

⁴¹ Bu değerlendirme yapılırken objektif ve sübjektif temelde hareket edilebilmektedir. Kişiye ilişkin belli verileri daha önce elinde bulunduran bir kişinin sahip olduğu erişim imkanlarıyla verinin, veri öznesinin kimliğini belirlenebilir kıldığı kabul edilebilir ya da objektif bir veri sahibinin elinde bulundurduğu aynı nitelikteki veri ile kişinin kimliğini tespit edebilip edemeyeceği değerlendirilmesi yapılabilir. Bkz. KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 41.

⁴² Veri öznesi olacak kişinin kimliğinin belirlenebilir olmasının tespitinde “kullanılması makul olan tüm vasıtaları” tüketilmek gerektiğine ilişkin bkz. Direktif md. 26. ; AKSOY, *Kişisel Verilerin Korunması*, s. 24.

⁴³ TBMM Adalet Komisyonu 117 Sıra Sayılı Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu <https://www.tbmm.gov.tr> (21.12.2017)

ilişkili olduğu kişiye ulaştırabilmektedir. Örneğin DNA analizi yoluyla saç ve doku incelemesinden kişinin kimliğinin belirlenebilmesi gelişen teknoloji sayesinde mümkün olabilmektedir.⁴⁴ Dolayısıyla daha önce saç veya dokunun, kişinin kimliğini belirlenebilir kılan bir veri olarak kabul edilebilmesi ve veri koruma yasalarının koruma kapsamına sokulabilmesi mümkün değilken bugün için aynı durum söz konusu değildir.

d. Kişiyi İlişkin Olma

Verinin bir kişi ile olan ilişki veya bağlantısı, kişisel veri olarak nitelendirilebilmesinin diğer bir önemli şartıdır. Genel anlamda bir kişi hakkındaki bilginin kişi ile ilişkili olduğu söylenebilir. Pek çok durumda bu ilişki kolay bir şekilde kurulabilirse de belli durumlarda bağlantı kurulmasını sağlamak için gerekli ipucuna kendiliğinden eldeki verilerle ulaşamayacaktır. Böyle durumlarda eldeki verinin; bir kimliğe, karaktere veya davranış şekline işaret etmesi veya bir kişinin davranış ya da olayları değerlendirme şeklinin tespitinde veya değerlendirmesinde kullanılması halinde kişiyle ilişkili olduğunu söyleyebiliriz.⁴⁵

Verinin ilk görünüşte bir kişi hakkında değil de bir eşya, olay veya süreç hakkında olduğu halde de bir verinin kişi ile ilişkili olduğunu düşünebilmek ve bağlantı kurabilmek mümkündür. Bu durumlarda veri ile kişi arasında “amaç”, “içerik” veya “sonuç” unsurları bakımından bir bağlantı aranmaktadır. Örneğin bir şirkete ait telefon kayıtlarının içerikleri, bu verilerin kullanılma amaçlarına göre şirketle, çalışanla veya temizlik personeliyle ilişkili olabilecektir. İçerik bakımında da; açıkça belirli bir hastayla ilişkilendirilmiş tıbbi bir analizin veya belli kişiye ait kimlik kartıyla birleştirilmiş barkodun da içerik itibarıyla kişi ile bağlantı kurulmasını sağladığı için kişisel veri olduğu söylenebilir. Bunun yanı sıra bir uydu takip sistemine bağlı olarak araçlarının konum bilgilerini takip edip bu bilgilere göre müşterilerine daha hızlı hizmet vermeyi amaçlayan bir taksi durağının, amaçların dışında bu sistem vasıtasıyla taksi şoförlerinin hız sınırına uyup uymadığı, hareket halinde veya bekleme de olup olmadığı gibi belli kişisel verilerine de erişebilmesi söz konusu olmaktadır. Bu

⁴⁴ AKSOY, *Kişisel Verilerin Korunması*, s. 25.

⁴⁵ Veri Çalışma Grubunun RFID Teknolojisiyle İlişkili Veri Koruma Konusundaki Çalışma Belgesi, 01/2005 (Working Document On Data Protection Issues Related to RFID Technology, Article 29 Data Protection Working Party)

durum uydu takip sistemine bağı olarak konum bilgilerinin işlenmesinin doğal bir sonucu olarak ortaya çıkmaktadır ve ilk etapta bu verilerin bir kişi ile ilişkili olabileceği kanaati oluşturmamaktadır.⁴⁶

Verilerin kişi ile olan bağlantısı; hukuka aykırı, olağanüstü veya beklenmedik yöntemler kullanılarak kuruluyor veya kurulabiliyorsa bu durumda kabul edilen anlamda verinin kişi ile ilişkili olduğunu ve kişisel veri kavramına dahil kabul edildiğini söyleyemeyiz.⁴⁷ Burada kimliği belirlenebilir kılmaya elverişli yöntemler noktasında yaptığımız açıklamaların göz önünde bulundurulması da bir gerekliliktir. Zira eldeki verinin, kişinin kimliğini belirli kılmaya elverişli olduğu değerlendirmesinde bulunabiliyorsak o veri artık kişiye ilişkin olma vasfını da elde etmiş olmaktadır.

2. Özel Nitelikli Kişisel Veri (Hassas Veri)

Hassas veriler; özellikli korumaya ihtiyaç duyan ve veri sorumlularına daha sağlam temellerde bu verileri işleme yükümlülüğü getiren özel nitelikli kişisel veri grubunun genel adıdır. Özel nitelikli kişisel veri, hassas veri veya verinin özel kategori edilmiş hali olarak nitelendirilebilen bu veri grubunun oluşturulmasının ardındaki düşünce; hassas veri grubuna dahil bilgilerin kötü niyetle kullanımının ve işlenmesinin, mahremiyet ya da ayrımcılığa maruz kalmama temel kişi hakları üzerinde olduğu gibi, diğer kişisel veri kategorilerine dahil verilerin kötüye kullanımına oranla daha vahim sonuçlar yaratabilecek olmasıdır.⁴⁸ Kişilerin cinsel tercihleri veya sağlık bilgileri gibi hassas nitelikli verilerinin, kötü niyetli kullanımı kişinin hem kendisi hem de çevresi için geri döndürülemez ve uzun süre etkisini sürdürecektir neticeler doğurmaya elverişlidir.⁴⁹ Dolayısıyla veri koruma hukukunun, kişisel verilerin işlenmesinin sağlayacağı yarar ve sebep olabileceği tehlike arasındaki dengenin sağlanması temel mantığına göre de bazı veri gruplarının kişisel veri olarak işlenmesi koşulları özel olarak düzenlenmelidir.⁵⁰ Zira bu veri grubuna dahil bilgilerin

⁴⁶ Veri Çalışma Grubu'nun 4/2007 Sayılı Kişisel Veri Kavramı Hakkında Görüşü (Opinion 4/2007 On The Concept Of Personal Data, Article 29 Data Protection Working Party).

⁴⁷ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 42.

⁴⁸ Veri Çalışma Grubu'nun Özel Veri Kategorisine İlişkin Tavsiye Belgesi (Advice Paper on Special Categories of Data "Sensitive Data", Article 29 Data Protection Working Party).

⁴⁹ Veri Çalışma Grubu'nun Özel Veri Kategorisine İlişkin Tavsiye Belgesi (Advice Paper on Special Categories of Data "Sensitive Data", Article 29 Data Protection Working Party).

⁵⁰ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 48.

ilişkin olduğu değerler, toplum içerisinde ayrımcılık yaratma potansiyeli taşıyan dini inanç, etnik köken, cinsel tercih gibi hassas kişilik değerleridir.⁵¹ Bu sebeple de hassas veri kategorisine dahil edilen kişisel verilere özel koruma statüsü sağlanması veri koruma hukukunun göz ardı etmemesi gereken bir gereksinimdir.⁵² Bu ihtiyaç karşısında pek çok ulusal veya uluslararası düzenlemeyle kişisel verilerin özel nitelikli grubu olarak hassas verilerin işlenmesi ayrıca ve özel olarak ele alınmıştır.

Uluslararası düzeyde veri koruma hukukunun ilk bağlayıcı metni olan Avrupa Komisyonunun 108 Sayılı Veri Koruma Sözleşmesi, hassas veri kategorisini; kişilerin ırksal kökenini, politik fikirlerini, dinini veya diğer inançlarını gösteren veya kişilerin sağlığı, cinsel hayatı veya mahkumiyeti ile bağlantılı olan her türlü kişisel verileri olarak belirlemiştir.⁵³ Avrupa Komisyonu bu veri grubuna dahil verilerin korunması konusunda üye devletlere, kapsamını belirleme inisiyatifini de kendilerine bırakarak, uygun teminatların sağlanması yükümlülüğünü de getirmiştir.⁵⁴ 95/46 Sayılı Veri Koruma Direktif'i de Sözleşme'de sayılan veri türlerine ek olarak "felsefi inanç", "sendikal bağlantı" ve "etnik köken" gibi verilerin de hassas veri kategorisine dahil olduğunu hüküm altına almıştır.⁵⁵ Aynı şekilde teknolojik gelişmelerle hayatımızda daha çok yer edinmeye başlayan "biometrik" ve "genetik veriler" de Regülasyon'un 9. maddesi ile özellikli kişisel veri olarak koruma altına alınmışlardır. Ulusal veri koruma mevzuatımızın da bu veri grubuna; kişilerin "kılık ve kıyafeti" ve "vakıf veya sendika üyeliği" hakkındaki bilgilerinin de dahil olduğunu kabul ettiğini görmekteyiz.⁵⁶

⁵¹ ŞİMŞEK, Oğuz, *Anayasa Hukukunda Kişisel Verilerin Korunması*, İstanbul, Beta Basım, 2008, s. 88.; KÜZECİ, *Kişisel Verilerin Korunması*, s.113.

⁵² AIHM de kişisel veri kategorisine dahil olduğu konusunda tereddüt yaratmayan; hücre örnekleri, parmak izi ve DNA profili gibi verilerden, kişiye ilişkin etnik köken gibi özel veri kategorisine dahil bazı verilere ulaştırabilecek olması dolayısıyla hücre örnekleri veya DNA profilinin daha özellikli olarak korunması gerektiğine işaret etmiştir. S. ve Marper-Birleşik Krallık Davası, No: 30562/04, 30566/04, Tarih; 04.12.2008, <https://hudoc.echr.coe.int> (23.01.2018).

⁵³ Adli sicil kayıtlarının özel veri kategorisinde yer almasının, en az sağlık verileri kadar önemli kabul edilmesi gerektiği ve kişilerin sosyal ve ekonomik hayatları üzerinde önemli etkileri olabileceğine ilişkin bkz. KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 50.

⁵⁴ Türkiye'nin de onaylanmasını uygun bularak ülkemizde 18.02.2016 tarihinden itibaren yürürlük kazanmış olan sözleşmeye göre; akit devletlerin hassas verileri işleyebilmesi ancak bu verilerin özel olarak korumasına ilişkin iç hukuklarında yeterli korumanın sağlanması koşuluyla gerçekleşebilecektir. ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 86.

⁵⁵ Direktif md. 8.

⁵⁶ KVKK md. 6.;Türk Ceza Kanunu'nun 135. maddesi ile de hassas veri kategorisine dahil kabul edilen veriler arasında; kişilerin siyasi, felsefi veya dini görüşleri, ırki kökenleri, ahlaki eğilimleri, cinsel yaşamları, sağlık durumları veya sendikal bağlantılarına ilişkin veriler sayılmıştır.

Dolaylı olarak da olsa, sayılan hassas veri kategorisine dahil verilere götüren, ulaştırın veya bu verilerle bağlantı kurulmasını sağlayan verilerin de özellikli olarak koruması gerekmektedir.⁵⁷ Hassas veri grubuna dahil olan veri türlerinin, veri koruma hukukuna ilişkin düzenlemelerde genel olarak sayılmak suretiyle sınırlarının belirlenmesi tercih edilmiştir. Özellikle uluslararası metinlerde bu sınırlandırılmış veri kategorisinin, üye devletler tarafından biyometrik veriler gibi belli veri türleri bakımından genişletilebilmesine imkan verilmiştir. Ancak hassas verilerin sayılarak belirlenmesi ve sınırlandırılması düşüncesine karşılık, her türlü verinin işleme amacına veya kullanılma bağlamına göre hassas veri olabileceği gerekçesiyle bu sınırlandırma şeklinin doğru olmadığı şeklinde eleştiriler de mevcuttur. Buna göre; işlenen her veri türünün, işleme amacına veya bağlamına göre kişinin hassas kabul edilen değerlerine yönelik olabilmesi ve hassasiyet kazanabilmesi mümkündür.⁵⁸ Dolayısıyla hassas veri kategorisine dahil verilerin sayılarak sınırlandırılması yerinde bir tespit yöntemi değildir.⁵⁹ Özellikle teknolojinin hızla gelişmekte olması ve biyometriklerin kullanımının artması gibi veri elde etme yöntem ve türlerinin sürekli değişmesi, hassas veri kategorisine dahil olabilecek verilerin de sürekli olarak güncellenmesini gerektirmektedir.⁶⁰ Dahası kapsamının sayma suretiyle sınırlandırılması bu veri grubunun oluşturulma amacına aykırı neticeler yaratmaya da elverişlidir.⁶¹ Doktrinde bu doğrultuda düşünen müelliflere göre de; kişisel verilerin işleme amacı, yöntemi, somut duruma ilişkin koşullar vb. kriterler dikkate alınmaksızın, baştan belli kategorik ayrımlara tabi tutulması doğru değildir. Zira hassas veya özel veri kategorisine dahil kabul edilmeyen sıradan bir kişisel veri de

⁵⁷ BAŞALP, *Kişisel Verilerin Korunması ve Saklanması*, s. 43.

⁵⁸ “Kimi zaman son derece basit ya da “zararsız” gibi görülen bilgiler de kullanım alanı içerisinde “hassas” olabilir. Nitekim Alman Anayasa Mahkemesi de kişisel bilgilerin önemine göre soyut bir ayrımın yapılmasını reddetmektedir. Mahkemeye göre kişisel verileri “önemliler” ve “daha az önemliler” olarak ayırmamak gerekir. Başlangıçta tehlike taşımayan basit bir bilgi, otomatik işleme sistemleri ile oldukça hassas bir nitelik kazanabilir.” KÜZECİ, Elif, “İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı”, *İnsan Hakları Yıllığı*, C. 32, 2014, s. 68.

⁵⁹ Hassasiyet, önceden veriyi nitelendiren bir özellik olarak hissedilemeyecektir. Fakat her türlü kişisel verinin işleme amacı veya koşullarına bağlı olarak hassasiyet kazanabilmesi mümkündür. Dahası bir verinin hassasiyetinin değerlendirilmesi veriye sadece bakmaktan ötesini gerektirir. SIMITIS, Spiros, “Revisiting Sensitive Data”, *Review Of The Answers To The Questionnaire Of The Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data*, Strasbourg, 1999, s.5. <https://rm.coe.int> (10.11.2017)

⁶⁰ KAYA, Cemil, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, C. 69, S. 1-2., 2011, s. 332.

⁶¹ MCCULLAGH, Karen, “Data sensitivity: proposals for resolving the conundrum”, *Journal of International Commercial Law and Technology*, C. II., S. 4, Manchester 2007, s. 190. <http://usir.salford.ac.uk/2745/>; KÜZECİ, *Kişisel Verilerin Korunması*, s. 50.

belli işleme faaliyetleri neticesinde hassasiyet kazanabilmesi mümkündür.⁶² Sıradan kişisel verilerin, işlenme koşulları veya işleme amacı doğrultusunda hassas veri kategorisine dahil edilebilir olması, özellikle kişinin görüntüsü ve/veya sesini içeren verileri de bazı durumlarda hassas veri olarak kabul edebilmemizi sağlaması bakımından önem taşımaktadır.⁶³ Bu konuda Avusturya, Danimarka, Fransa, İrlanda, İtalya, Norveç ve İsveç gibi ülkeler, kişinin ses ve görüntüsüne ilişkin verinin sınıflandırılması ile işlenme amacı arasındaki bağlantıyı vurgulamışken; fotoğraf veya videodaki verilerinin kişinin ırkı veya cinsel davranışlarına dair bir bilgi ortaya çıkarma potansiyeli taşıması halinde hassasiyet kazanacağı kanaati benimseyen, Almanya, İtalya ve Norveç gibi, ülkeler de bulunmaktadır.⁶⁴

Genel Veri Koruma Regülasyonu, Direktif ve Sözleşme'nin hassas veri kategorisine giren verileri sayma suretiyle (numerus clausus) sınırlandırılma yoluna gitmiş olması, bu konuya yönelik doktrindeki eleştiriler de nazara alındığında, ilk etapta bu veri türlerinin oluşturulma ve korunma ihtiyacını tam ve güncel olarak karşılayamayacağını düşündürebilmektedir. Ancak devletlerin, asgari koruma standartlarını karşılamak koşuluyla ulusal düzenlemelerde hassas veri kategorisine dahil olan veri türlerini genişletebilme özgürlüğü bulunmaktadır. Asgari koruma standartlarının ne surette sağlanmış olacağı belirsizlik yaratmaya elverişli bulunmakta ise de, bu noktada hassas verilerin işlenme yasağının istisnalarından yola çıkılarak değerlendirmede bulunulabilir. Hassas verilerin kural olarak işlenmemesi esas iken bu verilerin işlenebileceği genel istisnai haller; veri öznesinin açık rızasının mevcut

⁶² KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 48.; SEYREK TÜTÜNCÜBAŞI, Deniz, *Kişilerin Kendisine Ait Verilerin Kaderini Tayin Hakkının Ceza Hukuku Yoluyla Korunması*, (Yayınlanmamış Yüksek Lisans Tezi), Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir, 2015, s. 17.

⁶³ Örneğin; Bir kişinin dini inancını gösteren başı örtülü bir fotoğrafının veya engelli olduğunun anlaşılmasına olanak veren bir fotoğrafının kişisel veri olarak işlenmesi hali ile bu durumu beyan ederek veya raporlayarak işlemek arasında bu verilerin hassasiyet taşıdığı gerçeği karşısında bir fark olduğundan söz edilebilecek midir? Bkz. KAYA, Cemil, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", s. 330.; Naomi Campbell/MGN davasında Bayan Campbell'in fotoğraflarının onun etnik kökenine ilişkin hassas veri olarak kabul edilmesine karşın işlenme amacı bakımından hassas veri olarak kabul edilemeyeceği istikametinde karar verilmiştir. Campbell/Mirror Group Newspapers [2002] EWHC 299.; MENDOS KUŞKONMAZ, Elif, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013, s. 108.

⁶⁴ SIMITIS, Spiros, "Revisiting Sensitive Data", s. 7.; Örneğin; Kişinin gözlüklü şekilde çektiği olduğu resminden yola çıkılarak hassas veri kategorisine dahil olan sağlık bilgisine ulaşılabilir olması veya isminin dini inancını yansıtır nitelik taşıması gibi hallerde somut olayın koşulları ve verilerin işlenme özellikleri dikkate alınarak değerlendirmede bulunulması halinde bu veriler de hassas verilere ilişkin özellikli koruma kapsamında olabilecektir. KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 52.

olması ve hayati çıkarlarının korunması için verilerin işleme zorunluluğunun bulunması, kamuya yararına çalışan veri sorumlusunun bu amaçla verileri işlemesi, yargılama faaliyeti gereğiyle verilerin işlenmesi ve işleme konusu verilerin daha önce veri öznesi tarafından kamuya açıklanmış olması halleridir.⁶⁵

B. Kişisel Verilerin Korunması Kavramı, Gerekliliği ve Tarihsel Süreçte Gelişimi

1. Kişisel Verilerin Korunması Kavramı ve Kapsamı

Kişisel verilerin korunması; verilerin toplanması, değiştirilmesi ve benzer şekilde işlemesi süreci öncesinde veri öznesinin bu işlemlere rıza gösterip göstermeme iradesine sahip olmasını, işleme sırasında temel veri koruma ilkelerine uygun işlemenin gerçekleştirilmesinin sağlanmasını ve neticede bu veri koruma tedbirlerine riayet edilmeksizin hukuka aykırı verilerin işlenmesi karşısında hukuki yollara başvurulabilme güvencesini sağlayan temel bir kişilik hakkıdır.⁶⁶ Bu hakkın kullanılmasıyla amaçlanan; verilerin işlenmesine ilişkin üstün kamusal veya bireysel menfaatler ve işleme sebebiyle özel yaşamına yönelik bir müdahaleye maruz kalan veri öznesinin kişilik hakları arasındaki dengenin sağlanabilmesidir.⁶⁷ Bu doğrultuda istenilen kişisel verilerin hiçbir şekilde işlenmemesi değil,⁶⁸ belli güvence, sınırlandırma, ilkelere bağlı olarak ve veri öznesinin verileri üzerindeki denetim hakkını tamamen ortadan kaldırmaksızın verilerin işlenmesidir. Zira teknoloji çağının

⁶⁵ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 53.; KAYA, Cemil, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, s. 323

⁶⁶ AKSOY, *Kişisel Verilerin Korunması*, s. 1.

⁶⁷ “Kişisel verilerin hukuki niteliği hakkında farklı yaklaşımlar mevcuttur. Kişisel verileri Kıta Avrupası, kişilik hakkı kapsamında değerlendirirken, Amerikan hukuku mülkiyet hakkı kapsamında değerlendirmektedir. Ayrıca kişisel verileri, veri sahibinin kişisel bilgileri ile eser sahibinin eseri üzerindeki manevi hakları arasındaki benzerlikler kurarak fikri mülkiyet kapsamında değerlendiren görüş de mevcuttur. Kişilik hakkı görüşü, kişisel verilerin niteliğine daha uygun düşmektedir. Fakat kişilik hakkının kişiye sıkı sıkıya bağlı olma özelliğinin aksine, mülkiyet hakkı görüşünün değindiği üzere kişisel verilerin üçüncü kişilere aktarımı ve devri mümkündür. Bu yüzden kişisel verilerin daha etkin korunması adına, insan onuruna ve kişiliğin serbestçe geliştirilmesi hakkına dayanan, bilgilerin geleceğini belirleme hakkı türetilmiştir.” AYGÖZER, A. Çiğdem, *Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması*, (Yayınlanmamış Doktora Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2016, s. 254 ;“*Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.*” Anayasa Mahkemesi E: 2010/40, K: 2012/8, T: 19.01.2012.

⁶⁸ KÜZECİ, *Kişisel Verilerin Korunması*, s. 2.

kaçınılmaz bir gereği olarak her birimizin verileri işleme konusu yapılmak zorundadır.⁶⁹ Bu durum karşısında kişisel verilerin korunması; bilgi güvenliğine ilişkin alınacak önlemler ve hukuki düzenlemeler kanalıyla sağlanabilecektir.⁷⁰

Kişisel verilerin korunmasının, ulusal hukuki düzenlemelere konu edinilmeye başladığı 1970’li yıllardan itibaren, bilgi sistemlerinin kamusal ve özel kurumlar hatta bireyler tarafından kullanımının giderek yaygınlaşmasıyla uluslararası platformda da kişisel verileri koruyucu düzenlemeler yapılmaya başlanmıştır. Kişisel verilerin uluslararası hukukta korunmasına ilişkin girişimler ayrıca bu hakkın özel yaşam hakkı kapsamında kişilere sağlanan korumaya dahil olduğu yönünde içtihatlarla da vücut vermiştir.⁷¹ Özel yaşamın neye karşılık geldiği ve kapsamının ne kadar geniş tutulabileceği tartışılmakta olan bir husus olmakla birlikte kişiye ilişkin verilerin özel yaşama dahil olduğu hem uluslararası yüksek mahkemeler nezdinde hem de doktrinde kabul görmektedir.⁷² Bu iki hak bakımından da korunması amaçlanan değerler sadece insan olmakla doğrudan kazanılan insan onuru, kişilik ve kişisel otonomi gibi değerlerdir.⁷³ Kişisel verilerin korunmasını, hukuki uygulamada özel yaşam hakkından farklı biçimde görmeye mahal yoktur.⁷⁴

Bu istikamette Anayasa Mahkemesi’nin de kişisel verilerin korunmasına ilişkin temel değerlendirmesi; “Kişisel verilerin korunması temel hakkı, anayasa hukukunda esas olarak yüksek kişilik değerlerini korumaya yönelik bireysel haklara ilişkindir. Bu hak, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır.” şeklindedir.⁷⁵

⁶⁹ ARSLAN, Çetin, “Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması”, s. 480

⁷⁰ HENKOĞLU, *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, s. 20.

⁷¹ AIHS md. 8.; BM Medeni ve Siyasi Haklar Sözleşmesi md. 17.; ABTHŞ md. 7., 8.

⁷² HENKOĞLU, *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, s. 31.

⁷³ KÜZECİ, *Kişisel Verilerin Korunması*, s. 88.

⁷⁴ PURTOVA, Nadezhda, “Private Law Solutions In European Data Protection: Relationship To Privacy, And Waiver Of Data Protection Rights”, *Netherlands Quarterly of Human Rights*, C. 28, S. 2, 2010, s. 184.

⁷⁵ Anayasa Mahkemesi, E: 2013/84, K: 2014/183, T: 04.12.2014. <http://www.anayasa.gov.tr> (08.03.2018).

2. Kişisel Verilerin Korunmasının Tarihi Gelişimi ve Bilgi Toplumu

İlkel toplum, tarım toplumu, sanayi toplumu ve günümüz bilgi toplumu, dünyamızın belli bir istikamette evrildiği ve toplum içerisinde belli faktörlerin daha ön plana çıkmakla topluma yön verdiği tarihi süreçlerdir. Günümüz bilgi toplumunda ise, itibar sahibi olan enformasyon, veri, data gibi kavramlar olup bu kavramların tam manada anlaşılabilmesi ve birbirinden ayrıştırılabilmesi sorunlu bir alan yaratmaktadır. Bunun yanında güç ve her neye ilişkin olursa olsun bilgiyi elinde bulundurma, bilgi toplumunda güce eşdeğer tutulmaktadır. Zira bu toplumda ticareti yapılabilen bir nesne konumunda olan bilgi, ekonomik olarak da bir değere sahiptir.⁷⁶ Bilginin gittikçe itibar kazanan tarihsel süreç içerisindeki gelişimiyle eşdeğer olarak bilginin ilişkili olduğu kişilerin, kişisel verilerini korunma ihtiyacı ortaya çıkmış ve bu ihtiyaç giderek önem kazanmıştır.

Kişisel verilerin ve mahremiyetin korunması düşüncesinin tarihsel gelişim sürecindeki ilk görünümü; belli meslek mensuplarına meslekleri sebebiyle öğrendikleri bilgiler dolayısıyla getirilen sır saklama yükümlülüğüdür. Denilebilir ki; kişisel verilerinin korunması düşüncesi, M.Ö. 5. yüzyılda hekimin sır saklama yükümlülüğüne ilişkin olarak düzenlenmiş olan Hipokrat yeminden itibaren günümüze kadar uzun bir tarihi serüven geçirmiştir.⁷⁷ Modern anlamda ve günümüzdeki veri koruma şekillerine daha yakın haliyle verilerin korunması, 1960'lı yıllar itibarıyla toplumsal bir sorun olarak görülmüş ve 1970'li yıllardan itibaren de hukuki düzenlemelere konu edinilmeye başlamıştır.⁷⁸ Kişisel verilerin, gerek İsveç ve Almanya örneğinde olduğu gibi nüfus sayımı ve nüfusa ilişkin verilerinin veri bankalarında toplanması gibi yönetsel ihtiyaçlarla kamusal organlar tarafından, gerekse Amerika örneğinde olduğu gibi kişilerin kredi verilebilirlik değerlerini tespit etmek üzere ekonomik gerekçelerle özel kurumlar tarafından işlenmesi üzerine, kişilerin bu müdahalelere karşı korunması düşüncesi ilk defa yükselmiştir. Bu doğrultuda kişileri, verileri üzerinde yeniden denetim imkanına kavuşturmayı amaç edinen hukuki düzenlemeler de ilk kez Avrupa'da oluşturulmuştur.⁷⁹ Böylelikle kişisel verilerin korunması ulusal düzeyde hukuki düzenlemelere konu edilmeye

⁷⁶ AKSOY, *Kişisel Verilerin Korunması*, s. 3.

⁷⁷ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 6.

⁷⁸ KÜZECİ, *Kişisel Verilerin Korunması*, s. 20, 116.

⁷⁹ KÜZECİ, *Kişisel Verilerin Korunması*, s. 45.

başlamıştır.⁸⁰ Verilerin, teknolojik gelişmelerin sağladığı sınırsız imkanlar vasıtasıyla seyyal ve hızla yer değiştirebilir bir hal alması ise kişisel verilerin korunmasının uluslararası düzenlemelerle güvence altına alınmasını gerektirmiştir. Bu gibi ihtiyaçlarla ortaya çıkan veri koruma hukukunun uluslararası ve bağlayıcı ilk örneği olarak 1981 yılında kabul edilen 108 sayılı “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması” Avrupa Konseyi sözleşmesini gösterebiliriz. Bu sözleşmenin düzenlenmesinden bir yıl öncesinde ise OECD tarafından üye devletlere veri koruma hukukunun asgari prensiplerini belirlenmek suretiyle, ulusal düzenlemelerinde yol gösterici olmak amacıyla OECD Rehber İlkeleri düzenlenmiştir. Veri koruma hukuku bakımından Avrupa Birliği bünyesinde 1995 yılında 95/46 Sayılı Kişisel Verilerin Korunması Direktifi’nin yayınlanması ise gerek uluslararası düzenlemeler gerekse ulusal düzenlemeler açısından önemli bir dönüm noktasıdır.⁸¹ 95/46 Sayılı Direktif’in 2018 yılı itibarıyla yürürlük kazanacak olan 2016/679 sayılı Avrupa Birliği Veri Koruma Regülasyonu ile mülga edilecek olduğunun altını çizmekte de fayda görmekteyiz. Çalışmamızın ileriki kısımlarında uluslararası düzenlemelerde veri koruma hukukun kronolojisine ilişkin daha detaylı bilgiye yer verilecektir.

3. Kişisel Verilerin Korunması Gerekliliği

Bilgi, elde edilmesi günümüzdeki kadar kolay olmasa da tarihi süreçler içerisinde kişilerin denetim altında tutulması, kolay yönetimi gibi amaçlarla gerek devletler⁸² gerekse özel sektör için daima doyumsuz bir iştah yaratmıştır.⁸³ Toplum içerisinde bazen maddi çıkarların tatmini⁸⁴ amacı, bazense siyasi politikalarının

⁸⁰ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 10.

⁸¹ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 11.

⁸² Toplumsal yönetimin rasyonelliğini sağlamak üzere kurallar koyan devletin, bu kurallara uygun davranılıp davranılmadığına veya öngördüğü toplum düzenine muhalif faaliyetler yürütülüp yürütülmediğine ilişkin bilgi sahibi olma ve toplumu bu amaçla gözetim altında tutma eğilimi modernizme dayalı olarak ivme kazanmıştır. KARAKEHYA, Hakan, “Gözetim ve Suçla Mücadele”, Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 58, S. 2, 2009, s. 332.

⁸³ LYNKEY, Orla, *The Foundations of EU Data Protection Law*, United Kingdom, Oxford University Press, 2015, s. 1.; KARAKEHYA, “Gözetim ve Suçla Mücadele”, s. 324.

⁸⁴ Örneğin; bir kimsenin internetteki bir alışveriş sitesinde gerçekleştirdiği alışveriş veya gezinme sırasında cookies vb. yöntemlerle elde edilen verileri daha sonra kişiye benzer veya aynı ürüne ilişkin daha cazip bir teklif içeren mail, çevrimiçi reklamcılık vb. yöntemlerle ulaşılması ve kişinin alışveriş alışkanlıklarının yönlendirmesi aracı olarak kullanılabilir. Benzer şekilde, İngiltere Rekabet ve Piyasa Otoritesi(CMA) tarafından; giyim, sigorta ve online uygulama sektörlerinde tüketicilerin verilerinin ticari amaçla toplanma ve kullanılma yöntemlerine ilişkin yürütülen bir çalışma göstermiştir ki; müşterilere ait kişisel verilerin kullanılmasının, tüketici, firmalar ve

etkinliğini sağlamak, tehlikeden ve riskten kaçınmak⁸⁵, bireyleri kolay kontrol edebilmek ve yönlendirebilmek/yönetebilmek⁸⁶ gibi amaçlarla bazense sadece basit bir merak⁸⁷ sebebiyle kişilere ilişkin bilgilerinin elde edilmesi ve kişilerin gözlemlenmesi ihtiyacı duyulmuştur.⁸⁸ Modern dünyanın temel bir özelliği ve getirisi olarak⁸⁹, çeşitli ihtiyaçların tatmini amacına yönelik davranışları gözetim altında tutulan, bilgileri toplanan, işlenen veya oldukça hızlı biçimde aktarılan bireylerin, bu süreçlere ilişkin hiçbir hak sahibi olmaması⁹⁰, habersiz kalması veya müdahale imkanından yoksun bırakılması, kişinin özgür iradesine göre şekillendirebileceği kendine ait özel bir hayatının kalmamasına⁹¹ ve dolayısıyla kimliksel bunalıma girmesine yol açmak gibi ağır neticelere sebep olabilecektir.⁹² Kişinin kendisine ilişkin olan üzerinde kontrolsüz bırakılması, aslında onu kendisi yapan değerlerinin ve bireyselliğinin korunması olanağını da ortadan kaldıracaktır.⁹³ Bunun yanı sıra

sektörler için, ürünlerin ve hizmetlerin kişiselleştirilmesi, daha iyi müşteri analizi ve hedefli reklamcılık ve özel tekliflerle artan satışlar gibi önemli faydaları söz konusu olabilmektedir. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf (06.01.2018)

⁸⁵ Toplum içerisinde suça karışan insan oranındaki artışa ve özellikle terör gibi toplumsal tahribatı daha ağır suçların yaygınlaşmasına bağlı olarak devletlerin bireyler üzerindeki gözetimi de yoğunlaşmaktadır. Dahası devletin, tehlikeliliği azaltmak adına özel yaşamın gizliliği gibi temel haklarına yönelik müdahaleleri karşısında bireylerin, güvenlikten yana tercihte bulunarak zamanında kazanma mücadelesini verdiği bu gibi temel haklarından feragat ettiği görülmektedir. KARAKEHYA, “Gözetim ve Suçla Mücadele”, s. 320., 354.

⁸⁶ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 5.

⁸⁷ Bunun dışında, ticaretle uğraşan bir kişi için, müşterilerinin alışveriş alışkanlıklarından yola çıkarak kar artırmak; kamusal ve idari organlar için toplumsal refah, güven, istikrar ve belki iktidarın devamlılığının sağlanmak, kişisel verilerin toplanması veya işlenmesi için amaç edinilebilmektedir. KÜZECİ, *Kişisel Verilerin Korunması*, s.20.; OĞUZ, Habip, “Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum”, *Uyuşmazlık Mahkemesi Dergisi*, S. 3, 2013, s. 5.

⁸⁸ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 59.

⁸⁹ BAUMAN, Zygmunt, LYON, David, *Liquid Surveillance: A Conversation*, United Kingdom, Polity Press, 2013, s.7.; Modern bir sosyal devletin, halkın huzur ve istikrarını sağlamak üzere yönetim, planlama ve ihtiyaçların öngörülebilirliği sebepleriyle vatandaşlarının veya başkalarının kişisel verilerine ihtiyaç duyması olasıdır. KÜZECİ, *Kişisel Verilerin Korunması*, s. 23.

⁹⁰ Bu konuda 1983 yılında Alman Anayasa Mahkemesi’nin “*bilgilerin geleceğini belirleme hakkı*” nı ihdas eden ve nüfus sayım kanunun bu hakka yönelik bir ihlal yarattığı gerekçesiyle iptal edilmesi gerektiğine ilişkin kararı bir dönüm noktası oluşturmaktadır. KÜZECİ, *Kişisel Verilerin Korunması*, s. 76.

⁹¹ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 4.

⁹² KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s.70.; KARAKEHYA, “Gözetim ve Suçla Mücadele”, s. 354.

⁹³ Dahası özgür ve demokratik bir toplum ancak kendi geleceğini kendisi belirleyebilecek, hareket serbestisine sahip ve özel olarak da kişisel bir değer olarak verileri üzerinde serbest tasarruf yetkisine sahip bireyler tarafından oluşturulabilecektir. ÇEKİN, Mesut Serdar, “6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi”, *İÜHFİM*, C. 74, S. 2, 2016, s. 633.; Kişinin madden ve manen özgürlüğüne yönelik bir tehdit olarak gözetimi ve kişisel verilerin elde edilmesi iştahının çarpıcı sonuçları pek çok edebi çalışmaya da konu olmuştur. Bunların arasında George Orwell’ın “1984” ve Franz Kafka’nın “Dava” adlı eserleri gözetim toplumunun bireylerin kişilikleri üzerindeki ağır neticelerini göstermesi itibarıyla önemli nitelikte çalışmalardır.

kişisel taşıyan verilerin çeşitli şekillerde haksız kullanımı neticesinde veri sahibi kişinin, özel hayat mahremiyeti ve dolayısıyla kişilik hakları ihlal edilmiş olmaktadır. Bu ihlallerin de veri sahiplerinin maddi veya manevi olarak zarara uğramasına sebep olacağı şüphesizdir. Bütün bu gerekçelerle kişisel verilerin etkin şekilde korunması sağlanarak bireylerin maddi veya manevi varlıklarını korunmasına hizmet edilmiş olmaktadır.⁹⁴

Özetle kişinin, günümüz bilgi toplumunun bir üyesi olarak verilerinin toplanması, kaydedilmesi, işlenmesine imkan veren pek çok teknolojik vasıtanın mevcudiyeti⁹⁵ ve bu teknolojinin hızla gelişiminin ve mobil bilgisayar teknolojilerinin yaygın kullanımının olumsuz sonuçları arasında; bilginin hızlı ve hatta bilgi sahibi kişiden bağımsız şekilde yayılması, depolanabilmesini, erişilebilmesi ve işlenebilmesini gösterebiliriz.⁹⁶ Bilgi toplumunda verilerin gittikçe artan akışkanlığı ve insanlarda yarattığı sürekli olarak takip altında olduklarına ilişkin kaygılar ve karşı tarafta verilere duyulan gereksinim, veri korumasını ortaya çıkaran temel üç unsur olarak kabul edilebilir.⁹⁷

C. Kişisel Verilerin İşlenmesi Kavramı ve İşlemenin Kapsamı

Kişisel verilerin işlenmesi kavramının tam ve doğru olarak anlaşılabilmesi için öncelikli olarak bu sürece müdahil olan süreçlerin ve kişisel veri kavramının ele alınması gerekmektedir. Çalışmamızın bu kısmına kadar “kimliği belirli veya belirlenebilir kişiye ilişkin her türlü bilgi” kişisel veri olarak tanımlanmış ve tanım doğrultusunda tüm yönleriyle kişisel veri kavramı açıklanmaya çalışılmıştır. Bu noktada veri işleme sürecinin süreçlerinin veya baş aktörlerinin kimler olduğu ve nasıl tanımlandığının, ele alınması gerekecektir. Veri işleme sürecinde rol alan; veri öznesi, veri sorumlusu ve veri işlemecisi baş aktörlerini kısaca tanımak gerekirse, öncelikle veri öznesinin tanımlanması en doğrusu olacaktır. Veri öznesini; kendisini

⁹⁴ AKSOY, *Kişisel Verilerin Korunması*, s. 2.

⁹⁵ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 4.; Modern teknolojiyle üretilmiş yeni nesil araçların pek çoğunda yer tespitini sağlamaya yönelik GPS sistemleriyle araçların konum bilgilerinin toplanması ve kayıt altına alınması, hatta bu sistem sayesinde aracın yol tutuşu da dahil belli bilgilerin kayıt altına alınabiliyor olması teknolojinin kişisel verilerin toplanmasına hizmet eden vasıtalarının bir örneği olarak sunulabilir. KÜZECİ, *Kişisel Verilerin Korunması*, s. 42.

⁹⁶ LYNKEY, *The Foundations of EU Data Protection Law*, s. 2. ; EVANS, A., “European Data Protection Law”, *The American Journal of Comparative Law*, C. 29, S. 4, 1981, s. 571.

⁹⁷ KÜZECİ, *Kişisel Verilerin Korunması*, s. 21.

belirli veya belirlenebilir kılan verilerin ilişkili olduğu, verileri işleme konusu yapılan ve korunması gereken “ilgili kişi”⁹⁸olarak tanımlayabiliriz.⁹⁹

En genel şekliyle veri sorumlusu¹⁰⁰; Veri Koruma Direktif’i ve Regülasyon ile aynı doğrultuda ulusal veri koruma mevzuatımızın da benimsediği şekilde “kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi”¹⁰¹ olarak tanımlanmaktadır. Veri işlemecisi ise belirtilen şekilde tanımlanan veri sorumlusunun namına ve sorumludan aldığı yetkiye dayanarak verileri işleyen kişidir.¹⁰² Veri sorumlusu tarafından alınan karara bağlı olarak mevcudiyet kazanan veri işlemecisi; kişisel verilerin, kendi organizasyonu kapsamında veya daha geniş bir organizasyonun kısmen veya tamamen yetkilendirmesiyle işlenmesine karar verebilmektedir.¹⁰³ OECD Rehber İlkeleri’nde veri sorumlusu; bizzat sorumlu veya yetkili kıldığı temsilcisi tarafından toplanmış, yayılmış, depolanmış veya işlenmiş olup olmadığına bakılmaksızın kişisel verilerin, ulusal hukukta kullanılması ve kullanım içeriğinin belirlenmesi konusunda karar vermeye yetkili olan kişi olarak tanımlanmıştır.¹⁰⁴ 108 sayılı Avrupa Birliği Sözleşmesi’nin “otomatik veri dosyasının amacının ne olacağı, hangi kişisel veri kategorilerin kaydedilmesi gerektiği ve bunlara hangi işlemlerin uygulanacağı hakkında karar verebilecek olan gerçek veya tüzel kişiler, kamu kurumu, birimi veya ulusal kanunlara göre yetkili olan diğer kuruluşlar” şeklinde tanımladığı “dosya yöneticisi” de, bu tanımdan yola çıkılarak söylenilebilir ki veri sorumlusuna karşılık olarak kullanılmıştır.¹⁰⁵

Bu noktada veri sorumlusunun tespiti, veri koruma prosedürünün işletilebilmesi adına kritik öneme sahiptir. Zira veri sorumlusunun tespit edilmesi; veri

⁹⁸ KVKK md. 3. ç. bendinde ilgili kişi; kişisel verisi işlenen gerçek kişi olarak tanımlanmış olup, ulusal metinler de veri öznesinin genel kabul gören karşılığı olmuştur. Bkz. 01.09.2014 tarihinde TBMM tarafından onaylanması uygun bulunmuş 108 Sayılı “Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi” resmi çevirisi. <http://www2.tbmm.gov.tr/d24/1/1-0966.pdf> (01.02.2018).

⁹⁹ KÜZECİ, *Kişisel Verilerin Korunması*, s.17.

¹⁰⁰ Veri sorumlusu kavramını karşılık olarak “veri denetçisi” veya “veri kütüğü sahibi” terimlerinin de kullanıldığı görülmektedir. KÜZECİ, *Kişisel Verilerin Korunması*, s.18.

¹⁰¹ Direktif md. 2/e.; Regülasyon md. 4/7. Veri sorumlusu olarak gerçek ve tüzel kişilerin yanı sıra kamusal otorite, temsilci veya diğer makamlara da yer verilmiştir.

¹⁰² KVKK md. 3/ğ.

¹⁰³ Veri Çalışma Grubu’nun 1/2010 Sayılı Veri Sorumlusu ve İşlemecisi Kavramları Hakkındaki Görüşü (Opinion 1/2010 On The Concepts Of "Controller" And "Processor", Article 29 Data Protection Working Party)

¹⁰⁴ OECD Rehber İlkeleri md. 1/a.

¹⁰⁵ Avrupa Konseyi 108 sayılı Sözleşme md. 2/d.

koruma kurallarının ihlaline ilişkin kimin sorumlu veya muhatap tutulması gerektiği¹⁰⁶, yükümlülük getiren normların muhatabının kim olduğu ve veri öznesinin haklarını uygulamada kime karşı ve nasıl kullanabileceğinin belirlenmesini sağlamaktadır. Veri sorumlusunun veri koruma hukukunda bir yer işgal etmesinin de önemi büyüktür. Şöyle ki; veri işleminin tamamıyla otomatik sistemlere bağlı ve bir veri sorumlusu olmaksızın gerçekleştirilmesi, ilgili kişiyi de bu otomatik karar alma mekanizmalarının basit bir objesi haline getirecek ve kişisel verilerin korunması hakkı ve temel ilkelerini işlevsiz bırakacaktır.¹⁰⁷

1. Genel Olarak Veri İşleme Kavramı

Veri öznesi, sorumlusu ve işlemecisinin dahilinde gerçekleştirilen veri işleme; Avrupa Birliği Veri Koruma Direktifi'nde ve bu Direktif'i yürürlükten kaldırarak, 25 Mayıs 2018 tarihinden itibaren yürürlük kazanacak olan Genel Veri Koruma Regülasyonu'nda otomatik veya otomatik olmayan vasıtalarla, kişisel veriler ve verilere dahil unsurlar üzerinde gerçekleştirilen her türlü işlemi ifade edecek şekilde tanımlanmıştır.¹⁰⁸ Diğer bir deyişle; kişisel verilerin korunması alanı içerisinde bir veya birden fazla kişi veya kuruluşun müdahil olduğu sürece ilişkin tüm işlemlere genel olarak kişisel verilerin işlenmesi diyebiliriz.¹⁰⁹ Uluslararası düzenlemeler ile yapılan bu tanımlamalarla aynı istikamette 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nu 3/e. fıkrasına göre de işlemin otomatik veya otomatik olmayan ve hatta yarı otomatik olan yollardan gerçekleştirilmiş olması mümkün kabul edilmiştir.¹¹⁰ Münhasır olarak verilerin otomatik olarak işlenmesi karşısında bireylerin korunmasına yönelik düzenlenmiş olan Avrupa Konseyi 108 sayılı Sözleşmesi de “tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılmasını” verilerin işlenmesi olarak tanımlanmıştır.¹¹¹

¹⁰⁶ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 101.

¹⁰⁷ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 102.

¹⁰⁸ GDPR md. 4/2.

¹⁰⁹ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 55.

¹¹⁰ KVKK md. 3.

¹¹¹ Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi md. 2/c.

2. Veri İşlemenin Kapsamı

Kişisel veriler üzerinde, hangi fiillerin hangi yollarla gerçekleştirilmiş olmasının veri işleme olarak kabul edileceğinin tespiti, veri işlemenin kapsamını oluşturmaktadır. Genel anlamda veri işleme otomatik veya otomatik olmayan yollarla gerçekleştirilebilir. Verilerin otomatik veya yarı otomatik yoldan işlenmesi ile kast olunan bir otomasyon sistemi tarafından kullanılan yöntemlerle verilerin işlenmekte olmasıdır. Örneğin; bir işyerinde çalışan işçilerin verilerinin bilgisayar sistemi üzerinde işlenmesi¹¹² ya da bir üniversitenin, öğrencilerinin not veya öğrenim durumlarına ilişkin bilgilerini bir sistem üzerinde tutması verilerin otomatik yollarla işlenmesidir.

Verilerin otomatik veya otomatik olmayan yollarla işlenmiş olması, verilerin korunmasının kapsamına dair genel anlamda bir değişiklik yaratmamaktadır. Kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili olan bilginin kağıt üzerinde veya bilgisayarda tutulması arasında kişisel veri kabul edilmesi bakımından fark yoktur.¹¹³ Ancak kağıt üzerinden gerçekleştirilen veri işlemelerinin, diğer bir deyişle otomatik olmayan vasıtalarla işlemenin, ancak kaydedilme biçimi itibarıyla işleyene bu veriye erişim açısından belli bir kolaylık sağlaması,¹¹⁴ bir dosyalama sisteminin parçası olarak veya olması niyetiyle işlenmiş olması gerekmektedir.¹¹⁵ Bunun yanı sıra gerçek kişilerin, şahsi amaçlarla ve sırf kişisel veya ailevi ilişkilerine ilişkin olarak otomatik veya otomatik olmayan yollarla yaptığı veri işleme faaliyetleri koruma kapsamının dışındadır.¹¹⁶ Avrupa Konseyi 108 Sayılı Sözleşmesi gibi uluslararası bazı sözleşmeler ve ulusal düzenlemelerle de verilerin yalnızca belli surette işlenmesi korunabilmektedir. Ancak Sözleşme'nin de öngördüğü gibi sadece otomatik yollarla veri işleme faaliyetlerini korumakta olan düzenlemelerde, devletlere koruma kapsamını genişletebilme inisiyatifi de bırakılmaktadır.¹¹⁷

¹¹² BAŞALP, Kişisel Verilerin Korunması ve Saklanması, s. 33.

¹¹³ AKSOY, *Kişisel Verilerin Korunması*, s. 17.

¹¹⁴ Direktif Gerekeçe md.15. Erişim kolaylığı sağlamaya yönelik olarak verilerin alfabetik veya kronolojik bir sıralamaya tabi tutulmuş olması bu kapsamda veri işlemeye ilişkin örnek olarak gösterilebilir. Bkz. BAŞALP, Kişisel Verilerin Korunması ve Saklanması, s. 33.

¹¹⁵ Direktif md. 3/f.1.

¹¹⁶ Örneğin; mektuplaşma ve adres kayıtlarının tutulması gibi veri işleme faaliyetleri veri koruma hükümlerinin uygulama alanının dışında tutulmuştur. Bkz. Direktif Gerekeçe md.12.; KVKK md. 28/1 a.

¹¹⁷ İş bu sözleşme 18.06.2016 tarihinde Resmi Gazete' de yayınlanmış olup, bu tarihten itibaren ülkemizde yürürlük kazanmıştır. Türkiye, Sözleşme hükümlerinin yalnızca verilerin otomatik yollarla değil otomatik olmayan yollarla işlenmesi halinde de uygulanacağını kabul etmiş ve bu istikamette sözleşmenin uygulama kapsamını genişletici ek beyanlarda bulunmuştur. Kişisel

Otomatik veya otomatik olmayan yöntemlere dayalı olarak yapılan her türlü; toplama, kayıt altına alma, organize etme, depolama, değiştirme veya uyarılma, geri alma/kurtarma, sorma, kullanma, transfer yoluyla açığa çıkarma, yayımlama veya yayımlamaya uygun hale getirme, ilişkilendirilme veya kombinasyon kurma, bloke etme, silme, tahrip etme fiillerinin gerçekleştirilmesi veri işleminin kapsamındadır.¹¹⁸ Direktif'in belirlediği bu fiillere ek olarak Regülasyonun 4. maddesinde yapılandırma ve kısıtlama fiillerinin de işleme kapsamında olduğu kabul edilmiştir. Ulusal veri koruma mevzuatımıza göre de veri işleminin kapsamı; “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” şeklinde belirlenmiştir.

Kişisel verilerin, özellikle istatistiksel veya kamusal ihtiyaçların tespiti gibi amaçlarla işlenmesine ihtiyaç duyulması hallerinde çoğunlukla verilerin ilişkin olduğu kişilerin kim olduklarının bilinmesi gerekli değildir. Özellikle bu gibi durumlarda imkan oranında verilerin anonim olarak ya da takma adlaştırma veya şifreleme gibi yöntemlerle işlenmesi, hem veri öznesinin kişisel verilerinin korunması hakkının daha az zarar görmesini veya hiç zarar görmemesini hem de kişilerin ifade özgürlüğünü daha serbest şekilde kullanabilmesini sağlayacaktır.¹¹⁹ Veri öznesinin kimliğine erişimi dolaylı kılan tedbirler olarak; anonimleştirme veya takma adlaştırma yoluyla kişisel verilerin toplanması, tutulması veya benzer şekilde işlenmesi en sık kullanılan yöntemlerdendir. Verilerin anonimleştirilerek veya takma adlaştırılarak işlenmesi, verilerin koruması amacının sağlanmasına ve “işleminin asgariliği” gibi temel veri koruma ilkelerinin önemli ölçüde gerçekleştirilmesine imkan sağlamaktadır. Bütün bu

Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi (ETS 108) İle İlgili Beyanlar. <http://www2.tbmm.gov.tr/d24/1/1-0966.pdf> (30.01.2018)

¹¹⁸ AB Direktifi, m.2/b.; Avrupa Adalet Divanı'nın Bodil Lindqvist kararındaki değerlendirmesine göre de; kişilerin isim ve telefon numarası gibi verilerinin salt internet ortamına yüklenmesi otomatik yöntemlerle veri işleme olarak kabul edilebilmekteyken, bu verilerin internet sitesi üzerinden diğer kişilerin erişimine açık bulundurulmasının da veri transferi olarak değil verilerin işlenmesi kapsamında düşünülmesi gerekir. Divan'a göre kişisel verilerin internet vasıtasıyla üçüncü ülkede belli bir şahsa veya kuruma münhasır olarak gönderilmediği müddetçe kişisel veri transferi olarak değerlendirilmesi söz konusu olamayacaktır. Bunun dışında sadece internet ortamına verilerin yüklenmesi veri işleme olarak kabul edilmelidir. ATAD, Lindqvist Davası (C-101/01),T: 06.11.2003, <http://curia.europa.eu>

¹¹⁹ KÜZECİ, *Kişisel Verilerin Korunması*, s. 101.

gerekçeler ve önemi itibarıyla çalışmada da bu veri işleme yöntemleri kısaca ele alınmaya çalışmıştır.

a. Verilerin Anonim Olarak İşlenmesi

Verilerin ilişkin olduğu kişinin maskelenmesi,¹²⁰ isimsizleştirme anlamına gelen anonimleştirilmeye, kişisel verilerin işlenmesinde daha ziyade sonuçları itibarıyla yer verilmiş olduğunu görmekteyiz. Verilerin anonimleştirilerek işlenmesi¹²¹; “başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi”¹²² neticesinin yaratılmasını ifade etmektedir.¹²³ Anonimleştirme; kişisel verilerin kişinin kim olduğunun diğer bir deyişle teşhisinin geri dönülemez bir şekilde engellenmesi sağlanacak şekilde işlenmesinden meydana gelmektedir.¹²⁴

Vakıa çalışmaları, istatistiki veriler ve yayınlanan araştırmalar, verilerin tam anlamda anonim hale getirilebilmesinin ne derece güç olduğunu göstermektedir. Ancak bu güçlüğüne rağmen anonimleştirme verilerin işlenmesiyle amaçlanan yararın korunması ve tehlikenin azaltılması için iyi bir strateji olabilmektedir.¹²⁵ Bir verinin tam olarak anonimleştirilmesi ve kişilerin teşhis edilme imkanının ortadan kalkması halinde, bu veri hakkında hem ulusal hem de uluslararası veri koruma hukuku artık

¹²⁰ KÜZECİ, *Kişisel Verilerin Korunması*, s. 224.

¹²¹ Türkçe karşılığı anonimleştirme olarak kabul edilen, “anonymization” ; Kimliğin gizlenmesi, saklanması veya anonim hale getirilmesi eylem veya süreci olarak tanımlanmaktadır. Merriam Webster Sözlüğü, <https://www.merriam-webster.com/dictionary/data> (24.02.2018).

¹²² KVKK md. 3/b.; Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik md. 10/2, “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.” Bu Yönetmelik 30224 Sayı ve 28.10.2017 Tarihli Resmi Gazete’de yayımlanmış ve 01.01.2018 tarihinden itibaren yürürlük kazanmıştır.

¹²³ Alman Veri Koruma Kanunu’nda da anonimleştirme; “kişisel verilerin belirli ya da belirlenebilir gerçek kişiyle, kişisel yanda olgusal bağımsız bilginin bağlanamamasını veya bunun ancak fahiş oranda zaman, maliyet ve emek kaybı ile bağlanabilmesini sağlayacak şekilde değiştirilmesi” şeklinde tanımlanmıştır. KÜZECİ, *Kişisel Verilerin Korunması*, s. 223.

¹²⁴ Veri Çalışma Grubu’nun 5/2004 Sayılı Anonimleştirme Teknikleri Hakkındaki Görüşü (Opinion 05/2014 On Anonymisation Techniques, Article 29 Data Protection Working Party)

¹²⁵ Anonimleştirilmiş veri, kişinin rızasına dayanarak işlenmekte olan veriden daha güvenli bir işleme prosedürü sağlamaktadır. GÖZÜKÜÇÜK, Merve, *Veri İşleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirilmesi*, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2014, s. 115.

uygulanmayacaktır.¹²⁶

Bu doğrultuda Direktif, verinin, her ne surette gerçekleştirmiş olursa olsun, tüm olası ve makul yöntemlerle veri öznesinin teşhis edilmesine izin vermeme neticesini oluşturması halinde anonimleştirilmiş olduğunu kabul etmiş ve bu verileri Direktif'in veri koruma prensiplerinin uygulama alanı dışında tutmuştur.¹²⁷ Aynı şekilde, Genel Veri Koruma Regülasyonu'nda da veri öznesi kişinin kim olduğunun belli ya da belirlenebilir olmadığı anonimleştirilmiş kişisel veri ve kimliği belirli ya da belirlenebilir gerçek bir kişi ile ilişkili olmayan anonimleştirilmiş bilgi hakkında, Regülasyon'un veri koruma prensiplerinin uygulanamayacağı düzenleme altına alınmıştır.¹²⁸

b. Verilerin Takma Adlaştırılması

Takma adlaştırma¹²⁹; kayıt edilmiş bir sembolün (genellikle benzersiz olan, isim, kimlik numarası vb.) bir başkasıyla yerini değiştirmesinden ibarettir.¹³⁰ Alman Veri Koruma Kanunu'da takma adlaştırmayı “bir kişinin adının veya diğer bilinebilir özelliklerinin, veri öznesinin kimliğinin saptanmasını engellemek veya kimliğin saptanmasını oldukça güç duruma getirmek amacıyla bir etiket ile değiştirilmesidir.” şeklinde tanımlamıştır.¹³¹ Verilerin takma adlaştırılarak işlenmesi halinde kişilerin dolaylı olarak da olsa kimliklerinin teşhis edilebilmesi söz konusu olabilmektedir. Dolayısıyla bu yöntem tek başına kullanıldığında verilerin anonimleştirilmesi neticesi yaratamamaktadır. Takma adlaştırma yalnızca veri öznesinin orijinal kimliğiyle veri grubu arasındaki bağlantıyı zayıflatmaktadır. Buna dayalı olarak diyebiliriz ki;

¹²⁶ 6698 Sayılı Kişisel Verilerin Korunması Kanunu'na göre de; “verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi” uygulama alanı dışında sayılan istisnai hallerdendir. KVKK md. 28/1 b.

¹²⁷ Veri Çalışma Grubu'nun 5/2004 Sayılı Anonimleştirme Teknikleri Hakkındaki Görüşü (Opinion 05/2014 On Anonymisation Techniques, Article 29 Data Protection Working Party).

¹²⁸ Regülasyon Gerekçe md. 26.

¹²⁹ “Pseudonymisation” uluslararası metinlerde verilerin takma bir adla işlenmesine karşılık olarak kullanılmaktadır. Bkz. Regülasyon Gerekçe md. 26.

¹³⁰ Veri Çalışma Grubu'nun 5/2004 Sayılı Anonimleştirme Teknikleri Hakkındaki Görüşü (Opinion 05/2014 On Anonymisation Techniques, Article 29 Data Protection Working Party).

¹³¹ Alman Veri Koruma Kanunu md. 3/6 a.; KÜZECİ, *Kişisel Verilerin Korunması*, s. 223.

verilerin takma adlaştırılması kullanışlı bir güvenlik tedbiridir ancak tam olarak bir anonimleştirme yöntemi değildir.¹³²

Veri sorumlularının sıklıkla sandığı gibi bir veya daha fazla sembolün başkasıyla değiştirilmesi veya kaldırılması veriyi anonim hale getirmeyecektir. Bu konuda pek çok örnekte; takma adlaştırılmış bir veriden kişinin kimliğinin teşhisinin, orijinal veriden teşhisi kadar kolay olabilmesine rastlanabilmektedir. Verilerin anonimleştirilmiş olarak düşünülmesi için; orijinal verinin silinmesi, sembolleri genellemek veya kaldırmak gibi ekstra önlemler alınması gerekir.¹³³

II. KİŞİSEL VERİ KORUMASININ TEMEL İLKELERİ

Kişisel verilerin korunmasının temel ilkeleri; veri öznesi kişinin, verilerinin işlenmesi sırasında veya sonrasında ileri sürebileceği belli haklar ve veri sorumlularının işleme prosedüründe verilerin korunmasını güvence altına alacak belli yükümlülüklerle donatılmış olması ekseninde oluşturulmuş ilkelere dir. Amaçlanan; bu ilkelere riayet edilerek verilerin işlenmesi suretiyle, veri korumasının sağlanması ve ihlallerin önüne geçilmesidir. Bu doğrultuda hem uluslararası hem de ulusal veri koruma düzenlemelerinin veri korunmasına ilişkin farklı yaklaşımları olabilmesine rağmen, veri koruma ve işleme prosedürüne dair bazı ortak temel ilkelere yer vermiş olduklarını görmekteyiz.¹³⁴ 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Regülasyon'unun genel hükümlerden sonra ikinci sırada tam bir bölüm ayırdığı alan, veri korumasının temel ilkelerine ilişkindir. Regülasyon'un yürürlüğe girmesiyle hükümsüz kalacak olan 95/46 Sayılı Veri Koruma Direktifi'nde de aynı şekilde, veri koruma ilkelerine tam bir bölüm ayrılarak oldukça geniş bir şekilde ele alınmıştır. 2016 yılı itibarıyla yasalaşan ve yürürlük kazanan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda da sayılan uluslararası düzenlemelerle eşdeğer kapsamda olmasa da kişisel verilerin işlenmesinin temel ilkelerine yer vermiştir.

Yapılan çalışmanın bu kısmında, veri koruma hukukunun temel ilkelerinin anlam ve kapsamına ilişkin olarak uluslararası ve ulusal veri koruma düzenlemelerine

¹³² Anonimleştirme kavramının iki görünüm şekli bulunmaktadır; bunlardan ilki hiçbir şekilde kişinin kimliğine ulaştırma ihtimali olmayan tam anonimleştirme iken diğer anonimleştirme şekli olarak takma adlaştırmayı gösterebiliriz. Bkz. KÜZECİ, *Kişisel Verilerin Korunması*, s. 101.

¹³³ Veri Çalışma Grubu'nun 5/2004 Sayılı Anonimleştirme Teknikleri Hakkındaki Görüşü (Opinion 05/2014 On Anonymisation Techniques, Article 29 Data Protection Working Party).

¹³⁴ KÜZECİ, *Kişisel Verilerin Korunması*, s. 211.

bütün olarak bakılmaya ve bu ekseninde ilkeler açıklanmaya çalışılmıştır. Bunun yanı sıra güncelliği itibarıyla daha ziyade 2016/679 Sayılı Genel Veri Koruma Regülasyon'u ekseninde ve yeri geldiğinde Regülasyon ile 95/46 Sayılı Direktif hükümleri karşılaştırılarak konunun ele alınması tercih edilmiştir. Bu ana başlık altında verilerin korunmasına ilişkin temel ilkeler; veri korumasının esasına ilişkin, veri öznesinin haklarına ilişkin ve işleme prosedürüne ilişkin ilkeler şeklinde sınıflandırılarak incelenmiş ve bu şekilde konunun daha iyi anlaşılmasının sağlanması amaçlanmıştır.

A. Veri Korumanın Esasına Dair İlkeler

1. Veri Güvenliği ve Mahremiyeti

Kişisel verilerin mahremiyetinin korunması ve veri güvenliğinin sağlanması amaçları doğrultusunda veri işlemenin; uygun teknik veya organizasyonel önlemler alınarak, tahrip, yok olma, değiştirme, yetkisiz erişim, ifşa, verilerin kazara kaybı veya yetkisiz veya yasadışı işlenmesi gibi tehlikeleri azaltarak veri güvenliğini sağlayacak yol ve yöntemlerle gerçekleştirilmesi gerekmektedir.¹³⁵ Kısacası veri güvenliği ve mahremiyeti ilkesinin; kişisel verilerin makul güvenlik tedbirleri alınarak kayıp, yetkisiz erişim, tahrip, kullanım, değiştirme ve verilerin ifşası gibi risklere karşı korunmasını güvence altına almakta olduğu söylenebilir.¹³⁶ Bu tedbirlerin sınırını; korunmak istenen kişisel verinin özelliği, verinin işlenmesinin yaratacağı riskler ve modern teknoloji ve maliyet ilişkisinin hesaba katılarak uygun bir koruma seviyesinin sağlanması oluşturmaktadır.¹³⁷ Bu ilke, aynı zamanda veri sorumlusuna bağlı çalışan veya doğrudan veri işleyen kişilerin belli bir kanuni yükümlülüğü veya veri sorumlusunun talimatı olmadan verileri işleyememesini de gerektirmektedir.¹³⁸

¹³⁵ Veri Çalışma Grubu'nun WP 254 Sayılı Yeterlilik Referansı (WP254 Adequacy Referential, Article 29 Data Protection Working Party); Direktif md. 17.

¹³⁶ Kişisel Verilerin Sınır Ötesi Transferi ve Mahremiyetinin Korunması Kılavuzu 2013 (OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data, Revised 2013) http://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf (11.01.2018).; Avrupa Konseyi 108 sayılı sözleşmesi md. 7.; ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 24.

¹³⁷ Regülasyon md. 32/2.; Direktif md.17/1.

¹³⁸ Direktif md.17; Regülasyon md. 5/f.

Genel itibarıyla işleme sürecine konu edinilen verilerin, süreç boyunca maddi veya fiziki anlamda güvende olmasını temin etmeyi amaç edinen veri güvenliği ilkesi ve kişisel verilerin korunması yaygın kullanımın aksine aynı şeyi ifade etmemektedir. Kişisel verilerin korunması, veri öznesinin temel bir kişilik hakkıdır ve koruma alanını bu hakkın hukuksal sınırlarına bağlı kılınmıştır. Veri güvenliği ilkesi ise maddi ve şekli anlamda verilerin güvenliğini konu edinir. Dolayısıyla veri güvenliği ve kişisel verilerin korunması özellikle konuları ve kapsamaları itibarıyla farklılık arz etmektedirler.¹³⁹ Veri güvenliği ilkesi; kişisel verilerinin içinde yer aldığı taşıyıcı, sistem veya dokümanın korunmasını ve maddi anlamda veri güvenliğinin teminine ilişkin tedbirlerin sağlanması gereğini ifade etmektedir.¹⁴⁰ Bu ilkenin amaçladığı şekilde verilerin maddi anlamda güven içerisinde olmasının temini, esasında dolaylı olarak ve nihai anlamda veri öznesinin kişisel verilerinin korunmasına ilişkin temel hak ve özgürlüklerinin korunmasına veya diğer bir deyişle hukuksal sınırlarıyla kişisel verilerinin korunmasına¹⁴¹ da hizmet etmektedir.¹⁴² Kısacası veri güvenliğinin sağlanması da kişisel verilerin korunmasının bir gerçekleştiriliş biçimidir.

Veri güvenliğinin ve mahremiyetinin korunması ilkesi hem veri öznesini hem de veri sorumlusunu doğrudan belli yükümlülükler altında bırakan temel bir ilkedir.¹⁴³ Veri sorumlusunun veri işleme prosedürüne ilişkin veri güvenliğini temin etme yükümlülüğü karşısında ve öznesinin de verilerinin güvenli olarak işlenip işlenmediğini kontrol yükümlülüğü bulunmaktadır. Ulusal veri koruma mevzuatımız da veri güvenliğini sağlamaya ilişkin veri sorumlusunun yükümlülüklerini ayrı bir madde altında ele almış ve veri güvenliğini sağlamaya yönelik uygun teknik ve idari tedbirlerin alınmasının yanında veri sorumlusuna denetim ve bildirim yükümlülüğü gibi kapsamlı sorumluluklar da getirmiştir.¹⁴⁴

2. Hassas Verilerin İşlenmesi ve Özellikli Olarak Korunması

Sıradan kişisel verilere kıyasla daha fazla ve özel olarak korunma gereğiyle oluşturulmuş hassas veya özel nitelikli kişisel verilerin, kural olarak işlenmesi

¹³⁹ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 119.; ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 95.; KÜZECİ, *Kişisel Verilerin Korunması*, s. 15.

¹⁴⁰ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 1.

¹⁴¹ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 95.

¹⁴² KÜZECİ, *Kişisel Verilerin Korunması*, s. 262.

¹⁴³ Direktif md 16-17, Regülasyon md. 32.

¹⁴⁴ KVKK md.12/4.

yasaktır.¹⁴⁵ Zira hassas veri kategorisine dahil ettiğimiz sınırlandırılmış içerik gruplarının temel ortak noktasını; bu verilerin işlenmesinin kişilerin toplumda ayrımcılığa maruz kalması gibi uzun süreli ve geri çevrilemez neticeler yaratmaya elverişli olması oluşturmaktadır.¹⁴⁶ Dolayısıyla bu veri grubuna dahil olan ve işlenmesi ile benzer nitelikte bir ihlal yaratma potansiyeli taşıyan verilerin, bir işleme faaliyetine konu edinilmesi gerektiğinde daha temkinli yaklaşılmalıdır.

Bu doğrultuda özel nitelikli kişisel verilerin, hukuka uygun olarak işlenebileceği istisnai haller diğer kişisel verilerin işlenme koşullarından ayrı olarak düzenlenmiş ve bu surette bu veri grubuna özellikli bir koruma sağlanmaya çalışılmıştır. Veri öznesinin açık rızası doğrultusunda; iş hukukundan kaynaklanan ve bu hukuk kuralları çerçevesinde; rıza gösteremeyecek durumda olan kişinin hayati çıkarlarının korunması amacıyla; kamuya yararlı kurum ve kuruluşların kendi üyeleri veya amacıyla bağlantılı ilişki içerisinde olduğu kişiler hakkındaki; kişinin kendi iradesiyle kamuya mal etmiş olduğu konuya ilişkin olarak; savunma hakkının kullanılması gibi suçluların yargılanması prosedürünün gerekliliğiyle; kanundan doğan üstün kamu yararın sağlanması amacıyla; gerekliliğine uzmanlarınca karar verilmiş olan tıbbi tedavi kapsamında; halk sağlığıyla bağlantılı kamusal yarar için gerekli olması halinde; istatistiksel, bilimsel, tarihi veya araştırma amaçlarının ve kamu yararı için arşivleme amacının gereğiyle yapılan veri işlemleri, hassas verilerin işlenmesi yasağına ilişkin temel istisnai hallerdir. Ancak bu istisnaların ülke düzenlemeleriyle yeterli koruma sağlanmış olması ve hukuki dayanağının bulunması koşuluyla kapsamı genişletilebilmektedir.¹⁴⁷ Regülasyon'un hassas verilerin işlenme yasağı ve istisnalarına yer verdiği 9. maddesinden yola çıkarak sayılmış olan bu istisnai durumların yanı sıra üye devletlerin, genetik, biometrik ve sağlık verilerinin işlenmesine ilişkin daha sınırlandırıcı koşullar getirme ve sürdürme imkanları da mevcuttur.¹⁴⁸

¹⁴⁵ KÜZECİ, *Kişisel Verilerin Korunması*, s. 249.

¹⁴⁶ Veri Çalışma Grubu'nun Özel Veri Kategorisine İlişkin Tavsiye Belgesi (Advice Paper on Special Categories of Data "Sensitive Data", Article 29 Data Protection Working Party).

¹⁴⁷ Regülasyon md. 9; Gerekçe md. 52, 53, 54.

¹⁴⁸ Direktif de aynı istikamette üye devletlere bu istisnai hallerin kapsamını genişletebilme inisiyatifi bırakmıştır. md. 8/2.; Bunun yanı sıra hassas veri grubuna dahil tutulan bu verilerin işlenmesi prosedürünü takip etmek üzere, veri sorumlularının bir zorunlu veri koruma görevlisi (data protection officer) ile birlikte çalışmaları Regülasyon tarafından zorunlu tutulmuştur. Veri koruma görevlisine ilişkin detaylı açıklama için bkz. Veri Çalışma Grubunun Veri Koruma Görevlileri Hakkındaki Klavuzu (Guidelines on Data Protection Officers ('DPOs'), Article 29 Data Protection Working Party).

Ulusal veri koruma mevzuatımızda, özel nitelikli verilerin işlenmesinin yasak olduğuna ilişkin hükmün tek istisnası olarak, verilerin ilgili kişilerin rızasına dayalı olarak işlenmesi kabul edilmiştir. Ancak kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinin kanunda öngörülmüş olan belli hallerde ilgilinin rızası bulunmaksızın da işlenebileceği hüküm altına alınmıştır. Bunların dışında hassas veri kategorisi içerisinde sayılmış olan sağlık ve cinsel hayata ilişkin kişisel veriler ise sadece kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amaçlarından birine dayanılarak ve sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından, veri öznesinin rızası olmaksızın işlenebilecektir. Bu düzenlemeden yola çıkarak kişilerin sağlık ve cinsel hayatına ilişkin verilerinin kişinin rızası dışında işlenebildiği hallerin münhasır olarak sayılması suretiyle daha sıkı koşullara bağlı kılındığını söyleyebiliriz. Ancak hassas verilerin işlenmesi yasağına istisna olarak düzenlenen tüm bu hallerin kapsamının oldukça geniş tutulmuş olması ve kavram olarak belirsizliği haklı olarak eleştirilmektedir.¹⁴⁹ Bu şekilde istisnaların geniş tutulduğu hallerde, özellikle uygulama bakımından kuralların istisna haline gelmesi kaçınılmaz olacaktır.

B. Verinin İşlenme Usulüne Dair İlkeler

1. Hukuka ve Dürüstlük Kurallarına Uygunluk

Hukuk ve dürüstlük kurallarına uygunluk ilkesi, kişisel verilerin işlenmesine ilişkin temel bir ilke olup pek çok veri koruma ilkesine de kaynaklık etmektedir. “Hukuka uygun ve adil”¹⁵⁰ yada “hukuka ve objektif iyiniyet kurallarına uygun”¹⁵¹ işleme şeklinde ifade edilebilen bu ilke; veri sorumlusuna, kişisel verilerin işlenmesine ilişkin yetki kazandıran genel bir ilkedir.¹⁵² Hukuk kavramı ile kast olunan her türlü

¹⁴⁹ KARLIDAĞ, Serpil, “Ekonomi Politik Açıdan Kişisel Verilerin Korunması”, Amme İdaresi Dergisi, C. 46, S.1, 2013, s. 145., 147.

¹⁵⁰ Orijinal metinlerde bu ilke “lawful and fair” şeklinde ifade edilmiştir. Bkz. Direktif Gerekçe md. 28.

¹⁵¹ BAŞALP, *Kişisel Verilerin Korunması ve Saklanması*, s. 37.

