

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

İDARE HUKUKU BAĞLAMINDA KİŞİSEL VERİLERİN
KORUNMASI

Batuhan KÖSEMAN

Danışman
Doç. Dr. Lale Burcu ÖNÜT

İZMİR- 2023

TEZ ONAY SAYFASI



YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum “İdare Hukuku Bağlamında Kişisel Verilerin Korunması” adlı çalışmamın, tarafımdan, akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

.../.../2023

Batuhan KÖSEMAN



ÖZET
Yüksek Lisans Tezi
İdare Hukuku Bağlamında Kişisel Verilerin Korunması
Batuhan KÖSEMAN

Dokuz Eylül Üniversitesi
Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı
Kamu Hukuku Programı

Kişisel veriler tarihin birçok döneminde gerek özel sektör gerekse kamu kurum ve kuruluşları nezdinde çok önemli olmuştur. Özellikle teknolojide yaşanan gelişmeler kişisel verilerin elde edilmesi, depolanması, aktarılması gibi işleme süreçlerini kolaylaştırmıştır. Günümüzde kişisel veriler çeşitli amaçlarla ve sıklıkla işlenmektedir. Veri işleme faaliyetlerindeki artış, veri işleme etkinliklerinin kolaylaşması ve çeşitlenmesi, o verilerin ilişkili olduğu kişilerin temel hak ve özgürlüklerinin ihlal edilmesi tehlikesini de beraberinde getirmektedir. Nitekim kişisel verilerin korunmasında amaç, verinin korunmasından ziyade ilişkili olduğu kişilerin, başka bir ifadeyle kişisel verileri işlenen kişilerin temel hak ve özgürlüklerini korumaktır. Bu doğrultuda uluslararası alanda ve ulusal alanda kişisel verilerin korunması bakımından çok sayıda düzenleme gerçekleştirilmiştir. Ülkemiz özelinde de gerek Anayasamızın 20. maddesinin üçüncü fıkrası gerekse bu konuda özel ve kapsamlı ilk yasal düzenleme olan 6698 sayılı Kişisel Verilerin Korunması Kanunu, kişisel verilerin korunması alanındaki gelişmelerin mevzuatımıza doğrudan yansımalarını oluşturmaktadır. Çalışmamızda öncelikle, kişisel veri kavramına, bu kavramın tarihsel gelişimine, bu alandaki ulusal ve uluslararası düzenlemelere, kişisel verilerin korunması hakkının niteliğine, 6698 sayılı Kanun bakımından kişisel verilerin işleme süreci ve hukuki denetim sistemine değinilmiştir. Ardından konunun idare hukuku ve idari faaliyetler kapsamında işlenen kişisel verilere ilişkin yönüne dikkat çekilmek istenmiş ve idarenin birtakım faaliyet örnekleri

çerçevesinde kişisel verilerin korunması hakkında açıklamalarda bulunulmuştur.

Anahtar Kelimeler: Kişisel Veri, Kişisel Verilerin Korunması, Kişisel Verilerin İşlenmesi, Kişisel Verileri Koruma Kurumu, İdarenin Faaliyetleri.



ABSTRACT
Master's Thesis
Protection of Personal Data In The Context of Administrative Law
Batuhan KÖSEMAN

Dokuz Eylul University
Graduate School of Social Sciences
Department of Public Law
Public Law Programme

Personal data has been of great importance in many periods of history, both in the private sector and in government institutions and organizations. Especially, developments in technology have facilitated the processes of obtaining, storing, and transferring personal data. Nowadays, personal data is frequently processed for various purposes. The increase in data processing activities, and the ease and diversification of data processing activities, also bring the risk of violating the fundamental rights and freedoms of the individuals to whom the data is related. Indeed, the protection of personal data aims to safeguard the fundamental rights and freedoms of individuals whose personal data is processed, rather than just protecting the data itself. In this context, numerous regulations have been enacted internationally and nationally for the protection of personal data. In our country, the third paragraph of Article 20 of our Constitution and the Personal Data Protection Law No: 6698, which is the first special and comprehensive legal regulation on this matter, directly reflect the developments in the field of personal data protection in our legislation. In our study, firstly, the concept of personal data, its historical development, international regulations in this field, the nature of the right to personal data protection, the process of processing personal data under Law No. 6698, and the legal control system are discussed. Then, attention is drawn to the aspect of personal data processed within the scope of administrative law and administrative activities, and explanations are made regarding the protection of personal data through some examples of administrative activities.

Keywords: Personal Data, Protection of Personal Data, Processing of Personal Data, Personal Data Protection Authority, Activities of the Administration.



İDARE HUKUKU BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI

İÇİNDEKİLER

TEZ ONAY SAYFASI	ii
YEMİN METNİ	iii
ÖZET	iv
ABSTRACT	vi
İÇİNDEKİLER	viii
KISALTMALAR	xii

GİRİŞ	1
-------	---

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI, KİŞİSEL VERİLERİN KORUNMASI HAKKI, KİŞİSEL VERİLERİN KORUNMASINDA TEMEL AMAÇ VE TARİHSEL GELİŞİM

I. KİŞİSEL VERİ KAVRAMI VE UNSURLARI	2
A. Tanım	2
B. Kişisel Verinin Unsurları	5
1. Bir Veri Bulunması	5
2. Gerçek Kişiyeye Ait Veri	6
3. Kimliği Belirli veya Belirlenebilir Kişi	7
a. Kişi Kavramı	7
b. Kimliği Belirli veya Belirlenebilir Olmak	10
C. Özel Nitelikteki Kişisel Veriler	12
II. KİŞİSEL VERİLERİN KORUNMASI HAKKI VE HAKKIN NİTELİĞİNE İLİŞKİN YAKLAŞIMLAR	13
A. Bir Hak Olarak Kişisel Verilerin Korunması	13
B. Kişisel Verilerin Korunması Hakkının Niteliğine İlişkin Yaklaşımlar	14
1. Ekonomik Yaklaşım	14
a. Mülkiyet Hakkı Teorisi	15

b. Fikri Mülkiyet Hakkı Teorisi	16
c. Diğer Teoriler	17
d. Ekonomik Yaklaşım İlişkin Değerlendirmemiz	17
2. Sosyal-Hümanist Yaklaşım	18
3. Görüşlere İlişkin Değerlendirmemiz	20
III. KİŞİSEL VERİLERİN KORUNMASINDA TEMEL AMAÇ VE KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ	22
A. Kişisel Verilerin Korunmasında Temel Amaç	22
B. Tarihsel Gelişim Sürecinde Kişisel Verilerin Korunmasına İlişkin Temel Düzenlemeler	24
1. Genel Olarak	24
2. Uluslararası Düzenlemeler	31
a. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Düzenlemeleri	31
b. Birleşmiş Milletler Düzenlemeleri	32
c. Avrupa Konseyi Düzenlemeleri	35
(1) Genel Olarak	35
(2) Avrupa İnsan Hakları Sözleşmesi	36
(3) 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi	39
d. Avrupa Birliği'nde Kişisel Verilerin Korunması	43
(1) Genel Olarak	43
(2) Veri Koruma Direktifi	45
(3) Genel Veri Koruma Tüzüğü	51
3. Türkiye'de Kişisel Verilerin Korunmasına İlişkin Temel Düzenlemeler	61
a. Genel Olarak	61
b. Anayasamız	63
c. Kanunlar	64
(1) 6698 Sayılı Kişisel Verilerin Korunması Kanunu	64
(i) Genel Olarak	64

(ii) 6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı	65
(iii) 6698 sayılı Kişisel Verilerin Korunması Kanununun Kapsamı	66
(2) Diğer Kanunlar	69

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN İŞLENMESİ, DENETİM SİSTEMİ VE KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN İDARENİN UYGULAMA ÖRNEKLERİ

I. KİŞİSEL VERİLERİN İŞLENMESİ	70
A. Genel Olarak	70
1. Veri İşleme Faaliyeti	71
2. Veri Kayıt Sistemi	72
3. Veri Sorumlusu, Veri İşleyen ve İlgili Kişi	72
a. Veri Sorumlusu	72
b. Veri İşleyen	73
c. İlgili Kişi	75
B. Kişisel Verilerin İşlenmesi Sürecine Hâkim Olan Genel İlkeler	75
1. Hukuka ve Dürüstlük Kurallarına Uygun Olma İlkesi	76
2. Doğru ve Gerekliğinde Güncel Olma İlkesi	77
3. Belirli, Açık ve Meşru Amaçlar İçin İşlenme İlkesi	78
4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma İlkesi	79
5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme İlkesi	81
C. Kişisel Verilerin İşlenme Şartları	83
1. Genel Olarak	83
2. Özel Nitelikli Olmayan Kişisel Verilerin İşlenme Şartları (m.5)	84
a. İlgili Kişinin Açık Rızası (m.5/1)	84
b. İlgili Kişinin Açık Rızası Aranmadan Kişisel Verilerin İşlenebileceği Haller	87

(1) Kanunlarda Açıkça Öngörülmesi (m.5/2-a)	87
(2) Kişinin Kendisinin veya Bir Başkasının Hayatı veya Beden Bütünlüğünün Korunması İçin Zorunlu Olması (m.5/2-b)	89
(3) Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesinin Gerekli Olması (m.5/2-c)	90
(4) Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması (m.5/2-ç)	91
(5) İlgili Kişi Tarafından Alenileştirilmiş Olması (m.5/2-d)	92
(6) Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Veri İşlemenin Zorunlu Olması (m.5/2-e)	94
(7) Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması (m.5/2-f)	95
3. Özel Nitelikli Kişisel Verilerin İşlenme Şartları (m.6)	97
D. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi	104
1. Genel Olarak	104
2. Kişisel Verilerin İmhası	106
E. Kişisel Verilerin Aktarılması	113
1. Genel Olarak	113
2. Yurt İçinde Aktarım	113
3. Yurt Dışına Aktarım	116
II. İLGİLİ KİŞİNİN HAKLARI VE VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ	119
A. İlgili Kişinin Hakları	119
B. Veri Sorumlusunun Yükümlülükleri	123
1. Genel Olarak	123
2. Veri Sorumlusunun Aydınlatma Yükümlülüğü	124
3. Veri Güvenliğine İlişkin Yükümlülükler	131
4. Veri Sorumluları Sicili'ne (VERBİS'e) Kayıt Yükümlülüğü	135
5. Diğer Yükümlülükler	138

III. DENETİM SİSTEMİ	138
A. Genel Olarak	138
B. Yargı Dışı Denetim	139
1. Genel Olarak	139
2. Veri Sorumlusuna Başvuru	139
3. Kişisel Verileri Koruma Kurumu Tarafından Gerçekleştirilen Denetim	142
a. Kişisel Verileri Koruma Kurumu	142
b. Kişisel Verileri Koruma Kurulu	144
(1) Kişisel Verileri Koruma Kurulu'na Şikâyet	145
(2) Kişisel Verileri Koruma Kurulunun İdari Yaptırım Yetkisi	149
C. Yargısal Denetim	150
1. Genel Olarak	150
2. Adli Yargı Denetimi	151
a. Özel Hukuk Hükümleri Çerçevesinde Kişisel Verilerin Korunması	151
b. Ceza Hukukunda Kişisel Verilerin Korunması	153
3. İdari Yargı Denetimi	157
a. Kurul Kararlarının Yargısal Denetimi	157
b. Kişisel Verilerin İşlenmesine İlişkin İdari Yargı Denetimi	160
IV. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN İDARENİN UYGULAMA ÖRNEKLERİ	163
A. Genel Olarak	163
B. Elektronik Devlet (E-Devlet) Hizmeti Bakımından	164
C. Sağlık Hizmetleri Bakımından	167
D. Kolluk Faaliyetleri Bakımından	170
E. Bilgi Edinme Hakkı Bakımından	173
SONUÇ	176
KAYNAKÇA	178

KISALTMALAR

AB	Avrupa Birliđi
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
bkz.	Bakınız
C.	Cilt
çev.	Çeviren
DNA	Deoksiriboz nükleik asit
E.	Esas Sayısı
İYUK	İdari Yargılama Usulü Kanunu
K.	Karar Sayısı
m.	madde
MHRS	Merkezi Hekim Randevu Sistemi
M.Ö.	Milattan Önce
No.	Numara
OECD	Ekonomik İşbirliđi ve Kalkınma Örgütü
R.G.	Resmi Gazete
S.	Sayı
s.	sayfa
ss.	sayfadan sayfaya
TBB	Türkiye Barolar Birliđi
T.C.	Türkiye Cumhuriyeti
TCK	Türk Ceza Kanunu
USB	Universal Serial Bus
vb.	ve benzeri

GİRİŞ

Kişisel veriler, tarih boyunca gerek özel sektör gerekse kamu kurum ve kuruluşları tarafından önemli görülmüştür. Zira kişisel verilere sahip olmak, çeşitli alanlarda bu verilere sahip olanlara büyük bir güç kaynağı sağlamıştır. Bilişim teknolojilerinde yaşanan gelişmelerle birlikte kişisel verilere erişimin, bunların depolanması ve aktarılmasının oldukça hızlanması ve kolaylaşması ise kişilerin temel hak ve özgürlüklerinin ihlale uğratılması tehdidini beraberinde getirmiştir. Bu sebeplerle kişisel verilerin korunmasının bağımsız bir temel hak olarak ele alınması ve etkin güvencelerle korunması zaruret teşkil etmektedir. Hem uluslararası hem de ulusal alanda kişisel verilerin etkin bir şekilde korunabilmesi amacıyla yoğun çalışmalar yürütülmekte ve çeşitli hukuki düzenlemeler hayata geçirilmektedir. Çalışmamızın birinci bölümünde, öncelikli olarak bir temel oluşturmak amacıyla, kişisel veri kavramının tanımı ve unsurları ele alınmıştır. Ardından kişisel verilerin korunması alanının tarihsel gelişimi konusuna giriş yapılmış, özellikle bu alana öncülük eden uluslararası hukuki düzenlemelere ve ulusal mevzuatımız açısından konuya etraflıca değinilmeye çalışılmıştır. Daha sonra birinci bölümün son konusu olan kişisel verilerin korunması hakkına yer verilmiş ve bu hakkın hukuki niteliğine ilişkin teoriler çerçevesinde birtakım değerlendirmelerde bulunulmuştur. Çalışmamızın ikinci bölümünde, kişisel verilerin korunmasına yönelik daha teknik ve detaylı açıklamalarda bulunulmaktadır. Özellikle bu alanın ülkemizdeki temel yasal düzenlemesi olan 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri çerçevesinde kişisel verilerin işlenmesi, ilgili kişinin hakları, veri sorumlusunun yükümlülükleri, denetim sistemi gibi önemli konularda açıklamalar yapılmıştır. Çalışmanın temel amacı kişisel verilerin korunmasının idare hukuku bağlamında ele alınması olduğundan, ikinci bölümde son olarak, idarenin bazı faaliyet örnekleri çerçevesinde kişisel verilerin korunması konusuna açıklamalar getirilmiş ve bu alandaki uygulamanın bilhassa kamu kurum ve kuruluşlarınca daha nitelikli hale getirilebilmesi amacıyla çeşitli değerlendirmelere yer verilmiştir.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI, KİŞİSEL VERİLERİN KORUNMASI HAKKI, KİŞİSEL VERİLERİN KORUNMASINDA TEMEL AMAÇ VE TARİHSEL GELİŞİM

I. KİŞİSEL VERİ KAVRAMI VE UNSURLARI

A. Tanım

“Veri” kavramının Türk Dil Kurumu sözlüğünde birden fazla tanımı bulunmaktadır. Bu tanımlardan bir tanesinde veri kavramı, “*Bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done*” şeklinde ifade edilmiştir. Bir diğer tanımlamada ise veri kavramı, “*bilgi, data*” olarak belirtilmiştir¹. Bu tanımlardan hareketle, basit bir mantıkla kişisel veri kavramı ile ifade edilmek istenenin, bir kişiye ilişkin her türlü bilgi olduğunu söylemekte herhangi bir sakınca bulunmayacaktır. Ancak gerek uluslararası gerekse ulusal düzenlemelerde kişisel veri, hukuki bir kavram niteliğinde, bünyesinde hangi unsurları ihtiva ettiği de rahatlıkla anlaşılabilir bir biçimde, daha detaylı ve kapsamlı olarak tanımlanmıştır.

24.03.2016’da kabul edilen ve 7.04.2016 tarihli Resmî Gazete’de yayımlanan, “6698 sayılı Kişisel Verilerin Korunması Kanunu” (Kanun) esaslı bir tanımlama yapmıştır. Ancak bu kanun yürürlüğe girmeden önce de mevzuatımızdaki bazı düzenlemelerde, kişisel veri kavramı hakkında tanımlara yer verilmiştir. Örneğin, 28.07.2010 tarih ve 27655 sayılı Resmî Gazete’de yayımlanan “*Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği’nin*” 4. maddesinin f fıkrasında kişisel veri “*belirli veya kimliği belirlenebilir gerçek veya tüzel şahıslara ilişkin bütün bilgiler*” şeklinde tanımlanmıştır. Yine, 24.07.2012 tarih ve 28363 sayılı Resmî Gazete’de yayımlanan “*Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik’in*” 3/h maddesinde kişisel veri, “*belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler*” olarak ifade edilmiştir. Söz konusu düzenlemelerde, tüzel kişilerin de veri öznesi olarak

¹ Türk Dil Kurumu Güncel Türkçe Sözlüğü, <https://sozluk.gov.tr/>, (20.03.2022).

değerlendirildiği dikkatlerden kaçmamaktadır². Kişisel verilerin korunması alanındaki temel yasal düzenlememiz olan ve 7 Nisan 2016 tarihinde yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 3. maddesinde ise kişisel veri, “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” şeklinde tanımlanmıştır³. Bu tanım, çeşitli uluslararası düzenlemelerde yer alan kişisel veri tanımlamalarıyla paralel niteliktedir. Örneğin, Ekonomik İşbirliği ve Kalkınma Örgütü’nün (OECD) 23 Eylül 1980 tarihinde yayımlamış olduğu “Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeler” isimli belgede kişisel veri, “*belirli veya belirlenebilir bir kişi ile ilişkilendirilebilecek her türlü bilgi*” olarak tanımlanmıştır⁴. Avrupa Konseyi tarafından yayımlanan, 28 Ocak 1981 tarihli ve “108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi’nde” kişisel veri kavramı, Ekonomik İşbirliği ve Kalkınma Örgütü’nün (OECD) yayımlamış olduğu “Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler” metnindeki tanımlama ile tamamen aynı şekilde ifade edilmiştir⁵. Kişisel veri, tarafı bulunduğumuz Avrupa İnsan Hakları Sözleşmesi’nde (AİHS) ise açık bir şekilde tanımlanmamıştır. Ancak AİHS’nin uygulanmasını denetleme görevini yürüten Avrupa İnsan Hakları Mahkemesi (AİHM), vermiş olduğu kararlarda kişisel verilerin korunması hususunu, Avrupa İnsan Hakları Sözleşmesi’nin 8. maddesinde düzenlenen “Özel ve aile hayatına saygı hakkı” çerçevesinde, özel yaşamın gizliliğinin bir parçası

² Cemal Başar, **Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması**, DEÜ Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilimdalı Kamu Hukuku Programı Yayımlanmış Doktora Tezi, 2019, www.tez.yok.gov.tr, (10.06.2022), s. 8.

³ Resmî Gazete, 07.04.2016, S. 29677, <https://www.resmigazete.gov.tr>, (21.03.2022).