¹⁵² ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 46.

pozitif hukuk kuralı ve ulusal veya uluslararası düzenlemelerin tamamıdır.¹⁵³ İyiniyet ise genel anlamda bir kimsenin dürüst ve iyi ahlak sahibi olduğunu gösteren bir vasıfıdır.¹⁵⁴ Bu doğrultuda, iyiniyet kuralının da hukuk düzeninin ve bireyler arası güven temelli ilişkilerin devamını sağlamak üzere kullanılan temel bir vasıta olduğunu söyleyebiliriz. Veri koruma hukuku bakımından ise iyiniyet; veri öznesinin, kişisel verilerinin işleme konusu yapıldığı amaç ve veri işlemenin özel koşulları hakkında ve işlemenin amacının gerekleri nazara alınarak şeffaf bir veri işlemesi için gerektiği oranda bilgi sahibi edilmesini gerektirmektedir.¹⁵⁵

Kişisel verilerin hukuka ve dürüstlük kurallarına uygun işlenmesi hem ulusal veri koruma mevzuatımızda¹⁵⁶ hem de uluslararası düzenlemelerde verilerin işlenmesine ilişkin önemli bir sınırlandırma sebebi olarak düzenlenmiştir. Bu kapsamda verilerin ancak belli sebeplere bağlı olarak veya belli koşullar altında işlenmesi halinde hukuka uygun işlenmiş olabileceği kabul edilmiştir.¹⁵⁷ Diğer bir deyişle kişileri belirli veya belirlenebilir kılacak olan kişisel verilerin, ancak sayılı sebeplerden birine dayanılarak işlenmiş olması halinde hukuka uygun işlenmiş olduğu kabul edilebilecektir. Kişisel verilerin işlenmesinin hukuka uygun kılan bu halleri; veri öznesinin açık rızasına dayanarak kişisel verilerin işlenmesi, tarafı olunan bir sözleşmenin icrası veya ifası kapsamında verilerin işlenmesi, yasal zorunluklar sebebiyle kişisel verilerin işlenmesi, veri öznesinin veya başka bir gerçek kişinin yüksek menfaatleri gereği verilerin işlenmesi, kamu yararı veya resmi yetkinin kullanılması gereğiyle verilerin işlenmesi ve veri sorumlusu veya üçüncü kişilerin gözettiği meşru menfaatler gereği verilerin işlenmesi olarak sayabiliriz.

a. Açık Rızanın Kapsamında Verilerin İşlenmesi

Kişisel veriler hakkında kural olarak kişinin özel yaşamının bir parçası ve temel bir hakkı olan kişisel verilerinin mahremiyetinin korunması, unutulması, diğer insanlardan saklı tutulması veya sınırlı olarak dışarıya açıklığı gerekirken; kapsamı oldukça geniş olan kişisel verilerin işlenmesi eylemi ancak belli koşulların varlığı

¹⁵³ KÜZECİ, *Kişisel Verilerin Korunması*, s. 212.

¹⁵⁴ G. AKİPEK vd., *Türk Medeni Hukuku Başlangıç Hükümleri(Kişiler Hukuku)*, s. 148.

¹⁵⁵ Regülasyon Gerekece md. 60.

¹⁵⁶ KVKK md. 2/a.

¹⁵⁷ Regülasyon md. 6., Direktif md. 7.

halinde hukuka uygun olabilecektir.¹⁵⁸ Bu koşulların başında, ulusal ceza mevzuatımızdaki pek çok suç bakımından da hukuka uygunluk sebebi olarak kabul ettiğimiz, ilgilinin rızası gelmektedir. İlgilinin rızasıyla veri işlemenin hukuka uygun kabul edilmesi esasında veri işleme faaliyeti bakımından veri öznesinin, verilerinin geleceğini belirlemeye yönelik iradesinin bir değer kazanmasını ve veri işleme prosedüründe ilgilinin basit bir obje konumunda kalmaktan kurtulmasını sağlamaktadır.¹⁵⁹

Bu doğrultuda denilebilir ki; kişisel verilerin işlenmesi yasağının uygulanma alanını daraltan en kapsamlı unsur, ilgili kişinin işlemeye gösterdiği rızadır.¹⁶⁰ Veri öznesinin kişisel verilerin işlenmesine ilişkin verdiği rızanın muteber kabul edilebilmesi için pek çok nitelikle donatılmış olması gerekmektedir. Özellikle Regülasyon'un 4. maddesinin 11. fıkrasında yapılan tanımdan yola çıkarak; veri öznesinin kişisel verilerinin işlenmesine dair serbestçe verdiği, spesifik, bilgilendirilmiş/aydınlatılmış ve tereddütsüz/kesin kabul göstergesinin, geçerli bir rıza olarak kabul edilebileceğini söyleyebiliriz. Ulusal veri koruma mevzuatımız da açık rızayı; "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" şeklinde tanımlamıştır.¹⁶¹ Dolayısıyla rızanın geçerliliğinin temelini; kişinin serbest iradesi ile spesifik bir işleme faaliyetine veya veri öznesinin önceden bilgilendirilmiş olduğu, diğer bir söylemle aydınlatılmış olduğu, bir konuya ilişkin olarak verilmesi oluşturmaktadır.

Kişinin açık onayını gösteren rıza; sözlü, yazılı veya elektronik vasıtalarla¹⁶² oluşturulmuş olabilir. Rızanın açık veya örtülü olarak verilmesi arasında muteberlik bakımından bir fark bulunup bulunmadığı tartışmalıdır. Regülasyon'un gerekçe kısmında belirtildiği üzere; rıza beyanının belli bir şekilde verilmesi gerektiğine ilişkin bir sınırlandırma getirilmiş değildir. Ancak rızanın; kişinin serbest, belirli, aydınlatılmış ve tereddütsüz iradesini gösteren açık onay eylemi şeklinde

¹⁵⁸ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 107.

¹⁵⁹ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 108.

¹⁶⁰ BAŞALP, *Kişisel Verilerin Korunması ve Saklanması*, s.39.

¹⁶¹ KVKK md. 3/1 a.

¹⁶² Bu, bazen bir internet sitesini ziyaret ettiğimiz sırada bir kutuya tik atmak(opt-in), bilgi toplumu servislerine ilişkin teknik ayarların tercihi veya veri öznesinin kendisine önerilen verilerinin işlenmesine ilişkin kabulünü açıkça gösteren herhangi bir bağlantı veya ifade olabilir. Ancak rızanın elektronik vasıtalarla yöneltilen bir talebe bağlı olarak alındığı halde; bu talebin açık, kısa ve öz olması ve ilgili servisin kullanımını gereksiz yere aksatmaması gerekmektedir. Regülasyon Gerekçe md. 32.

verilebileceğini düzenlemiştir. Dolayısıyla kişinin, sessiz veya hareketsiz kalarak bir işleme ilişkin örtülü olarak gösterdiği onayının bu düzenlemeye göre itibar edilebilirliği bulunmamaktadır. Nitekim kişinin, kişisel verilerinin işlenmesine ilişkin herhangi bir talep karşısında veya elektronik yollarla yöneltilmiş rızasının mevcut olduğunu gösterir kutucuğun önceden işaretlenmiş olduğu bir ekran karşısında hareketsiz veya sessiz kalması geçerli bir rıza beyanı olarak kabul edilemez.¹⁶³ Ancak örtülü olarak verilmiş rıza ya da beyan davranışının da, koşullara göre değerlendirilerek kişinin serbest iradesini göstermeye elverişli bir tutum oluşturması, veri öznesinin mutlak kanaatini “şüpheye yer vermeyecek” şekilde yansıtabilmesi¹⁶⁴ ve nesnel bir değerlendirme neticesinde veri öznesinin onay gösterdiği çıkarımına götürebilmesi halinde geçerli bir rıza beyanı olarak kabul edilmesi gerektiği kanaati de doktrinde benimsenmektedir.¹⁶⁵

Eğer veri öznesinin samimiyeti veya özgür bir seçimi yoksa veya zararsız bir şekilde rızasını geri almıyor veya rıza vermekten kaçınıyorsa bu durumda rızanın serbest iradeye dayalı olarak verildiğinden bahsedemeyiz.¹⁶⁶ Diğer bir deyişle kişinin, verilerinin işlenmesine rıza gösterip göstermeme konusunda gerçek bir seçim hakkı mevcut olmalı¹⁶⁷ ve kişi rıza göstermemesine ilişkin bir gerekçe sunma mecburiyetinde bırakılmamalıdır.¹⁶⁸ Serbest iradeye dayalı bir rıza beyanının, bu surette bir tereddüt yaşanmaksızın verilmiş olması da rızanın muteberliğine dair asli

¹⁶³ Regülasyon da muteberlik tanınan “opt-in” rıza beyanın dışında, pazarlama amaçlı internet veya e-posta servisleri üzerinden veri öznesinin hareketsiz kalmasıyla “opt-out” rıza beyanıyla onayının elde edilmesi kabul edilmemiştir. Opt-out rıza beyanı; kişinin önceden işaretlenmiş bir kutucuğun mevcudiyeti karşısında eylemsiz kalmasını ve işareti kaldırmaya yönünde bir çaba göstermemesini bir onay göstergesi olarak kabul etmektedir. Dolayısıyla ilgilinin kişisel verileri üzerinde irade sergileyebilme vb. hakları daha zayıf bir koruma ile korunmuş olmaktadır. Bkz. KÜZECİ, *Kişisel Verilerin Korunması*, s. 244.; Regülasyon Gerekme md. 32.

¹⁶⁴ Ancak ilgilinin kendisine yöneltilen veri işleme amaçlı bir talep karşısında sessiz kalması, iradesini yansıtan başka bir unsur bulunmadığı sürece kesin bir kabul olarak kabul edilemez. BAŞALP, *Kişisel Verilerin Korunması ve Saklanması*, s. 40.

¹⁶⁵ KÜZECİ, *Kişisel Verilerin Korunması*, s. 239.; KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 45.

¹⁶⁶ Regülasyon Gerekçe md.42.

¹⁶⁷ Kişinin rıza göstermemiş olması halinde veri öznesi bir yaptırımla karşı karşıya kalacaksa, örneğin; sözleşmenin kurulmasının koşulu olarak rıza aranıyorsa da gerçek anlamda bir seçim hakkının veya irade serbestisinin bulunduğunu söyleyemeyiz. KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 132.

¹⁶⁸ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 107.; Özellikle hasta-hekim, işçi-işveren arasında olduğu gibi kişiler arasında dikey ilişki bulunan hallerde, işverenin kendisini işe almama veya işini kaybetme tehlikesi altında verilerinin işlenmesine ilişkin rıza gösteren bir işçinin vermiş olduğu rızanın tam anlamıyla özgür iradeye dayalı olarak verilmiş olduğu kabul edilemeyecektir. Bu gibi hallerde bağımlı konumda olan kişileri koruyucu bazı ek teminatlar oluşturulmalıdır. KÜZECİ, *Kişisel Verilerin Korunması*, s. 240.

bir özelliktir. Bunun dışında, veri öznesinin aydınlatılmış veya işlemeye dair bilinç sahibi¹⁶⁹ olarak rıza göstermiş olduğunun, ne surette sağlanmış olacağının da üzerinde durmak gerekmektedir. Kişinin, verilerinin işlenmesine yönelik kendisine yöneltilen talebin hangi amaçla ve kimin tarafından yapıldığını, işlemenin içeriğini, süresini ve verilerinin ne surette kullanılacağını¹⁷⁰ bilerek rıza göstermiş olması, rızanın belli bir bilinçle verilmiş olduğunu göstermektedir. Bunun dışında rızanın yazılı bir beyanla ve birden fazla işleme ilişkin olarak verilmesi söz konusu ise veri öznesi bu durumun ve rızanın kapsamının tam olarak farkında olmalıdır.¹⁷¹ Regülasyon'a göre de yazılı beyanın rıza dışında başka hususları da içeriyor olması durumunda; veri öznesinin kendisine yöneltilen rıza talebinin, diğer hususlardan açıkça ayırt edilebilir şekilde açık ve yalın bir dille yazılmış ve anlaşılabilir olması gerekir.¹⁷² Bütün bu koşulların rıza beyanının belli bir bilinç sahibi olarak verilmesini sağlamaya yönelik tedbirler olduğu şüphesizdir. Dahası veri öznesinin, verilerinin işlenmesine dair rıza göstermek veya göstermemek şeklinde sergilediği iradesi, verilerinin geleceğini belirleyebilme hakkının da münhasır bir kullanım şeklini oluşturmaktadır.

Günümüzde sosyal medya başta olmak üzere pek çok internet servisi ile kişisel verilerini bilinçsizce paylaşan çocukların, kişisel verileri üzerindeki tasarruf hakkı da yakın zamana kadar önemli tartışmalara konu oluşturmıştır. Bu konunun uluslararası boyutta ilk kez ele alınması Veri Koruma Regülasyon'u düzenlenmesinde gerçekleşmiştir. Düzenlemeye göre; çocukların doğrudan rıza talebine muhatap kılındığı hallerde, rıza ehliyeti ancak en az 16 yaşında olan çocuklara tanınmıştır. 16 yaşından küçük çocukların vermiş olduğu rızanın, veri öznesi çocuğa ait verilerin işlenmesini hukuka uygun kılması mümkün değildir. Ancak çocuk üzerinde velayet sahibi kişilerin izin vermesi veya rıza göstermesi koşuluyla, 16 yaş altındaki çocuğa ilişkin verilerin işlenmesi de hukuka uygun hale gelebilecektir.¹⁷³ Bu konuda ulusal veri koruma kanumuzda herhangi bir hüküm bulunmamaktadır. Dolayısıyla çocukların, kişisel verilerinin işlenmesine ilişkin göstermiş oldukları rızanın muteberliğinin, ulusal veri koruma hukukumuzda boşluk yaratan ve düzenlenmeye muhtaç bir husus olduğunu söyleyebiliriz.

¹⁶⁹ BAŞALP, Kişisel Verilerin Korunması ve Saklanması, s.39.

¹⁷⁰ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 133.

¹⁷¹ Regülasyon Gerekçe md. 42.

¹⁷² Regülasyon md. 7/2.

¹⁷³ Regülasyon md. 7/4.

b. Tarafı Olunan Bir Sözleşmenin İcrası veya İfası Kapsamında Verilerin İşlenmesi

Veri öznesinin kurmuş olduğu bir sözleşme hükümleri gereğince veya sözleşme öncesi tedbirlerin¹⁷⁴ icrası doğrultusunda kişisel verilerinin işlenmesi, veri öznesinin rızası aranmaksızın hukuka uygun kabul edilmektedir.¹⁷⁵ Ulusal veri koruma mevzuatımıza göre de; “bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması” işlemeyi hukuka uygun kılmaktadır.¹⁷⁶ Bu doğrultuda örneğin; bir kişi ve banka arasında yapılan kredi sözleşmesinin kurulması aşamasında, bankanın kişi adına kayıtlı menkul veya gayrimenkullerin mevcut olup olmadığını gösteren veya kişinin icra borcu bulunup bulunmadığını gösteren belli verileri kayıt altına alması durumunda, gerçekleştirilen veri işlemenin hukuka uygun olduğunu söylememiz gerekecektir.¹⁷⁷

c. Yasal Zorunluluklara Mutabık Kişisel Verilerin İşlenmesi

Veri sorumlusunun, bağlı olduğu ulusal veya uluslararası mevzuattan doğan hukuki yükümlülüklerini yerine getirebilmesi için zorunlu olarak gerçekleştirdiği veri işleme faaliyetleri de veri öznesinin rızası aranmaksızın hukuka uygun olacaktır.¹⁷⁸ Veri sorumlularının hukuki yükümlülük olarak böyle bir veri işleme mecburiyeti altında bırakılmasına, sosyal güvenlik ve iş hukuku veya vergi hukuku çerçevesindeki düzenlemeler örnek gösterilebilir.¹⁷⁹

¹⁷⁴ Sözleşme öncesi tedbir kavramına ilişkin değerlendirme için bkz. BAŞALP, Kişisel Verilerin Korunması ve Saklanması, s. 41.

¹⁷⁵ Regülasyon md. 6/b.; Direktif md. 7/b.

¹⁷⁶ KVKK md. 5/c.

¹⁷⁷ ERDEM, Tahir, “Kişisel Verilerin Korunması Konusunda Son Gelişmeler”, Vergi Sorunları Dergisi, S. 332, 2016, s. 104., (çevrimiçi) www.vergisorunlari.com.tr (14.03.2018).

¹⁷⁸ Regülasyon md. 6/c.; Direktif md. 7/c.; KVKK md. 5/ç.

¹⁷⁹ İş Kanunu’nun 75. maddesine göre de; işverenin, işçinin kimlik bilgilerini içeren özlük dosyasını tutması zorunluluk olarak düzenlenmiştir. Bu yükümlülüğe aykırı olarak işçinin özlük dosyalarını düzenlemeyen işverenin ayrıca bir yaptırıla karşı karşıya kalacağı da düzenlenmiştir. (İş K. Md. 104/1.); Vergi Usul Kanunu md. 5. “Aşağıda yazılı kimseler görevleri dolayısıyla, mükellefin ve mükellefle ilgili kimselerin şahıslarına, muamele ve hesap durumlarına, işlerine, işletmelerine, servetlerine veya mesleklerine mütaallik olmak üzere öğrendikleri sırları veya gizli kalması lazımgelen diğer hususları...” şeklinde devam eden maddeyle mükellefe ilişkin kişisel veri niteliğindeki bilgilerin belli kişiler dışında işlenmesinin ihlal oluşturacağı hüküm altına alınmıştır. K. DURMUŞ, Neslihan, “Ticari Sırların ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti”, Türkiye Adalet Akademisi Dergisi, S.31, 2017, s. 371.

d. Veri Öznesinin veya Başka Bir Gerçek Kişinin Yüksek Menfaatleri Gereği Verilerin İşlenmesi

Verileri işlenecek olan kişinin veya bir başka kişinin hayati çıkarlarının korunmasına ilişkin bir gereklilik olarak kişisel verilerin işlenmesi halinde, işlemenin hukuka uygun olduğu kabul edilmektedir. Ulusal mevzuatımızda veri işlemesini hukuka uygun kılacak hayati çıkarlar özelleştirilerek; hayat ve beden bütünlüğünün korunmasının zorunluluğu ve kişinin rıza gösterme ehliyeti veya yetisi bulunmaması koşullarının birlikte gerçekleşmesi aranmaktadır.¹⁸⁰

e. Kamu Yararı veya Resmi Yetkinin Kullanılması Gereğiyle Verilerin İşlenmesi

Kişisel veriler, kamusal bir makam veya kamu yararı için çalışan özel bir organizasyonun görevini yerine getirmesi için gerekli olduğunda işleme konusu olabilmektedirler. Bu doğrultuda işlemenin; veri sorumlusuna verilmiş resmi bir yetkinin kullanılması veya kamu yararı gereği gerçekleştirilmiş olması halinde veri öznesinin rızası aranmaksızın kişisel verilerin işlenmesinin hukuka uygun olduğu kabul edilecektir.¹⁸¹

f. Veri Sorumlusu veya Üçüncü Kişilerin Gözettiği Meşru Menfaatler Gereği Verilerin İşlenmesi

Kişisel verilerin; veri sorumlusunun meşru menfaatleri gereğince zorunlu olması ve ilgili veri öznesinin temel hak ve özgürlüklerine zarar vermemesi koşuluyla işlenmesi hukuka uygun bir veri işleme olarak kabul edilmektedir.¹⁸² 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nuna göre de kişisel verilerin böyle bir halde veri öznesinin rızası olmaksızın işlenmesi hukuka uygun kabul edilmektedir. Kanun'un 5. maddesinin gerekçesinde; “Buna göre, örneğin bir şirket sahibi, çalışanlarının temel hak ve özgürlüklerine zarar vermemek kaydıyla, onların terfileri, maaş zamları yahut sosyal haklarının düzenlenmesinde ya da işletmenin yeniden yapılandırılması

¹⁸⁰ KVKK md. 5/b.

¹⁸¹ Regülasyon md. 6/e.

¹⁸² KVKK md. 5/2 f.; Regülasyon veri sorumlusunun meşru menfaatleri gereği ile vb. bazı kişisel verilerin veri öznesinin rızası dışında işlenmesinin hukuka uygun kabul edilebildiği hallere ilişkin olarak veri öznesinin işlemeye itiraz edebilme hakkını düzenleyerek menfaat dengesinin sağlanmasını amaçlamıştır. Regülasyon md. 21.

sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işleyebilecektir. Burada, işletmenin yeniden yapılandırılması ya da ehliyetli ve liyakatli çalışanların terfi almaları, veri sorumlusu statüsündeki şirket sahibinin meşru menfaati cümlesindendir.”¹⁸³ şeklindeki açıklamayla veri sorumlusunun meşru menfaatinden ne anlaşılması gerektiğine açıklık getirilmeye çalışılmıştır.

2. Amaçla Bağlılık

Kişisel verilerin belli bir amaca bağlı olması, verilerin toplanmasından başlayarak veri işleme sürecinin her aşamasında aranması gereken temel bir veri güvenliği ilkesidir. ¹⁸⁴ Bu ilkenin gereğince veri işleminin yapıldığını söyleyebilmemiz için; veri sorumlusunun, verilerin işlenmesine ilişkin sürecin başlangıcı olarak kabul ettiğimiz toplama aşamasından itibaren, kişisel verilerin işlenmesini gerektiren hukuka uygun ve meşru amaçlarının ne olduğunu belirlemiş olması ve dahası verileri bu amaç doğrultusunda, amaçla sınırlı olarak ve amacın gerçekleşmesini sağlayamaya yetecek azami miktarda işlemesi gerekmektedir.

Kişisel verilerin işleme amacının; meşru, açık ve en geç verilerin toplanma aşamasında belirlenmiş olması gerekmektedir. Bu amacın gerçekleştirilmesi için; işlenen verinin, amacın gerçekleşmesinin sağlamaya elverişli, amaçla sınırlı ve alakalı olması gerekir. Amaçla bağlılık ilkesine göre; kişisel veriler ancak istenilen amaca ulaştıracak başka bir vasıta olmadığı takdirde işlenmeli ve bu surette işlenen veya depolanan veriler hem miktar hem de süre bakımından asgari hadde tutulmalı, minimize edilmeye çalışılmalıdır. Ayrıca kişisel verilerin gerekli olan amacı sağladıktan sonra daha fazla saklı tutulmasının önüne geçebilmek adına veri sorumlularının, saklı tuttukları verileri silme veya gözden geçirme periyotlarını, veri öznesinin de erişebileceği, şeffaflığı sağlamaya elverişli bir şekilde yayınlamış olması gerekmektedir. Bu surette aynı zamanda doğruluk değeri olmayan kişisel verilerin düzeltilmesi veya silinmesi için gerekli asgari çaba da gösterilmiş olacaktır.¹⁸⁵

Hukuka, kesin ve belirli bir amaca uygun şekilde toplanmış olan kişisel verilerin, bu amaçla uyumlu bir şekilde işlenmesi gereğine istisna olarak ulusal ve

¹⁸³ 6698 sayılı Kişisel Verilerin Korunması Kanunu Madde Gerekçesi.

¹⁸⁴ Direktif'in md.6/b.; BAŞALP, Kişisel Verilerin Korunması ve Saklanması, s. 37.

¹⁸⁵Regülasyon Gerekçe md. 39.

uluslararası düzenlemelerin ortak kabul ettiği bir hal; kişisel verilerin tarihi, istatistiksel veya bilimsel amaçlarla işlenmesi durumunun her halde amaçla bağlı olduğu varsayımdır.¹⁸⁶ Bu düzenlemenin temel amacının bilimsel ihtiyaçların karşılanmasına kolaylık sağlamak olduğu kabul edilse bile kişisel verileri bu gibi amaçlarla işlenen veri öznelerinin, kişisel verilerinin tam anlamıyla korumasız bırakılması düşünülemez. Bu durumun önüne geçmek adına hem Regülasyon hem Direktif, bu amaçlarla kişisel verilerin işlenmesine ilişkin alınması gereken tedbiri üye devletlerin sorumluluk alanlarına bırakmıştır.¹⁸⁷

3. Ölçülülük

Kişisel verilerin yasal, belirli ve kesin bir amaca uygun olarak toplanması ve bu amacın gereklerine göre işlenmesini ifade eden “amaçla bağlılık” ilkesinin doğal bir sonucu olarak ölçülülük ilkesi gündeme gelmektedir. Hukuken geçerli bir amaçla toplanmış olan verilerin, bu amacı gerçekleştirmek için ihtiyaç duyulandan fazla olmaması, elde tutulmaması,¹⁸⁸ depolanmaması gibi sınırlandırmalara mevzu kılınmasıyla amaçlanan orantılı ve ölçülü bir veri işlemenin gerçekleştirilmesidir. Dolayısıyla ulaşılmak istenilen amaç doğrultusunda toplanan verilerin, istenilen amaç için önemli ve gerekli olduğu oranda işlenmesi gerekmektedir. Verilerin işleme amacının ortadan kalkması, ulaşılmak istenen amaç için işleme konusu verilere ihtiyaç kalmaması veya amaca ulaşılmış olması dolayısıyla verilerin daha fazla tutulmasının gereksiz hale gelmesi hallerinde amaç ve veri arasındaki sebep sonuç ilişkisini ortadan kalkmış olacağından, verilerin toplanması veya işlenmesi amaç bakımından gereksiz ve dolayısıyla orantısız olacaktır.¹⁸⁹ Verilerin işlenmesiyle gerçekleşen kişisel verilerin korunması temel hakkına yönelik müdahale ve veri işleme amacı arasındaki orantılılık, işleme amacını sağlayabilmek için kişisel verilerin toplanması veya

¹⁸⁶ KVKK 28/c.; “Kişisel verilerin; millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi” kanunun uygulama alanı dışında tutulan istisnai haller arasında sayılmıştır.

¹⁸⁷ Regülasyon’un belli alanlarda ve belli hükümleri itibarıyla Direktif ile karşılaştırıldığı ayrıntılı tablo için bkz. <https://www.whitecase.com/publications/article/chapter-17-issues-subject-national-law-unlocking-eu-general-data-protection> (24.12.2017)

¹⁸⁸ Bu doğrultuda Avrupa İnsan Hakları Mahkemesi suç nedeniyle hükümlülere ilişkin parmak izi vb. kişisel verilerin toplanmasına izin veren düzenlemede; toplanan bu verilerin tutulma süresinin belirsizliği dolayısıyla düzenlemenin AİHS md. 8’e aykırılık teşkil ettiğine karar vermiştir. AİHM, S. ve Marper-Birleşik Krallık Davası, No: 30562/04 ve 30566/04, Tarih: 04.12.2008 <https://hudoc.echr.coe.int> (7.01.2018).

¹⁸⁹ KÜZECİ, *Kişisel Verilerin Korunması*, s. 227.

işlenmesine olan gereklilik ve işlemenin gerekliliği doğrultusunda kullanılan vasıtaların ulaşılmak istenen amaca yönelik uygunluğu, ölçülülük ilkesi kapsamında aranması gereken üç temel kriter olarak kabul edilmektedir.¹⁹⁰

Bir iş sözleşmesinin kurulmuş olmasının gerektirdiği işverene ait yükümlülüklerin yerine getirilmesi için, işçiye ilişkin toplanan verilerin işlenmesi hem toplanma amacıyla orantılı hem de bu amacın bir gereğidir.¹⁹¹ Ancak bu gerek üzerine daha önce toplanan verilerin, aradaki illiyet bağıını kaldıran bir durum oluşmasına rağmen, kurulu sözleşmenin hükümsüz hale gelmesi gibi, işveren tarafından işlenmeye devam edilmesi veya olası ileriki kullanımlara yönelik olarak depolanması yasaktır. Bu durum ölçülülük ilkesinin doğal bir sonucudur.¹⁹² Veri ekonomisi olarak da değerlendirebileceğimiz verilerin gerektiğinden fazla işlenmesinin önüne geçmeyi konu alan bu ilkenin amacı; kişilerin, verilerinin işlenmesinden doğan kişilik haklarının ihlal edilme riskinin en aza indirilmesidir.¹⁹³

4. Doğruluk ve Güncellik

Kişilerin, haklarında tutulan verilerin doğruluğunun ve güncelliğinin korunması, hem veri öznesi hem de kişisel verileri belli amaçlarla işleyen veri sorumluları bakımından önem taşıyan bir ilkedir.¹⁹⁴ Aynı zamanda bu ilkenin gereklerinin yerine getirilmesi, verilerin doğru ve güncel tutulmasının sağlanması, uluslararası düzenlemelerde üye devletler için bir yükümlülük olarak kabul edilmiştir.¹⁹⁵ Verilerin doğru ve güncel tutulması, aynı zamanda veri sorumluları için de önemli bir sorumluluk alanı yaratmaktadır.¹⁹⁶ Veri sorumluları, işlenme amacı göz önünde bulundurulduğunda doğruluk değeri veya güncelliği bulunmayan kişisel verilerin, gecikmeksizin düzeltilmesi veya silinmesini için her türlü makul önlemi almalıdır. OECD Rehber İlkeleri'nde bu ilke kapsamında; verilerin doğru ve güncel

¹⁹⁰ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 99.

¹⁹¹ İş K. md. 75.; BAŞALP, *Kişisel Verilerin Korunması ve Saklanması*, s. 38.

¹⁹² Regülasyon md. 5/c., e.; Direktif md. 6/c., e.

¹⁹³ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 118.

¹⁹⁴ KÜZECİ, *Kişisel Verilerin Korunması*, s. 225.

¹⁹⁵ BAŞALP, *Kişisel Verilerin Korunması ve Saklanması*, s. 38.

¹⁹⁶ Direktif md. 6/1 d.; 108 Sayılı Avrupa Konseyi Sözleşmesi md. 5/d.; Regülasyon 5/1 d.; KVKK 4/2 b.

tutulmasının yanında tam olarak yada eksiksiz tutulmasının sağlanması gerektiğine de değinilmiştir.¹⁹⁷

Daha önce şeffaflık ilkesinin bir gereği olarak üzerinde durduğumuz veri sorumlularınca kayıtlarını periyodik gözden geçirme ve silme tarihlerinin kişilerin erişimine açık bir şekilde yayınlanması uygulamasının, verilerin güncelliğini ve doğruluğunu sağlamak anlamında da olumlu sonuçları olacağı şüphesizdir.¹⁹⁸ Veri öznesinin bilgi edinme ve düzeltme haklarıyla da doğrudan bağlantılı olduğunu söyleyebileceğimiz verilerin doğru ve güncel tutulması ilkesi, veri işleyenler için de ağır yükümlülükler yaratmaktadır.¹⁹⁹ Buna göre, veri işleyenlerin de bu ilke kapsamında gerekli dikkat ve özeni göstererek verileri işlemesi beklenmektedir.

C. Veri Sahibi Kişinin Haklarına İlişkin İlkeler

Kişisel verilerin hukuka uygun şekilde işlenmesinin sağlaması amacıyla düzenleme altına alınmış kurallara yer veren ilkelerin yanı sıra, bu ilkelerin uygulanmasını sağlamaya veya kolaylaştırmaya yönelik olarak veri özneleri birtakım haklarla²⁰⁰, veri sorumluları da bazı yükümlülüklerle donatılmışlardır. Veri öznesinin işlenmekte olan kişisel verileri üzerindeki haklarını kullanabilmesi, veri sorumlusu ile şeffaf bir şekilde iletişim kurabilir olmasının sağlanması ile doğrudan bağlantılıdır. Bu gerekçelerle ulusal ve uluslararası düzenlemelerde; veri sorumlularının yükümlülüğü, veri öznelerinin de kişisel verilerinin korunmasına yönelik haklarını kullanmasını sağlayacak temel bir prensip olarak “şeffaflık” ilkesine yer verilmiştir. Şeffaflık ilkesi; kişisel verilerin işlenmesiyle ilişkili her türlü bilgi ve bildirimin; kolay ulaşılabilir ve anlaşılabilir, açık ve basit bir dil kullanılarak oluşturulmuş olmasını gerektirir.²⁰¹

Dolayısıyla denilebilir ki; şeffaflık ilkesinin özellikle veri öznesinin bilgi edinme hakkı ile doğrudan, veri öznesinin bu başlık altında yer verilen diğer haklarıyla da dolaylı olarak bağlantısı bulunmaktadır. Veri öznesine, kişisel verilerin doğrudan veya dolaylı korunmasını konu edinen ulusal ve uluslararası düzenlemelerde²⁰²

¹⁹⁷ OECD Rehber İlkeleri md. 8.; KÜZECİ, *Kişisel Verilerin Korunması*, s. 225.

¹⁹⁸ Regülasyon md. 5/a.; Gerekçe md. 39.

¹⁹⁹ Regülasyon md. 5/1 d.; KÜZECİ, *Kişisel Verilerin Korunması*, s. 226.

²⁰⁰ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 123.

²⁰¹ Regülasyon Gerekçe md. 39.

²⁰² Regülasyon md. 15., 22.; Sayılanlara ek olarak kişisel verilerin kanuna aykırı işlenmesi sebebiyle uğranılan zararın tazminini talep hakkı veri öznesinin hakları arasında düzenlenmiştir. Bkz. KVKK md. 11.

tanınmış temel haklar olarak; bilgi sahibi olduğu verilerine koşulsuz olarak erişim hakkı; hatalı, eksik veya güncel olmayan veri işlemlerinin düzeltilmesini talep edebilme hakkı; işleme konusu yapılmış verilerinin gecikmeksizin silinmesini/unutulmasını talep edebilme hakkı; veri işleminin sınırlandırılmasını talep edebilme hakkı; verilerinin taşınmasını talep edebilme hakkı; itiraz hakkı ve otomatik kararlarla maddi anlamda değerlendirilmeme haklarını sayabiliriz. Bu temel hakların pek çoğunun karşılanması, uygun şekilde kullanılabilmesi ve veri öznesinin işleme konusu yapılan verileri üzerinde denetim sağlayabilmesi için ²⁰³ veri sorumluları da belli yükümlülükler altında bırakılmıştır.²⁰⁴ Dahası veri sorumlularının bu doğrultudaki en temel yükümlülüğü veri öznesi tarafından kendisine yöneltilen hakkın kullanımına ilişkin talebin en kısa sürede yerine getirilmesidir. Genel Veri Koruma Regülasyonu da sayılan şekilde tanımlamış olduğu bu haklardan herhangi birinin kullanımına ilişkin veri öznesinin, veri sorumlusuna yönelttiği talebinin yerine getirilmesi için gereken bu asgari sürenin bir aylık bir zaman dilimiyle sınırlı tutulması gerektiğini öngörmüştür.²⁰⁵ Regülasyon'un veri sorumluları hakkında getirmiş olduğu bu süre sınırlamasının, veri sorumluları için daha meşakkatli uyum yükümlüklerine yol açacağı ise şüphesizdir.

1. Bilgi Edinme Hakkı

Veri öznesinin kişisel verilerinin işleme sürecine dair asgari bir takım bilgileri talep edebilme hakkına sahip olması, verilerin korunmasına ilişkin diğer ilke ve haklara kaynaklık eden ve işlerlik kazandıran, ilgilinin menfaati bakımından önem taşıyan ana bir ilkedir.²⁰⁶ Veri öznesinin bu hakka sahip olması aynı zamanda hukuka uygun veri işleminin de bir gereğidir. Bu doğrultuda bilgi edinme hakkının asgari kapsamına; verilerin herhangi bir işleme sürecinde kullanılıp kullanılmadığı, kullanılmışsa buna ilişkin ayrıntı, bu işlemin işleme amacına uygunluğu ve işleme amacı, verileri işleyen sorumluların veya yetkilendirildiği kişilerin veya verilerin transfer edildiği kişilerin kimlik bilgileri, alıcı veya alıcı gruplarının kimler olduğuna

²⁰³ KÜZECİ, *Kişisel Verilerin Korunması*, s. 229.

²⁰⁴ KVKK'nın 10. maddesinin son fıkrası da veri öznesinin kanunda sayılan haklarına ilişkin olarak veri sorumlusunun aydınlatma yükümlülüğü düzenleme altına alınmıştır.

²⁰⁵ Regülasyon md. 12/3., 4.; Gerekçe md. 59.; Benzer istikamette KVKK md. 13/2'de; "veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır." hükmünü ihtiva etmektedir.

²⁰⁶ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 91.

ilişkin bilgiler girmektedir. Hukuka ve dürüstlük kurallarına uygun veri işlemesi için veri sorumlusunun, veri öznesine ayrıca verilerin ne kadar süreyle veya hangi koşullara bağlı olarak depolanacağı, ilgilinin verilerin silinmesi, düzeltilmesi, işlemenin kısıtlanması veya işlemeye itiraz haklarının olduğu, üstün kamusal yarar gereği verilerin işlenmekte olduğu halde bu üstün kamusal yararın ne olduğu, veri öznesinin daha önce vermiş olduğu rızaya dayalı olarak gerçekleştirilen veri işlemeyi hukuka aykırı kılmayacak şekilde rızasını geri alabilme hakkının olduğu, bağımsız denetim organına şikayet hakkının bulunduğu, kişisel verinin orijinin ne olduğu ve mümkünse kamusal erişilebilir kaynaklardan gelip gelmediği, veri işlemenin veri öznesi bakımından tahmin edilen sonuçları, manası ve mantıksal içeriğine ilişkin anlamlı bilgi sağlaması gerekmektedir.²⁰⁷ Regülasyon'un bu istikametteki düzenlemesinin yanında uluslararası veri koruma belgelerinin pek çoğunun da ilgilinin bilgi alma hakkına yer verdiğini görmekteyiz.²⁰⁸ 108 Sayılı Avrupa Konseyi Verilerin Korunması Sözleşmesi'nin 8. maddesinde bu hakkın kapsamı; işleme konusu yapılmış bir verinin mevcudiyetine, varsa işlemenin amaçlarına, işleme sorumlusu kişilerin kimlik, yerleşim veya kurum bilgisine ilişkin tutulmuştur.

Veri öznesinin bilgi edinme hakkını kullanma şekli konusunda genel bir sınırlandırılma bulunduğu söylenemezse de bilgi edinmenin anlaşılır şekilde yapılması hakkın işlevsel kullanımının bir gereğidir. Buna karşılık veri öznesinin talep etmiş olduğu bilginin ilgisine anlayabileceği şekilde sunulması gerekmektedir.²⁰⁹ Veri öznesinin talebine karşılık, otomatik yöntemlere verilerin işlendiği durumda, veri sorumlusu işlemenin mantıksal yapısını ilgililerin anlayabileceği şekilde aktarmalıdır.²¹⁰ Bilgi edinme hakkının kullanılması talebi ile karşılaşan veri sorumlusunun, bu talebi öğrenmesinden itibaren makul bir süre içerisinde her halükarda bir ay içerisinde ve ücretsiz olarak yerine getirmelidir. Regülasyon'un bilgi edinme hakkının yerine getirilmesine ilişkin öngördüğü bu asgari zaman sınırlandırması yanında, bilgi edinme hakkına ilişkin belli istisnalara da yer vermiş olduğunu görmekteyiz. Veri öznesinin zaten bilgi sahibi olduğu konularda, tedariki imkansız olan veya orantısız bir çaba gerektiren kamu yararı, bilimsel, tarihi ve

²⁰⁷ Regülasyon md. 15.; Gerekçe md. 63.; Direktif md. 12.

²⁰⁸ OECD Rehber İlkeleri md. 13.

²⁰⁹ BAŞALP, Kişisel Verilerin Korunması ve Saklanması, s. 49.

²¹⁰ Direktif md. 12/a.

istatistiki amaçlarla toplanmış olan veriler hakkında ve kişisel verilerin devlet sırrı olarak saklı kalması gerekiyorsa bilgi edinme hakkı kullanılamayacaktır.²¹¹

Veri öznesinin, işleme sürecinin başından itibaren verilerinin işleme amacı konusunda bilgi sahibi olması aynı zamanda verilerinin geleceği üzerinde önceden karar verebilme inisiyatifine de kavuşmasını sağlayacaktır. Böylelikle veri öznesinin kişisel verileri, herhangi bir ihlale maruz kalmadan önleyici bir korumayla güvence altına alınmış olacaktır.²¹²

2. Erişim Hakkı

Veri öznesine, kişisel verilerinin hangi yol ve yöntemlerle, kimin tarafından ve ne zaman ve hepsinden önemlisi hangi amaçla işlendiğini bilebilme imkanı yaratan “şeffaflık ilkesi”²¹³, Regülasyon’un hukuka ve dürüstlük kurallarına uygun ve şeffaf yollardan verilerin işlenmesi hak ve yükümlüğüne ilişkin düzenlemesinin önemli bir sonucudur. Bu ilke öncelikli olarak kişisel verilerin, özellikle bilgisayarlaşmış verilerin kötüye kullanımının önüne geçmek adına, işleme sürecinde şeffaf ve kişilerin erişimine açık tutulmasını gerektirir.²¹⁴ Bu doğrultuda veri öznesinin kişisel verilerine ilişkin olarak temel bilgi alma hakkının ilerisinde ve veri koruma haklarını kuvvetlendirmek üzere, veri sorumluları veri öznelerinin kişisel verilerine erişimini sağlamakla yükümlü tutulmuşlardır. Bu erişim hakkı; veri öznesinin kişisel verilerinin herhangi bir işleme faaliyetine konu olup olmadığı bilgisini öğrenmesiyle başlamaktadır. Veri öznesinin kişisel verilerinin işleme konusu yapıldığını öğrenmesiyle; bu işlemenin amacının ne olduğu, verilerinin işlenmekte olduğu kategorilerin hangileri olduğu, verilerinin paylaşılabileceği alıcı gruplarının kimler olduğu, verilerinin depolanabileceği zaman dilimi; unutulma, düzeltme, işlemenin kısıtlanması veya işlemeye itiraz gibi haklarının mevcut olduğu; komisyona şikayet hakkının bulunduğu; veri öznesinden toplanmamış olan verilerin kaynağının ne olduğu ve veri öznesi üzerinde önemli etkileri olan otomatik işlenmenin mantıksal yapısının nasıl olduğu bilgisine erişim hakkı mevcuttur. Veri öznesinin bu konularda bilgiye erişim isteyebilme hakkının yanında, verilerinin herhangi bir işleme konusu yapılp

²¹¹ Regülasyon md. 14/5.

²¹² ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 83.

²¹³ Regülasyon md. 5/a.

²¹⁴ KÜZECİ, *Kişisel Verilerin Korunması*, s. 95.

yapılmadığını gösteren duruma ilişkin bir örnek talep etme hakkı dahi bulunmaktadır.²¹⁵

Veri öznesinin kendisine ait kişisel bir verinin işlenip işlenmediğine ilişkin bilgiye erişemediği koşulda, kişisel verilerinin korunması da söz konusu olamayacaktır. Kamusal organların, hukuk devletinin temel bir şartı olarak kamusal faaliyetlerini şeffaflık ilkesi doğrultusunda yürütmesi gereğinin; vatandaşlarının kişisel verilerinin işlenmesi konusunda da aynı şekilde şeffaf olmasını gerektirdiği şüphesizdir.²¹⁶ Bu doğrultuda veri işlem faaliyetlerine ilişkin sicillerin ilgili kişilere açıklığı ve erişilebilir olmasının da veri öznesinin erişim hakkını gerçekleştirmeye elverişli bir uygulama olduğunu söyleyebiliriz.

3. Düzeltme Hakkı

Veri öznesinin bilgi alma hakkı kapsamında veya bu haktan bağımsız olarak öğrendiği kendisiyle ilgili doğru olmayan kişisel verilerin, gecikmeksizin düzeltilmesini veya silinmesini talep etme hakkı mevcuttur. Veri Koruma Direktif'i veri öznesi hakkında toplanan, tutulan veya her hangi başka surette işleme konusu yapılan verilerin doğru veya gerçek durumu yansıtmıyor veya eksik olması hallerinde, veri öznesine düzeltme ve silme talep edebilme haklarının yanı sıra veriye erişimin engellenmesinin sağlanmasını isteme hakkını da tanımıştır.²¹⁷ Ancak erişimin geçici surette engellenmesi gibi önleyici bir tedbir olarak da düşünebileceğimiz bu hakkın uygulanabileceği durumlar düzenlenmemiştir.²¹⁸ Veri öznesinin düzeltme hakkını düzenleyen Genel Veri Koruma Regülasyonu'nun 16. maddesi ikinci fıkrasında düzeltme hakkının kapsamını daha da genişletmiş ve bu hakkın, aynı zamanda işleme

²¹⁵ Regülasyon md. 15/3.; Direktif md. 12.; KVKK md. 11/1 b.,c.,ç.

²¹⁶ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 88.; Özellikle kişisel verilerin korunması hakkı ile eşzamanlı olarak hukuki gelişimini gerçekleştiren ve bu hakkın tamamlayıcısı olarak da görülen "bilgi edinme hakkı"; kamusal organların, vatandaşları hakkında tuttuğu kişisel veri niteliğinde olabilen bilgi veya kendi hizmet, çalışma veya işlemlerine ilişkin bilgiye ulaşabilmesine hizmet etmektedir. Kişinin kendisi hakkında işleme konusu yapılan bir veri söz konusu olması halinde bu verilere erişebilmesine hizmet eden bilgi edinme hakkının; kişisel verilerin korunmasına ilişkin temel ilkelerin sağlamayı amaçladığı önleyici korumayı gerçekleştirebilme işlevi de bulunmaktadır. Aynı zamanda bir kişinin bilgi edinme hakkını kullanması halinde bir başka kişinin kişisel verilerinin, bu hakkın kullanımına karşılık olarak 3. kişilerle paylaşılması gibi ihlal yaratma, verilerin korunması hakkına yönelik bir müdahale oluşturabilme riski de gündeme gelebilecektir. KÜZECİ, *Kişisel Verilerin Korunması*, s. 105., 107.

²¹⁷ Direktif md. 12/b.; Bu hakka karşılık olarak Regülasyon'un 18. maddesinde münhasır bir hak olarak düzenlenmiş olan *işlemenin sınırlandırılması hakkı* gösterilebilir.

²¹⁸ KÜZECİ, *Kişisel Verilerin Korunması*, s. 235.

amacı göz önünde tutulduğunda eksik kalan kişisel verilerin tamamlanmasını talep etmeyi de içerdiği hüküm altına alınmıştır.²¹⁹ Böyle bir talep karşısında veri sorumlusu; en kısa süre içerisinde gerekli düzeltme veya eksikliğin giderimini gerçekleştirmek zorundadır. Veri sorumlusunun daha önce bu kişisel verileri paylaştığı alıcı veya alıcı gruplarına da, imkansız veya olağanüstü bir çaba gerektirmiyorsa bu düzeltmeyi bildirmesi gerekmektedir.²²⁰ Kişisel Veri Koruma Kanunu'nda da veri sorumlularına, daha önce verilerin eksik veya yanlış işlenmesi neticesinde veri öznesinin düzeltme hakkını kullandığını ve bu doğrultuda işlem yapıldığını verilerin aktarıldığı üçüncü kişilere bildirme yükümlülüğü getirmiştir.²²¹

4. Unutulma Hakkı

Genel olarak verilerin silinmesi hakkının karşıladığı kabul edilen unutulma hakkı, veri öznesine, verilerinin işlenmesine devam edilmesinin gerekçesiz kalması halinde veri sorumlusundan bu verilerin silinmesi, veri sorumlusunun hakimiyet alanından çıkartılması²²², kullanıcıların erişimine ve kullanımına geri dönülemez şekilde kapatılmasının sağlanması²²³ veya veriler üzerinde veri sorumlusunun kontrol imkanını yok edecek her türlü tedbirin alınması²²⁴ talebinde bulunabilme yetkisi sağlamaktadır.²²⁵ Unutulma hakkı, veri öznesine geleceğini özgürce şekillendirebilmesi için geçmişte üzerinde serbestçe tasarrufta bulunabilme imkanı

²¹⁹ Regülasyon md. 16.

²²⁰ Regülasyon md. 19.

²²¹ KVKK md. 11/d., f.

²²² BAŞALP, *Kişisel Verilerin Korunması ve Saklanması*, s. 50.

²²³ Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik md. 8.

²²⁴ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 93.

²²⁵ “Unutulma hakkı, internet ortamında bir haberin uzun süredir kolayca ulaşılabilir olması nedeniyle kişinin şeref ve itibarının zedelenmesi durumunda gündeme gelmektedir. Bu hakkın amacı, internetin yaygınlaşması ve sağladığı imkânlar nedeniyle ifade ve basın özgürlükleri ile kişilerin manevi varlığının geliştirilmesi hakkı arasında gerekli hassas dengenin kurulmasını sağlamaktır.” Anayasa Mahkemesi, N.B.B. Başvurusu.; “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 kullanılmamasını 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.” Yargıtay HGK., E: 2014/4-56, K: 2015/1679, T:17.6.2015.

yaratmaktadır.²²⁶ Diğer bir deyişle unutulma hakkı, geçmişte işlemiş olan verilerinin saklanıp saklanmaması konusunda tercihte bulunabilme yetkisinin veri öznesine devredilmesi neticesi yaratmaktadır.²²⁷ Bu hakkın yerine getirilmesi amacı doğrultusunda silmenin gerçekleştirilmesini sağlayacak yöntem ise; manuel gerçekleştirilen işlemlerde fiziki evrakın yok edilmesi, otomatik yöntemlerle veri işlemlerinde ise verilerin kayıtlı olduğu taşıyıcılarından veya ortamlardan çıkartılması veya verilerin kişi ile ilişkisini koparacak şekilde ayrıştırılarak yok edilmesidir.²²⁸

Regülasyon'un unutulma hakkını daha geniş ve bağımsız bir hak olarak düzenlediği 17. maddesiyle veri öznesine, belli hallerin gerçekleşmesine bağlı olarak veri sorumlusundan gecikmeksizin verilerinin silinmesini talep edebilme yetkisi tanınmıştır. Özellikle toplanma ve/veya işleme amacı için kişisel veriye ihtiyaç kalmamışsa; veri öznesinin rızasına dayalı olarak işlemenin yapıldığı hallerde rızanın geri alınmış olması sebebiyle işlemenin yasal temeli ortadan kalkmışsa; veri öznesi işlemeye itiraz etmiş veya kişisel verilerin işlenmesi başka bir sebeple Regülasyon'la bağdaşmıyorsa veri öznesinin, verilerinin silinmesini ve daha fazla işlenmemesini talep edebilme hakkı mevcuttur.²²⁹ Veri öznesinin, özellikle çevrimiçi ortamda unutulma hakkını kuvvetlendirecek şekilde verilerinin silinmesini talep etme hakkının kapsamı; verileri halka açıklayan veri sorumlularının, bu verileri işleyen üçüncü kişilere de verilerin çoğaltılmış nüshaları, kopyaları ve bağlantılarının silinmesine ilişkin bildirimde bulunmakla yükümlü tutulacak şekilde genişletilmelidir.²³⁰

Bu hakkın Avrupa Birliği Adalet Divanı tarafından konu edinildiği önemli kararlardan biri olarak Google Kararı'nı gösterebiliriz. Kararın konusunu; vatandaşların kendilerine ilişkin daha önce işlenmiş olan kişisel verilerin, "geçersiz, eksik veya daha sonradan ilgisiz hale gelmesi" sebepleriyle silinmesi gerektiğine ilişkin Google'a yönelttikleri talepleri oluşturmaktadır. Bu taleplerinin yerine getirilmemesi üzerine Divan'a taşınan olaya ilişkin olarak, 95/46 Sayılı Direktif'in 6. maddesi ekseninde ve kişilerin unutulma hakkının mevcut olduğu istikametinde karar

²²⁶ AKGÜL, , Aydın, "Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" ve AB Adalet Divanı'nın "Google Kararı"", Türkiye Barolar Birliği Dergisi, S. 116, 2016, s. 17.

²²⁷ LAÇİN, İrem, "Unutulma Hakkı", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Doç. Dr. Melike Batur Yamaner'in Anısına Armağan, C. 1, 2014, s. 395.

²²⁸ BAŞALP, Kişisel Verilerin Korunması ve Saklanması, s. 50.

²²⁹ Regülasyon Gerekçe md. 65.

²³⁰ Regülasyon Gerekçe md. 66

verilmiştir.²³¹ Yargıtay 4. Hukuk Dairesi'nin, yerel mahkeme tarafından kısmen kabul edilen manevi tazminat istemine itiraz edilmesi üzerine huzuruna taşınan bir olayda da; davacı şikayetçisi olduğu bir ceza dosyası kapsamında isminin kodlanılmaksızın bir eserde kullanılması üzerine bu durumun kişilik hakkını ihlal ettiği iddiasında bulunmuştur. Davacının iddiası ilk derece mahkemesince kısmen manevi tazminata hükmetmeye esas kabul edilmişse de Daire eserin bilimsel nitelik taşımakta olması dolayısıyla kişilik hakkı ihlali yaratmayacağı dolayısıyla istemin haksız olduğu ve kararın bozulması gerektiği doğrultusunda karar vermiştir. Ancak 4. Hukuk Dairesi'nin oy çokluğuyla verdiği bu kararın karşı oy gerekçesinde; davacının şikayetçisi/mağduru olduğu suçun niteliği itibarıyla da kişinin psikolojik olarak hayatı boyunca sarsılmasına sebep olabileceği ve kişinin özel hayat alanına dahil kişisel bir veri olarak korunması gereken adının, bir eserde kendi rızası olmaksızın yer almasının hukuka aykırı olduğu belirtilmiştir. Ayrıca bu durumun kişinin unutulma hakkına yönelik bir ihlal olduğu da vurgulanmıştır.²³² İlk derece mahkemesinin direnme kararının davalı vekilince temyiz edilmesi üzerine dosya, Yargıtay Hukuk Genel Kurulu'na gelmiştir. Hukuk Genel Kurulu'nca; *“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 zorunlu...”* görülmüştür.²³³

²³¹ ATAD, Google Spain & Mario Costeja Gonzalez Davası, C-131/12, T: 13.5.2014. https://curia.europa.eu/jcms/jcms/j_6/en/; BOZAN, Mısra, “Gizlilik, Bireysel Haklar ve Kişisel Verilerin Korunması”, 20. Türkiye'de İnternet Konferansı, (Çevrimiçi) <http://inet-tr.org.tr/inetconf20/kitap/inet15-MBorazan.pdf> (08.03.2018); AKGÜL, “Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı'nın “Google Kararı””, s. 31.

²³² Yargıtay 4. HD., E:2013/6256, K: 2013/12821, T: 03.7.2013.

²³³ “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.” Yargıtay HGK., E: 2014/4-56, K: 2015/1679, T: 17.6.2015.; “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 şeref ve itibarının korunması hakkı ve Anayasa'nın 20. maddesinin ü.üncü 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 imkan tanımayı kapsamaktadır.” Anayasa Mahkemesi N.B.B. Başvurusu.

5. İşlemenin Sınırlandırılması Hakkı

Verilerin bloke edilmesi olarak da nitelendirilebilen verilerin işlenmesinin kısıtlanması/sınırlandırılmasını talep edebilme hakkı; özellikle işlenmekte olan verilerin doğruluğu konusunda tereddüt bulunması, işlemenin hukuka aykırı olması veya işleme amacının gerçekleşmiş olması sebepleriyle veri sorumlusunun kendisine ait verileri silmesine veri öznesinin yasal suçlamalardan sıyrılma gibi şahsi gerekçelerle itiraz etmesi hallerinde ileri sürülen ve önem kazanan bir haktır.²³⁴ Verilerin kısıtlanması veya bloke edilmesi; verilerin yalnızca veri sorumlusunun kontrolünde tutulması ve sınırlı amaçla kullanılabilmesi, işlemenin engellenmesi²³⁵ veya veri sorumlusunun verilerin işlenmesine ilişkin yetkisinin önemli bir kısmının veya tamamının devam etmemesi²³⁶ anlamına gelmektedir. Verilerin kısıtlanma yöntemleri olarak; kısıtlanması talep edilen verilerin geçici olarak başka bir işleme sistemine taşınması, ilgili verilerin kullanıcıların erişimine kapatılması ya da geçici olarak yayınlanan verilerin internet sitesinden kaldırılması kullanılabilir. Verilere erişimin kısıtlanmış olması halinde bu durum sistemde açıkça gösterilmelidir.²³⁷ Ulusal veri koruma mevzuatımızda her ne kadar verilere erişimin kısıtlanmasına ilişkin veri öznesine doğrudan bir hak tanınmış değilse de; kendisi hakkında doğru olmadığını düşündüğü verilerinin bir internet sitesinde yayınlanmakta olmasının kişilik haklarına müdahale teşkil ettiği iddiasında bulunan veri öznesinin, yayının yapıldığı ve kendisi hakkında doğru olmayan verilerin işlendiği internet sitesine erişimin engellenmesini talep edebilme hakkı 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'u ile korunmaktadır.²³⁸

²³⁴ Regülasyon md. 18.

²³⁵ BAŞALP, Kişisel Verilerin Korunması ve Saklanması, s. 50; ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 90.

²³⁶ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 93.

²³⁷ Regülasyon Gerekçe md. 67.

²³⁸ 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun md. 9.; Bu tedbirin temel amacı, konusu suç teşkil eden internet içeriklerine Türkiye'den erişimin önüne geçilmesidir. Bu sebeple muhakemeye ilişkin bir fayda sağlamak düşüncesi taşımayan, erişimin engellenmesi tedbirinin bir muhakeme veya koruma tedbiri olduğunu söylemek doğru olmayacaktır. DÖNMEZER, Sulhi, ERMAN, Sahir, *Nazari ve Tatbiki Ceza Hukuku*, 14. Baskı, İstanbul, Der Yayınları, 2016, s. 139.

6. Verilerin Taşınması Hakkı

Veri öznesinin rızasına veya sözleşmeye dayalı olarak işlenen, veri öznesince temin edilmiş ve otomatik yöntemlerle işlenen kişisel verilerin; planlanmış, sürekli kullanılan ve makinece okunabilir bir formatta veri öznesince almasına ve engelsiz bir şekilde bir başka veri sorumlusuna iletilmesine imkan sağlayan hak, veri öznesinin veri transferini talep edebilme hakkıdır. Bu hak doğrudan ve kapsamlı bir şekilde Regülasyon'un 20. maddesi düzenlemesi ile veri koruma ilkeleri arasında yerini almıştır. Bu hakkın düzenleme konusu yapılması ve veri öznesine verilerin transferine ilişkin yetki tanınmış olmasının temel amacı ise; kişisel verilerin bir servis sağlayıcısından diğerine aktarımına olanak sağlamaktır. Bu şekilde kişisel verilerinin aktarımının kolaylaştırılması, servis sağlayıcıları arasındaki rekabeti de artıracaktır. Bu hakkın aynı zamanda veri öznesinin kendisiyle ilgili kişisel verileri üzerindeki idaresi ile, veri sorumlusu ve veri öznesi arasındaki ilişkinin yeniden dengelenmesi imkanı oluşturduğunu da söyleyebiliriz.²³⁹

Veri öznesinin; bir veri sorumlusu tarafından işlenen verilerini başka bir sorumluya aktarmaksızın sadece kendi kişisel kullanımı için kaydetmesi ve/veya bir başka servis sağlayıcıya aktarmasını sağlayan bu hakka konu olan kişisel verilerin yapılandırılmış, sürekli kullanılan, makinece okunabilir formatta olması önem taşımaktadır. Bu hak kapsamında bir veri öznesinin, internet üzerinden müzik yayın hizmeti veren ve kişinin güncel çalma listesini ve hangi şarkıyı ne sıklıkla dinlediğine ilişkin verilerini bu işleyen sorumludan, satın alacağı müziklerin tespiti için alması ya da daha önceki dinleme listesinin farklı bir müzik kanalına aktarılmasını için bu verilerin transferini talep edebilmesi söz konusu olabilecektir.²⁴⁰

Transferi talep edilen verilerin birden fazla kişiyi ilgilendirmesi halinde, veri sorumlusunca başka bir servis sağlayıcıya aktarılan veya veri öznesine belli formatta

²³⁹ HELVACIOĞLU, Asli Deniz, STAKHEYEVA, Hanna, "The Tale Of Two Data Protection Regimes: The Analysis Of The Recent Law Reform In Turkey In The Light Of EU Novelties", Computer Law&Security Review, C. 33, 2017, s. 818.; Veri Çalışma Grubu'nun 05.05.2017 Tarihli Verilerin Transferi Hakkındaki Kılavuzu (Guidelines on The Right To Data Portability, Article 29 Data Protection Working Party).

²⁴⁰ Kişisel verilerin, kişilerin erişimine ve servisler arası aktarımına olanak sağlayan bu hakkın kullanım ihtiyacını karşılamak üzere geliştirilmiş bazı programlar dahi mevcuttur. Taşınabilir ve güvenli bir şekilde kişilere, kişisel tüketim ve alışveriş verilerini kullanma, erişme ve gösterme imkanı sağlayan bir yenilikçi ve hükümet destekli programla; kişilere harcama alışkanlıklarını anlama konusunda yardım etme veya ihtiyaçlarını karşılamak için daha iyi öneriler sunabilecek programlar veya uygulamalar kullanabilme avantajı sağlama amaçlanmaktadır. <http://www.pcamidata.co.uk> (02.01.2018)

teslim edilen bu kişisel verilerin, talep edenin kontrollü altında olduğundan ve yalnızca kişisel ve ailevi amaçlarla istendiğinden emin olunmalı ve aktarılan veri sorumlusunun kendi çıkarları ve amaçları doğrultusuna verileri işlememesi sağlanmalıdır. Aksi takdirde bu şekilde gerçekleştirilen işlemenin hukuka aykırı olması kaçınılmazdır.²⁴¹

7. İtiraz ve İrade Sergileyebilme Hakkı

Kişisel verilerin hukuka ve iyiniyet kurallarına uygun işlenmekte olduğu ilgilinin rızası, sözleşme koşullarının yerine getirilmesi gibi hukuki düzenlemelerle sınırlandırılmış belli durumlar mevcuttur. Verilerin, kişinin iradesine tam manasıyla üstünlük tanınmaksızın üstün kamusal yarar veya yasal hükümler gereği gerekçelerine dayanarak hukuka uygun işlendiği hallerde, veri öznesine işlemeye itiraz hakkı tanınmıştır.²⁴² Bu durumlarda gerçekleştirilen veri işlemeye veri öznesinin itiraz hakkının düzenlenmiş olması, dolaylı olarak bu gerekçelerin işlemenin hukuka uygunluğunu sağlama noktasındaki kesinliğine gölge düşürmüş olmaktadır. Şöyle ki; kamusal yarar veya yasal hükümler gereği verileri işlenmekte olan ilgilinin, itiraz hakkını kullanmasıyla veri işleme hukuka aykırı hale gelecek ve işlemenin veri sorumlusunca gecikmeksizin sonlandırılması gerekecektir. Ancak veri sorumlusu, veri öznesinin özgürlükleri, hakları ve çıkarlarına üstün gelen işlemenin mecburi yasal temellerini ispat etmesi veya verileri işlemeye yasal hakların savunulması, kullanılması veya tesisi için gerek duyması hallerinde işlemeye devam edilebilecektir. Bunların dışında hiçbir gerekçeye dayanarak veri sorumlusunun, veri öznesince itiraz edilen işlemeye son vermemesi mümkün değildir.²⁴³ Aksi durumda ise ilgilinin kanun yollarına başvurma hakkı gündeme gelecektir.²⁴⁴

Bunun yanında Regülasyon'da veri öznesinin, doğrudan reklam amacıyla verilerinin işlenmesine, doğrudan reklam amacıyla verilerin işlenmesi suretiyle profil çıkarma da dahil, süresiz ve ücretsiz itiraz hakkını da özel olarak düzenlemiştir.

²⁴¹ Veri Çalışma Grubu'nun 05.05.2017 Tarihli Verilerin Transferi Hakkındaki Kılavuzu (Guidelines on The Right To Data Portability, Article 29 Data Protection Working Party).

²⁴² Bu hakkın "veri işlemeye itiraz ve otomatik bireysel kararların konusu olmama hakkı" şeklinde kullanıldığına da rastlanılmıştır. Bkz. KÜZECİ, *Kişisel Verilerin Korunması*, s. 235.

²⁴³ Regülasyon md. 21/1.; Direktif md. 14.

²⁴⁴ 108 Sayılı Avrupa Konseyi Veri Koruma Sözleşmesine göre de veri öznesinin; bilgi edinme, silme veya düzeltme gibi temel haklarının kullanımını etkisiz kılacak şekilde taleplerinin yerine getirilmemesi karşısında kanun yoluna başvurulabilme hakkı mevcuttur. md. 8.

Regülasyon’a göre veri öznesinin böyle bir hak sahibi olduğu anlaşılır biçimde ve başka her türlü bilgidan ayrıştırılmış olarak açıkça dikkatine sunulmalıdır.²⁴⁵

Ulusal mevzuatımız ise itiraz hakkını; işlenen verilerinin münhasır otomatik sistemler vasıtasıyla analiz edilmesi²⁴⁶ suretiyle veri öznesinin aleyhine bir sonuç çıkarılması halinde kullanılabilecek bir hak olarak düzenlemiştir.²⁴⁷ Kişinin verilerinin işlenmesine ilişkin itiraz hakkından farklı olarak ele alınması gereken “otomatik bireysel kararlara tabi olmama”²⁴⁸ hakkının temel amacı; kişilerin otomatik surette değerlendirilmesi sonucunda verilecek kararlara karşı irade göstererek bireysel özerkliğinin korunması ve otomatik karar alma sürecinde etkisiz basit bir obje konumuna sokulmasının engellenmesidir.²⁴⁹ Örneğin; iş arayan bir kişinin veya kredi başvurusunda bulunan bir kişinin tabi tutulduğu psikolojik bir testin otomatik değerlendirmesi sonucu işe alınmaması veya kredi vermeye uygun görülmemesi ilgilinin itiraz hakkı kapsamındadır.²⁵⁰ Veri Koruma Direktifi ve Regülasyon da kişilerin profillerinin çıkartılması²⁵¹ da dahil tutularak itiraz hakkını koruma altına almıştır. Regülasyon’un 22. maddesi kapsam itibariyle itiraz hakkını genişletmiş olmakla birlikte, otomatikleştirilmiş kararların konusu olmaya ilişkin itiraz hakkının sınırlandırılma koşullarını da düzenlemiştir. Buna göre; kişilerin açık rızası varsa, veri sorumlusuyla akdettikleri anlaşmanın ifası için gerekliyse ve veri sorumlusunun hakları, özgürlükleri ve yasal menfaatleri güvence altına alınmak suretiyle hukuki olarak yetki sağlanmışsa veri öznesinin kişisel verilerinin otomatik değerlendirmesi

²⁴⁵ Regülasyon md. 21/3., Gerekçe md. 70.

²⁴⁶ Verilerin kısmi olarak işlenmesi kişinin daha sınırlı olarak verilerinin kötüye kullanımına yol açabilecekken, kişiye ilişkin kısmi birden fazla verinin bir araya getirilmesi ile, kişilik profilinin çıkartılması ve otomatik kararlara konu edilme gibi temel hak ve özgürlükler bakımından daha ağır sonuçlar yaratmaya elverişli neticeler de oluşabilecektir. ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 1.

²⁴⁷ KVKK md. 11/g.

²⁴⁸ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 47.

²⁴⁹ KÜZECİ, *Kişisel Verilerin Korunması*, s. 236.; ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 47.

²⁵⁰ BAŞALP, *Kişisel Verilerin Korunması ve Saklanması*, s. 54.; Bu ilkenin düzenlenmesinin temel gerekçesi olarak kişilerin çıkarlarını önemli derecede etkileyecek kararların otomatik değerlendirmeler neticesinde değil, gerçek kişilerin takdirinde olması gerekliliği gösterilmektedir. Dolayısıyla işverenlerin veya diğer kurum ve kuruluşların bu ilkeye uygun şekilde karar alma mekanizmaları yaratmaları gerekecektir. KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 128.

²⁵¹ Profil çıkarma; gerçek bir kişinin kişisel yönlerini değerlendiren, özellikle de veri öznesinin iş hayatındaki performansı, ekonomik durumu, sağlığı, kişisel tercihleri veya ilgi alanları, güvenilirliği yönündeki tahmin veya analizler de dahil, her türlü otomatik veri işlemeyi içeren faaliyettir. Bkz. Regülasyon Gerekçe md. 71.

sonucu verilecek kararlara ve profilinin ıkarılmasına itiraz edebilmesi sz konusu olamayacaktır.²⁵²

III. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ULUSLARARASI DÜZENLEMELER

Günümüzde kişisel verilerin, bilgisayar vasıtasıyla işlenmesi manuel şekilde işlenmesine oranla daha fazla karşımıza çıkmaktadır. Bilgisayar sistemleriyle işlenen verilerin, bilişim teknolojilerinin sağladığı sınır tanımayan veri transferi gibi imkanlar dolayısıyla yalnızca ulusal veri koruma düzenlemeleriyle etkin şekilde korunabilmesi mümkün görülmemiştir. Bu doğrultuda 1980’li yıllar itibarıyla OECD, Avrupa Konseyi, Birleşmiş Milletler, Avrupa Birliği başta olmak üzere uluslararası organizasyonlar kişisel verilerin korunmasına ilişkin temel belli düzenlemeler öngörmüştür.²⁵³ Bu bağlamda kişisel verilerin münhasıran ele alındığı ve verilen korunmasına ilişkin özel olarak düzenlenen metinler yanında organizasyonların temel kurucu metinleri çerçevesinde de verilerin korunmasına ilişkin güvenceler temin edilmiş olduğunu görmekteyiz.

Çalışmamız kapsamında da OECD, Avrupa Konseyi, Birleşmiş Milletler ve Avrupa Birliği gibi organizasyon ve kuruluşlar tarafından veya bu kuruluşların bünyesinde oluşturulmuş uluslararası düzenlemeler belli oranda ele alınmaya çalışılmıştır. Kişisel verilerin korunmasının bilişim sistemleriyle olan ilişkisi itibarıyla sürekli gelişen ve güncel bir alan olması, mevcut düzenlemelerin zaman içerisinde yetersiz kalması veya düzenlenmemiş yeni alanların oluşması neticesi yaratabilmektedir. Bu hızlı gelişimin takibi bakımından nasıl ki hukuki düzenlemeler yetersiz kalabilmekteyse, çalışma genelinde bütün düzenlemelere yer vermekte yetersiz kalılabileceği de olası kabul edilmelidir. Bu doğrultuda ancak önem itibarıyla belli temel düzenlemelere yer verilmiş ve bu düzenlemeler önemli yönleriyle ele alınmaya çalışılmıştır.

²⁵² Direktif md. 15/2.

²⁵³ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 12.

A. OECD Düzenlemelerinde Kişisel Verilerin Korunması

Kişisel verilerin korunması alanında ulusal hukukları yaklaştırma girişimi; ilk olarak Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) tarafından 1980 yılında, “Özel Yaşamın ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Yönlendirici İlkeler”²⁵⁴ yayımlanarak gösterilmiştir.²⁵⁵ OECD Rehber İlkeleri, üye ülkeleri bağlayan çoğulcu demokrasi, insan haklarına saygı ve açık market ekonomisi gibi OECD’nin üç temel ilkesi lehine benimsenmiştir.²⁵⁶ Kişisel verilerin mahremiyetinin korunmasına ilişkin belli asgari standartların benimsenmesi, üye devletlerin ulusal hukuk kuralları ve uygulamaları arasındaki farklılıkların azaltılması, verilerin üye devletler arasında akışının meşru olmayan şekilde engellenmesinin önlenmesi ve üye devletlerin sınır ötesi veri akışının kısıtlaması neticesi yaratacak meşru olmayan gerekçelerinin ortadan kaldırılması amaçlarıyla oluşturulmuş olan Rehber İlkeler’in, üye devletleri bağlayıcılığı bulunmamaktadır. Tavsiye niteliğindeki bu düzenleme, üye devletlere verilerin korunmasına ilişkin getirilen Rehber İlkeleri iç hukuklarına aktarma konusunda tam bir serbestlik tanımaktadır.²⁵⁷ Ancak özellikle verilerin korunması konusunda üye devletler arasında işbirliği yapılması²⁵⁸, verilerin korunmasına ilişkin ulusal düzenlemelerde bu ilkelerin benimsenmesi ve verilerin sınır ötesi transferinin haksız engellenmemesi konuları düzenlemenin tavsiyede bulunduğu ve önemsedığı alanlardır. OECD Rehber İlkeleri serbest piyasa ekonomisini geliştirmeye ilişkin yönü de bulunan ilk uluslararası veri koruma düzenlemesidir.²⁵⁹ Bunun yanında düzenlemeyi önemli kılan başlıca özellik; uluslararası ölçekte konuyu ele alma ihtiyacına karşılık olarak düzenlenmiş ilk uluslararası metin olarak, daha sonra hazırlanan pek çok ulusal ve uluslararası veri koruma düzenlemesi için rehber niteliğinde olmasıdır.

OECD Rehber İlkeleri’nin her ne kadar üye devletler bakımından bağlayıcılığı bulunmaktaysa da, bu ilkeler değişen teknolojik gelişmelere uyum sağlayarak günümüzde bile hem özel sektörün hem de kamunun geniş çaplı ilgisini görmektedir.

²⁵⁴ OECD Kişisel Verilerin Sınır Aşan Transferi ve Mahremiyetin Korunması Rehber İlkeleri (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data). Orijinal metin için bkz. <http://www.oecd.org> (02.02.2018).

²⁵⁵ LYNKEY, *The Foundations of EU Data Protection Law*, s. 47.; KÜZECİ, *Kişisel Verilerin Korunması*, s. 130.

²⁵⁶ OECD Rehber İlkeleri

²⁵⁷ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 13.

²⁵⁸ OECD Rehber İlkeleri md. 20.

²⁵⁹ LYNKEY, *The Foundations of EU Data Protection Law*, s. 48.; AKSOY, *Kişisel Verilerin Korunması*, s. 4., 7.; KÜZECİ, *Kişisel Verilerin Korunması*, s. 130.

Ulusal veya uluslararası boyutta tüm veri işleme süreçlerine, veri türlerine ve bilgisayarlaştırılmış veri işlemenin tüm ortamlarına uygulanabilirliğini sürdüren OECD Rehber İlkeleri, günümüzde de veri koruma hukuku bakımından önemini korumaktadır. OECD Rehber ilkeleri, kişisel verilerin korumasına ilişkin amaçla bağlılık, ölçülülük, verilerin güvenliği ve kaliteli olması gibi ilkelerin, veri öznesinin katılımına ilişkin ilkelerin ve veri sorumlusunun hesap verebilirliğine dair temel ilkelerin yer aldığı rehber niteliğinde çerçeve bir düzenlemedir.²⁶⁰

Düzenlemenin ikinci kısmında yer verilen temel veri koruma prensipleri; toplamının sınırlandırılması prensibi, veri kalitesi prensibi, amaçla bağlılık prensibi, kullanımının sınırlandırılması prensibi, veri güvenliği prensibi, şeffaflık prensibi, hesap verilebilirlik ve veri öznesinin verileri üzerindeki kontrolünü sürdürmesini sağlayan haklarına ilişkin ilkelerden ibarettir.²⁶¹

B. Birleşmiş Milletler Temel Metinlerinde Kişisel Verilerin Korunması

Birleşmiş Milletler Örgütü 1945'te kurulmuş, halen 193 üyesi bulunan ve 21. yüzyılda insanlığın karşı karşıya geldiği barış, güvenlik, iklim değişikliği, insan hakları, cinsiyet eşitliği, terörizm gibi konularda, uluslararası karakterine ve kurucu sözleşmede benimsenen dünya barışını, güvenliğini korumak ve uluslararası ekonomik, toplumsal ve kültürel bir iş birliği oluşturmak gibi amaçlarına dayanarak harekete geçebilen uluslararası bir örgüttür.²⁶² Birleşmiş Milletler Kurucu Anlaşması'nın gerekçe kısmında; temel insan haklarının, insan kişiliğine mahsus değerlerin ve insan onurunun korunması, bunlara saygı gösterilmesi amaçlarına yer verilmiştir.²⁶³ Bu durum, günümüzde temel bir insan hakkı olarak kabul ettiğimiz kişisel verilerin korunması hakkı veya bu hakkı koruma alanında saklı tutan özel yaşamın gizliliği hakkının da Birleşmiş Milletler tarafından korunmasını gerektirmesi itibarıyla önemlidir.