⁴ Kaynak metin olan “Guidelines governing the protection of privacy and transborder flows of personal data” da kişisel veri kavramının tanımı İngilizcedir. Orijinal diliyle tanım, “Personal data” means any information relating to an identified or identifiable individual (data subject).” şeklindedir, bkz. <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>, (21.03.2022), s. 13.

⁵ “108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi’nin” İngilizce tam metni için bkz. <https://www.coe.int/en/web/data-protection/convention108andprotocol#:~:text=The%20Convention%20for%20the%20Protection,in%20the%20data%20protection%20field>, (21.03.2022), s. 1; Metnin Adalet Bakanlığı tarafından hazırlanmış Türkçe çevirisine ulaşmak için ise bkz. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjAi_Kg5v_5AhWjQfEDHUYUC5QQFnoECAQQAQ&url=https%3A%2F%2Finhak.adalet.gov.tr%2FResimler%2FDokuman%2F2712020140848108_tur.pdf&usg=AOvVaw2hjAruqXJ4TQzSKQiuqHqp, (21.03.2022).

olarak değerlendirmektedir⁶. Avrupa Birliği’nde kişisel verilerin korunmasına ilişkin olarak 25 Mayıs 2018 tarihinde “95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunması Hakkında Avrupa Parlamentosu ve Avrupa Konseyi Direktif’ini”⁷ (95/46/EC sayılı Direktif) ilga ederek yürürlüğe giren “Avrupa Parlamentosu ve Avrupa Konseyi’nin 2016/679 sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımı Konusunda Bireylerin Korunması Hakkında Tüzüğü” (2016/679 sayılı Genel Veri Koruma Tüzüğü), kişisel veri kavramını “kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi” olarak ifade etmiştir⁸.

İç hukukumuzda yargı kararlarında, kişisel veri kavramının tanımına ve hangi verilerin kişisel veri olarak değerlendirilebileceğine ilişkin örneklerle de yer verilmiştir⁹. Örneğin Anayasa Mahkemesi bir kararında, “Kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade etmektedir. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil;...kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır”¹⁰ diyerek kişisel veri kavramını tanımlamış ve kararında hangi verilerin kişisel veri olarak

⁶ Bahri Öztürk ve diğerleri, **Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı**, 2.Baskı, Seçkin Yayıncılık, Ankara, 2022, s. 16,17; Elif Küzeci, **Kişisel Verilerin Korunması**, 4.Baskı, On İki Levha Yayıncılık, İstanbul, 2021, (Kişisel Verilerin Korunması), s.153; AIHM Büyük Daire’nin 04.12.2008 tarih ve 30562/04 ve 30566/04 başvuru numaralı S. ve Marper/Birleşik Krallık Davası kararı, <https://hudoc.echr.coe.int/>, (22.07.2022); 09.10.2012 tarih ve 42811/06 başvuru numaralı Alkaya/Türkiye Davası kararı, <https://hudoc.echr.coe.int/>, (22.07.2022).

⁷ Avrupa Birliği’nde Genel Veri Koruma Tüzüğü’nün yürürlüğe girmesiyle ilga edilen 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunması Hakkında Avrupa Parlamentosu ve Avrupa Konseyi Direktif’inin 2/a maddesinde “any information relating to an identified or identifiable natural person (data subject)” demek suretiyle kişisel veri, “kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlanmıştır. Direktif’in orjinal dildeki metnine ulaşmak için bkz. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (22.07.2022).

⁸ Tüzüğün orijinal tam metni için bakınız: <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>, (22.07.2022).

⁹ Yargıtay 12. Ceza Dairesi’nin 13.01.2014 tarih, 2013/8389 E. ve 2014/62 K. sayılı kararında “Kişisel verilerin kaydedilmesi ve verileri hukuka aykırı olarak verme veya ele geçirme suçlarının maddi konusunu oluşturan “kişisel veri” kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı .kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir” ifadelerine yer verilmiştir. Kararın tam metni için bkz. <https://karararama.yargitay.gov.tr>, (05.07.2022).

¹⁰ Anayasa Mahkemesi’nin 09.04.2014 tarih ve 2013/122 E., 2014/74 K., <https://normkararlarbilgibankasi.anayasa.gov.tr/>, (05.07.2022), s. 2.

nitelendirilebileceğine ilişkin açıklama ve örneklemelerde bulunmuştur. Kararda “*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, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi*” verilerin kişisel veri niteliğinde olduğu belirtilmiştir.

B. Kişisel Verinin Unsurları

Kişisel veriye ilişkin tanımlamalara bir önceki başlık altında gerek ulusal gerekse uluslararası mevzuat açısından detaylıca değinmiştik. Bu bağlamda en genel ifadeyle kişisel veriyi, kimliği belirli veya belirlenebilir bir kişiye ilişkin bütün bilgiler olarak tanımlayabiliriz. Kişisel veriyi, kişisel olmayan verilerden ayırt edebilmek için ise iki ölçütten faydalanılabilir. Bir verinin kişisel veri olarak isimlendirilebilmesi için söz konusu veri, (i) bir kişiye ilişkin ve (ii) bu kişi de belirli veya belirlenebilir nitelikte olmalıdır¹¹. Ancak en başta veri kavramı ile ne anlaşılması gerektiğine genel hatları ile değinmekte yarar vardır. Kişisel verinin unsurları aşağıda ele alınmıştır.

1. Bir Veri Bulunması

Kişisel verilerin korunması alanında veri, bilgi ve enformasyon kavramlarının sıklıkla birbirleri yerine geçecek şekilde kullanıldığı görülmektedir. TDK’nın güncel türkçe sözlüğünde veri kavramına getirilen tanımlamalara daha önce değinmiştik. Bilgi kavramına ise TDK, “*insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat*”, “*öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek; haber, malumat, vukuf*” şeklinde tanımlamalar getirmiştir. Enformasyon kavramı ise TDK’da “*Danışma, haberleşme*” şeklinde tanımlanmıştır¹². Teorik temelde bu kavramlar birbirlerinden derin farklılıklar taşımaktadır. Ancak kısaca veri enformasyonun, enformasyon ise bilginin hammaddesini oluşturmaktadır¹³. Kavramlar arasındaki derin anlam ayrılıklarına girmek yerine bu şekilde bir kümelenendirme ile söz konusu

¹¹ Küzeci, Kişisel Verilerin, s. 10; Öztürk ve diğerleri, ss. 17,18.

¹² <https://sozluk.gov.tr/>, (22.07.2022)

¹³ Küzeci, Kişisel Verilerin, s. 9; İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayıncılık, Ankara, 2019, (Kişisel Veriler) ss. 31,32.

kavramları zihnimizde canlandırmak çalışmanın konusu açısından faydalı ve yeterli olacaktır. Söz konusu kavramlar çalışmamızda birbirleri yerine geçecek şekilde kullanılmıştır. Zira bu şekilde bir kullanım, kişisel verilerin korunması hakkının içeriğini daraltmak yerine koruma alanının kapsamını olması gerektiği düzeyde tutmaya ve uygulamada ortaya çıkabilecek zorlukları bertaraf etmeye daha uygundur.

Kişisel veriler, kişiye ilişkin tüm bilgileri içeren veriler olup bir kişinin yalnızca özel hayatı ile sınırlandırılmayacak kapsamdadır¹⁴. Örneğin, kişinin ekonomik ve sosyal yaşamına ilişkin bilgiler, iş ilişkilerine ilişkin bilgiler de bu kapsamdadır¹⁵. Kişinin sahip olduğu şifreler gibi gizli bilgileri ile fiziksel özellikleri, arabasının markası gibi herkes tarafından bilinebilecek, aleni nitelikteki bilgileri de kişisel veri olarak nitelendirilebilir. Bilginin öznel yahut nesnel olması da o bilginin kişisel veri olarak değerlendirilmesine engel teşkil etmemektedir. Örneğin, kişinin mesleği, saç veya sakal rengi gibi nesnel nitelikteki bilgiler ile kişinin hırslı, cimri veya güvenilir olduğuna ilişkin kişiden kişiye değişebilecek nitelikteki öznel düşünceler kişisel veri kapsamında değerlendirilebilmektedir. Yine kişisel verinin saklandığı ortam, yazılı, görüntülü olma gibi kayıt altına alınma şekli de söz konusu verinin kişisel veri niteliği bakımından önem arz etmemektedir. Ayrıca birazdan değinilecek diğer unsurları da taşıması kaydıyla bir kişi hakkındaki bilginin, kişisel veri olabilmesi için doğru bir bilgi olması şart değildir. Örneğin, kişinin iflas etmiş olduğuna veya iş ilişkilerinde dürüst davranmadığına ilişkin gerçekte bağdaşmayan nitelikteki bilgiler her ne kadar doğru olmayan bilgiler olsa dahi kimliği belirli bir kişiye ilişkin olduğundan kişisel veri olarak nitelendirilebilecektir¹⁶.

2. Gerçek Kişiye Ait Veri

6698 sayılı Kanun kapsamında bir kişisel veriden söz edebilmek için, o verinin doğrudan veya dolaylı olarak bir gerçek kişiye ilişkin olması gerekmektedir¹⁷. İlişkin olma kavramından veri ile kişi arasındaki bağlantının sağlanması kastedilmektedir. Bu bağlantı ise içerik, amaç ve sonuç olmak üzere üç yönden incelenebilir. İçerik

¹⁴ Başar, s. 10; Aksoy ss. 13,14.

¹⁵ Korkmaz, Kişisel Veriler, s.30.

¹⁶ Hüseyin Can Aksoy, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Çakmak Yayınevi, Ankara, 2010, ss.13-16.

¹⁷ Öztürk ve diğerleri, s. 17.

bakımından verinin kişi ile bağlantılı olması, verinin doğrudan kişiye ilişkin olması anlamına gelmektedir. Örnek olarak, bir iş başvurusu gerçekleştiren kişinin, başvuruda bulunduğu yere sunmuş olduğu özgeçmişinde yer verdiği bilgileri içerik yönünden kişi ile bağlantılıdır. Amaç yönünden veri ile kişi arasındaki bağlantı incelenecek olur ise burada veri, kişi ile ilgisi bulunan bir amaç vesilesiyle işlenmektedir. Örneğin, bir tekstil işletmesinde kullanılan bir makinenin üretim faaliyetlerine ilişkin veriler, o makineyi kullanarak iş gören işçinin verimliliğini tespit etmek amacı ile kullanılacaksa amaç yönünden kişi ile bağlantılı veri söz konusudur¹⁸. Amaç yönünden kişi ile bağlantılı veriye bir başka örnek ise, bir firmanın nakliye araçları üzerine yerleştirilen araç takip sisteminin çalışanın verimliliğini tespit amacıyla kullanılması halidir. Bu veriler de amaç bakımından kişi ile bağlantılı olup kişisel veri olarak kabul edilir¹⁹. Sonuç yönünden verinin kişi ile bağlantılı olması hali ele alınacak olur ise, yukarıda verilen firmanın nakliye araçlarına takmış olduğu araç takip sistemi örneğinden hareket edilebilir. Şöyle ki, ilgili firma nakliye araçlarına takmış olduğu araç takip sistemini çalışanın verimliliğini tespit etmek amacıyla takmamış olsa dahi, araç takip sistemi ile elde edilen veriler çalışanın verimliliğine ilişkin bilgilere ulaşılmasına da olanak sağladığından sonuç yönünden kişiyle bağlantılı olup kişisel veri niteliğindedir²⁰.

3. Kimliği Belirli veya Belirlenebilir Kişi

a. Kişi Kavramı

Kişi kavramı, insanı da içerisine alan hukuki bir kavramdır. Bu bağlamda hak sahibi olan, borç altına girebilen, haklarını kullanabilen, borcundan dolayı sorumlu tutulabilen gerçek veya tüzel varlığa kişi denmektedir²¹. Nitekim modern hukuk sistemlerine bakıldığında yalnızca insanların değil aynı zamanda hukukun aradığı

¹⁸ Korkmaz, Kişisel Veriler, s. 47.

¹⁹ Öztürk ve diğerleri, s. 18.

²⁰ Korkmaz, Kişisel Veriler, s. 47.

²¹ İhsan Erdoğan ve A. Dilşad Keskin, **Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku**, Gazi Kitabevi, Ankara, 2019, s. 209; Korkmaz, Kişisel Verilerin Korunması, s. 35.

koşulları taşıyan kişi ve mal topluluklarının da kişi olarak nitelendirildiği görülmektedir²².

Kişisel verilerin korunması bakımından ise kişi kavramının içeriğine hangi tür kişilerin dahil edileceği hususunda öğretide ve uluslararası mevzuatta bir görüş birliği bulunmamaktadır²³. Ancak uluslararası alanda genel eğilimin gerçek kişilerin korunmasının hedeflendiği yönünde olduğunu belirtmemizde bir sakınca yoktur. Zira bu konudaki başlıca uluslararası düzenlemelere bakıldığında örneğin, Avrupa Konseyi'nin 28 Ocak 1981 tarihinde imzaya açılan "108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin" "*Tanımlar*" başlıklı 2. maddesinde kişisel verilerin kimliği belirli veya belirlenebilir bir gerçek kişi (ilgili kişi) hakkındaki tüm bilgileri ifade ettiği belirtilmiştir²⁴. Konuya bir başka örnek ise Avrupa Birliği'nin 25 Mayıs 2018 tarihinde 95/46/EC sayılı Direktif'i ilga ederek yürürlüğe giren "2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü" isimli düzenlemedir. Tüzüğün "*Tanımlar*" başlıklı 4. maddesinde "*kişisel veri, tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir ('veri sahibi'); tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir*" demek suretiyle gerçek kişilerin kişisel verilerinin koruma kapsamına alınmasının hedeflendiği görülmektedir²⁵. Her ne kadar uluslararası alanda genel eğilim, gerçek kişilerin kişisel verilerinin korunması yönünde olsa da tüzel kişilerin de kişisel verilerinin korunmasına yönelik çeşitli düzenlemelere rastlanmaktadır. Nitekim bu doğrultudaki "2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliği Korunmasına İlişkin Direktif'in", başlangıç bölümünün 12. maddesi, elektronik haberleşme sektöründe gerçek kişiler ile birlikte tüzel kişilerin kişisel verilerinin de korumaya tabi tutulabileceğini ifade etmektedir. Ayrıca İsviçre, Avusturya, Danimarka ve İtalya gibi bazı Avrupa

²² Başar, s.13.

²³ Aksoy, s. 18; Korkmaz, Kişisel Veriler, s. 35; Başar, ss. 14-19.

²⁴ Metnin Türkçe çevirisi için bkz. https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf, (13.07.2022).

²⁵ Metnin orijinal hali için bkz. <https://gdpr-info.eu/art-4-gdpr>, (13.07.2022).

lkelerinin ulusal mevzuatlarına bakıldığında, tzel kiřilerin kiřisel verilerinin korunmasına ynelik dzenlemelerin mevcut olduėu grlmektedir²⁶.

lkemizde, 6698 sayılı Kanun “... *gerek kiřiye iliřkin her trl bilgiyi...*” diyerek sadece gerek kiřilerin kiřisel verilerini koruma kapsamında tutmuřtur. Ayrıca Kanunun “*Tanımlar*” bařlıklı 3. maddesinde veri sahibi veya veri znesi olarak adlandırabileceėimiz gerek kiři iin “ilgili kiři” kavramını tercih etmiř, bu kavramın aıklamasında ise ilgili kiři kavramı ile anlařılması gerekenin, kiřisel verisi iřlenen gerek kiři olduėunu belirtmiřtir. Bu baėlamda tzel kiřilerin kiřisel verileri 6698 sayılı Kanun koruması kapsamına girmemektedir. Ancak tzel kiřiler hakkındaki verilerle gerek kiřiye ulařılabiliyor ise bu durumda ilgili veriler, kiřisel verilerin korunması kapsamında deėerlendirilir²⁷. Kanaatimizce kiřisel verilerin korunması bakımından kiři kavramına sadece gerek kiřiler dahil edilmelidir. Zira kiřisel verilerin korunması hakkı, zel hayatın gizliliėinin temini ve bireylerin kiřisel zerkliėinin gerektirdiėi bilgi zerinde denetim hakkını saėlamayı amalayan baėımsız, temel bir insan hakkıdır. Tzel kiřilerin insana has nitelikteki bireyin zerkliėi ve insan hakları gibi salt insanın insan olmasından kaynaklanan zellikleri tařımaması, kiřisel verilerin korunması hukuku erevesinde bir korumadan faydalanamaması sonucunu doėurmaktadır. Ancak burada belirtmek gerekir ki, bu durum tzel kiřilerin verilerinin hibir řekilde hukuki korumadan faydalanamayacaėı anlamı tařımamaktadır. Nitekim tzel kiřilere ait veriler de alanına ve konunun muhteviyatına gre eřitli dzenlemelerle hukuki korumaya tabi tutulmaktadır. Nitekim tzel kiřilere ait verilerin korunması hukukumuzda ticari sırların konusunu oluřturmakta ve bu baėlamda esas zelliėi řeffaflık olan tzel kiřilerin gerekli grlen hallerde sır olarak adlandırılan gizli bilgileri Trk Ceza Kanunu’nun 239. maddesi ile korunmaktadır²⁸.

Aıklık getirilmesi gerekli bir diėer konu ise kiřisel verilerin korunması baėlamında lmř kiřilerin kiři olarak kabul edilip edilemeyeceėi hususudur. Bu konuda lkelerin i hukuklarında farklı yaklařımlar benimsedikleri ve buna baėlı olarak farklı hukuki dzenlemeler getirdikleri grlmektedir. rneėin Birleřik Krallık Veri Koruma Yasası’nın ilk maddesinde kiřisel veri yařayan gerek kiřiye iliřkin veri

²⁶ Aksoy, ss. 18,19; Korkmaz, Kiřisel Veriler, ss. 36,37.

²⁷ Kzeci, Kiřisel Verilerin, s. 363; ztrk ve diėerleri, s. 18.

²⁸ Kzeci, Kiřisel Verilerin, ss. 3,363,364; Korkmaz, Kiřisel Veriler, s. 39.

olarak belirtilmektedir. Japonya, İsveç, Güney Afrika gibi ülkelerde de benzer düzenlemeler yer almaktadır. Önemle belirtilmelidir ki, ölen kişilere ait verilerin kişisel veri kabul edilip edilmemesinde ulusal mevzuatın yaklaşımı ne olursa olsun, eğer ölen kişiye ilişkin verinin yaşayan bir kişiyi de etkilemesi ihtimali söz konusu ise bu durumda o verinin kişisel veri vasfı her halükârda olacaktır. Örneğin, genetik aktarımla geçebilen nitelikteki hemofili hastalığı, X kromozomuna bağlı bir hastalık olduğundan ve eğer ölen kişide bu hastalık var ise oğlunun da bu hastalığa sahip olması sonucu doğduğundan bu bilgi, kişisel veri mahiyetinde olup veri koruma yasalarının kapsamında kalacaktır²⁹.