Birleşmiş Milletler Şartı'nın sağlamış olduğu bu genel korumanın yanı sıra temel insan haklarına ve kişilerin özel yaşamının gizliliği hakkına spesifik olarak yer

²⁶⁰ OECD Rehber İlkeleri

²⁶¹ OECD Rehber İlkeleri, md. 7-14.

²⁶² Birleşmiş Milletler Resmi İnternet Sayfası, <http://www.un.org/en/sections/about-un/overview/index.html> (29.01.2018).

²⁶³ Birleşmiş Milletler Kurucu Sözleşmesi Türkçe orijinal metni için bkz. <http://www.unicankara.org.tr> (29.01.2018)

veren ve dolayısıyla kişisel verilerin korunması özelinde de başvurabileceğimiz Birleşmiş Milletler bünyesinde iki temel metin bulunmaktadır. Bu metinler ve konuya ilişkin düzenlemeleri; Birleşmiş Milletler Evrensel İnsan Hakları Beyannamesi'nin 12. maddesi²⁶⁴ ve Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'nin 17. maddesidir.²⁶⁵ Özel yaşamın korunmasını temel hakkı kapsamında; kişilerin özel yaşamı, aile yaşamı, şeref ve haysiyetinin korunması ve bu eksende kanuni güvencelerin sağlanması bu düzenlemelerde yer almaktadır.²⁶⁶ Bunun yanı sıra Birleşmiş Milletler, kişisel verilerin korunması münhasır alanına yönelik olarak da 1990 tarihinde, verilerin otomatik veya otomatik olmayan ancak elektronik ortamda/bilgisayarla işlendiği hallerde uygulanabilen, kişisel verilerin korunmasında benimsenmesi gereken, tavsiye niteliğindeki “Bilgisayarla İşlenmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler”i kabul etmiştir.²⁶⁷ Üye devletlerin kişisel verilerin korunmasına ilişkin yasal düzenlemelerine esas alınması tavsiye olunan bu ilkeler; hukuka ve dürüstlük kurallarına uygun verilerin toplanması ve işlenmesi, işlenen verilerin doğruluğunun sağlanması ve kontrolü, amacın belirliliği, ilgili kişinin erişim hakkına sahip olması, ayırım gözetmeme ilkesi, veri güvenliği ilkesi, denetleyici mercilerin oluşturulması ve sınır ötesi veri transferine ilişkin ilkelerden ibarettir.²⁶⁸

C. Avrupa Konseyi Düzenlemelerinde Kişisel Verilerin Korunması

Avrupa Konseyi, milletlerarası barışın sağlanması ve devamlılığını sağlamak üzere, demokrasi ve hukukun üstünlüğü prensipleri doğrultusundaki tüm ilke ve

²⁶⁴ İnsan Hakları Evrensel Beyannamesi Türkçe orijinal metni için bkz. <http://www.un.org.tr>.

²⁶⁵ Medeni ve Siyasi Haklar Sözleşmesinin Türkçe orijinal metni için bkz. <http://www.un.org.tr>; Birleşmiş Milletler İnsan Hakları Komitesi'nin Medeni ve Siyasi Haklar Sözleşmesi 17. maddesi “özel yaşamın korunması” hakkının içeriğine dair 16. Nolu Genel Yorumunda; kişisel verilerin kamu otoriteleri veya özel kurumlarca bilgisayar, veri bankası veya benzer vasıtalarla işlenmesinin yasal bir düzenlemeye bağlı olması gereğine ve bu düzenlemelerin verilerin işlenmesinde esas alınması gereken veri güvenliği, amaçla bağlı ve orantılılık gibi temel ilkelere uygun ve veri öznesinin bilgi edinme, düzeltme ve sildirme temel haklarını koruma altına alması gerektiğine yer verilmiştir. UYAR, Lema, *Birleşmiş Milletler'de İnsan Hakları Yorumları İnsan Hakları Komitesi ve Ekonomik, Sosyal ve Kültürel Haklar Komitesi, 1981-2006, İnsan Hakları Hukuku Çalışmaları*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2006, s. 36. (Çevrimiçi erişim: http://insanhaklarimerkezi.bilgi.edu.tr/media/uploads/2016/05/05/BMde_Insan_Haklari_Yorumlar_i_1981_2006.pdf)

²⁶⁶ BYGRAVE, Lee A., “Data Protection Pursuant to the Right to Privacy in Human Rights Treaties”, *International Journal of Law and Information Technology*, C. 6, S. 3, 1998, s. 2.

²⁶⁷ Orijinal metin için bkz. <http://www.refworld.org/pdfid/3ddcafaac.pdf> (29.01.2018).

²⁶⁸ ÜNSAL, Çağrı Zeybek, “Google’ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu Ve Avrupa Birliği’nin 95/46/Ec Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi”, *Hacettepe Üniversitesi Hukuk Fakültesi Dergisi*, C. 3, S. 1, 2013, s. 105.

değerlere bağlı kalarak sosyal ve ekonomik ilerlemeyi geliştirmek üzere Avrupa devletleri işbirliğiyle kurulmuş milletler arası bir kuruluştur.²⁶⁹ İnsan hakları ve temel özgürlüklerin korunması amacı ekseninde faaliyet gösteren Konsey'in, 4 Kasım 1950 tarihi itibarıyla Avrupa İnsan Hakları Sözleşmesi'ni kabul etmesi, insan hakları ve kişisel verilerin korunması alanlarının Avrupa hukukundaki önemini ve gelişimini önemli derecede artırmıştır.²⁷⁰ Özellikle, Türkiye'nin de 1987'de tanımış olduğu, Avrupa İnsan Hakları Sözleşmesi'nin koruma altına aldığı temel hak ve özgürlüklerin herhangi birinin ihlali sebebiyle Avrupa İnsan Hakları Mahkemesi'ne bireysel başvuru yoluyla, özel yaşam hakkını koruma altına alan 8. madde kapsamında verilmiş kişisel verilerin korunmasına ilişkin çok önemli kararlar bulunmaktadır.

AİHM'in geliştirdiği veri koruma hukukunun kapsamı ve özel yaşam hakkıyla olan yakınlığı eksenindeki içtihatların, veri koruma hukuku bakımından sağladığı korumanın sınırlı kalacağı düşüncesiyle²⁷¹ Avrupa Konseyi bünyesinde 1981 yılında imzaya açılan 108 Sayılı *Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında/Karşısında Gerçek Kişilerin Korunmasına İlişkin Sözleşme*, münhasır bazı alanlara yönelik olarak oluşturulan Avrupa Konseyi Bakanlar Komitesi Kararları²⁷² ve Avrupa Konseyi Bakanlar Komitesi Tavsiye Kararlar²⁷³ gibi kişisel verilerin korunmasına yönelik daha kapsamlı düzenlemeler oluşturulmaya çalışılmıştır. Avrupa Konseyi Tavsiye Kararları ile, sürekli gelişen ve değişen kişisel veri koruma alanının güncel sorunlarına karşı 108 Sayılı Sözleşme'nin yetersiz kaldığı hususlara ilişkin üye devletlere yol gösterici ve açıklayıcı çözüm önerileri getirilmesi amaçlanmıştır.

²⁶⁹ Avrupa Konseyi 1949 yılında 10 Avrupa ülkesinin kuruculuğuyla oluşturulmuş ve Türkiye statü metnini 1950 yılında kabul etmiştir. Avrupa Konseyi Statüsü Türkçe orijinal metni için bkz. http://uhdigm.adalet.gov.tr/sozlesmeler/coktarafli/soz/ak/turkce/001_tur.pdf (30.01.2018).

²⁷⁰ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 19.

²⁷¹ KÜZECİ, *Kişisel Verilerin Korunması*, s. 143.

²⁷² 108 Sayılı *Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında/Karşısında Gerçek Kişilerin Korunmasına İlişkin Sözleşme*'nin hazırlanmasında da önemli derece etkisi bulunan ve üye devletler bakımından bağlayıcı olan Avrupa Konseyi Bakanlar Komitesi'nin en önemli iki kararı olarak; "Özel Sektörde Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar" ve "Kamu Sektöründe Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına İlişkin Karar" gösterilebilir. ATAĞ, Songül, "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", *Türkiye Barolar Birliği Dergisi*, S.87, 2010, s. 100.

²⁷³ Örneğin; İşçi Verilerinin Korunmasına İlişkin Konsey Tavsiyesi; Kamu Sektöründe Otomatik Veri Bankaları Karşısında Bireylerin Mahremiyetinin Korunması İlke Kararı Res. (74) 29; Kişisel Verilerin Profil Çıkarma Bağlamında Otomatik İşlenmesi Karşısında Bireylerin Korunması Bakanlar Komitesi Tavsiye Kararı Rec. (2010) 13; Sigortacılık Amacıyla Kişisel Verilerin Toplanması ve İşlenmesi Hakkında Bakanlar Komitesi Tavsiye Kararı Rec. (2002) 9. <https://wcd.coe.int/rst/common/index.jsp> (21.02.2018).

1. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında/Karşısında Gerçek Kişilerin Korunmasına İlişkin Sözleşme

Kişisel verilerin, gelişen teknolojinin etkisiyle ve bu gelişime eşdeğer hızla kullanımının yaygınlaşması, sınır aşan trafiğinin artması ve verilerin kontrolünün zorlaşması Konsey bünyesinde verilerin münhasıran otomatik işleme tabi tutulması karşısında kişilerin korunması alanının özel düzenleme konusu yapılmasını gerektirmiştir.²⁷⁴ Bu doğrultuda hazırlanan 108 Sayılı Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında/Karşısında Gerçek Kişilerin Korunmasına İlişkin Sözleşme, 29.01.1981 tarihinde Avrupa Konsey'i üyesi olan ve sözleşmeye taraf olma iradesi gösteren Konsey dışındaki devletlerin²⁷⁵ imzasına açılmıştır.²⁷⁶

Türkiye her ne kadar 108 sayılı Sözleşmeye ve ek protokollere imzaya açıldığı tarihler itibarıyla taraf olma iradesini göstermişse de, uzun süre onay işlemlerini tamamlayıp Sözleşme'yi yürürlüğe koyamamış tek devlet olmuştur.²⁷⁷ Sözleşmenin “taraf devletlerin görevleri” madde başlığı altında 4. maddesi ile öngörmüş olduğu; taraf devletlerin iç hukuklarında, en geç sözleşmenin kendileri bakımından yürürlüğe girdiği tarihe kadar, verilerin korunmasına ilişkin bu sözleşmenin koruma altına aldığı temel ilkelere işlerlik kazandıracak gerekli tedbirlerin alınması ve düzenlemelerin yapılması yükümlülüğünün yerine getirilememiş olması bu durumun temel gerekçesi olarak gösterilmiştir. Ancak kişisel verilerin korunmasına ilişkin ulusal mevzuat oluşturma çabalarımızla eşdeğer yürütülen onaylama süreci 6669 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile 30.01.2016

²⁷⁴ MENDOS KUŞKONMAZ, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, s. 48.

²⁷⁵ Sözleşmenin etki alanını geniş tutulması amacı doğrultusunda Konsey üyesi olmayan devletlerin de Sözleşme'nin 23. maddesi ile sözleşmeye katılmaya davet edilebileceği düzenlenmiştir. ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 22.

²⁷⁶ 2001 yılında bu sözleşmeye ek; taraf devletlerin 108 Sayılı Avrupa Konseyi Sözleşmesi ile öngörülen yükümlülüklerini yerine getirip getirmediğini ve iç hukukta verilerin korunmasına ilişkin aldıkları önlemlerinin Sözleşme ve Protokol ile öngörülen ilkelere ve koruma seviyesine uyumlu olup olmadığını denetlemek üzere bağımsız kontrol organları oluşturulmasını öngören Protokol yayınlanmıştır. 2004 yılında yürürlüğe giren 181 sayılı Ek Protokol TBMM bu Protokolü 8 Kasım 2001 tarihinde imzalamıştır ve Protokol, 5 Mayıs 2016 tarihli 29703 sayılı Resmi Gazete'de yayımlanmış ve yürürlük kazanmıştır. 108 Sayılı Avrupa Konseyi Sözleşmesi'nin Türkçe orijinal metni için bkz. <http://www.resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf> (30.01.2018); Ek Protokol orijinal metni için bkz. <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626> (30.01.2018).; Türkiye bu Sözleşmeye taraf olmakla ve sözleşmeye uygun verilerin ulusal düzeyde korunmasına ilişkin asgari standardı sağlayarak aynı zamanda Europol Anlaşması'nın verilerin korunmasına ilişkin akit devletlerden aradığı bir koşulu da yerine getirmiş olacaktır. Europol Anlaşması md. 13-25 <http://www.interpol.pol.tr> (07.02.2018).

²⁷⁷ Bu Sözleşme Türkiye tarafından 28.01.1981 tarihinde imzalanmış, 17 Mart 2016 tarihinde yürürlük kazanmıştır.

tarihinde tamamlanmış ve Sözleşme 17 Mart 2016 tarihli ve 29656 sayılı Resmi Gazete’de yayımlanarak aynı tarihte ülkemizde yürürlüğe girmiştir.²⁷⁸ 108 Sayılı Sözleşme’nin ilgili maddesinin doğrudan çıkarımı olarak şunu söyleyebiliriz ki akit devletlerin, Sözleşme hükümlerini kendi iç hukuklarına aktarma yükümlülükleri mevcuttur.²⁷⁹ Ancak devletlere, bu aktarımı belli çekinceler koyarak²⁸⁰ ve Sözleşme ile öngörülen koruma seviyesinden daha fazla koruma sağlayacak şekilde genişletici düzenlemeler yaparak gerçekleştirebilme imkanı tanınmıştır.²⁸¹

Sözleşme’nin 1. maddesi ile konu ve amacı; taraf devletler nezdinde, uyruğu ve ikametine bakılmaksızın her gerçek kişinin temel hak ve özgürlüklerinin münhasıran kişisel verilerinin otomatik işleme tabi tutulması karşısında, özel hayata saygı hakkının korunması olarak düzenlenmiştir. Öz olarak verilerin korunması amacı taşıdığını söyleyebileceğimiz 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşme’si gerçek kişilere mahsus verilerin nispeten daha dar bir koruma alanı da yaratarak sadece otomatik sistemler vasıtasıyla işlenmeleri karşısında korumasını güvence altına alan, kamu ve özel sektör için bağlayıcılığı bulunan ilk uluslararası sözleşmedir.²⁸² Sözleşmenin temel amaçları arasında; taraf devletler arasında veri akışının serbestliğinin sağlanması ve ulusal düzenlemelerin uyumlu hale getirilmesi yer almaktadır. Sözleşmenin taraf devlerin iç hukuklarında kişisel verilerin korunması düzenlemelerinin uyumlaştırılmasına yönelik amacı, sözleşmenin imzaya açıldığı tarihten 8 yıl sonra yalnızca 8 üye devletin sözleşmeye taraf olduğunu ve bu devletlerin ulusal veri korunma düzenlemeleri

²⁷⁸ Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Gerekçesi için bkz. <http://www2.tbmm.gov.tr/d24/1/1-0966.pdf> (30.01.2018).

²⁷⁹ Sözleşme hükümlerinin taraf devletlerin iç hukuklarında doğrudan uygulanabilir olmadığı, iç hukukta uygulanabilmesi için bir uygulama kanunu ile hükümlerin detaylandırılması ve ülke koşulları için uygulanabilir hale getirilmesi gerektiğine ilişkin olarak bkz. AKILLIOĞLU, Tekin, "İdari Usul ve Kişisel Verilerin Korunması", s.3. www.idare.gen.tr/akillioğlu-idariusul.htm (30.01.2018).

²⁸⁰ Sözleşmenin onaylanması aşamasında Türkiye Hükümeti, Sözleşme hükümlerinin, yalnızca verilerin otomatik yollarla değil otomatik olmayan yollarla işlenmesi halinde de uygulanacağı ve “ *gerçek kişilerin tamamen şahsi veya aynı konutta yaşayanlarla ilgili faaliyetlerine ilişkin işlemesi, *kanun tarafından öngörülen kamu kayıtları, *kanuna uygun olarak kamu bilgisine sunulan bilgilere, *devlet kurumlarınca milli güvenlik, savunma ile soruşturma ve suç önleme amacıyla işlenen” veri türleri bakımından uygulanmayacağı yönünde beyanlarını dile getirmiştir. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Avrupa Konseyi Sözleşmesi (ETS 108) İle İlgili Beyanlar için bkz. <http://www2.tbmm.gov.tr/d24/1/1-0966.pdf> (30.01.2018).

²⁸¹ 108 Sayılı Sözleşme md. 3/2 a. , 11., 10.; ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 23.

²⁸² KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 144.; ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 22.; AKILLIOĞLU, "İdari Usul ve Kişisel Verilerin Korunması", s. 2.

arasındaki anlamlı farklılıklar bulunduğunu nazara alınarak denilebilir ki; tam olarak gerçekleştirilememiştir.²⁸³ Ancak sözleşmenin etkinliğine yöneltilen bu eleştirilere karşı, taraf olabilme iradesi gösteren her devletin katılımına açık oluşu ve bu devletleri bağlayıcılığının bulunması gibi sözleşmeyi halen güncel ve önemli kılan özelliklerinin mevcudiyeti de göz ardı edilmemelidir.²⁸⁴

2. AİHS 8. Madde Kapsamında Koruma

Avrupa İnsan Hakları Sözleşmesi, 1950’de Avrupa’da temel özgürlükler ve insan haklarını korumak üzere Avrupa Konseyi tarafından kabul edilmesinin ve 1953 yılı itibarıyla yürürlük kazanmasının ardından,²⁸⁵ 18.05.1954 tarihinde ülkemizde de onaylanma süreci tamamlanarak yürürlüğe girmiştir.²⁸⁶ Temel insan hakları ve özgürlüklerinin güvence altına alındığı bu Sözleşme’nin 8. maddesi düzenlemesine “özel yaşamın gizliliği ve korunması” konu edinilmiştir. Avrupa İnsan Hakları Sözleşmesi’nin iki bölümden oluşan 8. maddesinin ilk bölümünde; kişinin özel yaşamı, aile yaşamı, konutu ve haberleşme özgürlüğü gibi hakları teminat altına alınmıştır. Düzenlemenin ikinci bölümü ise, ilk fıkrada koruma altına alınan temel haklara yönelik müdahalelerin hangi durumlarda yasal kabul edilebileceğine ilişkin koşullara yer verilmiştir.²⁸⁷ Bu düzenlemeye göre; temel bir insan hakkı olarak özel yaşamın gizliliğine yönelik kamusal müdahaleler ancak; ulusal güvenlik, kamu güvenliği veya ülkenin ekonomik refahı, suç işlenmesinin önlenmesi, genel ahlak ve sağlığın korunması ya da başkalarının hak ve özgürlüklerinin korunması amaçlarıyla, demokratik toplumun gerektirdiği ölçüde ve yasayla gerçekleştirilmiş olması halinde meşru kabul edilebilecektir.²⁸⁸ Dolayısıyla Avrupa İnsan Hakları Mahkemesi’nin özel yaşamın korunması hakkının özel bir görünüm biçimi olarak kabul ettiği kişisel verilerin korunması hakkına yönelik müdahaleler de, ancak özel yaşamın gizliliği hakkının sınırlandırılmasına ilişkin koşullara yer veren 8. maddenin 2. fıkrasına göre

²⁸³ LYNSKEY, *The Foundations of EU Data Protection Law*, s. 48.

²⁸⁴ KÜZECİ, *Kişisel Verilerin Korunması*, s. 142.

²⁸⁵ Metnin tam adı “İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi” dir. Britannica Ansiklopedisi, <https://www.britannica.com>. (12.08.2017)

²⁸⁶ Sözleşmenin Türkçe orijinal metni için bkz. http://www.echr.coe.int/Documents/Convention_TUR.pdf (30.01.2018)

²⁸⁷ KİLKELLY, Ursula, *Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı (Avrupa İnsan Hakları Sözleşmesi’nin 8. Maddesinin Uygulanmasına İlişkin Klavuz)*, İnsan Hakları El Kitapları No. 1, Strasbourg, 2011, s. 4.

²⁸⁸ Avrupa İnsan Hakları Sözleşmesi md. 8.

gerçekleştirilmiş olması halinde AİHS'ne uygun kabul edilebilecek ve özel yaşam hakkına yönelik bir ihlal oluşturmayacaktır.²⁸⁹

Avrupa İnsan Hakları Sözleşmesi'nin uygulamasını denetlemekle mükellef yargısal organ olarak 1959 yılında kurulmuş olan Avrupa İnsan Hakları Mahkemesi; kişisel verilerin korunması hakkını, 8. madde teminat altına alınmış olan kişinin özel yaşamının mahremiyetinin korunması hakkını ilgilendiren bir husus olarak kabul etmiş ve bu istikamette verilerin korunmasıyla ilgili önemli kararlar vermiştir.²⁹⁰ Bu doğrultuda AİHM, Avrupa Konseyi ve Konsey kapsamındaki devletler nezdinde anayasa niteliğinde görülebilecek olan İnsan Hakları Avrupa Sözleşmesi'nin 8. maddesinin “özel hayatın gizliliği” alanı için sağladığı koruma kapsamında geliştirdiği içtihatlar doğrultusunda kişisel verilerin korunmasını da güvence altına almıştır.²⁹¹ Mahkeme'nin özellikle özel yaşamı ilgilendiren kişisel veriler olarak cinsiyet, yaş, parmak izi, DNA, fotoğraf vb. kişisel bilgilerini içeren nüfus sayımı²⁹²; polis kayıtları²⁹³ ve tıbbi kayıtlarının²⁹⁴ bireyin rızası olmaksızın tutulmasını veya herhangi bir surette işlenmesini özel yaşam hakkına yönelik yasa dışı müdahale olarak kabul ettiği ve bu istikamette verdiği kararları önemli kabul edilmektedir.²⁹⁵ Kişisel verilerin korunmasının, özel bir hükümle ayrı bir hak olarak düzenlenmemiş olması dolayısıyla oluşan boşluğu dolduracak şekilde ve 8. maddeye dayanarak, Mahkeme'nin esnek ve

²⁸⁹ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 31.

²⁹⁰ AİHM Rotaru-Romanya Davası, No: 28341/95; T: 04.05.2000; “Mahkeme, başvurunun siyasi faaliyetleri, polis tarafından gerçekleştirilen sorgu tutanakları, sabıka kaydı gibi bilgilerin gizli bir sicilde saklanması ve bu tür bilgilerin açıklanmasının 8. maddenin 1. fıkrasının kapsamına girdiğini, ayrıca iddia edildiği üzere bu bilgilerin kamuya açık faaliyetler veya siciller doğrultusunda tutulmuş olsa da kamuya açık bilgiler, düzenli olarak toplandığında ve yetkili makamlar tarafında dosyalarda saklandığında da özel hayat kapsamına girebilir olduğunu kabul etmektedir. Bu durum, özellikle söz konusu bilgiler kişinin geçmişine ilişkinse daha da geçerlidir. Bu bilgilerin bir kısmı elli yıldan uzun bir süre önce toplanmış olan, başvurunun hayatıyla ve özellikle eğitimi, siyasi faaliyetleri ve sabıka kaydıyla ilgili bazı bilgiler olduğuna dikkat çekmiştir. Mahkeme'nin görüşüne göre, bu tür bilgiler düzenli olarak toplandığında ve Devlet'in yetkilileri tarafından dosyada saklandığında, AİHS'nin 8. Madde 1. fıkrası açısından “özel hayat” kapsamına girmektedir. Özellikle bu davada, bilgilerin bir kısmı yanlış olduğu ve başvurunun itibarını zedeleyebileceği için, bu durum daha da geçerlidir.”

²⁹¹ MENDOS KUŞKONMAZ, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, s. 48.; “Avrupa İnsan Hakları Sözleşmesi'nde (AİHS) açık bir şekilde düzenlenmemekle birlikte, Sözleşme'nin uygulanmasına ilişkin Avrupa İnsan Hakları Mahkemesi (AİHM) kararlarında Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme'ye atıfta bulunulmakta ve bu verilerin özel yaşamın gizliliğinin bir parçası olduğu kabul edilmektedir.” Anayasa Mahkemesi E: 2015/32, K: 2015/102, T: 12.11.2015

²⁹² X- B. Krallık Davası, No: 9072/82, T: 06.10.1982,

²⁹³ Leander - İsviçre Kararı, No: 9248/81, Tarih: 26.03.1987; Murray - B. Krallık Davası, No: 14310/88, T: 28.11.1994; Shimovolos - Rusya Davası, No: 30194/09, Tarih: 21.07.2011.

²⁹⁴ Z.- Finlandiya Kararı, No: 22009/93, T: 25.02.1997; M.S.- İsveç Kararı, No: 20837/97, T: 27.08.1997

²⁹⁵ KİLKELLY, Ursula, s. 11-12.;

kapsamlı kararlar vermesi verilerin korunması alanında Avrupa ülkeleri için yol gösterici içtihatların oluşmasını sağlamıştır.²⁹⁶

D. Avrupa Birliği Dahilinde Kişisel Verilerin Korunması

Öncelikli hedef olarak ekonomik işbirliğinin artırılmasını benimsemiş olan Avrupa Birliği, 1958 yılında 6 Avrupa ülkesinin bir araya gelmesiyle oluşturulmuş uluslararası bir organizasyondur. Dahası Avrupa Birliği, halen hemen her kıtadan 28 üyesi olan, birincil hukuk olarak uygulan pek çok kurucu anlaşmasında, özellikle Lizbon Anlaşması ve Avrupa Birliği Temel Haklar Şartında, temellerini bulan insan onuru, özgürlük, demokrasi, eşitlik, hukuk devleti ve insan hakları gibi değerleri benimsemiş yegane politik ve ekonomik bir birliktir.²⁹⁷ Avrupa Birliği bünyesinde, devletlerin ortak ekonomik gerekçelerle kişisel verilerin sınır aşan transferine ilişkin taleplerinin artmasıyla, kişisel verilerin korunması alanında ulusal düzenlemelerin üzerinde yeknesak ve ortak bir düzenleme oluşturma ihtiyacı doğmuştur.²⁹⁸

Bu doğrultuda Avrupa Birliği Adalet Divanı tarafından alınan veri koruma hususuna ilişkin artan hacimli kararlarının ulusal veri koruma sistemlerinin entegrasyonuna olan iyileştirici etkisinin yanı sıra, Avrupa Birliğinin Lizbon Anlaşması'nı kabulüyle birlik bünyesinde kişisel verilerin işlenmesinin yasal rejimine dair önemli değişiklikler de vuku bulmuştur.²⁹⁹ Avrupa Birliği Temel Haklar Şartı 8. maddesiyle verilerin korunmasını, özel yaşam hakkını düzenlediği 7. maddesine ek ayrı bir hak olarak düzemekte iken³⁰⁰, Avrupa Birliği İşleyişi Hakkındaki Anlaşma'nın 16. maddesi ile de veri koruma mevzuatını oluşturmak için belli bir yasal temel yaratılmıştır.³⁰¹ Bütün bu düzenlemeler ekseninde görmekteyiz ki; Avrupa Birliği'nin veri koruma hukuku bakımından tutumu, “enformasyonel self determinasyon” hakkının da kaynaklık ettiği doğrultuda önleyicilikten yana olmuştur. Kişilerin kişisel

²⁹⁶ BYGRAVE, “Data Protection Pursuant to the Right to Privacy in Human Rights Treaties”, s. 6.; KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 153.; ATAĞ, “Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler”, s. 120.

²⁹⁷ Avrupa Birliği Resmi İnternet sayfası, https://europa.eu/european-union/about-eu/eu-in-brief_en

²⁹⁸ BAŞALP, *Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları*, Ankara, 2004, s. 27.

²⁹⁹ LYNKEY, *The Foundations of EU Data Protection Law*, s. 7.

³⁰⁰ Sözleşmenin orijinal metni için bkz. Charter Of Fundamental Rights Of The European Union, http://www.europarl.europa.eu/charter/pdf/text_en.pdf (31.01.2018)

³⁰¹ Sözleşmenin orijinal metni için bkz. Consolidated Version Of The Treaty On The Functioning Of The European Union (TFEU) <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT> (31.01.2018)

verilerinin hangi koşullar altında, kimler tarafından, ne kadar süreyle işleneceğine ilişkin önceden bilgi edinebilmesi ve karar verebilmesi, kısacası verilerinin geleceğini belirleme konusundaki irade serbestisiyle sağlanabilecek olan önleyicilik ancak ihlalden önce oluşturulmuş sistemli bir koruma ile mümkün olabilecektir.³⁰²

Avrupa Birliği bünyesinde kişisel verilerin korunması, temel metinlerdeki koruyucu hükümlerin yanı sıra, direktifler ve son dönemde de Genel Veri Koruma Regülasyonu'yla özel olarak düzenlenmiştir. Çalışma kapsamında; veri koruma hukuku bakımından Avrupa Birliği bünyesinde ve dışındaki ulusal ve uluslararası düzenlemelerin oluşturulmasında önemli etki ve katkıları bulunan 95/46 sayılı “Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi”, 2002/58/AT Özel Yaşamın ve Elektronik İletişimin Korunması Direktifi, 2016/680 Kişisel Verilerin Cezai Prosedür Gereği İşlenmesi Karşısında Gerçek Kişilerin Korunması Direktifi ve 2016/679 Sayılı Avrupa Birliği Veri Koruma Regülasyonu inceleme konusu yapılmaya çalışılmıştır.

1. Avrupa Birliği Temel Haklar Şartı

Avrupa Konseyi ve Parlamentosu'nun kişisel verilerin korunması alanına yönelik düzenlemiş olduğu 95/46/AT ve 97/66/AT nolu Direktif'lerinin yürürlüğe konulması sürecini takiben, 2000 yılında Avrupa Birliği Temel Hak ve Hürriyetler Şartı 8. maddesinde “kişisel bilgilerin korunması” başlığı altında kişisel verilerin korunması bağımsız bir temel hak ve hürriyet olarak düzenlenmiş ve bu metin 2009 yılında Lizbon Anlaşması'nın hukuki bağlayıcılık kazanmasıyla yürürlüğe girmiştir.³⁰³ ABTHŞ 8. maddesine göre; “(1) Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.(2) Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.(3) Bu kurallara uyulması,

³⁰² BAŞALP, Kişisel Verilerin Korunması ve Saklanması, s. 31.

³⁰³ Avrupa Birliği Temel Haklar Şartı (kısaca ABTHŞ olarak anılacaktır) orijinal metin için bkz. http://www.europarl.europa.eu/charter/pdf/text_en.pdf (07.02.2018); Lizbon Anlaşması 6. maddesi ile Avrupa Birliği Temel Haklar Şartı'nın Birliğin kurucu sözleşmeleriyle aynı hukuki değere sahip olduğu kabul edilmiştir. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT> (07.02.2016)

bağımsız bir makam tarafından denetlenecektir."³⁰⁴ Bu maddenin hazırlanmasında Avrupa Topluluğu Kurucu Sözleşmesi'nin 286. maddesi, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi, Avrupa Konseyi'nin 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında/Karşısında Gerçek Kişilerin Korunmasına İlişkin Sözleşme'si ve 95/46 sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktif'i esas alınmıştır.³⁰⁵

Temel Haklar Şartı'nın verilerin korunması hakkını, 7. maddesinde garanti edilmiş olan özel yaşamın gizliliği hakkından bağımsız bir temel hak olarak düzenlemiş olması ve Şart'ın bağlayıcılık kazanması ile; Avrupa Birliği kurumları, örgütleri ve üye devletlerine düzenlemeye uygun hareket etme negatif yükümlülüğü yüklenmiş olup, bu yükümlülükler aykırı davranılması halinde de vatandaşlara Avrupa Birliği Adalet Divanı'nda dava hakkını kullanarak verilerini etkin şekilde koruyabilme güvencesi yaratılmıştır.³⁰⁶ Verilerin korunması temel hakkını güvence altına alan Temel Haklar Şartı'nın 6. maddesine yönelik müdahalelerin, ABTHŞ'nin 52. maddesinde düzenlenmiş olan hak ve özgürlüklerin genel sınırlandırılma koşullarına uygun olmaması da üye devletlerin, Adalet Divanı'nca sorumlu tutulmasını gerektirecektir.³⁰⁷ ABTHŞ'nin 52. maddesine göre; temel hak ve özgürlüklerin sınırlandırılması ancak bir kanunla ve temel hak ve özgürlüklerin özüne dokunmaksızın gerçekleştirilebilir. Bunun yanında kişisel verilerin korunması gibi temel hakların sınırlandırılması; ölçülülük ilkesine, kamu yararı veya diğer kişilerin hak ve özgürlüklerinin gereklerine uygun olarak ve ancak gereklilik bulunan hallerde söz konusu olabilir.³⁰⁸

³⁰⁴ Avrupa Birliği Temel Haklar Şartı Türkçe orijinal metin için bkz. <https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708> (14.12.2017)

³⁰⁵ 303/17 Sayılı ve 14.12.2007 Tarihli Avrupa Birliği Resmi Gazetesi, Temel Haklar Şartına İlişkin Açıklamalar, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32007X1214%2801%29> (07.02.2018)

³⁰⁶ Avrupa Topluluğu Adalet Divanı'nın bu doğrultuda verilmiş olduğu önemli kararlar arasında; (C-465/00) Österreichischer Rundfunk ve (C-101/01) Bodil Lindqvist davalarını gösterilebiliriz. <http://curia.europa.eu> (07.02.2018); KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 183.

³⁰⁷ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 74.

³⁰⁸ ABTHŞ md. 52.

2. 95/46/AT Sayılı Avrupa Birliği Veri Koruma Direktifi

24. 10. 1995 tarihli, tam karşılığı “Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi” şeklinde olan, ancak “95/46 sayılı Veri Koruma Direktifi” olarak kısaltılmış şekliyle yaygın şekilde kullanılan, kişisel verilerin korunmasını temel bir insan hakkı olarak açıkça tanıyan düzenleme çalışma genelinde de kısaca “Direktif”³⁰⁹ şekilde anılmıştır. Bu düzenleme, Avrupa Birliği bünyesinde kişisel verilerin korumasına yer veren düzenlemeler arasında, Avrupa Birliği hukukuna veri koruma ilkelerini getirmesi ve Avrupa Birliği’nde kişisel verilerin korunmasının temel ölçütlerini saptaması itibarıyla en önemli olanıdır.³¹⁰ Direktif’in gerekçe kısmında açıkça ortaya konulduğu üzere Direktif’in temel amacı; veri koruması, güvenliği ve verilerin serbest dolaşımı alanlarına³¹¹ yönelik üye devletlerin farklı veri koruması eşikleri belirlemek suretiyle yaratacağı haksız rekabet ve olası ekonomik özgürlük ihlallerinin önüne geçilmesini sağlayacak yeknesak bir düzenleme oluşturulmasıdır.³¹² Direktifle korunmak istenen, birlik bünyesinde ortak pazarın mevcudiyeti, devamlılığı ve süregelen işlerliğidir. Direktif’in 1. maddesinde de bu düzenlenme amacı ve direktifin üye devletleri doğrudan bağlayıcılığı olduğunu hüküm altına alınmıştır.³¹³

Direktif’in üye devletlerden beklediği; gerçek anlamda birebir Direktif’e göre bir düzenleme yapmalarından ziyade, iç hukuklarında yarattıkları korumanın Direktif’de öngörülen asgari standartları sağlayacak ağırlıkta olması ve bu doğrultuda uygulanmasıdır.³¹⁴ Ancak tüm üye devletlerin Direktif’in 5. ve 17. maddeleri arasında düzenlenmiş bulunan temel veri koruma ve işleme ilkeleri doğrultusunda ulusal hukuklarında düzenleme yapmalarıyla birlik bünyesinde yeknesak bir veri koruma

³⁰⁹ Avrupa Birliği hukuku; Avrupa Birliği anlaşmaları ile sağlanmak istene amacı gerçekleştirmek üzere, Avrupa Birliği ülkelerinin tamamı veya bir kısmı için bağlayıcı olabilen veya bağlayıcılığı olmayan, regülasyon, direktif, karar, tavsiye ve görüş gibi hukuki işlemlerden oluşur. Direktif veya diğer bir adıyla yönerge; tüm üye devletlerin düzenleme konusunu belirtilen süreler dahilinde iç hukuklarına aktarma yükümlülüğünü getiren ve bağlayıcılığı olan hukuki nitelikteki düzenlemedir. https://europa.eu/european-union/eu-law/legal-acts_en (16.12.2017).

³¹⁰ GELLERT, Raphaël, GUTWIRTH, Serge, “The legal construction of privacy and data protection”, Computer Law & Security Review, C. 29, S. 5, 2013, s. 523.; ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 49.; KÜZECİ, *Kişisel Verilerin Korunması*, s.127.

³¹¹ EVANS, “European Data Protection Law”, s. 578.

³¹² Direktif Gerekçe md. 7.; Kişisel verilerin korunması alanında uyumlaştırma çabalarının oluşmasında özellikle etkili bir diğer etken olarak “tek iç pazar” düşüncesini gösterilebiliriz. KÜZECİ, *Kişisel Verilerin Korunması*, s. 177.

³¹³ AKSOY, *Kişisel Verilerin Korunması*, s. 7.

³¹⁴ KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 185.

eşiğine ulaşılmış ve veri koruması bakımından yeterlilik sağlanabilmiş olacaktır.³¹⁵ Direktif'in uygulanma alanı ve konuları belli kapsamda daraltılmıştır. Direktif'in uygulama dışında tuttuğu haller; veri sahibinin gerçek kişi dışında bir kişi olması ve işlemenin konusunun gerçek kişilerin sırf ailevi ilişkileri ve faaliyetlerine³¹⁶ veya ulusal güvenlik gibi topluluk hukukunun kapsamına girmeyen konulara³¹⁷ ve birliğin ortak dış ilişkileri ve güvenlik politikası kapsamında yürütülen aktivitelere ilişkin olmasıdır.³¹⁸

Direktif, kişisel verilerin üçüncü ülkeye aktarımını, ancak aktarımın yapılacağı ülkenin aktarım yapılanla eşdeğer veya Direktif'e göre yeterli kabul edilebilecek düzeyde bir veri korunmasını sağlanabilecek olmasına bağlı kılmıştır. Bu koşulu sağlamayan devletlere verilerin transfer edilemeyecek olması sebebiyle Direktif, verilerin serbest dolaşımının engellenmesine yol açtığı şeklinde eleştirilere maruz kalmıştır. Ancak buna rağmen Avrupa devletleri üzerinde etkinliğini ve AB veri koruma mevzuatındaki önemini Avrupa'ya kabullendirebilmiştir.³¹⁹

Bu Direktif'in 29. maddesi ile topluluk düzeyinde faaliyet gösteren, Direktif düzenlemelerinin üye devletlerde yeknesak bir şekilde uygulanmasını sağlama amaçlı; görüş, tavsiye ve danışma kararları vermekle yetkili bir Veri Çalışma Grubu (Article 29 Data Protection Working Party) oluşturulmuştur.³²⁰ Kişisel verilerin korunması alanına yönelik hazırlamış olduğu tavsiye kararları ve önerileri Direktif'in daha iyi ve

³¹⁵ BAŞALP, Nilgün, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara, 2004, s. 31

³¹⁶ Adalet Divanı'nda; ev sahiplerinin, can ve mal güvenliğini sağlamak amacıyla kendi evlerine taktıkları video kaydı yapan kameralarının kamusal alanları da görüntülemekte olması dolayısıyla, bu surette gerçekleştirilen kişisel veri işleminin salt kişisel ve ailevi ilişkilere ilişkin olmadığına ve Direktif'in uygulama alanında yer aldığına karar vermiştir. ATAD, Rynes Davası (Case C-212/13).

³¹⁷ Kamu güvenliği, milli savunma ve güvenlik ve cezai prosedürlere ilişkin devlet faaliyetleri gibi topluluk hukukunun uygulama alanı dışında olan konularda, Direktif'in de uygulanabilirliği bulunmamaktadır. Direktif'in uygulanma alanı dışında tutulan bu istisnai hallerin özellikle Europol ve Schengen Anlaşmaları'nın kişisel verilerin işlenmesine ilişkin hükümleri ile birlikte ele alınmasıyla topluluk bünyesinde hararetli tartışmalar yaşanmıştır. KÜZECİ, *Kişisel Verilerin Korunması*, s. 180-181.

³¹⁸ Direktif Gerekçe md.16.; Bu istisnai haller dışında, topluluğun kendi kurum ve organlarınca kişisel veri işleme faaliyetleri karşısında bireylerin korunması amaçlı düzenlemiş olan 41/2001 Sayılı *Topluluk Organları ve Kurumlarınca Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Karşısında Kişilerin Korunması Regülasyon'u* hükümlerine başvurulması gerekmektedir.

³¹⁹ KÜZECİ, *Kişisel Verilerin Korunması*, s. 186.

³²⁰ Veri Koruma Çalışma Grubu hakkında detaylı bilgi için bkz. http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

doğru anlaşılabilmesini sağlamakta olan Veri Çalışma Grubu, çalışma genelinde de başvurulan önemli bir kaynaktır.

95/46 Sayılı “Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi” pek çok hükmün aynen benimsenerek, belli alanlar ise daha genişletici veya ilk kez düzenlenerek “AB Parlamentosu ve Konseyi’nin 27 Nisan 2016 Tarihli ve 2016/679 Sayılı, 95/46/EC Sayılı Direktifi (Avrupa Birliği Veri Koruma Direktifi) Yürürlükten Kaldıran, Kişisel Verilerin İşlenmesi ve Verilerin Serbest Dolaşımı Karşısında Gerçek Kişilerin Korunmasına İlişkin Regülasyonu” ile yürürlükten kaldırılmıştır.³²¹

3. 2002/58/AT Sayılı Özel Yaşamın ve Elektronik İletişimin Korunması Direktifi

“Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin” 2002/58 Sayılı Avrupa Konseyi Direktifi, kısaca E-Komünikasyon Direktifi, Avrupa Konseyi ve Parlamentosu tarafından verilerin korunmasına ilişkin temel ölçütleri sağlamış olan 95/46 sayılı Direktif’in devamı ve tamamlayıcısı olarak, e-telekomünikasyon sektöründe temel hak ve özgürlüklerin, özellikle Avrupa Birliği Temel Haklar Şartı’nın 7. ve 8. maddesi ile güvence altına alınmış mahremiyet hakkının, korunmasına riayet edilmesi amacıyla 2002 yılında kabul edilmiş bir düzenlemedir.³²² E-Komünikasyon Direktifi, 95/46 Sayılı Genel Veri Koruma Direktif’inden farklı olarak hem gerçek hem de tüzel kişi veri öznesinin, kamusal elektronik haberleşme hizmetlerine konu olan kişisel verilerine ilişkin koruma sağlamaktadır. Bunun yanında kamusal olmayan haberleşme servislerince verilerin işlenmesinde ve verilerin kamusal elektronik haberleşme servislerince işlenmesi sırasında E-Komünikasyon Direktifi’nin özel bir koruma öngörmediği hallerde, veri sorumlusunun yükümlülüklerini ve veri öznesinin haklarını

³²¹ “General Data Protection Regulation” orijinal tam metni için bkz. <https://gdpr-info.eu> (21.01.2018).

³²² “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin” 2002/58 Sayılı Avrupa Konseyi Direktifi Gerekçe md. 2.; Direktif’in orijinal metni için bkz. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML> (04.02.2018); Bu Direktif’in yürürlüğe girmesiyle telekomünikasyon sektörüne münhasır olarak kişisel verilerin işlenmesine ve korunmasına ilişkin 1997 yılında çıkartılmış olan 97/66 sayılı Avrupa Konseyi Telekomünikasyon Veri Koruma Direktif’i feshedilmiş ve 2002/58 Sayılı Direktif bu Direktif’in yerini almıştır.

içeren temel hak ve özgürlüklerin korunmasına ilişkin tüm konularda 95/46 sayılı Veri Koruma Direktifi uygulanacaktır.³²³ E-Komünikasyon Direktifi, özellikle mahremiyet hakkı olmak üzere, kişisel verilerin elektronik iletişim sektöründe işlenmesiyle ilgili olarak, temel hak ve özgürlüklerin korunması için gerekli eşdeğer koruma seviyesinin sağlanmasını ve verilerin, elektronik iletişim donanımlarının ve servislerin Topluluk içerisinde serbest dolaşımının sağlanması için üye devletlerin düzenlemelerinin uyumlaştırılmasını amaç edinmiştir.³²⁴ Bu doğrultuda E-Komünikasyon Direktifi'nin düzenleme konusu olan öncelikli konular arasında; elektronik işlem güvenliği, iletişimin gizliliği, sınırlı veri işleme, çerez veya benzeri veri toplama araçlarının kullanımı, yer bilgilerinin işlenmesi, e- telekomünikasyon verilerinin saklanması yer almaktadır.³²⁵

4. 2016/680 Kişisel Verilerin Cezai Prosedür Gereği İşlenmesi Karşısında Gerçek Kişilerin Korunması Direktifi

“AB Parlamentosu ve Konseyi'nin 27 Nisan 2016 Tarihli ve 2016/680 sayılı Resmi Otoritelerce Cezai Yaptırımların İnfazı veya Ceza Gerektiren Suçların Önlenmesi, Tespiti, Kovuşturulması ve Soruşturulması Amacıyla İşlenmesi ve Bu Verilerin Serbest Dolaşımı Karşısında Gerçek Kişilerin Korunması Direktifi”³²⁶, 2016/679 Sayılı Avrupa Birliği Veri Koruma Regülasyon'u ile aynı tarihte kabul edilmiş³²⁷ ve Avrupa Birliği Resmi Gazetesi'nde yayınladığı 04.05.2016 tarihini takip eden günden itibaren yürürlük kazanmıştır.³²⁸ Bu Direktif gerçek kişilerin kişisel verilerinin, kamusal güvenliğe yönelik tehditlerin önlenmesi ve karşı konulması dahil cezai yaptırımların infazı veya suçun önlenmesi, araştırılması, tespiti ve soruşturulması amaçları doğrultusunda kamusal otoriteler tarafından işlenmesi karşısında korunmasına ilişkin kuralları getirmektedir. Kişisel verilerin kamusal otoriteler

³²³ 2002/58 sayılı Avrupa Konseyi Direktifi Gerekçe md. 10.

³²⁴ 2002/58 sayılı Avrupa Konseyi Direktifi md. 1.

³²⁵ KÜZECİ, *Kişisel Verilerin Korunması*, s. 205-206.

³²⁶ 2016/680 Sayılı Avrupa Parlamentosu ve Konseyi Direktifi orijinal metin için bkz. <http://eur-lex.europa.eu>

³²⁷ Her iki düzenleme de Avrupa Parlamentosu ve Konseyi tarafından 27.04.2016 tarihinde kabul edilmiştir. Regülasyon Gerekçesinin 19. maddesinde açıkça kişisel verilerin; suçların önlenmesi, araştırılması, tespiti veya soruşturulması amaçlarıyla veya cezaların infazı için kamusal makamlarca işlenmesinin özel bir düzenlemeye konu edilmesi gerektiğini, bu Regülasyon hükümlerinin belirtilen amaçlarla verilerin işlenmesi faaliyetlerine uygulanmayacağını vurgulamıştır. Bu doğrultuda uygulanması gereken düzenleme 2016/680 Sayılı Avrupa Parlamentosu ve Konseyi Direktifi'dir.

³²⁸ 2016/680 Sayılı Avrupa Parlamentosu ve Konseyi Direktifi md. 64.

tarafından işlenmekte olması bu Direktif hükümlerinin uygulanabilmesinin ön koşulunu oluşturmaktadır. Bunun dışında verilerin, otomatik veya yarı otomatik yöntemlerle veya bir dosyalama sisteminin parçası olarak/olması niyetiyle otomatik olmayan yollarla işlenmiş olması gerekmektedir.³²⁹ Bu Direktif kapsamında; kişisel verilerin belli, kesin ve yasal amaçlar için toplanması gerekir. Bu istikamette toplanan kişisel veriler, kamusal güvenliğe yönelik tehditlerin önlenmesi ve karşı konulması dahil cezai yaptırımların infazı veya suçun önlenmesi, araştırılması, tespiti ve soruşturulması ile örtüşmeyen amaçlar doğrultusunda işlenmelidir.³³⁰ Üye devletler, bu amaçlarla verileri işlenen şüpheli, sanık veya mağdur gibi farklı kişi gruplarından veri öznelerinin kişisel verileri arasında açık bir ayırıma gitmekle veri sorumlularının eksikliğini gidermelidirler.³³¹

Direktif'in uygulanma alanına ilişkin diğer önemli bir husus; Birlik bünyesinde kişisel verilerin İnterpol veya İnterpol'de temsilcisi bulunan ülkelere transfer edilmiş olması halinde, 2016/679 Sayılı Direktif, özellikle uluslararası transfere ilişkin olan hükümlerinin uygulanacak olmasıdır.³³²

5. 2016/679 Sayılı Avrupa Birliği Veri Koruma Regülasyonu

AB Parlamentosu ve Konseyi'nin 27 Nisan 2016 Tarihli ve 2016/679 Sayılı "95/46/EC Sayılı Direktifi (Avrupa Birliği Veri Koruma Direktifi) Yürürlükten Kaldıran, Kişisel Verilerin İşlenmesi ve Verilerin Serbest Dolaşımı Karşısında Gerçek Kişilerin Korunmasına İlişkin Regülasyonu"³³³ üye devletler bakımından 04.05.2016 tarihli Avrupa Birliği Resmi Gazetesi'nde yayımlanması takip eden 20. günden itibaren yürürlüktedir.³³⁴ Birlik bünyesinde veri koruma hukuku bakımından en etkili düzenleme olarak kabul edilen 95/46 Sayılı Direktif'i yürürlükten kaldıran Regülasyon'un uygulama tarihi olarak ise 25.05.2018 öngörülmüştür.³³⁵ Düzenlemenin yürürlük ve uygulama tarihleri arasındaki bırakılan bu 2 yıllık zaman

³²⁹ 2016/680 Sayılı Avrupa Parlamentosu ve Konseyi Direktifi Direktif md. 2.

³³⁰ 2016/680 Sayılı Avrupa Parlamentosu ve Konseyi Direktifi Gereke md. 29., md. 1/b.

³³¹ 2016/680 Sayılı Avrupa Parlamentosu ve Konseyi Direktifi md. 6.

³³² 2016/680 Sayılı Avrupa Parlamentosu ve Konseyi Direktifi Gereke md. 25.

³³³ Yaygın kısaltılmış şekliyle "GDPR(General Data Protection Regulation)" Genel Veri Koruma Regülasyonu orijinal metin için bkz. <http://eur-lex.europa.eu>.

³³⁴ 2016/679 Sayılı Genel Veri Koruma Regülasyonu'nun 25.05.2016 yürürlük tarihidir.

³³⁵ 2016/679 Sayılı Genel Veri Koruma Regülasyonu md. 99.

dilimi içerisinde, Birlik bünyesinde tüm veri işlemlerinin bu düzenlemeyle uyumlu hale getirilmesi gerekmektedir.³³⁶

Avrupa Birliği tarihinde, kişisel verilerin korunmasına yönelik bu düzenleme girişimine kadar, Komisyon'un böylesine geniş ve kapsamlı konuyu tek bir bağlayıcı metinle düzenlemiş olduğu bir düzenleme örneği bulunmamaktadır.³³⁷ Bu durum her ne kadar verilerin korunması alanında tüm Avrupa Birliği üyeleri bakımından doğrudan icra edilebilir tek bir bağlayıcı düzenlemenin uygulanabilmesinin ne derece zor olabileceğine yönelik bir eleştiri olarak ileri sürülmekteyse de, git gide veriye dayalı bir dünyaya dönüşen günümüz koşullarında kişisel verilerin korunması alanının böyle bir düzenlemeyle ele alınmasının çeşitli makul gerekçeleri de bulunmaktadır. 95/46 Sayılı Veri Koruma Direktif'i ile temel prensipleri belirlenmiş ve yerleşmiş olan veri koruma hukukunun, bu prensiplere bağlı kalınarak ancak Direktif'in eksik veya yetersiz kaldığı bazı alanlarda oluşan belirsizlikler ve uygulama farklılıkları giderilmek üzere yeniden düzenlenmesi ihtiyacı Avrupa Komisyon'unu Regülasyon'nu oluşturulmaya iten en etkin gerekçedir.³³⁸ Örneğin; 95/46 Sayılı Direktif'in sessiz kaldığı hayatta olmayan kişilerle ilişkili verilerin kişisel veri olarak kabul edilip edilemeyeceği konusu, üye ülkeler tarafından farklı şekilde değerlendirilerek uygulama farklılıklarına sebep olmuştur. Regülasyon'un uygulama kazanmasıyla bu benzeri konulardaki eksiklikler giderilmiş ve uygulama farklılıkları da ortadan kaldırılmış olacaktır.

Bunun dışında, farklı devletlerde yer alan orta, küçük veya mikro ölçekli ekonomik aktörler bakımından kişisel verilerin korunmasına ilişkin yasal kesinliğin ve şeffaflığın sağlanması; veri sorumluları, veri işlemecileri ve veri özneleri için tüm üye devletlerde aynı seviyede yasal yaptırım olan hak ve yükümlülüklerin sağlanması; eşdeğer yaptırım ve veri işleminin tutarlı denetiminin sağlanması için gerekli olan

³³⁶ 2016/679 Sayılı Genel Veri Koruma Regülasyonu Gerekçe md. 171. Özellikle veri öznesinin rızasına dayalı bir veri işleme söz konusuysa; Regülasyon'un uygulama tarihinden sonrada, veri sorumlusunun daha önce verilmiş olan rızaya dayalı olarak verileri işleyebilmesi ancak bu düzenlemenin koşullarına uygun şekilde rızanın temin edilmiş olmasına bağlıdır. Veri öznesinin Regülasyon'un uygulama tarihi öncesinde verdiği rıza, hukuka uygun veri işleme için Regülasyon'un aradığı rızaya ilişkin koşulları sağlamaktaysa veri sorumlusunun tekrar rıza almasına gerek olmadan işlemeye devam edebilmesi mümkündür.

³³⁷ DE HERT, Paul, PPAKONSTANTİNOU, Vagelis, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals", Computer Law&Security Review, C. 28, 2012, s. 142

³³⁸ 2016/679 Sayılı Genel Veri Koruma Regülasyonu Gerekçe md. 9.

farklı ülke denetim organları³³⁹ arasında etkili işbirliğinin kurulması ihtiyaçlarını karşılama amaçları da bu Genel Veri Koruma Regülasyon'u oluşturulmasına ilişkin önemli gerekçelerdendir.³⁴⁰ Bu doğrultuda, kişisel verilerin tutarlı ve ileri düzeyde korunmasının sağlanabilmesi³⁴¹ ve Birlik bünyesinde verilerin transferi karşısındaki engellerin ortadan kaldırılarak, iç piyasada kişisel verilerin serbest dolaşımının sağlanabilmesi ancak tüm üye devletlerde kişisel verilerin işlenmesi karşısında, gerçek kişilerin temel hak ve özgürlüklerinin korunmasının eşit seviyede olmasına bağlıdır. Ancak; kişisel verilerin korunmasına ilişkin Regülasyon'un sağlamış olduğu korumadan daha ileri bir koruma seviyesi sağlayan ulusal düzenlemelerin oluşturabilmesi veya hassas veriler gibi belli veri gruplarıyla ilgili olarak bu düzenleme hükümlerini özelleştirebilmesi yönünde üye devletlerin iradelerine de geçerlilik tanınmıştır. Bu sebepten Regülasyon'un ulusal düzenlemeleri tamamıyla dışladığını söylemek doğru olmayacaktır.³⁴²

2016/679 Sayılı Genel Veri Koruma Regülasyon'unun temel oluşturulma gerekçesinin ve sağlamak istediğinin bu aşamaya kadar yaptığımız açıklamalar doğrultusunda; en genel anlamda AB'nin "tek kıta, tek kanun" iradesi³⁴³ ekseninde hem şirketler hemde kişiler bakımından doğrudan uygulanabilirliği bulunan yeknesak bir veri koruma mevzuatının oluşturulması olduğu söylenebilir.³⁴⁴ Bu düzenleme, 95/46 Sayılı Direktif'de yer alan temel veri koruma ilkelerinin önemli bir kısmını aynen benimsemişken, Regülasyon'un veri koruma hukuku bakımından oldukça önemli bazı alanları ise ilk defa düzenlenmiş olduğunu görmekteyiz.³⁴⁵ Bu alanların

³³⁹ Bunun yanında birlik bünyesinde ulusal veri koruması denetim otoritelerinin başkanları ve AB Veri Koruması Denetçisi'nden oluşturulacak, birden fazla AB üyesi ülkede veri ihlali oluşturabilecek hallerde yetkili kabul edilen ve halihazırda mevcut Art. 29. Çalışma Grubu'nun yerine geçecek olan "Avrupa Birliği Veri Koruması Kurulu" (European Data Protection Board) ile yeknesak bir hukuk uygulamasının yaratılması amaçlanmaktadır. BAŞALP, Nilgün, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 21, S. 1, 2015, s. 86.

³⁴⁰ 2016/679 Sayılı Genel Veri Koruma Regülasyonu Gerekçe md. 13.

³⁴¹ VOIGT, Paul, *The EU General Data Protection Regulation (GDPR) A Practical Guide*, Springer International Publishing A.G., İsviçre, 2017, s.1.

³⁴² 2016/679 Sayılı Genel Veri Koruma Regülasyonu Gerekçe md. 10.

³⁴³ BAŞALP, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", s. 86.

³⁴⁴ AB hukukuna göre; bir direktif, diğer adıyla yönergenin düzenlenme amacı doğrultusunda, üye devletlerin ulusal düzenlemelerini kendi takdir ettikleri yol veya yöntemlerle gerçekleştirebilmeleri mümkün olabilmektedir. Ancak bir tüzük veya regülasyon yürürlüğe girmekle, üye devletlerin iç hukukun bir parçası haline gelir ve doğrudan uygulanabilirlik ve bağlayıcılık kazanırlar. AKINCI, Ayşe Nur, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi", Çalışma Raporu, T.C. Kalkınma Bakanlığı Yayınları, 2017, s. 14.

³⁴⁵ Bu çalışmamızın, genel veri koruma kavram ve ilkelerine ilişkin açıklamalarının, daha ziyade güncelliği bulunan bu düzenleme esas alınarak ve mümkün mertebede diğer uluslararası ve ulusal düzenlemelerle mukayese edilerek yapılmaya çalışılmış olduğunun altını çizmek isteriz.

başında; 95/46 Sayılı Direktif'in sessiz kaldığı bir husus olan ölü kişilere ait kişisel verilerin, Regülasyon'un sağladığı koruma alanının dışında olduğunu tespit eden ve bu alanı belirsizlikten kurtaran düzenlemesini gösterebiliriz. Regülasyon'un 27. madde numaralı gerekçesi açıkça rahmetli olmuş kişilerin kişisel verilerine bu Regülasyon'un hükümlerinin uygulanmayacağını belirtmişken, üye devletlere bu verilerin işlenmesi karşısında koruma sağlayan kuralları sağlayabilme inisiyatifi de tanınmıştır.³⁴⁶ Bu durum Direktif'in belirsiz bıraktığı bir alan olduğu için konuya ilişkin farklı ülke uygulamalarına rastlanabilmekteydi.³⁴⁷ Benzer şekilde Direktif'in düzenlemeyi ihmal ettiği bir konu olarak, kişisel verilerin işlenmesine ilişkin çocuğun rızasının kabul edilebilirliği gösterilebilir. Regülasyon'un 8. maddesine göre; bilgi toplumu servisleri tarafından doğrudan çocuğa yöneltilmiş olan verilerinin işlenmesine ilişkin rıza teklifi, ancak çocuğun en az 16 yaşında olması halinde bir anlam ifade edecektir. Kural olarak, çocuğa ilişkin kişisel verilerin işlenebilmesi için çocuğun en az 16 yaşında olması gerekmektedir. Eğer çocuk 16 yaşın altındaysa işleme ancak kanuni temsilci veya velisinin rızasına dayalı olarak hukuka uygun olabilecektir.³⁴⁸ Diyebiliriz ki; hukuka uygun bir veri işleme faaliyetine çocuğun rıza gösterebilmesi için en az 16 yaşında olması aranmaktadır.³⁴⁹

Kişisel verilerin transferi ve ihlalin öğrenilmesi/bildirilmesi hakları da ilk defa Regülasyon ile düzenlenmiş, veri öznesinin verileri üzerindeki kontrolünün yeniden teminine hizmet eden önemli haklardır. Kişisel verilerin transferi hakkının iki temel unsuru bulunmaktadır; veri öznesinin, tekrar işlenebilecek bir formatta kendisine ilişkin kişisel verileri elde edebilmesi ve asıl veri sorumlusundan hiçbir engel veya problem olmaksızın başka bir veri sorumlusuna verilerini transfer edebilmesi.³⁵⁰ Bu hakkın; veri öznelerine, verilerini bir veri sorumlusundan diğerine serbestçe taşıyabilme yetkisi kazandırarak, kişisel verilerini denetimi altında tutabilme imkanı sağlaması beklenmektedir. Regülasyon'un veri öznelerine kazandırdığı bir diğer hak

³⁴⁶ 2016/679 Sayılı Genel Veri Koruma Regülasyonu Gerekçe md. 27., 158.

³⁴⁷ HELVACIOĞLU, STAKHEYEVA, "The Tale Of Two Data Protection Regimes: The Analysis Of The Recent Law Reform In Turkey In The Light Of EU Novelties", s. 815; DE HERT, PAKONSTANTINO, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals", s. 142.

³⁴⁸ 2016/679 Sayılı Genel Veri Koruma Regülasyonu md. 8., Gerekçe md. 38.

³⁴⁹ HELVACIOĞLU, STAKHEYEVA, "The Tale Of Two Data Protection Regimes: The Analysis Of The Recent Law Reform In Turkey In The Light Of EU Novelties", s. 815.

³⁵⁰ 2016/679 Sayılı Genel Veri Koruma Regülasyonu'nun 20. maddesinde bu hak "right to data portability" olarak düzenlenmiştir.; DİKER VANBERG, Aysem, "The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?", Journal of Internet Law, C.21, S. 7, 2018, s. 11.

da unutulma hakkıdır.³⁵¹ Unutulma hakkı verilerin depolanmasına ilişkin ilkelerle yakın ilişkili bir haktır.³⁵² Bu hak veri öznesine, veri sorumlusundan kendisine ilişkin, toplanma amacı bakımından daha fazla gerekli olmayan veya hukuka aykırı olarak işlenmiş olan kişisel verilerinin gecikmeksizin silinmesini talep edebilme yetkisini sağlamaktadır.³⁵³ Regülasyon'un hukuka aykırı veri işleme veya benzer surette ihlal teşkil eden eylemler karşısında öngördüğü yaptırımların, Direktif'e oranla çok daha yüksek olması yaptırımların caydırıcılığı bakımından önemli bir adımdır. Bu doğrultuda veri sorumlusunun bildirim yükümlülüğü de etkin bir düzenlemedir. Kişisel verilere yetkisiz erişilmesi, hukuka aykırı transferi veya depolanması gibi bir kişisel veri ihlalinin meydana gelmesi halinde, veri sorumluları bu durumu, ortaya çıkmasından itibaren en geç 72 saat içerisinde denetleyici makamlara bildirmekle yükümlüdür.³⁵⁴

Doktrinde; Regülasyon'un, üye devletlerin veri koruma mevzuatlarını tamamen veya kısmen devre dışı bırakarak doğrudan uygulanma ve bu surette yeknesak bir uygulama sağlayabilmek amacıyla düzenlenmiş olmasının, Birlik bünyesinde amaçların aksine belirsizliğe ve uyum eksikliğine yol açacağı şeklinde eleştirilmesine sebep olmuştur. Buna göre Regülasyon'un amaçladığı şekilde tek bir veri koruma mevzuatının tüm üye devletlerde uygulanması, gerçekleştirilemez bir iş olarak görülmüştür.³⁵⁵ Henüz uygulama kazanmış olan Regülasyon'a yönelik bu eleştirilerin haklı veya haksızlığını ise zaman gösterecektir.

³⁵¹ 2016/679 Sayılı Genel Veri Koruma Regülasyonu md. 17.

³⁵² HELVACIOGLU, STAKHEYEVA, "The Tale Of Two Data Protection Regimes: The Analysis Of The Recent Law Reform In Turkey In The Light Of EU Novelities", s. 816.

³⁵³ Bu hakka ilişkin güzel bir örnek olarak Google davası gösterilebilir. Davanın konusunu vatandaşların, arama motorlarından kendi kişisel bilgileri ile bağlantının geri çekilmesi talepleri oluşturmaktadır. ATAD, Google Spain & Mario Costeja Gonzalez Davası, C-131/12, T: 13.5.2014, https://curia.europa.eu/jcms/jcms/j_6/en/; BAŞALP, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", s. 93.

³⁵⁴ Bu hakkın "veri ihlalinin öğrenilme hakkı" olarak kısaca adlandırılması da mümkündür. 2016/679 Sayılı Genel Veri Koruma Regülasyonu md. 33/1.; Gerekçe md. 85.; HELVACIOGLU, STAKHEYEVA, "The Tale Of Two Data Protection Regimes: The Analysis Of The Recent Law Reform In Turkey In The Light Of EU Novelities", s. 817.

³⁵⁵ DE HERT, PAKONSTANTINO, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals", s. 142.



İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN ULUSAL DÜZENLEMELER VE CEZA HUKUKU ÖZELİNDE KORUNMASI

I. GENEL OLARAK

Kişisel veri kavramı, günümüzde,³⁵⁶ gelişen teknoloji ve bu gelişime bağlı olarak değişen kişisel korunma ihtiyacımıza, kişilik haklarımıza³⁵⁷ ve hukuki menfaatlerimize konu olan önemli bir kavram haline gelmiştir.³⁵⁸ Kişisel verilerin korunması ihtiyacının oluşmasında da etkili temel faktörler olarak ekonomik ve teknik gelişmeler gösterilmektedir. Özellikle ceza hukuku bakımından, teknik gelişmelere bağlı olarak klasik suç tiplerinin işlenme şekillerinin değişmesiyle, bu suçlarla korunmak istenen mevcut hukuksal yararlar ek veya daha önce korunmakta olmayan yeni hukuksal yararlar ortaya çıkmaktadır. Bu durumda, ceza kanunları ortaya çıkan bu hukuksal yararların korunmasını sağlayacak yeni suç tipleri ihdas etmektedir.³⁵⁹

³⁵⁶ Kişisel veri kavramına ilişkin daha önceki bölümde yapmış olduğumuz tanımlamalara benzer şekilde Türk Ceza Kanunu 135. maddenin gerekçesinde de “gerçek kişiyle ilgili her türlü bilgi, kişisel veri kabul edilmelidir” açıklamasına yer verilmiştir.; Devlet Denetleme Kurulu’nun 27 / 11/ 2013 tarihli ve 2013/3 sayılı Raporu’nun sonuç kısmında yapmış olduğu değerlendirmesine göre de kişisel veri; “kimliği belirli veya belirlenebilir bir gerçek kişiyle ilgili her türlü veri olarak tanımlanmaktadır. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, cihaz kimlikleri, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.”

³⁵⁷ KANADOĞLU, Korkut, Türkiye Barolar Birliği Özel Yaşamın Gizliliği Panel Konuşması, 18.11.2008, Ankara.

³⁵⁸ “Kişisel verilerin korunması, çağımızda, insan hakları kavramı ve korunması bilincinin gittikçe gelişmesine paralel olarak önemini artırmaktadır. Kişisel verilerin korunması hakkının temel amacı, bireyin özel yaşamının gizliliğinin güvence altına alınması yoluyla kişiyi korumaktır. Bilgi toplumunda giderek oldukça önemli bir konu haline gelen kişisel verilerin korunması hakkı, bireyin, demokratik bir hukuk devletinde özgür iradesiyle kendi yaşamını bizzat düzenleyebilmesinin bir gereği olarak karşımıza çıkmaktadır. Diğer taraftan bireyin kişiliğini serbestçe geliştirmesi, kişiliğinin korunması ve özgür bireylerden oluşan bir toplum düzeninin oluşturulması, ancak bireyin kişisel verilerine ilişkin hakkının korunmasıyla mümkündür. Bu hak yukarıda ifade edildiği üzere TC Anayasası’nın 20/2 maddesinde açık bir şekilde düzenlenmiştir.” Yargıtay HGK., E: 2014/4-56, K: 2015/1679, T:17.6.2015.

³⁵⁹ Meselâ günümüzün motorlu taşıtlarının gelişmesi kendine özel bir hukuk dalı olarak “trafik hukukunun” ortaya çıkmasına yol açmıştır. TIEDEMAN, Klaus,(çev. Feridun Yenisey),

Ülkemizde de kişisel verilerin korunması hukuksal yararı, ilk kez 5237 sayılı ve 01.06.2005 yürürlük tarihli Türk Ceza Kanunu'nda kişisel verilere karşı işlenen suçların ihdas edilmiş olmasıyla güvence altına alınmıştır. 5237 sayılı Kanun'un yürürlük tarihi itibarıyla, kişisel verilerin korunmasının temel esas ve usullerini belirleyen ulusal bir kanunumuz bulunmamaktaydı. TCK'da da kişisel veri kavramına ilişkin bir tanımlanmaya yer verilmiş değildi. TCK'da, kişisel verilerin hukuka aykırı kaydedilmesi, verilmesi, yayılması, ele geçirilmesi ve yok edilmemesi suç olarak düzenlenmişken, kişisel veri kavramının ne olduğu tam olarak bilinmemekteydi. Bu durum haklı olarak, TCK'nın bu hükümlerinin suçların ve cezaların kanuniliği prensibine aykırı olduğu eleştirilerine sebep olmuştur. Hatta bu eleştiriler Anayasa Mahkemesi'nin de inceleme konusu haline getirilmiş, lakin Mahkeme tarafından da haksız görülmüştür.³⁶⁰ Bugün itibarıyla, 2010 yılı Anayasa değişikliği ile Anayasa'nın 20. maddesine ek üçüncü fıkrasında, kişisel verilerin korunması hakkı ve kişisel verilerin korunmasının temel esas ve usullerin düzenlendiği özel bir kanunun hazırlanması güvence altına alınmıştır. Bu istikamette de 7 Nisan 2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu Resmi Gazete'de yayımlanarak yürürlüğe girmiş ve artık bu eleştirilerin haklı bir yanı da kalmamıştır. Dolayısıyla, ulusal bir veri koruma kanununa kavuşmuş olmanın ülkemizde kişisel verilerin korunmasına ilişkin sağlamış olduğu genel faydanın yanında, Türk Ceza Kanunu'nun kişisel verilere karşı işlenen suçları bakımından da, kişisel veri kavramının belirlenmesi ve verilerin hukuka uygun işlenme ilkelerinin düzenlenmiş olması itibarıyla önemi büyüktür.

Kişisel verilerin korunması, AB bünyesinde gerek Anayasal düzenlemelere konu edinilerek, gerekse münhasır veri koruma mevzuatlarıyla esas ve usulleri düzenlenerek, devletin vatandaşlarına sağlamakla mükellef olduğu, negatif bir statü hakkı olarak ele alınmıştır. ABD'de ise farklı bir yaklaşım benimsemiş ve kişisel veriler ekonomik bir güç olarak kabul edilmiştir. Bu itibarla da kişisel verilerin korunması inisiyatifi daha ziyade özel sektörün eline bırakılmıştır.³⁶¹ Bu yaklaşımları uyumsallaştırmak amacıyla kişisel verilerin korunması 1970'li yıllardan itibaren uluslararası düzenlemelere konu edinilmeye başlanmıştır. Türkiye'de ise, özellikle

“Bilgisayarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 41, S. 1-2, 1975, s. 319.

³⁶⁰ Anayasa Mahkemesi, E: 2015/32, K: 2015/102, T: 12.11.2015.

³⁶¹ KARLIDAĞ, “Ekonomi Politik Açıdan Kişisel Verilerin Korunması”, s. 149.

ulusal bir veri koruma düzenlemesi yapma sürecimizin 1989 yılından 2016 yılına kadar sürmüş olması kişisel verilerin korunmasına ilişkin hukuki düzenlemeler noktasında, Avrupa'yı oldukça geriden takip etmekte olduğumuzu göstermektedir. Ancak kişisel verilerin korunması hakkı, 2010 yılı Anayasa değişikliğine kadar doğrudan bir Anayasa hükmüne konu edilmemişe de, 1982 Anayasa'sının özellikle başlangıç kısmında vatandaşların maddi ve manevi varlığını geliştirebilme özgürlüğü çerçevesinde ve özel yaşamın gizliliği hakkı bünyesinde korunmaktaydı. Bunun yanı sıra, Türkiye'nin tarafı olduğu ve mahkeme olarak yargılama yetkisini de tanıdığı, AİHS'nin 8. maddesinde düzenlenen "özel ve aile hayatına saygı hakkı" kapsamında AİHM'in geliştirdiği içtihatlar doğrultusunda ülkemizde kişisel verilerin korunmasına ilişkin etkin bir koruma mevcuttu.³⁶² Dolayısıyla kişisel verilerin kamusal veya özel kişi ve kuruluşlarca hukuka aykırı olarak işlenmesi, TC. Anayasa'sı ve diğer ulusal yasalarımızın yanı sıra, AİHS'in 8. maddesinin de ihlaline sebep olmaktadır.³⁶³ Türkiye'nin, özellikle Avrupa Konseyi tarafından imzaya açıldığı 1980 yılı itibarıyla ilk imza veren devletlerden biri olmasına rağmen, onaylanma sürecini uzun süre tamamlayamadığı 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi de 17.03.2016 tarihi itibarıyla iç hukukumuzda dahil edilmiştir. Bu durum da ulusal veri koruma hukukumuz bakımından önemli bir gelişme olarak kabul edilmektedir.³⁶⁴

Çalışmanın bu bölümü; kişisel verilerin korunmasının doğrudan veya dolaylı olarak konu edinildiği ulusal düzenlemelere ve bu düzenlemeler arasında Türk Ceza Kanunu'nun, kişisel verilerin suç olarak düzenlenmiş olan belli hukuka aykırı işleme türleri, karşısında öngörmüş olduğu korumaya ayrılmıştır.

³⁶² Türkiye Cumhuriyeti Anayasası 90. maddesi 5. fıkrasına göre usulüne göre yürürlüğe konulmuş uluslararası sözleşmeler kanun hükmündedir. Buna göre Türkiye'nin tarafı olduğu AİHS ve Sözleşme ile düzenlenen temel hak ve hürriyetlere ilişkin aykırılık iddialarını inceleyen AİHM kararlarının, Türk hukuk uygulaması bakımından dikkate alınması Anayasal bir gerekliliktir. KÜZECİ, "İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı", s. 62.

³⁶³ ÜNVER, Yener, "Kişisel Verilerin Korunması", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, S. 1, 2008, s. 192.

³⁶⁴ 108 Sayılı Avrupa Konseyi Sözleşmesi'ne ek 181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol de 05 Mayıs 2016 tarihinde Türk hukukuna dahil edilmiştir. Kişisel Verilerin Korunması Kurulu Yayınları, "Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler", s. 10-11. <http://www.kvkk.gov.tr> (01.03.2018).

II. TEMEL ULUSAL DÜZENLEMELERDE KİŞİSEL VERİLER

A. Anayasa’ da Kişisel Verilerin Korunması

Kişisel verilerin korunması, Anayasal temelli insan onuru ve kişiliğine ilişkin temel bir kişilik hakkıdır. Zira kişisel verilerin korunması sadece işleme konusu yapılan maddi verinin değil, aynı zamanda bu verinin ilişkili olduğu yaşam alanına dair değerlerin de korunması anlamına gelmektedir.³⁶⁵ Bu doğrultuda kişisel verilerin korunması hakkının sınırlandırılması veya kamusal müdahale konusu yapılabilmesi ancak müdahalenin Anayasal temel hak ve özgürlüklerin sınırlandırılma rejimine uygun olarak gerçekleştirilmiş olması halinde hukuka uygun kabul edilebilecektir.³⁶⁶ Türkiye Cumhuriyeti Anayasası’nın giriş kısmında demokratik bir hukuk devletinde yaşayan bireylerin maddi ve manevi varlığını serbestçe geliştirebilme özgürlüğü güvence altına alınmış olup, bu özgürlük kişilerin verileri üzerinde serbestçe tasarrufta bulunarak kendi geleceğini şekillendirebilmesi şeklinde de tezahür edebilen kişisel verilerin korunması hakkıyla da doğrudan ilişkilidir.³⁶⁷ Bu doğrultuda, kişinin maddi ve manevi olarak kişiliğini serbestçe geliştirebilmesini gerçekleştirmeyi amaç edinmeleri itibarıyla kişisel verilerin korunması hakkıyla aynı istikamette Anayasa’ımızda düzenlenmiş temel haklar arasında; kişinin dokunulmazlığı, maddî ve manevi varlığı (md. 17),³⁶⁸ haberleşme hürriyeti (md. 22), din ve vicdan hürriyeti (md. 23), düşünce ve kanaat hürriyeti (md. 24), düşünceyi açıklama ve yayma hürriyeti (md. 25) ve Anaysamızın 20. maddesinde düzenlenmiş olan ve ikinci fıkrası ile kişisel verilerin korunmasını da güvence altına almakta olan özel hayatın gizliliği hak ve özgürlüklerini gösterebiliriz.³⁶⁹ Türkiye Cumhuriyeti Anayasa’sının, 2010 yılında 5982 sayılı Kanun’la yapılan değişiklikle “özel hayatın gizliliği” madde başlıklı, özel hayatın ve aile hayatının gizliliğini ve dokunulmazlığını konu edinen 20. maddesi dahil

³⁶⁵ DİNÇ, Engin, *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye’nin Durumu*, (Yayınlanmamış Yüksek Lisans Tezi), Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Diyarbakır, 2006, s. 68.

³⁶⁶ ŞİMŞEK, *Anayasa Hukukunda Kişisel Verilerin Korunması*, s. 1.

³⁶⁷ ARSLAN, “Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması”, s. 448.

³⁶⁸ SEYREK TÜTÜNCÜBAŞI, *Kişilerin Kendisine Ait Verilerin Kaderini Tayin Hakkının Ceza Hukuku Yoluyla Korunması*, s. 20.

³⁶⁹ “Ayrıca kişisel verilerin hukuka aykırı olarak işlenmesi, 1982 Anayasası’nın 17. maddesi ile güvence altına alınan kişi dokunulmazlığı, kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı ile Anayasanın 20 ve 22. maddelerinde düzenlenen özel hayatın gizliliği ve korunması hakkının ihlali anlamına da gelmektedir.” KVK Kurumu Yayınları, Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı, s. 6. <http://www.kvkk.gov.tr> (03.03.2018).

pek çok maddesi değiştirilmiş ve bu değişikliklerle kişilere temel hak özgürlüklere ilişkin ek güvenceler sağlanmıştır. Bu istikamette daha önce Anayasa'mızın doğrudan koruması altında olmayan kişisel verilerin korunması hakkı, 2010 yılı değişikliği ile 20. maddenin üçüncü fıkrasında düzenleme altına alınmıştır. Söz konusu fıkra da kişisel verilerin korunması hakkı; "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." şeklinde düzenlenmiştir.

Bu hükümle Türkiye Cumhuriyeti sınırları içerisinde yaşayan herkesin kişisel verilerinin korunmasını talep edebilme hakkının mevcudiyeti tanınmış ve aynı zamanda kişisel verilerin korunmasına ilişkin olarak veri öznesinin bilgi edinme, erişim, düzeltme ve kişisel verilerinin silinmesini talep edebilme hakları da güvence altına alınmıştır. Kişisel verilerin işlenmesini hukuka uygun kılan temel haller olan; ilgilinin açık rızasının bulunması ve kanun hükmü gereğince verilerin işlenmesi hallerinin de maddede düzenlenmiş olması önemli görülmektedir. Anayasa madde 20 ile, sağlanmış olan bu temel güvence ve prensipler dışında kişisel verilerin korunmasına ilişkin gerekli usul ve esasın düzenlenmesi, kanun koyucunun iradesine bırakılmıştır. Bu doğrultuda 6698 sayılı Kişisel Verilerin Korunması Kanunu ile ulusal hukukumuzda kişisel verilerin korunmasının temel usul ve esasları düzenlenmiştir

Anayasa Mahkemesi itiraz ve bireysel başvuru yoluyla önüne getirilen vakıa ve düzenlemelere ilişkin olarak kişisel verilerin korunması hakkının temel prensipleri ve sınırlandırılmasının yasal rejimini öngören önemli içtihatlarla imza atmıştır. Bu istikamette Anayasa Mahkemesi tarafından karşılaşılan iptal davalarında konu; çoğunlukla kişisel veri niteliğindeki bilgilerin işlenmesine ilişkin esas ve usullerin düzenlenmesinin doğrudan yürütme organına bırakarak, kişisel verilerin korunması hakkının keyfi müdahalelere maruz kalmasına yol açabilecek kanun hükümlerine ilişkin olmuştur. Örneğin; 5809 sayılı Elektronik Haberleşme Kanunu'nun 51. maddesi'nin "kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir." şeklindeki düzenlemesi, Anayasa Mahkemesi'nce; "*Anayasa'nın 20. maddesinin üçüncü*

fıkrasının son cümlesinde, " Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır. Yasama yetkisinin devredilemezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisini Bilgi Teknolojileri ve İletişim Kurumuna veren itiraz konusu kural, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırı" kabul edilmiştir.³⁷⁰ Benzer bir iptal kararı da İstatistik Kanunu'nun 8. maddesi hakkında; "Bir ülkede en güçlü veri tekeli idaredir. Bu gücün sınırlandırılması özel yaşamın ve düşünce ve kanaat özgürlüğünün korunması bakımından önemlidir. Anayasa'nın 20. ve 25. maddelerinde yer alan güvencelere rağmen itiraza konu 8. madde hükmüyle kişiler, bilgi toplama, saklama, işleme ve değiştirme tekeli olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamanın sınırlarına yasal düzenlemede yer verilmemiştir." gerekçesiyle verilmiştir.³⁷¹ Yine Anayasa Mahkemesi'nin, temel bir anayasal hak olarak, kişisel verilerin korunması hakkının sınırlandırılmasının ancak sınırlandırmanın açıkça kanunen öngörülmüş olması halinde söz konusu olabileceğine işaret ettiği ve bu doğrultuda 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un ilgili maddelerinin iptaline ilişkin verdiği kararının gerekçesi de; "Özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililer hakkında rızaları olmaksızın bilgi toplanmasının her zaman söz konusu kişinin özel hayatını ilgilendireceği kuşkusuzdur. İptali istenilen kurallar, kişinin açık rızası olmaksızın kişisel verilerine ulaşılmasına ve bu kişisel verilerin işlenip, bilgi halinde TİB'e teslim edilmesine olanak tanımaktadır.

³⁷⁰ Anayasa Mahkemesi, E: 2013/122, K: 2014/74, T: 09.04.2014.

³⁷¹ Anayasa Mahkemesi, E: 2006/167, K: 2008/86, T: 20.03.2008.; "Yasama yetkisinin devredilemezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Kurumun faaliyet alanı kapsamında elde ettiği sağlık bilgilerinin korunması, paylaşılması ve tutulmasına yönelik usul ve esasları belirleme yetkisini Çalışma ve Sosyal Güvenlik Bakanlığına veren itiraz konusu kurallar, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırıdır." Anayasa Mahkemesi, E: 2014/74, K: 2014/201, T: 25.12.2014.

Anayasa'nın 20. maddesinin üçüncü fıkrasında " Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına iliskinesas ve usuller kanunla düzenlenir." denilmektedir. Anayasa'nın bu hükmünde yer alan kişisel verilerin işlenmesine ilişkin "kanunda öngörülen hallerin" nelerden ibaret olduğu 5651 sayılı Kanun'da açıkça belirtilmemiştir. İptali istenilen kurallar, Anayasa'da yer alan güvenceye rağmen, kişilere ait her türlü kişisel veri, bilgi ve belgelerin konu, amaç ve kapsam bakımından yeterli sınırlamaya tabi kılınmaksızın koşulsuz olarak TİB'e verilmesine imkân tanımakta, böylece kişiler idareye karşı korumasız hale getirilmektedirler. Dolayısıyla iptali istenilen kurallar, belirli ve öngörülebilir olmadığından kişilerin kişisel verilerin korunması hakkını usulsüzce sınırlandırmakta ve Anayasa'nın 20. maddesine aykırılık teşkil etmektedir." şeklindedir.³⁷²

Anayasa Mahkemesi'nin kişisel verilerin korunması hakkına yönelik hukuka aykırı müdahale bulunduğu gerekçesiyle vermiş olduğu ihlal kararları yanında, kamu düzeni ve güvenliği, kamusal çıkarların üstünlüğü ve toplumsal refahın sağlanması gibi gerekçelere bağlı olarak kişisel verilerin sınırlandırılmasını hukuka uygun kabul ettiği önemli kararları da mevcuttur.³⁷³ Örneğin; başvurucunun, Hane Halkı Bütçe Anketi istatistiğine katılacak örnek hane olarak TÜİK tarafından evinin belirlenmesi

³⁷² Anayasa Mahkemesi, E: 2014/87, K: 2015/112, T: 8.12.2015.; "Dava konusu kural, yukarıda belirtilen kişisel veri niteliğinde olan ve ciddi suçların tespiti, soruşturulması ve kovuşturulmasında kullanılmak üzere gerçek ve tüzel kişilere ilişkin trafik bilgisinin, işlenmemiş veri hâlinde süreli olarak muhafaza edildiği erişim veya yer sağlayıcılardan, TİB tarafından herhangi bir gerekçe veya neden göstermeksizin temin edilmesine olanak sağlamaktadır. Söz konusu verilere ulaşılabilirlik, kişilerin tercihleri, düşünceleri ve davranışları hakkında fikir verebileceğinden kişilerin özel hayatlarına müdahale edilme riskini içermektedir. Kuralda, temin edilecek bilgiyle ilgili olarak herhangi bir konu ve amaç sınırlaması bulunmadığı gibi bilginin kapsamı, ne şekilde kullanılacağı, tutulacağı süre, temin edilme gerekçesi gibi hususlarla ilgili olarak da herhangi bir belirlilik bulunmamaktadır." Anayasa Mahkemesi, E: 2014/149, K: 2014/151, T: 2.10.2014.

³⁷³ Kişisel verilerin korunması hakkının ihlali iddiasının ilk kez huzuruna taşındığı bir iptal davasında Makeme;"1774 sayılı Yasa'nın 2. maddesinde sayılan özel veya resmî her türlü konaklama tesislerinden Bakanlar Kurulu'nca belirlenenlerde tutulacak kayıtların genel kolluk kuvvetlerinin bilgisayar terminallerine bağlanması zorunluluğunu getiren dava konusu kuralın, kamu düzeni, genel asayiş ve kamu yararını sağlama amacına yönelik olması ve demokratik toplum düzeninin gereklerine de aykırı bir yönü bulunmaması nedeniyle, Anayasa'nın 2. 13. ve 20. maddelerine aykırı olmadığı sonucuna varılmıştır. İptal isteminin reddi gerekir." kararını vermiştir. Anayasa Mahkemesi, E: 1996/68, K: 1999/1, T: 06.01.1999.; Anayasa Mahkemesi, E: 2014/180, K: 2015/30, T: 19.03.2015.; Anayasa Mahkemesi, E: 2010/40, K: 2012/8, T:19.01.2012; "Somut başvuru açısından, belirli suçlar nedeniyle hakkında kamu davası açılmış olan şahıslar hakkındaki derdest dava bilgilerinin GBT sistemine kaydının yapıldığı, kamu düzeni ve güvenliğinin temini şeklindeki meşru temelleri içerdiği anlaşılan uygulama kapsamında söz konusu bilgilerin özellikle yapılan güvenlik taramaları ve güvenlik soruşturmalarında kullanıldığı, ilgili bilgilerin toplanma, paylaşım, kullanım ve silinmesine ilişkin hususların ayrıntılı olarak düzenlendiği anlaşılmaktadır. Söz konu başvuruya konu müdahalenin demokratik toplumda gerekli ve ölçülü olmadığı söylenemez." Anayasa Mahkemesi, Bülent Kaya Başvurusu.

üzerine yapılan anket kapsamında; hane sahibinden, hane halkının alışveriş alışkanlıkları, harcamaları, gelir ve gider kaynakları ve dağılımlarının belli istatistik belirteçlerine göre kayıt altında tutulması talep edilmiştir. Başvurucunun çalışma yoğunluğu gerekçesiyle ankete katılmaktan muaf tutulmasına ilişkin talebi TÜİK ilgili müdürlüğü tarafından reddedilerek, istenilen bilgileri vermemesi halinde idari para cezası ödeme külfeti altında kalacağı başvurucuya tebliğ olunmuştur. Bu doğrultuda başvuru tarafından, kendisinden istenilen bilgilerin ve bu verilerin kayıt altına alınmasının özel yaşamın gizliliğine ilişkin bir müdahale teşkil ettiği gerekçesiyle, olağan kanun yolları tüketilmiş ve Anayasa Mahkemesi'ne bireysel başvuruda bulunulmuştur. Mahkeme kişiden istatistiki amaçlarla talep edilen bilgilerin kişisel veri niteliği taşıdığını, kişisel verilerin T.C. Anayasası'nın 20. maddesi ile temel bir anayasal hak olarak düzenlenmiş olduğunu ve temel hak ve özgürlüklerin sınırlandırılma rejimine uygun olarak bu hakkın da sınırlandırılabilceği kabul etmiştir. Devletin, resmi kuruluşları vasıtasıyla vatandaşlarına ilişkin belli verileri kamusal refah ve istikrarın sağlanması gerekçeleriyle toplayabileceği, bu durumun özel yaşam hakkına yönelik bir müdahale teşkil ettiği, ancak bu müdahalenin kanuni bir dayanağının bulunması, kamu düzeni ve ülkenin ekonomik refahı gibi meşru gerekçelere dayanması dolayısıyla yapılan müdahalenin, hukuka aykırı olmadığına karar verilmiştir.. Ayrıca demokratik bir toplum gereklerine uygun olarak istenilen bilgilerin verilmemesi karşısında öngörülen idari para cezasının miktarının düşüklüğü de nazara alındığında yapılan müdahale ölçülü de bulunmuştur.³⁷⁴ Yine Mahkeme,

³⁷⁴ Anayasa Mahkemesi Defne Samyeli Başvurusu, B.No: 2014/4399, Karar Tarihi: 21.09.2016.; Karara konu 5429 Sayılı Türkiye İstatistik Kanun'unun 8. maddesi doğrultusunda kişiler "kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle" yükümlü tutulmuştur. Bu düzenleme Anayasa Mahkemesi tarafından "özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililer hakkında rızası olmaksızın bilgi toplamasının her zaman söz konusu kişinin özel hayatını ilgilendireceği kuşkusuz. Anket formlarında yer alan bazı sorular özel yaşamın gizliliği ile düşünce ve kanaatin açıklanması sonucunu doğurabilir. Bir ülkede en güçlü veri tekeli idaredir. Bu gücün sınırlandırılması özel yaşamın ve düşünce ve kanaat özgürlüğünün korunması bakımından önemlidir." gerekçesi doğrultusunda iptaline karar verilmiştir. Anayasa Mahkemesi'nin bu kararı, kişisel verilerin korunması temel hakkının Anayasal güvence altında olmadığı başvurunun gerçekleştirildiği zaman itibarıyla, kişisel verilerin kamusal makamlarca başvuru konusu düzenlemede olduğu gibi sınırları belli olmaksızın elde edilmesine ilişkin girişimlerin özel yaşamın korunmasına ilişkin Anayasa md. 20 kapsamında bir müdahale teşkil ettiğinin tespit etmekte olması bakımından önemlidir. Anayasa Mahkemesi, E: 2006/167, K: 2008/86, T: 20.03.2008.; Bu karar doğrultusunda; "İstatistikî birimler, ülkenin ekonomi, sosyal, demografi, kültür, çevre, bilim, teknoloji ve ihtiyaç duyulan diğer alanlardaki resmi istatistikleri üretmek üzere, Anayasa'da belirlenen temel haklar ve ödevler çerçevesinde, kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle yükümlüdür." şeklinde yeniden düzenlenen Kanun'un 8. maddesinin 2010 yılında itiraz yoluyla Anayasa Mahkemesi'nin önüne taşınması üzerine bu kez Mahkeme, "istatistikî birimlerin

6222 sayılı Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun'un 5. maddesi ile getirilen elektronik kart uygulamasına ilişkin kuralların Anayasa 10., 17., 20. ve 59. maddelerine aykırılığı ileri sürülerek iptallerine yönelik başvurunun; *“İtiraz konusu kurallar, sporda şiddetin önlenmesi, kamu düzeninin ve güvenliğinin sağlanması, bireylerin can ve mal güvenliğinin temin edilmesi, vergi kaçırılmasını engellemek gibi demokratik toplum düzeni yönünden zorlayıcı toplumsal ihtiyaçları karşılamaya yöneliktir. Kurallar ile özel hayatın ve kişisel verilerin korunması haklarına bir sınırlama getirilmiş ise de bu sınırlandırma Anayasa ile Devlete yüklenen demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır. Ayrıca öngörülen sınırlandırma için kullanılan araç, hak ve özgürlüğü en az sınırlayacak, amaca uygun dengeli bir orantı oluşturmakta, kamu düzeni ve güvenliğinin korunması şeklindeki kamu yararı ile kişisel verilerin korunması hakkı arasında makul denge kurmaktadır. Dolayısıyla sınırlamanın, ölçülülük ve demokratik toplum düzeninin gereklerine aykırılık teşkil ettiği söylenemez.”* gerekçesiyle reddedilmesine karar vermiştir.³⁷⁵ MİT'in yetkilerini düzenleyen 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 6. maddesinin b. ve c. bentlerinin *“dava konusu kuralda, kamu kurum ve kuruluşlarıyla özel kurum ve kuruluşların uhdesinde bulunan bilgi, belge, veri ve kayıtların MİT tarafından temin edilebileceği belirtilmektedir. İstenilebilecek bu bilgiler arasında özel hayatın gizliliği kapsamında kalacak bilgiler ve kişisel veriler de bulunabileceğinden, kuralla özel hayatın gizliliği ve kişisel verilerin korunması haklarına sınırlama getirildiği”,* Anayasa'nın 20. maddesine aykırı olduğu ve iptallerinin gerektiğine ilişkin açılan dava

kendilerinden istenen bilgileri geçerli bir mazereti olmaksızın belirlenen şekil ve sürede, eksiksiz ve hatasız olarak verme zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmıştır. Bu durumda dava konusu iki hüküm birlikte değerlendirildiğinde bireylerin temel haklarının korunmasının idari ve adli makamların sorumluluğuna bırakıldığı görülmektedir. İdari makamlar bireyin temel haklarını ihlal edecek şekilde bilgi talep etmeme yükümlülüğündedirler. İdari makamların bu ödevini yerine getirmemesi halinde istatistikî bi-rimler haklarını yargı makamları önünde arayabileceklerdir. Bu durumda itiraz konusu kurallarla bireyin hakları ile kamu yararı arasında makul bir denge kurulduğu ve bireyin haklarına ölçsüz bir müdahaleye izin verilmediği anlaşıldığından Anayasanın 2. Maddesindeki hukuk devleti ilkesine aykırılık görülmemiştir” şeklinde karar vermiştir. Anayasa Mahkemesi, E: 2010/12, K: 2011/135, T: 12.10.2011.

³⁷⁵ Mahkemenin öte yandan ilgili hükmün elektronik kart oluşturmak amacıyla alınan kişisel bilgilerin reklam ve pazarlanmasına ilişkin yetkinin ve merkezi veri tabanında tutmak yetkisinin üçüncü kişilere devredilebileceğine ilişkin düzenlemenin ilgili bentlerinin *“demokratik toplum düzeninin oluşturulması, korunması ve geliştirilmesi açısından, sportif faaliyetlerde yaşanan şiddetin önlenmesi için alınması gereken tedbirlerden olduğu söylenemeyeceği, aynı zamanda söz konusu yetkilerin federasyona verilmesi suretiyle özel hayatın ve kişisel verilerin korunması haklarına getirilen sınırlandırma, sportif faaliyetlerde yaşanan şiddeti önleme amacını gerçekleştirmeye elverişli olmadığından, dolayısıyla belirtilen amaç için gerekli ve elverişli olmayan kuralların, ölçülülük ilkesine de uygun”* görülmediğine ve iptalinin gerektiğine karar verilmiştir.

da Anayasa Mahkemesi müdahalenin “*demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmakta*” olduğu, dolayısıyla iptal talebinine konu düzenlemelerin Anayasa’ya aykırı olmadığına ve reddi gerektiğine karar vermiştir.³⁷⁶

Bireysel başvuru yoluyla huzuruna gelen ve yargılama makamlarının ihlali gerçekleştiren konumunda olduğu, somut bir olaya ilişkin olarak da Mahkeme; “*yargı mercilerinin tarafların iddia ve taleplerini değerlendirmede takdir yetkileri olduğu açık olmakla birlikte kişilerin mahremiyeti, dolayısıyla özel hayatı üzerinde önemli etkiler doğurabilecek konulara ilişkin taleplerin reddi durumunda bunun gerekçelerinin ayrıntılı şekilde kararda gösterilmesi, hakkaniyete uygun bir yargılamanın gereğidir.*” değerlendirmesinde bulunarak ihlal kararı vermiştir. Mahkeme, somut olayda; başvuran tarafından açılan hukuk davasının, üçüncü kişilere kapalı olarak yapılmasına yönelik başvuranın talebinin ilk derece ve temyiz mahkemelerince herhangi bir gerekçe gösterilmeksizin reddedilmiş olması ve konu itibarıyla davacıya ait hassas veri niteliğinde bilgileri içeren somut davanın üçüncü kişilere açık görülmesi neticesinde kişinin mahremiyeti ve özel hayatının ihlal edilmiş olduğuna karar vermiştir.³⁷⁷

³⁷⁶ “Dava konusu kuralda, kamu kurum ve kuruluşlarıyla özel kurum ve kuruluşların uhdesinde bulunan bilgi, belge, veri ve kayıtların MİT tarafından temin edilebileceği belirtilmektedir. İstenilebilecek bu bilgiler arasında özel hayatın gizliliği kapsamında kalacak bilgiler ve kişisel veriler de bulunabileceğinden, kuralla özel hayatın gizliliği ve kişisel verilerin korunması haklarına sınırlama getirildiği açıktır. Ancak bu sınırlama, 2937 sayılı Kanun’un 4. maddesiyle MİT’e verilen görevlerin, yani ülkenin varlığına, bağımsızlığına, güvenliğine ve anayasal düzenine karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında milli güvenlik istihbaratını devlet çapında oluşturma ve istihbarata karşı koyma görev ve sorumluluğunun yerine getirilebilmesini, dolayısıyla millî güvenliği, kamu düzenini ve suç işlenmesinin önlenmesini sağlamak amacıyla getirilmekte olup demokratik toplum düzeni bakımından alınması gereken tedbirler kapsamında kalmaktadır.” Anayasa Mahkemesi, E: 2014/122, K: 2015/123, T: 30.12.2015.

³⁷⁷ “Somut olayda, yargılamanın ü.üncü kişilere kapalı yapılması talebi hakkında İş Mahkemesinin 9/2/2010 tarihli duruşma tutanağında dava dilekçesinin mahiyeti gereği davacı vekilinin gizlilik talebinin reddine karar verildiği belirtilmiştir. Yukarıda belirtildiği üzere HIV enfeksiyonu rahatsızlığı olan kişilerin uzun zamandır ön yargı ve kınamaya maruz kalan zayıf bir grup olduğu, söz konusu dışlanma, damgalanma ve ön yargıların özellikle iş hayatında mevcut olması durumunda kişiler üzerindeki etkilerinin çok daha yıkıcı olabileceği dikkate alındığında başvuruçunun gizlilik talebi, özel hayata saygı hakkına ilişkin makul ve savunulabilir niteliktedir. Yargı mercilerinin tarafların iddia ve taleplerini değerlendirmede takdir yetkileri olduğu açık olmakla birlikte kişilerin mahremiyeti, dolayısıyla özel hayatı üzerinde önemli etkiler doğurabilecek konulara ilişkin taleplerin reddi durumunda bunun gerekçelerinin ayrıntılı şekilde kararda gösterilmesi, hakkaniyete uygun bir yargılamanın gereğidir. İş Mahkemesince dava dilekçesinin mahiyeti gereği gizlilik talebinin reddedildiği belirtilmekle birlikte söz konusu ifade muğlak olup hangi somut nedenlere bağlı olarak gizlilik kararı verilmediğini açıklamaktan uzaktır. Kararın temyizi aşamasında aynı iddialar ileri sürülmüş olmasına rağmen temyiz hakkında verilen kararda da bu hususlara ilişkin bir gerekçeye yer verilmediği anlaşılmıştır. Bu bağlamda söz konusu kararların konuyla ilgili ve yeterli gerekçe içermediği kabul edilmelidir. Açıklanan nedenlerle başvuruçunun, Anayasa’nın 20.

B. Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Veriler

Kişisel verilerin korunması, uluslararası düzlemde uluslararası aktörler tarafından ve ulusal düzlemde pek çok Avrupa Devleti tarafından 1970’li yıllardan itibaren hukuksal düzenlemelere konu edilmiştir. Kişisel verilerin korunmasına ilişkin olarak mevcut hükümleri genişletici yorumlara açık kılarak (AİHS md. 8), özel hüküm getirerek (ABTHŞ md. 8) veya konuyu özel olarak düzenleme konusu yaparak ele alan uluslararası düzenlemelerin pek çoğunda, Türkiye devleti imzası bulunmaktaysa³⁷⁸ da, ülke olarak kişisel verilerin korunması hukukunu geriden takip etmekte olduğumuzu söyleyebiliriz. Ancak özellikle 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun yürürlük kazanması³⁷⁹ ve 108 sayılı Avrupa Konseyi Sözleşmesi’nin onaylanma sürecinin tamamlanarak iç hukukumuzda dahil edilmesi ile ülkemizde kişisel verilerin korunması hukuku ivme kazanmıştır.

Bu düzenlemeler eksenin de, kişisel veri kavramının belirlenmesine ilişkin kimliği belirli veya belirlenebilir bir kişi ile ilişkili olma gibi temel unsurlar geliştirilebilmişse de bu kavrama dahil olan veri türlerinin tek tek sayılmak suretiyle sınırlandırılabilmesi mümkün görülmemiştir.³⁸⁰ Bu durumun oluşmasına her ne kadar teknolojik gelişmeler doğrultusunda gün geçtikçe yeni veri üretim araçlarının ve veri

maddesinde yer alan özel hayata saygı hakkının unsurlarından olan kişisel verilerin korunması hakkının ihlal edildiğine karar verilmesi gerekir.” Anayasa Mahkemesi, T.A.A. Başvurusu.

³⁷⁸ Türkiye Avrupa Konseyi’nin 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında/Karşısında Gerçek Kişilerin Korunmasına İlişkin Sözleşme’nin imzaya açıldığı tarih itibarıyla ilk imzalayan devletlerden birisidir. Ancak sözleşmenin onaylanarak yürürlüğe konulması iç hukuk düzenlemelerinin tamamlanmasına kadar ötelenmiş ve Sözleşme, 6698 sayılı Kanun’un yürürlüğe girmesinin akabinde 17.03.2016 tarihi itibarıyla iç hukukumuzda dahil edilmiştir. Bu duruma ilişkin Sözleşme’nin 4. maddesi gereğince, iç hukukta kişisel verilerin korunmasına yönelik yasal düzenleme yapılması zorunlu tutulmuş olması gösterilmektedir.

³⁷⁹ “Türkiye’de kişisel verilerin korunmasına ilişkin özel bir kanun çıkarmak için ilk kez 1989 yılında bir komisyon oluşturulmuştur. Bu komisyon henüz çalışmalarını tamamlayamadan dağılmıştır. 2000 yılında yeni bir komisyon oluşturulmuş ve bu komisyon üç yıllık bir çalışmanın neticesinde bir kanun tasarısı hazırlamıştır. Fakat hazırlanan tasarı çeşitli nedenlerle kanunlaşamamıştır. 2008 ve 2014 yıllarında, Adalet Bakanlığı öncülüğünde yeni bir tasarı hazırlanıp Türkiye Büyük Millet Meclisi’ne (TBMM) sunulmuşsa da yasama dönemi sona erdiği için ilgili kanun teklifleri kadük hale gelmiştir. Bu kapsamda 26 Aralık 2014 tarihinde “Kişisel Verilerin Korunması Kanunu Tasarısı” TBMM Başkanlığına sunulmuştur. Tasarı, 24 Mart 2016 tarihinde kanunlaşmış ve 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiş, böylece kişisel verilerin korunması için gerekli hukuksal altyapı tamamlanmıştır.” KVK Kurumu Yayınları, Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı, s. 3. <http://www.kvkk.gov.tr> (08.09.2017).

³⁸⁰ “Kuralda yer alan "kişisel veri" kavramı teknolojik gelişmelere bağlı olarak çok farklı şekillerde ortaya çıkabileceğinden bu kapsama giren tüm verilerin kanun koyucu tarafından önceden öngörülebilmesi ve tek tek sayılabilmesi mümkün değildir. Bununla birlikte gerek ulusal ve uluslararası mevzuat gerekse yargı içtihatları çerçevesinde "kişisel veri" kavramının, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmektedir.” Anayasa Mahkemesi, E: 2015/32, K: 2015/102, T: 12.11.2015.

türlerinin ortaya çıkmakta olması gerekçe gösterilebilirse de, kişinin nitelendirilebilmesi, betimlenebilmesi veya belirlenebilmesine imkan veren ve insan zihninin sınırsızlığı doğrultusunda çoğaltılabilecek olan pek çok enformasyonun kişisel veri olabilirliğinin bu duruma temel olarak etkili olduğunu söylememiz gerekir. Örneğin kişilerin parmak izi veya ses renginin³⁸¹ kişisel veri olarak kabulü mümkün görülmektedir ve bu verilere gerek kamusal kurumlarca kamu yararı veya toplumsal refah gibi gerekçelerle, gerekse özel sektör tarafından daha maddi faydaya dayanan gerekçelerle ihtiyaç duyulabilmektedir. Kişisel verilerin işlenmesini kaçınılmaz kılan modern toplumda baş gösteren bu ihtiyaç karşısında, verileri işleme konusu yapılan bireyin ve özel yaşam alanına dahil olduğundan kuşku duyulmayan kişisel verilerinin korunmasının sağlanması demokratik bir hukuk devletinin pozitif yükümlülüğü olarak görülmektedir. Devlet, bu yükümlülüğünü kişisel verilerin korunmasını anayasal bir hak olarak güvence altına alarak ve verilerin işlenmesine ilişkin temel esas ve usulleri düzenleyen münhasır veri koruma kanunları ihdas ederek yerine getirebilmektedir. Türkiye Cumhuriyeti Anayasası'nın 20. maddesi ek 3. fıkrasıyla herkesin *"kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip"* olduğu düzenleme altına alınmış ve kişisel verilerin korunmasına ilişkin temel usul ve esasların kanunla belirlenmesi gereğine işaret edilmiştir. Bu doğrultuda 6698 sayılı Kişisel Verilerin Korunması Kanun'u ile kişisel verilerin işlenmesine ve gizliliğinin korunmasına ilişkin temel usul ve esaslar düzenleme altına alınmıştır.

Temel 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 düzenlemek"* (KVKK md. 1) şeklinde kabul edilen Kişisel Verilerin Korunması Kanun'un oluşturulmasını gerektiren çok sayıda sebep mevcuttur. Bu sebepler arasında ilk olarak Anayasa'nın 20. maddesi ile kişisel verilerin işlenmesine ilişkin temel usul ve esasların kanunla düzenlenmesi kuralının öngörülmüş olmasının gösterilmesi gerekir. Zira 6698 sayılı Kanun'un yürürlükte olmadığı dönemde Anayasa Mahkemesi, kişisel verilerin işlenmesine ilişkin temel prensiplerin kanunla düzenlenmesi gerektiği ve bu nitelikte bir düzenlemenin henüz mevcut olmamasına rağmen kişisel verilerin işlenmesi konusunda ucu açık şekilde yürütme organın yetkilendirildiği pek çok düzenlemenin

³⁸¹ AİHM, P.G.ve J.H./ United Kingdom, <https://hudoc.echr.coe.int> (7.01.2018).

iptaline hükmetmiştir.³⁸² Kişisel verilerin korunmasına ilişkin 5237 sayılı Türk Ceza Kanunu'nun 135. ve devam eden maddeleri ile düzenlenen suç tipleri bakımından da kişisel veri kavramının ve kişisel verilerin işlenmesinin temel esas ve usullerin düzenlendiği bir mevzuata ihtiyaç duyulmuştur. Özellikle kişisel veri kavramına ilişkin bir tanımın yapılmamış olması, TCK'nın ilgili hükümlerinin kanunilik prensibine aykırı olduğu şeklinde eleştirilmesine de sebep olmuştur.³⁸³ Bunun dışında Avrupa Birliği ile yürütülen üyelik müzakereleri, uluslararası işbirliği ve ticaretin geliştirilmesi ihtiyacı ve gerek uluslararası gerekse ulusal kurumlarla kişisel verilerin paylaşılmasında yaşanan güçlüklerin ortadan kaldırılması amacı ulusal bir veri koruma düzenlemesinin hazırlanmasına yöneltten etkenler arasında gösterilmektedir.³⁸⁴ Kişisel verilerin yabancı şirketler tarafından gerçekleştirecek yatırımlara bağlı olarak ülkemize transferine de, bugüne kadar ülkemizde kişisel verilerin korunmasına ilişkin etkin koruma sağlayacak ulusal bir düzenlemenin mevcut olmaması engel teşkil etmiştir. Dolayısıyla bu durum, yabancı sermayeyi ülkemize yatırım yapma düşüncesinden caydırabilen bir unsur da olmuştur.³⁸⁵

³⁸² “5754 sayılı Kanun'un 66. maddesinin birinci fıkrasının (f) bendiyle eklenen itiraz konusu son cümlesinde ise bu kişi ve grupların sağlık bilgilerinin nasıl tutulacağına ilgili kuruluşların görüşleri alınarak hazırlanacak yönetmelik ile düzenleneceği hüküm altına almıştır. Yasama yetkisinin devredilemezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Kurumun faaliyet alanı kapsamında elde ettiği sağlık bilgilerinin korunması, paylaşılması ve tutulmasına yönelik usul ve esasları belirleme yetkisini Çalışma ve Sosyal Güvenlik Bakanlığına veren itiraz konusu kurallar, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırıdır. Açıklanan nedenlerle, itiraz konusu kurallar Anayasa'nın 20. maddesine aykırıdır. İptalleri gerekir.” Anayasa Mahkemesi, E: 2014/74, K: 2014/201, T: 25.12.2014.; “T.C. Anayasası'nın 20. maddesinin 3. fıkrasında yer alan düzenlemeye uygun olarak kişisel verilerin korunmasına ilişkin yasal düzenleme halihazırda bulunmadığından, mesai takibinin parmak izi yöntemiyle yapılmasında, uygulamanın sınırlarını, usul ve esaslarını gösteren bir yasal dayanağının bulunmaması, toplanan verilerin ileride başka bir şekilde kullanılamayacağına dair bir güvencenin mevcut olmaması göz önüne alındığında...” Danıştay 5. Daire, E: 2013 / 5342, K: 2013 / 9525, T: 10.12.2013.

³⁸³ “Başvuru kararında özetle, ceza mevzuatında kişisel verilerle ilgili bir tanım ve sınırlandırma yapılmadığından, itiraz konusu kuralın suçta ve cezada kanunilik ve belirlilik ilkelerine ve Anayasa'nın 38. maddesine aykırı olduğu ileri sürülmüştür.” Anayasa Mahkemesi, E: 2015/32, K: 2015/102, T: 12.11.2015.

³⁸⁴ “Ülkemizde kişisel verilerin korunmasına ilişkin kanuni bir düzenleme olmaması sebebiyle, polis birimleri arasında etkin bir işbirliğini hayata geçiren EUROPOL 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.” 6698 sayılı Kanun Genel Gereğesi.

³⁸⁵ 6698 sayılı Kişisel Verilerin Korunması Kanunu Genel Gereğesi.; KVK Kurumu Yayınları, “Ulusal ve Uluslararası Alanda Kişisel Verilerin Korunmasına Duyulan İhtiyaç”, s. 6. <http://www.kvkk.gov.tr> (08.09.2017).

Sonuç olarak ülkemizin kişisel verilerin korunmasına ilişkin yürütülen mevzuat oluşturma çabalarının, 6698 sayılı Kanun'un hazırlanması ve yürürlük kazanmasıyla neticelenmiş olması ülkemiz adına oldukça önemli bir adım olarak kabul edilmelidir.³⁸⁶ Özellikle AB ülkeleri ile gerçekleştirilecek veri transferleri bakımından Türkiye'nin güvenilir ülke statüsü kazanması adına 6698 sayılı Kanunu ile önemli bir kriter tamamlanarak uluslararası ekonomik ve adli işbirliği kanallarının işletilmesine de etkinlik kazandırılmıştır.³⁸⁷ Ülkemiz adına pek çok açıdan önemli getirileri olacağının şüphesiz olduğu Kişisel Verilerin Korunması Kanunu'nun ilgili hükümlerine, çalışmanın ilk bölümünde incelenen kişisel verilerin korunmasının temel kavram, ilke ve prensiplerine ilişkin konularda yer verilmeye çalışılmış, çalışmanın bu kısmında da kısaca 6698 sayılı Kanun'un kapsamına ve denetime ilişkin düzenlemelerine değinilmekte fayda görülmüştür.

1. Kanun'un Kapsamı ve Uygulama Alanı

95/46 AT sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi esas alınarak hazırlanmış olan 6698 sayılı Kanun'un uygulanma alanı ve kapsamı; "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" şeklinde belirlenmiştir.³⁸⁸ Kişisel veri kavramı, verilerin otomatik veya otomatik olmayan vasıtalarla işlenmesi gibi kavramların üzerinde daha önceki bölümlerde ayrıntılı olarak durulduğundan burada tekrara düşmemek adına bu kavramlara ilişkin açıklamada bulunmak yerine daha ziyade Kanun'un özellikli olarak kapsamına dahil olan ve tamamen veya kısmen kapsamının dışında tuttuğu hususlara değinilecektir.

³⁸⁶ Kanun'un, amaçlandığı üzere kişisel verileri toplanan veya işlenen kişilerin korunmasına yönelik olacak şekilde ilgili kişilerin hak ve yetkilerinin ayrıntılı düzenlenmesine yer vermesi gerekmekte iken, mevcut hükümler daha ziyade verileri toplayan veya işleyen kişilerin hak ve yetkilerini düzenleme amaç ve hedefine yönelik olmuştur. ÜNVER, "Kişisel Verilerin Korunması", s. 196.

³⁸⁷ AKINCI, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi", s. 2., 4.; "Böylece, gerek yurtdışında operasyonları olan Türk şirketlerinin, gerekse Türkiye'de operasyonları olan yabancı şirketlerin veri transferinde aldıkları izinlere ilişkin önemli bir maliyet tasarrufu sağlanacaktır." KESER BERBER, KAYA, *Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, İstanbul, 2014, s. 73.

³⁸⁸ KVKK md. 2.

Toplumsal yaşamda varlığını sürdüren her vatandaşın gerek kamusal ihtiyaçlarla, gerekse alışveriş yapmak gibi günlük ihtiyaçları karşılama amaçlarıyla isteği doğrultusunda veya zorunlu olarak özel veya kamusal kişi veya kişilerle paylaştığı kişisel verilerinin, işlenmesine ilişkin kurallar, bu verilerin toplanmasının sınırı veya toplanan verilerin güvence altına alınmasını sağlayacak temel usul ve esaslar 6698 sayılı Kanun’la düzenlenmiştir.³⁸⁹ Bu doğrultuda kişisel verilerin gerek özel sektör gerekse kamu sektörü tarafından işlenmekte olması fark yaratmamaktadır. Kanun’un kişisel verilerin işlenmesinde uyulması gereken kurallarının uygulanabilmesi veya veri öznesinin haklarından istifade edebilmesi bakımından, verilerin kimin tarafından işlenmekte olduğu önem arz etmez. Aynı durum verilerin otomatik veya otomatik olmayan yollarla işlenmesi açısından da geçerli kabul edilmiştir. Ancak otomatik olmayan yollarla işlenen kişisel verilerin bir veri kayıt sisteminin parçası olmaması halinde Kanun hükümlerinin uygulama alanına dahil olmadığı 6698 sayılı Kanun’un gerekçesinde özel olarak vurgulanmıştır.³⁹⁰ Benzer bir hükme 95/46 sayılı Direktif’in kapsamının düzenlendiği 3. maddesinde de yer verilmiştir.³⁹¹ Yine Direktif ile paralel olarak Kanun, sadece gerçek kişilere ait kişisel verileri koruma altına almakta olup, tüzel kişilere ait verilerin bu Kanun kapsamında sağlanan korumadan faydalanması imkanı bulunmamaktadır. Ancak tüzel kişiye ait olan bir veriden yola çıkılarak gerçek bir kişinin belirlenebilmesi mümkün oluyor ise yine bu verilerin de 6698 sayılı Kanun’un koruma kapsamında olduğu kabul edilmektedir.³⁹²

Kanun’un tamamen veya kısmen kapsamı dışında tutulan hususlara yer veren 28. maddesi ile 6698 sayılı Kanun’un genel uygulanma sınırları belirlenmiştir. Bu maddeye göre;

³⁸⁹ ŞEN, Ersan, “Kişisel Verilerin Korunması Kanunu Tasarısı’nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi”, İstanbul Barosu Dergisi, C. 83, S. 3, 2009, s. 1999.

³⁹⁰ “Bu kapsamda, otomatik olmayan yollarla işlenen kişisel veriler bir veri kayıt sisteminin parçası değilse Kanun kapsamında değerlendirilmeyecektir. Ancak, bu hüküm anılan verilerin kişisel veri niteliğini etkilemeyeceğinden, bu tür verilere ilişkin hukuka aykırı eylemler 5237 sayılı Türk Ceza Kanunu uyarınca suç teşkil etmeye devam edecektir.” 6698 sayılı Kanun Madde Gerekçesi.

³⁹¹ Bu düzenleme 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Regülasyonu’nun 25.05.2018 tarihi itibarıyla uygulanmaya konulmasıyla mülga edilmiş olacaktır. 6698 sayılı Kanun’un, Avrupa Birliği veri koruma hukuku düzenlemeleri ve özellikle 2016/679 sayılı Genel Veri Koruma Regülasyonu (GDPR) ile uyumlu olacak şekilde düzenlenmesi gereken hükümlerinin ayrıntılı değerlendirilmesine ilişkin olarak bkz. KESER BERBER, Leyla, KAYA, Mehmet Bedii, *Türkiye’de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, s. 59-74.

³⁹² KVK Kurumu Yayınları, 6698 Sayılı Kişisel Verilerin Korunması Kanun’unun Amacı ve Kapsamı, s.5. <http://www.kvkk.gov.tr> (08.09.2017).

“ a. Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.

b. Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

c. Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

ç. Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d. Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.” koşullarının gerçekleştiği haller, Kişisel Verilerin Korunması Kanun’un hükümlerinin uygulama alanı dışında tutulmuştur.

Bu noktada Kanun’un uygulama alanı dışında kabul ettiği bu istisnai halleri ve özellikle c., ç. ve d. bentlerinde yer verilen kapsamı belirsiz kavramları içeren halleri nazara aldığımızda,³⁹³ 28. madde hükmüyle Kanun’un uygulama alanının oldukça

³⁹³ “Bunun gibi kişisel verilerin, milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi istisna olarak düzenlenmektedir. Buna göre Milli İstihbarat Teşkilatı ile diğer istihbarat birimlerinin milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik faaliyetler kapsamında işlediği veriler Kanun kapsamı dışında tutulmaktadır. Aynı şekilde belirtilen amaçlarla, suç gelirlerinin aklanması, terörizmin finansmanının önlenmesi ve mali suçların araştırılması konusunda; yetkili birim tarafından yürütülen faaliyetler kapsamında işlenen veriler de bu istisna kapsamındadır. Bu konulardaki yetkili birimin; milli savunmayı, milli güvenliği kamu güvenliğini, kamu düzenini ve ekonomik güvenliği sağlamaya yönelik olmak üzere mali araştırma yapmak, mali istihbarat elde etmek ve üretmek, veri toplamak, şüpheli işlem bildirimleri ve diğer bildirimleri almak, analiz etmek, değerlendirmek, inceleme yapmak ve ilgili kurumlarla paylaşmak suretiyle işlediği veriler de kapsam dışında tutulmaktadır. Ayrıca, kişisel verilerin; soruşturma, kovuşturma, yargılama ve infaz mercileri ile disiplin soruşturma ve kovuşturma makamları tarafından ilgili kanun hükümleri uyarınca işlenmesi de kapsam dışında tutulmuştur.” 6698 sayılı Kanun Madde Gerekeçesi.; Kişisel verilerin korunmasına ilişkin hükümlerin uygulama alanı dışında tutulan; istihbari veya koruyucu faaliyetler kapsamında ve milli savunma, milli güvenlik, kamu düzeni veya ekonomik güvenlik gerekçeleriyle verilerin işlenmesi hallerinde, verilerin işlenmesine gerekçe oluşturan sayılı kavramlar ortak mutabık bir tanımlaması yapılamayan kavramlardır. Dolayısıyla bu kavramların uluslararası

daraltılmış olduğunun altını çizmemiz gerekir.³⁹⁴ Özellikle istisnai hallere ilişkin bu hüküm, Kanun'un kişisel verilerin korunması amacından ziyade, kamu kurum ve kuruluşlarınca kişisel verilerin serbest biçimde işlenebilmesine meşruiyet kazandırma düşüncesiyle hazırlanmış olduğu yönünde düşünce ve eleştirilere sebep olmaktadır.³⁹⁵ Maddenin ikinci fıkrasında da, kısmen Kanun kapsamı dışında kalan hususlar düzenlenmektedir. İkinci fıkra kapsamında getirilen Kanun'un uygulama alanı dışında tutulan istisnai haller ise sadece; *"Kanun'un amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla, veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10. madde, zararın giderilmesini talep etme hakkı hariç ilgili kişinin haklarını düzenleyen 11. madde ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16. madde hükümlerine"* ilişkin olarak uygulanabilir. Bu madde hükümlerinin; kişisel verilerin suç işlenmesi ve suç soruşturması için duyulan ihtiyaç kapsamında işlenmesi, veri öznesi tarafından daha önce alenileştirilmiş olan verilerin işlenmesi, kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için kişisel verilerin işlenmesi ve bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için duyulan gerekçe kişisel verilerin işlenmesi hallerinde uygulanması mümkün değildir. Bu istisnai haller dışında kalan durumlarda kişisel verilerin, Kanun'un öngördüğü temel ilke ve prensiplere uygun olarak işlenip işlenmediğini denetlenmek üzere Kişisel Verilerin Korunması Kurumu ihdas edilmiştir.

2. Kişisel Verileri Koruma Kurumu

6698 sayılı Kanun'un düzenlenmesinde esas alınan 95/46 AT sayılı Direktif ve Türkiye'nin onaylanmasını uygun bularak iç hukukuna dahil ettiği 108 sayılı Avrupa

düzenleme ve içtihatlarla göre çerçevesi belirlenerek, idarenin keyfi uygulamalarının ve özel hayatın gizliliğinin ihlaline yönelik hukuka aykırı müdahalelerinin önü alınmalıdır. KILINÇ, Doğan, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 61, S. 3, 2012, s. 1160; ŞEN, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", s. 1206.

³⁹⁴ DİNÇ, *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye'nin Durumu*, s. 96.

³⁹⁵ "Bu bakımdan, her ne kadar Kanun'un adı "Kişisel Verilerin Korunması Kanunu" olarak öngörülmüş ise de, kanaatimizce kanun koyucu tarafından amaçlanan, kişisel verilere Kurul tarafından kolayca ulaşılması, bu bilgilerin denetlenmesi ve saklanmasıdır." ŞEN, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", 1201.

Konseyi Sözleşmesi ek 181 sayılı Protokol³⁹⁶ ile taraf devletler kişisel verilerin korunmasının etkinliğini sağlayacak bağımsız bir denetim mekanizması oluşturmakla yükümlü tutulmuştur. Bu doğrultuda Kişisel Verilerin Korunması Kanunu'nun 6. bölümü, Kişisel Verileri Koruma Kurum'u ve Teşkilatı'na ayrılmıştır. Bu bölümde uluslararası düzenlemelere uyum sağlayacak bağımsız bir denetim organı teşekkül ettirmek üzere hükümlere yer verilmiştir. Kurum, temel görevleri;³⁹⁷ veri korumasına ilişkin ulusal mevzuata ve iç hukukumuzda dahil edilen bağlayıcılığı uluslararası mevzuatlara aykırılıkların tespiti ve bu hukuka aykırılıklara müdahalede bulunulması, veri sorumlularının denetlenmesi ve yaptırım uygulanması olan bağımsız bir denetim mekanizması olarak düzenlenmiştir. Bu doğrultuda Kişisel Verileri Koruma Kurumu'nun hiçbir kurum veya kuruluştan emir ve talimat almaksızın tam bağımsız olarak görevlerini yerine getirmesi gerekmektedir. Bu denetim organının, veri koruma ilkelerine aykırı her türlü veri işleme faaliyeti karşısında tarafsız ve bağımsız müdahalede bulunabilmesi, aynı zamanda veri koruma ilkelerinin işlev kazanabilmesi ve ülkemizin uluslararası düzenlemelerle öngörülen etkili veri koruma seviyesinin sağlandığı güvenli devlet statüsünü kazanılabilmesi için de önem taşımaktadır.³⁹⁸ Bu doğrultuda bağımsızlık ve tarafsızlığın yalnızca denetime tabi olan makamlara ilişkin olarak değil devlete karşı da sürdürülebilmesi gerekir.³⁹⁹ Devletin, denetim mekanizması üzerinde herhangi bir surette baskı veya dayatmada bulunmasına imkan

³⁹⁶ Taraf devletlerin 108 Sayılı Avrupa Konseyi Sözleşmesi ile öngörülen yükümlülüklerini yerine getirip getirmediğini ve iç hukukta verilerin korunmasına ilişkin aldıkları önlemlerinin Sözleşme ve Protokol ile öngörülen ilkelere ve koruma seviyesine uyumlu olup olmadığını denetlemek üzere bağımsız kontrol organları oluşturulmasını öngören Sözleşmeye ek işbu Protokol yayınlanmıştır. 2004 yılında yürürlüğe giren 181 sayılı Ek Protokol, TBMM tarafından 8 Kasım 2001 tarihinde imzalamış ve 5 Mayıs 2016 tarihli 29703 sayılı Resmi Gazete'de yayımlanarak yürürlük kazanmıştır.

³⁹⁷ Bağımsız denetim organlarının uluslararası düzenlemelere göre yerine getirmesi gereken temel görevleri; araştırma, ihlal karşısında müdahalede bulunma ve dava ve şikayet yetkisini kullanarak sorumluların denetlenmesini sağlamaktır. KÜZECİ, *Kişisel Verilerin Korunması*, s. 274.; Direktif md. 28.

³⁹⁸ KESER BERBER, KAYA, *Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, s. 73.

³⁹⁹ Almanya'da; Kamu kurumları tarafından veri işlemenin denetlenmesi ve kamusal olmayan kurum ve kuruluşlarca gerçekleştirilen veri işlemenin denetlenmesi için farklı makamlar bulunmaktadır. Bu makamlardan ilki federal seviyede bağımsız denetçilerce denetlenirken; özel sektör tarafından veri koruma ilkelerine riayet edilip edilmediğini denetlenme görevine haiz makamlar federal seviyede devlet tarafından denetlenmektedirler. Avrupa Birliği Adalet Divanı, Alman Federal devleti tarafından denetim makamları üzerindeki bu nitelikteki bir denetlemenin gerçekleştirilmiş olması sebebiyle, veri koruma ilkelerine uygunluğu denetlemekle görevli ve 95/46 sayılı Direktif'in 28. maddesi doğrultusunda teşekkül etmiş "tam bağımsız" bir denetim organının bulunmadığı, devletin ilgili madde yükümlülüklerine aykırı hareket ettiği doğrultusunda karar vermiştir. ATAD, Commission v. Germany Davası (C-518/07); ALTINIŞIK, Ulvi (Çev.), "Avrupa Birliği Adalet Divanı'nın C-518/07 Sayılı Veri Koruma Kurumlarının Bağımsızlığına İlişkin Kararı", *Küresel Bakış*, S. 6, 2012, s. 81., 82.

verecek, kurum ve devlet arasında hiçbir bağlantının bulunmamasına bu noktada dikkat edilmesi gerekmektedir. Kişisel Verileri Koruma Kurul'u, Kurum'a bağlı olarak ve 6698 sayılı Kanun'la öngörüldüğü şekilde Kurum'un karar organı olarak görev yapmaktadır. Kurum'un en önemli organı olan Kişisel Verileri Koruma Kurulu'nun üyelerinin seçiminde, yürütme organından bağımsız bir usulün benimsenmemiş olması ise, Kurum'un tam bağımsız bir denetim organı olarak görev yapamayacağı yönündeki eleştirilere sebep olmuştur.⁴⁰⁰ Özellikle kişilerin temel hak ve özgürlük alanına dahil kişisel verilerinin korunmasına ilişkin etkili bir görev yürütmesi gereken böyle bir makamın organlarının seçilmesinde, yürütme organına bağlı kalınmasıyla veri koruma hukukunun evrensel ilkelerine aykırı bir usulün benimsenmiş olduğu doktrinde dile getirilmiştir.⁴⁰¹ Bu noktada getirilen eleştirilere yönelik ve Kurul'un üyelerinin seçimine dair diğer bir görüş de; yürütmekte olduğu görev itibarıyla doğrudan temel hak ve özgürlüklerin korunmasını konu edinen böylesine önemli bir Kurul'un üyelerinin seçiminin, tek bir makama bağlı kalınmaksızın, aday gösteren ve seçim yapan makamların farklı makamlar olmasına da özen gösterilerek, kadrolaşmayı engelleyecek bir usulle yapılması gerektiği şeklindedir.⁴⁰²

Kişisel Verileri Koruma Kurul'unun organlarının seçilmesi usulü dışında, Kurum'un bütçesi bakımından da tam bağımsızlığı sağlamaktan uzak olduğu yönünde eleştiriler dile getirilmektedir.⁴⁰³ Kanun, Kurum'un gelirlerini; “genel bütçeden yapılacak hazine yardımları, Kurum'a ait taşınır ve taşınmazlardan elde edilen gelirler, alınan bağış ve yardımlar, gelirlerinin değerlendirilmesinden elde edilen gelirler ve diğer gelirler” olarak sınırlandırmıştır. Bu gelir türleri arasında; hazine yardımlarına ve Kurum'un aldığı bağış ve yardımlara yer verilmiş olması, özellikle Kurum'un kendi bütçesini oluşturma ve harcamalarını karşılayabilme yetisinin de henüz bulunamadığını düşünürsek, Kurum'un kendisine gelir sağlayan bu kamusal veya özel kurum ve kuruluşlara karşı tam bağımsız ve tarafsız olabilmesi ihtimalini oldukça zayıflatmış olacaktır. Bu eleştiriler doğrultusunda Kişisel Verilerin Korunması Kurum

⁴⁰⁰ “Kurul, dokuz üyeden oluşur. Kurulun beş üyesi Türkiye Büyük Millet Meclisi, iki üyesi Cumhurbaşkanı, iki üyesi Bakanlar Kurulu tarafından seçilir.” 6698 sayılı Kanun md. 21/ 2.

⁴⁰¹ ARSLAN, Çetin, “Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması”, s. 480.

⁴⁰² ŞEN, “Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi”, s. 1212.

⁴⁰³ KESER BERBER, KAYA, *Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, s.70.

ve Kurulu'nun yapılanmasının yeniden gözden geçirilmesi, kanaatimizce ülkemizin uluslararası veri koruma standartlarına tam olarak ayak uydurabilmesi adına önemli bir gerektir.

Kurum'un karar organı olan Kişisel Verileri Koruma Kurulu'nun görevlerine Kanun'da bir kısmı toplu, bir kısmı dağınık olarak yer verilmiştir.⁴⁰⁴ "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" (md. 6) olarak sınırlandırılan özel nitelikli kişisel verilerin işlenmesine ilişkin gerekli ve yeterli önlemin alınması;⁴⁰⁵ kişisel verilerin yurt dışına aktarılmasında, aktarımın yapılacağı ülkedeki ve Türkiye'deki veri sorumlusunca yeterli koruma bulunduğunu yazılı olarak taahhüt etmeleri üzerine kişisel verilerin yabancı ülkeye aktarılmasına izin verilmesi; bunun dışında kişisel verilerin yeterli düzeyde korunacağını öngörüldüğü ülkelerin bir listesinin hazırlanması ve bunun ilan edilmesi (md. 9) Kurul'un temel görevleri arasındadır. Kurul gerek görürse, kişisel verilerin hukuka aykırı yollarla ele geçirildiğine ilişkin veri sorumlularınca yapılan ihbar doğrultusunda haberdar olduğu durumu kendi internet sitesinde veya uygun gördüğü bir başka yöntemle ilan edebilir (md. 12/5.).⁴⁰⁶ İlgili kişiler, Kişisel Verileri Koruma Kanunu'nun uygulanmasıyla ilgili olarak ilgili kişilerin veri sorumlusuna ilettiği taleplerinin süresinde cevaplanmaması veya cevabın yetersiz olması veya reddedilmesi halinde Kurul'a başvurarak konuya ilişkin bir karar verilmesini talep edebileceklerdir.⁴⁰⁷ Kurul, kendisine yapılan başvurular hakkında ancak veri sorumlusuna başvuru yolu tüketilmişse bir karar verilebilecektir (md. 14). Bunun dışında Kurul, ihbar suretiyle veya re'sen haberdar olduğu ihlal iddialarına ilişkin görev alanına giren konularda inceleme yapmak ve inceleme sonucunda bir ihlalin varlığı anlaşılırsa tespit edilen hukuka aykırılığın giderimi için veri sorumlusuna bildirimde bulunmakla görevlidir. Kendisine yapılan başvurularda benzer ihlal

⁴⁰⁴ Kurul'un çalışma usul ve esaslarını, görevlerini, yetkilerini ve sorumluluklarını belirlemek amacıyla, Kurum tarafından Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik hazırlanmış ve 16.11.2017 tarihli ve 30242 sayılı Resmi Gazete'de yayınlanmıştır.

⁴⁰⁵ "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurumu'nun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı için bkz. <http://www.resmigazete.gov.tr> (09.03.2018).

⁴⁰⁶ Bu duruma ilişkin Kurul'un 21.12.2017 tarihinde vermiş olduğu 2017/62 nolu kararı örnek gösterebilmemiz mümkündür.

⁴⁰⁷ Kurum'un Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında hazırlamış olduğu Tebliğ'i 10.03.2018 tarihli 30356 sayılı Resmi Gazetede yayınlanmıştır.

şekillerinin yaygınlaştığını tespit etmişse Kurul, ihlallerin tamamına cevap verecek ilke kararlar alarak ve bu kararları öngördüğü şekilde yayınlayabilmektedir.⁴⁰⁸ İhlalin telafisi güç veya imkansız zarar doğurması ve açıkça hukuka aykırı bulunması halinde, idari yargılama usulünde benimsenmiş olan yürütmenin durdurulması usulüne benzer şekilde, Kurul'un da kişisel verilerin işlenmesinin veya yurt dışına aktarılmasının durdurulmasına ilişkin karar verebilme yetkisi bulunmaktadır.⁴⁰⁹ Kurul'un ihlali gerçekleştiren veri sorumlusuna hiçbir savunma hakkı tanımaksızın ve gerekçe göstermeksizin böyle bir karar verebilecek olmasının, özellikle büyük şirketlerin ticari faaliyetleri gereği verileri transfer etmek veya işlemek zorunda olduğu durumlarda, önemli zararların doğmasına sebep olabileceği kanaatindeyiz. Kurul, Veri Sorumluları Sicili'nin tutulmasına ilişkin gözetim ve sicile kayıt zorunluluğunun istisnalarını düzenleme konularında da yetki sahibidir⁴¹⁰ (md.16). Kurul'a Kanun'da dağınık şekilde yer verilen saymış olduğumuz görevler dışında 22. madde kapsamında da çeşitli görevler yüklenmiştir.⁴¹¹ 6698 sayılı Kanun ve diğer mevzuatla kendisine verilen görevleri kapsamında, ilgili veya üçüncü kişilere ilişkin öğrenmiş oldukları sırların, Kurul üyeleri tarafından kanunen yetkili kılınan merciler dışında açıklaması yasaktır. Kurul üyelerine yüklenen bu sır saklama yükümlülüğü görev süresinin sona ermesinden sonra da devam edecektir (md. 23/4). Üyelerin, bu yükümlülüğe aykırı

⁴⁰⁸ Kurul kendisine yapılan ihbarlar neticesinde haberdar olduğu yaygın bir ihlal probleminin önüne geçebilmek adına; “Bankacılık ve sağlık sektörleri başta olmak üzere birden fazla çalışan ile birlikte bitişik düzende hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik işlemlerinin yapıldığı kuruluşlar ile belediye, vergi ve nüfus ile ilgili işlemler gibi hizmetlerin verildiği kamu ve özel sektör kurum ve kuruluşlarının, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12 nci maddesi uyarınca kişisel verilerin korunması ile ilgili olarak; banko/gişe/masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirlerine yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymasını, görmesini, öğrenmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirlerin alınmasına” şeklinde karar vermiştir. Karar No: 2017/62, T: 21.12.2017.

⁴⁰⁹ “İdari işlemin uygulanması halinde telafisi güç veya imkânsız zararların doğması ve idari işlemin açıkça hukuka aykırı olması şartlarının birlikte gerçekleşmesi durumunda, davalı idarenin savunması alındıktan veya savunma süresi geçtikten sonra gerekçe göstererek yürütmenin durdurulmasına karar verebilirler. Uygulanmakla etkisi tükenecek olan idari işlemlerin yürütülmesi, savunma alındıktan sonra yeniden karar verilmek üzere, idarenin savunması alınmaksızın da durdurulabilir.” İYUK md. 27.

⁴¹⁰ Kişisel Verileri Koruma Kurumu tarafından hazırlanmış olan Veri Sorumluları Sicili Hakkında Yönetmelik (“Yönetmelik”) 30.12.2017 tarihli ve 30286 sayılı Resmi Gazetede yayımlanmış ve 01.01.2018 tarihinde yürürlüğe girmiştir.

⁴¹¹ “Kişisel verilerin temel hak ve özgürlükleri koruyacak şekilde işlenmesi, kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerinin karara bağlanması, Veri Sorumluları Sicilinin tutulmasının sağlanması, kişisel verilerin işlenmesi konusunda gerekli düzenleyici işlemlerin yapılması, kişisel verilerin Kanun'a uygun olarak işlenip işlenmediğinin incelenmesi, idari yaptırımların uygulanması, stratejik planın ve bütçenin kabul edilmesi gibi görevler Kurulun görevleri arasında sayılmaktadır.” 6698 sayılı Kanun Madde Gerekçesi.

davranmaları ise TCK'nın 136. maddesinde düzenlenmiş olan kişisel verileri hukuka aykırı olarak verme veya yayma suçundan cezalandırılmalarını gerektirecektir.

C. Diğer Temel Ulusal Metinlerle Kişisel Verilerin Korunması

Toplumsal düzen içerisinde yaşanan kişilerin, gündelik yaşamlarının tüm alanlarında kişisel verilerinin başkalarıyla paylaşmak zorunda olması, kişisel verilerin korunmasının pek çok hukuk disiplini tarafından güvence altına alınmasını gerektirmiştir. Bu doğrultuda, “*Temel amacı, bireyin özel yaşamının gizliliğinin güvence altına alınması yoluyla kişiyi korumak*”⁴¹² olan kişisel verilerin korunması hakkı, 4721 sayılı Türk Medeni Kanunu'nun 24. ve 25. maddelerinin kişiliğin korunmasına ilişkin sağladığı koruma ile güvence altına alınmıştır.⁴¹³ Kişisel verilerin korunmasına kaynaklık eden “enformasyonel self determinasyon hakkı” uluslararası düzenleme ve içtihadlarda; kişinin, kişisel verileri üzerinde serbestçe tasarrufta bulunarak demokratik bir devlet düzeni içerisinde kişiliğini, maddi ve manevi varlığını özgürce şekillendirebilme ve devam ettirebilme özgürlüğü olarak tanımlanır.⁴¹⁴ “Kişiliğin Korunması” başlığını taşıyan TMK'nın 24. maddesi de; “*Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hakimden, 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 düzenlemesiyle kişilik hakkına yönelik saldırılar karşısında bireylerin şahsiyetinin korunmasına hizmet etmektedir. Türk Medeni Kanunu'nun 25. maddesinde de kişilik haklarına saldırı niteliği taşıyan eylemler karşısında şahsiyetin korunmasına yönelik açılacak olan dava türlerine yer vermektedir.

Kişilerin özel hukuk ilişkileri dolayısıyla, özel hukuk gerçek veya tüzel kişileri ile paylaşmış olduğu kişisel verilerinin bu kişiler tarafından işlenmesini meşru kılan

⁴¹² Yargıtay HGK, E: 2014/4-56, K: 2015/1679, T: 17.6.2015.

⁴¹³ OĞUZ, “Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları Ve Ülkemizdeki Durum”, s. 15.

⁴¹⁴ “Bireyin kendisine ilişkin herhangi bir bilginin, kendi rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılamaması, kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır. Bu husus, bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkına işaret etmektedir.” KILINÇ, Doğan, “Anayasa Mahkemesinin Özel Hayatın Korunmasına İlişkin 2013/1614 Sayılı Kararı Üzerine Değerlendirmeler”, International Journal Of Legal Progress, C.1, S. 2, 2015, s. 197.

çok sayıda kanuni düzenleme arasında öncelikle İş Kanunu'nun ilgili hükümlerinin ele alınması gerekmektedir. 4857 sayılı İş Kanunu'nun 75. maddesine göre işverenin, çalıştırdığı her işçiye ait bir özlük dosyası hazırlama zorunluluğu bulunmaktadır.⁴¹⁵ İşçinin kimlik bilgileri ve kanunla işveren tarafından işçiye ilişkin düzenlenmesi zorunlu bulunan her türlü belge ve kaydın yer aldığı bu özlük dosyalarının talep edildiği zaman yetkililerle paylaşılması da işveren için bir zorunluluk olarak öngörülmüştür. Öngörülen şekilde Kanun'undan aldığı yetkiyle işçinin kişisel verilerini toplayan, depolayan veya üçüncü kişilerle paylaşan iş verenin, bu yetkisini hukuka ve dürüstlük kurallarına uygun olarak yerine getirmesi gerekir. Aksi halde işveren, hem 75. maddenin 3. fıkrasında öngörülen “işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamak” yükümlülüğünü hem de Kişisel Verilerin Korunması Kanunu'nun düzenlemiş olduğu verilerin işlenmesine ilişkin temel esas ve ilkeleri ihlal etmiş olacaktır. Bunun yanı sıra ihlalin niteliğine göre işverenin, 5237 sayılı TCK'nın kişisel verilerinin korunması hukuksal yararını güvence altına alan suç tiplerinden birini de işlemiş olması gündeme gelebilecektir. 4857 sayılı Kanun'la düzenlenmiş olan işverenin, işçinin kişisel verilerini yükümlülük olarak işlemesi ve aktarması dışında, işçi ve işveren arasında kurulan özel sözleşme hükümlerine göre de işçinin kişisel verilerini işleyebilmesi mümkündür. Bu şekilde işçinin, iş verenle imzaladığı iş sözleşmesi hükümlerine göre veya başka herhangi bir şekilde kişisel verilerinin işlenmesine ilişkin rızasının bulunduğunu kabul etmiş olması, işçinin kişisel verilerinin işveren tarafından işlenmesini hukuka uygun kılacaktır. Bunu kişisel verilerin belli işlenme şekillerini suç olarak düzenleyen ceza hukukumuzda, ilgilinin rızası olarak da kabul etmekteyiz.

Kamusal makamlar tarafından, kişisel verilere daha çok kamusal düzenin, refah ve istihdamın sağlanması ve sürdürülmesi gerekçeleriyle ihtiyaç duyulmaktadır. Bu istikamette, ülkemizde kamusal makamlara kişisel verilerin işlenmesi yetkisi veren pek çok hukuki düzenleme mevcuttur.⁴¹⁶ Örneğin; 29.04.2016 tarihi 5490 sayılı Nüfus

⁴¹⁵ İş verenin Kanun'un 75. maddesinde öngörülen işçi özlük dosyalarını düzenlememesi hali, Kanun'un 104. maddesi ile işverene yaptırım uygulanması gereken “işin düzenlenmesine ilişkin hükümlere aykırılık” halleri arasında kabul edilmiştir.

⁴¹⁶ Ancak bu yetkilerin ve kişisel verilerin işlenmesinin sınırlarının, temel hak ve özgürlüklerin sınırlandırılmasına ilişkin Anayasal prensiplere uygun olacak şekilde, kanunlarla öngörülmüş olması gerekir. Anayasa Mahkemesi, E: 2014/74, K: 2014/201, T: 25.12.2014.; Anayasa Mahkemesi, E: 2006/167, K: 2008/86, T: 20.03.2008.

Hizmetleri Kanunu 1. maddesinde; kanunun amacının *“kişinin doğumundan ölümüne kadar kişisel ve medeni durumuna, uyrukluğuna ve bunlarda meydana gelebilecek değişikliklere ait doğal ve hukuki olayların belirlenip saptanması, bu amaçla düzenlenmiş kütüklere yazılması, elektronik ortamda ulusal adres veri tabanının oluşturulması, nüfus kayıtları ile adres bilgilerinin ilişkilendirilmesini sağlamak”* olduğu ifade edilmiş ve bu amaç istikametinde vatandaşların kişisel verileri niteliği taşıyan bilgileri nüfus kütüklerinde kayıt altına alınmaktadır.⁴¹⁷ 5490 sayılı Kanun’la aynı yıl yürürlük kazanmış olan 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu’nun 23. maddesi de üye işyerlerine, kart hamillerine ilişkin kart kullanımı sonucu öğrenmiş oldukları bilgileri özel olarak koruma yükümlülüğü getirmiştir. İşyerlerinin, bu yükümlülüğe aykırı davranması ise 39. madde düzenlemesi ile adli para cezası ve/veya hapis cezası yaptırımına bağlanmıştır. Bunun dışında kişilere ait; *“kesinleşmiş ceza ve güvenlik tedbirlerine mahkûmiyete ilişkin bilgilerin otomatik işleme tâbi bir sistem kullanılarak toplanmasına, sınıflandırılmasına, değerlendirilmesine, muhafaza edilmesine ve gerektiğinde en seri ve sağlıklı biçimde ilgililere bildirilmesine dair usul ve esaslar”*⁴¹⁸ Adli Sicil Kanunu’nun düzenlenme amaç ve kapsamını oluşturmaktadır. Bu düzenlemelere göre kamu yararının sağlanmasına yönelik belli amaçlar doğrultusunda, kamusal organlar her ne kadar verileri işleme konusunda kanunen yetki sahibi kılınmışsa da, bu yetkinin 6698 sayılı Kişisel Verilerin Korunması Kanununda öngörülen kişisel verilerin işlenmesine ilişkin genel esaslar ve ilkeler doğrultusunda kullanılması gerekmektedir. Aksi halde bu kurum veya kuruluşların hukuka uygun bir veri işleme faaliyetinin gerçekleştirildiğini söyleyemeyiz.

Kişisel verilerin, kamusal makamlarca hukuka uygun olarak işlenmesi sırasında veya görevi gereği başka herhangi bir şekilde, kamusal personel tarafından öğrenilmiş olması halinde özel olarak korunması gereğiyle oluşturulmuş ve kişisel verilerin korunması amacına da hizmet eden yerel mevzuatımızda pek çok hüküm bulunmaktadır.⁴¹⁹ Bu düzenlemeler arasında öncelikli olarak 213 sayılı Vergi Usul Kanunu’nun “vergi mahremiyeti” başlığı taşıyan 5. maddesini değerlendirmek

⁴¹⁷ Nüfus Hizmetleri Kanunu’nun 9. maddesi ile nüfus kayıtlarının ve kayıtların tutulmasına dayanak oluşturan belgelerin gizliliği güvence altına alınmıştır.

⁴¹⁸ 5352 sayılı Adli Sicil Kanunu md. 1.