Türk hukuku açısından bir değerlendirme yapılması gerekirse, mevzuatımızda 6698 sayılı Kanunun bu konuya ilişkin açıklama getirmediği görülmektedir. Ancak Türk Medeni Kanunu'nun kişiliğin başlangıcı ve sonu üst başlıklı 28. maddesi *“Kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer”* demek suretiyle ölümü kişiliğin doğal bir sona erme sebebi olarak nitelendirmiştir. Bu çerçevede 6698 sayılı Kanun'daki kişisel veri kavramı ile yaşayan gerçek kişilere ait verilerin anlaşılması gerektiği sonucuna ulaşılır³⁰.

b. Kimliği Belirli veya Belirlenebilir Olmak

Kişisel verinin unsurlarından bir diğeri ise, kimliği belirli veya belirlenebilir bir kişinin bulunmasına ilişkin olup, kimliğin hangi hallerde belirli veya belirlenebilir olduğunu tespit etmek gerekmektedir. Kimliğin belirli olması, bir grup insan arasından o kişinin dolaysız bir biçimde ayırt edilebilmesi anlamını taşımaktayken; kimliğin belirlenebilirliği ise her ne kadar o kişi henüz bir grup insan arasından ayırt edilememişse de söz konusu kişinin diğerlerinden ayırt edilebilmesinin mümkün olduğu anlamını taşımaktadır³¹. Bir başka ifadeyle kimliğin belirli olması, o bilgi ile kişi arasında doğrudan bağlantı kurulmak suretiyle o kişiyi diğerlerinden ayırt etmeyi; kimliğin belirlenebilir olması ise söz konusu bilgi ile kişi hakkındaki daha önce edinilen bilgilerin ilişkilendirilmesi suretiyle kişinin diğerlerinden ayırt edilebiliyor

²⁹ Başar, s. 19; Aksoy, s. 20,21; Korkmaz, Kişisel Veriler, s. 40.

³⁰ Başar, s. 21.

³¹ Aksoy, s. 21.

olmasını ifade etmektedir³². 6698 sayılı Kanunun gerekçesinde ise ilgili durum “*bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder*” şeklinde açıklanmıştır³³. Konuyu bir örnekle açıklamak gerekirse, bir kişi kimlik kartındaki kimlik numarası ile doğrudan diğer insanlardan ayırt edilebilmektedir. O kişinin anne, baba adının, telefon numarasının, doğum yeri ve tarihinin, ev ve işyeri adresi gibi bilgilerin bilinmesi ise o kişiyi doğrudan olmasa da dolaylı bir şekilde diğer insanlardan ayırt edebilmeye olanak tanımaktadır. Her somut olay açısından bir kişinin kimliğinin belirli veya belirlenebilir olması ayrı bir değerlendirmeye tabi tutulmalıdır³⁴. Çünkü kişisel veri kavramı niteliği itibarıyla dar bir çerçevede değerlendirilmeye müsait bir kavram değildir. Kişiyi tanımlanabilir kılması açısından yer, zaman gibi faktörlere bağlı olarak da değişiklik gösterebilmektedir. Bu bağlamda bir örneklendirme yapacak olursak, “beyaz ayakkabılı kişi” ifadesini genel olarak kullandığımızda, bu ayakkabıya sahip binlerce ve hatta belki de milyonlarca kişi bulunması sebebiyle söz konusu ifadenin bir kişiyi tanımlanabilir kılma özelliğine sahip olmadığını ve kişisel veri olarak kabul edilemeyeceğini söyleyebiliriz. Ancak aynı ifadeyi beyaz ayakkabı giymiş tek bir kişinin bulunduğu bir toplulukta ifade ettiğimizde, o kişi diğerlerinden ayırt edilebilir hale gelmekte, bir başka ifadeyle “beyaz ayakkabılı kişi” ifadesi o kişiyi tanımlanabilir kılmaktadır. Bu son durumda kullanılan ifade kişisel veri niteliğine sahip olmaktadır. Görüldüğü üzere farklı durumlarda aynı kavramlar birinde kişisel veri niteliğinde iken diğerinde kişisel veri niteliğine sahip değildir³⁵. Gerçek kişinin kimliğini belirli veya belirlenebilir kılma özelliğine sahip bütün veriler kişisel verilerin korunması hakkı kapsamındadır. Belirli veya belirlenebilir olma ayrımının hakkın korunmasına dahil olma durumu bakımından bir farkı bulunmamaktadır. Herhangi bir veri, bir gerçek

³² Korkmaz, *Kişisel Veriler*, s. 41; Ayrıca belirlenebilirlik kıstasına ilişkin öğretide ileri sürülen mutlak ve nispi belirlenebilirlik görüşleri hakkında bilgi edinmek için bkz. Mesut Serdar Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu**, On İki Levha Yayıncılık, İstanbul, 2018, s. 35.

³³ bkz. <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>, (22.07.2022).

³⁴ Öztürk ve diğerleri, s. 18.

³⁵ Murat Volkan Dülger, **Kişisel Verilerin Korunması Hukuku**, Hukuku Akademisi Yayıncılık, İstanbul, 2019, (Kişisel Veriler Hukuku) s. 12.

kişiyi belirli veya belirlenebilir kılıyorsa o veri artık kişisel veridir ve hakkın korunması yükümlülüğü doğmuş olmaktadır³⁶.

Anonimleştirilmiş veriler, bir başka deyişle kimliği belirli veya belirlenebilir gerçek kişiyle hiçbir bağlantısı kalmamış veriler ise kişisel verilerin korunması kapsamına girmemektedir. Nitekim Avrupa Birliği Genel Veri Koruma Tüzüğü'nün başlangıç kısmının 26. bölümünde bu hususa işaret edilerek, Tüzük hükümlerinin istatistiksel ve araştırma amaçları da dahil olmak üzere anonim hale getirilmiş verilerin işlenmesine uygulanmayacağı ifade edilmiştir³⁷.

C. Özel Nitelikteki Kişisel Veriler

Kişisel verilerin korunmasına ilişkin gerek uluslararası gerekse ulusal düzenlemelerin birçoğunda bazı veri gruplarına, özel bir önem atfedilmekte ve daha yüksek düzeyde bir koruma getirilmektedir. Özellikle ilgili kişinin ayrımcılığa uğramasına yol açabilecek bu verilerin sınırlı koşullar altında işlenmesi ilgili kişinin özel olarak korunmasına hizmet etmektedir³⁸. Özel nitelikli veriler veya hassas veriler olarak adlandırılan bu veri gruplarının içeriği dikkatlice incelendiğinde, özel nitelikli verilerin bireyin temel hak ve özgürlükleriyle daha yakından bir ilişki hali içerisinde olduğu ve bu verilerin kötüye kullanılması halinde bireylerin çok ciddi bir tehdit, zarar ve mağduriyet hali ile karşı karşıya kalabilecekleri görülmektedir³⁹. Bu çerçevede uluslararası alanda 95/46/EC sayılı Avrupa Birliği Direktifi⁴⁰, Avrupa Birliği Genel Veri Koruma Tüzüğü⁴¹, 108 sayılı Avrupa Konseyi Sözleşmesi⁴² ve Birleşmiş Milletler Rehber İlkeleri⁴³, özel nitelikli hassas verilere ilişkin olarak özel bir koruma ihtiva etmektedir. Buna karşın OECD Rehber İlkeleri'nde düzenlemeyi hazırlayan uzman heyetin evrensel olarak bir hassas veri kategorisinin bulunmadığı görüşü sebebiyle özel nitelikli hassas verilere ilişkin özel bir koruma getirilmemiştir⁴⁴.

³⁶ Öztürk ve diğerleri, s. 18; Aksoy, s. 22.

³⁷ Başar, s. 22.

³⁸ Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Basım, İstanbul, 2008, s. 86.

³⁹ Dülger, *Kişisel Veriler Hukuku*, s. 14.

⁴⁰ 95/46/EC sayılı Avrupa Birliği Direktifi'nin 8. maddesi.

⁴¹ Avrupa Birliği Genel Veri Koruma Tüzüğü'nün 9. maddesi.

⁴² 108 Sayılı Avrupa Konseyi Sözleşmesi'nin 6. maddesi.

⁴³ Birleşmiş Milletler Rehber İlkeleri 5. ilke.

⁴⁴ Küzeci, *Kişisel Verilerin*, s. 277.

II. KİŞİSEL VERİLERİN KORUNMASI HAKKI ve HAKKIN NİTELİĞİNE İLİŞKİN YAKLAŞIMLAR

A. Bir Hak Olarak Kişisel Verilerin Korunması

İnsan hakları en yaygın tabiriyle, insanın insan olmaktan kaynaklı sahip olduğu haklardır. Başka bir ifadeyle insan hakkı, hangi ırksal, dini, zümrevi, etnik veya mesleki topluluktan olursa olsun her kişinin yalnızca insan olmasından kaynaklanan değeri korumaya yönelik eylem potansiyelinin başkalarınca tanınması ve her türlü dış müdahaleye karşı korunması gereken en üstün ahlaki iddia veya taleptir⁴⁵. Demokratik toplumlarda temel hak ve özgürlükler, ünlü Alman hukukçusu George Jellinek'in ortaya koyduğu, günümüzde de yaygın bir şekilde kullanılan sınıflandırma yöntemi çerçevesinde üç kategoriye ayrılmaktadır. Bunlar negatif statü hakları, pozitif statü hakları ve aktif statü haklarıdır. Söz konusu sınıflandırmanın esasını devletin temel hak ve özgürlüklerin gerçekleştirilmesi konusundaki pozisyonu belirlemektedir. Bu sınıflandırmaya göre, negatif statü hakları bakımından devletin bu haklara müdahaleci bir tutumda bulunmaması yeterli görülmekteyken, pozitif statü hakları bakımından devletin bu hakları gerçekleştirmeye yönelik faaliyetlerde bulunması gerekmektedir⁴⁶. Kişisel verilerin korunması hakkı, hakkın genel çerçevesi ve özü birlikte değerlendirildiğinde negatif statü haklarından biri olarak kabul edilebilir⁴⁷. Nitekim Anayasamızda da bireylerin kişisel verilerinin korunmasını isteme hakkını düzenleyen hükme “*Kişinin Hakları ve Ödevleri*” başlığını taşıyan ikinci bölümde yer verilmiştir. Ancak bireylerin verilerinin korunmasını sağlayacak düzenlemelerin yapılması ve bu korumanın gerçekleşmesinde denetim vazifesi üstlenecek bağımsız denetim organlarının kurulması gibi devletin asli görevlerinin de bulunduğu düşünüldüğünde⁴⁸, kişisel verilerin korunması hakkının pozitif statü haklarına benzer yönlere sahip olduğu da dikkatlerden kaçmamaktadır. Belirtmek gerekir ki kişisel verilerin korunması verilerin işlenmesinin veya kullanılmasının mutlak bir biçimde

⁴⁵ Halil Kalabalık, **İnsan Hakları Hukuku**, 5.Baskı, Seçkin Yayıncılık, Ankara, 2017, s. 27.

⁴⁶ Mehmet Akad ve diğerleri, **Genel Kamu Hukuku**, 10.baskı, Der Yayınları, İstanbul, 2014, s. 261.

⁴⁷ Duman, s. 144.

⁴⁸ Küzeci, Kişisel Verilerin, s. 84.

yasaklanması anlamını taşımamaktadır. Kişisel verilerin korunması ile aslında hukuka aykırı şekilde verilerin işlenmesi yasaklanmaktadır⁴⁹.

Kişisel verilerin korunması hakkının, başka birçok hak ve özgürlükle yakından ilişkili olduğunu daha önce de belirtmiş idik. Özellikle kişisel verilerin korunmasının tarihsel sürecine ilişkin yapmış olduğumuz açıklamalarda sıklıkla belirtmiş olduğumuz üzere, dünyada yaşanan teknolojik gelişmeler kişisel verilerin korunması hakkının temel bir hak olarak korunması gerekliliğini ortaya çıkaran en önemli faktördür⁵⁰. Zira teknolojik imkanlarla, saniyeler içerisinde ve kolaylıkla kişisel verilere erişilebiliyor, bu verilerin depolanabiliyor ve çok uzak coğrafyalara dahi aktarılabilir olması bireylerin karşı karşıya kaldığı tehlikeleri tedirgin edici boyutlarda artırmıştır.

Kişisel verilerin korunması hakkının başta Avrupa olmak üzere çeşitli coğrafyalarda bağımsız temel bir hak olarak değerlendirilmeye başlanması bu hakkın niteliğine ilişkin tartışmaları da beraberinde getirmiştir. Mukayeseli hukuk çerçevesinde konu irdelendiğinde karşımıza Anglo-Amerikan ve Kıta Avrupası hukuk ekollerinin başlıca iki farklı yaklaşımı çıkmaktadır. Anglo-Amerikan hukuk ekolünde konuya ekonomik bir yaklaşımda bulunulmakta ve kişisel verilerin korunması hakkı mülkiyet ve/veya fikri mülkiyet hakları kapsamında değerlendirilmektedir. Kıta Avrupası hukuk ekolünde ise kişisel veriler sosyal ve hümanist bir yaklaşım ile temel insan hakları ve kişilik hakkı çerçevesinde ele alınmaktadır⁵¹.

B. Kişisel Verilerin Korunması Hakkının Niteliğine İlişkin Yaklaşımlar

1. Ekonomik Yaklaşım

Kişisel verilerin korunmasına ilişkin ABD'deki yaklaşım daha çok ekonomik ve ticari temellidir. Zira ABD'de, Kıta Avrupası'ndaki "*bilgi toplumu*" olgusunun yerine "*bilgi ekonomisi*" olgusu esas alınmaktadır. Gelişmiş bir ekonomik sisteme

⁴⁹ Bayram Doğan, **Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı**, Adalet Yayınevi, Ankara, 2022, s. 35.

⁵⁰ Dülger, İnsan Hakları Bağlamında, ss. 75,76.

⁵¹ Sinan Sami Akkurt, Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış, **Kişisel Verileri Koruma Dergisi**, Cilt: 2, Sayı: 1, 2020, ss. 21,22.

sahip ABD’de Kıtta Avrupa’sında olduđu gibi kişisel verilerin korunmasına yönelik katı ve sistematik düzenlemeler yerine sektörel çözümlerin getirildiđi görölmektedir⁵². Ekonomik hak yaklaşımının temelinde kişisel verilerin mülkiyet hakkına ve/veya fikri mülkiyet hakkına dayandığını öne süren görüşler mevcuttur⁵³.

a. Mülkiyet Hakkı Teorisi

Kişisel verilerin, hukuki niteliđi itibarıyla mülkiyet hakkı olduğunu ileri süren yaklaşıma göre kişisel veriler, sadece bireylerin kişiliğinin uzantısı olmayıp kişiliğın de ürünüdür. Kişisel veriler, ilişkin olduđu kişinin sahipliğine tabi olup herkesin kendi mülkiyetindeki bu verileri hangi şartlar altında kullanabileceğini kontrol edebilmesi gerekmektedir. Bilginin bir güç olarak kabul edildiđi günümüzde kişisel veriler önemli bir ticari değere sahiptir. İşte tam da bu noktadan hareketle, mülkiyet hakkı teorisini savunanlar kişisel verileri kullananların, verilerini kullandıkları kişilere bu kullanımdan kaynaklı adil bir bedel ödemesi fikrini ileri sürmektedirler. Veri pazarında yaşanan hareketlilik nedeniyle veri sahipleri bu alanda oldukça küçük bir role sahip olup bu hareketlilik çođu zaman veri sahiplerinin haberi dahi olmaksızın mağdur olabileceđi sonuçlara sebebiyet verebilmektedir⁵⁴. Oysa mülkiyet hakkı yaklaşımı sayesinde veri sahipleri deđişen tercihlerine göre ya özel hayatının gizliliğine önem göstererek kişisel verilerinin kullanımına, aktarımına izin vermeyecek ya da kendisi için uygun gördüđu anlaşmaları yapmak suretiyle söz konusu verilerin kullanımının karşılığını alabilecektir⁵⁵. Bununla birlikte, hemen hemen tüm hukuk sistemlerinde mülkiyet hakkının korunmasına ilişkin yerleşmiş bir sistem bulunduğundan kişisel verilerin korunması için başkaca bir sisteme ihtiyaç kalmayacak ve veri sahipleri etkili bir korumadan yararlanabilecektir⁵⁶.

Mülkiyet hakkı yaklaşımına teoride yöneltlen başlıca iki temel eleştirisi bulunmaktadır. Bunlardan ilki, mülkiyet hakkının doğası geređi kişisel verilerin bu hak çerçevesinde ele alınamayacağıdır. Zira mülkiyet hakkı, hak sahibine biri aktif diğeri pasif iki yetki vermektedir. Bunlardan pasif yetki hakkın konusunu koruma;

⁵² Küzeci, Kişisel Verilerin, s. 68.

⁵³ Doğan, s. 76.

⁵⁴ Aksoy, ss. 57,58.

⁵⁵ Küzeci, Kişisel Verilerin, s. 69; Korkmaz, Kişisel Veriler, s. 86.

⁵⁶ Doğan, s. 78.

aktif yetki ise hak sahibine hakkın konusunu dilediği gibi kullanma, yararlanma ve tasarrufta bulunma yetkisi vermektedir. Özellikle aktif yetki bakımından kişisel veriler üzerinden gerçekleştirilecek tasarruflar bazı sorunlara yol açabilecektir. Örneğin, kişisel verilerin veri sahibi tarafından bir başkasına rıza ile devredildiği düşünüldüğünde, verilerin yeni sahibi olan devralanın bu verileri mülkiyet hakkına dayanarak üçüncü bir kişiye satması doğal karşılanabilecektir. Oysa veri sahibi verilerinin üçüncü kişiye devrini istemiyor olabilir. Başka bir deyişle burada, mülkiyet hakkı yaklaşımının, veri sahibinin verilerinden mutlak olarak soyutlanması sonucunu doğurması eleştirilmektedir⁵⁷. Mülkiyet hakkı yaklaşımına getirilen diğer eleştiri ise gerek devlet-bireyler gerekse özel sektör teşebbüsleri-bireyler arasında yaşanacak veri alım satımlarında, bu alışverişin eşit konumda olmayan iki taraf arasında yapılıyor olmasıdır. Nitekim tarafları bu şekilde teşekkül edecek bir alışverişte daha zayıf durumda olması pek muhtemel olan bireylerdir. Böylece pazarlığın eşit koşullara sahip taraflarca yapılmamasından kaynaklı olarak yarar sağlayanların devlet veya özel şirketler, zarar görenin ise bireyler olduğu bir tablo meydana gelmektedir⁵⁸.

b. Fikri Mülkiyet Hakkı Teorisi

Kişisel verilerin niteliğine ilişkin özellikle ABD’de getirilen yaygın yaklaşımlardan bir diğeri kişisel verilerin fikri mülkiyet hakkı niteliğinde olduğudur. Bu yaklaşıma göre bireyler nasıl ki kitap, resim gibi düşünce ürünleri üzerinde fikri mülkiyet hakkından kaynaklı olarak birtakım manevi haklara sahipse kişisel veriler bakımından veri sahipleri de verileri üzerinde benzer haklara sahiptir⁵⁹. Bu yaklaşımı savunanlara göre, fikri mülkiyet hukuku özelinde eser sahibinin eseri umuma arz, eserde değişiklik yapma ve eserde değişiklik yapılmasını yasaklama gibi yetkileri ile veri sahibinin kişisel verileri üzerindeki denetim ve tasarruf yetkileri benzer olarak görülmektedir. Ancak bilinmektedir ki, fikri mülkiyet haklarının konusunu genel itibariyle eser sahipliğinden kaynaklanan haklar oluşturmakta ve söz konusu eser de düşünsel bir emeğin ürünü olarak ortaya çıkmaktadır. Buna karşılık her kişisel verinin ilgisinin düşünsel bir emeğinin ürünü olarak ortaya çıktığından bahsedilemez.

⁵⁷ Aksoy, s. 65.

⁵⁸ Küzeci, Kişisel Verilerin, s. 70; Korkmaz, Kişisel Veriler, s. 87.

⁵⁹ Dülger, Kişisel Veriler Hukuku, s. 45.