⁴¹⁹ 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun md. 22.; 6698 sayılı Kişisel Verilerin Korunması Kanunu md. 23/ 4.

gerekecektir. Kişilerin ekonomik ilişkilerine ilişkin pek çok verisini kamusal makamlarla, usulüne uygun bir vegilendirme için paylaşması zorunluluğu bulunmaktadır. Bu doğrultuda paylaşımda bulunulan kişilerin, yani kamusal personelin; *“görevleri dolayısıyla, mükellefin ve mükellefle ilgili kimselerin şahıslarına, muamele ve hesap durumlarına, işlerine, işletmelerine, servetlerine veya mesleklerine mütaallik olmak üzere öğrendikleri sırları veya gizli kalması لازمگelen diğer hususları”* başka insanlara aktarmaları, kendilerinin veya üçüncü kişilerin yararına kullanmaları 213 sayılı Kanun’un 5. madde düzenlemesi ile yasaklanmıştır. Bu düzenlemeyle, kişilerin vergi mahremiyeti kapsamında korunması gereken bilgileri arasında kişisel veri niteliği taşıyanlarına ilişkin de koruma sağlanmış olacaktır. Bunun dışında VUK madde 5’e benzer bir düzenlemeye 6183 sayılı Amme Alacaklarının Tahsili Usulü Hakkında Kanun’da “sırrın ifşası” olarak yer verilmiştir. Sır veya mahremiyet gibi tanımlanması güç kavramların kapsamına nelerin dahil olduğunun sayılması usulü benimsenerek, bu Kanun’ların ilgili hükümlerine açıklık getirilmeye çalışılmıştır.⁴²⁰ 213 sayılı ve 6183 sayılı Kanun’ların ilgili hükümleriyle sınırlandırılmış olan, sır veya mahrem kabul edilen ve kişisel veri niteliğinin de taşıyan bu bilgiler, yine Kanun’larda sayılmış kişi veya kişilerce ve görevleri gereği öğrenilmiş olunması halinde korunmaktadır. Bunun dışındaki ihtimallerde ise kişisel verilerin korunmasına ilişkin genel hükümlere yer veren 6698 sayılı Kişisel Verilerin Korunması Kanun’u ve 5237 sayılı Türk Ceza Kanunu’na başvurmak gerekecektir.

Son olarak; “içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenleme” amacı ile hazırlanmış olan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun kapsamında da kişisel verilerin işlenmesi ve korunmasına ilişkin çeşitli hükümlerin yer aldığını görmekteyiz. Özellikle Kanun’un erişimin engellenmesi usulü ile kişisel verilerin korunması arasında özel olarak bağlantılı olan hususların bulunmakta olduğunu söylemeliyiz.⁴²¹

⁴²⁰ K. DURMUŞ, “Ticari Sırların ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti”, s. 374.

⁴²¹ KESER BERBER, KAYA, *Türkiye’de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, s.53.; Ayrıca konunun kişisel verilerin korunmasına ilişkin temel ilkelerle olan ilişkisi bkz. s. 34.

III. TÜRK CEZA MEVZUATINDA KİŞİSEL VERİLERİN KORUNMASI

Suçların, cezaların ve güvenlik tedbirlerinin düzenleme altına alındığı 5237 sayılı Türk Ceza Kanunu'nun ve "*ceza muhakemesinin nasıl yapılacağı hususundaki kurallar ile bu sürece katılan kişilerin hak, yetki ve yükümlülüklerini*" düzenleyen 5271 sayılı Ceza Muhakemesi Kanunu'nun Türk ceza mevzuatının temel düzenlemeleri olarak, kişisel verilerin korunmasına ilişkin hükümleri çalışmamızın bu kısmında ele alınacaktır. Kişisel verilerin suç ve cezalarla bağlantılı olarak işlenmesi farklı düzenlemelere konu edilmişse de çalışmanın bu kısmında daha ziyade Türk Ceza Kanunu'nun "*özel hayata ve hayatın gizli alanına karşı suçlar*" başlığı altındaki dokuzuncu bölümünde yer verilen kişisel verilerin hukuka aykırı olarak işlenmesine ilişkin öngörülmüş suç tipleri incelenmiştir. Özel hayatın gizliliğinin korunması veya özel hayata saygı gösterilmesi hem insan haklarına ilişkin temel uluslararası düzenlemeler, hem de ulusal düzenlemelerle güvence altına alınmış temel bir kişilik hakkıdır. Bu hakkın farklı şekillerde ihlal edilebilir olması dolayısıyla kanun koyucu farklı suç tipleri düzenleyerek, bu fiilleri ceza yaptırımına bağlamıştır.⁴²²

Anayasa Mahkemesi de kişisel verilerin korunması hukuksal yararının, özel hayat alanıyla olan bağlantısını, mahremiyet hakkı temelinde; "Özel yaşama saygı hakkı kapsamında korunan hukuksal çıkarlardan biri de bireyin mahremiyet hakkıdır. Ancak mahremiyet hakkı sadece yalnız bırakılma hakkından ibaret olmayıp, bu hak bireyin kendisi hakkındaki bilgileri kontrol edebilme hukuksal çıkarını da kapsamaktadır. Bireyin kendisine ilişkin herhangi bir bilginin, kendi rızası olmaksızın açıklanmaması, yayılmaması, bu bilgilere başkaları tarafından ulaşılamaması ve rızası hilafına kullanılamaması, kısaca bu bilgilerin mahrem kalması konusunda menfaati bulunmaktadır. Bu husus, bireyin kendisi hakkındaki bilgilerin geleceğini belirleme hakkına işaret etmektedir." şeklinde açıklamıştır. Bu itibarla, kişilerin kendilerine

⁴²² "Özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Orada cereyan edenlerin yalnız kendisi veya kendisinin bilmesini istediği kimseler tarafından bilinmesini istemek hakkı, kişinin temel haklarından biridir. Bu niteliği sebebiyledir ki, özel hayatın gizliliğine dokunulmaması, insan haklarına ilişkin beyanname ve sözleşmelerde korunması istenilmiş, ayrıca tüm demokratik ülke mevzuatında açıkça belirlenen istisnalar dışında bu hak devlet organlarına, topluma ve diğer kişilere karşı korunmuştur. İnsanın mutluluğu için büyük önemi olan özel hayata saygı gösterilmesi hakkı onun kişiliği için temel bir hak olup yeteri kadar korunmadığı takdirde kişilerin ve dolayısıyla toplumun kendini huzurlu hissedip güven içinde yaşaması mümkün değildir. Bu nedenlerle söz konusu gizliliği çeşitli biçimde ihlal eylemleri suç sayılarak ceza yaptırımlarına bağlanmıştır." Anayasa Mahkemesi, E: 1986/24, K: 1987/8, T: 31.3.1987.

ilişkin bilgileri kontrol edebilme, daha özel anlatımla kişisel verilerinin hukuka aykırı kullanımı, toplanması, işlenmesi veya aktarılması karşısında irade sergileyebilme özgürlüğünün özel hayat kapsamında korunması gerektiği şüphesizdir. Dolayısıyla kişilerin verileri üzerindeki tasarruf hakkının korunması pek çok hukuki düzenlemeyle güvence altına alınmıştır. Ancak günümüzde kişisel verilerin bilgisayar ortamlarıyla işlenmesinin yaygınlaşması karşısında, bu hakka yöneltilen tehlikenin boyutları da giderek artmaktadır. Kişisel verilerin hukuka aykırı olarak işlenmesine ilişkin ihlallerin boyutlarının bu şekilde giderek artmakta olası ve kişisel verilerin diğer hukuk dallarınca yeterince korunamaması gerçeği kişisel verilerin ceza hukuku yoluyla korunması zorunluluğunu ortaya çıkarmıştır.⁴²³ Dolayısıyla 765 sayılı Türk Ceza Kanun'un doğrudan korunma ihtiyacı duymadığı kişisel verilerin hukuka aykırı olarak işlenmesine ilişkin eylemler, 5237 sayılı Türk Ceza Kanunu kapsamında suç olarak düzenlenmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanunu da kişisel verilere ilişkin işlenen suçlar bakımından 5237 sayılı Türk Ceza Kanunu'na atıf yapmaktadır.⁴²⁴ Mukayeseli hukuklarda da kişisel verilerin korunması çeşitli hüküm ve yaptırımlarla ceza hukuku düzenlemelerine konu edilmiştir.⁴²⁵

Ceza hukukunda suç sebebiyle yapılan yargılamanın usulünü ceza muhakemesi hukuku düzenler. Ceza usul hukukunun konusunu ise; kişilerin bir suçu işleyip işlemediğinin belirlenme şekli ve ne şekilde yargılama yapılarak ceza verileceği usulü

⁴²³ ÜNVER, Yener, “TCK ve CK Tasarısının İnternet Açısından Değerlendirilmesi”, s. 94.

⁴²⁴ 5237 sayılı Türk Ceza Kanunu'nun kişisel verilere ilişkin suçları düzenleme altına aldığı 135 ila 140 ncı madde hükümleriyle, bu suçları işleyen kişiler hakkında hapis cezası uygulanacağı öngörülmüştür. Kişisel verilere karşı işlenen bu suçlarda özgürlüğü bağlayıcı cezaların yaptırım olarak uygulanacağına ilişkin düzenleme eleştirmektedir. Bu eleştirilere göre; “ticari ve ekonomik konularda getirilen bu tür hürriyeti bağlayıcı cezalar, gerek Türk ve yabancı yatırımcıların ilgili ticari konuyu riskli olarak değerlendirerek yatırımlarını farklı alanlara ve hukuk ikliminin yabancı yatırımcı için cazip olduğu ülkelere kaydırmasına olabilecektir.” ve bu suçları işleyenlere hapis cezası yerine para cezası yaptırımının uygulanmasının yabancı sermaye ve yatırımlar açısından teşvik edici olabilecektir. KESER BERBER, KAYA, *Türkiye’de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, s. 71; Kanaatimizce de mukayeseli hukuklarda kişisel verilere ilişkin suçlara karşılık öngörülen hapis ve adli para cezasının seçenek yaptırım olarak öngörülmesi yerinde olabilir.

⁴²⁵ Fransa ve Belçika’da kişisel verilerin hem taksirle hem de kasten işlenmesi suç olarak düzenlenmişken, kişisel verilerin AB dışında herhangi bir ülkeye transferi de özel olarak cezalandırılmaktadır. İngiltere kişisel verileri koruma kanunu (Data Protection Act) kişisel verilerin ele geçirilmesini, satılmasını, satış amaçlı reklama konu edilmesini suç olarak düzenlemiştir. İsviçre’de ise kişisel verilerin ele geçirilmesi veya kamu görevlilerince ifşa edilmesi İsviçre Ceza Kanunu’nun 179. maddesiyle hapis veya para cezası yaptırımına bağlanmıştır. AKYÜREK, Güçlü, “Kişisel Veriler ve Özel Hayatın Gizliliği Hakkı”, Suç ve Ceza Dergisi, S. 3, 2011, s. 51.; Kişisel verilere karşı işlenen bu suç tipleri karşısında, ülke düzenlemelerinin pek çoğunda para cezası yaptırımının uygulanması tercih edilmektedir.

oluşturmaktadır.⁴²⁶ Soruşturma ve kovuşturma gibi iki temel evreden oluşan ceza muhakemesinde, suç izlerinin araştırılması, ipucu aranması ve bu vasıta ile suç işleyen kişiye ulaşılmaya çalışılması soruşturma evresinde re'sen gerçekleştirilen işlemlerdendir.⁴²⁷ Bu işlemlerin konusunu ise genellikle suçun mağduru veya şüpheliye ilişkin kişisel veriler oluşturmaktadır. Türk Ceza Muhakemesi Kanunu, kişisel verilerin işlenmesini zorunlu olarak gerektiren, suç işlendiğini ispata yarayan bu işlemlerin kim tarafından, hangi koşullarla ve ne zamana kadar gerçekleştirilebileceğini ve işlenen verilerin yok edilmesine ilişkin koşulları düzenleyerek kişisel verilerin korunmasına hizmet etmektedir.

Çalışmanın bu kısmında, öncelikle kısaca ceza muhakemesi hukukunda kişisel verilerin işlenmesini gerektiren soruşturma veya kovuşturma işlemlerinin neler olduğu ve kişisel verilerin hangi usullerle elde edildiğine daha sonrada kişisel verilere karşı işlenen suç tiplerinin suç inceleme metodolojisine uygun incelemesine yer verilmiştir.

A. Ceza Muhakemesi Kanunu'nun Kişisel Verilere İlişkin Hükümleri

Bir toplum içerisinde yaşayan bireylerin, günlük yaşam içerisinde karakteristik davranışlarının, hareketlerinin, alışveriş eğilimlerinin, telefon konuşmalarının, parmak izinin, fotoğrafının ve hatta DNA analizi verileri gibi kişisel verilerinin toplanması veya saklanması veya başka surette işlenmesine ilişkin rıza göstermesinin en önemli dayanaklarından birisi toplumsal veya bireysel güvenliğinin sağlanmasıdır. Günümüzde, kamusal güvenliğin sağlanması ve kamuyu tehlike altında bırakacak eylemler karşısında önleyici tedbirlerin etkin şekilde alınabilmesi veya kişilerin kendilerini bir suç şüphesi altında kalmaktan kurtarabilmesi adına konum bilgileri, telefon sinyalleri, PNR numaraları gibi kişisel verilerinin işlenmesi makul görülebilmekte ve hatta kişiler gönüllülükle bu işlemlere katılım gösterebilmektedir.⁴²⁸ Ceza muhakemesi hukukunda da bahsettiğimiz amaçlar ekseninde özellikle toplumsal açıdan tehlikelilik arz eden kişilerin tespiti, ele geçirilmesi ve asayişin korunması adına suç mahalli veya bedenden örnek alınması ve incelenmesi, telefon dinlemeleri veya

⁴²⁶ CENTEL, Nur, ZAFER, Hamide, *Ceza Muhakemesi Hukuku*, 12. Baskı, İstanbul, Beta Basım, 2015, s. 3.

⁴²⁷ YENİSEY, Feridun, NUHOĞLU, Ayşe, *Ceza Muhakemesi Hukuku*, İstanbul, Bahçeşehir Üniversitesi Yayınları, 2014, s. 324.

⁴²⁸ KÜZECİ, *Kişisel Verilerin Korunması*, s. 55.

sinyal bilgilerinin tespiti gibi önleyici veya adli amaçlı işlemler vasıtasıyla kişisel veriler işlenmektedir.

Bu aşamada ceza muhakemesi hukukunda kişisel veriler, suç işlenmesinin önlenmesine yönelik bazı önleyici kolluk faaliyetleri kapsamında veya bir suç işlendiğine ilişkin halin soruşturma makamlarınca öğrenilmesiyle başlayan araştırma yükümlülüğü ve maddi gerçeğin ortaya çıkartılması amacıyla delil toplanması kapsamında işleme konusu yapılabilmektedir. Bu surette ceza muhakemesi hukuku kapsamında kişisel verilerin işlenmesinin, ceza muhakemesinin ana amacı olan maddi gerçeğin ortaya çıkarılmasına ve suçla ilgili önemli delillerin elde edilmesine hizmet etmekte olmasının yanında; özel hayatın gizliliği, kişisel verilerin korunması ve beden ve vücut dokunulmazlığı gibi temel kişilik haklarına ilişkin önemli bir müdahale niteliği taşıdığı da şüphesizdir.⁴²⁹

Önleyici kolluk faaliyetleri kapsamında; kolluk görevlilerince istihbarat amacıyla veya ruhsat, ehliyet ve sair belgenin verilmesinin ön koşulu olarak kişilerle ilişkili kişisel veri niteliğindeki bilgilerin bir sistem üzerinde işlenmesinin koşulları 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nda düzenlenmiştir. Kanun'un özellikle *“parmak izi ve fotoğrafların kayda alınması”* başlıklı 5. maddesi kolluğa, kişilerin; *“her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge”* alabilme talebiyle başvurmuş olması, genel veya özel kolluk veya özel güvenlik görevlisi olarak işe başlamış olması, Türk vatandaşlığına başvurmuş veya sığınma talebinde bulunmuş olması, gözaltına alınmış olması veya rızasıyla paylaşımda bulunmayı talep etmesi hallerinde parmak izi, kimlik bilgileri ve resimlerinin özgü bir sisteme kaydedilmesi yetkisi vermektedir. Bu yetki kapsamında parmak izi, kimlik bilgileri ve fotoğraf gibi kişisel verilerin kayıt altına alınması, vatandaşlar üzerindeki devlet gözetimin en etkin uygulanma biçimlerinden biri olarak görülmektedir.⁴³⁰ Kanun, her ne kadar bu verilerin kullanılma amacına ve gizliliğine ilişkin devam eden fıkralarda, yeterli korumayı sağlamaya yönelik sınırlamalara yer vermişse de, herhangi bir suç şüphesi altında dahi bulunmayan kişilere ait parmak izi ve fotoğraf gibi önemli kişisel verilerin ancak *“kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden*

⁴²⁹ DAĞ, Güray, *Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması*, (Yayınlanmamış Doktora Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2011, s. 294.

⁴³⁰ KARAKEHYA, “Gözetim ve Suçla Mücadele”, s. 343.

itibaren seksen yıl geçtikten sonra” sistemden silinebileceği şeklindeki hükmün de kişisel verilerin korunması hakkına yönelik ölçsüz müdahalelere zemin yaratılmış olduğu kanaatindeyiz.

Kamusal güvenliğin sürdürülmesine ve tehlikeliliğin önlenmesine yönelik kolluk tarafından yürütülen istihbari faaliyetler kapsamında da kişisel verilerin toplanması, işlenmesi ve paylaşılması söz konusu olabilmektedir. Kolluğun gelecekteki tehlikeli bir durumu engelleyebilmesi, önleyebilmesi amacı doğrultusunda tedbir alması; kişisel verilerin elde edilmesini, saklanması, aktarılmasını, karşılaştırılmasını veya bunlardan yararlanılmasını ifade eder.⁴³¹ Önleme amaçlı durdurma ve kimlik sorma faaliyeti kapsamında (PVSK md. 4)⁴³², önleme amaçlı gerçekleştirilen arama kapsamında (PVSK md. 9) ve 2559 sayılı Kanun’un 13. maddesine 02.01.2017 tarihinde dahil edilen “kayıp çocukların araştırılması” başlıklı ek 13/A maddesi kapsamında kolluk, kamusal güvenliğin istikrarı amacı doğrultusunda kişisel verileri işlemektedir. Özellikle kayıp çocukların bulunması amacıyla ve sulh ceza hakiminin veya gecikmesinde sakınca bulunan hallerde mülki amirin yazılı veya daha sonra yazılı hale getirmek üzere sözlü emriyle, kolluğun kayıp çocuğa ait banka hesaplarının hareketlerine, telekomünikasyon yoluyla yapılan iletişimine ve sinyal bilgilerine ulaşabilmesi kapsamında çocuğun kişisel verileri işleyebilme yetkisi ilgilinin menfaatine hüküm ve sonuç doğurmaya elverişli önemli bir düzenlemedir.⁴³³

Kişisel verilerin, suç işlenmesinin önlenmesinde olduğu gibi, suçların soruşturulması veya kovuşturulması sırasında kanuna uygun olarak işlenebilmesi

⁴³¹ “Kolluk görevlileri önleyici hizmetleri yerine getirmek için araştırma yapacak, bil-belge-doküman toplayacak, yaptığı araştırma neticesinde elde ettiği bulguları işleme tabi tutarak suçun önlenmesine yönelik istihbarat elde etmiş olacaktır.” KARABULUT, Ramazan, *Kişisel Verilerin Korunması ve Kolluk Hizmetleri*, (Yayınlanmamış Yüksek Lisans Tezi), Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Diyarbakır, 2014, s. 102.

⁴³² “Kolluğun, “kimlik sorma” ile “kimlik tespit etmesi” kurumları birbirinden esasen farklı işlemlerdir. Kimlik sorma işlemi sırasında kimliği sorulan kişi kayıtlara geçirilemezken, kimlik tespit etme işlemi, bir kişinin kayıtlara geçirilmesi söz konusudur.” ERDAĞ, Ali İhsan, “Kolluğun “Durdurma ve Kimlik Sorma” Yetkisi (PVSK madde 4/A)”, Ankara Barosu Dergisi, S. 4, 2010, s. 45.

⁴³³ Bu maddenin gereğine uygun olarak kişisel verilerin işlenmesinin aynı zamanda 6698 sayılı Kanun’un 5. maddesinde sayılan veri öznesinin rızası aranmaksızın kişisel verilerin hukuka uygun işleme halleri arasında sayılan; “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.” haliyle de ilişkilendirilebileceğini düşünmekteyiz.

mümkündür.⁴³⁴ Bu evrelerde kişisel verilerin işlenmesini hukuka uygun kılan temel koşullara, Türk Ceza Muhakemesi Kanunu'nun çeşitli maddelerinde yer verilmiştir. Ceza muhakeme usulünde soruşturma ve kovuşturma evreleri birbirlerini takip eden evrelerdir.⁴³⁵ Her iki evre hem kendi içerisinde hem de bir diğer evreye geçilmesinde, şüpheyi daha çok kuvvetlendirmeyi sağlayacak veya tamamen yok edecek delillerin ele geçirilmiş olmasıyla ilerleme kat edebilmektedir. Yani ceza muhakemesinde hakimin bir hükme varmasının, maddi meseleyi çözmesinin temel koşulu delillerin bize gösterdiği gerçeği doğru tahlil edebilmekten geçer.⁴³⁶ Beyan ve belirti delilleri olarak genel anlamda kabul gören, delillerin tasnifine ilişkin ayrıma göre; kişisel verileri daha ziyade belirti delili olarak görmekte olduğumuzu söyleyebiliriz. Belirti delilleri de kendi içerisinde eşyaya veya şahsa ait olmak üzere iki grup altında incelenirler.⁴³⁷ Şahsa ait belirtiler daha ziyade şahsa ilişkin olduklarından konumuzu oluşturan kişisel verilerin de daha çok bu delil grubu altında ele alındığını söyleyebiliriz. Ancak eşyaya ait belirti delillerinin de bir kişi ile ilişkilendirilebilmesi mümkünse kişisel veri olarak kabul edilebileceği şüphesizdir. Örneğin; soruşturma aşamasında iletişimin dinlenilmesi veya teknik araçla izleme tedbirine başvurularak elde edilmiş olan ses ve görüntünün suçu işleyen kişinin veya üçüncü bir kişinin belirlenmesine imkan sağlaması halinde, bu kişilere ait kişisel veri olarak kabul edilmesi gerekir. Bunun dışında olay mahallinde bulunmuş eşyaya ait bir belirti delilinin de analiz edilmesiyle kişisel bir veri elde edilmesi söz konusu olabilecektir.⁴³⁸ Örneğin; suç mahallinde bulunan ve suçun işlenmesinde kullanılan silaha ait merminin bir belirti delili olduğu ve eşyaya ilişkin olduğu şüphesizdir.⁴³⁹ Bu merminin, balistik incelemesi neticesinde hangi silahtan çıkmış olduğunun veya silahın ruhsat sahibinin

⁴³⁴ GÖNEN, Serkan, ULUS, Halil İbrahim, YILMAZ, Ercan Nurcan, "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme", Bilişim Teknolojileri Dergisi, C. 9, S. 3, 2016, s. 233.

⁴³⁵ ÖZTÜRK, Bahri, *Uygulamalı Ceza Muhakemesi Hukuku*, Ankara, Ankara Üniversitesi Basımevi, 1991, s. 26.

⁴³⁶ YENİSEY, NUHOĞLU, *Ceza Muhakemesi Hukuku*, s. 183.

⁴³⁷ Örneğin; şüpheli veya sanığın kan grubu, parmak izi ve hatta suç sırasında veya sonrasındaki ruh hali belirti delilleri olarak kabul edilmektedir. YENİSEY, NUHOĞLU, *Ceza Muhakemesi Hukuku*, s. 213.

⁴³⁸ TEKİN, Nurullah, "Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi", Uyuşmazlık Mahkemesi Dergisi, S. 4, 2014, s. 246.

⁴³⁹ Eşyaya ilişkin belirti delilleri arasında ; suçun işlenmesinde kullanılan tabanca bıçak gibi araçlar veya sahte para gibi suçun işlenmesiyle ele geçirilen eşya veya fren izi gibi suçun işlenmesi sırasında oluşan belirtiler yer almaktadır. YENİSEY, NUHOĞLU, *Ceza Muhakemesi Hukuku*, s. 213.

belirlenmesine imkan vermesi halinde kişiyle ilişkilendirilebilir bir veri olduğunu söyleyebiliriz.

Ceza muhakemesi usulünde özellikle belirti delillerinin doğru tahlil edilebilmesi, muhakeme hukukunun asıl amacı olan maddi gerçeğin ortaya çıkarılabilmesi açısından hayati öneme sahiptir. Dahası doğru şekilde değerlendirebildiğimiz takdirde bu deliller bize olayın gerçekte nasıl gerçekleşmiş olduğunu en tarafsız şekilde anlatabilecek delillerdir. Eşyaya veya kişiye ilişkin olabilen bu belirti delillerini değerlendirmede, yargılama mercilerinin bilirkişi veya keşif gibi yardımcılara da başvurabilmesi mümkündür.⁴⁴⁰ Türk Ceza Muhakemesi Kanunu her ne kadar bu yöntemlere başvurulmasını takdiri olarak düzenlemiş olsa da, belli konulara ilişkin ihtilafın çözümünde bilirkişi incelemesinin yapılması zorunlu tutulmuştur. Bilirkişi incelemesine zorunlu başvurularak mağdur, şüpheli/sanık veya 3. kişiyle ilişkili kişisel verilerin elde edilmesini, işlenmesini ve adli mercilerle paylaşılmasını gerektiren Türk Ceza Muhakemesi Kanunu’nun 74. ila 89. maddeleri arasında düzenlenmiş olan bu haller; şüpheli veya sanığın akıl sağlığının yerinde olup olmadığının incelenmesi (md. 74), şüpheli veya sanığın ve diğer kişilerin beden muayenesi ve vücudundan örnek alınması (md. 75-77), moleküler genetik incelemeler (md. 78)⁴⁴¹ ve otopsi (md. 87) yapılmasını gerektiren hallerdir.⁴⁴² Bunun dışında CMK’nın 81. maddesi ve PVSK’nın Ek 6. maddesinde düzenlenmiş olan teşhis veya fiziki kimliğin tespiti işleminin yerine getirilmesi sırasında da şüpheli veya sanığa ait “fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri” gibi kişisel veriler kayıt altına alınarak, soruşturma dosyasında saklanmaktadır.

Ceza muhakemesinde, kişisel verilerin konu edinildiği diğer bir muhakeme aracı ise koruma tedbirleridir. Koruma tedbirlerine; muhakeme usulünde kesin bir hükmün kurulmamış olduğu evrede, “*muhakemenin yapılabilmesini sağlamak ve/veya*

⁴⁴⁰ CENTEL, ZAFER, *Ceza Muhakemesi Hukuku*, s. 273.

⁴⁴¹ CMK’nın 80. maddesi; şüpheli veya sanığın ve diğer kişilerin beden muayenesi ve vücudundan örnek alınması ve moleküler genetik inceleme yapılması sonucunda elde edilen bilgilerin kişisel veri olduğunu ve başka bir amaçla kullanılması yasağını hüküm altına almıştır. Ayrıca maddenin ikinci fıkrası ile kişisel veri niteliğindeki bu bilgilerin “*kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde*” derhal yok edileceği düzenlenmiştir.

⁴⁴² “CMK’nın 75 ve 76’ncı maddelerine göre şüpheli, sanık ya da mağdurdan alınan kan veya benzeri biyolojik örnekler ile saç, tükürük, tırnak örnekleri; 78’inci maddeye göre bu örnekler üzerinde yapılan moleküler genetik inceleme sonuçları kişisel veri niteliğindedir.” ŞENER, Gülnihal, “Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu”, *Adalet Dergisi*, S. 39, 2011, s. 75.

verilecek kararın kağıt üzerinde kalmasını önlemek ve/veya delil temin veya muhafaza etmek”⁴⁴³ amacıyla başvurulmaktadır. Kişisel veri niteliği taşıyan delillerin elde edilmesi neticesi yaratan veya kişisel verileri konu edinen Türk Ceza Muhakemesi Kanunu’nun düzenlediği koruma tedbirleri ise; şüpheli, sanık veya diğer kişilerin üst, eşya, konut veya ona ait yerlerin aranması (md. 116-122), ispat aracı olarak faydalı olacağına inanılan eşya veya kazanca elkonulması (md. 123), somut delile dayalı kuvvetli şüphe sebepleri altında şüpheli veya sanığa ait taşınmaz, hak ve alacaklara elkonulması (md. 128), “bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma” (md. 134), telekomünikasyon yoluyla yapılan iletişimin denetlenmesi (md. 137-138)⁴⁴⁴, kamu görevlilerinin gizli soruşturmacı olarak görevlendirilmesi (md. 139)⁴⁴⁵, şüpheli veya sanığın kamuya açık yerlerde ve işyerlerinde teknik araçla izlenmesi ve görüntü kaydı alınmasıdır (md.140). Bu tedbirlerin uygulanması sırasında veya sonrasında; şüpheli veya sanığa ait telekomünikasyon yoluyla iletişiminin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirmesiyle elde edilen içerikler; görevlendirilmiş gizli soruşturmacının elde ettiği suçla bağlantısı bulunmayan kişisel bilgiler ve teknik araçla izleme yapılarak ele geçirilen kovuşturma bakımından gerekli olmayan kişisel veri niteliğinde de olabilecek olan bu delillerin, öngörülen süreler içerisinde veya derhal yok edilmesi Türk Ceza Muhakemesi Kanunu ile güvence altına alınmıştır. Kanun’da yer alan, koruma tedbirlerinin uygulanmasıyla elde edilen delillerin yok edilmesinin öngörüldüğü bu düzenlemeler ve tedbirlerin süresine ilişkin sınırlandırıcı hükümler, uygulanan tedbirlerle kişilerin özel yaşamlarına ve kişisel verilerin korunması hakkına doğrudan yapılan müdahalenin hukuka uygunluğunun sağlanmasına hizmet etmektedir.⁴⁴⁶ Hukuka aykırı olarak uygulanan koruma tedbirleri sonucunda elde

⁴⁴³ ÖZTÜRK, Bahri, *Ceza Muhakemesi Hukuku*, 11. Baskı, Ankara, Seçkin Yayınları, 2017, s. 443.

⁴⁴⁴ Mukayeseli hukukta da yaygın bir şekilde düzenleme konusu yapılmış olan, telefon dinlemeleri vasıtasıyla delil elde etme aracının sağlıklı sınırlar içerisinde tutulmasını sağlamak adına üç ana kuralla ihtiyaç duyulmuştur. Bunlar; orantılılık, vazgeçilmezlik yani başka surette delil etme olanağının bulunmaması ve kanuna uygunluk diğer bir söylemle bir hakimin karar vermiş olmasıdır. PRADEL, Jean, Çağdaş Sistemlerde Karşılaştırmalı Ceza Usulü, Çev. Sulhi Dönmezer, Beta Basım, İstanbul, 2000, s. 171.

⁴⁴⁵ “CMK md. 139/4’de gizli soruşturmacının kişisel veri toplayabilip toplayamayacağı düzenlenmemiştir. Ancak, CMK. md. 139/6’ya göre; gizli soruşturmacı görevlendirilmesi suretiyle elde edilen kişisel bilgilerin, bu gizli soruşturmacının görevlendirildiği ceza soruşturması ve kovuşturması dışında kullanılamayacaktır. Esasında CMK. md. 139/6’nın düzenleniş biçimi, CMK. md. 138/2 veya 140/4’deki hüküm gibi bir düzenlemenin yapılmak istenmesi ve fakat başarısız olunmasını göstermektedir.” ÜNVER, “Kişisel Verilerin Korunması”, s. 192.

⁴⁴⁶ AİHM; DNA profillerinin suçların aydınlatılması veya önlenmesi amacıyla depolanması veya kullanılmasında hukuka uygun hareket edilmediği takdirde kişilerin özel yaşamlarının gizliliğini

edilen delillerin veya kişisel verilerin ceza yargılama usulü bakımından delil olarak kullanılabilirliği de bulunmamaktadır.⁴⁴⁷

B. Türk Ceza Kanunu’nda Kişisel Verilere İlişkin Suçlar

1. Genel Olarak

Kişisel verilerin korunması ve işlenmesine ilişkin temel prensiplerin belirlenmesi amacı doğrultusunda hazırlanan 6698 sayılı Kanunu’nun, kişisel verilerin hukuka uygun işlenmesine ilişkin öngörmüş olduğu temel veri koruma ilkelerini ihlal niteliğindeki hareketler, 5237 sayılı TCK’da düzenlenmiş olan kişisel verilere karşı

güvence altına alan AİHS’in 8. maddesinin ihlal edilmiş olacağına hükmetmiştir. AİHM, Van Der Velgen/ Hollanda Davası, <https://hudoc.echr.coe.int> (7.01.2018).

⁴⁴⁷ “Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmeliğin 14/1. maddesinde " Bu Yönetmelik 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." ve 14/3. maddesinde ise "Bilirkişi tarafından yapılan analizler sonucu elde edilen bulgular ilgili makama gönderilir; bulgular üzerinden moleküler genetik analizler için izole edilen DNA örnekleri bilirkişi tarafından rapor hazırlandıktan sonra imha edilir ve bu husus raporda açıkça belirtilir." hükümlerine amirdir. Gerek Kanunlarımızda ve gerekse Yönetmelik hükümlerinde adli soruşturma sebebiyle alınan örnekler üzerinde yapılan inceleme sonuçlarının bir sisteme kaydedileceğine dair bir hüküm bulunmamaktadır. Yine Yönetmeliğin 13/3. maddesinde "Yapılacak incelemeler için resmen atanan veya bilirkişilikle yükümlü olan ya da soruşturma veya kovuşturmayı yürüten makama mensup olmayan veya bu makamın soruşturma veya kovuşturmayı yürüten dairesinden teşkilât yapısı itibarıyla ve objektif olarak ayrı bir birimine mensup olan görevliler, bilirkişi olarak görevlendirilebilirler. Bu kişiler, teknik ve teşkilât bakımından uygun tedbirlerle yasak moleküler genetik incelemelerin yapılmasını ve yetkisiz üçüncü kişilerin bilgi edinmesini önlemekle yükümlüdürler. İncelenecek bulgu, bilirkişiye ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilir." hükmünü amirdir. Bu hükmün, Yönetmeliğin 14/1-3. maddeleri ile birlikte yorumlanmasından, incelenecek bulgunun bilirkişiye ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verilmesi karşısında zaten bilirkişi tarafından bir sisteme kaydının fiilen imkansız olmasının sağlanmasının amaçlandığı açıkça anlaşılmaktadır. Sanık tüm aşamalarda atılı suçları işlemediğini, suçsuz olduğunu savunmuştur. Sanık, katılana ait evin balkonunun altında bulunan şapkanın kendisine ait olduğunu, ancak olay mahalline nasıl konulduğunu bilmediğini beyan etmiştir. Bu itibarla sanığın daha önce işlediği başka bir suç sebebiyle hukuka uygun olarak alınıp alınmadığı dahi tespit edilmemiş vücut örnekleri üzerinde yapılan çalışma sonucu elde edilen genotip özelliklerinin hukuka aykırı olarak bir sisteme kaydedildiği ve yargılama konusu olayımızda olay mahallinde bulunan şapka üzerinden alınan materyal üzerinde genotip incelemesi yapılarak sisteme yüklenen sonuçlarla karşılaştırılıp sanığa ait olduğunun tespit edilmesinin 5271 Sayılı CMK’nın 217/2. maddesinde öngörülen "Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir." hükmüne açıkça aykırı olduğu sabittir. Türkiye Cumhuriyeti Anayasası ve Kanunlarımızdaki hükümler çerçevesinde, yasak delil niteliğindeki bilirkişi raporu haricinde sanığın atılı suçları işlediğine dair mahkumiyetini gerektirir kesin ve inandırıcı delilin yargılama dosyası arasında bulunmadığından beraatine karar verilmesi ” Yargıtay 17. CD., E: 2015/22839, K: 2017/2999, T: 14.3.2017. (Karşı oy); Yargıtay 17. CD., E: 2016/10020, K: 2016/11226, T: 1.11.2016 (Karşı oy) www.kazanci.com (08.02.2018); DAĞ, *Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması*, s. 293.

işlenen suçlara vücut vermektedir.⁴⁴⁸ Bu doğrultuda, her ne kadar verilerin işlenmesi kapsamında ele alınan fiilleri tam olarak karşılamasa da,⁴⁴⁹ 5237 sayılı Türk Ceza Kanunu'nun 135., 136. ve 138. maddeleri; kişisel verilerin hukuka aykırı olarak kaydedilmesini, verilmesini, yayılmasını, ele geçirilmesini ve yok edilmemesini suç olarak düzenlemektedir. Bu düzenlemelerin genel gerekçesi ise; *“çağımızda kişilerle ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alış verişi yapılan mağazaların müşterilerine ilişkin kayıtlar, böylece tutulmaktadır. 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 ifade edilmiştir.⁴⁵⁰

765 sayılı Türk Ceza Kanunu'nda da kişisel verilerin korunması amacına dolaylı olarak hizmet eden hükümlere yer verilmiş olduğu görülmektedir. Ancak bu hükümlerin lafzı ve kapsamı itibarıyla sağladığı koruma; her türlü kişisel veri ve verilerin tüm işleme şekil ve araçlarını bakımından uygulanabilir değildir. “Sırrın masuniyeti aleyhine cürümler” arasında sayılan mülga TCK'nın 195, 196, 197, 198 ve 200. maddelerinin konusunu, kişisel verilere ilişkin doğrudan bir nitelendirme yapılmış olmamakla birlikte, kişiler arasındaki mektup, posta, telgraf veya kapalı zarf içeriğinde yer alan sır niteliğindeki bilgiler oluşturmaktadır. Bu bilgilerin kişisel veri niteliğinde olması da çok yüksek ihtimaldedir.⁴⁵¹ Bu anlamda 765 sayılı Kanun'un döneminde kişisel verilerin tamamen korunmasız bırakılmış olduğunu söylemek doğru olmaz. Ancak toplumsal yaşamda meydana gelen teknolojik değişiklikler beraberinde⁴⁵², kişisel verilerin hukuka aykırı olarak işlenmesi karşısında bireylerin özel yaşamının özel olarak korunması ihtiyacını meydana getirmiştir.⁴⁵³ Kişisel veri ceza normlarıyla daha doğrudan korunması gereken bir değerdir. Bu değere ilişkin

⁴⁴⁸ KVKK md. 17. “1. Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ncı madde hükümleri uygulanır.”; KORKMAZ, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, s. 112.

⁴⁴⁹ AKDAĞ, Hale, “Türk Ceza Hukukunda Kişisel Verilerin Korunması İlkeleri”, Ankara Üniversitesi Hukuk Fakültesi, (Prof. Dr. Nevzat Toroslu'ya Armağan), C. 1, 2015, s. 35.

⁴⁵⁰ 5237 sayılı TCK 135. Madde Gerekçesi

⁴⁵¹ ÜNVER, Yener, “TCK ve CK Tasarısının İnternet Açısından Değerlendirilmesi”, s.95.

⁴⁵² “Yeni hukuksal değerlerin ortaya çıkması, çoğu kez beraberinde ceza hukuku korumalarını da getirir. çevre, atom, trafik, gen teknolojisi vs. alanlarında sürekli yeni ihlal modellerinin doğduğu ve bunlara paralel olarak batı ülkelerinde de yeni suç tiplerinin yaratıldığı da bir gerçektir.” ÜNVER, Yener, “TCK ve CK Tasarısının İnternet Açısından Değerlendirilmesi”, s. 54.

⁴⁵³ ÜNVER, Yener, “TCK ve CK Tasarısının İnternet Açısından Değerlendirilmesi”, s.62, 80.

müdahaleler, ceza mevzuatımızın koruması gereken yeni bir ihlal modeli olarak ortaya çıkmıştır. Bu ihtiyaçla ilgili olarak hukuki konusu “özel hayatın gizliliği”⁴⁵⁴ ve kişisel verilerin korunması hakkı olan kişisel verilere karşı işlenen suç tipleri, 5237 sayılı Türk Ceza Kanunu’nda düzenlenmiştir.

5237 sayılı Kanun’un kişisel verilere karşı suçları ihdas ettiği dönem itibarıyla, kişisel verilerin korunmasının temel ilke ve kavramlarını düzenleyen ne ulusal bir mevzuatımız ne de iç hukukumuza dahil olmuş uluslararası bir sözleşme bulunmamaktaydı. Her ne kadar 5237 sayılı Kanun’un gerekçesi kişisel verilere karşı işlenen suçlarla ilgili olarak Türkiye’nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme’nin ilgili hükümlerine geçerlilik tanıdığını açıklamışsa da bu açıklamanın sözleşmeye yürürlük kazandırabilecek hukuki bir bağlayıcılığı bulunmadığı şüphesizdir. 5237 sayılı TCK’nın yürürlüğe girmesinin üzerinden geçen 13 yıl ve 1989 yılından beri süren kanun yapım çalışmaları neticesinde, kişisel verilere ilişkin temel kavram ve ilkeler bakımından başvurabileceğimiz bir ulusal veri koruma mevzuatına kavuşmuş bulunmaktayız. Aynı zamanda bu süreç sonrasında 108 sayılı “Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair” Avrupa Konseyi Sözleşme’nin de onaylanma süreci tamamlanarak, Sözleşme hükümleri iç hukukumuza dahil edilmiştir. Bu doğrultuda henüz 6698 sayılı Kanun’un tasarı aşamasındayken kamuoyuna yansıyan tartışmaların ve ilgili suç tiplerinin ihlaline ilişkin TCK’nın 135. ve 136. maddelerinin kapsamında açılan davaların da giderek artmakta olduğu gözlemlenmiştir.⁴⁵⁵ Bu durum kanaatimizce hem halkımızın hem de yargı mercilerimizin konuya ilişkin bilinçlerinin artmasına bağlı olarak gelişmeye devam edecektir. Elbette bir toplumda suç işleme oranının artmasının toplum açısından olumlu bir tarafının bulunduğunu söyleyemeyiz. Ancak vatandaşların ve yargı makamlarının, temel bir anayasal kişilik hakkı olarak, kişisel verilerinin korunmasına ilişkin talep sunmalarının ve ihlallere karşı korunmaya çalışmalarının,

⁴⁵⁴ AKDAĞ, “Türk Ceza Hukukunda Kişisel Verilerin Korunması İlkeleri”, s. 28.

⁴⁵⁵ Konuya ilişkin Adalet Bakanlığı’nın sunmuş olduğu istatistiklere göre kişisel verilerin hukuka aykırı kaydedilmesi iddiasıyla TCK’nın 135. maddesinin ihlaline ilişkin açılan dava sayısı 2011 yılında 198 iken 2013 yılına gelinceye kadar %20 artış göstermiş ve 236 olmuştur, 136. maddenin ihlali iddiasıyla açılan dava sayısında ise %50’ye varan artış yaşanmıştır. KESER BERBER, KAYA, *Türkiye’de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, s.45,46.

lkemizde “kişisel verilerin korunması kltrnn”⁴⁵⁶ kazanılabilmesi adına nemli bir etkisi olacaktır.

2. Kişisel Verilerin Kaydedilmesi Suçu

a. Genel Olarak

zel hayatın ve hayatın gizli alanının ihlaline ynelik suçlar TCK’nın dokuzuncu blmnde dzenlenmiř olup, kiřilerin zel hayat alanına dahil bir unsur olduėu kabul edilen kiřisel verilere karřı iřlenen suçlara da bu blmde yer verilmiřtir. Kanun’un 135. maddesinde kiřisel verilerin hukuka aykırı olarak kaydedilmesi suçu iki fıkra halin de dzenlemiřtir. Birinci fıkra ile genel olarak kiřisel verilerin hukuka aykırı kaydedilmesi yaptırımı baėlanmıřken, maddenin ikinci fıkrası ise suçu hassas veri kategorisine dahil kiřisel veriler hakkında iřlenmiř olmasını cezanın artırılmasını gerektiren nitelikli bir olarak dzenlemiřtir. Bu fıkranın 24/3/2016 tarihli ve 6698 sayılı Kanun ile deėiřtirilmeden nceki hali⁴⁵⁷ uygulamada ve doktrinde farklı yorumlara sebep olmakta iken, maddenin mevcut deėiřlikten sonraki dzenleniř biçiminin uygulama ve doktrinindeki kafa karıřıklıklarının giderilmesi adına oldukça yerinde olduėunu syleyebiliriz. zellikle maddenin nceki řeklinin ilk fıkra ve ikinci fıkrada ngrlen fiilleri aynı yaptırımı baėlamıř olması ve ikinci fıkranın suç oluřturan fiillerin iřleniř řekline iliřkin belirsizliėi, doktrinde deėiřik kanaatlerin benimsenmesine sebep olmuřtur. Bir kısım mellif kiřisel verilerin kaydedilmesi ve ikinci fıkrada tahdidi olarak sayılmıř olan bilgilerin veri olarak kaydedilmesinin aynı anlama gelmediėini, ilk fıkranın “kiřisel verileri kayıt etmeyi” yasaklanmakta iken ikinci fıkra ile “ kiřisel veri olarak kayıt etme” yasaklanmaktadır grřn benimsemiřtir.⁴⁵⁸ Maddenin bu řekildeki lafzının ve yorumlanmasının kiřisel verilerin korunması amacını tam olarak saėlamaya elveriřli olmadıėı ve konuya iliřkin dzenlemenin asıl amacının ikinci fıkrada sayılan hassas veri niteliėindeki verilere

⁴⁵⁶ TOPAL, Cansu, İnternet ve Hukuk Sempozyumu, İstanbul, 2018.

⁴⁵⁷ Maddenin ikinci fıkrasının 6698 sayılı Kanun ile deėiřikliėe uėramdan nceki hali; “Kiřilerin siyasi, felsefi veya dini grřlerine, ırkı kkenlerine; hukuka aykırı olarak ahlaki eėilimlerine, cinsel yařamlarına, saėlık durumlarına veya sendikal baėlantılarına iliřkin bilgileri kiřisel veri olarak kaydeden kimse, yukarıdaki fıkra hkmne gre cezalandırılır.” řeklinde dir.

⁴⁵⁸ HAFIZOėULLARI, Zeki, ZEN, Muharrem, *Trk Ceza Hukuku zel Hkmler Kiřilere Karřı Suçlar*, 5. Baskı, Ankara, Usa Yayıncılık, 2016, s. 289.

yönelik daha fazla koruma sağlanması olduğu kanaatindeki müelliflerin de katkısıyla düzenleme bugünkü şeklini almıştır.⁴⁵⁹

TCK'nın suçun maddi konusu olan kişisel verilere ilişkin bir tanımlamada bulunmamış olmasının, suçta ve cezada kanunilik ilkesine aykırılık teşkil ettiği şeklindeki yerinde olmayan eleştiriler ve itirazlar Anayasa Mahkemesi'ne de taşınmıştır. Anayasa Mahkemesi, ceza mevzuatının düzenleme konusu yaptığı her suça ilişkin her unsura yer veremeyecek kazuistik bir düzenleme olmaması ve gelişen teknolojiyle kişisel veri kavramının kapsamının da sürekli değişebilir olduğu gerekçeleriyle bu itirazın yerinde olmadığına hükmetmiştir.⁴⁶⁰ Bunun yanında TCK'nın 135. maddesinin gerekçesiyle de, kişisel veri kavramı; "gerçek kişiyle ilgili her türlü bilgi" şeklinde tanımlanmıştır. Gerekçe, bu tanımlamada ve aynı zamanda kişisel verilere karşı işlenen diğer suçlara ilişkin kavramların yorumlanmasında, Türkiye'nin 1981 yılında taraf olma iradesini sergilemiş olduğu 108 sayılı Avrupa Konseyi Sözleşmesi'nin hükümlerinin geçerli olacağını belirtmiştir. Ancak bu Sözleşme onaylanma sürecini tamamlayarak, 17.03.2016 tarihi itibarıyla ülkemiz bakımından hukuki uygulanabilirlik kazanmıştır. Dolayısıyla 6698 sayılı Kişisel Verilerin Korunması Kanunu ve 108 sayılı Avrupa Konseyi Sözleşmesi, TCK'nın kişisel verilerin hukuka aykırı olarak işlenmesi karşısında düzenlemiş olduğu suçlarının doğru şekilde anlaşılması ve uygulanabilmesini sağlayacak temel usul ve esaslara ilişkin başvurulması gereken birincil kaynaklardır. Bu çalışmada da 108 sayılı Avrupa Konseyi Sözleşmesi ve 6698 sayılı Kanun'un düzenlemesinden, yargı kararlarından ve doktrindeki farklı görüşlerden yola çıkılarak kişisel verilere karşı işlenen suç tipleri suç inceleme metodolojisine uygun olarak incelenmeye çalışılmıştır.

⁴⁵⁹ ÖZBEK, V. Özer, DOĞAN, Koray, BACAŞIZ, Pınar, TEPE, İlker, *Türk Ceza Hukuku Özel Hükümler*, 11.Baskı, Ankara, Seçkin Yayıncılık, 2017, s. 578.

⁴⁶⁰ "Kuralda yer alan "kişisel veri" kavramı teknolojik gelişmelere bağlı olarak çok farklı şekillerde ortaya çıkabileceğinden bu kapsama giren tüm verilerin kanun koyucu tarafından önceden öngörülebilmesi ve tek tek sayılabilmesi mümkün değildir. Bununla birlikte gerek ulusal ve uluslararası mevzuat gerekse yargı içtihatları çerçevesinde "kişisel veri" kavramının, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmektedir "kişisel veri" kavramının bu çerçevede doktrin, uygulama ve yargı kararlarında belirlenerek anlam ve içeriğinin gelişip değişeceğinde kuşku yoktur. Dolayısıyla başvuru kararında her ne kadar ceza mevzuatında "kişisel veri" ile ilgili bir tanım ve sınırlandırmanın yapılmadığı, bu nedenle itiraz konusu kuralın belirsiz olduğu ileri sürülmüş ise de ulusal ve uluslararası mevzuat ile yargı içtihatları dikkate alındığında kuralın belirsiz olduğundan söz edilemeyeceği açıktır." Anayasa Mahkemesi, E: 2015/32, K: 2015/102, T: 12.11.2015.

b. Suçla Korunan Hukuksal Yarar

Kişisel verilerin hukuka aykırı olarak kaydedilmesini yaptırım altına alan bu suç ile korunan hukuksal yarar; kişilerin özel yaşam alanına dahil olan kişisel verilerinin korunması hakkıdır. Kişilerin kendilerine ilişkin her türlü bilgi üzerinde, kendi belirlediği sınırlar içerisinde tasarruf edilmesi, kişinin bu yöndeki iradesine saygı gösterilmesini isteyebilmesi ve maddi anlamda da kişisel verilerinin güvenliğinin sağlanmasını talep edebilmesi bu hakkın kapsamını oluşturmaktadır. Kişilerin özel yaşamlarının gizliliğine yönelik bir müdahalede bulunularak, kişisel verilerine iradesi dışında ulaşılması ve bunların kaydedilmesi doğrudan kişisel verilerin korunması hakkının ihlaline yol açmaktadır.⁴⁶¹

Kişisel verilerin korunması hakkı ve özel yaşamın gizliliği arasındaki ilişkinin açıklanmasına ilişkin yorum farklılıkları doğrultusunda, doktrinde de bu suçla korunan hukuksal yararın ne olduğu konusunda ortak bir kanaate varılabilmiş değildir. Kişisel veriyi “kişinin nefesine ait bilgiler” olarak tanımlayan Hafizoğulları, TCK’nın özel hayatın ve hayatın gizli alanının korunma altına alındığı dokuzuncu bölümünde düzenlenmiş olan bu suçta; kişilerin özel hayatlarına dahil olan kişisel verilerinin gizliliğinin korunması hususundaki ferdi ve kamusal yararın, korunan hukuksal yarar olduğunu benimsemektedir.⁴⁶² Bu kanaate göre; kişisel veriler de gizli olarak kabul edilen hayat alanımıza dahil sır niteliğindeki bilgiler olarak kabul edilmektedir. Halbuki 135. madde kişisel verilerin hukuka aykırı olarak kaydedilmiş olmasını aramakta ve bu verilerin, her ne kadar tabiatı gereği genellikle sır niteliğindeki bilgiler olsalar da, gizli veya sır kapsamında olmasını aramamaktadır.⁴⁶³ Yargıtay’ımız da bu konuda; “*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.*” şeklindeki görüşü benimsemektedir.⁴⁶⁴ Suçla korunan hukuksal yarara ilişkin benimsenmiş olan farklı

⁴⁶¹ ŞENER, “Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu”, s. 74.

⁴⁶² HAFIZOĞULLARI, ÖZEN, *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar*, s. 287.

⁴⁶³ DÜLGER, M. Volkan, *Bilişim Suçları ve İnternet İletişim Hukuku*, 5. Baskı, Ankara, Seçkin Yayınları, 2014, s. 622.

⁴⁶⁴ Yargıtay CGK., E: 2012/12-1510, K: 2014/331, K: 17.06.2014 www.kazanci.com (04.01.2018).; SOYASLAN, Doğan, *Ceza Hukuku Özel Hükümler*, 11. Baskı, Ankara, Yetkin Yayınları, 2016, s.

bir görüş de; kişisel verinin konusunu oluşturan değere göre korunan hukuksal yararın belirlenmesi gerektiği istikametindedir. Buna göre örneğin; kişisel verinin kişinin sağlık durumuna ilişkin bir bilgi içeriyor olması halinde, korunan hukuksal yarar kişinin sağlık hakkı olur.⁴⁶⁵

Sonuç olarak kanaatimiz; bu suç tipinin, hem kişisel verileri hem de kişisel verilerin güvenliğinin korunması hukuksal yararını, diğer bir deyişle kişisel verilerin korunması hakkına ilişkin hukuksal yararı sağlamaya yönelik düzenlenmiş olduğudur.⁴⁶⁶

c. Suçun Unsurları

i. Maddi Unsurlar

1. Suçun Konusu

Bu suçun maddi konusunu kişisel veriler oluşturmaktadır. Kişisel veri kavramı en genel anlamda kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili her türlü bilgi olarak tanımlanmaktadır.⁴⁶⁷ Bu kapsamda kişiye ilişkin; “*adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim*⁴⁶⁸, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi,

349; MENDOS KUŞKONMAZ, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, s. 133.

⁴⁶⁵ SEYREK TÜTÜNCÜBAŞI, *Kişilerin Kendisine Ait Verilerin Kaderini Tayin Hakkının Ceza Hukuku Yoluyla Korunması*, s. 80.

⁴⁶⁶ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 622.

⁴⁶⁷ 6698 sayılı Kanun md. 3, 108 Sayılı Avrupa Konseyi Sözleşmesi md. 2. ; Kişisel veri kavramının, uluslararası ve ulusal metinlerde benimsenen bu genel tanımlamadan yola çıkılarak, temel unsurlarıyla birlikte detaylı açıklamasına çalışmamızın ilk bölümünde yer verilmiştir. Bkz. s. 5-8.

⁴⁶⁸ Olayda katılanın, lise yıllarında ve mezuniyet işlemlerinde kullandığı vesikalık resminin bir internet sitesinde memleket, isim gibi bilgileri uydurularak bir sosyal medya hesabı oluşturulmuş olmasına ilişkin eylemde; gerçek bir kişiye ait olan vesikalık resim kişisel veri olarak kabul edilmektedir. İstanbul 25. Asliye Ceza Mahkemesi. DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 637.; “*Sanığın genel yayın yönetmenliğini yaptığı gazetede köşe yazarı olarak çalışan katılanın yazdığı köşesinde kullanılan fotoğrafın, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle sanık tarafından internetteki özel bir arkadaşlık sitesine kimlik, adres ve telefon bilgileri verilmeksizin ve erkek arkadaşı aradığı açıklamasıyla konulması eylemi, TCK’nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma*

*e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.”*⁴⁶⁹ Ayrıca rapor veya analiz yolu ile de kişinin kimliğine ulaşılabilenkte ise, özellikle kişinin sağlık durumuna ilişkin bilgileri düzenleyen belgelerde olduğu gibi, bu belgelerin de kişisel veri olduğunu söyleyebiliriz.⁴⁷⁰ Bunun yanı sıra anonimleştirilmiş verilerinden yola çıkarak bir kişinin kimliğini tespit etmemiz veya belirlememiz söz konusu olmayacağından, bu verilerin kişisel veri olarak kabul edilmesi ve bu suçun konusunu oluşturması söz konusu olamayacaktır.⁴⁷¹

Ceza mevzuatımızda, bu suçun konusunu oluşturan kişisel veri kavramından ne anlaşılması gerektiğine ilişkin bir tanımlama yer almamaktadır. Kanun koyucu bu kavramın anlam ve içeriğinin; uluslararası düzenlemelerin, doktrin, uygulama ve yargı kararlarının ekseninde belirlenmesinden yana bir irade sergilemiştir.⁴⁷² Bu durumun

suçunu oluşturmaktadır.” Yargıtay CGK, E: 2012/12-1510, K: 2014/331, T: 17.6.2014, www.kazanci.com (04.06.2017).

⁴⁶⁹ Anayasa Mahkemesi, Esas Sayısı : 2014/196 Karar Sayısı : 2015/103 Karar Tarihi : 12.11.2015

⁴⁷⁰ KVK Kurumu Yayınları, 6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar, s. 18. <https://www.kvkk.gov.tr> (09.02.2018).; “Örneğin, telefon bankacılığında müşterinin bankaya talimat verdiği sesi sisteme kaydedildiği zaman, bu kaydedilen talimatlar kişisel veri olarak düşünülmelidir. Ayrıca, güvenlik kamera sistemi tarafından kaydedilen görüntüler bireylerin tanınabilir olması ölçüsünde kişisel veri olabilir.” TEKİN, “Kişisel Verilerin Korunması İle İlgili Türkiye’deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi”, s. 228.

⁴⁷¹ AKINCI, “Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi”, s. 29.

⁴⁷² Zira ceza hukukunda yorum serbesttir, ancak suç ve ceza içeren hükümlerin kıyasa yol açacak biçimde geniş yorumlanması yasaktır. Suç tipinde yer alan unsurların kıyasa yol açmayacak şekilde yorum yoluyla ne anlama geldiğinin belirlenbilmesi mümkündür. ÖZBEK, V. Özer, DOĞAN, Koray, BACAŞIZ, Pınar, TEPE, İlker, *Türk Ceza Hukuku Özel Hükümler*, 11.Baskı, Seçkin Yayıncılık, Ankara, 2017, s. 570. ; Bu istikamette Yargıtay Ceza Genel Kurulu nelerin kişisel veri olabileceğine ilişkin şöyle bir sınıflandırma yapmıştır; “a- Yaşam şekline ilişkin kişisel veriler: Kişilerin üçüncü kişiler tarafından ayırimcılığa uğramaması ve haysiyetinin korunmasıyla ilişkili olarak, dini inançları, cinsel tercihleri, etnik kökeni, suç geçmişi, politik eğilimleri ve kişisel özel aktivitelere ilişkin bilgiler bu bağlamda sayılabilecektir. b- Ekonomik ve finansal kişisel veriler: Suçlular tarafından suistimale ve kimlik hırsızlığına hedef olmamak için kişinin mali varlığı, sahip olduğu hisse ve hesaplar, borçları, yaptığı alış verişler, kredi kartlarına ilişkin veriler. Ayrıca sayılan bu bilgiler ile kişinin nerede ve kimlerle bulunduğu, sağlık bilgilerine ilişkin bilgiler de ortaya çıkarılabileceğinden ve varlık bilgisinin toplumsal açıdan da özel sayılmasından dolayı önemi artmaktadır. c- Bilişim alanına ilişkin kişisel veriler: e-postaların bizzat adresleri veya şifreleri, internet ortamında paylaşılan kişisel veriler mahrem olarak değerlendirilebilir. Bunun önemi şu bakımdan artmaktadır. İnternette gezinti yapan kişi birçok kişisel bilgileri paylaşmakta, bu bilgiler kayıt altına alınmakta, yine internet erişimine ilişkin iz kayıtlarının hizmet sağlayıcı ve sunucu sahipleri tarafından tutulabiliyor olması nedenleriyle artmaktadır. d- Sağlıkla ilgili kişisel veriler: Sağlık verileri kişilerin iş güvenliğini, toplum içindeki statüsünü ve sigorta kapsamını etkileyen hassas bilgilerdir. Ayrıca sağlık verileri kişilerin sosyal yaşantısı ve psikolojik durumları hakkında bilgi edinilmesine neden olabilir. Biyometrik (Kişinin kendine özgü fiziksel veya biyolojik niteliklerine dayalı olarak insanların kimliğini tespit için dijital teknolojiden faydalanma bilimi) veriler de kişisel veriler arasındadır. e- Politik kişisel veriler: Toplum içinde yaşayan kişilerin siyasi tercihleri toplum katmanları arasında bilinme halinde ayırimcılığa maruz kalma ihtimali

temel gerekçesi olarak da kişisel veri kavramının kapsam bakımında sınırlandırılmasının güç olması gösterilmektedir. Her geçen gün, teknolojik gelişmeler sayesinde kişilerle ilişkilendirilebilen yeni bir veri türü orta çıkmaktadır. Bu durumda, kanun koyucunun kişisel veri kavramının kapsamını tam ve eksiksiz olarak belirleyebilmesi imkan dışıdır.⁴⁷³ Bunun yerine kavramın temel unsurlarından yola çıkılarak hangi tür bilgilerin kişisel veri olduğunun tespit edilmesi daha yerinde kabul edilmektedir.

Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçuna konu oluşturan, kişisel veri kavramına ilişkin tartışılmasını gerekli gördüğümüz iki temel husus bulunmaktadır. İlki; tüzel kişilere veya merhum kişilere ait kişisel verilerin de hukuka aykırı olarak kaydedilmesinin bu suçun konusunu oluşturup oluşturmayacağı, ikincisi ise; kişilerin kendileri tarafından alenileştirilmiş olan veya kamuya açık hayatı kapsamında herkesin ulaşabileceği verilerinin suçun konusuna dahil olup olmadığıdır. Bu konulardan ilki daha ziyade suçun mağdurunu da ilgilendirmekte olduğundan bu tartışmaya suçun mağdurunun incelendiği sırada girmek daha yerinde olacaktır. Bu kısımda veri sahibinin kendisi tarafından alenileştirilmiş olan kişisel verilerin, TCK kapsamında korunmakta olup olmadığına belirlenmesi suçun tespiti açısından hayati öneme sahiptir. Zira uygulamada da bu sebeple, istikrarlı kararların verilememekte olduğu gözlemlenmiştir. Türk Ceza Kanunu'nun konuya ilişkin bir açıklık getirmemiş olması dolayısıyla verilerin korunmasına ilişkin özel düzenlemelerden yola çıkılarak bu sorunun çözülmesi gerekecektir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun bazı hükümlerinin uygulanmayacağı istisnai hallerin düzenlendiği 28. maddesinin ikinci fıkrasında; "İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi" istisnai bir hal olarak yer almaktadır. Bu istisnai haller Kanun'un belli maddelerine ilişkin olarak getirilmiş olup, bu düzenlemeden yola çıkarak alenileştirilmiş verilerin kişisel veri olarak kabul edilemeyeceği çıkarımında bulunmamız doğru olamayacaktır.⁴⁷⁴ Ancak 6698 sayılı Kanun'un 5. maddesinde,

bulunduğundan bu bilgilerde kişisel veridir." Yargıtay CGK, E: 2012/12-1510, K: 2014/331, T: 17.6.2014 www.kazanci.com (04.06.2017).

⁴⁷³ Anayasa Mahkemesi, E: 2015/32, K: 2015/102, T: 12.11.2015.

⁴⁷⁴ 6698 sayılı Kanun'un 28. Maddesinin ikinci fıkrasında mutlak surette kapsamına dahil olmayan ve koruması dışında kalan, kişinin sırf kişisel ve ailevi ilişkiler kapsamında işlemiş olduğu veriler gibi veri ve fiillerin TCK'ya göre suç konusu veya suç oluşturabilmesi mümkündür. Zira 6698 sayılı Kanun'un ilgili hükmü bir hukuka uygunluk sebebi öngörmemiş sadece Kanun'un kapsamını dışında tutulan kişi ve fiillere ilişkin istisnaları düzenlemiştir. ŞEN, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", s. 1200.

hukuka uygun bir veri işlemenin temel koşulu olan, ilgilinin rızası aranmaksızın kişisel verilerin işlenebileceği haller arasında, kişisel verilerin ilgili kişinin kendisi tarafından alenileştirilmiş olmasına yer verilmiştir. Bu durumda ilgili kişinin kendisi tarafından herkesin bilgisine açık hale getirilmiş kişisel verileri, rızası aranmaksızın işlenebilecektir.⁴⁷⁵ Kanaatimizce bu hüküm de kişinin kendisi tarafından alenileştirilmiş verilere karşı TCK'nın öngörmüş olduğu suçların işlenmeyeceği anlamına gelmeyecektir ancak konunun, bu düzenleme doğrultusunda hukuka uygunluk halleri arasında değerlendirilmesi kanaatimizce daha doğru olacaktır.

Uygulamada Yargıtay Ceza Genel Kurulu, gazetede köşe yazarı olan katılanın, yazdığı köşesinde kullanılan fotoğrafının, katılanın rızası olmadan arkadaşlık sitesine konulması eyleminin, kişisel verilerin hukuka aykırı olarak yayılmasını suç olarak düzenleyen TCK'nın 136. maddesinin suç tanımına uyduğuna karar vermiştir. Zira Mahkeme'ye göre kişisel verilerin korunmasına ilişkin suçlarda korunan değer verinin ilgilisi olan kişinin kişilik hakkıdır. Bu hak kapsamında, kişinin daha önce kendisi tarafından alenileştirmiş olması suretiyle de olsa herkes tarafından bilinen, ulaşılabilen verileri de hukuka aykırı müdahalelere karşı korunmaktadır.⁴⁷⁶ Dülger'e göre de kişinin kendi rızasıyla/iradesiyle sosyal medya üzerinde yayınladığı ve herkesin bilgisine açık kıldığı kendisine ilişkin verilerinin de üçüncü kişilerin müdahaleleri karşısında korunması gerekmektedir. Zira kişinin, verilerinin kendisi tarafından alenileştirilmiş olması, bu müdahalelere ilişkin rızasının da bulunduğu anlamında yorumlanamaz.⁴⁷⁷ Buna karşın doktrinde; kişinin kendisi tarafından alenileştirilen, herkes tarafından bilinebilecek hale getirilen bir verinin işlenmesinde, korunması gereken bir hukuki yararın kalmadığı da kabul edilmektedir.⁴⁷⁸ Herkes tarafından bilinen veya kolaylıkla bilinmesi mümkün olan verilerin hukuka aykırı olarak

⁴⁷⁵ KVK Kurumu Yayınları, 6698 Sayılı Kanun'da Yer Alan Kurumsal Terimler, s. 9. <https://www.kvkk.gov.tr> (09.02.2018).

⁴⁷⁶ Yargıtay CGK., E: 2012/12-1510, K: 2014/331, K: 17.06.2014.; "Oluşa ve dosya kapsamına göre, bir avukatlık bürosunda takip elemanı olarak çalışan sanığın, avukat olan katılanın facebook adlı sosyal paylaşım sitesinde yer alan resmini, onun sayfasından temin edip, aynı sitede, bir ön ad ile beraber katılanın adı ve soyadını taşıyan sahte hesap bir açarak, bu hesap üzerinden, ele geçirdiği katılana ait resmi, onun bilgisi ve rızası dışında yayımladığı olayda; Katılanın resmini, belirli olmayan ve birden fazla kişi tarafından algılanabilme imkanı bulunan facebook adlı sosyal paylaşım sitesinde, hukuka aykırı olarak yayan sanığın eyleminin, verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğunun kabulünde bir isabetsizlik görülmediğinden" Yargıtay 12. CD., E: 2013/27402, K: 2014/15379, T: 23.6.2014 www.kazanci.com (08.02.2018).; SEYREK TÜTÜNCÜBAŞI, *Kişilerin Kendisine Ait Verilerin Kaderini Tayin Hakkının Ceza Hukuku Yoluyla Korunması*, s. 80.

⁴⁷⁷ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 629.

⁴⁷⁸ ERDEM, "Kişisel Verilerin Korunması Konusunda Son Gelişmeler, s. 104.

işlenmesinin suç oluşturduğunu kabul etmenin maddenin kapsamını fazlaca genişleteceği, bu doğrultuda kişisel veri kavramının dar yorumlanması gerektiği ileri sürülmektedir.⁴⁷⁹ Yargıtay 12. Ceza Dairesi 10.02.2014 tarihinde vermiş olduğu bir kararında da; *“herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler, yasal anlamda “kişisel veri” olarak değerlendirilemez, aksinin kabulü; anılan maddenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçlar doğurur”* şeklinde aynı istikamette kanaatte bulunmuştur.⁴⁸⁰ Buna karşılık suçun konusunu oluşturan kişisel veri kavramının belirtilen istikamette soyut ve genel bir biçimde sınırlandırılması yerine, her olayın özelliği nazarında yorumlanarak, somut duruma ilişkin olarak sınırlandırılmasının daha yerinde olacağı kanaati de doktrinde savunulmaktadır.⁴⁸¹

Sonuç olarak kanaatimiz; bu suçla konu olan kişisel verilerin hem TCK hem de 6698 sayılı Kanun’da nitelendirildiği şekilde özel, gizli veya mahrem olmasının değil bir kişiyle ilişkilendirilebilir olmasının aranması gerekmektedir. Kaydedilmek suretiyle işleme konusu yapılan kişisel veriler bakımından mağdurun, yani verinin ilişkilendirilebildiği kişinin, işlenmesinden rahatsız olacağı nitelikte bir kişisel veri

⁴⁷⁹ “Hastanın herkese anlattığı ya da hastanın bir bacağının olmaması, felçli olması gibi doğası itibarıyla açık olan bilgiler, kişisel veri olarak değerlendirilemez.” YOKUŞ SEVÜK, Handan, “Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması”, V. Türk - Alman Tıp Hukuku Sempozyumu, Türkiye Barolar Birliği Yayınları, 2008, Ankara, s. 796. Farklı istikamette; “Kanımızca kişisel veri tanımı itibarıyla kişiyi belirlenebilir kılan ona ait tüm bilgiler olduğu için dış görünüşünden anlaşılan veriler de bu kapsama girer. Fakat bu veriler kişinin dış görünüşünden anlaşılabiliyorsa ya da sahibinin rızasıyla dışa vurulmakta ise hukuka uygunluk nedenleri gündeme gelecektir.” İTİŞGEN, Rezzan, “Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu”, Türkiye Adalet Akademisi Dergisi, S. 23, 2015, s. 184.

⁴⁸⁰ Yargıtay 12. CD., E: 2013/30406, K: 2014/2980, T: 10.02.2014.; ““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...” Yargıtay 12. CD., E: 2012/17703, K: 2012/18222, T: 11.09.2012.; “Sanığın kovuşturma aşamasında verdiği ifadesinde “Davaya konu fotoğrafları ben facebook isimli sosyal paylaşım sitesinden aldım. Ben bu sitede kendisi ile arkadaşım. Zaten bu fotoğrafları herkese açtım, müştekinin benim elimde herhangi bir fotoğrafı yoktur.” şeklindeki savunması, katılanın kovuşturma aşamasında verdiği ifadesinde “benim fotoğraflarım arkadaşım olmayanlara engelli idi. Sadece bir tane profil fotoğrafım herkese açtım. Sanık büyük ihtimalle o fotoğrafımı almış olabilir.” şeklindeki beyanı dikkate alındığında, bahse konu fotoğrafın, katılanın herkese açık profilinden elde edildiği, bu fotoğraflara kolaylıkla ulaşılabilirdiği, fotoğrafın özel hayata dair olduğuna dair bir iddiada da bulunulmadığı dikkate alındığında, özel hayata dair olmayan, herkese açık facebook profilinden kolaylıkla elde edilen fotoğrafların, ilgilinin isim ve soyismi kullanılmadan, sadece başka bir facebook profilinde yayınlanması eyleminin suç olarak kabul edilemeyeceği” Yargıtay 12. CD., E: 2015/4349, K: 2016/5349, T: 30.03.2016.; Yargıtay 12. CD., E: 2012/31601, K: 2013/23586, T: 28.10.2013 www.kazanci.com (08.02.2018).

⁴⁸¹ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 624.

olması bu suçun oluşması için yeterlidir. Suçun oluşması için ayrıca bu verinin gizli ya da aleniyete kavuşmamış olması gibi bir niteliğe sahip olması aranmamalıdır.⁴⁸² Bu suçun konusunun kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin özel nitelikli veriler olması, cezayı artıracak nitelikli bir hal olarak 135. maddenin ikinci fıkrasında düzenlenmiştir.

2. Fail ve Mağdur

TCK'nın 135. maddesi “hukuka aykırı olarak kişisel verileri kaydeden kimse” den bahsetmekte olduğundan bu suçun faili herkes olabilir. Ancak, gerek TCK'nın 20. maddesi gerekse Anayasa'nın 38. maddesinde korunmakta olan, ceza sorumluluğunun şahsiliği prensibi gereği tüzel kişilerin bu suçun faili olabilmesi mümkün değildir. Suçun tüzel kişilerin yarına işlenmesi mümkün olduğu gibi bu durumda TCK'nın 140. maddesinde öngörüldüğü üzere tüzel kişiler hakkında güvenlik tedbirleri uygulanabilecektir.⁴⁸³ Tüzel kişiler hakkında uygulanacak yaptırımların, bu anlamda suç ve cezaların şahsiliği prensibine aykırılık teşkil etmeyecek ağırlıkta ve tüzel kişilerin organlarının hukuka uygun davranma sorumluluğunu artıracak nitelikte olması gerekmektedir.⁴⁸⁴ Ayrıca bu suçun failinin kamu görevlisi olması da, suçun temel şekline oranla verilecek cezayı yarı oranda artıracak nitelikli bir hal olarak düzenlenmiştir. (TCK md. 137)

Bu suçun mağduru bakımından özellik arz eden bir hüküm bulunmadığından, herkes suçun mağduru olabilir. Ancak tüzel kişilerin bu suçun mağduru olup olamayacağına ilişkin doktrinde farklı kanaatte olan müellifler bulunmaktadır. Kanun'un lafzında suçun mağduruna ilişkin bir sınırlandırma bulunmadığı gerekçesiyle bir kısım müellif gerçek veya tüzel kişi herkesin bu suçun mağduru

⁴⁸² AKDAĞ, “Türk Ceza Hukukunda Kişisel Verilerin Korunması İlkeleri”, s. 27.

⁴⁸³ 6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre; “kişisel verilerin işleme amaçlarını ve yöntemlerini belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiler” veri sorumlusu olarak kabul edilmekte ve kişisel verileri işleme konusunda gerçekleştirdikleri faaliyetler kapsamında bizatihi kendileri hukuken sorumlu tutulacaklardır. KVK Kurumu Yayınları, 6698 Sayılı Kanun'da Yer Alan Kurumsal Terimler, s. 5. <https://www.kvkk.gov.tr> (03.09.2017).