Kişinin biyometrik verileri, yara izleri gibi verileri buna örnek verilebilir. Bu sebeple fikri mülkiyet hukukuna konu fikri eserler ile veri koruma hukukundaki kişisel verilerin benzer olduğunu söylemek doğru olmayacak, benzer olmayan konuları benzemiş gibi aynı hükümlerle koruma girişiminde bulunmak ise kişisel verilerin korunması hukukunun özüne ve ruhuna aykırı olacaktır⁶⁰. Ayrıca bu yaklaşıma, mülkiyet hakkı teorisinde getirilen eleştirilerin tamamı da yine eleştiri olarak getirilebilecektir⁶¹.

c. Diğer Teoriler

Kişisel verilerin hukuki niteliğine ilişkin olarak ekonomik hak yaklaşımı çerçevesinde ileri sürülen görüşlerin sorunlu yönlerini gören kimi yazarlar, tamamen bu yaklaşımdan ayrılmadan ancak sorun teşkil eden belli bazı noktalarda çözümler öneren yeni teoriler de ortaya koymuşlardır. Bunlara örnek olarak güven teorisi ve kişisel verilerin ticari sırlar gibi korunmasını öngören yaklaşımlar verilebilir⁶².

d. Ekonomik Yaklaşım İlişkin Değerlendirmemiz

Hukuki niteliği itibarıyla kişisel verilerin ekonomik açıdan ele alındığı, özellikle mülkiyet/fikri mülkiyet hakkı olduğunu ileri süren görüşlere yöneltilen eleştirilerin oldukça yerinde olduğu düşüncesini taşıyoruz. Kanaatimizce, kişisel veriler bu yaklaşımlar çerçevesinde kabul edilir ise mülkiyet hakkının sağlamış olduğu kapsamlı yetkilerin kullanılması sonucunda bireyle bu verilerin ilişkisinin sonlanabileceği gibi gerçek hayatta çok tehlikeli sonuçları olan bir durum ortaya çıkmaktadır. Bireyle, kendisine ilişkin kişisel verileri arasında sıkı bir bağ bulunmaktadır. Her ne kadar birey, kişisel verileri üzerinde tasarruf yetkisine sahip olsa da bu tasarruflar neticesinde verileri devralanın kullanımlarına karşı bireyin gerek insanlık onuru gerekse diğer birçok temel hak ve özgürlüğü bakımından korunmaya devam etmesi hukuki bir zorunluluktur. Bu gerekliliğin ekonomik hak yaklaşımlarının içeriği ve mantığıyla örtüşmediğini belirtmek gerekir. Bununla birlikte hiç şüphesiz

⁶⁰ Akkurt, s. 24.

⁶¹ Küzeci, Kişisel Verilerin, s. 72.

⁶² Küzeci, Kişisel Verilerin, s. 72.

ki, kişisel verilerin günümüzde çok önemli bir ekonomik değeri bulunmaktadır. Ancak kişisel verilerin ekonomik değerinin olması, verilerin yalnızca ekonomik hakların dar çerçeveli korumasına tabi tutulacağı anlamını taşımamaktadır. Zira kişisel veriler, çeşitli yönleri bulunan ve kapsamlı bir koruma gerektiren, içeriği oldukça geniş bir kavram olarak hayatımızda yer almaktadır.

2. Sosyal-Hümanist Yaklaşım

Kişisel verilerin hukuki niteliğinin ekonomik bir hak olduğunu ileri süren görüşler karşısında özellikle Avrupa’da benimsenen yaklaşım, kişisel verilerin, özel hayatın gizliliği, insan onuru ve genel kişilik hakkıyla ilgili temel bir insan hakkı olduğu yaklaşımıdır⁶³. Avrupa’da yaşanan Yahudi soykırımı ve II. Dünya Savaşı gibi acı tecrübelerin ardından bilgi mahremiyetinin bir yurttaşlık hakkı olduğu, özel hayatın gizliliği, insanlık onuru ve kişilik hakkının mutlak surette korunması gerektiği bilinci önem kazanmaya başlamıştır⁶⁴. Federal Almanya Anayasa Mahkemesi’nin 1983 yılında vermiş olduğu Nüfus Sayımı Kararı örneğinde olduğu gibi insan onurunun ve insanların kişiliklerini serbestçe geliştirebilmelerinin hem bireysel hem de kamusal anlamda önemini vurgulayan çeşitli gelişmeler, kişisel verilerin korunması hususunun, temel nitelikte bir insan hakkı olduğu yaklaşımını tarihsel süreç içerisinde güçlendirmiştir⁶⁵.

Kıta Avrupası hukuk ekolünde kişisel verilerin, insan hakkı yaklaşımı çerçevesinde özellikle kişilik hakkının bir parçası olarak nitelendirildiğini söylemek mümkündür⁶⁶. Belirtmekte fayda var ki, insan hakları ve kişilik hakkı kavramları özü itibarıyla birbirleriyle keskin ayrımları olmayan, tümleşik nitelikte kavramlardır⁶⁷. Kişisel verilerin korunmasını kişilik hakkı çerçevesinde ele alan görüşler konuya çok yönlü bir şekilde yaklaşmaktadır. Öncelikle kavramsal bir inceleme yapmak gerekirse kişilik hakkı, her ne kadar üzerinde uzlaşa sağlanmış ortak bir tanıma sahip olmasa da öğretide ve çeşitli yargı kararlarında, kişilik değerleri üzerinde yer alan genel bir hak olarak tanımlanmaktadır. Kişilik hakkının içeriğine dahil edilebilecek değerlerin ise

⁶³ Korkmaz, Kişisel Veriler, s. 89; Küzeci, Kişisel Verilerin, s. 74.

⁶⁴ Akkurt, s. 25; Dülger, Kişisel Veriler Hukuku, s. 45.

⁶⁵ Küzeci, Kişisel Verilerin, ss. 75-77.

⁶⁶ Aksoy, s. 47.

⁶⁷ Akkurt, s. 25.

maddi, manevi, sır çevresi, mesleki ve ticari değerler olduğu ifade edilmektedir. Kişilik hakkı, bireyin yalnız kalmayı istediği, kendini geliştirdiği, yalnızca kendisinin belirlediği ve güvendiği insanları dahil ettiği dar yaşam alanı olarak ifade edilebilecek sosyal alanda bir koruma getirdiği gibi bireyin dış dünyadaki ifadeleri, görüntüsü ve itibarı gibi değerleri üzerinde de koruma sağlamaktadır. Genel kişilik hakkı çerçevesinde kişisel verilerin korunması hakkı ele alındığında birey, kendisine ilişkin veriler üzerinde hangi verilerini kimlerle paylaşacağı, hangi verilerini kamuya açıklayacağı gibi konularda tasarruf özgürlüğüne sahip kabul edilmektedir. Ayrıca birey hangi verilerinin kimler tarafından bilinebilir olduğuna ilişkin tahminlerde de bulunabilmektedir. Tüm bunlar bireyin yaşamını özgürce şekillendirebilmesine olanak sağlamaktadır⁶⁸.

Kişisel verilerin korunması hakkı, geçmişten günümüze özel hayatın gizliliği hakkı ile ilişkilendirilmiş ve bu hakkın özel bir görünümü olarak karşımıza çıkmıştır. Kişisel verilerin korunmasını hukuki nitelik bakımından insan hakkı olarak nitelendiren yaklaşıma göre, özel hayatın gizliliği üç alan teorisi çerçevesinde incelenmektedir. Bunlar genel yaşam alanı, özel yaşam ve gizli alandır. Genel yaşam alanı kişinin herkesle paylaştığı, kamuya açık yaşam alanı iken⁶⁹; özel yaşam alanı kişinin rızası doğrultusunda yakın çevresi ile paylaşımında bulunduğu alandır. Gizli alan ise kişinin yalnızca kendisine sakladığı, rızası olmaksızın paylaşılamayacak mahrem alanı olarak tanımlanabilir⁷⁰. Her ne kadar, kişisel verilerin korunması hakkı, çoğu zaman özel hayatın gizliliği hakkının bir parçası olarak karşımıza çıksa da özellikle yaşanan teknolojik gelişmelerin de etkisiyle özel hayatın gizliliği hakkının sağlayabileceği koruma kişisel verilerin korunması bakımından yetersiz kalmaya başlamış ve kişisel verilerin korunması hakkının ayrı bir hak alanı olarak tanımlanması gerekmiştir⁷¹. Gerçekten de kişisel verilerin korunması hakkı, bireyin yalnızca özel hayatına ilişkin verilerinin değil kendi rızası ile alenileştirmiş olduğu verileri de dahil olmak üzere bütün verilerinin korunabilmesine olanak sağlamaktadır. Kaldı ki, kişisel

⁶⁸ Korkmaz, Kişisel Veriler, ss. 90,91.

⁶⁹ Küzeci, Kişisel Verilerin, s. 79.

⁷⁰ Ayça Cankurt, **Kişisel Verilerin Korunmasında İdarenin Etkisi**, (Yayımlanmamış Yüksek Lisans Tezi), Karabük Üniversitesi Lisansüstü Eğitim Enstitüsü, Karabük, 2021, <https://tez.yok.gov.tr/UlusalTezMerkezi/>, (15.12.2022), s. 33.

⁷¹ Dülger, Kişisel Veriler Hukuku, s. 46.

verilerin korunması hakkının hukuki niteliğini, salt özel hayatın gizliliğine indirgeyen görüşlere yönelik getirilen eleştirilerden en önemlilerinden bir tanesi de kaynağını bu düşünceden almaktadır⁷². Ancak belirtmekte fayda var ki, kişisel verilerin korunması hakkı ile özel hayatın gizliliği hakkı tek bir ortak temeli esas alan iki haktır. Bu ortak temel ise insan onurudur. Her iki hak da insanın insan olmasından kaynaklanan değerleri korumaya ve bireyi kendine ait değerler üzerinde denetim sahibi kılmaya yönelmiştir⁷³. Bireyin kendisine ait verilerinin büyük bir çoğunluğu, aynı zamanda özel yaşamının bir parçasını oluşturduğundan kişisel verilerin korunması hakkını, özel yaşamın gizliliği hakkından tamamen soyutlamak da mümkün gözükmemektedir. Bu sebeple özel hayatın gizliliği hakkının gerekliliğine ilişkin değerlendirmeler kişisel verilerin korunması bakımından da dikkate alınmalıdır⁷⁴.

3. Görüşlere İlişkin Değerlendirmemiz

Kişisel verilerin korunması hakkının hukuki niteliğine ilişkin ileri sürülen görüşler, birçok yönüyle kişisel veri kavramının önemini ortaya koymaktadır. Hiç şüphesiz kişisel verilerin korunması hakkı, birçok temel insan hakkı ile yakından ilişkilidir. Bununla birlikte özellikle özel sektör bakımından kişisel verilerin taşımış olduğu ticari ve ekonomik değerın günümüzde yadsınamayacak düzeyde olduğunu da ayrıca ifade etmemiz gerekir. Ancak ekonomik hak yaklaşımı ve daha özelinde mülkiyet hakkı/fikri mülkiyet hakkı gibi kişisel verilerin korunmasını, ekonomik değerini önceleyerek ele alan yaklaşımların kişisel verilerin korunması hakkının niteliğini açıklamada uygun yaklaşımlar olmadığı kanaatindeyiz. Zira kişisel verilere alınıp satılabilen bir ürün muamelesi yapmanın, veri sahibinden soyutlanabileceği gibi bir sonuca yol açması riski bulunmaktadır. Oysa kişisel veriler, veri sahibi ile sıkı bir ilişki içerisinde olup her ne kadar veri sahibinin rızası ile devredilebilmesi mümkün kabul edilebilse de veri sahibinin bu verileri üzerinde denetim, bilgi alma ve verilerinin kötüye kullanılmasına karşı korunması ihtiyacı sürekli olarak devam etmektedir.

Kanaatimizce kişisel verilerin korunması hakkının hukuki niteliği insan hakkı yaklaşımı çerçevesinde genel kişilik hakkı olarak kabul edilmelidir. Çünkü kişilik

⁷² Akkurt, s. 26.

⁷³ Küzeci, Kişisel Verilerin, s. 88.

⁷⁴ Küzeci, Kişisel Verilerin, s. 85.

hakkı kavramı insanı insan kılan maddi-manevi tüm değerlere ilişkin bir haktır ve birey kişiliğinin korunmasını bu hak çerçevesinde herkese karşı etkili olacak şekilde isteyebilmektedir. Başka bir ifadeyle kişilik hakkı, kişinin maddi ve manevi varlığını geliştirmeye, saygı görmeye ve özgür olmasına ilişkin bir haktır. Kişilik hakkı kapsamındaki değerlere, bireyin yaşamı, beden bütünlüğü, onuru, saygınlığı ve özel hayatının gizliliği örnek olarak verilebilir⁷⁵. Öncelikle ifade etmeliyiz ki, kişisel verilerin korunması hakkını kişilik hakkı içerisinde, yalnızca özel yaşam ve mahremiyet hakkı kavramlarına indirgeyen görüşler⁷⁶ de bulunmakla birlikte biz bu görüşlerin isabetsiz olduğu kanaatini taşıyoruz. Zira böyle bir yaklaşım, bireyin yalnızca özel yaşam ve sır alanı olarak isimlendirilen yaşam alanlarındaki verileri bakımından koruma sağlarken, kamusal yaşam alanlarındaki verilerinin ise korumasız kalmasına sebebiyet verebilecektir. Kişisel verileri korunması hakkının hukuki niteliği bakımından 1983 yılında Alman Anayasa Mahkemesi tarafından verilmiş olan Nüfus Sayımı kararının belirleyici kabul edilebileceğini düşünüyoruz. Kararda, Alman Anayasasının insan onurunun korunması, kişiliğin maddi ve manevi olarak geliştirilmesi hakkı ile ilgili maddeleri yorumlanmış, “*enformasyonel self determinasyon hakkı*” isimli bir kavram ortaya konularak bu hakkın, kişilik hakkı çerçevesinde insan onurunun korunması ve insanın maddi-manevi varlığını geliştirmesi hakkının içeriğine dahil olduğu belirtilmiştir⁷⁷. Enformasyonel self determinasyon hakkı, bilgilerin geleceğini belirleme hakkı olarak da ifade edilmektedir. Bilgilerin geleceğini belirleme hakkı bireyleri, kişisel verilerinin sınırsız bir biçimde toplanması, saklanması ve aktarılmasından korumaya yönelmiştir. Bu ise anayasal düzenin merkezinde bulunan özgür bireyin onuru ile yakından ilişkilidir. Zira, bireyin hangi verilerinin kimler tarafından ne amaçla ve ne süre ile kullanıldığını/kullanılabileceğini bilmesi ve bunlar üzerinde denetimi bulunması gerekmektedir. Aksi halde o bireyin özgürce karar verme, kişiliğini geliştirme, kamusal yaşama katılma hakkı ciddi zararlar görecektir ve bütün bunların sonucu olarak da demokratik toplumun sürekliliğini sağlamak güçleşecektir⁷⁸. Tüm bu açıklamalardan hareketle, biz de kişisel verilerin korunması hakkının insan hakkı

⁷⁵ Rona Serozan, “Kişilik Hakkının Korunmasıyla İlgili Bazı Düşünceler”, **İstanbul Üniversitesi Mukayeseli Hukuk Araştırmaları Dergisi**, Cilt:11, Sayı:14, 1977, s. 93.

⁷⁶ Aksoy, s. 70.

⁷⁷ Aksoy, s. 71.

⁷⁸ Küzeci, Bilgilerin Geleceğini Belirleme, ss. 56,57.

yaklaşımı çerçevesinde değerlendirilmesi gereken, genel kişilik hakkının özel bir görünümü olduğu kanaatini taşıyor ve Alman Anayasa Mahkemesi'nin kararının konunun açıklığa kavuşturulmasında yeterli ve isabetli olduğunu düşünüyoruz. İfade etmek gerekir ki, kişisel verilerin korunması hakkı kanaatimizce, genel kişilik hakkı çerçevesinde bu hakkın özel bir görünümü olup günümüzde yaşanan özellikle bilişim teknolojilerindeki gelişmelerin de etkisiyle, taşıdığı önem gereği, hukuki düzenlemelere bağımsız bir hak alanı olarak konu edilmelidir. Bu durum hakkın, insan hakkı yaklaşımı çerçevesinde genel kişilik hakkının bir parçası olduğu gerçeğini değiştirmemektedir.

III. KİŞİSEL VERİLERİN KORUNMASINDA TEMEL AMAÇ VE KİŞİSEL VERİLERİN KORUNMASININ TARİHSEL GELİŞİMİ

A. Kişisel Verilerin Korunmasında Temel Amaç

Kişisel verilerin korunmasına ilişkin çalışmamızın bu bölümüne kadar yapılan açıklamalar, kişisel verilerin tarih boyunca neden korunmak istendiği hakkında bizlere açıkça fikirler veriyor ise de ayrı bir başlık altında kişisel verilerin korunması ile amaçlananın ne olduğuna değinmek konunun içselleştirilmesi bakımından faydalı olacaktır.

Kişisel veriler tarih boyunca bireylerin yaşamlarını özgürce geliştirebilmeleri ve sürdürebilmeleri bakımından vazgeçilmez öneme sahiptir. Kişisel verilerin korunması hakkı esasında haklar ve özgürlükler yelpazesindeki birçok temel hak ve özgürlük ile doğrudan temas halindedir. Örneğin, yaşam hakkı, özel hayatın gizliliği hakkı, düşünce ve kanaat hürriyeti, din ve inanç özgürlüğü bunlardan bazılarıdır⁷⁹. Ancak her ne kadar kişisel veriler birçok hak ve özgürlük ile doğrudan temas halinde olsa da dünyada çeşitli gelişmeler ve değişimler kişisel verilerin korunmasının zaman içerisinde bağımsız ve temel bir hak olarak nitelendirilmesi zarureti ortaya koymuştur.

⁷⁹ Dülger, İnsan Hakları Bağlamında, s. 76.

Kişisel verilerin korunması ile genel olarak, verilerin değil, verilerin ilişkin olduğu kişilerin korunması ve kişilerin kendilerine ait verilerin geleceğini belirlemek noktasında denetim hakkını elinde bulundurması amaçlanmaktadır⁸⁰. Bireye ait verilerin gerek devlet gerekse özel sektör ve kişiler karşısında korumaya tabi tutulması, bireyin özgür iradesiyle kararlar alabilmesini, maddi ve manevi varlığını bu özgür iradesi doğrultusunda geliştirebilmesini sağlamaktadır. Uzak tarihten bu yana devletlerin, yakın tarihte ise hem kamu hem de özel sektörün kişisel verilere olan ilgisi başta teknolojik gelişmeler olmak üzere çeşitli sebeplerle bir hayli artmıştır. Kamu sektörünün ve özel sektörün kişisel verilere olan ilgisi farklı amaçlar için olsa da bu amaçların hepsinde ortak bir nokta bulunmaktadır. Bu ortak nokta, “*verimliliğin artırılması*” olarak ifade edilebilir. Zira kamu sektörü ulusal egemenlik, toplumsal gereksinimlerin karşılanması, kamu hizmetlerinin etkili yürütülebilmesi, kamu güvenliğinin sağlanması gibi çeşitli konularda kişisel verileri kullanarak verimliliği artırmaya çalışırken; özel sektör kişisel verileri kullanmak suretiyle mal ve hizmetleri daha hızlı bir biçimde hedef kitleye ulaştırma ve daha çok kazanç sağlamayı amaçlayarak bu konulardaki verimliliği artırma gayretindedir⁸¹. Hiç şüphesiz kamu sektörü ve özel sektörün bu yaklaşımlarında bireyin faydasına olan birçok durum söz konusudur. Ancak tüm bunların yanında işlenen kişisel verilerin keyfi olarak kullanılması, aktarılması, bireyin temel hak ve özgürlüklerine hukuka aykırı biçimde müdahalede bulunulması tehlikesi de beraberinde gelmektedir⁸².

Genel olarak kişisel verilerin korunması ile amaçlananın, verilerin işlenmesi ile sağlanacak faydalar ile karşı karşıya kalınabilecek tehlikeler arasında hukuka dayalı bir dengenin kurulması olduğu ifade edilebilir. Bununla birlikte bir hukuka uygunluk sebebi bulunmaksızın veya veri sahibinin rızası olmaksızın kişisel verilere yönelik gerçekleştirilebilecek müdahalelere karşı bireyleri ve onların kişisel verileri üzerinde karar verebilme hürriyetlerinin korunması da kişisel verilerin korunmasında hedeflenmektedir⁸³. Diğer bir ifadeyle kişisel verilerin korunması, kişisel verilerin

⁸⁰ Küzeci, *Kişisel Verilerin*, s. 14.

⁸¹ Küzeci, *Kişisel Verilerin*, s. 25.

⁸² Başar, s. 119.

⁸³ Berat Duman, **Anayasa Hukukunda Kişisel Verilerin Korunması**, (Yayınlanmamış Doktora Tezi), Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2020, <https://tez.yok.gov.tr/UlusalTezMerkezi/>, (15.12.2022), ss. 144,145.

herhangi bir sınırlama olmaksızın ve hukuka aykırı olarak elde edilmesi, kullanılması ve devri karşısında kişilerin korunmasını amaçlayan bir temel hak korumasıdır⁸⁴.

B. Tarihsel Gelişim Sürecinde Kişisel Verilerin Korunmasına İlişkin Temel Düzenlemeler

1. Genel Olarak

Kişisel verilerin korunması alanının temel bazı ilkeleri çok eski tarihlerde ortaya çıkmış ve günümüzde de geçerliliğini korumaktadır. Bu ilkelerin oluşmasında birtakım meslek mensupları ile bireyler arasındaki güvene dayalı ilişkilerin etkili olduğunu söylemek mümkündür. Konuya örnek olarak, hekimlerin hastaları hakkındaki sağlık verilerini başkalarıyla paylaşmaması kuralı verilebilir. “*Hekimin sır saklama yükümlülüğü*” olarak adlandırılan bu ilke M.Ö. 5. yüzyıldan bu yana geçerliliğini koruyan temel ilkelerden bir tanesidir. Yine din adamları ve avukatlar gibi başka meslek mensuplarında da benzer gelişmeler gözlemlenmektedir⁸⁵. Kişisel veriler, tarihi süreç içerisinde her daim önemli olmuştur. Nitekim insanın doğasında olan “merak” duygusu bireyleri başka bireyler hakkında bilgi sahibi olmaya itmiştir. Bununla birlikte devletler de kamu düzenini ve güvenliğini sağlamak, akılcı yönetim politikaları üretebilmek yahut da tarihin belirli dönemlerinde yurttaşları gözetim altında tutmak gibi amaçlarla bireylerin kişisel verilerine erişme eğiliminde olmuştur⁸⁶. Ancak her ne kadar kişisel veriler tarih boyunca bu kadar önem taşımış ise de bugün anladığımız anlamda kişisel verilerin korunması kavramı nispeten yakın tarihlerde ortaya konulmuş ve oldukça yeni bir alandır. Özellikle teknolojiye ve buna bağlı olarak veri işleme yöntemlerinde yaşanan gelişmeler bireylerin kişisel verilerinin sistematik bir şekilde hukuki olarak korunmasını gerektirmiştir. Bir başka ifadeyle, uzun yıllar boyunca kişilerin mahremiyetinin bir parçası olarak karşımıza çıkan kişisel

⁸⁴ Şimşek, s. 5.

⁸⁵ Küzeci, Kişisel Verilerin, s. 115; Aydın Akgül, **Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi**, (Yayımlanmamış Doktora Tezi), Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli, 2013, www.tez.yok.gov.tr/UlusalTezMerkezi/, (21.08.2022), (Verilerin Korunması), s. 109.

⁸⁶ Korkmaz, Kişisel Veriler, s. 79; Aksoy s. 3.

verilerin korunması, 20. yüzyılda bilgi teknolojileri ve veri işleme etkinliklerinde yaşanan devrimsel nitelikteki gelişmeler ile bağımsız bir temel hak olarak nitelendirilmeye ve bu bağlamda korunmaya başlanmıştır⁸⁷.

Bugünkü anladığımız anlamıyla kişisel verilerin korunması, kaynağını 1960 ile 1970’li yıllarda yaşanan gelişmelerden almaktadır. 1960’lı yıllardan itibaren çarpıcı bir şekilde ortaya çıkan bilgisayar teknolojisi sunduğu olanaklarla birlikte aynı zamanda birtakım önemli sorunları da beraberinde getirmiştir. Zira artık bireylere ait kişisel veriler, çok hızlı ve pratik bir şekilde toplanabilmekte, aktarılabilmekte ve farklı kaynaklardan getirilen bilgilerle ilişkilendirilebilecek bir biçimde depolanabilmektedir. Nitekim bilgisayarların bu özellikleri taşıması, o tarihlerde devletlerin de dikkatini çekmiş ve yurttaşlarına ait bilgilerin tek bir veri merkezinde toplanması fikrinin doğmasına sebebiyet vermiştir. Ancak bu düşünce bireylerin temel hak ve özgürlüklerinin ihlaline sebebiyet verebileceği, devletin bireyler karşısında fazlasıyla güçlü bir konuma geleceği, insanları denetim ve gözetim altında hissettireceği gibi gerekçelerle yoğun tepkilerle karşılaşmıştır. Özellikle 2. Dünya Savaşı’nın ardından çok ağır bir tahribata maruz kalan Avrupa kıtasında devletlerin sınır tanımayan denetim, gözetim ve işleme gibi faaliyetlerinden fazlasıyla zarar görmüş Avrupa toplumu, yeniden bu tür sonuçlara sebebiyet verebilecek gelişmelere oldukça temkinli yaklaşmıştır. Gerçekten de otomatik olarak verilerin işlenmesine olanak tanıyan teknolojik gelişmelerin kullanımında hukuki bir denetim ve şeffaflık mutlaka gerekmektedir⁸⁸.

Aynı tarihlerde Avrupa kıtasının dışında, Amerika Birleşik Devletleri’nde de, kişisel verilerin korunmasına ilişkin önemli gelişmeler yaşanmakta idi. 1960’lı yıllarda dönemin Amerika Birleşik Devletleri Başkanı John F. Kennedy bütün ABD vatandaşlarının bilgilerinin bir araya toplandığı bir ulusal kişisel veri merkezi kurma girişiminde bulunmuştur. Ancak bu girişim Amerika’da “*right to be alone*”, Türkçe ifadesiyle “*yalnız kalma*” hakkına bir saldırı olarak nitelendirilmiş ve hayata geçirilmesi engellenmiştir. Yalnız kalma hakkı düşüncesinde, 1890’da Samuel D. Warren ve Louis D. Brandeis’in geliştirdiği özel hayat hakkı (*right to privacy*) fikrinin önemli katkısı olmuştur. Yalnız kalma hakkı yaklaşımı, bireylerin düşüncelerinin,

⁸⁷ Çekin, ss. 5-7.

⁸⁸ Küzeci, Kişisel Verilerin, ss. 115-117; Çekin s. 5.

kişisel bilgilerinin ne kadarının başkalarına aktarılabilceğine yine bireylerin kendisinin karar vermesinin doğru olacağını ileri sürmektedir. Bu gelişmeler ışığında her ne kadar ulusal kişisel veri merkezi kurulması girişimi engellenmişse de Amerika Birleşik Devletleri'nde özel hayatı koruyan bir yasa ancak 1974 yılında "Gizlilik Yasası" (*Privacy Act*) adıyla hayata geçirilebilmiştir⁸⁹. Çıkarılan bu yasa kamu sektörüne yönelik hazırlanmış olup özel sektörü kapsamamaktadır. Yasa uyarınca kişisel verilerin kamu otoritelerince işlenmesi sürecinde özenli ve dikkatli davranılması, verilerin korunması amacıyla yetkisiz kişilerce bu verilere erişimin engellenmesi gibi hususlar düzenleme konusu yapılmıştır⁹⁰.

Kişisel verilerin korunması alanında hazırlanan ilk yasal düzenleme ise Hessen eyaletinde (Almanya) 1970 yılında hazırlanmış ve yürürlüğe konmuştur. Amerika'da 1960'lı yıllarda yaşanan kişisel veri merkezi kurulması gelişmelerine benzer şekilde Almanya'nın Hessen eyaletinde de "*Hessen Planı*" çerçevesinde bir federe merkezi veri bankası kurulması tasarlanmış ancak tasarının özel hayatın gizliliği üzerindeki olası etkileri yoğun tartışmalara sebep olmuştur. Ardından Hessen eyaletinde verilerin korunması hakkında yasal düzenleme yapılmıştır. Söz konusu düzenlemeyi takip eden süreçte ise 1977 yılında Almanya'da federal düzeyde ayrı bir veri koruma yasası kabul edilmiştir. Ancak belirtmek gerekir ki, Almanya'nın Federal düzeyde kabul ettiği bu veri koruma yasasından önce 1973 yılında İsveç'te kabul edilen veri yasası bu alanda yürürlüğe konan ilk ulusal yasa düzenlemesi olma özelliğini taşır⁹¹. Veri koruma yasası ihtiyacı doğrultusunda yapılan düzenlemeleri 1978 yılında Fransa, 1984'te İngiltere ve İsviçre takip etmiş ve daha sonrasında ise tüm Avrupa'da yayılarak devam etmiştir⁹².

Kişisel verilerin korunmasına ilişkin yasal düzenlemeler, başlarda devletin birey karşısında veri merkezleri kurmak gibi yöntemlerle aşırı güçlenmesine karşı bir tepki olarak doğmuş ve bu düzenlemeler ile devletin denetlenebilirliğini, şeffaflığını sağlamak amaçlanmıştır. Nitekim bu tepkinin bir sonucu olarak da birçok devlette veri bankaları kurulması girişimi başarısız olmuştur. Kişisel verilerin korunmasına ilişkin hazırlanan ilk yasal düzenlemelerin ortak noktasının birey ile devlet arasında, kişisel

⁸⁹ Öztürk ve diğerleri, s. 48.

⁹⁰ Başar, s. 131.

⁹¹ Küzeci, Kişisel Verilerin, s. 118; Korkmaz, Kişisel Veriler, s. 80.

⁹² Öztürk ve diğerleri, s. 48.

verilerin işlenmesi bağlamında bir denge sağlamak olduğu rahatlıkla söylenebilir. Fakat ilerleyen zamanlarda bilgi teknolojilerinde yaşanan değişim ve gelişimin hız kesmeden devam etmesi artık yalnızca devletlerin değil özel sektörde de pek çok veri bankasının kontrolsüzce kurulabilmesi tehlikesini beraberinde getirmiştir. Söz konusu durum ise kişisel verilerin işlenmesine yönelik yaklaşımın, münferit veri işleme süreçlerinin kontrolünden ziyade bireylerin hem kamuya hem de özel sektöre yöneltebileceği genel nitelikte bir kişisel verilerin korunmasını talep etme hakkı olarak gelişmesine ve değişmesine sebep olmuştur. Bu yaklaşım değişiminden önce kişisel verilerin korunması yalnızca veri bankalarındaki bilgilere ulaşma ve doğruluğunu sağlamak ile sınırlı iken, bu yaklaşım değişikliğinden sonra artık bireyler hangi verilerinin işlenip işlenmeyeceğine kendisi karar verebilmekte, veri işleme sürecinde de başka birtakım haklara sahip olmaktadır⁹³.

Kişisel verilerin korunması alanında böyle bir yaklaşım değişikliği gerçekleşirken, Federal Almanya Anayasa Mahkemesi tarafından 1983 yılında verilen “*Nüfus Sayımı Kararı*”, konuya ilişkin yapılan tartışmalarda adeta yol gösterici bir niteliğe sahiptir ve ülke sınırlarını aşacak düzeyde ses getirmiştir. Nitekim bu kararın sonrasında kararda yer verilen değerlendirmeler, birçok ülkenin yasal düzenlemelerine ve 95/46/EC sayılı Avrupa Birliği Veri Koruma Direktifi’ne önemli etkilerde bulunmuştur. Söz konusu karar, o dönemde Almanya Parlamentosunca oybirliği ile kabul edilmiş bulunan Nüfus Sayımı Yasası’nın bazı hükümlerinin Anayasa’ya aykırı olduğundan bahisle iptaline ilişkindir. Nüfus Sayımı Yasası’nda, Almanya’da 1983 yılında yapılması planlanan nüfus sayımına ilişkin olarak memurların insanların evlerine giderek onlara, içerisinde çeşitli ve kapsamlı soruların bulunduğu bir anket çalışması yapması öngörülüyordu. Bu ankette yer alan sorular, bireylerin ikametgâh bilgileri, medeni durumları, gelirleri, eğitim durumları gibi çeşitli bilgilerinin toplanmasını sağlayacak nitelikteydi ve anket sorularının insanlar tarafından yanıtlanması yasa gereği zorunlu tutulmuştu. Ayrıca bunların yanında söz konusu yasa, toplanan bilgilerin uzun süre saklanmasına, çeşitli amaçlarla yerel yönetimlerle paylaşılmasına ve istatistiki amaçların yanında ikametgâh kayıtlarının karşılaştırılmasına da olanak sunmaktaydı. Almanya’daki vatandaşlar, anket aracılığıyla sorulan soru ve toplanan bilgilerin tekrardan kendileriyle

⁹³ Küzeci, *Kişisel Verilerin*, ss. 120,121; Korkmaz, *Kişisel Veriler*, s. 80; Öztürk ve diğerleri, s. 50.

ilişkilendirilebilecek surette işlenmesinden endişe duyuyorlardı. Bu denli kapsamlı kişisel bilgilerin, yapılacak anket aracılığıyla toplanacak ve kayıt altına alınacak olması, Almanya kamuoyunda ilgili yasal düzenlemeye karşı büyük bir tepki doğmasına sebep olmuştur. Federal Almanya Anayasa Mahkemesi, her ne kadar söz konusu yasal düzenlemenin genel amacı olan nüfus sayımı hususunu Anayasa'ya uygun görse de yasada bireylerin birtakım temel hak ve özgürlüklerinin korunması için yeterince önlem alınmadığına hükmetmiştir. Mahkeme kararında, insanlık onuru ve bireyin özerk gelişimi hakkından hareketle “*bilgilerin geleceğini belirleme hakkı*” adında bir hak tanımlamasında bulunmuş, devletin kişisel verileri toplaması, kayıt altına alması ve tüm bu eylemlerinin doğurabileceği hukuki sonuçlar hakkında önemli değerlendirmelere yer vermiştir. Kişilerin, hangi verilerinin ne amaçlarla işlendiğini, ne kadar süre kullanıldığını ve saklandığını bilmesinin demokratik bir toplumun gerekliliklerinden olduğunu kararında ifade eden Mahkeme, özellikle otomatik veri işleme teknolojilerinin gelişip yaygınlaşmasının kişisel verilerin işlenmesi, aktarılması, birbirleriyle ilişkilendirilmesi ve kişilerin ayrıntılı bilgiler içeren profillerinin çıkarılabilmesi gibi imkanları sağladığını, bu durumun ise kişilerin sürekli kayıt altında oldukları hissine kapılmalarına sebep olabileceğini, kişilerin kamusal yaşama katılımlarını etkileyebileceğini, özgür bir şekilde kişiliklerini geliştirmelerine ve demokratik haklarını kendi tercihleri doğrultusunda kullanmalarına engel oluşturabileceğini ifade etmiştir. Mahkeme, devletin üzerine düşen görevleri yerine getirmesinde elbette birtakım kişisel verileri toplayabileceğini, kayıt altında bulundurabileceğini ve aralarında ilişkilendirme yapabileceğini ancak bilgilerin geleceğini belirleme hakkının, tam da bu noktada devreye gireceğini ve bu veri işleme sürecinin demokratik toplum düzeninin gerekleri ile bireylerin temel hak ve özgürlüklerine zarar vermeyecek biçimde gerçekleştirilmesi gerektiği değerlendirmesinde bulunmuştur. Başka bir ifade ile Mahkemeye göre bilgilerin geleceğini belirleme hakkı, mutlak ve sınırsız bir hak olmayıp bireylerin kişilik hakları ile resmi veya özel kuruluşların bilgilendirilmesi arasında menfaatlerin detaylıca değerlendirilmesi suretiyle bir denge kurulmasına hizmet etmektedir⁹⁴.

⁹⁴ Elif Küzeci, İstatistiki Birimler ve Bilgilerin Geleceğini Belirleme Hakkı, **İnsan Hakları Yılı**, Cilt:32, 2014, (Bilgilerin Geleceğini Belirleme), s. 53,54; Çekin, s. 6,7; Küzeci, Kişisel Verilerin, s. 123; Korkmaz, Kişisel Veriler, s. 81.

Sürekli gelişmekte ve değişmekte olan bilişim teknolojilerine bağlı olarak kişisel verilerin işlenmesinde gerçekleşen pratik uygulamalar ve artış, tarihsel süreç içerisinde kişisel verilere yönelik korumanın uluslararası düzenlemelere konu edilmesine sebebiyet vermiştir. Özellikle kişisel verilerin sınır ötesi aktarımı uygulamalarının yoğunluk kazanması, devletlerce kişisel verilerin korunmasına ilişkin getirilen ulusal düzenlemelerin uluslararası birtakım ilke ve normlarla uyumlaştırılması zarureti doğurmuştur⁹⁵. Bununla birlikte insan hakları ihlallerine sebebiyet verebilecek unsurlardan bir tanesi de devletler olduğundan devletleri bağlayabilecek nitelikte uluslararası koruma mekanizmalarına ihtiyaç duyulmuştur⁹⁶. Kişisel verilerin korunması alanındaki uluslararası düzenlemelere her ne kadar daha sonra detaylı bir şekilde değinilecek olsa da bu başlık altında uluslararası düzenlemelerin tarihsel gelişimine kısaca yer vermek faydalı olacaktır. Öncelikle bu alandaki ilk uluslararası düzenleme Ekonomik İşbirliği ve Kalkınma Örgütü'nün (OECD) 23 Eylül 1980 tarihinde kabul ettiği “*Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler*” başlıklı düzenlemedir. Söz konusu düzenleme üye ülkeler nezdinde bağlayıcı bir nitelik taşımamakta olup tavsiye niteliğindedir.

Kişisel verilerin giderek bir güç kaynağı haline gelmesi ve öneminin artması üzerine Avrupa Konseyi de bu konu ile ilgili bir düzenleme hazırlamıştır⁹⁷. 28 Ocak 1981 tarihinde imzaya açılan ve 1 Ekim 1985 tarihinde yürürlüğe giren 108 sayılı “*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*” kişisel verilerin korunmasına ilişkin olarak uluslararası düzeyde gerçekleştirilen ilk kapsamlı sözleşme olma özelliğini taşımaktadır. Ayrıca bu sözleşme halen, kişisel verilerin korunması alanında bağlayıcılığı olan tek uluslararası metin niteliğindedir⁹⁸.