⁴⁸⁴ ASLAN, M. Yasin, “Türk Hukukunda Tüzel Kişilerin Ceza Sorumluluğu”, Ankara Barosu Dergisi, C. 68, S. 2, 2010, s. 30.

olabileceği görüşündedir.⁴⁸⁵ Buna karşılık tüzel kişiler, hem ulusal veri koruma mevzuatımızın hem de konuya ilişkin çoğu uluslararası düzenlemenin kişisel verilere ilişkin sağladıkları korumanın kapsamı dışında tutulmuşlardır. Türk Ceza Kanunu da bu istikamette 135. maddesinin gerekçesinde kişisel verileri, yalnızca gerçek kişilerle ilişkilendirilebilen veriler olarak kabul etmektedir.⁴⁸⁶ Dolayısıyla “suçun maddi konusunun ait olduğu kimse”⁴⁸⁷ olarak tanımlanan suç mağdurunun,⁴⁸⁸ bu suç bakımından kanaatimize göre bir tüzel kişi olabilmesi söz konusu değildir.⁴⁸⁹ Merhum kişilerin bu suçun mağduru olup olmayacağı, diğer bir deyişle bu kişilere ait kişisel verilerin suçun konusunu oluşturup oluşturamayacağı ulusal veri koruma mevzuatımızda ve ceza mevzuatımızda açıklık bulunmayan bir husustur. Bu konuda, uluslararası veri koruma düzenlemeleri arasında anayasal nitelik taşıdığını söyleyebileceğimiz, 2016/679 Sayılı Avrupa Birliği Veri Koruma Regülasyonu, merhum kişilere ait verilerin, düzenleme kapsamında sağlanan korumanın dışında tutulduğunu özellikle belirtmiştir. Ancak ulusal mevzuatımız bakımından bu düzenlemenin rehber niteliğinde bir düzenleme olabilmekten başka bir bağlayıcılığı yoktur. Bu konuda ceza hukukumuzda suç mağduru olabilecek kişilerin suçun işlendiği sırada hayatta olması gerektiği istikametindeki genel prensibinden yola çıkılarak,⁴⁹⁰ merhum kişilerin kişisel verilerinin bu suçun maddi konusunu oluşturamayacağını söyleyebiliriz. Ancak verilerin işlenme şekline göre ölenin yakınlarının da bu suç bakımından mağdur olabilmesi tartışılabilir bir konudur.

⁴⁸⁵ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 623.; SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 350.; ŞEN, “Kişisel Verilerin Korunması Kanunu Tasarısı’nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi”, s. 1203.

⁴⁸⁶ “Madde metni kısıtlama getirmemekle birlikte gerekçesi, sadece gerçek kişilerin bu suçun mağduru olabileceklerine işaret ederek, madde metnini ve amacını aşan bir ibareye yer vermiştir. Oysa korunması gerekli kişisel veriler, sadece gerçek kişilere değil, tüzel kişilere de ait olabilir. Gerçek kişilerden ayrı bir hukuki varlıkları ve kimlikleri bulunan tüzel kişilerin de kendi yapılarına özgü kişisel verilerinin olacağı tartışmasızdır. Kanun koyucu, “kişi” ve “kişisel” kavramları ile yalnızca gerçek kişilere güvence sağlamayı hedeflememiştir.” ŞEN, “Kişisel Verilerin Korunması Kanunu Tasarısı’nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi”, s. 1203.

⁴⁸⁷ ARTUK, Mehmet Emin, GÖKCEN, Ahmet, YENİDÜNYA, Caner, *Ceza Hukuku Genel Hükümler*, 8. Baskı, Ankara, Adalet Yayınevi, 2014, s. 283.; DEMİRBAŞ, Timur, *Ceza Hukuku Genel Hükümler*, 12. Baskı, Ankara, Seçkin Yayıncılık, 2017, s. 556.

⁴⁸⁸ Aksi istikamette suçun mağduru olabilmek için kaydedilen verinin maliki yada zilyedi olmanın gerekmediği, mağdurla ilişkin olarak verinin ele geçirilmiş olmasının yeterli olduğuna ilişkin bkz. MENDOS KUŞKONMAZ, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, s. 154.

⁴⁸⁹ ŞENER, “Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu s. 76.; Bir şirketin ticari sırları gibi veriler, kişisellikten ziyade kurumsallık niteliği taşımakta olmaları dolayısıyla TCK’nın 135. maddesi ve devamındaki hükümlerinde düzenlenmiş olan suçların konusu olamayacaktır. ÖZBEK, DOĞAN vd., *Türk Ceza Hukuku Özel Hükümler*, s. 571.; KOCA, Mahmut, ÜZÜLMEZ, İlhan, *Türk Ceza Hukuku Genel Hükümler*, 3. Baskı, Ankara, Seçkin Yayıncılık, 2010, s. 152.

⁴⁹⁰ ARTUK, GÖKCEN, YENİDÜNYA, *Ceza Hukuku Genel Hükümler*, s. 285.

Özellikle suçların içtimaı bahsinde ele alacağımız, kişisel verilerin kaydedilmesi fiilinin aynı zamanda kişinin şeref ve haysiyetini rencide edebilecek nitelik de taşıması halinde, merhum olan kişi bakımında ölünün hatırasına hakaret suçu işlenmiş olacaktır. Bu durumda da suçun mağdurları ölenin yakınları olacaktır.

3. Hareket

TCK'nın 135. maddesinde düzenlenen bu suçun oluşabilmesi için kişisel verilerin hukuka aykırı olarak kaydedilmesi aranmaktadır. Kanun'un ikinci fıkrası, 24/3/2016 tarihli ve 6698 sayılı Kanunun 30. maddesiyle değiştirilinceye kadar doktrinde maddenin fıkraları arasındaki üslup farkı uzunca süre tartışılmıştır.⁴⁹¹ Mevcut düzenlemeyle suçun her iki fıkra bakımından da verilerin hukuka aykırı kaydedilmesi eylemi ile işlenebileceğini söyleyebiliriz.

Kaydetmek, en basit anlamda, bir bilgisayar ortamına⁴⁹² veya kağıt üzerine kişisel verilerin yerleştirilmesi veya işlenmesi olarak tanımlanabilir.⁴⁹³ Bu anlamda verilerin otomatik veya otomatik olmayan vasıtalarla işlenmesi arasında 6698 sayılı Kanun'da benimsendiği şekilde TCK'da da bir fark gözetilmemiştir.⁴⁹⁴ Dolayısıyla bu suçun, verilerin kaydedilmesini sağlayacak her türlü hareketle ve vasıta ile işlenebilecek, serbest hareketli bir suç olduğunu söyleyebiliriz.⁴⁹⁵ Gerekçede belirtildiği üzere; verileri kaydetme; bir CD, flash bellek, harici disk veya ses kayıt cihazına⁴⁹⁶ verilerin kopyalanması, depolanması,⁴⁹⁷ dijital ortama yerleştirilmesi⁴⁹⁸ suretiyle gerçekleştirilebileceği gibi, kağıt üzerine kalemle veya başka şekilde not

⁴⁹¹ “kişisel verileri kaydetmek” ve “veri olarak kaydetmek” eylemlerine ilişkin tartışmalar için bkz s. 73.

⁴⁹² Kaydetmek kavramı; bilişim alanında “elektronik veya sayısal araçlarda bilgiyi korumaya almak.” olarak tanımlanmaktadır. TDK Güncel Türkçe Sözlük, www.tdk.gov.tr (14.03.2018).

⁴⁹³ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 624.

⁴⁹⁴ “Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.” 6698 sayılı Kanun md. 2.

⁴⁹⁵ Aksi kanaat hareketin şeklinin tipte ayrıca belirlenmiş olduğu ve suçun bağlı hareketli olduğuna ilişkin bkz. ÖZBEK, DOĞAN vd., *Türk Ceza Hukuku Özel Hükümler*, s. 574.

⁴⁹⁶ “Sanık hakkında iletişimin tespiti kararı da bulunmadığından, hükme dayanak yapılan iletişimin tespiti tutanaklarının” içeriğine göre, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçuna vücut verebilecektir. Bu konu içtima bahsinde ayrıca haberleşmenin gizliliği ihlal suça bakımından da ele alınacaktır. Yargıtay 1. CD., E: 2008/8783, K: 2009/437, T: 06.02.2009 www.kazanci.com (08.02.2018).

⁴⁹⁷ SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 350.

⁴⁹⁸ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 624.

almak, çizmek, işaretlemek⁴⁹⁹ şeklinde de gerçekleştirilebilir. Bunun yanı sıra doktrinde; Kanun'un gerekçesindeki açıklamanın aksine bu suçun işlenebilmesi için verilerin mutlaka bir araç kullanılarak kaydedilmesi gerektiği, dolayısıyla kağıt üzerine yazmak, ezberlemek veya okumak suretiyle kişisel verilerin kaydedilmiş olmayacağı yönünde isabetli görmediğimiz kanaatler de mevcuttur. Buna göre, kişisel veriler daha çok bilişim sistemleri üzerinde ve bir bilişim aracına ihtiyaç duyularak kaydedilmektedir.⁵⁰⁰ Ancak bu sebeple suçun oluşabilmesi için verilerin kaydedilmesinde bir aracın kullanılmasını aramak yerine, kaydetme eyleminin verilerin saklanması ve tekrar kullanılmasına elverişli şekilde gerçekleştirilmiş olması kanaatimizce yeterli ve daha yerinde olacaktır.⁵⁰¹ Örneğin; bir arkadaşımızdan başka bir arkadaşımızın telefon numarasını istediğimiz de ve numarayı telefonumuza veya ajandamıza kaydettiğimizde kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunu işlemiş oluruz. Her ne kadar hukuka uygun olarak elde etmiş olsa da, karşı tarafın rızası olmaksızın telefonundaki numarayı bizimle paylaşan kişi de kişisel verilerin hukuka aykırı olarak verilmesi suçunu işlemiş olur.⁵⁰²

Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu, kişisel verilerin kaydedilmesi işleminin gerçekleşmesiyle tamamlanmış olan ve somut başkaca bir sonuç doğurması aranmayan neticesiz bir suç olarak kabul edilmektedir.⁵⁰³ Ancak doktrinde her suçun muhakkak bir neticesinin olduğu ve şekli suçlarda, tıpkı hakaret, iftira, tehdit suçlarında olduğu gibi, bu neticenin harekete bitişik olabileceği kanaatini benimseyen müellifler⁵⁰⁴; kişisel verilerin kaydedilmesi suçunda da kaydetme

⁴⁹⁹ HAFIZOĞULLARI, ÖZEN, *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar*, s. 288.

⁵⁰⁰ ÖZBEK, DOĞAN vd., *Türk Ceza Hukuku Özel Hükümler*, s. 574.; DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 625.

⁵⁰¹ ŞENER, “Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu, s. 76.

⁵⁰² “Bu açıklamalar ışığında somut olay incelendiğinde, sanık Turgut'un, ayrıldığı kız arkadaşı olan şikayetçinin, kendisinde kayıtlı olan kişisel veri niteliğindeki telefon numarasını, şikayetçinin rızası dışında diğer sanık Onur'a verdiği olayda; şikayetçinin telefon numarasını hukuka aykırı olarak yayan sanık Turgut ile telefon numarasını hukuka aykırı olarak ele geçiren sanık Onur'un eyleminin, TCK'nın 136/1. maddesine uyan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden, ayrı ayrı mahkumiyetleri yerine, “telefon numarası vermek şeklinde gerçekleşen eylemin kişisel verilerin ele geçirilmesi ve yayılması olarak değerlendirilemeyeceği” biçimindeki isabetsiz gerekçeyle beraatlerine karar verilmesi” Yargıtay 12. CD., E: 2014/607, K: 2014/16665, T: 7.7.2014 www.kazanci.com (08.02.2018).; AKDAĞ, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s. 109.

⁵⁰³ Suçun tamamlanması için bir neticenin ve dış dünyada bir değişikliğin gerçekleşmesinin aranmadığı suç tiplerine “sırf hareket suçu” veya her suçun bir neticesi olduğu ve şekli suçlarda bu neticenin harekete bitişik olduğu kabulünde bulunan müelliflere göre “neticesi harekete bitişik suç” denilmektedir. KOCA, ÜZÜLMEZ, *Türk Ceza Hukuku Genel Hükümler*, s. 164.

⁵⁰⁴ HAKERİ, Hakan, *Ceza Hukuku Genel Hükümler*, 14. Baskı, Ankara, Adalet Yayınevi, 2012, s. 148.; İÇEL, Kayıhan, *Ceza Hukuku Genel Hükümler*, 4. Baskı, İstanbul, Beta Basım, 2017, s. 283.

eyleminin neticeyi içinde barındıran, hareketin yapılmasıyla neticenin eş zamanlı olarak gerçekleştiği diğer bir deyişle hareketin neticeden yer ve zaman bakımından ayrılması mümkün olamayan neticesi harekete bitişik bir suç olduğunu kabul etmektedirler.⁵⁰⁵ Katıldığımız bu kanaate göre; kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu, netice olarak kaydetmenin gerçekleşmiş olmasının aranmasını gerektiren, neticesi harekete bitişik bir suçtur. Bu suça ancak kaydetmenin gerçekleşmemiş olduğu ve icra hareketlerinin tamamlandığı aşamada teşebbüs gündeme gelebilecektir. Böyle bir durumla karşılaşılması ise neticesi harekete bitişik suçlar bakımından oldukça istisnaidir.⁵⁰⁶ Hafızogulları'na göre de; neticesiz ani hareketli bir suç olmakla birlikte, bu suçun kayıt işinin bitirilmesinden önceki aşamada teşebbüs aşamasında kalabilecektir.⁵⁰⁷

ii. Manevi Unsur

Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu kasten işlenebilen bir suç olarak Kanun'da düzenlenmiştir.⁵⁰⁸ Failin suç işlemeye yönelik kastının doğrudan veya olası kast olması mümkündür. Ancak suç tipinde bu suçun taksirle işlenebilirliğine ilişkin özel bir hüküm yer almadığından, taksirle işlenen verilerin hukuka aykırı olarak kaydedilmesi suçu cezalandırılamamaktadır. Bu suçun özellikle 1. fıkrası ve 2. fıkrasında sayılan bazı verilerin, özel olarak hukuka aykırılık bilinciyle kaydedilmiş olmasının, tipiklikte aranması ise doktrinde tartışılan bir konu olmuştur. Bazı yazarlar; suç tipinde "hukuka aykırılık" özel olarak yer almaktaysa, hukuka

⁵⁰⁵ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 625.

⁵⁰⁶ "Neticesi harekete bitişik suçlardan olan cinsel saldırı suçu vücuda dokunulmasıyla, nitelikli cinsel saldırı suçu mağdurun vücuduna organ veya sair bir cisim sokulması ile tamamlanmaktadır. 6545 sayılı Kanunla yapılan değişiklik sonrasında ise cinsel davranışın sarkıntılık düzeyinde kalması hâlinde daha az cezaya hükmolunması öngörülmüştür. Neticesi harekete bitişik suçlarda icra hareketlerinin bölünebildiği durumlarda suça teşebbüs mümkün olduğundan, fail cinsel saldırı suçunu işlemek kastıyla doğrudan doğruya icra hareketlerine başlamış, ancak elinde olmayan engel nedenlerle tamamlayamamış ise suça teşebbüs söz konusu olacaktır." Yargıtay CGK., E: 2014/572, K: 2015/2, T: 17.02.2015. www.legalbank.net (01.02.2018).

⁵⁰⁷ HAFIZOĞULLARI, ÖZEN, *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar*, s. 288.

⁵⁰⁸ "Açıklanan nedenlerle; sanığın Astronomi Bölümü'nde öğretim üyesi olduğu halde Matematik Bölümü öğrencisi katılan hakkında eğitim ve öğretim hakkını engelleyecek şekilde yetkisiz tutanaklar tuttuğu gibi, bina ana girişinde kapıdan içeri girişi engelleyecek şekilde durduğu, kapıyı arkadan tuttuğu, rızası dışında fotoğraf çektiği, katılan perukla dahi geldiğinde bu şekilde engellemelerde bulunduğu, katılanın başörtülü olması nedeni ile hakaret oluşturan beyanlarda bulunduğu tutanaklar, belirtilen tanık ifadeleri ile anlaşılmıştır. Sanığın çekmiş olduğu fotoğrafları dosyaya ibraz etmiş olması nedeniyle TCK'nın 135. maddesindeki kişisel verilerin hukuka aykırı olarak kaydedilmesi kastıyla hareket etmediği kanaatine varılmıştır." Yargıtay 4. CD., E: 2013/835, K: 2013/17101, T: 03.06.2013www.kazanci.com (08.02.2018).

aykırılığın tipikliğin bir unsuru olarak ele alınması ve failin suçu bu bilinçle işlemiş olmasının aranması gerektiği kanaatindedir. Dolayısıyla bu kanaate göre, failin kastının hukuka aykırılığı da kapsamı gerekmektedir⁵⁰⁹ ve suç sadece doğrudan kastla işlenebilmektedir.⁵¹⁰ Failin, hukuka aykırı olarak hareket ettiğine ilişkin bilinci tam olmalıdır. Diğer bir kısım müellif ise; Kanun normunda hukuka aykırılığa özel olarak yer verilmiş olmasını, suç tipindeki fiilin hukuka uygun olarak da gerçekleştirilebileceğini belirtmek amacıyla yer verildiğine dayandırarak açıklamaktadırlar. Buna göre; 135. madde de suç olarak düzenlenmiş olan kişisel verilerin kaydedilmesi fiilinin, hukuka uygun olarak da gerçekleştirilebilmesi mümkündür ve kanun lafzında arandığı gibi hukuk düzenine bir aykırılık bulunmadıkça suç da oluşmayacaktır.⁵¹¹ Dahası bu kanaate göre; kişisel verilerin bir hukuk normuna dayanılarak işlenmiş olmasının, Kanun'un suç olarak düzenlediği bu eylemi hukuka uygun kılabilmesi için, Kanun'un lafzında verilerin “hukuka aykırı olarak” kaydedilmesi, ibaresine özel olarak yer vermiş olması gerekmektedir.⁵¹² Kanaatimizce isabetli olmayan bu görüş, hukuka aykırılık bahsinde tekrar değerlendirilecektir. Buna karşılık Kanun'un lafzında “hukuka aykırı olarak” ifadesine yer verilmiş olmasının, aslında özel bir anlam taşımadığı, hukuka aykırılığa özel olarak yer veren diğer suç tiplerine ilişkin uygulamalar da gözlemlendiği üzere bu suçlara ilişkin yargılamada farklı bir usul benimsenmemiş olduğunu söyleyebiliriz. Buna göre, Kanun'un lafzında hukuka aykırılığın özel olarak yer aldığı suçlarda da diğer suç tiplerinde olduğu gibi hukuka aykırılık karine olarak mevcut kabul edilmektedir ve yargılamada hakim in özel olarak failin hukuka aykırılık bilinci taşıyıp taşımadığına ilişkin bir ispat faaliyeti yürütebilmesi söz konusu değildir.⁵¹³

⁵⁰⁹ “Kişinin, bir daha kanıt elde etme olanağının bulunmadığı ve yetkili makamlara başvurma imkanının olmadığı ani gelişen durumlarda, örneğin; kendisine karşı işlenmekte olan (cinsel saldırı, hakaret, tehdit, iftira veya şantaj gibi) bir suç söz konusu olduğunda ya da kendisine veya aile birliğine yönelen, onurunu zedeleyen, haksız bir saldırıyı önlemek için, kaybolma olasılığı bulunan kanıtların kaybolmasını engelleyip, yetkili makamlara sunarak güvence altına almak amacıyla, saldırıyı gerçekleştiren tarafın bilgisi ve rızası dışında, özel hayata ait bilgileri okuma, konuşma ve haberleşme içeriklerini veya özel hayata ilişkin ses ve görüntüleri dinleme, izleme ya da kaydetme, kişisel verileri kaydetme, ele geçirme ve yayma eylemlerinin hukuka aykırı olduğunu kabul etmek mümkün olmadığı gibi, esasen bu hallerde, kişinin hukuka aykırı hareket ettiği bilinciyle hareket ettiğinden de söz edilemeyeceği gözetildiğinde” Yargıtay 12. CD., E: 2013/14958, K: 2014/3723, T: 17.02.2014 www.kazanci.com (08.02.2018).

⁵¹⁰ KOCA, ÜZÜLMEZ, *Türk Ceza Hukuku Özel Hükümler*, s. 506.; MENDOS KUŞKONMAZ, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, s. 144.

⁵¹¹ ŞENER, “Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu, s. 78., 84.;

⁵¹² ÖZBEK, DOĞAN vd., *Türk Ceza Hukuku Özel Hükümler*, s. 579.

⁵¹³ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 628.

Kunter'e göre; suç tipinde hukuka özel aykırılığın arandığı hallerde; hem failin hukuka aykırı hareket ettiği bilincine sahip olması özel olarak aranmalıdır hem de ispata ilişkin olarak, savcı tarafından iddia edilenin aksine failin hukuka aykırılığın bilincinde olmadığını ispat etme mükellefiyeti bulunmaktadır. Buna göre failin, hukuka aykırılık bilinciyle hareket etmediğini ispat etmesi, aynı zamanda suçun manevi unsurunun da bulunmadığının da ispatlanmış olduğu anlamına gelecektir.⁵¹⁴ Kanaatimizce de suç tipinde özel olarak aranan “hukuka aykırılık” suçun manevi unsuruyla ilişkili olarak ele alınması gereken bir husus olup, her somut olayda failin bu bilinçle hareket edip etmediği değerlendirilmelidir.

iii. Hukuka Aykırılık Unsuru

Ceza hukuku bakımından hukuka aykırılık; failin işlediği tipe uygun fiil ile hukuk düzeni arasında çatışma bulunması⁵¹⁵, “fiilin hukuk nizamına uygun olmaması”⁵¹⁶ olarak tanımlanmaktadır. Hukuk düzeni ile kast olunan ceza hukuku değil bütün hukuk düzenleri ile suç teşkil eden fiilin aykırılığıdır. Eğer ki bir hukuk normuyla fiil, hukuka uygun kabul edilmişse artık bu fiilin suç olarak cezalandırılabilirliği söz konusu olamayacaktır. Zira hukuk düzeni bir bütündür. Birine göre hukuka uygun kabul edilen eylemin diğeri tarafından suç olarak kabul edilmesi mümkün değildir. Bu itibarla şunu diyebiliriz ki; ceza hukuku bakımından suç olarak kabul edilen her eylem aslında hukuk düzeni ile çatışma içerisindedir, velev ki bu eylemi hukuka uygun kılacak bir kural getirilmiş olmasın. Tipiklikte, “hukuka aykırılık” özel olarak aransa da aranmasa da, suç teşkil eden fiile izin veren bir hukuk normunun mevcut olması, fiil ile hukuk düzeni ile arasındaki çatışmayı ortadan kaldıracaktır. Böylelikle eylem hukuka uygun hale gelmiş olacaktır ve bu durum, ceza kanunlarında suç olarak düzenlenmiş olan her türlü eylem için söz konusu olabilir. Bu sebeple, TCK'nın 135. maddesinde suç olarak düzenlenen, kişisel verilerin kaydedilmesi fiiline de, tipiklikte hukuka aykırılığın özel olarak yer alıp almamasına bakılmaksızın, hukuk düzeni içerisindeki bir normla izin verilebilmesi mümkündür. Bu durumda kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun oluşmasına engel bir hukuka uygunluk sebebinin mevcut olduğunu söylememiz gerekecektir.

⁵¹⁴ KUNTER, Nurullah, *Suçun Maddi Unsurları Nazariyesi*, İstanbul, İsmail Akgül Matbaası, 1954, s. 66.

⁵¹⁵ ALACAKAPAN, Uğur, *Suçun Unsurları*, Ankara, Sevinç Matbaası, 1975, s. 95.

⁵¹⁶ KUNTER, , *Suçun Maddi Unsurları Nazariyesi*, s.110.

Dolayısıyla bu suç tipinde, suç teşkil eden kişisel verilerin kaydedilmesi fiilinin hukuka uygun olarak da gerçekleştirilebileceğine işaret etmek için, hukuka aykırılığın özel olarak düzenlenmiş olduğu şeklindeki kanaate iştirak edemiyoruz.⁵¹⁷

Hukuka uygunluk sebepleri, ceza hukukunun suç saydığı bir fiilin yapılmasına yetki tanınması veya yapan kişi bakımından fiilin görev olarak düzenlenmiş olması şeklindeki fiilin gerçekleşme aşamasından önce mevcut olması gereken sebeplerdir. Bu sebeplerin fiilin işlenmesinden önceki aşamada mevcut olmadıkları takdirde, gerçekleştirilen eylemin sonradan bu sebeplerden birinin oluşmasına bağlı olarak hukuka uygun hale gelmesi söz konusu olamaz.⁵¹⁸ Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu bakımından da ilgilinin rızası ve kanun hükmünün yerine getirilmesi hukuka uygunluk sebeplerinin, suçun işlenmemiş olduğu aşamada mevcut olması halinde, işlenen bu fiilden dolayı faile ceza verilemeyecektir.⁵¹⁹

İlgilinin rızası, 5237 sayılı Türk Ceza Kanunu’nun 26/2. fıkrasındaki “Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez” şeklindeki düzenlemesine göre; failin, en geç suçun icra hareketlerine başlamış olduğu sırada mevcut olan ilgilinin rızasına bağlı olarak işlediği suç niteliğindeki eylemi cezalandırılmayacaktır. Bu düzenleme ilgilinin, kendisine karşı gerçekleştirilen ve suç teşkil eden fiile ilişkin gösterdiği rızanın taşıması gereken bazı özelliklere de işaret etmektedir. Buna göre suç teşkil eden fiilin, münhasıran kişinin üzerinde mutlak surette tasarruf edebileceği bir hakka yönelmiş olması veya diğer bir deyişle gösterilen rızanın üzerinde mutlak surette tasarruf edilebilen bir hakka ilişkin olarak verilmesi gerekmektedir. Bu sınırlandırıcı hüküm uyarınca, ilgilinin rızasının hukuka uygunluk sebebi olarak kabulü ancak belli istisnai hallerde söz konusu olabilmektedir. Zira ceza mevzuatımızda düzenlenmiş olan pek çok suç tipi ile korunan hukuksal yarar; münhasıran kişilerin şahsi yararına değil, bunun yanında toplumsal yarara da yöneliktir. Kanaatimizce, korunan hukuksal yararın, kişilerin kişilik olarak gelişimi ve

⁵¹⁷ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 627.; ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 579.

⁵¹⁸ Hukuka uygunluk sebepleri eylemi en geç gerçekleştirilmeye başladığı andan itibaren hukuka uygun hale getirmektedirler. ALACAKAPAN, *Suçun Unsurları*, s. 79.

⁵¹⁹ “Kişinin rızası ile kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı muhakkaktır. Belirli nitelikteki kişisel verilerin kayda alınması kanun hükmünün gereği olarak yapılmaktadır. Bu bakımdan, çeşitli kamu kurumlarında verilen kamu hizmetinin gereği olarak kişilerle ilgili bazı bilgiler ilgili kanun hükümlerine istinaden kayda alınmaktadır. Bu durumlarda, söz konusu suç oluşmayacaktır.” TCK Gereke Madde 135.

kendi kaderini tayin edebilme özgürlüğü ile bağlantılı olduğu hallerde, ilgilinin suç teşkil eden fiile gösterdiği rıza hukuka aykırılığı ortadan kaldıracaktır.⁵²⁰ Bu durumda suç tipinde korunan hukuksal yarara göre üzerinde mutlak surette tasarruf edilebilecek bir hak olup olmadığı değerlendirmesi yapmak gerekirse; TCK'nın 135. maddesinde düzenlenen kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunda korunan hukuksal yarar, genelde özel yaşamın gizliliği özelde ise kişisel verilerin korunması hakkı oluşu ve bu hakların temelini de kişilerin kendi kaderini tayin edebilme özgürlüğü oluşturduğu için, bu suç bakımından ilgilinin üzerinde mutlak surette tasarruf edebileceği bir hakkının bulunduğu ve rızanın bir hukuka uygunluk sebebi olarak kabul edilebileceğini söyleyebiliriz. Ancak doktrinde bu suçun kişilerin özel hayatlarına dahil olan kişisel verilerinin gizliliğinin korunması hususundaki ferdi ve kamusal yararın korunması hukuksal yararını konu edindiği istikametindeki kanaatlere de rastlanmaktadır.⁵²¹ Ancak, bu müellifler aynı zamanda ilgilinin suça göstermiş olduğu rızayı da hukuka uygunluk sebebi olarak kabul etmekte ve kanaatimizce bu hususta çelişmektedirler. Doktrinde bir başka değerlendirmeye göre de; suçun soruşturulması ve kovuşturulması bakımından şikayet aranmadığından ve re'sen soruşturulan bu tarz suçlarda kural olarak, mağdurun üzerinde mutlak surette tasarruf edebileceği bir hakkının bulunmadığı kabul edildiğinden, ilgilinin rızasının kişisel verilere karşı işlenen suçlarda hukuka uygunluk sebebi olarak kabul edilmesi söz konusu değildir.⁵²²

6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre de kişisel verilerin işlenmesi yasağına ilişkin temel istisna veya işlemeyi hukuka uygun kılan temel sebep;⁵²³ ilgilinin, “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan”⁵²⁴ açık rızasının bulunmasıdır. Bu düzenlemeye göre, ilgili tarafından verilebilecek rıza, aynı zamanda veri sorumlusunun verileri hangi sınır, kapsam, şekil ve süre koşullarında işleyebileceğine ilişkin yol göstericilik niteliği de

⁵²⁰ ARTUK, GÖKCEN, YENİDÜNYA, *Ceza Hukuku Genel Hükümler*, s. 433.

⁵²¹ HAFIZOĞULLARI, ÖZEN, *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar*, s. 287.

⁵²² ÖZBEK, DOĞAN vd., *Türk Ceza Hukuku Özel Hükümler*, s. 582.

⁵²³ “Açık rıza, 6698 sayılı Kanun'da hem özel nitelikli kişisel veriler, hem de özel nitelikli olmayan kişisel veriler bakımından temel hukuka uygunluk sebebi olarak öngörülmüştür. Buna göre sırasıyla Kanun'un; 5. maddesinin, 1. fıkrasına göre “Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez”, 6. maddesinin 2. fıkrasına göre “Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır”, 8. maddesinin 1. fıkrasına göre “Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz”, 9. maddesinin 1. fıkrasına göre “Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.” KVK Kurumu Yayınları, Açık Rıza, s. 2., <https://www.kvkk.gov.tr> (08.01.2018).

⁵²⁴ KVK md. 3/1 a.

taşımaktadır.⁵²⁵ 6698 sayılı Kanun'un veri işlemeye ilişkin verilebilecek açık rızanın taşınması gereken unsurlarının, TCK'nın 26. maddesine göre daha sınırlandırıcı olduğu şüphesizdir.⁵²⁶ Hukuka uygun veri işlemenin temel koşulları arasında sayılan ilgilinin rızasına ilişkin aranan bu özellikler çalışmamızın ilk bölümünde kapsamlı olarak ele alındığından burada tekrara düşmemek adına konudan bu kadar bahsedilmesi uygun görülmüştür.⁵²⁷ Ancak her iki düzenleme bakımından da rızanın muteberlik taşıyabilmesinin ortak koşulları; ilgilinin rıza göstererek üzerindeki haklarından vazgeçtiği değerin anlam ve içeriğinin ayırdında olması,⁵²⁸ ne şekilde verildiği fark etmeksizin verilen rızanın serbest iradeye dayanması⁵²⁹ ve kişisel verilerin kaydedilmesine/işlenmesine ilişkin rızanın en geç eylemin gerçekleştirildiği sırada verilmiş olmasıdır.⁵³⁰

Kişisel verilerin hukuka aykırı olarak kaydedilmesine ilişkin ilgilinin göstermiş olduğu rıza; uygulamada, genellikle kişilerin kendi iradeleriyle sosyal medya üzerinden ve herkese açık olarak paylaştıkları kişisel verilerinin, bu şekilde paylaşılmış olmasının başkaları tarafından işlenmesine ilişkin rızaları olduğu anlamına

⁵²⁵ KVK Kurumu Yayınları, Açık Rıza, s. 4., <https://www.kvkk.gov.tr> (02.03.2018).

⁵²⁶ “Kanuna göre açık rızanın üç unsuru vardır:

- a. Belirli bir konuya ilişkin olma: Açık rıza beyanının kapsamı genel nitelikte olmamalı, belirli bir sunulması için kişisel verilerinizin işlenmesine açık rıza veriyor musunuz?” biçiminde rıza alınması durumunda, rıza “belirli bir konuya ilişkin” olmayacağı için geçerli bir rıza olarak kabul edilmeyecektir.
- b. Bilgilendirmeye dayanma: Elde edilecek kişisel verilerin hangi amaçlarla kullanılacağı açıkça belirtilmeli, kişinin anlamayacağı terimler ya da yazılı bilgilendirme yapıldığında okumakta güçlük çekeceği oranda küçük puntolar kullanılmamalıdır.
- c. Özgür iradeyle açıklanmış olma: Bir irade beyanı olan “rıza” beyanının kişinin özgürlüğünü etkileyecek hallerden arınmış olması gerekmektedir. Bu doğrultuda, “açık rıza” beyanını veren veri sahibinin iradesini bozacak bir durum mevcut olmamalıdır.” KVK Kurumu Yayınları, 6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar, s. 21., <https://www.kvkk.gov.tr> (02.03.2018).

⁵²⁷ Bkz. s. 24-26.

⁵²⁸ Verilerinin kaydedilmesine yönelik olarak veri öznesinin veya mağdurun vermiş olduğu rızanın, konu, amaç vb. hususlara ilişkin aydınlatılmış yada diğer bir deyişle bilgilendirilmiş olarak verilmesi rızaya muteberlik kazandıracak önemli bir unsur olarak kabul edilmektedir. Bu unsurun yerine getirilmesiyle dolaylı olarak da kişisel verilerin “amaçla bağlılık ilkesine” uygun olarak işlenmesi temin edilmiş olabilecektir. AKDAĞ, “Türk Ceza Hukukunda Kişisel Verilerin Korunması İlkeleri”, s. 34.; 6698 sayılı Kanun md. 4

⁵²⁹ “Tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi gerekir. Özellikle işçi-işveren ilişkisinde, işçiye rıza göstermeme imkânının etkin bir biçimde sunulmadığı veya rıza göstermemenin işçi açısından muhtemel bir olumsuzluk doğuracağı durumlarda, rızanın özgür iradeye dayandığı kabul edilemez.” KVK Kurumu Yayınları, Açık Rıza, s. 7., <https://www.kvkk.gov.tr> (02.03.2018).

⁵³⁰ “Bilgilendirmenin mutlaka verinin işlenmesinden önce yapılması gerekir. İşlenecek verinin niteliği, aynı zamanda bilgilendirme düzeyini belirleyecektir. İlgili kişinin aydınlatılması aynı zamanda kişinin kendi geleceğini belirleme hakkının bir yansıması oluşturmaktadır.” KVK Kurumu Yayınları, Açık Rıza, s. 6., <https://www.kvkk.gov.tr> (02.03.2018).

gelip gelemeyeceği tartışmaları ile karşımıza çıkmaktadır. Hem 6698 sayılı Kanun’a hem de TCK’ya göre kişilerin herhangi bir şekilde bağlı kalmaksızın rıza beyanında bulunmaları mümkündür. Türk Ceza Hukuku’na göre rızanın; açık veya zımni, yazılı veya yazısız olarak verilebilmesi mümkündür.⁵³¹ 6698 sayılı Kanun’a göre de açık rızanın muteberliği, en azından kişinin rıza gösterdiğine ilişkin tereddüt bırakmayacak belli emarelerin mevcut olmasına bağlı kabul edilmiştir.⁵³² Bu durumda, kişinin kendisi hakkında herkese açık olarak paylaştığı bilgilerin, başkaları tarafından işlenmesine ilişkin rızasının bulunduğu kabul edilebilmesi kanaatimizce, en azından somut olayda buna ilişkin belli ipuçlarının bulunmasına bağlı olmalıdır. Kişilerin bu eyleminin, kişisel verilerin işlenmesine yönelik genel geçer bir rıza beyanı olarak kabul edilmesi, aynı zamanda kişisel verilerin hukuka aykırı olarak işlenmesini suç olarak düzenleyen maddelerin konuluş amacı ve ruhuna da aykırılık teşkil edecektir.⁵³³ Yargıtay Ceza Genel Kurulu’nun da, kişinin köşe yazarlığı yaptığı gazetede herkesin erişimine açık olarak yer alan resminin, başkaları tarafından işlendiği olayda; resmini kendi rızasıyla herkese açık olarak internete yüklemiş olması sebebiyle ilgilinin, zımni olarak daha sonraki kişisel verilerinin işlenmesi niteliğindeki eylemlere de rıza göstermiş bulunduğu çıkarımı kabul edilmeyerek, bu eylemin suç oluşturduğu istikametinde içtihatla bulunulmuştur.⁵³⁴

İşçinin kişisel verilerinin, işveren tarafından hukuka aykırı olarak kaydedilerek işlenmiş olduğu iddiasıyla, Anayasa Mahkemesi’nin önüne gelen bir uyuşmazlıkta da Mahkeme; işçinin, iş sözleşmesinde yazan yasaklayıcı hükümleri imzalamakla işverenin bu hükümler uyarınca gerçekleştirdiği veri işleme faaliyetleri karşısında korunmasını bekleyemeyeceği ve gerektiğinde verilerin işveren tarafından işlenebileceğine ilişkin sözleşmede ikazda da bulunulduğundan, işçinin rızasının

⁵³¹ ARTUK, GÖKCEN, YENİDÜNYA, *Ceza Hukuku Genel Hükümler*, s. 439.

⁵³² Bkz. s. 24.

⁵³³ SEYREK TÜTÜNCÜBAŞI, *Kişilerin Kendisine Ait Verilerin Kaderini Tayin Hakkının Ceza Hukuku Yoluyla Korunması*, s. 98.; “Örneğin; daha önce bir yerel gazetede yer almış olan bilginin daha sonra, televizyonda, internette veya ülke çapında yayımlanan tirajı yüksek bir gazetede yer alması, şüphesiz çok daha fazla sayıda insan tarafından öğrenilmesine ve ilgili olduğu kişinin haklarının daha ağır ihlaline yol açacaktır.” AKDAĞ, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s. 122.

⁵³⁴ “Sanığın genel yayın yönetmenliğini yaptığı gazetede köşe yazarı olarak çalışan katılanın yazdığı köşesinde kullanılan fotoğrafın, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle sanık tarafından internetteki özel bir arkadaşlık sitesine kimlik, adres ve telefon bilgileri verilmeksizin ve erkek arkadaşı aradığı açıklamasıyla konulması eylemi, TCK’nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçunu oluşturmaktadır.” Yargıtay CGK., E: 2012/12-1510, K: 2014/331, T: 17.06.2014 www.kazanci.com (04.01.2018).

mevcut olduğunun kabul edilerek ihlalin bulunmadığına karar vermiştir. Kararın gerekçesi; “İş sözleşmelerinin parçası olan düzenlemeler ile şirket kaynaklarının, bilgisayarların, kurumsal e-posta hesaplarının kişisel amaçlar doğrultusunda kullanımı kesin şekilde yasaklanmış; gerektiğinde yazışmaların ve iletişim kayıtlarının takip edilebileceği ve incelenebileceği hususunda başvuruculara gerekli uyarılar ve bilgilendirmeler yapılmıştır. Bunun yanında, kurumsal olmadığı sürece kişisel hesapların ve kişisel iletişim vasıtalarının mesai saatleri içerisinde kullanılma imkânı olmasına ve buna ilişkin bir engel bulunmamasına rağmen, yapılan işin gerekleriyle ilgisi olmayan yazışmaların iş sözleşmelerine aykırı biçimde mesai saatleri içerisinde kurumsal hesaplar üzerinden gerçekleştirildiği anlaşılmaktadır. Bu nedenlerle başvurucuların kurumsal e-posta hesapları üzerinden gerçekleştirdikleri kişisel yazışmaların korunması konusunda makul bir beklenti içinde oldukları sonucuna ulaşamaz.”⁵³⁵ şeklindedir.

Benzer bir olay da Yargıtay 9. Hukuk Dairesi; “İşverenin kendisine ait bilgisayar ve e-mail adresleri ile bu adreslere gelen e-postaları her zaman denetleme yetkisi bulunmakta” olduğunun kabulüne dayanarak, işçinin bu e-posta hesapları üzerinden işveren hakkında hakaret içeren maillerin gönderilmiş olmasını haklı fesih sebebi olarak kabul etmiştir.⁵³⁶ Ancak kararda benimsenen şekilde işverenin, her koşulda işçinin işyerinde kullandığı ve kendisine ait kişisel verilerin bulunduğu bilgisayar ve e-postaları denetleyebilme veya bunları kaydedebilme yetkisinin bulunduğu kabul edilebilirliği söz konusu olamaz. Eğer ki, işçi ve işveren arasında imzalan iş sözleşmesi hükümlerinde veya başka bir şekilde, işçiye tahsis olunan bilgisayar ve e-posta hesaplarının, işveren tarafından her zaman denetlenebileceği konusunda işçi bilgilendirilmemişse işverenin, işçiye ait kişisel verileri kararda belirtilen şekilde kaydetmesi eylemine ilişkin işçinin rızasının bulunduğu da kabul edilemeyeceğinden, yapılan işleme hukuka aykırı olacaktır. Ancak işletmede çalışan kişilerin rızasına dayanarak, işyerine ait bilgisayar ve işyeri uzantılı e-postaların işveren tarafından denetlenmesi ve kaydedilmesi, özel hayatın gizliliğinin ihlali ve

⁵³⁵ Anayasa Mahkemesi, Ömür Kara - Onursal Özbek Başvurusu

⁵³⁶ Yargıtay 9. HD., E: 2010/37516, K: 2009/447, T: 13.12.2010.

kişisel verilerin hukuka aykırı olarak kaydedilmesi suçları, bakımından hukuka uygunluk sebebi olarak kabul edilebilecektir.⁵³⁷

Türk Ceza Kanunu'nun 24. maddesi ile hukuka uygunluk sebepleri arasında kabul ettiği ve 6698 sayılı Kanun'un da 5. maddesinin 2. fıkrasının a. bendinde yer verdiği kişisel verilerin işlenmesini hukuka uygun kılan istisnai hallerden birisi de;⁵³⁸ “kanunun hükmünün yerine getirilmesi” dir. Buna göre; kişisel verilerin bir hukuk normuna uygun olarak kaydedilmesi işlenen hukuka aykırı fiili, suç olmaktan çıkarmaktadır.⁵³⁹ Kanun hükmünün icrası; hukuk düzenine dahil bir normun, bu tüzük veya yönetmelik de olabilir, kişilere belli koşullar söz konusu olduğunda bazı davranışlarda bulunabilme yetkisi tanınması olarak tanımlanmaktadır.⁵⁴⁰ Bu yetki daha ziyade kamusal düzen, istikrar ve refahın gereklerine uygun kamusal faaliyet yürüten kişi ve kurumlara tanınmaktadır. Örneğin; “*kesinleşmiş ceza ve güvenlik tedbirlerine mahkûmiyete ilişkin bilgilerin otomatik işleme tâbi bir sistem kullanılarak toplanmasına, sınıflandırılmasına, değerlendirilmesine, muhafaza edilmesi*” amacıyla düzenlenmiş olan Adli Sicil Kanunu, kişisel veri niteliği taşıyan mahkumiyet bilgilerinin adli sicillerde kayıt altına alınması, saklanması ve depolanmasına ilişkin yetki verici hükümler içermektedir.⁵⁴¹ Bu itibarla adli sicil kayıtlarını Adli Sicil

⁵³⁷ TEZCAN, Durmuş, “Özel Hayatın Gizliliğini İhlal ve Kişisel Verilerin Kaydedilmesi Suçu İle İlgili Bazı Gözlemler”, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 71, S. 1, 2013, s. 1161-1164.

⁵³⁸ Kişisel verilerin işlenmesine ilişkin temel esas ve usulleri düzenleyen 6698 sayılı Kişisel Verilerin Korunması Kanunu 5. maddesinde hangi hallerde kişisel verilerin işlenmesinin/kaydedilmesinin kanunun tanıdığı yetki çerçevesinde olabileceği düzenleme altına alınmıştır. Kanun'un 5. maddesine göre; kişisel verileri işlenen ilgilinin işlemeye rızasının bulunması temel hukuka uygun veri işleme sebebi olarak kabul edilmiştir. Bunun yanında; hukuk düzenine dahil olan diğer kanunlarda açıkça kişisel verilerin kaydedilebileceğinin öngörülmüş olması; ilgilinin kişisel verilerinin kaydedilmesine rıza gösterebilecek durumda olmaması veya hukuken rıza verme ehliyeti olmaması veya kendisi veya başka bir kişinin hayat ve vücut bütünlüğünün korunması için verilerin kaydedilmesi zorunluluğunun olması; ilgilinin tarafı olduğu bir sözleşmenin ifası veya kurulması gereğince kişisel verilerin kaydedilmesi gerekliliğinin bulunması; kişisel verilerin, veri sorumlularının hukuken yükümlü oldukları sorumluluklarını yerine getirmeleri için işlenmesinin zorunlu olması; kaydedilen verilerin ilgili kişinin kendisince alenileştirilmiş olması; bir hakkın kurulması, kullanılması veya korunması için kişisel verilerin kaydedilmesinin zorunlu olması ve ilgilinin temel hak ve özgürlüklerine zarar vermeyecek surette, veri sorumlusunun haklı çıkarları için kişisel verilerin kaydedilmesinin zorunlu olması hallerinde kişisel verilerin, ilgilinin rızası olup olmadığına bakılmaksızın işlenebilmesi 6698 sayılı Kanun'a göre mümkündür.

⁵³⁹ AKDAĞ, “Türk Ceza Hukukunda Kişisel Verilerin Korunması İlkeleri”, s. 31.

⁵⁴⁰ ARTUK, GÖKCEN, YENİDÜNYA, *Ceza Hukuku Genel Hükümler*, s. 376.

⁵⁴¹ 2937 sayılı MİT Kanunu 6. maddesi de Teşkilatın, doğrudan veya dolaylı olarak kişisel verilerin kayıt altına alınmasına ilişkin yetki sahibi olduğunu düzenlenmektedir. Örneğin; 6. maddeye 2005 yılında ek fıkra olarak getirilmiş hüküm; “Bu Kanunun 4 üncü maddesinde sayılan görevlerin yerine getirilmesi amacıyla Anayasanın 2 nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerinin önlenmesine ilişkin olarak, hâkim kararı veya gecikmesinde sakınca bulunan hallerde MİT

Kanunu’nda öngörülen usulle tutan kamu görevlilerinin, kişisel verilerin kaydedilmesi suçundan cezalandırılması söz konusu olamayacaktır. Bunun dışında 5490 sayılı Nüfus Hizmetleri Kanunu gereğince tutulacak aile kütüklerine; vatandaşların ad, soyad, ana adı, baba adı, dini, yerleşim yeri gibi pek çok kişisel verisinin kaydedilebileceği de kanunen öngörülmüştür. 5271 sayılı Ceza Muhakemesi Kanunu uyarınca da kişisel verilerin işlenmesinin kanunen öngörüldüğü pek çok hal bulunmaktadır.⁵⁴² Yine 5429 sayılı Türkiye İstatistik Kanunun 7. maddesi uyarınca istatistik üretimi için gerekli görülen her türlü verinin istatistik birimlerinden (veri sahiplerinden) istenebilmesi ve bunların kayıt altına alınabilmesi kanun gereğince mümkün ve hukuka uygundur.

e. Suçun Özel Görünüş Biçimleri

i. Teşebbüs

TCK’nın 135.maddesinde düzenlenen bu suç, hukuka aykırı olarak verilerin kaydedilmesi eyleminin gerçekleştirilmesiyle tamamlanmış olan neticesi harekete bitişik bir sırf hareket suçudur. Kural olarak sırf hareket suçları teşebbüse elverişli kabul edilmemektedir.⁵⁴³ Ancak doktrinde hareketin parçalara ayrılabilirliği söz konusu ise, sırf hareket suçlarına da teşebbüsün mümkün olabileceği kanaati kabul görmektedir.⁵⁴⁴ Buna göre, failin iradesi dışındaki sebeplerle kişisel verilerin kaydedilmesine yönelik hareketi kesintiye uğrarsa, hareketin kesintinin gerçekleştiği aşamaya kadar gerçekleştirilen şekli başka bir suçu oluşturmuyorsa, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu teşebbüs aşamasında kalmış olacaktır.⁵⁴⁵ Örneğin; verilerin fail tarafından ele geçirildiği ancak kaydedilememiş olduğu

Müsteşarı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir.” şeklindedir.

⁵⁴² Kişisel verilerin ceza yargılamasında delil elde etmek amaçlı işlendiği bu hallere ilişkin ayrıntı için bkz. s. 70.

⁵⁴³ İÇEL, *Ceza Hukuku Genel Hükümler*, s. 524.; HAKERİ, *Ceza Hukuku Genel Hükümler*, s. 149.

⁵⁴⁴ “Neticesi harekete bitişik suçlarda icra hareketlerinin bölünebildiği durumlarda suça teşebbüs mümkündür. Eğer, fail cinsel saldırı suçunu işlemek kastıyla doğrudan doğruya icra hareketlerine başlamış, ancak elinde olmayan engel sebeplerle tamamlayamamış ise suça teşebbüs mevcuttur. Dikkat edilmelidir ki, vücuda dokunulduğu takdirde cinsel saldırı suçu tamamlanacaktır.” Yargıtay CGK., E: 2013/14-97, K: 2013/331, T: 05.07.2013 www.kazanci.com (04.01.2018).; SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 352.; DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 647.

⁵⁴⁵ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 625.

aşamada, failin kaydetmeye teşebbüsten değil kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçunun tamamlanmış şeklinden cezalandırılması gerekmektedir.⁵⁴⁶

ii. İştirak

TCK'nın 135. maddesinde suç olarak düzenlenmiş olan kişisel verilerin hukuka aykırı olarak kaydedilmesi eyleminin birden fazla faille gerçekleştirildiği durumda failler arasında suç ortaklığı (iştirak) gündeme gelecektir. Bu suç bakımından iştirak bahsinde değinilmesi gereken özellikli bir durum söz konusu olmayıp, TCK'nın 37, 38, 39 ve 40. maddelerinde sınıflandırdığı üzere, faillik, azmettirme ve yardım etme şeklinde suça iştirake ilişkin genel hükümlerin kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunda da uygulanması gerekmektedir.

iii. İçtima

Fail tarafından gerçekleştirilen eylemin hukuka aykırılığının tek bir suç tipi ile karşılanamayıp, kanunun birden fazla hükmü ile eylemin ilişkilendirilerek hukuka aykırılığın karşılanabildiği hallerde suçların içtimaı gündeme gelmektedir.⁵⁴⁷ 5237 sayılı Türk Ceza Kanunu, "*işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren*" kişinin eylemini, suçların fikri içtimasına ilişkin 44. maddesinde düzenlemiş olup, bu nitelikte bir eylemde bulunan faile en ağır cezayı gerektiren suçtan ceza verilmesini hüküm altına almıştır.⁵⁴⁸ Bu hükmün, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu bakımından üzerinde durulmasını gerektiren bir hüküm olduğunu söylememiz gerekmektedir. Özellikle, hukuksal konusu özel yaşamın gizliliğinin korunması olan TCK'nın dokuzuncu bölümündeki diğer suçlarla ve bilişim alanında işlenen onuncu bölümündeki suçlarla, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun içtimaı konusu uygulama ve doktrinde yorum farklılığı yaratmış bir husustur. Öncelikle kişisel verilere karşı işlenen diğer suç tipleriyle, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun tek fiille gerçekleştirilmiş olmasının, oldukça karşılaşılan bir ihlal şekli olduğunu

⁵⁴⁶ ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 582.

⁵⁴⁷ İÇEL, *Ceza Hukuku Genel Hükümler*, s. 574.

⁵⁴⁸ "6698 sayılı Kişisel Verilerin Korunması Kanunu'nda özel bir düzenleme yer almamakla birlikte, bir fiilin hem kabahat hem de suç oluşturması halinde faile sadece suçtan dolayı yaptırım uygulanması gerekmektedir." KVK Kurumu Yayınları, 6698 sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar, s. 76., <https://www.kvkk.gov.tr> (02.03.2018).

söyleyebiliriz. Failin tek bir fiili ile, aynı mağdura ilişkin kişisel verileri, hem kaydetme hem de yayma suçunu aynı anda işleyebilmesi mümkündür. Örneğin bir sosyal paylaşım sitesine veya kişilerin online erişim sağlayabileceği bir internet sitesine, mağdura ilişkin kişisel verilerin kaydedilmesi eylemi, aynı zamanda bu kişisel verilere üçüncü kişilerin erişmesini sağlayacağından, TCK'nın 136. maddesinde düzenlenen kişisel verilerin hukuka aykırı olarak verilmesi veya yayılması suçuna da vücut verecektir.⁵⁴⁹ Bu durumda “*bir fiille birden fazla farklı suçun oluşmasına sebebiyet veren*” faile, TCK'nın 44. maddesinde düzenlenen fikri içtima kuralı doğrultusunda en ağır cezayı gerektiren suç olarak, sadece kişisel verileri hukuka aykırı olarak verme veya yayma suçundan ceza verilmesi gerekir. Bu halde kişisel verileri yayma fiilinin haksızlık içeriğinde, 135. maddede düzenlenmiş olan kaydetme fiilin haksızlık içeriği de erimiş olacaktır.⁵⁵⁰

Bunun dışında özel hayata ve hayatın gizli alanın karşı işlenen suçların yer verildiği TCK'nın dokuzuncu bölümünde düzenlenmiş bulunan; kişiler arasındaki haberleşmelerin gizliliğinin ihlali (md. 132) ve kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi (md. 133) suçlarının konusu olan haberleşme veya konuşmaların, içeriğinin kişilere ilişkin kişisel veri niteliğinde bilgiler ihtiva ediyor olması durumunda, failin bu suçlarla birlikte aynı zamanda kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunu da işlemiş olacağı şüphesizdir.⁵⁵¹ Fail, haberleşme veya konuşmaları bir cihazla kayıt etmek şeklinde gerçekleşen tek fiiliyle, hem kişisel verilerin kaydedilmesi hem de aleni olmayan konuşmaların kaydedilmesi veya haberleşmenin gizliliğinin ihlali suçlarını işlemiş olacak ve fikri içtima hükümlerine göre gerçekleştirilen bu suçlardan daha ağır cezayı gerektiren, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçundan cezalandırılması gerekecektir.⁵⁵² Ayrıca gerçekleştirilen haberleşme veya konuşmanın birden fazla kişiye ait kişisel veriyi içeriyor olması halinde, tek fiille kişisel verilerin ilişkili olduğu kişi sayısı kadar suç

⁵⁴⁹ Kanaatimizce yerinde olmayan aksi istikamette değerlendirme olarak; “somut olayımız açısından, sanık tarafından oluşturulan sahte facebook profilinde, katılanın facebook profilinden elde edilen resimlerin yayınlanması eyleminin suç olarak kabul edilmesi halinde, eylemin kişisel verilerin kaydedilmesi suçunu değil, verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturabileceği” Yargıtay 12. CD., E: 2015/4349, K: 2016/5349, T: 30.3.2016 www.kazanci.com (08.02.2018).

⁵⁵⁰ ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 582

⁵⁵¹ AKDAĞ, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s. 116.

⁵⁵² KOCA, ÜZÜLMEZ, *Türk Ceza Hukuku Özel Hükümler*, s. 498.; GÜLTEKİN, N. Melek, *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*, (Yayımlanmamış Yüksek Lisans Tezi), Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2012, s. 154.

işlenmiş olacaktır ve faile verilecek cezada zincirleme suç hükümlerine göre de artırım yapılacaktır. Doktrinde bu suçların içtimaina ilişkin diğer bir görüşe göre; kişisel verilerin kaydedilmesi suçunun konusunu her hangi bir şekilde kaydedilmiş olan kişisel veri oluştururken, TCK'nın 132. veya 133. maddelerinin kapsamına, kişisel verilerin kaydedilme şekli ve niteliği itibarıyla sınırlandırılmış daha özel nitelikteki veriler girmektedir. Bu itibarla 132. ve 133. maddelerin, 136. maddeye göre daha özel nitelikte düzenlemeler olduğu kabul edilmektedir. Bu düzenlemeler arasında bahsettiğimiz şekilde bir birleşme olması halinde ise; TCK'nın 136. maddesinin değil, sadece belli surette kaydedilmiş kişisel verileri konu edinen ve bu surette 136. maddeye göre daha özel nitelikte olan, TCK'nın 132. ve 133. maddelerin uygulanması gerektiği ileri sürülmektedir.⁵⁵³

Bu istikamette, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu ile özel hayatın gizliliğinin ihlali suçunun içtimaina ilişkin doktrininde bazı yazarlarca da benimsenmiş olan, Yargıtay'ın bir içtihadında da; *“bir özel hayat görüntüsü ya da sesinin, “kişisel veri” olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi eyleminin, 5237 sayılı TCK'nın 134/1. maddesinin 2. cümlesinde tanımlanan özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilmesi gerektiği, kişinin özel hayatına ilişkin görüntü, fotoğraf ya da sesin, 5237 sayılı TCK'nın 135. maddesi kapsamında kişisel veri olarak kabul edilemeyeceği, iddiaya konu olayda, mağdurenin çıplak vaziyetteki görüntü ve fotoğraflarının kaydedilmesinden ibaret eylemin, “Kişisel verilerin kaydedilmesi” suçunu oluşturmayacağı, çekimin, mağdurenin bilgisi ve rızası kapsamında gerçekleşmesi nedeniyle, özel hayatın gizliliğini ihlal suçunun da oluşmadığı anlaşıldığından, yapılan yargılama sonucunda, sanığa yüklenen suçun yasal unsurlarının oluşmadığı”* kabul edilmektedir.⁵⁵⁴ Bu karara göre Yargıtay'ın kabulünün; kişilerin özel hayatının gizliliğini ihlal niteliği taşıyan fotoğraf veya sesin

⁵⁵³ AKDAĞ, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s. 117.; “Sanığın babası, ayrı yaşadığı eşi ve kayın validesi ile aralarında geçen konuşmaların TCK'nın 133/2. maddesine göre “söyleşi” niteliğinde olduğu halde, dosya kapsamına uygun olmayan gerekçelerle ve suç vasfında yanılıya düşülerek, müştekiye ait konuşmaların “kişisel veri” olduğu sonucuna varılıp sanığın TCK'nın 135/1. maddesine göre cezalandırılmasına karar verilmesi” Yargıtay 12. CD., E: 2013/14958, K: 2014/3723, T: 17.02.2014 www.kazanci.com (08.02.2018).

⁵⁵⁴ Yargıtay 12. CD., E: 2012/17703, K: 2012/18222, T: 11.09.2012 www.kazanci.com (08.02.2018).

kaydedilmesi eyleminin TCK'nın 134. maddesi kapsamında,⁵⁵⁵ bunun dışında özel hayatın gizliliğinin ihlali niteliği taşımayacak fotoğraf veya sesin kaydedilmesi eylemlerinin TCK'nın 135. maddesi kapsamında cezalandırılması gerektiği istikametinde olduğunu söyleyebiliriz.⁵⁵⁶ Doktrinde kararın her ne kadar gerekçe bakımından yeterince açık olmadığı ve kendi içerisinde çelişki taşıdığı düşünülmekteyse⁵⁵⁷ de, bu kararla benzer istikamette, eylemlerin korunan hukuksal değere olan etkisine göre suç tipinin belirlenmesinin gerektiği kabulünü benimseyen müellifler de mevcuttur.⁵⁵⁸ Buna göre; kişisel verilerin fail tarafından kişilerin özel hayatlarına müdahalede bulunma ya da vakıf olma düşüncesine dayalı olarak mı, yoksa bir “dosyalama sistemi”⁵⁵⁹ kapsamında verileri kaydetmek amacıyla mı kaydedilmiş olduğu değerlendirmesi yapılarak bu suçlardan hangisinin işlenmiş olduğu tespit edilebileceği ileri sürülmektedir.⁵⁶⁰ Bu istikamette başka bir kararda da Yargıtay; “sanığın, resim çekme sistemi çalışır vaziyetteki taşınabilir telefonunu, kimlikleri tespit edilemeyen mağdurelerin, etek altına ve bacak, göğüs gibi erojen bölgelerine odaklayarak, onların bilgi ve rızaları dışında, fotoğraflarını çekmesi şeklinde gelişen eyleminin, 5237 sayılı TCK'nın 134/1. maddesinin 2. cümlesinde düzenlenen özel hayatın gizliliğini ihlal suçunu oluşturacağı”⁵⁶¹ istikametinde değerlendirmede bulunmuştur. Konuya ilişkin kanaatimiz, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu ile özel hayatın gizliliğinin ihlali suçu arasında Kanun'un dokuzuncu

⁵⁵⁵ Ses veya görüntünün veri olarak kaydedilmiş ve ilgilisinin rızası olmaksızın bunlar açıklanmışsa da 134/2. Fıkrasına göre failin cezalandırılması gerekir. SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 352.

⁵⁵⁶ “Katılanın facebook sayfasında yer alan resmin, özel yaşam alanına dair ve özel hayatının gizliliğini ihlal edecek nitelikte olmadığı dikkate alınarak, kişisel veri niteliğindeki resmini, onun isim ve soy ismiyle birlikte, belirli olmayan ve birden fazla kişi tarafından algılanabilme imkanı bulunan facebook adlı sosyal paylaşım sitesinde, hukuka aykırı olarak yayan sanığın sübut bulan eyleminin, TCK'nın 136/1. maddesinde tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçu kapsamında değerlendirilmesi gerekirken, delillerin takdirinde yanılığa düşülerek, oluşa ve dosya kapsamına uygun düşmeyen yazılı gerekçelerle, sanık hakkında beraat kararı verilmesi” Yargıtay 12. CD., E: 2014/1950, K: 2014/26159, T: 22.12.2014 www.kazanci.com (08.02.2018).

⁵⁵⁷ KESER BERBER, KAYA, *Türkiye’de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, s. 56,57,58.; KARABULUT, *Kişisel Verilerin Korunması ve Kolluk Hizmetleri*, s. 65.

⁵⁵⁸ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 649.

⁵⁵⁹ “Veri kayıt sistemi : Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir. Bu sistemler elektronik yahut fiziki ortamda oluşturulabilir. Veri kayıt sisteminde kişisel veriler; ad-soyad veya kimlik numarası üzerinden sınıflandırılabilceği gibi, kredi borcunu ödemeyenlere ilişkin oluşturulacak sınıflandırma da bu kapsamda değerlendirilecektir.” KVK Kurumu Yayınları, 6698 Sayılı Kanun’da Yer Alan Kurumsal Terimler, s. 7., <https://www.kvkk.gov.tr> (02.03.2018).

⁵⁶⁰ OĞUZ, “Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum”, s. 20.

⁵⁶¹ Bu karar bakımından dikkat çekilmesi gereken bir başka husus ise; çekilen fotoğraflardan görüntülerin kime ait olduğunun anlaşılamaması sebebiyle, aslında kimliği belirli veya belirlenebilir bir kişi ile ilişkilendirilebilme unsuru bulunmadığından olayda bir kişisel verinin de bulunmadığıdır. Yargıtay 12 CD., E: 2012/18221, K: 2012/16872, T: 11/09/2012 www.kazanci.com (08.02.2018).

bölümünde düzenlenen özel hayata ve hayatın gizli alanını koruma altına alan diğer suç tipleriyle olduğu gibi özel genel norm ilişkisi bulunduğu istikametindedir. Bu durumda failin, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunu işlemiş olması halinde bu suç ile birlikte genel norm olan 134. maddeden ayrıca cezalandırılması gerekmeyecektir.⁵⁶² Ancak, aynı bölüm altında düzenlenmiş olan TCK'nın 132. ve 133. maddeleri ile kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun düzenlendiği 135. maddesi arasında somut bir özel genel norm ilişkisi bulunduğu söylenemez. Bu durumda kişisel veri niteliğinde bilgi taşıyan, kişiler arasındaki konuşma veya haberleşmenin kaydedilmesi halinde failin tek bir fiille birden fazla suç işlemiş olacak ve TCK'nın 44. maddesi ile düzenlemiş olan fikri içtima kuralları istikametinde en ağır cezayı gerektiren suçtan cezalandırılması gerekecektir.

Bilişim alanında veya bilişim sistemlerine karşı işlenen suçlar ve kişisel verilere karşı işlenen suçlar arasındaki ilişki de içtima bahsinde üzerinde durulması gereken önemli bir husustur. Bu konuda doktrinde bir kısım müellif kişisel verilerin kaydedilmesi suçunu işleyen kişinin, “bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden” kişiden başka kimse olamayacağı kanaatiyle iki suç arasında geçit suç ilişkisi olduğu benimsemektedir. Kişisel verilerin kaydedilmesi suçunun uygulamada daha ziyade bilişim sistemlerine girerek ve bir süre sistemde kalınarak işlenmekte olduğu, dolayısıyla TCK'nın bilişim sistemine hukuka aykırı olarak girmeyi suç olarak düzenlediği 243. maddesinin 135. madde bakımından geçit suç olduğu kabul edilmektedir.⁵⁶³ Ancak bu kanaatin özellikle 135. maddenin gerekçesindeki kaydetmenin otomatik veya otomatik olmayan şekilde olabileceği istikametindeki açıklama, nazara alındığında kabul edilebilirliği bulunamamaktadır. Yine TCK'nın 244. maddesi ile “*bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi*” cezalandırılmaktadır. Bu maddenin suç olarak düzenlediği “*sisteme veri yerleştirme*” fiili ile kişisel verilerin kaydedilmesi fiilinin aynı anda gerçekleştirilebilmesi veya aynı

⁵⁶² KOCA, ÜZÜLMEZ, *Türk Ceza Hukuku Özel Hükümler*, s. 508.

⁵⁶³ SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 352.; BÜK, Alaattin, *Elektronik Ortamda Saklanan Kişisel Verilerin Elde Edilmesi / Değiştirilmesi Suretiyle İşlenen Suçların Ceza Hukuku Açısından Değerlendirilmesi*, (Yayınlanmamış Doktora Tezi), T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara, 2015, s. 227.

anlama gelebilmesi mümkün olabilmektedir. Böyle bir durumda iki suç tipi arasında fikri içtima hükümleri uygulanarak en ağır cezayı gerektiren TCK'nın 135. maddesine göre failin cezalandırılması gerektiği istikametindeki benimsemiş olduğumuz kanaate⁵⁶⁴ karşılık olarak; doktrinde bu iki suç tipi arasındaki özel genel norm ilişkisi bulunduğu ve TCK'nın 244. maddesinin eylem unsurunun yalnızca bilişim sistemine yapılan kaydı kapsadığı dolayısıyla TCK'nın 136. maddesine göre daha özel bir düzenleme olduğu gerekçesiyle failin yalnızca bu maddeye göre cezalandırılması gerektiği kanaati de kabul edilmektedir.⁵⁶⁵

Bunun dışında kişisel verilerin hukuka aykırı olarak kaydedilmesi eyleminin aynı zamanda kişilerin şeref ve haysiyetinin zedelenmesine sebep olması halinde de failin hem TCK'nın 125. maddesinde düzenlenmiş olan hakaret suçunu hem de kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunu işlemiş olacağı şüphesizdir. Bu durumda da iki suç arasında fikri içtima hükümleri uygulanması gerekecektir.⁵⁶⁶ Bu istikamette Yargıtay Ceza Genel Kurulu'nun önüne gelen uyuşmazlığa göre; *“Sanığın genel yayın yönetmenliğini yaptığı gazetede köşe yazarı olarak çalışan katılanın yazdığı köşesinde kullanılan fotoğrafın, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle sanık tarafından internetteki özel bir arkadaşlık sitesine kimlik, adres ve telefon bilgileri verilmeksizin ve erkek arkadaşı aradığı açıklamasıyla konulması eylemi, TCK'nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçunu oluşturmaktadır. Bununla birlikte sanığın eylemi, aynı zamanda katılanın onur, şeref ve saygınlığını rencide edebilecek nitelikte olması nedeniyle TCK'nın 125. maddesinin birinci ve dördüncü fıkrası uyarınca alenen hakaret suçunu da oluşturmaktadır. Bu nedenle hukuki anlamda tek fiil sayılması gereken eylem ile hem TCK'nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçu, hem de aynı kanunun 125/1-4 maddesinde düzenlenen alenen hakaret suçu olduğundan, sanık hakkında farklı nev'iden fikri içtima hükümlerinin uygulanması ve oluşan suçlardan en ağır cezayı gerektiren kişisel verileri hukuka aykırı olarak yayma suçundan sanığa ceza tayin edilmesi gerekmektedir.”*⁵⁶⁷ şeklinde karar vermiş olduğunu görüyoruz. Bunun yanı sıra mağdurun köşe yazarlığı yaptığı gazetede yer alan fotoğrafının,

⁵⁶⁴ GÜLTEKİN, *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*, s. 155.

⁵⁶⁵ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 647.

⁵⁶⁶ GÜLTAŞ, Veysel, *Özel Hayata Karşı Suçlar*, 2. Baskı, Ankara, Bilge Yayınevi, 2017, s. 217.

⁵⁶⁷ Yargıtay CGK., E: 2012/12-1510, K: 2014/331, T: 17.6.2014 www.kazanci.com (04.01.2018).

kararda da altı çizildiği üzere, mağdurun varsayımsal rızası gibi hukuka uygun kabul edilebilecek hiçbir sebep olmaksızın bir internet sitesinde yayınlanması eylemi aynı zamanda TCK'nın 135. maddesinde düzenlenmiş olan kişisel verilerin hukuka aykırı olarak kaydedilmesi suçuna da vücut vermektedir. Bu durumda failin özel bir arkadaşlık sitesine mağdurun fotoğrafını, erkek arkadaş aradığı açıklamasıyla yayınlaması şeklindeki eylemi, hem hakaret suçunu (TCK125) hem de kişisel verileri hukuka aykırı olarak kaydetme (TCK 135) ve yayma suçlarını (TCK 136) oluşturmakta olduğunu söylemek gerekmektedir. Failin kararda belirtilen şekildeki tek hareketi ile birbirinden farklı üç suç oluşmaktadır. Bu durumda da kararda işaret edildiği üzere failin bu suçlardan en ağır cezayı gerektiren suç olan TCK'nın 136. maddesine göre cezalandırılması gerekecektir. Kanaatimizce Yargıtay Ceza Genel Kurulu'nun bu kararının, kişisel verilerin hukuka aykırı olarak kaydedilmesi ve haberleşme veya kişiler arasındaki konuşmaların kaydedilmesi suçlarının içtimai noktasında da kıyasen uygulanabilirliği söz konusu olabilecektir. Bu durumda TCK'nın 132 ve 133. maddeleri ile 135. maddesi arasında bir özel genel norm ilişkisi aranmaksızın, doğrudan failin tek hareketi ile birden fazla farklı suçun meydana geldiği kabul edilerek suçların içtimai, Yargıtay'ın ilgili kararı nazara alındığında, daha yerinde olacaktır.

f. Nitelikli Haller

Suçun temel düzenleniş şeklinde ilaveten aranan ve suçun daha ağır veya daha hafif bir sonuç yaratmasına sebep olarak, suçun temel şekli için öngörülen cezanın artırılarak veya azaltılarak verilmesinin gerektiği haller suçun nitelikli halleridir.⁵⁶⁸ TCK'nın 135. maddesinin ikinci fıkrasında; kişisel verilerin kaydedilmesi suçunun konusunun, hassas nitelikte kişisel veri olması halinde suçun temel şekline göre verilecek olan cezanın yarı oranında artırılacağı düzenlenmiştir. Bunun dışında kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun, failin şahsından kaynaklanan bir nitelikli hali olarak; TCK'nın 137. maddesinde suçun, “kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle” veya “belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle” işlenmesi hali düzenlenmiştir. 137.

⁵⁶⁸ ARTUK, GÖKCEN, YENİDÜNYA, *Türk Ceza Hukuku Genel Hükümler*, s. 286.

maddede sayılan bu hallerden en az birinin gerçekleşmiş olması durumunda, faile verilecek cezanın yarı oranında artırılmasını gerektirmektedir.

i. Suçun Konusunun Özel Nitelikli Veri Olması

TCK'nın 135. maddesinin ikinci fıkrasında sayılan hassas veri veya özel nitelikli verilerin, hukuka aykırı olarak kaydedilmesi halinde kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun temel şekline ilişkin verilecek cezanın yarı oranda artırılması gerekmektedir. TCK'nın 135. maddesinde sayılan özel nitelikli veriler ise; kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin kişisel verilerdir. Özel nitelikli veri, 6698 sayılı Kanun'un 6. maddesinde; *"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."* şeklinde tanımlanmıştır.⁵⁶⁹ Özel nitelikli verilerin hukuka aykırı olarak işlenmesinin, diğer verilerin hukuka aykırı olarak işlenmesine göre daha ağır sonuçlar yaratmaya elverişli olması, hem 6698 sayılı Kişisel Verilerin Korunması Kanun'u hem de 5237 sayılı TCK'nın bu verilerin işlenme koşullarının ve hukuka aykırı olarak kaydedilmesi karşısında uygulanacak olan yaptırımının özel olarak düzenleme altına alınmasını gerektirmiştir. Bu doğrultuda, TCK'nın 135. maddesinin 2. fıkrasındaki düzenlemesi ile özel nitelikli verilerin hukuka aykırı olarak kaydedilmesi fiilinden ötürü failin daha ağır cezalandırılmasını öngörmüş olması, kişileri bu verileri hukuka aykırı olarak işlenmekten daha fazla caydırma ve bu verileri özellikli olarak koruma amacını sağlamaya yönelik bir güvencedir. 5237 sayılı TCK'nın 135. maddesi ile özel nitelikli veri kategorisine dahil tutulan veriler sınırlı olarak sayma yoluyla belirlenmiştir. Dolayısıyla bu veri grubuna dahil olan bilgilerin herhangi bir şekilde genişletilebilmesi mümkün değildir. Özel nitelikli verilerin sınırlı olarak sayma suretiyle belirlenmesi usulü uluslararası düzenlemelerde de genellikle benimsenmiş olan bir yöntem olmakla beraber, katıldığımız kanaate hassas verilerin

⁵⁶⁹ "Bu kavram, İsviçre Verilerin Korunması Hakkında Federal Kanunu'nun 3. maddesinin c bendinde açıklanmıştır. Bu hükme göre, özellikle korunmaya muhtaç kişisel veri'den anlaşılması gereken husus, dinsel, dünya görüşü, politik veya sendikal bakış açıları veya faaliyetler, sağlık, gizli-özel yaşam, ırki menşee, sosyal yardım önlemleri, idari veya ceza hukuku soruşturmaları ve yaptırımlar hakkındaki veriler anlaşılmalıdır." ÜNVER, "Kişisel Verilerin Korunması", s. 184.

bu şekilde sınırlandırılmasının çok da yerinde olmadığı istikametindedir.⁵⁷⁰ Zira bazen bu şekilde sınırlı olarak sayılan hassas veri kategorisi içerisinde kabul edilmeyen basit bir kişisel verinin de kullanılma amaç, içerik veya sonuç itibarıyla ilişkilendirilerek hassas nitelikli bir veri korumasına sahip olması gerekebilecektir. Örneğin; normalde özel nitelikli bir kişisel veri olarak kabul edilmeyen bir fotoğrafın, kişilerin toplum içerisinde ayrımcılığa maruz kalması neticesi yaratabilecek ten rengi gibi fiziksel bir özelliğini göstermekte olması halinde ve kullanılma amacı veya şekline göre özel olarak korunması gereken veri kategorisi içerisine dahil edilmesi gerekebilir. Bu durumda bu veriyi işleyen failin de daha ağır cezalandırması gerekecektir.