Birleşmiş Milletler bünyesinde kişisel verilerin korunması alanına ilişkin uluslararası düzenlemelere örnek olarak ise, 14 Aralık 1990 tarihli ve üye ülkelerin kişisel verilerin korunması konusunda asgari düzeyde bir standarda sahip olmalarını

⁹⁵ Başar, s. 135; Küzeci, *Kişisel Verilerin*, s. 128; Akgül, *Verilerin Korunması*, s. 112.

⁹⁶ Başar, s. 131.

⁹⁷ Sinem Göçmen Uyarer, **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, 2. Baskı, Seçkin Yayıncılık, Ankara, 2020, s. 47.

⁹⁸ Küzeci, *Kişisel Verilerin*, s. 144.

temin etmek amacıyla hazırlanan “*Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler*” başlıklı düzenleme verilebilir⁹⁹.

Avrupa Birliği’nde ise 1990’lı yıllarda kişisel verilerin korunması alanında yapılan çalışmalar neticesinde 24 Ekim 1995 tarihli “*95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif*” hazırlanmıştır. Bu düzenleme ile asıl amaçlanan husus Avrupa Birliği (AB) üyesi ülkelerdeki kişisel verilerin korunması mevzuatının uyumlaştırılmasıdır. Nitekim AB üyesi ülkeler, kişisel verilerin korunmasına ilişkin yasal düzenlemelerini bu Direktifi esas alarak hazırlamıştır. Tam da burada belirtmek gerekir ki, 6698 sayılı Kişisel Verilerin Korunması Kanunumuz da 95/46/EC sayılı Direktif esas alınarak oluşturulmuş bir yasal düzenlemedir¹⁰⁰. Ancak AB bünyesinde hazırlanan bu Direktif halihazırda ilga edilmiş durumdadır. Çünkü Avrupa Birliği’nde söz konusu Direktifin artık çağın ihtiyaçlarını karşılayamadığı, gelişen teknolojiye bağlı olarak oluşan sorunları çözmede yetersiz kaldığı gerekçelerinden hareketle bir veri koruma reformu hazırlığına girişilmiştir. Bu doğrultuda gerçekleştirilen çalışmalar neticesinde yukarıda bahsi geçen Direktif ilga edilerek “*Avrupa Birliği Genel Veri Koruma Tüzüğü*” isimli düzenleme kabul edilmiş ve 25 Mayıs 2018 tarihinde bu düzenleme tüm üye devletlerde yürürlüğe girmiştir¹⁰¹.

Bu başlık altında son olarak ifade etmek gerekir ki, 1948 tarihli BM İnsan Hakları Evrensel Beyannamesi ile Avrupa İnsan Hakları Sözleşmesi’nde özel hayatın gizliliğinin korunmasına ilişkin hükümler yer almaktadır. Kişisel verilerin korunması hakkı da dolaylı olarak özel hayatın gizliliğinin korunması ile yakından ilişkili olduğundan bu belgeler bakımından, özel hayatın gizliliği içerisinde bir korumaya tabidir. Nitekim AİHS’de kişisel verilerin korunmasına ilişkin doğrudan bir düzenleme bulunmadığını ancak AİHM’in içtihatlarında konunun AİHS’in 8. maddesindeki “*Özel Hayatın ve Aile Hayatının Korunması*” başlıklı hüküm çerçevesi içerisinde değerlendirildiğini ve bu kapsamda bir korumaya tabi tutulduğunu daha önce belirtmiş idik¹⁰².

⁹⁹ Korkmaz, Kişisel Veriler, s. 82.

¹⁰⁰ Öztürk ve diğerleri, s. 49.

¹⁰¹ Küzeci, Kişisel Verilerin, ss. 221,222.

¹⁰² Aynı yönde bkz. Başar, ss. 139, 155.

2. Uluslararası Düzenlemeler

a. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Düzenlemeleri

OECD, üye devletlerin ekonomik gelişimlerini desteklemek ve küresel ticaretin büyümesini sağlamak amacıyla 1961 yılında kurulmuştur. Bu nitelikteki bir uluslararası kuruluşun kişisel verilerin korunması hakkında uluslararası arenadaki ilk düzenlemeyi hayata geçirmesi hem konunun genel olarak önemine hem de kişisel verilerin ekonomik yönüne vurgu yapmaktadır¹⁰³. OECD'nin yayınlamış olduğu Rehber İlkeler tavsiye niteliğinde olup, üye ülkelerin bu ilkeleri iç hukuklarına dahil etme zorunlulukları bulunmamaktadır. Ancak her ne kadar böyle bir mecburiyet söz konusu değil ise de düzenlemenin öngördüğü kapsamlı ilkelerin, daha sonrasında birçok devletin ve uluslararası kuruluşun getirdiği düzenlemelere etkide bulunduğu gözlemlenmiştir¹⁰⁴. Söz konusu metinde, veri toplamanın sınırlılığı ilkesi, veri kalitesi ilkesi, amacın belirliliği ilkesi, kullanımın sınırlılığı ilkesi, veri güvenliği ilkesi, açıklık ilkesi, bireysel katılım ilkesi, hesap verilebilirlik ilkesi olmak üzere bugün birçok güncel veri koruma düzenlemesinde karşımıza çıkan temel ilkeler yer almıştır¹⁰⁵. Zaman içerisinde teknolojiye yaşanan hızlı değişim ve gelişim, kişisel verilerin korunmasına yönelik birtakım yeni sorunları beraberinde getirmiş ve bu alanda daha önce yapılan hukuksal düzenlemelerin güncel sorunlara yanıt verebilmesi için yenilenmesini zorunlu kılmıştır. Bu sebeple OECD 2013 yılında Rehber İlkeleri yeniden düzenlemiş, daha önceki metinde yer alan ilkeler yeni metinde muhafaza edilmekle birlikte söz konusu metne, veri ihlali halinde bildirimde bulunma yükümlülüğü, kişisel verilerin işlenmesinde rıza kavramı ve veri sorumlusunun kişisel verilerin sınır ötesi aktarımında sorumlu tutulması gibi birtakım yeni düzenlemeler eklenmiştir¹⁰⁶.

¹⁰³ Küzeci, Kişisel Verilerin, ss. 129-131

¹⁰⁴ Dülger, Kişisel Veriler Hukuku, s. 50; Göçmen Uyarer, s. 51.

¹⁰⁵ bkz. <https://www.oecd.org>, (21.08.2022).

¹⁰⁶ Göçmen Uyarer, s. 45; Öztürk ve diğerleri, s. 51.

b. Birleşmiş Milletler Düzenlemeleri

Birleşmiş Milletler Örgütü, 2. Dünya Savaşı'nın ardından 26 Haziran 1945'te imzalanan, 24 Ekim 1945'te ise yürürlüğe giren Birleşmiş Milletler Şartı ile kurulmuştur. Birleşmiş Milletler Şartı'nın 1. maddesinde özetle, uluslararası barış ve güvenliğin korunması, ekonomik, sosyal ve kültürel alandaki sorunların çözümünde ve temel hak ve özgürlüklere saygının geliştirilip güçlendirilmesinde uluslararası anlamda işbirliğinin sağlanmasının amaçlandığı ifade edilmiştir¹⁰⁷. Kişisel verilerin korunması hakkı da temel haklara ve özgürlüklere saygının esas alındığı Birleşmiş Milletler düzenlemeleri içerisinde özel hayatın gizliliği bağlamında ele alınmaktadır¹⁰⁸. Bu çerçevede 10 Aralık 1948 tarihinde kabul edilen İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi, *“Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır.”* düzenlemesini ihtiva eder¹⁰⁹. Avrupa Konseyi Danışma Meclisi, İnsan Hakları Evrensel Beyannamesi'nin 12. maddesine dayanarak 1970 yılında vermiş olduğu bir kararında özel hayatın gizliliği hakkına ilişkin önemli açıklamalarda bulunmuştur. Söz konusu kararda Danışma Meclisi, özel hayata saygının bireylerin yaşamlarını istediği şekilde sürdürebilmesi olduğunu, özel hayata yönelik dışarıdan yapılması muhtemel müdahalelerin mümkün olduğunca sınırlandırılması gerektiği, özel hayatın gizliliği hakkının kapsamına kişilerin özel hayatlarının, aile hayatlarının, maddi ve manevi bütünlüklerinin, ev hayatlarının girdiği, kişilerin hukuka aykırı şekilde dinlenmemesi ve gözetlenmemesi, özel yazışmalarından gizlice yararlanılmaması gerektiği ifade edilmiştir¹¹⁰. İnsan Hakları Evrensel Beyannamesi'ndeki özel hayatın gizliliği düzenlemesine benzer başka bir düzenleme yine, Birleşmiş Milletler bünyesinde temel hak ve özgürlükler bağlamında öne çıkan uluslararası metinlerden bir tanesi olan *“Medeni ve Siyasi Haklara İlişkin Uluslararası*

¹⁰⁷ Birleşmiş Milletler Şartı'nın orijinal metni için bkz. <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>, (12.09.2022); Birleşmiş Milletler Şartı'nın Türkçe çevirisi için bkz. https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf, (12.09.2022).

¹⁰⁸ Korkmaz, Kişisel Veriler, s. 158.

¹⁰⁹ Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi'nin Türkçe çevirisi için bkz. <https://www.hsk.gov.tr/Eklentiler/Dosyalar/9a3bfe74-cdc4-4ae4-b876-8cb1d7eeae05.pdf>, (12.09.2022).

¹¹⁰ Korkmaz, Kişisel Veriler, s. 159.

Sözleşme”de yer alır. Bu sözleşme 1966 yılında imzaya açılmış ve 1976 yılında yürürlüğe girmiştir. Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşmenin 17. maddesinde “(1) Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz. (2) Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir.” düzenlemesi yer alır¹¹¹. Birleşmiş Milletler İnsan Hakları Komitesi’nin 1988 yılındaki 32. oturumunun 16 numaralı Genel Yorumu’nda 17. maddeye ilişkin olarak, kamu makamları ile özel kişi veya kurumların bilgisayarlarında, veri bankalarında ya da bunlara benzer cihazlarında kişisel bilgilerin toplanması veya saklanması faaliyetlerinin bir hukuki düzenlemeye tabi olarak gerçekleştirilmesi gerektiği, devletlerin bireylerin özel hayatlarına ilişkin kişisel bilgilerine bu bilgileri edinme ve kullanma yetkisine sahip olmayanlarca erişilmesine engel olma, bu türdeki bilgilerin Sözleşme’nin amaçlarına aykırı kullanılmasını önleme yükümlülüğünün bulunduğu, veri tabanlarında veya kişisel dosyalarda bireylerle ilgili kişisel bilgiler bulunuyorsa bireylerin kendilerine ait bu kişisel bilgilerin neler olduğunu, hangi amaçla ve hangi kamu otoritesi veya özel kişi/kuruluş tarafından saklandığını bilme haklarının olduğu, söz konusu dosya ve veri tabanlarının yanlış kişisel bilgileri ihtiva ediyor olması halinde veya bu bilgilerin hukuka aykırı bir biçimde toplanmış yahut kullanılıyor olması halinde her bireyin bu bilgileri düzeltme veya ortadan kaldırılmalarını talep etme hakkının olduğu ifade edilmiştir¹¹².

Bilgisayar teknolojilerinde yaşanan gelişmelere bağlı olarak Birleşmiş Milletler bünyesindeki kişisel verilerin korunması konusunda ilk doğrudan düzenleme olan “*Bilgisayarlarla İşlenen Kişisel Veri Dosyaları Hakkında Rehber İlkeler*”, 14 Aralık 1990’da Birleşmiş Milletler Genel Kurulu tarafından kabul edilmiştir¹¹³. Tıpkı OECD’nin yayımlamış olduğu Rehber İlkeler metninde olduğu gibi Birleşmiş Milletler’in yayımlamış olduğu Rehber İlkeler de üye devletler bakımından tavsiye

¹¹¹ “Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme’nin” Türkçe çevirisi için bkz. https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020093321bm_05.pdf, (12.09.2022).

¹¹² Lema Uyar, **Birleşmiş Milletler’de İnsan Hakları Yorumları**, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2006, ss. 35,36.

¹¹³ Dülger, *Kişisel Veriler Hukuku*, s. 53; Başar, s. 136.

niteliğinde olup hukuki bağlayıcılıkları bulunmamaktadır¹¹⁴. Söz konusu metin ile amaçlanan, ulusal mevzuatlarında konu ile ilgili düzenleme bulunmayan Birleşmiş Milletler üyesi devletlerin düzenleme yapmalarına teşvikte bulunmak, ulusal ve uluslararası kuruluşların kişisel verilerin korunmasına ilişkin temel ilkeler doğrultusunda hareket etmelerini sağlamaktır¹¹⁵. Birleşmiş Milletler Rehber İlkeleri, yalnızca bilgisayarlar aracılığıyla işlenen kişisel veriler hakkında uygulama alanına sahip olup aynı zamanda üye devletlerin ulusal düzenlemelerinde bulunması gereken asgari standartları da saptamaktadır¹¹⁶. Düzenleme daha detaylı incelendiğinde, iki temel başlık etrafında oluşturulduğu, bunlardan ilkinin altında ulusal mevzuatlar bakımından getirilmesi önerilen teminatların bulunduğu; ikinci ana başlıkta ise bu ilkelerin uluslararası kuruluşlar tarafından işlenen veriler hakkında uygulanmasının ele alınmakta olduğu görülmektedir¹¹⁷. Ayrıca Birleşmiş Milletler Rehber İlkeleri, kişisel verilerin korunması amacıyla bağımsız denetim organlarının oluşturulmasını öngören uluslararası alandaki ilk metin olma özelliğine sahiptir¹¹⁸. Düzenlemenin ilk ana başlığı altında devletlerin ulusal mevzuatlarında kişisel verilerin korunmasına ilişkin getirmeleri önerilen güvenceler temel olarak şu şekildedir: yasal ve dürüst yollarla verilerin toplanması ve işlenmesi ilkesi, verilerin doğruluğu ilkesi, amacın belirli olması ilkesi, ilgili kişi tarafından erişim sağlanması ilkesi, ayrımcılık yapmama ilkesi, istisnai düzenleme yapabilme ilkesi, veri güvenliği ilkesi, denetim ve yaptırım ilkesi ile verilerin sınır ötesi akışı ilkesi¹¹⁹. Görüldüğü üzere günümüzde kişisel verilerin korunması alanında bu alana ilişkin temel nitelikte sayılan ilkeler, BM Rehber İlkeleri ile düzenleme altına alınmıştır. Ancak her ne kadar durum böyle ise de bir diğer tavsiye niteliğindeki uluslararası düzenleme olan OECD Rehber İlkeleri'ne kıyasla BM Rehber İlkeleri, gerek ulusal gerekse uluslararası alanda daha sınırlı bir etkiye sahip olmuştur¹²⁰. Bu durumun nedeni olarak ise hem BM Rehber İlkeleri'nin tavsiye niteliğinde olması hem de aynı nitelikteki OECD Rehber İlkeleri'nin bu alandaki ilk uluslararası düzenleme olması gösterilebilir¹²¹.

¹¹⁴ Göçmen Uyarer, ss. 45,46.

¹¹⁵ Küzeci, Kişisel Verilerin, s. 136; Korkmaz, Kişisel Veriler, s. 160.

¹¹⁶ Aksoy, s. 6.

¹¹⁷ Başar, s. 137.

¹¹⁸ Korkmaz, Kişisel Veriler, s. 160.

¹¹⁹ Küzeci, Kişisel Verilerin, s. 136; Göçmen Uyarer, ss. 46,47.

¹²⁰ Korkmaz, Kişisel Veriler, s. 160.

¹²¹ Küzeci, Kişisel Verilerin, s. 137.

c. Avrupa Konseyi Düzenlemeleri

(1) Genel Olarak

İkinci Dünya Savaşı'nın Avrupa'da bırakmış olduğu enkazın ardından Avrupa'nın demokratik esaslı temeller üzerinden yeniden inşasına yoğun çaba harcanmıştır. Bu doğrultuda gerçekleştirilen eylemlerden bir tanesi de Avrupa Konseyi'nin kurulmasıdır. Avrupa Konseyi'nin Statüsüne Dair Sözleşme, 5 Mayıs 1949 tarihinde imzaya açılmış olup 3 Ağustos 1949 tarihinde yürürlüğe girmiştir. Avrupa Konseyi'nin temel amacı, Avrupa'da barışı kalıcı kılmak, hukukun üstünlüğü, demokrasi ve insan hakları ilkelerini sürekli bir şekilde koruyup güvence altına almaktır. Bu amaç doğrultusunda Avrupa Konseyi 1950 yılında Avrupa İnsan Hakları Sözleşmesini kabul etmiştir¹²². AİHS yürürlükte olduğu tarihten bugüne, insan haklarının güvence altına alınması noktasında uluslararası nitelikteki en etkili düzenlemelerden bir tanesi olarak varlığını sürdürmektedir.

Kişisel verilerin korunması bakımından Avrupa Konseyi düzenlemelerine değinecek olursak, bu konuda akla gelen ilk uluslararası düzenleme AİHS'tir. AİHS'in kişisel verilerin korunması konusunda nasıl bir öneme sahip olduğu aşağıda, ayrı bir başlık altında, detaylı bir şekilde ele alınmaktadır. Bununla birlikte Avrupa Konseyi bünyesinde kişisel verilerin korunmasına yönelik 1973 ve 1974 yıllarında otomatik veri bankalarındaki kişisel verilerin korunması amacıyla iki tavsiye kararı yayımlanmış, sonrasında ise 1981 yılında 108 Sayılı "*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*" kabul edilmiştir¹²³. Aşağıda Avrupa Konseyi'nin hazırlayıp yürürlüğe koyduğu kişisel verilerin korunması alanında önem atfeden uluslararası düzenlemeler ayrıntılı olarak incelenmektedir.

¹²² Akgül, Verilerin Korunması, ss. 119,120.

¹²³ Küzeci, Kişisel Verilerin, s. 139.

(2) Avrupa İnsan Hakları Sözleşmesi

Avrupa İnsan Hakları Sözleşmesi (AİHS), 4.11.1950’de kabul edilmiş ve 3.09.1953’de yürürlüğe girmiş uluslararası bir sözleşmedir. İkinci Dünya Savaşı’nda yaşanan tecrübeler, savaşın ardından Avrupa’da, bireylerin devlet karşısında daha fazla korunması, etkili bir şekilde hak arayabilmelerinin sağlanması ve hukukun üstünlüğü ilkesinin yerleşmesi ihtiyacını ortaya koymuştur. AİHS ile esas olarak kişilerin sosyal, kültürel ve ekonomik haklarından önce sivil ve politik haklarının korunarak güvence altına alınması amaçlanmaktadır¹²⁴. AİHS’in özgün bir düzenleme olması, hiç şüphesiz temel hak ve özgürlükleri güvence altına almaya odaklanması ve bunun sağlanması adına özel bir yargısal denetim mekanizması öngörmesinden kaynaklanmaktadır. Bu durum AİHS’i, insan haklarının korunması konusunda uluslararası alanda en gelişmiş düzenleme modeli olma niteliğine kavuşturmuştur. Ülkemiz de AİHS’e taraf devletlerden bir tanesidir. Söz konusu Sözleşme 4 Kasım 1950 yılında Türkiye tarafından imzalanmış ve bu Sözleşmenin uygun bulunmasına dair kanun 1954 yılında Resmî Gazete’de yayımlanmıştır¹²⁵. Her ne kadar ülkemiz açısından Sözleşme’ye taraf olma tarihi bir hayli eski olsa da AİHM’in zorunlu yargı yetkisi ülkemiz tarafından 28 Ocak 1990 tarihinde kabul edilmiştir¹²⁶. AİHS, vatandaş veya yabancı Sözleşme’ye taraf ülkelerdeki bütün kişiler bakımından uygulanacaktır¹²⁷.

AİHS’te kişisel verilerin korunmasına yönelik doğrudan bir düzenleme bulunmamaktadır. AİHS’in uygulanmasını denetleme görevini yürüten AİHM ise vermiş olduğu kararlarda, somut olayı değerlendirmek suretiyle eğer olayda kişisel verilerin korunması söz konusu ise bu hususu m.8’de yer alan “*Özel ve aile yaşamına*

¹²⁴ Göçmen Uyarer, ss. 51,52.

¹²⁵ Başar, s. 151.

¹²⁶ Göçmen Uyarer, s. 52.

¹²⁷ Akgül, Verilerin Korunması, s. 120.

saygı hakkı”¹²⁸ çerçevesinde ele almaktadır¹²⁹. AİHM daha önce vermiş olduğu birçok kararında, Sözleşmenin canlı ve yaşayan bir belge olduğunu ifade etmiş ve Sözleşme hükümlerini yorumlarken günün koşullarını dikkate alarak hareket etmiştir. Kişisel verilerin korunması hususunun tarihsel süreç içerisinde bağımsız temel bir hak niteliğine kavuşması ve bu hakka yönelik ihlallerin bireylerin özellikle özel hayatlarına etkiye bulunuyor olması, kişisel verilerin AİHM tarafından Sözleşmenin 8. maddesi kapsamında değerlendirilmesine sebebiyet vermiştir¹³⁰. AİHM’in kişisel verilerin korunmasına ilişkin ilk kararı Klass ve diğerlerinin, Almanya’ya karşı yapmış oldukları başvuru üzerine verilmiştir¹³¹. Karara konu başvuruda, beş Alman avukat, telefon yazışma ve görüşmelerinin gizli bir şekilde takip edilmesine olanak tanıyan mevzuat hükümlerine ilişkin şikâyetle bulunmaktadır. Mahkeme ise konuyu AİHS’in 8. maddesi çerçevesinde yorumlamış ve kararında, ihtilaf konusu mevzuat hükümlerinin demokratik kurumların korunabilmesi için kesin bir biçimde gerekli olması halinde uygulanabileceğini, son dönemde demokratik toplumların gelişmiş terör ve casusluk faaliyetleriyle karşı karşıya kaldığını, Devletin bu gibi faaliyetlerle mücadelesinde birtakım gizli izleme yöntemlerine başvurusunun gereklilik arz edebileceğini, iletişim araçları üzerindeki gizli teknik takibi olanaklı kılan mevzuat hükümlerinin istisnai koşullarda ve ulusal güvenlik yahut suçun önlenmesi amaçlarıyla kullanılabileceğini, somut olay bakımından bu unsurların sağlandığından bahisle Sözleşmenin 8. maddesinin ihlalinin söz konusu olmadığını ifade etmiştir¹³². AİHM’in, kişisel verilerin korunmasına ilişkin olarak vermiş olduğu önemli kararlardan bir tanesi de S. ve Marper’in Birleşik Krallık’a karşı yapmış olduğu başvuruya ilişkindir. Söz konusu karara konu başvuruda başvurucular genel olarak, resmi makamlarca haklarında yürütülen soruşturma ve kovuşturmalar neticesinde

¹²⁸ AİHS’in 8. maddesi şu şekildedir: “(1) Herkes özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir. (2) Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzeninin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir”. Görüldüğü üzere hükmün birinci paragrafında hakkın özüne ilişkin açıklamada bulunulmuş ve ardından ikinci paragrafında hangi hallerde bu hakkın sınırlamaya tabi tutulabileceği ifade edilmiştir.

¹²⁹ Öztürk ve diğerleri, s. 51; Küzeci, Kişisel Verilerin, s. 153;

¹³⁰ Göçmen Uyarer, s. 52.

¹³¹ Küzeci, Kişisel Verilerin, s. 158.

¹³² Avrupa İnsan Hakları Mahkemesi, **Tematik Bilgi Notu-Kitle Gözetim**, Çev. T.C. Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü İnsan Hakları Daire Başkanlığı, 2017, https://www.echr.coe.int/Documents/FS_Mass_surveillance_TUR.pdf, (01.09.2022), s. 1.

verilen kovuşturmayaya yer olmadığı kararı ve beraat kararlarından sonra parmak izlerinin, hücre örneklerinin ve genetik profillerinin muhafaza edilmeye devam edilmesinden ötürü şikâyetle bulunmaktadır. Başvurucuların 8. madde yönünden ihlal iddialarına dayanak yaptıkları hususa ayrıca değinmekte yarar vardır. Şöyle ki başvurucular, kendilerinden ceza takibi sürecinde alınmış bulunan parmak izleri, DNA profilleri ve hücre örneklerinin muhafaza edilmesinin özel yaşamlarına saygı gösterilmesi hakkına saldırı niteliğinde bulunduğunu, çünkü bu verilerin bireysel kimliklerine sıkı sıkıya bağlı ve kontrollerinin kendilerinde olması gereken türde veriler olduklarını, ancak olayda çok sayıda özel bilginin kendi kontrolleri dışına çıkmış olduğunu, tüm bunlar ile birlikte söz konusu verilerin muhafaza edilmesinin toplum tarafından kınanmış hissetmelerine sebep olduğunu ve bunun gibi psikolojik sonuçların ağır neticelerinin bulunduğunu ileri sürmüşlerdir. Mahkeme ilgili başvuruya ilişkin vermiş olduğu kararında ise muhafaza edilen her bir kategori için ayrı ayrı değerlendirmede bulunmuştur. Değerlendirmelerin ortak noktası ise parmak izleri, hücre örnekleri ve DNA profillerinin muhafaza edilmesinin bireylerin özel yaşamlarına ilişkin ciddi kaygı ve ağır tehlikeleri beraberinde getirmesidir. Mahkeme, başvuranların yukarıda belirtilen türdeki kişisel verilerinin muhafaza edilmesinin kamunun çıkarları ile özel çıkarlar arasında bir denge sağlamadığından, Devletin kendisine tanınan takdir yetkisi sınırlarını aştığından, olayda başvurucuların özel yaşamlarına saygı gösterilmesi haklarına ölçüsüz bir biçimde saldırı bulunduğu ve saldırı niteliğindeki bu müdahalenin demokratik bir toplumda gerekli olarak görülmediğinden bahisle AİHS'in 8. maddesinin ihlal edildiğine karar vermiştir¹³³.

AİHS'te kişisel verilerin korunmasına ilişkin doğrudan bir düzenleme bulunmaması, Sözleşme çerçevesinde bu konu hakkında yapılacak bazı yorumlamaların sınırlı kalmasına sebebiyet verebilecek niteliktedir. Bunun sebebi ise AİHS'in yalnızca taraf devlet organlarının işlediği veriler bakımından bir güvence sağlayabilecek olmasından kaynaklanır. Diğer bir deyişle Sözleşmenin kişisel verilerin işlenmesi konusunda getirdiği güvencelerin, özel kişiler veya özel sektör tarafından işlenen veriler bakımından da uygulanabilirliği konusunda tereddütler oluşmaktadır. Ancak AİHM'in vermiş olduğu bazı kararlarda, özellikle Sözleşmenin 8. maddesi hükmü açısından yapılacak yorumlamanın özel kişi veya sektörleri de dolaylı bir

¹³³ Karara erişim için bkz. <https://hudoc.echr.coe.int/tur?i=001-114903>, (03.09.2022).

şekilde etkileyecek şekilde olduğu görülmektedir. Şöyle ki bu kararlarda AİHM, devletin bireyin özel hayatının gizliliği açısından bu alana müdahalede bulunmamak anlamında negatif bir yükümlülüğünün bulunması yanında, aynı zamanda bu hakkın temini noktasında pozitif düzenleme ve tedbirleri alma yükümlülüğünün de bulunduğunu ifade etmektedir. Bu şekilde, özel kişi veya özel sektör tarafından işlenen verilerin, hakkın korunmasını sağlayacak önlemler ve koşullar çerçevesinde işlenebilmesi mümkün hale gelecektir¹³⁴. Bu duruma kişisel verilerin korunması açısından daha açıklayıcı bir değerlendirme yapmak gerekir ise, AİHS m.8 kapsamında devletin negatif yükümlülüğü, kişisel verilerin Sözleşmeye aykırı şekilde işlenmesinden kaçınmak iken; devletin pozitif yükümlülüğü kişisel verilerin korunmasına ilişkin hususları düzenleyerek yürürlüğe koymak ve güvenceleri sağlamaktır¹³⁵.

(3) 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

1980’li yılların başında bilgi teknolojilerinde yaşanan hızlı gelişim ve değişimler, özel hayatın gizliliğine ilişkin geleneksel kurallarla kişisel verilerin tam anlamıyla korunamayacağı sonucunu ortaya çıkarmış ve bu alanda özel birtakım düzenleme ve araçlara ihtiyaç duyulmasına sebebiyet vermiştir. Nitekim AİHS’teki özel yaşamın gizliliğine ilişkin düzenlemenin kişisel verilerin korunması anlamında sınırlı bir koruma sunması Avrupa Konseyi’ni konu ile ilgili özel ve küresel nitelikte bir düzenleme yapma yoluna götürmüştür¹³⁶. Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde imzaya açılan ve 1 Ekim 1985 tarihinde yürürlüğe giren 108 sayılı “*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*” (108 sayılı Sözleşme), kişisel verilerin korunması alanında bağlayıcılık taşıyan ilk uluslararası düzenlemedir¹³⁷. Kişisel verilerin korunması alanında oldukça önemli bir yeri bulunan 108 sayılı Sözleşme, kendisinden sonra gerçekleştirilen bu

¹³⁴ Küzeci, Kişisel Verilerin, ss. 153,154.

¹³⁵ Başar, ss. 154,155.

¹³⁶ Küzeci, Kişisel Verilerin, s. 145.

¹³⁷ Murat Volkan Dülger, İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması, **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:5, Sayı:1, 2018, (İnsan Hakları Bağlamında), s. 86.

alandaki gerek ulusal gerekse uluslararası birçok düzenlemeye kaynaklık etmiş ve rehber olmuştur. 108 sayılı Sözleşme'nin en önemli özelliklerinden bir tanesi, sözleşmenin yalnızca Avrupa Konseyi üye devletlerin değil aynı zamanda Avrupa Konseyi'ne üyeliği bulunmayan devletlerin de imzasına açılmış bir uluslararası sözleşme olmasıdır. Bu duruma, kişisel verilerin korunması meselesinin gelişen teknolojinin de etkisiyle küresel bir sorun haline gelmiş olması sebep olarak gösterilebilir¹³⁸. Türkiye sözleşmeyi 28 Ocak 1981 tarihinde imzalamış ise de uygun bulma kanunu uzun bir süre çıkarılamamıştır. 17 Mart 2016 tarihli 29656 sayılı Resmî Gazete'de yayımlanan uygun bulma kanunu ile 108 sayılı Sözleşme ülkemiz açısından bağlayıcı nitelikte olmuştur¹³⁹. Sözleşme ile gerçek kişilere ait kişisel verilerin otomatik işleme tabi tutulması sırasında bu kişilerin özel hayatına saygı hakkının güvence altına alınması amaçlanmış olup, bu amaç doğrultusunda sözleşmeye taraf devletlerin sözleşme hükümlerini ülkelerinde bulunan herkes için uygulanabilecek şekilde iç hukuklarına aktarma yükümlülükleri bulunmaktadır¹⁴⁰. 108 sayılı Sözleşme'nin 3. maddesinin 1. fıkrasında “*Taraflar, işbu Sözleşmeyi kamu sektöründe ve özel sektörde, otomatik kişisel veri dosyalarına ve kişisel verilerin otomatik işleme tabi tutulması konusunda uygulamayı taahhüt ederler*” düzenlemesine yer verilmiştir. Görüldüğü üzere, kamu ve özel sektör tarafından gerçekleştirilen kişisel verilerin otomatik yollarla işlenmesi faaliyeti, 108 sayılı Sözleşmenin koruması kapsamında yer almaktadır. Yine hem sözleşmenin isminden hem de sözleşme hükümlerinden açıkça görüldüğü ve anlaşıldığı üzere, sözleşme ile esas hedeflenenin, otomatik yollarla işlenen kişisel verilerin güvence altına alınması olduğu söylenebilir. Ancak bu sınır kesin bir sınır olarak anlaşılmamalı ve sürecin tamamı yerine bir kısmının otomatik yollarla gerçekleştirilmiş olmasının da Sözleşme kapsamında değerlendirileceği ifade edilmelidir. Elle işlenen veriler ise 108 sayılı Sözleşme bakımından kapsam dışında bırakılmıştır¹⁴¹. Sözleşme'nin getirdiği güvenceler çerçevesinde esas kural “*otomatik işleme*” faaliyetlerine ilişkin ise de Sözleşme'nin 3. maddesinin 2. fıkrasının c bendi ile taraf devletlerin sözleşmeyi, otomatik bilgi işlemeye konu olmayan kişisel veri işleme faaliyetleri hakkında da uygulayabileceği ifade edilmiştir. Ayrıca aynı fıkranın

¹³⁸ Göçmen Uyarer, s. 48; Korkmaz, Kişisel Veriler, ss. 163.

¹³⁹ Dülger, Kişisel Veriler Hukuku, s. 54; Başar, s. 142.

¹⁴⁰ Avrupa Konseyi'nin 108 sayılı Sözleşmesi m.1; Öztürk ve diğerleri, s. 51.

¹⁴¹ Küzeci, Kişisel Verilerin, s. 146.

b bendinde, taraf devletlerin sözleşmede yer alan hükümleri gerçek kişiler haricinde vakıflar, dernekler, topluluklar, şirketler, kurumlar ve tüzel kişiliği olsun yahut olmasın, doğrudan veya dolaylı bir şekilde gerçek kişilerin bir araya gelmek suretiyle oluşturduğu her türde kuruluşlar hakkında da uygulayabileceği belirtilmektedir. Sözleşmeye taraf devletlerin, veri öznesi ve veri işleme yöntemi bakımından sözleşmenin kapsamını ilgili hüküm çerçevesinde genişletici bir yaklaşıma sahip olmasının, Sözleşme hükümlerinin uygulanmasına engel oluşturmayacağı açıkça anlaşılmaktadır.

108 sayılı Sözleşme aynı zamanda sözleşmeye taraf her devletin bir temsilcisinden oluşan Danışma Komitesi kurulacağını da öngörmüştür. Bu Danışma Komitesi'nin başlıca görevleri sözleşmenin uygulanması ve değişikliği konusunda teklifler sunmaktır. Nitekim bu doğrultuda Danışma Komitesi, 2001 yılında 108 sayılı Sözleşmenin eki niteliğinde bir protokol yayımlamış ve bu protokol 2004 yılında yürürlüğe girmiştir. Danışma Komitesi'nin yayımlamış olduğu *“181 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol”*de sözleşmeye taraf devletlerin, iç hukuklarında kişisel verilerin korunmasına ilişkin almış oldukları tedbirlerin 108 sayılı Sözleşmeye ve ek protokoldeki ilke ve esaslara uygunluğunu denetlemekle görevli bağımsız kontrol organları oluşturmaları gerektiği ifade edilmektedir. Söz konusu kontrol organlarının sayısı bir veya birden fazla olabilecektir. Bu anlamda taraf devletlerin takdir hakkı bulunmaktadır¹⁴². Türkiye'nin 8 Kasım 2001 tarihinde imzaladığı bu protokol 5 Mayıs 2016 tarihinde Resmî Gazete'de yayımlanarak iç hukukumuza dahil edilmiştir¹⁴³.

Avrupa Konseyi Bakanlar Komitesi'nin 108 sayılı Sözleşmenin uygulanması hakkında aldığı tavsiye kararlarına da değinmek gerekir. Zira kişisel verilerin korunması alanındaki çeşitlilik ve dinamizm her konunun Sözleşme hükümleri içerisinde detaylıca düzenlenmesini olanaksız kılmaktadır. Bu anlamda verilen tavsiye kararlarına, internet ortamında özel yaşamın korunması, sigorta işlemlerinde veya istatistiki amaçlarla toplanan ve işlenen kişisel verilerin korunması, tıbbi verilerin korunması hakkında tavsiye kararları örnek verilebilir¹⁴⁴.

¹⁴² Korkmaz, Kişisel Veriler, s. 166; Dülger, Kişisel Veriler Hukuku, s. 56.

¹⁴³ Öztürk ve diğerleri, s. 52.

¹⁴⁴ Başar, ss. 148,149.

Çalışmamızın çeşitli yerlerinde sıklıkla vurguda bulunduğumuz kişisel verilerin korunması alanındaki dinamik yapı ve bilişim teknolojilerinde yaşanan önemli gelişme ve değişimler, Avrupa Konseyi nezdinde de 108 sayılı Sözleşmeyi çağın değişen şartlarına ve güncel sorunlarına karşı yenileme ihtiyacını doğurmuştur. Nitekim 108 sayılı Sözleşme, Avrupa Konseyi Bakanlar Komitesi'nin 18 Mayıs 2018 tarihli kararı ile yenilenmiştir. Söz konusu düzenleme, 108 sayılı sözleşmenin modernize edilmiş hali olduğundan “*Convention 108+*” olarak isimlendirilmektedir¹⁴⁵. Bu sebeple biz de ilgili düzenlemeyi “*Sözleşme 108+*” olarak ifade etmekte sakınca görmüyoruz. 108 sayılı Sözleşmenin yenilenmesi faaliyetine ihtiyaç duyulmasının nedenlerinin açıklandığı metinde, gün geçtikçe artan bilgi ve iletişim teknolojilerinin kullanımının ve küresel anlamda veri işleme süreçlerinin yoğunlaşmasının bireylerin temel hak ve özgürlüklerine, özellikle de özel yaşamın gizliliği hakkına yönelik ihlallerin artmasına sebebiyet verdiği ifade edilmiştir¹⁴⁶. Avrupa Konseyi, 108 sayılı Sözleşmenin modernizasyonu ile hedeflenenin “*yeni bilgi ve iletişim teknolojilerinin kullanımından kaynaklanan zorluklarla başa çıkmak ve sözleşmenin etkin uygulamasını güçlendirmek*” olduğunu belirtmektedir¹⁴⁷. Nitekim Sözleşme 108+’da bilişim teknolojilerindeki gelişmeler de dikkate alınmak suretiyle veri koruma mekanizmalarının daha da güçlendirildiği dikkatlerden kaçmamaktadır. Ayrıca Sözleşme’nin amacının bireysel özerklik ve insan onuru odağında bir yaklaşımla belirlenmesi son derece önemlidir. Her ne kadar Sözleşme 108+ henüz yürürlüğe girmemiş olsa da Avrupa Konseyi’ni böyle bir girişimde bulunmaya iten sebepler ve yenileme faaliyeti ile Sözleşmeye getirilen veri koruma mekanizmaları, kişisel verilerin korunması alanında ileriye dönük risk analizleri başta olmak üzere muhtelif tespitlerin de daha kapsamlı bir biçimde yapılabilmesine olanak sağlar niteliktedir¹⁴⁸. Yenilenen metinde özellikle, veri işleme sürecinin şeffaf bir şekilde gerçekleşmesinin öngörülmesi, veri işleyen konseptinin tanımlanması, veri işlemede ölçülülük, asgarilik, hesap verilebilirlik prensiplerine değinilmesi, genetik,

¹⁴⁵ Dülger, Kişisel Veriler Hukuku, s. 55.