Günlük hayatta kişisel veriler en fazla sağlık hizmetlerinden yararlanan sırada işlenmektedir ve bu hizmetlerden faydalanmak için yetkililerle paylaşılan kişisel veriler genellikle kişilerin sağlık durumlarına ilişkin özel nitelikli verilerdir. Kişisel sağlık verileri bu itibarla; kimliği belirli veya belirlenebilir bir hastayla ilişkilendirilebilen ve bu kişilerin sağlık durumuyla ilgili her türlü kişisel veri olarak tanımlanabilir. Buna göre hastanın, bir sağlık kurumuna başvurduğu andan tedavisi ve hatta tedavi sonrası kontrolleri tamamlanıncaya kadar geçen süreç içerisinde yetkili kişilerle paylaştığı bilgi, kan, doku, film, reçete gibi verilerinin tamamı hastaya ait özel nitelikli veridir.⁵⁷¹

i. Suçun Kamu Görevlisi Tarafından ve Görevinin Sağladığı Kolaylıkla İşlenmesi

Kanun'un dokuzuncu bölümünde yer verilen özel hayata ve hayatın gizli alanına karşı suçlara ilişkin ortak bir nitelikli hal olarak TCK'nın 137. maddesinin 1. fıkrasında; bu suçların kamu görevlisi tarafından ve görevinin verdiği yetkiyi kötüye kullanarak gerçekleştirilmiş olması düzenlenmiştir. Maddenin düzenleniş şeklinde "ve" bağlacına yer verilmiş olması dolayısıyla, bu nitelikli halin söz konusu olabilmesi

⁵⁷⁰ Ayrıntılı değerlendirme için bkz. s. 11.

⁵⁷¹ "Hastanın öyküsü, fiziki ve psikolojik durumuna ilişkin kayıtlı bilgiler, teşhis, tedavisine ilişkin tüm gözlemler, muayene, tahlil ve tetkik sonuçları ve bu bilgileri içeren hasta dosyası kişisel veri kapsamındadır. Vak'aların ilk durumları ile hastalıkların seyir ve sonucunu tespit için çekilen film, fotoğraf ve slaytlardan kim olduğu anlaşılıyorsa bu tür kayıtlar, hasta giriş kaydı, hastalara içerden ve damardan verilen, kullanılan ve uygulanan bütün ilaçlar ve tedbirlerle, gündelik iâşe maddelerinin yazıldığı hasta tabelası, tabelada yazılı ilaç, tedavi gibi tedbirleri hastalara uygulayan hemşirelerin uygulama sonuçlarını yazdıkları hemşire defterlerinin kişisel veri olarak kabulü gerekir." SEVÜK, "Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması", s. 797.

için kamu görevlisi olma ve görevinin verdiği yetkiyi kötüye kullanma koşullarının birlikte gerçekleşmiş olması gerekmektedir.

Kamu görevlisi TCK'nın 6. maddesinde; *“kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi”* olarak tanımlanmıştır. Kişisel verilerin kaydedilmesinde daha ziyade kamusal makamlarla muhatap olduğumuz düşünüldüğünde, görevinin verdiği yetkiyi kötüye kullanarak veya yetkisini aşarak vatandaşlara ait kişisel verileri kaydeden kamu görevlilerinin, TCK'nın 135. maddesinde düzenlenmiş olan kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun bu nitelikli halinden sorumlu tutulması sıklıkla gündeme gelmektedir. Örneğin; bir müdafî avukatının, dosyada delil olarak sunulmak üzere kendisine teslim olunan müvekkile ait özel yaşam alanına ilişkin bir fotoğrafı, bir internet sitesine koyması halinde avukatın⁵⁷² kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun nitelikli halinden sorumlu tutulması gerekecektir.⁵⁷³ Kamu görevlisi kavramı ceza hukuku bakımından diğer hukuk dallarına göre daha geniş yorumlanmaktadır ve az veya çok kamusal görev yürüttüğü, kamu adına hizmet gördüğü kabul edilen her kişi kamu görevlisi olarak kabul edilmektedir.⁵⁷⁴ Kamu görevinin kötüye kullanıldığının tespiti ise; kişilerin yürütmekle görevli olduğu kamu hizmeti ile gerçekleştirilen hukuka aykırı eylemin ilişkisine göre yapılacaktır. Buna göre; fiil kamu görevlisinin görev alanıyla bağlantılı değilse bu nitelikli halin kapsamına girdiği söylenemeyecektir.⁵⁷⁵ *“Kendisi ve eşi de memur olan sanığın, yapacakları şikayete konu olmak üzere eşi ile aynı işyerinde ebe olarak çalışan katılanın doğum belgesini hastaneden alarak, il sağlık müdürlüğüne verdikleri şikayet dilekçesinin ekinde sunmaları şeklinde gerçekleşen somut olayda, katılana ait doğum belgesinin kişisel veri olması, memur olarak çalışan sanığın başkasına ait bilgileri içeren bir belgeyi velevki yapacağı şikayet başvurusuna konu olsa dahi almasının hukuka aykırı olacağını bilebilecek durumda bulunması, suça konu doğum belgesini şikayet dilekçesine eklemek suretiyle burada yer alan ve kişisel veri niteliğinde bulunan bilgilerin katılanın rızası dışında başkalarınca öğrenilmesine neden*

⁵⁷² Avukatlık, noterlik, bilirkişilik veya tanıklık gibi kamusal görevleri yerine getiren kişilerin de kamu görevlisi olduğuna ilişkin olarak bkz. ŞENER, “Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu s. 81.

⁵⁷³ ZAFER, Hamide, *Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması*, İstanbul, Beta Basım, 2010, s. 215.

⁵⁷⁴ CENTEL, Nur, ZAFER, Hamide, ÇAKMUT, Özlem, *Kişilere Karşı İşlenen Suçlar*, 3. Baskı, İstanbul, Beta Basım, 2016, s. 253.

⁵⁷⁵ ŞENER, “Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu s. 81.

*olunması” şeklindeki olayda failin kamu görevlisi olması ve bu görevini kötüye kullanması neticesinde mağdura ait kişisel verileri ele geçirmiş olduğunu söylememiz gerekecektir.*⁵⁷⁶ Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun bu nitelikli halinin gerçekleştirilme şekline ilişkin diğer bir örnek olayda Yargıtay; *“katılanın görevli olduğu okulda hizmetli olarak çalışan sanığın bayan öğretmenlerin kullandığı tuvalete görevinin sağladığı kolaylıktan yararlanmak suretiyle gizli kamera yerleştirdiği anlaşılmışna rağmen sanık hakkında 5237 sayılı TCK’nın 137/1-b maddesinin tatbik edilmemesi kanuna aykırı”* kabul etmiştir.⁵⁷⁷

ii. Suçun Belli Bir Meslek ve Sanatı İfa Etmenin Sağladığı Kolaylıkla İşlenmesi

TCK’nın 137. maddesinin ikinci fıkrasında; *“belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle”* işlenmesi kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun cezasını artıran nitelikli bir hal olarak düzenlenmiştir. Bu nitelikli halin uygulanabilmesi için failin, icra ettiği mesleği ve sanatı ile gerçekleştirdiği hukuka aykırı kaydetme fiili arasında bir bağ bulunması gerekir.⁵⁷⁸ Failin suça konu kişisel verilere meslek ve sanatı gereği ulaşmış ise bu bağın kurulabilirmiş olduğu söylenebilir.⁵⁷⁹ Örneğin; serbest muhasebecilik yapan bir kişinin, mükellefleri hakkında mesleği icabı bilgi sahibi olduğu belli konuları şahsi bilgisayarında kayıt altına alması veya depolaması halinde, icra edilen muhasebecilik mesleğinin sağladığı kolaylıkla suçun işlenmiş olduğu kabul edilebilecektir. Bu nitelikli hale ilişkin olarak; suçun işlenişinin ve kişisel verilerin kaydedilmesinin kolaylaşmasının daha ziyade failin bilişim sektöründe faaliyet göstermesinden kaynaklı olabileceği de doktrinde ileri sürülmektedir.⁵⁸⁰ Zira, bilişim sektörüne ilişkin bir meslek ve sanat icra etmenin, hem kişisel verileri elde etmeyi hem de kaydetmeyi fail bakımından kolaylaştıracağı şüphesizdir.⁵⁸¹ Bu durumda failin bu kolaylık nispetinde daha fazla cezalandırılması gerekecektir.

⁵⁷⁶ Yargıtay CGK., E: 2012/12-1514, K: 2014/312, T: 10.6.2014 www.kazanci.com (08.02.2018).

⁵⁷⁷ Yargıtay 12. CD., E: 2011/ 12221, K: 2012/12232, T: 16.05.2012 www.kazanci.com (08.02.2018).

⁵⁷⁸ ZAFER, Hamide, *Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması*, s. 216.

⁵⁷⁹ ŞENER, “Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu s. 82.

⁵⁸⁰ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 626.

⁵⁸¹ “elektronik mühendisi olan sanığın, teknik servis elemanı olarak çalıştığı sırada, T Tıp Merkezi’nde oluşturduğu Coteks adlı bilgi sistemine girerek, psikiyatri anabilim dalında tedavi gören mağdura

g. Yaptırım

TCK'nın dokuzuncu bölümünde düzenlenen özel hayata ve hayatın gizli alanına ilişkin diğer suç tiplerinden farklı olarak, kanun koyucu kişisel verilere karşı işlenen suçların soruşturulması ve kovuşturulması, mağdurun şikayetine bağlı tutulmamıştır. Dolayısıyla, kişisel verilerin hukuka aykırı olarak kaydedilmesi, verilmesi, yayılması, ele geçirilmesi veya yok edilmemesi suçlarından birinin işlendiğinin öğrenilmesiyle kamusal makamlarca, re'sen suçun soruşturulmasına başlanması gerekir. Suçun temel şekli için öngörülen 1 yıldan 3 yıla kadar hapis cezasının, suçun konusu (TCK md.135/2.) veya failin şahsına bağlı olan (TCK md.137) nitelikli hallerinden birinin gerçekleşmesi hallerinde yarı oranında artırılarak takdir olunması gerekir. Hukuka aykırı olarak verilerin kaydedilmesi suçu, bu suça ilişkin 8 yıllık dava zamanaşımı süresi içerisinde ve görevli olan mahkeme asliye ceza mahkemelerince kovuşturulur. Bunun dışında TCK'nın 140. maddesi ile kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun işlenmesi dolayısıyla tüzel kişiler hakkında güvenlik tedbirine hükmedilebileceği düzenlenme altına alınmıştır.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nu da, kişisel verilere karşı işlenen suçlara ilişkin yaptırımları, TCK'nın ilgili maddelerine atıf yaparak düzenlemiştir. 6698 sayılı Kanun'un 18. maddesi ile de kabahatler ve bu kabahatler için öngörülen yaptırımlar düzenlenmiştir. Kanun, kabahatlere ilişkin yaptırım olarak, mukayeseli hukukta da benimsendiği üzere, daha ziyade para cezası yaptırımını öngörmüştür. Türk Ceza Kanunu'muzda da kişisel verilere karşı işlenen suçlar karşısında, özgürlüğü bağlayıcı cezalara alternatif olarak veya münhasıran, adli para cezası yaptırımına da yer vermesi gerektiği kanaatindeyiz. Böyle bir düzenleme aynı zamanda mukayeseli hukukla da uyumlu bir ceza yaptırımının öngörülmüş olmasını sağlayacaktır. Ayrıca günümüzde parayla satın alınabilen bir varlık haline gelmiş olan kişisel verilerin, bir menfaat sağlamak düşüncesiyle veya başkasına zarar vermek amacıyla kaydedilmiş olması hallerinde, faile daha ağır ceza verilmesini sağlayacak düzenlemelere ceza mevzuatımızda yer verilmesi gerekmektedir.⁵⁸²

hemşirenin bilgilerini okuyup, hastane çalışanlarına ifşa ettiği” Yargıtay 12. CD., E: 2012/13104, K: 2012/14146, T: 05.06.2012 www.kazanci.com (08.02.2018).

⁵⁸² Federal Alman Veri Koruma Mevzuatı'nın 44. maddesi ile de; 43. maddede sayılan idari yaptırımlardan birini gerektirecek bir ihlalin; para karşılığında ya da kendisi veya başkasının yararına olarak ya da başkasının zararına olarak gerçekleştirmesi halinde faile 2 yıla kadar hapis veya adli para cezası verilebileceği düzenlenmiştir. Bundesdatenschutzgesetz (BDSG) ss. 44.

3. Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu

a. Genel Olarak

5237 sayılı Türk Ceza Kanunu'nun 136. maddesi, "*kişisel verileri hukuka aykırı olarak verme veya ele geçirme*" madde başlığı altında; kişisel verilerin, her ne surette olursa olsun, hukuka aykırı olarak ele geçirilmesini, başkalarına verilmesini veya yayılmasını, kişisel verilerin hukuka aykırı olarak kaydedilmesinden bağımsız bir suç olarak düzenlemiştir.⁵⁸³ Madde gerekçesinde de özel olarak açıklandığı üzere bu suçun konusunu oluşturan kişisel verilerin, hukuka uygun veya hukuka aykırı olarak kaydedilmiş olması suçun oluşumu bakımından önem arz etmeyecektir. Dolayısıyla, kişilerin kendi rızası dahilinde veya hukuka aykırı herhangi bir şekilde ve internet gibi açık erişim vasıtalarıyla kişilerin bilgisine açık bulunan ad soyad, kimlik numarası vb. kişisel bilgilerinin, hukuka aykırı olarak ele geçirilmesi veya üçüncü kişilere verilmesi, aynı zamanda bilişim alanında kimlik hırsızlığı suçuna da vücut veren⁵⁸⁴ bir suç olarak 136. madde kapsamında cezalandırılmaktadır. Ülkemizde kişisel verilerin hukuka aykırı olarak yayılması suçuna ilişkin önemli bir olayın oluşu şöyledir; Yüksek Seçim Kurulu, 2009 yılında gerçekleştirilen yerel seçimlerde oy kullanacak vatandaşların, hukuka uygun şekilde kaydedilmiş olduğunu kabul ettiğimiz ad, soyad, kimlik numarası, ikametgah vb. bilgilerini seçmen listeleriyle askıya çıkarmıştır ve bu bilgiler, bir internet sitesi üzerinden kişilerin satın alabileceği bir program aracılığıyla, hukuka aykırı olarak üçüncü kişilerin erişimine açık hale getirilmiş, diğer bir deyişle pazarlanmıştır.⁵⁸⁵ Günümüzde de, kişisel verilerin, ekonomik olarak karşılık gören bir değer haline gelerek özel sektör için de öneminin giderek artmakta olması somut olay benzeri vakıaların çok daha yaşanacağı istikametinde endişelere sebep olmaktadır. Bu itibarla, ülkemizde vatandaşların kişisel verilerinin güvende olduğuna olan inancı her geçen gün biraz daha azalmaktadır. Kişilerdeki bu güvensizliği yıkabilmek ancak kanunlarımızın kişisel verilerin

⁵⁸³ "Kişisel veri güvenliğini ihlal etmeye yönelik saldırıların yanısıra, kişisel verilerin hukuka aykırı olarak açıklanması ya da paylaşılması gibi konular başlıca kişisel veri güvenliği ihlallerindendir. Bu ihlaller, kullanıcıların dikkatsizlik, dalgınlık veya tecrübesizlik gibi zayıf yönlerinin kullanılması suretiyle kötü amaçlı yazılım içeren elektronik posta ekinin açılması veya elektronik postanın yanlış alıcıya gönderilerek kişisel verilerin üçüncü kişilerin erişimine açılması şeklinde de ortaya çıkabilmektedir." KVK Kurumu Yayınları, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), s. 9.

⁵⁸⁴ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 649.

⁵⁸⁵ KARLIDAĞ, "Ekonomi Politik Açıdan Kişisel Verilerin Korunması", s. 145., 146.

güvenliğini sağlamaya yönelik hükümlerinin doğru tatbik edilmesi, bu yükümlülüklere aykırı davrananların kesintisiz takibi ve caydırıcı yaptırımların uygulanması gibi tedbirler sayesinde sağlanabilecektir.⁵⁸⁶

Kişisel verilerin korunması hakkının tarihteki ilk görünüm şekli olarak kabul edilen hekimlerin sır saklama yükümlülüğü kapsamında da aslında; kişisel verilerin hukuka aykırı olarak üçüncü kişilere anlatılması, paylaşılması veya yayılması koruma altına alınmaya çalışılmıştır. Dolayısıyla Hipokrat'tan günümüze kadar sır saklama yükümlülüğü altında bulunan hekimler, bu yükümlülüklerine aykırı davranışları halinde aynı zamanda, TCK'nın 136. maddesini de ihlal etmiş olacaklardır.⁵⁸⁷ 6698 sayılı Kanunu'nun; verilerin işlenmesine ilişkin temel ilkeleri,⁵⁸⁸ veri öznesinin haklarına ve veri sorumlularının yükümlülüklerine yer veren maddeleri ile kişisel verilerin önleyici olarak korunması sağlanmaya çalışılmaktadır. Bu düzenlemeler arasında özellikle, veri sorumlularının veri güvenliği ilkesine aykırı davranması ve yükümlülüklerini yerine getirmemesi, TCK'nın 136. maddesi kapsamında da bu kişilerin sorumlu tutulmalarını gerektirecektir. Zira veri güvenliği ilkesi kapsamında veri sorumlularının; *“kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak”* yükümlülükleri bulunmaktadır.⁵⁸⁹ Bunun dışında veri işleyenler ve sorumluları, *“veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar”* şeklindeki 12. maddenin 4. fıkrasındaki düzenlemeyle aynı zamanda sır saklama yükümlülüğü altında bırakılmışlardır. Bu yükümlülükler aykırı davranılması da 6698 sayılı Kanun'da kabahat olarak düzenlemiştir. Bu durumda veri sorumlularının veya veri işleyenlerin, suç işleme kastıyla da hareket etmiş olmaları halinde sır saklama yükümlülüklerine

⁵⁸⁶ 6698 sayılı Kanun'un 19. maddesi ile kurulmuş olan Kişisel Verileri Koruma Kurumu'nun 2017/61 karar numaralı ve 21.12.2017 tarihli “Rehberlik Hizmeti Veren İnternet Sitelerinde/Uygulamalarda Kişisel Verilerin Korunması” kararının uygulamaya yansıyan bu konuda verilmiş önemli bir karar olduğunu düşünmekteyiz.

⁵⁸⁷ SEVÜK, “Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması”, s. 811.

⁵⁸⁸ “136. maddede düzenlenen suçun seçimlik hareketlerini oluşturan, kişisel verinin ele geçirilmesi, verinin başkasına verilmesi ve yayılması, dürüst ve hukuka uygun toplama ve işleme ayrıca amaçla bağlılık ilkesinin bir görünümü olarak karşımıza çıkmaktadır.” BÜK, *Elektronik Ortamda Saklanan Kişisel Verilerin Elde Edilmesi / Değiştirilmesi Suretiyle İşlenen Suçların Ceza Hukuku Açısından Değerlendirilmesi*, s. 85.

⁵⁸⁹ 6698 sayılı Kişisel Verilerin Korunması Kanunu md. 12.

aykırı olarak kişisel verileri üçüncü kişilerle verme veya yayma eylemleri, hem TCK 136'da öngörülen verileri hukuka aykırı olarak verme veya yayma suçunu hem de 6698 sayılı Kanun'un 18. maddesine göre veri güvenliği ilkesinin ihlali kabahatini oluşturacaktır. 6698 sayılı Kanun ile veri güvenliği ilkesinin ihlali kabahatine karşılık ayrıca idari bir yaptırım öngörülmüş olmasına rağmen, bu kabahatle korunmak istenen hukuki yarar kişilerin kamusal makamlara olan güveni iken TCK'nın 136. maddesi kişilerin özel yaşamlarının gizliliği ve kişisel verilerin korunması hukuki yararını korumakta olan bir suç tipidir. Bu durumda şahsi kanaatimiz failin, hem TCK'nın 136. maddesinde düzenlenmiş olan suçtan hem de 6698 sayılı Kanun'un 18. maddesinde düzenlenmiş olan kabahatten dolayı ayrı ayrı cezalandırılması gerektiği şeklindedir.⁵⁹⁰ Bu konuda, Kişisel Verileri Koruma Kurumu'nun yorumu da failin, sadece suç oluşturan fiilden dolayı sorumlu tutulması gerektiği istikametindedir.⁵⁹¹

b. Suçla Korunan Hukuksal Yarar

Yargıtay Ceza Genel Kurulu'nun, kişisel verilere karşı işlenen suçlara ilişkin ayrıntılı değerlendirmede bulunduğu 17.06.2014 tarihli içtihadında da işaret ettiği üzere bu suçla korunan hukuksal yarar; *"TCK'nın 136. maddesinde tıpkı 135. maddesinde olduğu gibi korunan hukuki değer genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özelde ise kişisel veriler."*⁵⁹² olarak kabul edilmektedir.

⁵⁹⁰ "Ceza Hukuku ve İdari Ceza Hukukunun öngördüğü yasak ve yaptırımlar farklı hukuki yarar, konu ve unsurları öngörebilir. Bu sebeple, bir eylemde her ikisinde düzenlenen yasakların ihlal edildiği durumda, ne bis in idem prensibinin her bir hukuk dalı için geçerli olacağı, fakat birbirleri arasında bağlayıcılık taşımayacağı savunulabilir. Örneğin, trafik kuralını ihlal etmek suretiyle mala veya cana zarar veren ya da trafik güvenliğini ve dolayısıyla topluma karşı suç işleyen failin, hem trafik kuralını ihlal etmesi ve hem de toplum güvenliğini tehlikeye düşürmesi sebebiyle idari ve adli yaptırımların birlikte uygulanması suretiyle birlikte cezalandırılması mümkündür." ŞEN, Ersan, "Ne Bis In Idem Prensibi", <http://t24.com.tr/yazarlar/ersan-sen/ne-bis-in-idem-prensibi>, 7328 (10.06.2018).; Kural failin hem suç hem de kabahat olarak tanımlanmış olan bir fiiline, sadece suçtan dolayı yaptırım uygulanması iken (Kabahatler Kanunu md. 15/3) bu duruma istisna hem suç hem de kabahat oluşturan fiile kabahatten dolayı ayrıca ceza verileceğine ilişkin özel bir düzenlemenin mevcut olması olarak düzenlenmiştir. DEMİRBAŞ, *Ceza Hukuku Genel Hükümler*, s. 205.

⁵⁹¹ "6698 sayılı Kişisel Verilerin Korunması Kanunu'nda özel bir düzenleme yer almamakla birlikte, bir fiilin hem kabahat hem de suç oluşturmaları halinde faile sadece suçtan dolayı yaptırım uygulanması gerekmektedir." KVK Kurumu Yayınları, 6698 sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar, s. 76.

⁵⁹² Yargıtay CGK., E: 2012/12-1510, K: 2014/331, T: 17.06.2014 www.kazanci.com (04.01.2018).

c. Suçun Unsurları

i. Maddi Unsurlar

1. Suçun Konusu

Bu suçun maddi konusunu kişisel veriler oluşturmaktadır. TCK'nın 135. maddesinde düzenlenmiş olan, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunda da aynı hukuki konunun benimsenmiş ve kişisel veri kavramına ilişkin ayrıntılı açıklamaya bu suçun hukuki konusunun ele alındığı başlık altında yer verilmiş olduğundan bu kısımda tekrar suçun hukuki konusuna ilişkin açıklamada bulunmaktan imtina edilmiştir.

2. Fail ve Mağdur

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçunda fail ve mağdur bakımından, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçundan (TCK md.135) farklı olarak özellik arz eden bir durum bulunmamaktadır. Bu suçun faili ve mağduru kural olarak herkes olabilecektir ancak tüzel kişilerin suçun mağduru olabilirliliği söz konusu değildir. Bu konuya ilişkin kanaatimiz hakkında ayrıntıya, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu altında yapılan açıklamalarda yer verilmiştir.

3. Hareket

TCK'nın 136. maddesi “*kişisel verileri hukuka aykırı olarak verme veya ele geçirme*” madde başlığının altında; kişisel verilerin ele geçirilmesini, başkasına verilmesini veya yayılmasını yaptırım altına almaktadır. Öncelikle madde başlığı ve madde metni arasında uyumsuzluk bu suçun düzenleniş şekline ilişkin dikkat çekmekte olan bir husus olmuştur. Tipiklikte kişisel verilerin hukuka aykırı olarak yayılması da yer almakta iken, madde başlığında sadece verilerin verilmesi veya ele geçirilmesinin düzenlenmiş olması, doktrinde bu itibarla maddenin düzenleniş şeklinin eleştirilmesine sebep olmuştur. Bunun yanı sıra, kişisel verilerin yetkisiz kişilerce ele geçirilmesine karşı kişilerin korunması amacına hizmet eden bu madde hükmüne göre

verilerin; hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi cezalandırılmaktadır.⁵⁹³ Bu fiillerin icra edilmesi ile suç gerçekleşmiş olmakta ve hareket sonucunda bir zararın doğması veya menfaatin sağlanması gibi bir neticenin ortaya çıkması aranmamaktadır. Dolayısıyla bu suç tipe uygun hareketin gerçekleştirilmiş olmasıyla tamamlanan neticesi harekete bitişik (sırf hareket) soyut bir tehlike suçudur.

Yargıtay 12. Ceza Dairesi'nce verilen bir kararda suçun tipikliği; *“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 başkasına verilmesi, yayılması ya da ele geçirilmesi eyleminin TCK'nın 136/1. maddesinde düzenlenen “Verileri hukuka aykırı olarak verme veya ele geçirme” suçu kapsamında değerlendirilecektir.”*⁵⁹⁴ şeklinde açıklanmıştır. Dahası, hukuka uygun veya aykırı olarak kaydedilmiş olabilecek kişisel verilerin, hukuka aykırı olarak ele geçirilmesi, verilmesi veya yayılması seçimlik hareketlerinden birinin gerçekleşmesi bu suçun oluşması ve tamamlanması için yeterlidir. Suç tipinde seçimlik olarak öngörülmüş hareketlerin birinin değil de birden fazlasının birlikte gerçekleştirilmesi durumunda yine tek suç oluşacak ancak bu durumda cezanın miktarı suçun seçimlik olarak öngörülen tek bir fiile gerçekleştirilmiş şekline verilecek cezaya oranla daha ağır olacak şekilde belirlenecektir. Hukuka uygun veya aykırı olarak verilerin kaydedilmesi çeşitli şekillerde gerçekleşebilir. Örneğin; mobil bankacılık hizmetlerinden faydalanırken güvenlik ve kimlik tespiti amaçlı, müşteri hizmetleri yetkilisiyle annemizin kızlık soyadına varacak derecede gizlilik taşıyan kişisel verilerimizi paylaştığımızda veya sürücü belgesi, pasaport gibi belgelerin alınması

⁵⁹³ “Sanık ...'nin, kendisi ile aynı köyde yaşamasından dolayı tanıdığı ve kendisinden 31 yaş küçük olan 17 yaşındaki mağdur ...'ın facebook hesabından ele geçirdiği resmini, onun bilgisi ve rızası dışında, kendi facebook hesabına profil resmi olarak eklediği olayda, mağdura ait facebook hesabından herkes tarafından erişilip, kolaylıkla elde edilebilen ve mağdurun özel yaşam alanına dair olmayıp, günlük kıyafetleriyle poz vermiş şekilde çektiği kişisel veri niteliğindeki resmini, mağdura ait kimlik, adres, telefon vb. bilgilere yer vermeksizin, aynı sitedeki kendisine ait profilde, hukuka uygunluk nedenlerinin bulunmamasından dolayı hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle başkalarının görgüsüne sunan sanığın eyleminde TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunun yasal unsurlarının oluştuğuna dair yerel mahkemenin kabulünde bir isabetsizlik görülmemiş” Yargıtay 12. CD., E: 2016/9759, K: 2017/10938, T: 26.12.2017 www.kazanci.com (08.02.2018).

⁵⁹⁴ Yargıtay 12. CD., E: 2013/30406, K: 2014/2980, T: 10.02.2014 www.kazanci.com (08.02.2018).

sırasında emniyet görevlilerince parmak izimiz alındığında, bu kişiler kişisel verilerimizi hukuka uygun olarak kaydetmiş olmaktadır.⁵⁹⁵ Verdiğimiz örnek üzerinden devam edersek; banka görevlisinin kendisinin yetkisi olmamasına rağmen müşterilere ait suçun konusu oluşturabilecek bir kişisel veriyi kaydedip, başkasına vermesi halinde, kişisel verilerin hukuka aykırı olarak kaydedilmesi ve verilmesi suçları gerçekleşmiş olacaktır. Bunun dışında kişisel verilerin ele geçirilmesi, yayılması veya başkasına verilmesi fiillerinin otomatik veya otomatik olmayan vasıtalar kullanılarak gerçekleştirilebilmesi de mümkündür.

Bu suça ilişkin uygulamada karşılaşılan en yaygın ihlal şekli, kişisel verilerin hukuka aykırı olarak yayılması şeklinde gerçekleşmektedir.⁵⁹⁶ “Yaymak” kavramı TDK Güncel Türkçe Sözlüğünde; “birçok kimseye duyurmak” olarak tanımlanmaktadır.⁵⁹⁷ Kişisel verilerin hukuka aykırı olarak yayılması ise; otomatik veya otomatik olmayan yöntemler kullanılarak verilerin başka insanlara duyurulması⁵⁹⁸, ifşa edilmesi⁵⁹⁹ veya birden fazla kişinin öğrenebileceği şekilde insanların bilgisine sunulması⁶⁰⁰ olarak tanımlanabilir. Kişisel verilerin yayılması, aslında vermekle aynı manaya gelmekte olup,⁶⁰¹ yaymada verilen kişi sayısı birden fazla olduğu için genellikle bu amaçla bir araç kullanılması gerektiği kanaati de doktrinde ileri sürülmektedir. Kanaatimizce isabetli olmayan bu görüşe göre; verilerin kulaktan kulağa bir araç kullanılmaksızın aktarılması kişisel verilerin verilmesi veya yayılması suçunu oluşturmayacaktır.⁶⁰² Günümüzde kişisel verilerin yayılmasında ve başkalarına verilmesinde kullanılması tercih edilen araçlar, daha çok kişiler arasındaki bilgi aktarımını çok daha hızlı ve kolay kılan; e-posta, CD, SMS veya internet içerik

⁵⁹⁵ İTİŞGEN, “Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu”, s. 187.

⁵⁹⁶ “Bu kapsamda somut olayda, sanığın genel yayın yönetmenliğini yaptığı gazetede köşe yazarı olarak çalışan katılanın yazdığı köşesinde kullanılan fotoğrafın, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle sanık tarafından internetteki özel bir arkadaşlık sitesine kimlik, adres ve telefon bilgileri verilmeksizin ve erkek arkadaşı aradığı açıklamasıyla konulması eylemi, TCK’nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçunu oluşturmaktadır.” Yargıtay CGK, E: 2012/12-1510, K: 2014/331, T: 17.06.2014 www.kazanci.com (04.01.2018).

⁵⁹⁷ TDK Güncel Türkçe Sözlük, <http://www.tdk.gov.tr> (03.03.2018).

⁵⁹⁸ HAFIZOĞULLARI, ÖZEN, *Ceza Hukuku Özel Hükümler*, s. 290.

⁵⁹⁹ İfşa etmek yazılı veya sözlü bir vasıta kullanılarak veya kullanılmaksızın gizli olan bir şeyin ortaya çıkartılmasıdır. KOCA, Mahmut, ÜZÜLMEZ, İlhan, *Türk Ceza Hukuku Özel Hükümler*, 3. Baskı, Ankara, Adalet Yayınevi, 2016, s. 477.

⁶⁰⁰ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 651.

⁶⁰¹ “Örneğin, bir kişiye mail ortamında kişisel verinin aktarımı verme olarak nitelendirilirken; bu kişisel verinin sosyal bir paylaşım sitesine konulması yayma fiilidir.” İTİŞGEN, “Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu”, s. 188.

⁶⁰² ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 584.

sağlayıcıları (Facebook, Twitter, Instagram vb.) gibi bilişim vasıtaları olmaktadır.⁶⁰³ Ancak verilerin başka insanlara duyurulmasını sağlayacak mektup, telgraf, faks gibi eski usul haberleşme araçlarıyla veya bir araç kullanılmaksızın da kişisel verilerin verilmesi veya başkalarına yayılması mümkündür.⁶⁰⁴

Kural olarak kişisel verileri başkalarına yaymak için failin, bu verileri elinde bulunduruyor olması gerekir.⁶⁰⁵ Ancak bu bulundurma hukuka uygun veya hukuka aykırı surete gerçekleştirilmiş olabilir. Failin verileri daha önce nasıl elinde bulundurduğu değil, bundan sonra hukuka aykırı olarak verileri başka insanlara aktarma kastının mevcut olması bu suç bakımından önemli ve yeterlidir. Failin bunun dışında veri sahibi kişiye zarar vermek veya menfaat sağlamak gibi bir kastının bulunması da aranmamaktadır.⁶⁰⁶ Ancak şahsi kanaatimiz, böyle bir kasıtlı veya bir çıkar sağlama amacıyla hareket etmiş olması halinde, faile daha fazla ceza verilmesini sağlayacak 135. ve 136. maddelere ilişkin nitelikli bir halin düzenlenmesi gerektiği istikametindedir. Bunun dışında kişisel verilerin hukuka aykırı yayılması suçunun

⁶⁰³ “İncelenen dosya içeriğine göre; sanığın, bir dönem duygusal boyutta arkadaşlık ilişkisi içerisinde olduğu mağdurenin, adı, soyadı, mezun olduğu okul bilgileri, ikamet ettiği eve ait adres bilgileri ile birlikte, mağdurenin günlük hayatta çekilmiş fotoğrafı ile oturduğu eve ait dış cepheden çekilmiş fotoğrafları, mağdure tarafından arkadaşlıklarına son verilmesine tepki olarak ve mağdurenin bilgisi ve rızası dışında, “facebook” adlı sosyal paylaşım sitesinde yayınladığı olayla ilgili olarak, mağdurenin, aktif kullanımında olan, herkes tarafından bilinmeyen veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, ancak sınırlı bir çevre ile paylaştığı adres bilgilerini, adı, soyadı, kendisine ve oturduğu eve ait fotoğrafı ile birlikte rızası dışında, başkalarının bilgisine sunan sanığın eyleminin TCK'nın 136/1. maddesindeki “Verileri hukuka aykırı olarak verme veya ele geçirme” suçunu oluşturacağı”, Yargıtay 12. CD., E: 2013/30406, K: 2014/2980, T: 10.02.2014.; “Sanık Özgür’ün, ilköğretim çağındaki kız öğrenciler ile iletişim kurmada kolaylık sağlaması için, onların öğretmenleri olan mağdurlar Fatma ve Medine’nin adı, soyadı ve resimlerini kullanarak, sahte facebook hesabı açma eylemlerinin verileri hukuka aykırı olarak verme veya ele geçirme suçunu” Yargıtay 12. CD., E: 2015/2878, K: 2016/4067, T: 15.3.2016.; “Sanığın, eski okul arkadaşı olan mağdurun, ad ve soyadı ve fotoğrafı ile internette facebook sosyal paylaşım sitesinde mağdur adına herkese açık sahte üye profili oluşturarak, profil sayfasında mağdurun telefon numarasını yayımlaması biçimindeki eyleminin, TCK'nın 136/1. maddesine uyan, verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu gözetilmeden” Yargıtay 12. CD., E: 2013/26654, K: 2014/15414, T: 23.6.2014 www.kazanci.com (08.02.2018).

⁶⁰⁴ “Bu açıklamalar ışığında somut olay incelendiğinde, sanık Turgut’un, ayrıldığı kız arkadaşı olan şikayetçinin, kendisinde kayıtlı olan kişisel veri niteliğindeki telefon numarasını, şikayetçinin rızası dışında diğer sanık Onur’a verdiği olayda; şikayetçinin telefon numarasını hukuka aykırı olarak yayan sanık Turgut ile telefon numarasını hukuka aykırı olarak ele geçiren sanık Onur’un eyleminin, TCK'nın 136/1. maddesine uyan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden, ayrı ayrı mahkumiyetleri yerine, “telefon numarası vermek şeklinde gerçekleşen eylemin kişisel verilerin ele geçirilmesi ve yayılması olarak değerlendirilemeyeceği” biçimindeki isabetsiz gerekçeyle beraatlerine karar verilmesi” Yargıtay 12. CD., E: 2014/607, K: 2014/16665, T: 7.7.2014 www.kazanci.com (08.02.2018).

⁶⁰⁵ HAFIZOĞULLARI, ÖZEN, “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar”, s. 21.

⁶⁰⁶ YILMAZ, Sabire Sanem, *Tıp Alanında Kişisel Verilerin Hukuka Aykırı Olarak Verilmesinin Ceza Hukuku Açısından Değerlendirilmesi (Sır Saklama Yükümlülüğü Kapsamında)*, (Yayımlanmamış Yüksek Lisans Tezi), Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2014, s. 82.

ihmali veya icrai hareketle işlenebilmesi de mümkündür. Veri sahibinin rızası olmaksızın kişisel verilerinin bir internet sitesinde paylaşılması fiili icrai hareketle kişisel verilerin hukuka aykırı olarak yayılması iken, başta kişinin rızası bulunmakta ve paylaşım bu rızaya dayalı olarak yapılmaktayken rızanın kalkmasına rağmen veriler paylaşılmaya devam edildiği takdirde ihmali hareketle kişisel verilerin hukuka aykırı olarak yayılması suçu işlenmiş olacaktır.⁶⁰⁷ İhmali hareketle kişisel verilerin hukuka aykırı olarak yayılması suçunun olduğu Anayasa Mahkemesi'ne taşınmış olan somut bir olayda da; başvurucunun kendisi hakkında sicil raporlarını içeren evrakın, hazırlandığı makamca “gizli” gizlilik derecesi belirtilerek ancak “kişiyeye özel” kaydı konulmaksızın postaya teslim edilmiş olması sebebiyle ulaştığı kamu kurumundaki bütün aşamalarda, kişiyeye özel kaydı bulunmadığından, evrak açılarak kaydı yapıldığından ulaşması gereken birime kadar pek çok kişi tarafından içeriği öğrenilmiştir. Somut bu olayda kişisel veri niteliği taşıyan kişiyeye ilişkin sicil notlarını içeren evrakın gönderici makamın ihmali olarak kişiyeye özel kaydı koymaksızın göndermek şeklindeki hareketiyle kişisel verilerinin hukuka aykırı olarak yayılması suçunu işlemiş olduğu AYİM Başsavcılığı tarafından görüş olarak ileri sürülmüştür.⁶⁰⁸

Kişisel verilerin ele geçirilmesi; en genel anlamda verilere sahip olmak veya verileri yakalamak şeklinde tanımlanmaktadır.⁶⁰⁹ Yargıtay'da kişisel verilerin ele geçirilmesini; “*kişisel verilerin kayıtlı olduğu belgelerin alınması ya da kayıtlı olduğu bilişim sisteminden ele geçirilmesi*” olarak tanımlamaktadır. Yine Yargıtay'a göre; “*ele geçirme fiili, başkasının hakimiyeti altında bulunan bir kişisel verinin, failin hakimiyeti altına girmesi ile gerçekleşmiş olacak*” kabul edilmektedir. Doktrinde bazı yazarlar ele geçirmenin kaydetme dışında bir yöntemle gerçekleşmiş olması halinde de bu fıkra kapsamına girebileceğini zira kaydetmenin 135. madde ile cezalandırılan bir eylem olduğu kanaatindeyken;⁶¹⁰ böyle bir ayrıma girmeksizin kişisel verilerin cd-

⁶⁰⁷ GÜLTEKİN, *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*, s. 164.

⁶⁰⁸ “Başvurucunun talebine konu sicil notlarının “gizli” gizlilik derecesiyle ancak “kişiyeye özel” tasnifi yapılmaksızın postaya verildiği belirtilmiştir. Görüş yazısında, bu yüzden evrakın ulaştığı her aşamada evrak memurlarınca açılarak kaydının yapılıp numara verilmesi suretiyle ilgili birime ulaştırıldığı tespitine yer verilmiştir. Başsavcılık, başvurucunun “kişiyeye özel” sicil bilgilerinin içinde yer aldığı zarfın sadece başvuru tarafından açılacak şekilde tebligata çıkarılması gerektiği halde bunun yapılmayarak evrakın başkalarına öğrenilmesine yol açıldığını vurgulamıştır. Sonuç olarak başvurucunun mesleki faaliyetlerine ilişkin önemli bilgileri içeren sicil raporlarının başkalarına öğrenilebilmesinin mümkün kılındığı anlaşıldığından somut olayda devletin özel hayata saygı hakkı kapsamında kişisel verilerin korunmasına ilişkin pozitif yükümlülüklerinin yerine getirilmediği anlaşılmaktadır.” Anayasa Mahkemesi, Nurcan Belin Başvurusu.

⁶⁰⁹ HAFIZOĞULLARI, ÖZEN, *Ceza Hukuku Özel Hükümler*, s. 290.

⁶¹⁰ ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 584.

rom ya da hafıza kartına kaydedilerek bilgisayarlardan alınması ile bilgisayarların hafıza kartlarının sökülüp alınmasının da aynı kapsamda olduğu değerlendirilebilmektedir.⁶¹¹ Verilerin ele geçirilmesi bilişim sistemleri üzerinde, “cookies”, “truva atları” ve benzer casus programlarla insanlar farkında olmaksızın dahi gerçekleştirilebilmektedir.

Somut bir olayda da; “*elektronik mühendisi olan sanığın, teknik servis elemanı olarak çalıştığı sırada, T Tıp Merkezi’nde oluşturduğu Coteks adlı bilgi sistemine girerek, psikiyatri anabilim dalında tedavi gören mağdure hemşirenin bilgilerini okuyup, hastane çalışanlarına ifşa ettiği*” görülerek, Yargıtay 12. Ceza Dairesi’nce TCK’nın 136. maddesindeki suçtan cezalandırılması gerektiğine karar vermiştir.⁶¹² Bu olayda fail, mesleğinin sağladığı kolaylıktan yararlanmak suretiyle hem kişisel verilerin hukuka aykırı olarak ele geçirilmesi hem de yayılması suçlarını işlemiştir. Yargıtay’ın önüne gelmiş somut bir başka uyuşmazlıkta da; bir gazete muhabiri, takma isim kullanarak hayatını anlatan bir kitap yazmış olan, mağdurun gerçek kimliğini ortaya çıkarmak için yaptığı araştırma neticesinde mağdurun gerçekte kim olduğunu tespit etmiştir. Daha sonra konuyu çalıştığı gazetede haber yapmış ve bu haberle mağdurun kimliği ve kitapta yer alan kişisel verilerini üçüncü kişilerin bilgisine açık hale getirilmiştir. Yargıtay olaya ilişkin olarak failin, haber verme hakkının sınırlarını aştığına ve kişisel verilerin hukuka aykırı olarak ele geçirilmesi ve yayılması suçlarını işlemiş olduğuna hükmetmiştir.⁶¹³ Somut olayda Yargıtay’ın da kabul etmiş olduğu üzere kişisel verilerin ele geçirilmesi suçunun oluşabilmesi için; verilerin fail tarafından bir sistemden kendi hakimiyet alanına sokulması ile verinin sadece ne

⁶¹¹ “Diğer sanıklarla kart kopyalamak üzere anlaşılıp karşılığında menfaat elde ettiği anlaşılan sanığın eyleminin, çalıştığı restorana 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’nın 136. maddesinde düzenlenen birden fazla kişiye ait kişisel verileri hukuka aykırı olarak ele geçirme suçunu oluşturduğu” Yargıtay 8. CD., E: 2017/15706, K: 2018/866, T: 31.1.2018 www.kazanci.com (08.02.2018).; DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 552.; SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 354.

⁶¹² Yargıtay 12. CD., E: 2012/13104, K: 2012/14146, T: 05.06.2012 www.kazanci.com (08.02.2018).

⁶¹³ “İncelenen dosya kapsamına göre, Gazete muhabiri olan sanığın mağdurla takma isim kullanarak yazmış olduğu kitap hakkında iki kez röportaj yaptığı, daha sonra mağdurun gerçek kimliğini tespit etmek amacıyla araştırma yaparak mağdurun İlköğretim okulunda İngilizce öğretmeni Y.Ç.Y olduğunu tespit ettiği, bu bilgileri Güneş Gazetesi’nin internet sitesinde “Kocasını 300 erkekle nasıl aldattığını kitabında ballandıra ballandıra anlatan kadının izini süren Güneş, insanın kanını donduran bir gerçeğe ulaştı” başlığıyla vererek haber verme sınırlarını aştığı, eyleminin kişisel verileri ele geçirmek ve yaymak suçunu oluşturduğu sabit olduğundan...” Yargıtay 12. CD., E: 2011/15721, K: 2012/11074, T: 26.04.2012 www.kazanci.com (08.02.2018).

olduğunun sisteme girilerek öğrenilmesi arasında bir fark bulunmamaktadır.⁶¹⁴ Dolayısıyla, bu suç kapsamında kişisel verilerin ele geçirilmesinin mutlaka bir araç kullanımını gerektirmez, doğrudan okuma veya izleme gibi yöntemlerle kişisel verilerin içeriğine hakim olmakla da gerçekleştirilebileceğini kabul edebiliriz.

ii. Manevi Unsur

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçunu kasten işlenebilen bir suçtur. Suçun taksirle işlenebilen şekli özel olarak düzenlenmiş olmadığından bu suçun taksirle işlenebilmesi mümkün değildir. Kanun'un lafzına göre bu suçun genel kastla işlenebilen bir suç olduğunu söyleyebiliriz. Ancak doktrinde TCK'nın 135. maddesinde düzenlenmiş olan kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunda olduğu gibi, bu suçun tipikliğinde de "hukuka aykırı olarak" ibaresine özel olarak yer verilmiş olması dolayısıyla suçun sadece doğrudan kastla işlenebilecek olduğu, olası kastla işlenebilmesinin mümkün olmadığı kanaati ileri sürülebilmektedir.⁶¹⁵ Bu kanaate karşılık olarak genel kastla işlenebilen suçların kural olarak olası kastla da işlenebilirliği bulunduğu ve bu suç tipinin de olası kastla işlenebileceği de kabul edilmektedir.⁶¹⁶ Buna göre örneğin; hastanelerde doktorların muayene odalarına, hastaların sırasıyla girmesinin sağlanması ve karışıklık çıkmasının engellenmesi amacıyla dijital ekranlarda hasta isim ve sırasının yayınlanması eylemi kişisel verilerin hukuka aykırı olarak yayılması suçunun olası kastla işlenebilen haline ilişkin bir örnek olarak gösterilmektedir. Zira bu ekranlarda; hastanın ad soyad, hangi doktora muayene olduğu, rahatsızlığının ilgili bulunduğu hastalık branşı gibi bilgilere yer verilmeyle, bu bilgiler hastanede bulunun her türlü kişinin erişimine açık hale getirilmiş olmaktadır. Bu durumda fail, hastalara ilişkin ekranda gösterilen kişisel verileri öğrenilirse öğrenilsin mantığıyla diğer kişilerin erişimine açık hale getirmiş olmakla birlikte, özel olarak bu verilerin yayılmasını isteme iradesi bulunmadığı, yani verileri yaymak için doğrudan bir kastla değil de olası kastla hareket etmiş olduğu

⁶¹⁴ "Bilişim alanındaki suçlarda amaç veriyi ve sistemi korumak ise de, kişisel verilere ilişkin suçlarda verinin korunması amaç değil, kişinin korunmasının aracıdır. Dolayısıyla önemli olan birinin normalde ulaşmaması gereken bir bilgiye ulaşmasının engellenmesidir." AKDAĞ, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s. 125.

⁶¹⁵ GÜLTAŞ, *Özel Hayata Karşı Suçlar*, s. 229.; İTİŞGEN, "Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu", s. 191.

⁶¹⁶ ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 586.

söylenilebilecektir.⁶¹⁷ Kanaatimiz bu durumda failin, hukuka aykırılık bilinci bulunmaksızın hareket etmiş olduğu kabul edilerek kişisel verilerin hukuka aykırı olarak yayılması suçundan dolayı cezalandırılmayacağı istikametindedir. Buna karşılık kişisel verileri, ihmali olarak kabul edilebilecek somut davranış şekline uygun olarak başkalarının erişimine açık kılan kişilerin veri işleyicisi veya veri sorumlusu olarak 6698 sayılı Kanun kapsamında sorumluluğu doğabilecektir.

iii. Hukuka Aykırılık

Kişisel verilerin hukuka aykırı olarak verilmesi, ele geçirilmesi veya yayılması suçunu hukuku uygun kılabilen sebepler; ilgilinin rızası veya kanun hükmünün icrası olabilir. Buna göre veri öznesinin rızasıyla veya kanunun emretmiş olması sebebiyle kişisel verilerin ele geçirilmesi, verilmesi veya yayılması halinde TCK'nın 136. maddesinde düzenlenmiş olan bu suç oluşmayacaktır.⁶¹⁸ İlgilinin rızası ve kanun hükmünün icrası hukuka uygunluk sebepleri, kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu bakımından da failin fiili ve hukuk düzeni arasındaki çatışmayı ortadan kaldıran sebepler olup, bu suç başlığı altında ayrıntılı olarak değerlendirilmiştir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 8. ve 9. maddeleriyle; kişisel verilerin aktarılması ve kişisel verilerin yurt dışına aktarılması koşulları düzenleme altına alınmıştır. Bu maddelere göre, kişisel verilerin aktarılmasında temel koşul ilgilinin açık rızasının bulunmasıdır. Ancak ilgilinin rıza bulunmadığı bazı hallerde de kişisel verilerin yurtiçi veya yurtdışına aktarılması 6698 sayılı Kanun'a göre hukuka uygun kabul edilmektedir. Bu haller aynı zamanda kişisel verilerin ve özel nitelikli kişisel verilerin ilgilinin rızası olmaksızın işlenebileceği haller olarak da düzenlenmiştir.⁶¹⁹ 6698 sayılı Kanun'un özel olarak şartlarını düzenlediği bu hallerde kişisel verilerin verilmesi veya yayılması, TCK'nın 136. maddesinde düzenlenen suç bakımından kanun hükmünün icrası kapsamında hukuka uygunluk sebebi olacak ve

⁶¹⁷ YILMAZ, *Tıp Alanında Kişisel Verilerin Hukuka Aykırı Olarak Verilmesinin Ceza Hukuku Açısından Değerlendirilmesi (Sır Saklama Yükümlülüğü Kapsamında)*, s. 82.

⁶¹⁸ Örneğin; TCK 278., 279. ve 280. maddeleri gereğini yerine getirerek yetkili makamlara suç işlendiğini bildiren kişilerin, bu bildirimlerini yerine getirmesi sırasında şüpheliye ilişkin bazı verileri vermeleri söz konusu olabilecektir. Dolayısıyla Kanun'un bu hükümleri yapılan fiilleri hukuka uygun kılacaktır.

⁶¹⁹ 6698 sayılı Kanun md. 5/2., md. 6/3.

suç oluşturmayacaktır.

Bunun dışında; görevin ifası ve hakkın kullanılması sebeplerinin, karşılıklı olarak gerçekleştirilen kişisel verilerin verilmesi ve ele geçirilmesi fiillerini hukuka uygun kılabilceği hallere de uygulamada rastlayabilmekteyiz. Örneğin; Avukatın soruşturma veya kovuşturmanın her aşamasında dosyayı inceleyebilme, hatta belli koşullarda dosyadan örnek alabilme yetkisi Türk Ceza Muhakemesi Kanunu'nda avukata tanınmış bir yetkidir. Bu yetkisini kullanarak soruşturma dosyasını inceleme talebini savcıya ileten avukata, içerisinde taraflara ilişkin pek çok kişisel veri de bulunan dosyanın verilmesi savcı bakımından görevin ifası, avukat tarafından ele geçirilmesi ise hakkın kullanılması hukuka uygunluk sebeplerinin söz konusu olması sebebiyle bu kişiler bakımından, kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu oluşamayacaktır.⁶²⁰ Bunun dışında Cumhuriyet savcısı, hakim veya mahkemelerin de CMK'nın 332. maddesine göre kişisel veri içeren belge ve bilgi taleplerini; uyuşmazlık konusuyla elverişli bir bağlantı bulunan nitelikte bilgilere ilişkin olarak ve bu belgeleri dosya kapsamında dikkatli şekilde muhafaza ederek ilgisiz kişilerce öğrenilmemesi için gerekli dikkati göstererek gerçekleştirmeleri gerekmektedir. Aksi takdirde kişisel verilerin ele geçirilmesi veya muhakemenin açıklığı sebebiyle üçüncü kişilere yayılmasının, kanun hükmünün icrası hukuka uygunluk sebebine dayanarak gerçekleştirilmiş hukuka uygun bir işleme olduğunu söyleyemeyiz.⁶²¹ Hakkın kullanılması bu suç bakımından basının haber verme hakkı kapsamında da ele alınması gereken bir hukuka uygunluk sebebidir.⁶²² Kişilere ilişkin

⁶²⁰ ÜNVER, "Kişisel Verilerin Korunması", s. 192

⁶²¹ "Mahkeme sağlığa ilişkin verileri yargılamada hangi amaç için istediğini, ne kadar süreliğine istediğini ve hangi bilgiyi istediğini açıkça yazmalı ve dosya ile ilgili olmayan veriler dosya arasına alınmamalıdır. Kişinin sağlık verileri hassas veriler olarak kabul edildiğinden, örneğin hekim ile hasta ilişkisinde hastanın özellikle gizli olarak kalmasını istediği sırları mahkeme ile yargılama için dahi olsa paylaşılmamalıdır. Bu veriler her fırsatta yargılamada doğrudan ve başkaca bir delil bulunduğu durumlarda ilk başvuru delil niteliğinde olmamalıdır." YILMAZ, *Tıp Alanında Kişisel Verilerin Hukuka Aykırı Olarak Verilmesinin Ceza Hukuku Açısından Değerlendirilmesi (Sır Saklama Yükümlülüğü Kapsamında)*, s. 66.

⁶²² "Bakkallar, Bayiler ve Kuruyemişçiler ... üyelerinde bir kısmının oda yönetiminde yolsuzluk yapıldığı iddiasıyla şikâyetçi olmaları üzerine oda başkanı olan katılan hakkında Cumhuriyet Başsavcılığınca başlatılan soruşturmanın kamuoyuna yansımından sonra, katılanın oda bütçesinden karşılanan bir eğitim toplantısı için gidilen otelin hamamında bir bayana kese yaptırırken, yönetim kurulu üyesi sanık ... tarafından rızası dahilinde çekilen fotoğrafının diğer bir yönetim kurulu üyesi sanık ... tarafından, katılanın rızası dışında "konyatanitim.com" isimli internet haber sitesinde köşe yazarlığı yapan sanık ...'a verildiği, sanık ...'ın da, yolsuzluk iddialarını ve oda bütçesinden karşılanan semineri haber yaparken davaya konu fotoğrafı kullandığı, bu haberin fotoğrafla birlikte sanık ...'in sahibi ve genel yayın yönetmeni olduğu internet sitesinde, sonrasında da ulusal basında ve çeşitli internet sitelerinde yayımlandığı olayda; basın özgürlüğünün fotoğrafların yayımlanmasını da kapsamı, fotoğraf ile birlikte ilgili haberin basının haber verme hakkı sınırları içerisinde, güncel, görünür gerçeğe ve ölçülülük ilkesine uygun olması, hakkında

verilerin, basın tarafından haberlere konu edilebilirliği ancak haber verme hakkının hukuki sınırları içerisinde yapılmış bir haber söz konusuysa hukuka uygun kabul edilebilecektir.⁶²³ Bunun yanı sıra basının haber verme hakkı kapsamında hukuka uygun olarak yapmış olduğu bir haberin aradan belli bir zamanın geçmesiyle güncelliğini veya içeriğinin aksini ispatlayan olayların gelişmesiyle doğruluğunu kaybetmesi gibi hallerin gerçekleşmiş olmasına rağmen, haberin yapıldığı gazete, dergi veya internet sitesinin arşivlerinde kişilerin erişimine açık olarak bu haberin bulundurulmaya devam etmesi kişisel verilerin hukuka aykırı olarak yayılması suçunu oluşturacağı şüphesizdir.⁶²⁴

e. Suçun Özel Görünüş Biçimleri

i. Teşebbüs

Kişisel verilere karşı işlenen suç tipleri, TCK'da suç oluşturan kaydetme, ele geçirme, verme veya yayma fiillerinin gerçekleşmiş olmasıyla tamamlanmış olacak şekilde düzenlenmiştir. Kanun'a göre; bu suçun tamamlanması için ayrıca bu fiillerin gerçekleştirilmesi dışında bir neticenin oluşup oluşmadığına bakılmaz. Bu itibarla sırf hareket veya neticesi harekete bitişik bir suç olduğunu kabul ettiğimiz kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçunun, icra hareketlerinin parçalara ayrılabilirdiği halde teşebbüs aşamasında kalabileceği kabul

başkanı olduğu oda ile ilgili yolsuzluk iddiaları bulunan katılanın konumu ve yürüttüğü hizmetin niteliği gereği haberin kamuyu ilgilendirmesi, kamuoyunun haberi öğrenmekte menfaatinin bulunması, haberin veriliş şeklinin haberle uyumlu olması, kullanılan ifadelerin ve yayımlanan fotoğrafın, habere konu olayla düşünsel bağlantısının bulunması karşısında sanığa yüklenen özel hayatın gizliliğini ihlal suçunun yasal unsurlarının oluşmadığının kabulü gerekmektedir." Yargıtay CGK., E: 2015/10, K: 2015/510, T: 15.12.2015 www.kazanci.com (04.01.2018).

⁶²³ "Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre, Gazete muhabiri olan sanığın mağdurla takma isim kullanarak yazmış olduğu kitap hakkında iki kez röportaj yaptığı, daha sonra mağdurun gerçek kimliğini tespit etmek amacıyla araştırma yaparak mağdurun İlköğretim okulunda İngilizce öğretmeni Y.Ç.Y olduğunu tespit ettiği, bu bilgileri Güneş Gazetesi'nin internet sitesinde "Kocasını 300 erkekle nasıl aldattığını kitabında ballandıra ballandıra anlatan kadının izini süren Güneş, insanın kanını donduran bir gerçeğe ulaştı" başlığıyla vererek haber verme sınırlarını aştığı, eyleminin kişisel verileri ele geçirmek ve yaymak suçunu oluşturduğu sabit olduğundan" Yargıtay 12. CD., E: 2011/15721, K: 2012/11074, T: 26.04.2012 www.kazanci.com (08.02.2018).

⁶²⁴ "Başvuranların isimlerinin ad ve soyadı şeklinde açıkça yazılması suretiyle "örgüt, fuhuş ve insan ticareti" gibi kelimelerin yanında anılmaya devam etmesinin, şeref ve haysiyetlerine karşı bir eylem olduğu gibi, bu sebeple gözaltına alındıkları bilgisinin arşivlenmesinin kişisel verilerin izinsiz olarak işlenmesi ve yayınlanması anlamına geleceği" Yargıtay 19. CD., E: 2016/15510, K: 2017/5325, T: 5.6.2017www.kazanci.com (08.02.2018).

edilmektedir.⁶²⁵ Dolayısıyla, öngörülen suç oluşturan verme, yayma veya ele geçirmeye yönelik icrai hareketlerin failin iradesinde olmayan sebeplerle kesintiye uğraması halinde, bu suç teşebbüs aşamasında kalmış olacaktır.⁶²⁶ Örneğin: bilişim yoluyla gönderilen verilerin sistemde bir arıza çıkarak göndericiye ulaşamaması halinde veya bir bilgisayarın sistemine kişisel verileri kendi cihazına aktarmak amacıyla yetkisiz olarak giren kişinin verileri ele geçiremeden sistemden atılması halinde suçun teşebbüs aşamasında kaldığını söyleyebiliriz. Bu aşamada failin yetkisiz olarak bilişim sistemine girmesi ayrı bir suç olarak TCK'nın 243. maddesinde düzenlenmiş olduğundan failin bu suçun tamamlanmış şeklinden mi yoksa TCK'nın 136. maddesine teşebbüsten mi cezalandırılacağı sorusu akla gelebilir. Bu sorunun çözümü ancak, failin kastına bağlı olarak bulunabilecektir. Buna göre; fail, kişisel verileri elde etme kastıyla sisteme girmişse teşebbüs aşamasında kalmış verileri ele geçirme suçundan, böyle bir kastı bulunmaksızın sisteme girmişse tamamlanmış bilişim sistemine hukuka aykırı olarak girme suçundan cezalandırılması gerekecektir.⁶²⁷ Bunun yanı sıra failin sisteme yetkisi dahilinde girerek kişisel verileri hukuka aykırı olarak ele geçirme iradesinin sistemden atılması sebebiyle yarıda kalması halinde de failin teşebbüs aşamasında kalmış kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçundan cezalandırılması gerekecektir.

⁶²⁵ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 654.; “Örneğin yetkisiz bir kişinin açık kalmış bir bilgisayarda hiçbir işlem yapmaksızın hasta ismine bakması ya da tedavi sonucuna bakması, kendi hakimiyetine geçirme söz konusu olmasa dahi ya da hakimiyetine geçirecek iken elektriklerin gitmesi ve kayıt altına alamaması..” YILMAZ, *Tıp Alanında Kişisel Verilerin Hukuka Aykırı Olarak Verilmesinin Ceza Hukuku Açısından Değerlendirilmesi (Sır Saklama Yükümlülüğü Kapsamında)*, s. 84.

⁶²⁶ “Sanıkların, işlem yapmaya gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmek için ATM cihazına yerleştirdikleri düzenek ve hafıza kartında herhangi bir bilgi bulunup bulunmadığı araştırılıp, bilgi bulunması halinde eylemlerinin TCK'nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme, bulunmaması halinde ise kişisel verileri hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturacağı gözetilmeden eksik araştırma ile yazılı şekilde aynı Kanun'un 245/2. ve 35. maddeleri uyarınca hükümler kurulması” Yargıtay 8. CD., E: 2016/12565, K: 2017/12892, T: 20.11.2017 www.kazanci.com.; “Sanıkların, ATM cihazına yerleştirdikleri düzenekle işlem yapmaya gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmeye çalışmaktan ibaret eylemlerinin TCK'nın 136, 35. maddelerde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturduğu gözetilmeden, yazılı şekilde hüküm kurulması” Yargıtay 8. CD., E: 2015/9508, K: 2015/21080, T: 7.9.2015 www.kazanci.com (08.02.2018).; SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 356.

⁶²⁷ AKDAĞ, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, s. 129.

ii. İştirak

Bu suç bakımından iştirak bahsinde üzerinde durulması gereken özel bir hüküm bulunmadığından, TCK'nın 4. bölüm başlığı altında düzenlenen suça iştirake ilişkin genel hükümlerin uygulanması gerekir. Dolayısıyla suçun müşterek faillik şeklinde veya şerikliğin diğer şekillerine uygun olarak işlenebilmesi mümkündür. Bu aşamada kişisel verilerin veri sorumlusu ve veri işleyicisi olan kişiler arasında hiyerarşik bir ilişki bulunması dolayısıyla azmettirme veya dolaylı faillik bakımından önem arz edebileceği durumlarla karşılaşılabilmesi ihtimal dahilindedir.

iii. İçtima

TCK'nın 136. maddesinin tipikliğinde, kişisel verilerin hukuka aykırı olarak başkasına verilmesi, yayılması veya ele geçirilmesi suç olarak düzenlenmiş olan fiillerdir. Suç oluşturan bu fiillerin devamlılık gösterecek şekilde işlenebilmesi mümkündür. Özellikle kişisel verilerin yayılması seçimlik hareketinin mütemadi şekilde gerçekleştirilmesi sıklıkla karşılaşılmakta olan bu suça ilişkin bir işleniş biçimidir. Örneğin; herkesin erişimine açık bir internet sitesinde, kişisel veri niteliğindeki bir bilginin veya bir fotoğrafın, hukuka aykırı olarak paylaşılması halinde bu verinin siteden kaldırılmadığı her gün kesintisiz olarak suç işlenmeye devam edilmektedir.⁶²⁸ Böyle bir durumda suç, kesintinin gerçekleştiği anda gerçekleşmiş olacaktır ve zamanaşımı bu andan itibaren hesaplanmaya başlanacaktır. Suçun mütemadi suç şeklinde işlenmesi mümkün olduğu gibi zincirleme suç şeklinde işlenebilmesi de mümkündür. Tek bir suç işleme düşüncesi kapsamında aynı kişiye ait aynı veya farklı bir kişisel verinin belli zaman aralıklarıyla bir başkasına verilmesi veya yayılması halinde failin, zincirleme suç hükümlerine göre cezalandırılması gerekecektir. Ancak bir veri bankasından kişisel verilerin belli zaman aralıklarıyla ve tek suç işleme kararının icrası kapsamında ele geçirilmesi halinde zincirleme suç hükümlerini uygulayamayız. Çünkü bu durumda verilerin sahibi yani suçun mağduru olan kişiler farklı kişiler olabileceğinden aynı kişiye karşı işlenmiş suçtan bahsedemeyeceğiz.⁶²⁹ Ancak tek seferde bir veri bankasından birden fazla farklı kişiye ait kişisel verinin ele geçirilmiş olması halinde yine tek fille birden fazla kişiye karşı

⁶²⁸ İTİŞGEN, “Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu”, s. 196.

⁶²⁹ İTİŞGEN, “Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu”, s. 196.

aynı suçun işlenmiş olması sebebiyle zincirleme suç hükümlerinin uygulanması gerekecektir.

İçel'e göre; "failin bir suçu işlemek için aynı hukuki değeri koruyan daha hafif bir suçtan geçmek zorunda olduğu hallerde" geçit suç veya geçitli suç söz konusu olur. Geçit suçun bu tamından yola çıkarak taşınması gereken unsurlarını; amaç suçla aynı hukuksal yararı korumaya yönelmiş olması, amaç suçun işlenebilmesi için daha hafif bir suç olarak geçilmesinin zorunlu olması, fail ve mağdurunun amaç suçla aynı kişi olması, gerçekleştirilmesi istenen amaç suç ve failin geçit suça vücut veren hareketi arasında nedensellik bağının bulunması ve failin başlangıçtan itibaren bu amaç suçu işlemeye yönelik kastının bulunması şeklinde sayabiliriz. Bu koşulların mevcut olduğu ve iki suç tipinin birlikte gerçekleştirilmiş olduğu halde failin, sadece amaç suçtan cezalandırılması gerekecektir.⁶³⁰ Doktrinde TCK'nın 136. maddesinde düzenlenmiş olan kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçu ile kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu ve yine bilişim sistemine girme suçu (TCK md. 243) arasında geçit suç ilişkisi bulunduğu istikametinde kanaatler bulunmaktadır.

Kişisel verilerin hukuka aykırı olarak kaydedilmesi ve hukuka aykırı olarak yayılması veya verilmesi filleri uygulamada aynı hareketle tek defada veya birbirini takip eden hareketler olarak öncelik sonralık ilişkisi içerisinde karşımıza çıkabilmektedir. Daha önce kişisel verilerin hukuka aykırı olarak kaydedilmesi ve hukuka aykırı olarak yayılmasının tek hareketle gerçekleştirilmiş olması halinde bu suçların içtimainın ne şekilde olması gerektiği yönündeki kanaatler üzerinde durmuştuk.⁶³¹ Bu iki suç tipine vücut veren hareketlerin öncelik sonralık ilişkisi içerisinde ayrı ayrı gerçekleştirilmiş olduğu hallerde suçların içtimainın ne şekilde olacağı ise doktrinde; bu iki suç tipi arasında görünüşte içtima biçimi olarak geçit suç ilişkisi bulunup bulunmadığı istikametinde tartışmalara sebep olmuştur.⁶³² İki norm arasında kanunda açıkça öngörülmemiş örtülü, görünüşte birleşme türlerinden geçit suç ilişkisi kurulmaya yönelik düşünsel faaliyetler neticesinde kişisel veriler hukuka

⁶³⁰ İÇEL, Kayıhan, "Görünüşte Birleşme (İçtima) İlkeleri ve Yeni Türk Ceza Kanunu", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, S. 14, 2008, s. 47.

⁶³¹ Bkz. s. 87.

⁶³² "İnternet üzerinden iletişime geçip, kameralı sohbet yapmaya başladığı katılan ve mağdurların müstehcen görüntülerini bilgisayarına depoladığının ve bu şekilde elde ettiği görüntüleri internet ortamında yayımladığının" Yargıtay 12. CD., E: 2014/10400, K: 2015/51, T: 12.1.2015 www.kazanci.com (08.02.2018).

aykırı olarak kaydedildikten sonra başkalarına verilmiş veya yayılmışsa; verme veya yayma şeklindeki fiilini gerçekleştirebilmesi için kaydetme fiilinin işlenmesi kaçınılmazdır ve kişisel verilerin hukuka aykırı olarak kaydedilmesi geçit suç niteliğindedir.⁶³³ Doktrinde bir başka görüş ise; failin bu iki farklı suçu oluşturan ayrı filleri gerçekleştirme kastına bağlı olarak suçlar arasında geçit suç ilişkisi kurulması gerektiği istikametindedir. Buna göre eğer fail, TCK'nın 136. maddesinde düzenlenmiş olan kişisel verileri hukuka aykırı olarak verme veya yayma suçunu işlemek kastıyla kişisel verileri kaydetmişse, bu durumda kişisel verilerin hukuka aykırı olarak kaydetme şeklindeki suç kişisel verilerin verilmesi veya yayılması suçu için geçit bir suç niteliğinde olacak ve fail sadece TCK'nın 136. maddesinde düzenlenmiş olan suçtan cezalandırılacaktır. Buna karşılık, eğer daha önce hukuka aykırı olarak kaydedilmiş olan verinin sonradan oluşan bir kastla hukuka aykırı olarak verme veya yayma için kullanmışsa, farklı zamanlarda gerçekleştirilmiş olan kişisel verileri kaydetme ve verme veya yayma suçları arasında geçit suç ilişkisi bulunduğu bahsedilemez. Bu durumda fail her iki suçtan ayrı ayrı cezalandırılacaktır.⁶³⁴ İki suç tipi arasındaki görünüşte içtima ilişkisi bulunduğu istikametindeki bu kanaatlerin aksine doktrinde çoğunluk görüşü; iki suç arasında geçitli suç ilişkisinin kurulabilmesi için aranan failin bir suçu işlemek için daha hafif bir suçu işleme zorunluluğunun bulunmadığı gerekçesiyle geçit suç ilişkisi kurulamayacağı istikametindedir. Dolayısıyla madde gerekçesinde de vurgulandığı üzere, kişisel verilerin hukuka aykırı olarak kaydedilmiş olması zorunluluğu olmaksızın, yani TCK'nın 135. maddesinde düzenlenmiş olan kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu işlenmeksizin, TCK'nın 136. maddesinde düzenlenmiş olan kişisel verilerin hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek suçu işlenebileceği için, benimsediğimiz kanaat bu iki suç tipi arasında geçit suç ilişkisi bulunmadığı istikametindedir.⁶³⁵

Doktrinde, kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçu ile bilişim alanında işlenen suçlar arasında benzer istikamette bir düşünsel faaliyette bulunularak yine bir geçit suç ilişkisi kurulmaya çalışılmıştır. Buna göre TCK'nın 243. maddesinde düzenlenmiş olan bilişim sistemine hukuka aykırı

⁶³³ SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 356.

⁶³⁴ GÜLTEKİN, *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*, s. 174.

⁶³⁵ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 655.; İTİŞGEN, "Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu", s. 197.

olarak girme ve kalmaya devam etme fiili kişisel verilerin hukuka aykırı olarak verilmesi, ele geçirilmesi veya yayılması suçu bakımından geçit suç niteliğinde görülmüştür.⁶³⁶ Failin kişisel verileri bir bilişim sistemi kullanmaksızın ele geçirmesi, yayması veya başkalarına vermesi, her ne kadar uygulamada daha ziyade bilişim sistemleri kullanılarak bu fiiller gerçekleştirilmekteyse de, mümkündür. Dolayısıyla, bilişim sistemine girme veya sistemde hukuka aykırı olarak kalmaya devam etme şeklinde işlenen TCK'nın 243. maddesinde düzenlenmiş olan suça başvurmak, daha ağır suç olarak kabul ettiğimiz kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunun işlenebilmesi için zorunlu değildir. Ayrıca bu iki suçun aynı hukuksal değeri korumaya yönelik düzenlenmiş olduğu da söylenemeyeceğinden, aralarında bu itibarla da bir geçit suç ilişkisi kurulamayacağını söylemek gerekmektedir.⁶³⁷ Bu durumda kanaatimiz; failin bir bilişim sistemine girerek ve orda kalmaya devam ederek kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirmesi halinde, bilişim sistemine girme ve verileri ele geçirme şeklinde failin iki farklı hareketi ve bunların iki farklı şekilde dış dünyaya yansması söz konusu olduğu için, failin her iki suçtan ayrı ayrı cezalandırılması gerektiği istikametindedir.⁶³⁸

TCK'nın 244. maddesinin 2. fıkrasında, bilişim sistemindeki verilerin başka yere bir gönderilmesi seçimlik hareketi, “*Sistemi engelleme, bozma, verileri yok etme veya değiştirme*” suçuna vücut veren bir hareket olarak düzenleme altına almıştır.⁶³⁹

⁶³⁶ SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 355.; “TCK md. 136’da yer alan “hukuka aykırı olarak verileri ele geçirme suçu”nun oluşması için TCK md. 243/1’deki sisteme hukuka aykırı olarak girmenin gerçekleşmesi gerekmektedir.” MAHMUTOĞLU, Fatih Selami, “Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, ÜHFM, C. 71, S. 1, 2013, s. 865.

⁶³⁷ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 655.

⁶³⁸ İTİŞGEN, “Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu”, s. 197.;

⁶³⁹ “Suça sürüklenen çocuğun, mağdurla aralarında husumet başladığı dönemde, daha önce bildiği mağdura ait elektronik posta adresinin ve bu adresle bağlantı kurulan facebook hesabının internet şifresini ve ismini değiştirerek, hakkı bulunmadığı halde bilişim sistemindeki mağdura özel kısma girdiği ve mağdura ait facebook hesabı üzerinden, mağdur tarafından yazılıyormuş algısı doğuracak şekilde, mağdurun arkadaşlık listesindeki kişilerle cinsel içerikli sohbet yapıp, hukuka aykırı olarak sistemde kalmaya devam ederek, mağdurun sistemdeki kendisine ait kısma erişimini engellediği anlaşılmakla; suça sürüklenen çocuğun, mağdura ait elektronik posta adresinin ve bu adresle bağlantı kurulan facebook hesabının internet şifresini, daha önceden bildiği ve iddianamede, suça sürüklenen çocuğun mağdura ait başka bir kişisel veriyi, hukuka aykırı olarak ele geçirdiği, başkasına verdiği ya da yaydığının iddia edilmediği nazara alındığında, suça sürüklenen çocuğun eyleminde TCK'nın 136/1. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme suçunun yasal unsurlarının oluşmadığı, Ancak; bilişim sistemindeki mağdura özel kısma girip, hukuka aykırı olarak sistemde kalmaya devam eden ve mağdurun bilişim sistemindeki kendisine ait kısma erişimini engelleyen suça sürüklenen çocuk hakkında, TCK'nın 244/2. maddesindeki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan mahkumiyet kararı verilmesi

Verilerin başka yere gönderilmesi seçimlik hareketi, gönderilen verinin aynı zamanda kişisel veri niteliği taşıması halinde, kişisel verilerin hukuka aykırı olarak verilmesi veya yayılması suçunun da oluşmasına sebep olabilecektir.⁶⁴⁰ Bu durumda fail, verileri gönderme şeklindeki tek hareketiyle, hem kişisel verilerin hukuka aykırı olarak yayılması veya verilmesi suçunu (TCK md. 136) hem de TCK'nın 244. maddesinde düzenlenmiş olan “*Sistemi engelleme, bozma, verileri yok etme veya değiştirme*” suçunu işlemiş olacaktır.⁶⁴¹ Doktrinde fikri içtima hükümleri uygulanarak failin, en ağır cezayı gerektirenden suçtan cezalandırılması gerektiğini düşünen⁶⁴² müelliflerin yanı sıra iki suç tipi arasında özel genel norm ilişkisi bulunduğundan failin sadece 244. maddede düzenlenmiş olan suçtan cezalandırılması gerektiği de kabul edilmektedir.⁶⁴³ Buna göre; bilişim sistemi vasıtasıyla kişisel verilerin gönderilmiş olması halinde, kullanılan vasıta itibarıyla TCK'nın 244. maddesindeki suç daha özel nitelikli bir düzenleme olarak kabul edilmektedir.

Bunun dışında kişisel verilerin hukuka aykırı olarak verilmesi veya yayılması suçu ile TCK'nın 258. maddesinde düzenlenmiş olan “*göreve ilişkin sırrın açıklanması*” suçunun birlikte gerçekleşmesi de uygulamada karşılaşılabilmektedir. TCK'nın 258. maddesine göre “görevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği ve gizli kalması gereken belgeleri, kararları ve emirleri ve diğer tebligatı açıklayan veya yayınlayan veya ne suretle olursa olsun başkalarının bilgi edinmesini kolaylaştıran” kamu görevlisi failin, bu suçun konusunu oluşturan belgelerin aynı zamanda kişisel veri niteliğinde bilgiler içeriyor olması halinde, kişisel verilerin hukuka aykırı olarak verilmesi veya yayılması suçundan da sorumlu tutulması gerekecektir. Bu durumda failin, tek hareketiyle birden fazla farklı suç oluşmuş

gerekirken” Yargıtay 12. CD., E: 2014/6905, K: 2014/22910, T: 17.11.2014 www.kazanci.com (08.02.2018).

⁶⁴⁰ “Somut olayda; sanığın, tamir için katılanın kendisine bıraktığı dizüstü bilgisayarında bulunan fotoğrafları ile messenger programında oturum açmak için kullandığı elektronik posta adres ve şifrelerini mesleğinin sağladığı kolaylıktan yararlanarak ele geçirip veri taşımakta kullanılan flash diske aktararak, elektronik posta adres ve şifre bilgilerini kullanarak açtığı katılana ait messenger oturumunda, kendisine ait başka bir hesabı, katılanın hesabına arkadaş olarak eklemesi, bilahare katılanın elektronik posta adresinin şifresini değiştirerek messenger programına girişini engellemesi şeklindeki eyleminin, TCK'nın 136/1. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçu ile TCK'nın 244. maddesinin 2. fıkrasında düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu oluşturduğu” Yargıtay 12. CD., E: 2013/15899, K: 2014/8411, T: 7.4.2014 www.kazanci.com (08.02.2018).

⁶⁴¹ GÜLTEKİN, *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*, s. 176.

⁶⁴² YENİDÜNYA/DEĞİRMENCİ, *Mukayeseli Hukukta ve Türk Hukukunda: Bilişim Suçları*, Legal Yayıncılık, İstanbul, 2003, s. 32.

⁶⁴³ GÜLTEKİN, *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*, s. 178.

olacaktır ve fikri içtima hükümleri doğrultusunda failin, daha ağır ceza gerektiren kişisel verilerin hukuka aykırı olarak verilmesi veya yayılması suçunun kamu görevlisi tarafından gerçekleştirilmiş nitelikli halinden sorumlu tutulması gerekecektir. Nitekim kanaatimiz, TCK'nın 258. maddesindeki “göreve ilişkin sırrın açıklanması” suçunun, kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçuna göre daha genel nitelikte bir norm olması itibarıyla da böyle bir halde failin, TCK'nın 136. maddesinden cezalandırması gerektiği yönündedir.

f. Nitelikli Haller

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçunun, failin şahsından kaynaklanan nitelikli hali olarak; TCK'nın 137. maddesinde suçun “kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle”⁶⁴⁴ veya “belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle” islenmesi düzenlenmiştir.⁶⁴⁵ Bu halde faile verilecek cezanın suçun temel şekline göre

⁶⁴⁴ “İncelenen dosyada, Türkiye çapındaki vergi dairelerinin, defterdarlıkların ve Vergi Dairesi Başkanlığı'nın bütün işlemlerinin bilgisayar ortamında gerçekleştirilmesine olanak sağlayan, vergi mükelleflerinin vergi ile ilgili işlemleri ve kişisel bilgilerinin kayıt altına alındığı Maliye Bakanlığı Gelir İdaresi Başkanlığı Vergi Daireleri Otomasyon Projesi (VEDOP) sistemine giriş yapılarak, Cumhurbaşkanı, Başbakan, bakanlar, milletvekilleri, politikacılar, bürokratlar, diplomatlar, bilim adamları, gazeteciler, sanatçılar, sporcular, iş adamları gibi içinde bulundukları konum, mesleki faaliyetleri veya görevleri sebebiyle kamuoyu tarafından tanınan kişilerin, kişisel verilerinin ele geçirilip, basın ve yayın organlarında ifşa edildiğinden bahisle başlatılan adli soruşturma sonunda” Yargıtay 12. CD., E: 2013/25410, K: 2014/20333, T: 20.10.2014 www.kazanci.com (08.02.2018).

⁶⁴⁵ “Mağdurun, doktor olarak çalıştığı özel hastanede farklı kadınlarla cinsel ilişkiye girdiği esnada gizlice kaydettiği görüntüleri bilgisayarına depoladığı ve 2010 yılı içerisinde arızalanan bilgisayarının tamiri için sanık ...'ın çalışmakta olduğu firmayla anlaştığı, sanık ...'ın mağdura ait bilgisayarı tamir ederken, mağdurun cinsel içerikli görüntülerini fark edip, kişisel hard diskine bu görüntüleri kopyaladığı ve adı geçen sanığın firmadan ayrıldığı 2012 yılında, arkadaşları olan diğer sanıklar ... ve ... ile fikir ve eylem birliği içerisinde hareket ederek, mağdurdan görüntüleri iade etme karşılığında para talep edip, aksi takdirde görüntüleri yayacakları tehdidiyle mağdura şantaj yaparak, söz konusu görüntüleri CD'ler halinde çoğalttıkları ve sanıkların 15.6.2012 günü kolluk görevlilerince yakalandıkları olayda, sanık ...'ın mesleğinin sağladığı kolaylıktan yararlanmak suretiyle ele geçirip, birlikte hareket eden sanıklar tarafından şantaj suçunda kullanılmak için çoğaltılan mağdurun cinsel mahremiyetine dair görüntülerin, mağdurun özel yaşam alanı kapsamında bulunduğu gözetilerek ve TCK'nın 61/1. maddesinde yer alan ölçütler de nazara alınarak, görüntü veya seslerin kaydedilmesi suretiyle özel hayatın gizliliğini ihlal suçundan dolayı sanık ...'ın TCK'nın 134/1-2, 137/1-b; TCK'nın 37/1. maddesi yollamasıyla aynı Kanun'un 134/1-2; sanıklar ... ve ...'nin TCK'nın 37/1. maddesi yollamasıyla aynı Kanun'un 134/1-2. maddeleri gereğince ve anılan suç açısından 5.7.2012 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren 6352 Sayılı Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun'un 81. maddesiyle yapılan değişiklikler de dikkate alınarak, şantaj suçundan dolayı sanıkların TCK'nın 37/1. maddesi yollamasıyla aynı Kanun'un 107/2. maddesi atfıyla 107/1. maddesi uyarınca ve her iki suçtan temel cezalarda asgari haddin uzaklaşımak suretiyle mahkumiyet hükümleri kurulması gerekirken, yasal ve yeterli olmayan yazılı gerekçelerle sanıklar hakkında TCK'nın 136/1. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçundan dolayı

yarı oranında artırılacağı hüküm altına alınmıştır. Bu nitelikli haller aynı zamanda kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu içinde geçerlidir ve detaylı açıklamaya bu suç başlığı altında yer verilmiştir.

g. Yaptırım

Kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi suçu, TCK'da, kişisel verilere karşı işlenen diğer suç tipleri gibi re'sen takip edilen, soruşturulma ve kovuşturulması şikayete bağlı olmayan bir suç olarak düzenlenmiştir. Kişisel verilerin hukuka aykırı olarak verildiği veya ele geçirildiğinin yetkili merciler tarafından ihbar veya diğer herhangi bir yolla öğrenilmesiyle failerin soruşturulması ve kovuşturulmasına başlanması kamusal makamlar için bir zorunluluktur.⁶⁴⁶ Suçun takibi şikayete bağlı olmadığından ve şikayete tabi olmamakla birlikte uzlaşmaya tabi olarak sayılan suçlar arasında yer almadığından bu suçu işleyen failin ve mağdurun uzlaştırılması mümkün değildir. Bu suçun işlenmesi dolayısıyla tüzel kişiler hakkında TCK'nın 140. maddesinde öngörüldüğü üzere güvenlik tedbirleri uygulanması gerekecektir. Suçun temel şekli için kanunda öngörülen ceza iki yıldan dört yıla kadar olup, 137. maddedeki nitelikli hallerden birinin gerçekleşmiş olması halinde bu ceza yarı oranında artırılacaktır. Bu durumda suçun temel şekline ilişkin 8 yıl olarak uygulanan dava zaman aşımının, nitelikli şeklinin işlenmiş olması halinde üst sınırın 5 yıldan fazla hapis cezasını gerektirmesinden ötürü 15 yıl olarak uygulanması gerekecektir.

mahkumiyet hükümleri kurulması" Yargıtay 12. CD., E: 2015/5128, K: 2016/10207, T: 15.6.2016 www.kazanci.com (04.01.2018).

⁶⁴⁶ "Dosya kapsamına göre; erkek arkadaşının sanık D. ile kendisini aldattığını düşünen sanık A.'nın, bir sosyal paylaşım sitesine "O. E." adıyla üyelik işlemleri yaparak, elektronik posta adresi oluşturduğu sitede, bir başka bayana ait göğüs dekoltesi bir resim koyup, sanık D.'ye ait cep telefonu numarasına da yer vermesi sonucu, tanımadığı kişiler tarafından telefonundan aranarak cinsel içerikli arkadaşlık teklifleri alan sanık D.'nin, cep telefonu numarasını yayan kişinin sanık A. olduğunu öğrenmesi üzerine, kendisini telefonundan arayan tanımadığı kişilere, telefon numarasını değiştirdiğini belirterek, sanık A.'nın kullanımındaki cep telefonu numarasını verdiği ve sanık A.'nın da tanımadığı kişiler tarafından telefonundan aranarak rahatsız edilmesi üzerine her iki sanığın birbirlerinden şikayetçi olup, bilahare şikayetlerinden vazgeçtikleri olayda, TCK'nın 139/1. maddesi gereğince, sanıkların üzerlerine atılı verileri hukuka aykırı olarak verme veya ele geçirme suçunun, soruşturulması ve kovuşturulmasının şikayete bağlı olmadığı gözetilmeden, kovuşturma aşamasında her iki mağdur sanığın şikayetlerinden vazgeçtiklerinden bahisle, yazılı şekilde düşme kararı verilmesi, kanuna aykırı olup..." Yargıtay 12. CD., E: 2012/22005, K: 2013/24489, T: 04.11.2013 www.kazanci.com (04.01.2018).

4. Verilerin Yok Edilmemesi Suçu

a. Genel Olarak

Kişisel verilerin korunması ve işlenmesinde uyulması gereken, en temel ilkelerden biri de verilerin “amaçla bağlantılı, sınırlı ve ölçülü işlenmesi” ilkesidir. Bu ilkeye göre; kişisel verilerin, kaydedilme amacını gerçekleştirmek için gerekli olan miktarda ve bu amacın gerçekleşmesini sağlayacak süreyle veri sorumluları tarafından işlenmesi veya kayıt altında tutulması gerekmektedir. Bu ilkenin diğer bir boyutu; başlangıçta hukuka uygun olarak toplanmış da olsa toplanma amacı için gereksiz hale gelmesi veya bu amacın gerçekleşmesi/tamamlanması ya da gerçekleşme imkanının kalmaması gibi durumlarda kaydedilmiş olan kişisel verilerin silinmesi veya anonim hale getirilmesini gerektirmesidir.⁶⁴⁷ 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 4. maddesiyle güvence altına alınmış olan verilerin hukuka uygun işlenmesine ilişkin ilkelere ve 7. maddesindeki verilerin silinmesine ilişkin yükümlülöklere aykırı olarak kişisel verilerin tutulmaya devam edilmesi, unsurlarını detaylı olarak ele alacağımız Türk Ceza Kanunu’nun 138. maddesi ile düzenlenmiş olan “kişisel verilerin yok edilmemesi” suçuna vücut vermektedir.⁶⁴⁸ Bu istikamette 6698 sayılı Kanun’un 17. maddesinin ikinci fıkrasında da özel olarak, verileri 6698 sayılı Kanun’da öngörölen yükümlölöklere aykırı olarak silmeyen veya anonim hale getirmeyenlerin, TCK’nın 138. maddesine göre cezalandırılacağı hüküm altına alınmıştır. 6698 sayılı Kanun’un genel düzenlemesinin yanı sıra pek çok mevzuatla kişisel veri niteliği taşıyan belge veya bilgilerin, hukuka uygun belli bir amaç istikametinde toplanması veya depolanması meşru kılınmıştır.⁶⁴⁹ Bu belge veya bilgilerin tutulması için kanunlarda öngörölen muhafaza sürelerinin dolmasına rağmen veya 6698 sayılı Kanun’un 7. maddesine göre yok edilmesi gerektiği halde, kişisel veriler yok edilmemiş veya anonim hale getirilmemişse bu yükümlölöğe aykırı

⁶⁴⁷ “Unutulma hakkına gelince; 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.” Yargıtay HGK., E: 2014/4-56, K: 2015/1679, T: 17.06.2015 www.kazanci.com (04.01.2018).

⁶⁴⁸ AKDAĞ, “Türk Ceza Hukukunda Kişisel Verilerin Korunması İlkeleri”, s. 37.

⁶⁴⁹ Ayrıca 138. maddenin ikinci fıkrasında Ceza Muhakemesi Kanunu’na göre toplanmış olan verilerin öngörölen sürelerde yok edilmemiş olması nitelikli olarak düzenlenmiştir.

davranan kişiler, TCK'nın 138. maddesinde düzenlenmiş olan kişisel verileri yok etmeme suçunu işlemiş olacaktır. Şüphesiz ki ilgili mevzuatlarda öngörölmüş süreler sonunda veya 6698 sayılı Kanun'a göre yok edilmesi gereken kişisel verilerin, hukuka uygun olarak depolandıkları yerde sonsuza kadar tutulmaya devam edilmesi kişilerin, bilgilerinin sürekli olarak başkalarının elinde olduđu düşüncesine kapılarak kişisel güvensizlik⁶⁵⁰ ve özel hayatlarının gizliliğı ihlali tehdidi içerisinde yaşamalarına sebep olacaktır.⁶⁵¹

b. Suçla Korunan Hukuksal Yarar

Kişisel verilerin yok edilmemesi suçu ile korunan hukuksal yarar, TCK'da düzenlenmiş olan kişisel verilere karşı işlenen diğer suçlarla da korunan hukuksal yarar olan; kişisel verilerin korunması hakkı ve bu yarara ek olarak kamu idaresine duyulan güven olarak kabul edilmektedir.⁶⁵² Bunun yanında doktrinde, kişisel verilerin yok edilmemesi suçunun her ne kadar kamu idaresinin güvenilirliğini genel anlamda korumaya çalıştığı kabul edilmekteyse de kişisel verilerin yok edilmemesi suçunun, özel hayata ve hayatın gizli alanına karşı işlenen suçlar arasında düzenlenmiş olması itibarıyla koruduğı hukuksal yararın kamu idaresinin güvenilirliği olamayacağı iddia edilmektedir.⁶⁵³ Bu istikamette çoğunluk görüşü; bu suçla münhasıran veri sahiplerinin özel hayatının gizliliğı hukuksal yararının korunmak istendiğine ilişkindir.⁶⁵⁴

Kanaatimize göre; bu suçla kişisel verilerin korunması hakkının içeriğini oluşturan; kişisel veriler ve kişisel verilere sahip olan kişilerin korunması, korunması gereken hukuki bir değer olarak kabul edilmekteyken, bu değere ek olarak kamu idaresine duyulan güven de korunmak istenmektedir. Zira kişisel verileri hukuka uygun sebeplerle kamusal makamlar tarafından toplanmış olan kişiler, bu verilerin sonsuza kadar kamu idaresinin uhdesinde tutulmayacağı ve kamu idaresinin işleyişi için bu verilere duyulan ihtiyacın ortadan kalkması halinde verilerinin silineceğine

⁶⁵⁰ MENDOS KUŞKONMAZ, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, s. 160.

⁶⁵¹ HAFIZOĞULLARI, ÖZEN, "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar", s. 22.

⁶⁵² SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 357.; DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 657.

⁶⁵³ GÜLTEKİN, *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*, s. 183.

⁶⁵⁴ GÜLTAŞ, *Özel Hayata Karşı Suçlar*, s. 262; ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 587.; HAFIZOĞULLARI, ÖZEN, *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar*, s. 291.

ilişkin kamu idaresine karşı bir güven duymaktadır. Bu istikamette, kişisel verilerin kanunlarla belirlenen süreler içerisinde ve görevli makamlarca yok edilecek olduğuna ilişkin vatandaşların kamu idaresine karşı duyduğu bu güvene aykırılık, yok etme yükümlülüğü bulunan kişilerin TCK'nın 138. maddesine göre cezalandırılmasını gerektirmektedir.

c. Suçun Unsurları

i. Maddi Unsurlar

1. Suçun Konusu

TCK'da kişisel verilerin korunmasına ilişkin düzenlenmiş olan diğer suç tiplerinde olduğu gibi kişisel verilerin yok edilmemesi suçunun hukuki konusunu da kişisel veriler oluşturmaktadır. TCK'nın 138. maddesinin gerekçesinde açıkça belirtildiği üzere suçun konusunu oluşturan bu verilerin hukuka uygun olarak kaydedilmiş olması gerekmektedir. Zira 138. madde ile de mevzuata uygun olarak kaydedilmiş olan verilerin yine mevzuatta öngörülen süreler içerisinde yok edilmemiş olması cezalandırılmaktadır. Bunun dışında doktrinde bu suçun hukuki konusunu oluşturan kişisel verilerin, 138. maddenin lafzına göre taşınması gereken bir diğer nitelik olarak sistem içinde kayıtlı olmasının aranması gerektiği şeklinde değerlendirmede bulunmuştur.⁶⁵⁵ Ancak günümüzde her ne kadar verilerin daha ziyade bir bilişim sistemi içerisinde tutulması tercih edilmekteyse de, 138. maddenin lafzının kişisel verilere karşı işlenen suç tiplerinde olduğu gibi hem otomatik hem de otomatik olmayan vasıtalarla işlenmiş her türlü kişisel veri hakkında uygulanabilecek şekilde geniş yorumlanması gerektiği kanaatimizdir.

138. maddenin ikinci fıkrasına göre; suçun hukuki konusunun, “Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi

⁶⁵⁵ ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 588.

gereken veri olması” ise faile verilecek olan cezanın bir kat artırılması gerektiren nitelikli bir hal olarak düzenlenmiştir.⁶⁵⁶

2. Fail ve Mağdur

Kişisel verileri yok etmeme suçu, fail bakımından özellik arz eden, özgü bir suç olarak düzenlenmiştir. Buna göre suçun faili, ancak kanunla verileri yok etmekle görevlendirilmiş ve verileri belli süreler içerisinde yok etme yükümlülüğü olan kamu görevlisi veya özel kişiler olabilecektir. TCK’nın 138. maddesinin lafzında fail, “verileri sistem içinde yok etmekle yükümlü olan” herhangi bir kişi olarak kabul edilmiş olduğundan, bu yükümlüğün özel bir kişi veya kişilere ait olabilmesi mümkün olabileceği gibi kamu görevlisi olan bir kişiye de ait olabilmesi mümkündür. Doktrinsel kabule ve uygulamaya göre ise; bu yükümlülük daha ziyade kamu görevlilerinin şahsında doğmakta ve kişisel verileri yok etmeme suçu genelde kamu görevlisi olan kişilerce işlenmektedir.⁶⁵⁷ 6698 sayılı Kanun’un 7. maddesiyle de kişisel verilerin yok edilmesi veya anonim hale getirilmesine ilişkin olarak veri sorumluları yükümlü tutulmuştur. Kanun’a göre veri sorumlusu; “kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi” olarak tanımlanmaktadır.

Bu suçun mağduru, kural olarak suçun hukuki/maddi konusu olan hukuka uygun olarak kaydedilmiş verilerin sahibi gerçek kişilerdir.⁶⁵⁸ Ancak doktrinde, suçla korunan hukuksal yararla bağlantılı olarak suç mağdurunun belirlenmesi yoluna da gidilmiştir. Buna göre; suçla korunan hukuksal yararı salt kişilerin özel hayatının gizliliği olarak kabul eden müellifler, suçun mağdurunun sadece kişisel verileri hukuka uygun olarak sisteme kaydedilen⁶⁵⁹ ancak belirlenen süreler geçmiş olmasına rağmen yok edilmeyen gerçek kişiler kabul etmekteyken,⁶⁶⁰ bu suçun aynı zamanda “kamu idaresinin güvenilirliği ve işleyişi” hukuksal yararını da korumakta olduğunu kabul eden müellifler, mağdurun belli bir gerçek kişi değil kamu olduğu kanaatini

⁶⁵⁶ CMK md. 80., 135/3., 137., 139/6., 140/4.; Ayrıntı için bkz. s. 71.

⁶⁵⁷ HAFIZOĞULLARI, ÖZEN, *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar*, s. 292.; GÜLTAŞ, *Özel Hayata Karşı Suçlar*, s. 264.

⁶⁵⁸ Mağdurun suçun maddi konusunun ait olduğu kimse olduğu istikametinde bkz. ARTUK, GÖKCEN, YENİDÜNYA, *Ceza Hukuku Genel Hükümler*, s. 283.; DEMİRBAŞ, *Ceza Hukuku Genel Hükümler*, s. 556.

⁶⁵⁹ ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 588.

⁶⁶⁰ GÜLTAŞ, *Özel Hayata Karşı Suçlar*, s. 264.

benimsemektedir. İkinci kanaati benimseyen müelliflere göre; kişisel verileri yok edilmeyen gerçek kişiler ancak bu suçtan zarar gören kişi olarak kabul edilmektedir.⁶⁶¹ Buna karşılık doktrinde, suçla kamu idaresine duyulan güvenin de korunan bir hukuksal yarar olarak benimseyip mağdurun, hem kamu idaresi hem de verileri yok edilmeyen gerçek kişiler olduğu kanaati de kabul görmektedir.⁶⁶²

Kişisel verilerin tutulmasının, depolanmasının veya kaydedilmesinin, işleme amacına göre makul sayılabilecek bir süreyle sınırlı olmasını gerektiren ve kişisel verilerin korunmasına ilişkin temel ilkelerden bir olan ölçülülük ilkesi; bu suçla korunan hukuksal yarara eşdeğer bir faydanın sağlanmasına hizmet etmektedir. Kanaatimizce; kişisel verilerin korunması ilkeleri gibi bu suçu ihlal edilebilecek kişiler bakımından da herhangi bir ayırım gözetilemeyecektir. Yani kamu görevlisi olsun olmasın herkes bu suçun faili olabilir. Yine kişisel verilerin yok edilmesinin ihmal edilmesi suçunun mağdurunun da verileri hukuka uygun olarak kayıt altına alınmış olan gerçek kişiler olduğu kanaatimizdir.

3. Hareket

Bu suçun hareket unsurunu, hukuka uygun olarak kayıt altına alınmış olan kişisel verilerin hukuka aykırı olarak kayıtlı tutulmaya devam edilmesi, verilerin silinmesi veya yok edilmesi yükümlülüğünün ihmal edilmesi oluşturmaktadır. Bu itibarla suç ihmali hareketle işlenebilen bir suç tipidir. Kanun bu suçu işlemeye elverişli ihmali hareketin, taşınması gereken bazı özellikler üzerinde özellikle durmuştur. Bunlardan ilki ihmali hareketin kanundan doğmuş olması, yani maddi veya şekli anlamda bir kanunla⁶⁶³ verilerin yok edilmesi yükümlülüğünün öngörülmüş olmasıdır. İkincisi kanundan doğan bu yükümlülüğün yine ilgili kanunda öngörülen süreler geçmiş olmasına rağmen ihmal edilmiş olmasıdır. TCK'nın 138. maddesini,

⁶⁶¹ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 658.

⁶⁶² SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 358.

⁶⁶³ Mutlaka bir kanunla değil idarenin düzenleyici bir işlemiyle de verilerin silinmesine ilişkin bir yükümlülük öngörülmüş olabilir veya kanunla öngörülmüş olan yükümlülüğün hangi süreler içerisinde ve kimin tarafından yerine getirileceği yine idarenin düzenleyici bir işlemiyle belirlenmiş olabilir. ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 588.; Örneğin; Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti Dinlenmesi Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş Görev ve Yetkileri Hakkında Yönetmelik 11. maddesi ;“Dinlemenin içeriğine ilişkin kayıtlar ilgili kurumların en üst amirinin ve bu kayıtların Başkanlıkta da tutulması halinde Başkanın denetimi altında en geç on gün içinde yok edilir.”

düzenlenme amacına uygun yorumladığımızda “kanunların belirlediği süreler”, verilerin sistemden silinmesi için değil, sistemde tutulması için izin verilen süreler olarak kabul edilmelidir.⁶⁶⁴ Buna göre; “kanunlarla belirlenen sürelerin” geçmiş olması⁶⁶⁵ veya ayrıca tespit edilmesi gereken bir olayın gerçekleşmiş olması gibi bir vadenin tamamlanması⁶⁶⁶, hukuka uygun olarak kayıt altına alınmış olan verilerin silinmesi için öngörülmüş olabilir. Bunun dışında ihmali hareketin bu yükümlülüğü yerine getirmesi gereken kişi tarafından gerçekleştirilmiş olması, yani kanunen bu yükümlülüğü yerine getirecek bir kişinin belirlenmiş olması gerekmektedir.⁶⁶⁷ Bu belirleme ismen veya ifa edilen göreve göre yapılmış olabilir.

6698 sayılı Kanun’un 7. maddesi ile de verilerin yok edilmesine ilişkin; “bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.” şeklinde bir hüküm öngörülmüştür. Buna göre, Kanun’un 5. ve 6. maddelerinde kişisel verilerin işlenmesi için gerçekleşmesi gereken koşulların ortadan kalkması halinde⁶⁶⁸ veri sorumlularının verileri silme, yok etme veya anonim hale getirme yükümlülükleri doğmaktadır. Veri sorumlularının, kişisel verileri res’en silme, yok etme veya anonim hale getirme yükümlülüklerine ilişkin süreler ve usul, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 11. maddesinde özel olarak düzenlenmiştir.⁶⁶⁹ Kanun’un veri

⁶⁶⁴ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 660.

⁶⁶⁵ Adli sicil ve arşiv bilgilerinin silinmesi hakkında 5352 sayılı Adli Sicil Kanunu’nun 12. maddesi ile 15 ila 45 yıl arasında belli vadeler öngörülmüştür.

⁶⁶⁶ Örneğin; CMK md. 80/2’ye göre, genetik inceleme sonuçlarının yok edilmesi için öngörülen vade; “kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi” şeklindedir.

⁶⁶⁷ HAFIZOĞULLARI, ÖZEN, “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar”, s. 22.

⁶⁶⁸ Bu maddelerde sayılan hukuka uygun olarak verilerin işlenebileceği koşulların ortadan kalktığı; “kişisel verileri işlemeye esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası; taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi; kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması; kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması; kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması” hallerinde kişisel verilerin imhası gerekmektedir. KVK Kurumu Yayınları, 6698 Sayılı Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar, s. 58. <https://www.kvkk.gov.tr> (04.02.2018).

⁶⁶⁹ “1. Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.
2. Periyodik imhanın gerçekleştirileceği zaman aralığı, veri sorumlusu tarafından kişisel veri saklama ve imha politikasında belirlenir. Bu süre her halde altı ayı geçemez.

sorumluları için öngörmüş olduğu, usul ve esasları Yönetmelik’te belirlenmiş olan, bu yükümlülüğüne aykırı davranması halinde veri sorumlularının, TCK’nın 138. maddesinde düzenlenmiş olan kişisel verileri yok etmeme suçundan sorumlu tutulmaları gerekecektir. Bu yaptırım, 6698 sayılı Kanun’un 17. maddesinin ikinci fıkrasında, veri sorumlularının hem verilerin silinmesi hem de anonim hale getirilmesine ilişkin yükümlülüklerine aykırı davranmaları halinde uygulanması gereken bir yaptırım olarak öngörülmüştür. TCK’nın 138. maddesine göre failin, sadece görevli olduğu halde verileri silmekten imtina etmiş olması veya silmeyi ihmal etmiş olmasına ilişkin ihmali hareketinin cezalandırılacağı öngörülmüşken, 6698 sayılı Kanun silmeye alternatif olarak verilerin anonim hale getirilmemesinin⁶⁷⁰ de TCK’nın 138. maddesine göre cezalandırılması gerektiği düzenleme altına alınmıştır.

Silmek kavram olarak; “ortadan kaldırmak, yok etmek”⁶⁷¹ anlamlarına gelmekte olup, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’te kişisel verilerin silinmesi; “kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi” olarak tanımlanmaktadır. Kişisel verilerin silinmesinin, verilerin kayıt altında tutulma şekline veya kullanılan program çeşidine göre muhtelif yöntemleri olabilmektedir. Bu yöntemlere örnek olarak; manuel olarak kayıt altında bulunan kişisel veriler bakımından karartma yöntemiyle, otomatik yöntemlerle işlenerek bir taşınabilir bellek üzerinde tutulan kişisel veriler için de uygun format veya yazılım kullanılarak verilerin silinmesini gösterebiliriz.⁶⁷² Bu işlemlerle amaçlanan, verileri saklamaya elverişli tüm kayıt ortamlarından kişisel verilerin, geri döndürülemeyecek veya yeniden kullanılamayacak şekilde yok edilmesidir. Doktrinde, TCK’nın 138. maddesiyle yalnızca bir sistem içerisinde tutulmakta olan hukuka uygun işlenmiş kişisel verilerin yok edilmemesi ihmali hareketinin cezalandırmakta olduğu şeklinde

3. Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusu, 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.

4. Kurul, telafisi güç veya imkansız zararların doğması ve açıkça hukuka aykırılık olması halinde, bu maddede belirlenen süreleri kısaltabilir.” Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik md. 11.

⁶⁷⁰ “Anonimleştirme: Daha öncesinde bir kişiyle ilişkilendirilmiş olan verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.” KVK Kurumu Yayınları, 6698 Sayılı Kanun’da Yer Alan Kurumsal Terimler, s. 8. <https://www.kvkk.gov.tr> (04.02.2018).

⁶⁷¹ TDK Güncel Türkçe Sözlüğü, www.tdk.gov.tr (03.01.2018).

⁶⁷² Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, KVK Kurumu Yayınları, Ankara, 2018, s. 9.

kanaat sahibi müelliflere göre;⁶⁷³ kişisel verilerin silinmesi ancak verileri bir sistemden yok etmeye elverişli hareketlerle gerçekleştirilebilecektir. Buna göre, ancak verilere erişim için verilen komutun geçersiz kalmasını sağlayacak her türlü usulle sistemden silinebilecek olan bir kişisel verinin hukuka uygun olarak kaydedilmiş olduğu sistemden yok edilmemesi halinde, TCK'nın 138. maddesinde düzenlenmiş olan suç oluşabilecektir.⁶⁷⁴

Kişisel verileri yok etmeme suçu; failin, verilerin kayıtlı tutulabileceği süreler geçmiş olması ve kendisinin bu sürelerde verileri silmekle yükümlü olmasına rağmen verileri yok etmediği süre boyunca işlenmeye devam edilmekte olan mütemedi bir suçtur.

ii. Manevi Unsur

TCK'nın 135. maddesinde düzenlenmiş olan kişisel verileri yok etmeme suçu, genel suç işleme kastıyla işlenebilecek, failin özel bir kast ya da saikle hareket etmesini gerektirmeyen ve taksirli hareketle işlenebilirliği bulunmayan bir suç tipidir. Failin, kanunla öngörülen süreler içerisinde kişisel verileri yok etme yükümlülüğünü bilerek ve isteyerek ihmal etmiş olması gerekir. Ancak sürelerin hesaplanmasında hataya düşülmüş olması veya yükümlülüğün unutulması ihmal edilmiş olması halinde, failin suç işleme kastının fiili hatadan ötürü ortadan kalkacağı kabul edilmektedir.⁶⁷⁵

iii. Hukuka Aykırılık

Bir kanun hükmünün sağladığı yetki kapsamında hukuka uygun ve belli bir süreye bağlı olarak kayıt altına alınmış olan kişisel verilerin, bu sürelerin sonunda yok edilmemesini hukuka uygun kılabilecek bir hukuka uygunluk sebebi bulunmamaktadır. Doktrinde, bu suç tipi ile özel hayatın ve kişisel verilerin korunması hakkına ilişkin hukuksal yararın yanı sıra, vatandaşların kamu düzenine karşı duyduğu güveninin de korunmakta olduğunu kabul eden ve kamu düzenini bu suçun mağduru olarak gören müellifler, bu suçun mağduru olarak kamuyu kabul etmiş olduklarından

⁶⁷³ ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 588.

⁶⁷⁴ BÜK, *Elektronik Ortamda Saklanan Kişisel Verilerin Elde Edilmesi / Değiştirilmesi Suretiyle İşlenen Suçların Ceza Hukuku Açısından Değerlendirilmesi*, s. 131.

⁶⁷⁵ HAFIZOĞULLARI, ÖZEN, “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar”, s. 22.

ötürü her ne kadar verileri silinmeyen ilgili kişinin rızası bulunsa da bu rızanın suçu hukuka uygun kılan bir sebep olarak kabul edilemeyeceği kanaatine sahiptir.⁶⁷⁶ Buna karşılık ilgilinin rızasının, bu suçu hukuka uygun kılabilen bir sebep olarak kabul edilememesine ilişkin bir diğer gerekçe ise; kanunen verilerin silinmesinin zorunlu kılındığı bir kural mevcut iken ilgilinin kanun hükmüne aykırılığa rıza göstermesinin muteber kabul edilemeyeceği ileri sürülmüştür. Ancak verilerin belli bir sürede silinmesini öngören düzenlemede ilgilinin rızasının verilerin yok edilmesi yükümlülüğüne istisna olarak düzenlenmiş olması halinde, kişilerin vermiş olduğu rızanın bir anlam ifade edebilecek ve failin yükümlülüğe aykırı davranışını hukuka uygun kılacaktır.⁶⁷⁷ Buna göre, kanunun yapılmasını emrettiği bir işleme karşılık, işlemin taraflarından biri olarak kabul edilen ilgili kişinin tek başına işlemin yapılmamasına rızası olduğunu beyan etmesi bu işlemi gerçekleştirecek olan kişiyi yükümlülük altından kurtarmaya yetmeyecektir. Ancak verilerin yok edilmesi yükümlülüğünü öngören kanun, ilgilinin rızası varsa bu yükümlülüğün ortadan kalkacağını da istisna olarak düzenleme altına almış ise, verilen rızanın hukuken bir değeri olacaktır. Kişisel verilerin yok edilmemesi suçu ile korunan hukuksal yarar her ne kadar kişisel verilerin korunması hakkı olsa da, 138. madde ile cezalandırılmakta olan verilerin silinmesi yükümlülüğünün kasten ihmal edilmiş olmasıdır. Dolayısıyla, veri sahibi olan ilgili kişinin kişisel verilerinin silinmemesine ilişkin vermiş olduğu rızanın, bu suçla cezalandırılmakta olan kanunla yükümlü kılınan bir görevin yerine getirilmemiş olması hukuka aykırı fiilini, hukuka uygun kılabilmesi bizce de kabul edilemez. Şüphesiz ki kamusal veya özel kişi ve kişilerce hukuka uygun olarak toplanmış olan verilerin, sonsuza kadar bu kişilerin elinde tutulmasının veya öngörülen sürede silinmemesinin yaptırıma bağlanmış olması ile özel hayatın gizliliği ve kişisel verilerin korunması hakkına yönelik önemli bir koruma sağlanmaktadır.

⁶⁷⁶ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 661.

⁶⁷⁷ HAFIZOĞULLARI, ÖZEN, *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar*, s. 292.

e. Suçun Özel Görünüş Biçimleri

i. Teşebbüs

Kişisel verileri yok etmeme suçu, kanunda belirlenen sürelerin geçmesine rağmen sistem içerisinde verileri yok etmekle görevli olan kişilerin bu görevlerini yerine getirmeyi ihmal etmeleri halinde cezalandırılmalarını öngören ihmali bir suçtur. İhmali hareketle işlenen suça teşebbüs olunamayacağından, doğası gereği bu suçun da teşebbüse elverişli olduğu söylenemeyecektir. Bunun yanı sıra verilerin yok edilmesi için öngörülmüş olan sürelerin geçmesiyle suç gerçekleşmiş olacağı ve suçun tamamlanması için kanunla öngörülen sürelerin geçmesinin ayrıca bir sonuç doğurması da aranmadığından, kişisel verileri yok etmeme suçunun neticesiz bir sırf hareket suçu olduğunu söyleyebiliriz. Buna göre suçun sırf hareket veya diğer bir kabulle neticesi harekete bitişik bir suç olması⁶⁷⁸ itibarıyla da kural olarak teşebbüse elverişli olmadığını ancak icra hareketleri kısımlara ayrılabilirdiği takdirde teşebbüs aşamasında kalabilmesinin söz konusu olabileceği doktrinde kabul edilmektedir.⁶⁷⁹ Kanaatimiz de bu suçu oluşturan silme yükümlülüğünün yerine getirilmemesi şeklindeki ihmali hareketin, teşebbüs aşamasında kalmasının mümkün olamayacağı istikametindedir.

ii. İştirak

Kişisel verilerin yok edilmemesi suçuna iştirak bahsinde özellik arz eden durum; suçun faili bakımından özgü suç niteliğinde olmasıdır. Failinin ancak belli özellikler taşıyabilen kişiler olabileceği kabul edilen suç tipi özgü suç olarak tanımlanmaktadır. Bu özellikler; cinsiyet gibi doğal veya failin mesleği gibi hukuki nitelikler şeklinde iki kategori altında sınıflandırılabilirler.⁶⁸⁰ Kişisel verileri yok etmeme suçunun da faili, ancak kanunen belirlenen süreler içerisinde verileri yok etme yükümlülüğü altında olan kişiler olabilir. TCK'nın 40. maddesinin ikinci fıkrasında, özgü suçların işlenişine iştirak eden diğer kişilerin ancak azmettiren veya yardım eden olarak sorumlu tutulabileceği, failin ise sadece özel faillik niteliğini taşıyan kişi

⁶⁷⁸ SOYASLAN, *Ceza Hukuku Özel Hükümler*, s. 359.

⁶⁷⁹ GÜLTAŞ, *Özel Hayata Karşı Suçlar*, s. 264.; ÖZBEK, DOĞAN, *Türk Ceza Hukuku Özel Hükümler*, s. 590.

⁶⁸⁰ DEMİRBAŞ, *Ceza Hukuku Genel Hükümler*, s. 489.

olabileceği düzenlenmiştir. Dolayısıyla, kanunen kişisel verileri yok etmekle yükümlü tutulmuş kişilerin, kasten gerçekleştirmiş oldukları öngörülen süreler içerisinde verileri yok etmeme ihmali hareketlerinin icrasına katılan diğer kişiler ancak yardım etme veya azmettirme şeklinde suça iştirakten sorumlu tutulabileceklerdir. Örneğin; kanunen kişisel verileri yok etmekle görevlendirilmiş olan bir personelin, böyle bir yükümlülüğü bulunmayan amirinin yönlendirmesi veya birlikte verdikleri karar kapsamında kanunda öngörülen süreler geçmesine rağmen verileri yok etmeyi ihmal etmesi halinde amirin, icra hareketleri üzerindeki etkisi araştırılmaksızın, bu olay bakımından azmettiren veya yardım eden olarak sorumlu tutulması gerekecektir. Bunun dışında doktrinde, suçun ihmali hareketle işlenen bir suç olması dolayısıyla, suçun nasıl işleneceği konusunda yol göstermek veya fiilin işlenmesine ilişkin yardımda bulunarak icrasını kolaylaştırmak şeklinde, bu suça yardım eden olarak iştirakin suçun doğası gereği çok mümkün olamayacağı kanaati de ileri sürülmektedir.⁶⁸¹

iii. İçtima

Bir kişinin, birden fazla suç işlemiş olması halinde sorumluluğunun ne şekilde belirleneceğine karar verilmesinde, sayıca fazla olan bu suçların içtimaı gündeme gelmektedir.⁶⁸² Kişisel verileri yok etmeme suçunun birden fazla kez işlenmiş olması veya bu suçu oluşturan hareketin başka bir suça da vücut vermesi hallerinde suçlar arasında bir içtima ilişkisi kurulması gerekecektir. Kişisel verileri yok etmeme suçunun, aynı kişiye karşı birden fazla kez veya tek fiile birden fazla kişiye karşı zincirleme suç şeklinde işlenebilirliği karşısında kural olarak bir engel bulunmuyorsa da kanaatimiz; bu suçun aynı mağdura karşı, tek suç işleme kararının icrası kapsamında birden fazla kez işlenmesi şeklinde zincirleme olarak işlenmesinin uygulamada çok karşılaşılabılır olmadığı istikametindedir. Zira, tek suç işleme kararının icrası kapsamında aynı kişiye ait kişisel verilerin, kanunen öngörülmüş sürelerde yok edilmesinin değişik zamanlarda ihmal edilebilmesi, bu suçun ayrıca mütemadi suç niteliğinde olabileceği de düşünüldüğünde, çok ihtimal dahilinde değildir. Ancak tek fiille aynı suçun birden fazla kişiye karşı işlenebilmesi bu suç bakımından oldukça karşılaşılabılır bir ihlal şeklidir. Örneğin; çok failli bir suçun

⁶⁸¹ DÜLGER, *Bilişim Suçları ve İnternet İletişim Hukuku*, s. 662.

⁶⁸² İÇEL, *Ceza Hukuku Genel Hükümler*, s. 571.

soruşturulması kapsamında suç şüphelileri hakkında Cumhuriyet savcısı tarafından telekomünikasyon yoluyla yapılan iletişiminin denetlenmesi koruma tedbirinin uygulanması kararı alınmış ve bu karar kapsamında birden fazla şüphelinin konuşmalarının dinlenmiş ve kayda alınmış olan bir olayda, Cumhuriyet savcısı tarafından verilen bu kararın CMK'nın 135. maddesine göre derhal hakimın onayına sunulması ve 24 saat içerisinde hakim tarafından onaylanması gerekmektedir. Buna karşılık 24 saatlik sürenin dolması veya hakimın tedbirin uygulanmasını onaylamaması halinde, CMK'nın 137. maddesine göre tedbir kararının derhal kaldırılması ve bu zamana kadar yapılmış olan dinleme kayıtlarının en geç on gün içinde yok edilmesi gerekmektedir. CMK'nın 137. maddesinde öngörülen bu sürede kayıtların yok edilmemiş olması halinde, tek bir ihmali hareketle birden fazla şüpheliye ait kişisel verilerin yok edilmemesi suçu işlenmiş olacaktır. Bu durumda yok etme yükümlülüğünü ihmal eden failin, tek fiille birden fazla kişiye karşı aynı suçu işlemesi sebebiyle zincirleme suç hükümlerine göre, tek bir kişisel verilerin yok edilmemesi suçuna ilişkin ancak belli nispette artırılarak, cezalandırılması gerekecektir (TCK md. 43).

TCK'nın 257. maddesinde düzenlenmiş olan kamu görevlisinin görevini kötüye kullanması suçu ve TCK'nın 138. maddesinde düzenlenmiş kişisel verileri yok etmeme suçu arasındaki içtima ilişkisi de bu aşamada üzerinde durulması gereken bir konudur. Bir kamu görevlisinin, kişisel verileri yok etme yükümlülüğünü ihmal etme şeklinde TCK'nın 138. maddesini ihlal eden hareketinin aynı zamanda bu kamu görevlisinin görevini kötüye kullanması suçunu oluşturacağı da şüphesizdir. Ancak TCK'nın 257. maddesinin lafzında “kanunda ayrıca suç olarak tanımlanan haller dışında” genel norm olarak bu maddenin uygulanacağı özellikle vurgulanmıştır. Bu halde kanunda öngörülen verileri yok etme yükümlülüğünü ihmal eden kamu görevlisi, ihmali tek hareketiyle hem kişisel verileri yok etmeme hem de görevi kötüye kullanma suçunu işlenmiş olacaktır. TCK'nın 138. maddesinin kişisel verileri yok etme yükümlülüğünün ihlalini suç olarak düzenlemiş olması itibarıyla bu halde failin, özel norm olarak sadece TCK'nın 138. maddesinden cezalandırılması gerekmektedir. Bunun yanı sıra hukuka uygun olarak kaydedilmiş kişisel verileri kanunda öngörülen süreler içerisinde yok etmeyen failin, aynı zamanda bu kişisel verileri başkalarına vermesi veya yayması halinde hem TCK'nın 138. maddesinden hem de 136. madde ile düzenlenmiş olan kişisel verileri hukuka aykırı olarak verme, yayma veya ele

geçirme suçundan gerçek içtima hükümlerine göre ayrı ayrı sorumlu tutulması gerekecektir.

f. Nitelikli Haller

21.02.2014 tarihinde TCK'nın 138. maddesine ek ikinci fıkra olarak, 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 5. maddesiyle; "suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır." şeklindeki hüküm eklenmiştir. Bu düzenlemenin niteliğinin; suçun temel şekline oranla verilecek olan cezanın artırılmasını gerektirecek, suçun konusu itibarıyla özellik arz eden nitelikli bir hal olduğunu söyleyebiliriz. Bu halin gerçekleşebilmesi için; Ceza Muhakemesi Kanunu'nun ilgili maddelerinin gereğince hukuka uygun olarak kaydedilmiş olan kişisel verilerin, yine CMK'da öngörülen sürelerde yok edilme yükümlülüğüne aykırı olarak sistemde tutulmaya devam edilmesi gerekmektedir. Türk Ceza Muhakemesi Kanunu'nun kişisel verileri konu edinen düzenlemeleri çalışmamızın önceki kısımlarında incelenmiş olup, bu hallere ilişkin ayrıntılı olarak açıklamalarda ilgili başlık altında yer verilmiştir. Bunun yanı sıra, CMK'nın 80. maddesinin ikinci fıkrasında genetik inceleme sonuçları hakkında; 81. maddesinin ikinci fıkrasında fiziki kimliğin tespiti amacıyla kayıt altına alınan kişisel veriler hakkında; 137. maddesinin üçüncü fıkrasında telekomünikasyon yoluyla yapılan iletişimin tespiti veya dinlemeye ilişkin kayıtlar hakkında; 139. maddesinin altıncı fıkrasında gizli soruşturmacı görevlendirilmesi suretiyle elde edilen kişisel bilgiler hakkında ve 140. maddesinin dördüncü fıkrasında teknik araçla izleme neticesinde elde edilmiş olan deliller hakkında CMK'nın ilgili maddelerinde öngörülmüş olan belli sürelerin geçmesi veya belli koşulların gerçekleşmesi halinde bu verilerin yok edilmesine ilişkin yükümlülüklerle aykırı davranılması faile, TCK'nın 138. maddesinin temel şekline göre daha ağır ceza verilmesini gerektirmektedir.

g. Yaptırım

Kişisel verileri yok etmeme suçuna ilişkin olarak TCK'nın 138. maddesinde öngörülen temel yaptırım; bir yıldan iki yıla kadar hapis cezası iken, suçun ikinci

fıkradaki nitelikli halinin gerçekleşmiş olması halinde faile verilecek olan ceza, bir kat artırılarak takdir edilebilmektedir. Kişisel verilere karşı işlenen diğer suç tiplerinde olduğu gibi bu suçun da, soruşturulması ve kovuşturulması re'sen yapılmaktadır. Bu suçu işleyen fail hakkında, iki yıl veya daha az süreli hapis cezasına hükmedilmiş ve hükmün açıklanmasının geri bırakılmasına ilişkin diğer koşulların da sağlanmış olması halinde hükmün açıklanmasının geri bırakılmasına karar verilmesi mümkündür. Kişisel verileri yok etmeme ihmali hareketini gerçekleştirmiş olan failin, gerek temel şekli gerekse nitelikli şekli bakımından bu suçtan dolayı dava edilebileceği süre ise temadının sona erdiği andan itibaren 8 yıllık dava zamanaşımı süresi ile sınırlıdır.⁶⁸³

⁶⁸³ **ARTUK**, Mehmet Emin, **GÖKCEN**, Ahmet, **YENİDÜNYA**, Caner, *Ceza Hukuku Genel Hükümler*, 10. Baskı, Ankara, Adalet Yayınevi, 2016, s. 1007.

SONUÇ

Kişinin görüntüsü, sesi, sağlık durumu, eğitimi, ekonomik durumu, adli veya idari siciline işlenmiş bilgileri gibi her zaman herkesle paylaşmak istemeyebileceği, diğer insanlardan ayırt edilmesini sağlayacak ve kendisiyle ilişkili olan her türlü bilgisi, kişisel veri olarak kabul edilmektedir. Toplumsal bir ortamda yaşayan bireyler, özellikle modern teknoloji karşısında, mahremiyet ve özel yaşam alanına dahil olan bu verileri tek başına korumakta oldukça zorlanmaktadır. Bu durum devlete, vatandaşların özel yaşamının, aile yaşamının ve kişisel verilerinin korunmasına ilişkin pozitif ve negatif bazı yükümlülükler yüklemektedir. Kişisel verilerin korunmasının anayasal bir kişilik hakkı olarak düzenlenmesi ve bu hakkın korunmasına ilişkin temel esas ve usullerin bir mevzuatla düzenlenmesi, devletin yükümlülükleri arasındadır. Kişisel verilerin korunmasına dair bu temel esas ve usullere aykırılıklar ve verilerin hukuka aykırı olarak işlenmesi karşısında ise kişiler, hukuki ve/veya cezai sorumluluk altında kalacaktır. Bu doğrultuda bu çalışmanın temel amacını, ülkemizde kişisel verilere ceza hukuku yoluyla yeterli bir koruma sağlanabilip sağlanamadığının tespit edilmesi oluşturmaktadır. 2016 yılı, özellikle 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlük kazanmasıyla, ülkemizde kişisel verilerin korunması hukukuna bir dönüm noktası yaşatmışken, kişisel verilere karşı işlenen suçlar 5237 sayılı TCK'nın yürürlük kazandığı 1 Haziran 2005 tarihinden beri cezai yaptırım altındadır. Ancak kişisel verilerin korunmasının temel kavramları, ilkeleri, usul ve esaslarını düzenleme altına alan bir düzenleme bulunmayışı kişisel verilere karşı işlenen suçlara ilişkin olarak hem doktrin hem de uygulamada farklı değerlendirme ve içtihatlarla sebep olmuştur. Bu çalışmada özellikle 6698 sayılı Kanun ve bu Kanun'u takiben iç hukukumuzda dahil olunan 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında/Karşısında Gerçek Kişilerin Korunmasına İlişkin Sözleşme hükümleri ekseninde, kişisel verilerin cezai yaptırımlarla korunmasında bilinmesi gereken temel kavramlara açıklık ve güncellik kazandırılmaya çalışılmıştır. Bunun yanı sıra ulusal düzenlemelerimizin eksik kaldığı noktalarda özellikle 2016/679 sayılı Avrupa Birliği Veri Koruma Regülasyonu ve uluslararası düzenlemelere de başvurulmuş kaynaklardandır.

TCK'nın dokuzuncu bölümünün 135. ve 138. maddeleri arasında düzenleme altına alınmış olan kişisel verilere karşı işlenen suçların, hukuki konusu, mağduru ve hukuka uygunluk sebepleri gibi unsurları içtihat farklılığı yaratan temel konulardandır.

Bu sebeplerle yüksek mahkeme kararları da kişisel verilerin korunmasına ilişkin TCK'da düzenlenmiş olan suçlara ilişkin belirli bir istikamet kazanamamıştır. Özellikle kişisel veri kavramının sınırlarının tam ve doğru bir şekilde tespit edilebilmesi bu noktada önemli ihtilaflı hususlardandır. Bu ihtilafların çözümü noktasında, kanaat gösterdiğimiz doğrultuda, ilk etapta 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndaki uluslararası düzenlemelerle örtüşen kişisel veri tanımlamasının ve 6698 sayılı Kanun'un 19. maddesi doğrultusunda kurulmuş Kişisel Verileri Koruma Kurulu tarafından çıkartılan yönetmelik ve rehberlere başvurulması yerinde olacaktır. Uluslararası mahkemelerin içtihatları da bu doğrultuda uygulama için yol gösterici nitelikte enstrümanlar arasındadır. Böylelikle Türk Ceza Kanunu'nun kişisel verilerin korunması amacına hizmet eden ilgili hükümlerinin kanunilik ilkesine aykırı olduğu istikametindeki eleştiriler de bu açıklamalar ekseninde çürütülmüş olacaktır.

TCK'nın 135. maddesinin ikinci fıkrasının 24/3/2016 tarihli ve 6698 sayılı Kanunun 30. maddesiyle değiştirilmiş şekli de hassas verilerin kaydedilmesi karşısında kişilere, kişisel verilerin kaydedilmesine göre daha ağır bir cezai yaptırım getirmiş olması itibarıyla önemli ve olumlu bir değişiklik olmuştur. Ancak maddenin lafzında kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin hassas verilerinin “hukuka aykırı olarak” kaydedilmesine tipiklikte özellikle yer verilmiş olması uygulamada halen belirsizlik yaratmaktadır. Bu doğrultuda maddenin düzenleniş amacına uygun olarak hükmün yeniden düzenlemeye muhtaç kısımları halen mevcuttur. Zira maddenin hassas veri kategorisi içerisinde saymış olduğu veri grupları da 6698 sayılı Kanun ile tam olarak örtüşmemektedir. Bu durum, temel amacı; hassas veya özel nitelikli verilerinin hukuka aykırı olarak işlenmesi karşısında kişilerin yaşayacak oldukları daha ağır mağduriyetin etkin şekilde önlenmesi ve caydırılması olan bu hükmün, bu amaca aykırı olarak 6698 sayılı Kanun ile çelişmesine sebep olmaktadır.

Kişisel verilere karşı işlenen suçlara ilişkin TCK düzenlemelerinin ortak olarak eleştirilen kısmı ise; kaydetme, hukuka aykırı olarak verme, yayma, ele geçirme ve yok etmeme gibi ceza kanunumuzun suç olarak düzenlediği fiiller yerine, bu eylemlerden daha geniş bir eylem olan kişisel verilerin “hukuka aykırı işlenmesinin” yaptırım altına alınmamış olmasıdır. TCK'nın ilgili maddelerinin düzenlenmiş olduğu zaman dilimi itibarıyla, hukuka uygun veri işlemenin temel ilke ve esaslarının

düzenlendiği bir mevzuatın bulunmayışı kanun koyucuyu bu istikamette bir düzenleme yapmaya itmişse de günümüz de kişisel verilerin her türlü hukuka aykırı işleme sayılacak eylem karşısında korunması önemli bir ihtiyaçtır. Bu istikamette hem kişisel verilerin hem de hassas verilerin hukuka aykırı olarak işlenmesinin TCK'da suç olarak düzenlenmesinin daha yerinde olacağı şahsi kanaatimizdir. TCK'nın kişisel verilere karşı işlenen suçların kasten işlenebilen şeklinin yanı sıra uygulama da sıklıkla karşılaşılabılır olan taksirle işlenen şeklini de yaptırım altına alması gerekmektedir. Bunun yanı sıra kişisel verilerin, mukayeseli hukukta olduğu gibi belli bir menfaat sağlanmak için işlenmesi veya kişilerin zararına olarak işlenmesi hallerinin de daha ağır cezalandırılmayı gerektirecek nitelikli haller olarak düzenlenmesi yerinde olacaktır.

Bütün bu olumlu ve olumsuz değerlendirmelerimizin yanı sıra kişisel verilerin etkin şekilde korunması, birincil sırada kişilerde kişisel verilerinin korunması konusunda bir kültürün oluşmuş olmasına bağlıdır. Kişisel verilerimiz her ne kadar çoğu zaman biz farkında olmaksızın bilişim sistemleri vasıtasıyla ele geçirilmekte ve kaydedilmekteyse de teknoloji toplumunda yaşayan bireyler olarak her türlü bilişim aracının bize sunduğu veya karşılaştığımız kişisel verilerimizi paylaşmaya ilişkin talepler karşısında sorgulayıcı olmak zorundayız. Kişisel verilerin korunması, öncelikli olarak kişilerin verilerin ne şekilde hukuka uygun ne şekilde hukuka aykırı olarak işlenmiş olacağı bilincine sahip olmasına bağlıdır. Bu bilincin oluşmasında mahkemelerimizin vermiş olduğu doğru ve yol gösterici kararların da önemli etkisinin olacağı şüphesizdir. Ülkemizde Kişisel Verileri Koruma Kurumu da bu istikamette oldukça titiz çalışmalar yapmakta ve ülkemizde kişisel verilerin korunması alanında bir kültürün oluşmasına hizmet etmektedir. Mukayeseli hukukta ve uluslararası örgütlerin önderliğinde yapılan ve vatandaşların veri koruma bilincini artıran sosyal projelerin ülkemizde de yapılması ve yaygınlaştırılması, toplumda veri koruma kültürünün oluşması, kişisel verilere karşı gerçekleştirilen ihlallerin ve dolayısıyla da mahkemelerin iş yükünün azaltılması adına fayda sağlayacaktır.



KAYNAKÇA

AKDAĞ, Hale, “Türk Ceza Hukukunda Kişisel Verilerin Korunması İlkeleri”, Ankara Üniversitesi Hukuk Fakültesi, (Prof. Dr. Nevzat Toroslu’ya Armağan), C. 1, 2015, s. 27-48.

AKGÜL, Aydın, “Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı””, Türkiye Barolar Birliği Dergisi, S. 116, 2016, s. 11-38.

AKILLIOĞLU, Tekin, “İdari Usul ve Kişisel Verilerin Korunması”, www.idare.gen.tr/akkillioglu-idariusul.htm (30.01.2018)

AKINCI, Ayşe Nur, “Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi”, Çalışma Raporu, T.C. Kalkınma Bakanlığı Yayınları, 2017.

AKSOY, Hüseyin Can, *Kişisel Verilerin Korunması*, Ankara, Çakmak Yayınevi, 2010.

AKYÜREK, Güçlü, “Kişisel Veriler ve Özel Hayatın Gizliliği Hakkı”, Suç ve Ceza Dergisi, S. 3, 2011, s. 43-59.

ALACAKAPAN, Uğur, Suçun Unsurları, Ankara, Sevinç Matbaası, 1975.

ALTINIŞIK, Ulvi (Çev.), “Avrupa Birliği Adalet Divanı’nın C-518/07 Sayılı Veri Koruma Kurumlarının Bağımsızlığına İlişkin Kararı”, Küresel Bakış, S. 6, 2012.

ARSLAN, Çetin, “Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması”, Bahçeşehir Üniversitesi Hukuk Fakültesi Kazancı Hakemli Hukuk Dergisi, S. 79-80, 2011, s. 447-487.

ARTUK, Mehmet Emin, **GÖKCEN**, Ahmet, **YENİDÜNYA**, Caner, *Ceza Hukuku Genel Hükümler*, 8. Baskı, Ankara, Adalet Yayınevi, 2014.

ARTUK, Mehmet Emin, **GÖKCEN**, Ahmet, **YENİDÜNYA**, Caner, *Ceza Hukuku Genel Hükümler*, 10. Baskı, Ankara, Adalet Yayınevi, 2016.

ASLAN, M. Yasin, “Türk Hukukunda Tüzel Kişilerin Ceza Sorumluluğu”, Ankara Barosu Dergisi, C. 68, S. 2, 2010, s. 30-37.

ATAK, Songül, “Avrupa Konseyi’nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler”, *Türkiye Barolar Birliği Dergisi*, S.87, 2010, s. 90-120.

AYGÖZER, A. Çiğdem, *Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması*, (Yayınlanmamış Doktora Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2016.

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

BAŞALP, Nilgün, “Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri”, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, C. 21, S. 1, 2015, s. 77-105.

BAUMAN, Zygmunt, **LYON**, David, *Liquid Surveillance: A Conversation*, United Kingdom, Polity Press, 2013.

BÜK, Alaattin, *Elektronik Ortamda Saklanan Kişisel Verilerin Elde Edilmesi / Değiştirilmesi Suretiyle İşlenen Suçların Ceza Hukuku Açısından Değerlendirilmesi*, (Yayınlanmamış Doktora Tezi), T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara, 2015.

BYGRAVE, Lee A., “Data Protection Pursuant to the Right to Privacy in Human Rights Treaties”, *International Journal of Law and Information Technology*, C. 6, S. 3, 1998.

CENTEL, Nur, **ZAFER**, Hamide, *Ceza Muhakemesi Hukuku*, 12. Baskı, İstanbul, Beta Basım, 2015.

CENTEL, Nur, **ZAFER**, Hamide, **ÇAKMUT**, Özlem, *Kişilere Karşı İşlenen Suçlar*, 3. Baskı, İstanbul, Beta Basım, 2016.

ÇEKİN, Mesut Serdar, “6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi”, *İÜHFM*, C. 74, S. 2, 2016, s. 629-644.

DAĞ, Güray, *Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması*, (Yayınlanmamış Doktora Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2011.

DE HERT, Paul, **PAPAKONSTANTİNOU**, Vagelis, “The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals”, *Computer Law&Security Review*, C. 28, 2012, s. 130-142.

DEMİRBAŞ, Timur, *Ceza Hukuku Genel Hükümler*, 12. Baskı, Ankara, Seçkin Yayıncılık, 2017

DİKER VANBERG, Aysem, “The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?”, *Journal of Internet Law*, C.21, S. 7, 2018, s. 11.

DİNÇ, Engin, *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye’nin Durumu*, (Yayınlanmamış Yüksek Lisans Tezi), Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Diyarbakır, 2006, s. 68.

DÖNMEZER, Sulhi, **ERMAN**, Sahir, *Nazari ve Tatbiki Ceza Hukuku*, 14. Baskı, İstanbul, Der Yayınları, 2016.

DÜLGER, M. Volkan, *Bilişim Suçları ve İnternet İletişim Hukuku*, 5. Baskı, Ankara, Seçkin Yayınları, 2014.

ERDEM, Tahir, “Kişisel Verilerin Korunması Konusunda Son Gelişmeler”, *Vergi Sorunları Dergisi*, S. 332, 2016, s. 97-115. www.vergisorunlari.com.tr (14.03.2018).

EVANS, A., “European Data Protection Law”, *The American Journal of Comparative Law*, C. 29, S. 4, 1981, s. 571-582.

G. AKİPEK, Jale vd., *Türk Medeni Hukuku Başlangıç Hükümleri (Kişiler Hukuku)*, İstanbul, Beta Basım, 10. B., 2013.

GELLERT, Raphaël, **GUTWIRTH**, Serge, “The legal construction of privacy and data protection”, *Computer Law & Security Review*, C. 29, S. 5, 2013, s. 522-530.

GÖNEN, Serkan, **ULUS**, Halil İbrahim, **YILMAZ**, Ercan Nurcan, “Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme”, *Bilişim Teknolojileri Dergisi*, C. 9, S. 3, 2016, s. 0-229.

GÖZÜKÜÇÜK, Merve, *Veri İşleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirilmesi*, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2014.

GÜLTAŞ, Veysel, *Özel Hayata Karşı Suçlar*, 2. Baskı, Ankara, Bilge Yayınevi, 2017.

GÜLTEKİN, N. Melek, *Kişisel Verilerin Ceza Hukuku Yönünden Korunması*, (Yayımlanmamış Yüksek Lisans Tezi), Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2012.

HAFIZOĞULLARI, Zeki, **ÖZEN**, Muharrem, *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar*, 5. Baskı, Ankara, Usa Yayıncılık, 2016.

HAKERİ, Hakan, *Ceza Hukuku Genel Hükümler*, 14. Baskı, Ankara, Adalet Yayınevi, 2012.

HELVACIOĞLU, Asli Deniz, **STAKHEYEVA**, Hanna, “The Tale Of Two Data Protection Regimes: The Analysis Of The Recent Law Reform In Turkey In The Light Of EU Novelties”, *Computer Law&Security Rewiev*, C. 33, 2017, s. 811-824.

HENKOĞLU, Tülay, *Bilgi Güvenliği ve Kişisel Verilerin Korunması*, Ankara, Yetkin Yayınları, 2015.

İÇEL, Kayıhan, *Ceza Hukuku Genel Hükümler*, 4. Baskı, İstanbul, Beta Basım, 2017.

İMRE, Zahit, “Şahsiyet Haklarından Şahsın Özel Hayatının ve Gizliliklerinin Korunmasına İlişkin Meseleler”, *İÜHF Mecmuası*, C. 39, S. 1-4, 1974, s. 147-168.

İTİŞGEN, Rezzan, “Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu”, *Türkiye Adalet Akademisi Dergisi*, S. 23, 2015, s. 179-202.

K. DURMUŞ, Neslihan, “Ticari Sırların ve Kişisel Verilerin Korunması Kapsamında Vergi Mahremiyeti”, *Türkiye Adalet Akademisi Dergisi*, S.31, 2017, s. 371-409.

KANADOĞLU, Korkut, *Türkiye Barolar Birliği Özel Yaşamın Gizliliği Panel Konuşması*, 18.11.2008, Ankara.

KARABULUT, Ramazan, *Kişisel Verilerin Korunması ve Kolluk Hizmetleri*, (Yayımlanmamış Yüksek Lisans Tezi), Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Diyarbakır, 2014.

KARAKEHYA, Hakan, “Gözetim ve Suçla Mücadele”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, C. 58, S. 2, 2009, s. 319-357.

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

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

KESER BERBER, Leyla, **KAYA**, Mehmet Bedii, *Türkiye’de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, İstanbul, 2014.

KILINÇ, Doğan, “Anayasa Mahkemesinin Özel Hayatın Korunmasına İlişkin 2013/1614 Sayılı Kararı Üzerine Değerlendirmeler”, International Journal Of Legal Progress, C.1, S. 2, 2015, s. 177-204.

KİLKELLY, Ursula, *Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı (Avrupa İnsan Hakları Sözleşmesi’nin 8. Maddesinin Uygulanmasına İlişkin Klavuz)*, İnsan Hakları El Kitapları No. 1, Strasbourg, 2011.

KOCA, Mahmut, **ÜZÜLMEZ**, İlhan, *Türk Ceza Hukuku Genel Hükümler*, 3. Baskı, Ankara, Seçkin Yayıncılık, 2010.

KOCA, Mahmut, **ÜZÜLMEZ**, İlhan, *Türk Ceza Hukuku Özel Hükümler*, 3. Baskı, Ankara, Adalet Yayınevi, 2016.

KORKMAZ, İbrahim, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, Ankara, Seçkin Yayıncılık, 2017.

KUNTER, Nurullah, *Suçun Maddi Unsurları Nazariyesi*, İstanbul, İsmail Akgül Matbaası, 1954.

KÜZECİ, Elif, *Kişisel Verilerin Korunması*, (Yayımlanmamış Doktora Tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü Ankara, 2010.

KÜZECİ, Elif, “İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı”, İnsan Hakları Yıllığı, C. 32, 2014, s. 53-75.

LAÇİN, İrem, “Unutulma Hakkı”, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Doç. Dr. Melike Batur Yamaner’in Anısına Armağan, C. 1, 2014, s. 391-419.

LYNSKEY, Orla, *The Foundations of EU Data Protection Law*, United Kingdom, Oxford University Press, 2015.

MCCULLAGH, Karen, “Data sensitivity: proposals for resolving the conundrum”, *Journal of International Commercial Law and Technology* , C. II., S. 4, Manchester 2007, s. 190-201, <http://usir.salford.ac.uk/2745/> (11.12.2017)

MENDOS KUŞKONMAZ, Elif, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013.

OĞUZ, Habip, “Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları Ve Ülkemizdeki Durum”, *Uyuşmazlık Mahkemesi Dergisi*, S. 3, 2013, s. 1-38.

ÖZBEK, V. Özer, **DOĞAN**, Koray, **BACAKSIZ**, Pınar, **TEPE**, İlker, *Türk Ceza Hukuku Özel Hükümler*, 11.Baskı, Ankara, Seçkin Yayıncılık, 2017.

ÖZTÜRK, Bahri, *Uygulamalı Ceza Muhakemesi Hukuku*, Ankara, Ankara Üniversitesi Basımevi, 1991.

ÖZTÜRK, Bahri, *Ceza Muhakemesi Hukuku*, 11. Baskı, Ankara, Seçkin Yayınları, 2017.

PRADEL, Jean, *Çağdaş Sistemlerde Karşılaştırmalı Ceza Usulü*, Çev. Sulhi Dönmezer, Beta Basım, İstanbul, 2000.

PURTOVA, Nadezhda, “Private Law Solutions In European Data Protection: Relationship To Privacy, And Waiver Of Data Protection Rights”, *Netherlands Quarterly of Human Rights*, C. 28, S. 2, 2010, s. 179-198.

SEYREK TÜTÜNCÜBAŞI, Deniz, *Kişilerin Kendisine Ait Verilerin Kaderini Tayin Hakkının Ceza Hukuku Yoluyla Korunması*, (Yayınlanmamış Yüksek Lisans Tezi), Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir, 2015.

SIMITIS, Spiros, “Revisiting Sensitive Data”, *Review Of The Answers To The Questionnaire Of The Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data*, Strasbourg, 1999.

SOYASLAN, Doğan, *Ceza Hukuku Özel Hükümler*, 11. Baskı, Ankara, Yetkin Yayınları,

2016.

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

ŞEN, Ersan, “Ne Bis In Idem Prensibi”, <http://t24.com.tr/yazarlar/ersan-sen/ne-bis-in-idem-prensibi,7328> (10.06.2018)

ŞENER, Gülnihal, “Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu”, *Adalet Dergisi*, S. 39, 2011, s. 72-86.

ŞİMŞEK, Oğuz, *Anayasa Hukukunda Kişisel Verilerin Korunması*, İstanbul, Beta Basım, 2008.

TEKİN, Nurullah, “Kişisel Verilerin Korunması İle İlgili Türkiye’deki Kanun Tasarısının

Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi”, *Uyuşmazlık Mahkemesi Dergisi*, S. 4, 2014, s. 222-262.

TEZCAN, Durmuş, “Bilgisayar Karşısında Özel Hayatın Korunması”, *Anayasa Yargısı Dergisi*, C. XIII, Ankara, 1991, s. 385-392.

TEZCAN, Durmuş, “Özel Hayatın Gizliliğini İhlal ve Kişisel Verilerin Kaydedilmesi Suçu İle İlgili Bazı Gözlemler”, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, C. 71, S. 1, 2013, s. 1159-1164.

TİEDEMAN, Klaus,(çev. Feridun Yenisey), “Bilgisayarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi”, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, C. 41, S. 1-2, 1975, s. 319-332.

TOPAL, Cansu, *İnternet ve Hukuk Sempozyumu*, İstanbul, 2018.

UYAR, Lema, *Birleşmiş Milletler’de İnsan Hakları Yorumları İnsan Hakları Komitesi ve Ekonomik, Sosyal ve Kültürel Haklar Komitesi, 1981-2006, İnsan Hakları Hukuku Çalışmaları*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2006.

ÜNSAL, Çağrı Zeybek, “Google’ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu Ve Avrupa Birliği’nin 95/46/Ec Sayılı Veri Koruma Direktifi

Açısından Değerlendirilmesi”, Hacettepe Üniversitesi Hukuk Fakültesi Dergisi, C. 3, S. 1, 2013, s. 99-124.

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

VOIGT, Paul, *The EU General Data Protection Regulation (GDPR) A Practical Guide*, Springer International Publishing A.G., İsviçre, 2017.

YENİSEY, Feridun, **NUHOĞLU**, Ayşe, *Ceza Muhakemesi Hukuku*, İstanbul, Bahçeşehir Üniversitesi Yayınları, 2014.

YILMAZ, Sabire Sanem, *Tıp Alanında Kişisel Verilerin Hukuka Aykırı Olarak Verilmesinin Ceza Hukuku Açısından Değerlendirilmesi (Sır Saklama Yükümlülüğü Kapsamında)*, (Yayımlanmamış Yüksek Lisans Tezi), Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2014, s. 82.

YOKUŞ SEVÜK, Handan, “Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması”, V. Türk - Alman Tıp Hukuku Sempozyumu, Türkiye Barolar Birliği Yayınları, 2008, Ankara.

ZAFER, Hamide, *Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması*, İstanbul, Beta Basım, 2010.