¹⁴⁶ Göçmen Uyarer, s. 50; Sözleşme 108+’nın tam metnine ulaşmak için bkz. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf, (08.09.2022).

¹⁴⁷ <https://www.coe.int/en/web/data-protection/convention108/modernised>, (08.09.2022)

¹⁴⁸ Küzeci, Kişisel Verilerin, s.149.

biyometrik, etnik köken ve sendika üyeliği gibi verilerin de hassas veri kategorisine dahil edilerek hassas verilerin kapsamının genişletilmesi öne çıkan başlıca düzenlemelerdir¹⁴⁹.

d. Avrupa Birliği'nde Kişisel Verilerin Korunması

(1) Genel Olarak

Avrupa Kıtası'nda birlik oluşturma düşüncesi, buradaki devletlerin kuruluşları ile eş zamanlı olarak gündeme gelmeye başlamış bir konudur. Nitekim Avrupa'da yaşanan çeşitli savaşlar neticesinde imzalanmış barış antlaşmalarında “birlik”, “federasyon” fikirlerinin ileri sürüldüğü görülmektedir. Özellikle 2. Dünya Savaşı'nın ardından bu savaşın olumsuz etkilerini giderebilmek amacıyla örgütlenme tüm Dünya'da olduğu gibi Avrupa'da da önemli bir olgu ve yöntem olmuştur¹⁵⁰. 1950'li yıllarda Avrupa Kömür ve Çelik Topluluğu, Avrupa Atom Enerjisi Topluluğu ve Avrupa Ekonomik Topluluğu'nun kurulması ile birlikte Avrupa Birliği'nin kurulması sürecindeki ilk adımlar atılmıştır. 1992 yılında akdedilen Maastricht Antlaşması ile bu üç topluluğun birlikte birinci sütununu oluşturduğu üç sütunlu yapının üzerinde Avrupa Birliği'nin kuruluşu sağlanmıştır. Yapının diğer sütunları ise ortak dışişleri ve güvenlik politikası ile adalet ve içişleri oluşturmakta olup bu iki sütun hükümetler arası bir niteliğe sahipti. Yukarıda bahsi geçen ve ilk sütunu oluşturan üç topluluk, Avrupa Birliği oluşturulana kadarki süreçte, tüzel kişiliğe sahip uluslararası hukuk süjeleri olarak andlaşmalar akdedebilmekte ve uluslararası örgütlere üye olabilmekteydi. Bu durum Avrupa Birliği'nin kurulmasını takiben, Birliğin bu üç örgütten ayrı ve bağımsız bir tüzel kişiliği olup olmadığı tartışmalarını beraberinde getirmiştir. 2007 yılında imzalanan ve 2009 yılında yürürlüğe konulan Lizbon Andlaşması neticesinde bu tartışmalar kesin olarak sonlandırılmış, üç sütundan oluşan yapı ortadan kaldırılarak bütün sütunlar Avrupa Birliği çatısı altında birleştirilmiş, kurumsal bir oluşum sağlanmış ve Avrupa Birliği'nin tüzel kişiliğe sahip olduğu açıkça ifade edilmiştir¹⁵¹.

¹⁴⁹ Öztürk ve diğerleri, s. 52; Göçmen Uyarer, s. 51; Başar, ss. 151.

¹⁵⁰ Akgül, Verilerin Korunması, s. 135.

¹⁵¹ Ahmet M. Güneş, “Bir Uluslararası Hukuk Süjesi Olarak Avrupa Birliği”, **Türkiye Adalet Akademisi Dergisi**, Sayı:19, Ekim 2014, ss. 128,129; Başar, s. 165.

Avrupa Birliği'nin temelinde, kişilerin, mal ve hizmetler ile sermayenin serbestçe dolaşımı düşüncesi bulunmaktadır. Diğer bir deyişle, Avrupa Birliği, kendine has ekonomik ve siyasi bir ortaklık olup yurttaş hakları, ekonomi, sanayi, siyasi, dış politika gibi alanlarda amaçlanan bütünleşme arzusunun kurumsal bir tezahürü olarak oluşturulmuştur. Her ne kadar böyle bir bütünleşme gayesi söz konusu olsa da söz konusu oluşum, bir federal devlet yapılanması niteliğinde olmayıp Birlik üyesi her devletin kendi egemenlik hakkı bulunmakta ve her üye devlet uluslararası alanda kendisini temsil edebilmektedir¹⁵². Yukarıda ifade edilen amaçların gerçekleştirilebilmesi açısından Avrupa Birliği'nde, kişisel verilerin korunması konusuna da büyük önem atfedilmiştir. Zaman içerisinde Birlik üyesi devletlerin, ulusal mevzuatlarında, kişisel verilerin korunmasına yönelik getirmiş olduğu düzenlemelerin farklılıklar taşıması, konuya ilişkin ulusal mevzuatlar arasında kapsamlı bir uyumlaştırma faaliyeti yürütülmesini zorunlu kılmıştır. Elbette Avrupa Birliği bünyesinde kişisel verilerin korunması konusunda gerçekleştirilen düzenlemelerin yegâne hedefinin üye devletlerin mevzuatlarında bir uyum sağlanması olmadığı belirtilmek gerekir. Bununla birlikte bireylerin temel hak ve özgürlüklerinin korunması daima ana hedeflerden bir tanesi olmuştur¹⁵³. Avrupa Birliği'nde kişisel verilerin korunmasına ilişkin oldukça geniş bir mevzuat ve bu alanda faaliyet yürüten birçok kurum bulunmaktadır. Nitekim yukarıda kişisel verilerin korunması hukukunun tarihçesinde de belirtmiş olduğumuz üzere bu alana kaynaklık eden birçok ulusal ve uluslararası düzenleme ilk olarak Avrupa'da ortaya çıkmıştır¹⁵⁴. Bu durumun en önemli sebeplerinden bir tanesi de Avrupa'da teknolojik gelişmelerin daha erken yaşanmış olması ve bu gelişmelere bağlı olarak kişisel verilere yönelik tehditlerin daha erken doğmuş olmasıdır. İfade etmek gerekir ki, gerek teknolojik gelişmelerin gerekse gelişmiş hukuk bilincinin etkisiyle Avrupa Birliği kişisel verilerin korunması konusunda öncü bir konuma sahiptir¹⁵⁵. Avrupa Birliği bünyesinde kişisel verilerin korunması alanında doğrudan rol oynayan kurum ve birimler oldukça fazla sayıdadır. AB Komisyonu, AB Konseyi ve Parlamentosu, Avrupa Birliği Adalet Divanı, Avrupa Veri Koruma Otoritesi, 95/46/EC sayılı Direktif'in 29. maddesindeki düzenlemeye

¹⁵² Küzeci, Kişisel Verilerin, s. 173.

¹⁵³ Başar, ss. 165,169.

¹⁵⁴ Küzeci, Kişisel Verilerin, s. 174.

¹⁵⁵ Dülger, Kişisel Veriler Hukuku, s. 57.

dayalı olarak bu alanda danışma organı niteliğinde kurulan Veri Koruma Grubu, yine 95/46/EC sayılı Direktif'in 31. maddesi uyarınca kurulan ve yalnızca danışma organı değil aynı zamanda kişisel verilerin korunmasına ilişkin önemli düzenlemelerin kabulünde de onayı gereken bir organ olan Komite, 95/46/EC sayılı Direktif'i ilga eden 2016/679 sayılı Genel Veri Koruma Tüzüğü ile Veri Koruma Grubu'nun yerine getirilen Avrupa Veri Koruma Kurulu, AB nezdinde kişisel verilerin korunması alanında faaliyet yürüten kurum ve organlara örnek olarak verilebilir¹⁵⁶. Avrupa Birliği nezdinde kişisel verilerin korunmasına ilişkin öne çıkan hukuki metinler ise “Avrupa Birliği Temel Haklar Şartı”, “95/46/EC sayılı Avrupa Birliği Veri Koruma Direktifi”, “2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü”dür. Bu metinlerden özellikle “Avrupa Birliği Veri Koruma Direktifi” ve daha sonra onun yerine geçen “Avrupa Birliği Genel Veri Koruma Tüzüğü”, doğrudukları etki bakımından çok önemli metinler olup, yalnızca Birlik üyesi ülkeler için değil aynı zamanda Birlik üyesi olmayan birçok devletin bu alandaki hukuki düzenlemeleri bakımından da model ve rehber olarak kabul edilmektedir¹⁵⁷. Bu hukuki düzenlemeler aşağıda detaylı bir şekilde incelenmektedir.

(2) Veri Koruma Direktifi

Kısaltılmış ifadesiyle 95/46/EC sayılı Veri Koruma Direktifi olarak da adlandırabileceğimiz, 24 Ekim 1995 tarihli ve “95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunması Hakkında Avrupa Parlamentosu ve Avrupa Konseyi Direktifi”, kişisel verilerin korunması alanının temel yapı taşlarından bir tanesi olarak görülmektedir¹⁵⁸. Direktif ile en başta bireylerin temel hak ve özgürlüklerinin, kişisel verilerin korunması bağlamında güvence altına alınması hedeflenmiştir. Direktif'in bir diğer amacı ise Avrupa Birliği üyesi devletlerin mevzuatlarındaki kişisel verilerin korunmasına ilişkin farklılıkları ortadan kaldırarak aynı düzeyde koruma sağlamak ve bu şekilde kişisel verilerin Birlik üyesi devletler arasındaki dolaşımının güvenlik riski olmaksızın serbestçe gerçekleşebilmesini

¹⁵⁶ Küzeci, Kişisel Verilerin, ss. 174-178.

¹⁵⁷ Başar, s. 166.

¹⁵⁸ Göçmen Uyarer, s. 58.

olanaklı kılmak olmuştur¹⁵⁹. Gerçekten de Avrupa Birliği'nin kuruluş amaçlarından biri olan kişilerin, malların, hizmetlerin ve sermayenin üye ülkeler arasında serbestçe dolaşımı düşüncesi¹⁶⁰, kişisel verilerin de bu serbest dolaşımın önemli bir parçası olmasından hareketle ciddi bir korumaya tabi tutulmasını gerektirmektedir. Halihazırda 95/46/EC sayılı Direktif yürürlükte değildir. 25 Mayıs 2018 tarihinde Avrupa Birliği nezdinde yürürlüğe giren “*Genel Veri Koruma Tüzüğü*” ile Direktif ilga edilmiştir. Ancak her ne kadar şu anda ilga edilmiş bir düzenleme olsa da Direktif, kişisel verilerin korunması alanında ortaya konmuş en temel düzenlemelerden bir tanesidir ve kabul edildiği tarihten itibaren hem Avrupa Birliği üyesi devletlerde hem de Türkiye dahil dünyanın pek çok ülkesinde bu alanda gerçekleştirilen hukuki faaliyetlere büyük ölçüde etkide bulunmuştur¹⁶¹.

Direktif'in 1. maddesinin birinci fıkrasında düzenlemenin amacı ifade edilmiştir. İlgili hükümde, “*Direktif uyarınca üye devletler, gerçek kişilerin temel hak ve özgürlüklerini ve özellikle kişisel verilerin işlenmesiyle ilgili olarak mahremiyet haklarını koruyacaklardır*” ifadesi yer almaktadır. Aynı maddenin ikinci fıkrasında ise “*Üye devletler 1. Paragrafta bağlantılı nedenlerle üye devletler arasında kişisel verilerin serbest akışını ne kısıtlayacak ne de yasaklayacaktır*” hükmü yer alır. Görülmektedir ki Direktif ile, gerçek kişilerin temel hak ve özgürlüklerinin kişisel verilerin korunması ve mahremiyet hakkı çerçevesinde koruma altına alınması, bu konuda Birlik üyesi devletler arasında yeknesak bir hukuk oluşturulması, yine Birlik içerisinde kişisel verilerin güvenle, serbest bir biçimde dolaşımı mümkün kılınarak ticaretin ve bilgi toplumunun gelişmesinin kolaylaştırılması ve kişisel veriler için üst düzey bir koruma sağlanması amaçlanmaktadır¹⁶². Bütün AB üyesi devletler nezdinde bağlayıcılığa sahip olan bu metin, üye devletlerin Direktifte yer alan düzenlemeler paralelinde, bunlara eş düzeyde yasalar oluşturulabileceğini buna karşın üye devletler arasında serbest bir şekilde veri dolaşımını engelleyecek herhangi bir yasal düzenleme yapamayacaklarını öngörmektedir¹⁶³. Bu noktada akla gelebilecek ilk soru Direktif ile üye devletlerde bir yasal uyumlaştırma hedeflenmekte iken Avrupa Birliği'nin kendi kurum ve organlarında işlenen kişisel verilerin nasıl bir korunmaya tabi tutulduğu

¹⁵⁹ Aksoy, s. 14.

¹⁶⁰ Küzeci, Kişisel Verilerin, s. 184.

¹⁶¹ Küzeci, Kişisel Verilerin, s. 183; Korkmaz, Kişisel Veriler, s. 210; Göçmen Uyarer, s. 60.

¹⁶² Korkmaz, Kişisel Veriler, s. 210; Göçmen Uyarer, ss. 58,59.

¹⁶³ Başar, s. 171.

sorusudur. 18 Aralık 2000 tarihli ve 45/2001/AT sayılı Tüzük bu sorunun yanıtıdır. Zira 45/2001/AT sayılı Tüzükte, Avrupa Parlamentosu, Avrupa Komisyonu, AB Konseyi, Avrupa Adalet Divanı ile Birlik hukuku çerçevesinde oluşturulan diğer organ ve kurumların kişisel verilerin işlenmesi konusunda uyacakları kural ve esaslar düzenlenmiştir¹⁶⁴.

Direktif'in 2. maddesinde çeşitli tanımlamalara yer verilmiştir. İlgili maddenin a bendinde kişisel veri *"kimliği belirli veya belirlenebilir bir gerçek kişi (veri sahibi) ile ilgili her türlü bilgi"* şeklinde tanımlanmıştır. Aynı bendin devamında ise kimliği belirlenebilir kişiden ne anlaşılması gerektiği *"doğrudan veya dolaylı olarak, özellikle bir kimlik numarasına veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktöre atıfta bulunularak tanımlanabilen kişi"* şeklinde ifade edilmiştir. Görüldüğü üzere Direktif, gerçek kişilerin kişisel verilerini korumaktadır. İlgili kişinin belirlenmesine olanak tanımayan anonim veriler ile tüzel kişilere ait veriler Direktif'in koruma kapsamının dışında tutulmuştur. Ancak Direktif üye devletlerin tüzel kişilerin verilerinin korunması konusunda düzenleme yapabilmelerine izin vermektedir. Ayrıca söz konusu hükümde kişiler hakkında her türlü bilginin kişisel veri olarak kabul edildiği ifade edilmektedir. Burada önem arz eden husus ilgili verilerin kimliği belirli veya belirlenebilir olan gerçek kişi ile ilişkilendirilebilir nitelikte olması durumudur¹⁶⁵. Direktif'de oldukça geniş bir veri tanımlaması yapılması, bireyin fiziksel ve ruhsal bütünlüğünün korunmasına odaklanılmış olduğunu ayrıca göstermektedir¹⁶⁶. Yine aynı maddenin b bendinde ise kişisel verilerin işlenmesi kavramı ile neyin anlaşılması gerektiği açıklığa kavuşturulmuştur. Hükümde kişisel verilerin işlenmesi, otomatik olsun veya olmasın kişisel veriler üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, saklama, uyarılma veya değiştirme, geri alma, danışma, kullanma, iletim yoluyla açıklama, yayma veya başka bir şekilde kullanıma sunma, hizalama veya birleştirme, engelleme, silme veya imha etme vb. işlemler olarak tanımlanmıştır. Dikkat edilecek olursa hükümde, kişisel verilerde gerçekleştirilecek tüm işlemlerin işleme faaliyeti olarak

¹⁶⁴ Küzeci, Kişisel Verilerin, s. 186.

¹⁶⁵ Korkmaz, Kişisel Veriler, s. 214,215; Akgül, Verilerin Korunması, ss. 150, 151; Başar, s. 173.

¹⁶⁶ Akgül, Verilerin Korunması, s. 150.

değerlendirileceği anlaşılmaktadır. Maddede sınırlayıcı bir sayım yerine örnekseyici bir sayım yönteminin tercih edildiği açıkça ortadadır¹⁶⁷.

Direktif'in 3. maddesi düzenlemenin kapsamını açıklamaktadır. Hükmün birinci fıkrasında Direktif hükümlerinin, tamamen veya kısmen otomatik yollarla işlenen ya da otomatik olmayan yollarla bir veri kayıt sisteminin parçası olarak işlenen veya işlenebilecek olan veriler için uygulanabileceği ifade edilmiştir. Direktif ile, veri işleme usulünün kapsamı geniş tutularak neredeyse bütün kişisel verilerin Direktif'in koruması kapsamına alınması hedeflenmiştir. Ayrıca aynı maddenin ikinci fıkrasında Direktif hükümlerinin uygulanmayacağı durumlar da belirtilmiştir. Direktifin Avrupa Birliği Kurucu Antlaşması'nın V. ve VI. başlıkları çerçevesinde düzenlenen konular gibi topluluk hukukunun dışında kalan alanlarda ve genel asayiş, devletin güvenliği, savunma, devletin ceza hukukuna ilişkin faaliyetleri çerçevesinde kişisel verilerin işlenmesinde uygulanmayacağı öngörülmüştür¹⁶⁸. Bir başka istisna da üçüncü fıkarda getirilmiş ve kişinin kişisel veya aile yaşantısı içerisinde gerçekleştirmiş olduğu veri işleme faaliyetlerinin Direktif hükümlerinin kapsamı haricinde tutulduğu ifade edilmiştir¹⁶⁹.

Direktif'in bir diğer önemli hükmü 6. maddesidir. Zira 6. maddede kişisel verilerin işlenmesi sürecine hâkim olan temel ilkelere yer verilmiştir. Hükmü göre veriler, hukuka uygun ve adil bir şekilde, belirli, açık ve meşru amaçlarla toplanmalı, bu amaçlarla uyumlu olmayan bir biçimde kullanılmamalı, ölçülülük ilkesine uygun bir şekilde işlenmeli, işlenen kişisel veriler doğru ve gerektiğinde güncel olmalı, veriler uygulanan işlemin amacının gerektirdiği süre boyunca bulundurulmalıdır. Söz konusu ilkeler halen geçerliliğini korumakta ve bu alana yön verir niteliktedir¹⁷⁰.

Direktif'in 7. maddesi kişisel verilerin hangi hallerde hukuka uygun bir şekilde işlenebileceğini düzenlemektedir. Hükmün a bendinde ilk olarak, veri sahibinin herhangi bir kuşkuya yer vermeyecek şekilde rıza göstermesi halinde o kişinin kişisel verilerinin işlenebileceği belirtilmiştir. İlgili hükmün b bendinde ise, veri sahibinin tarafı olduğu bir sözleşmenin ifası için veya bir sözleşmeye girmeden önce veri sahibinin talebi üzerine işlemin gerekli olması halinde yine o kişinin kişisel

¹⁶⁷ Başar, s. 175.

¹⁶⁸ Küzeci, Kişisel Verilerin, s. 187.

¹⁶⁹ Başar, s.173.

¹⁷⁰ Göçmen Uyarer, s. 59; Öztürk ve diğerleri, s. 53.

verilerinin işlenebileceği ifade edilmiştir. Ayrıca maddenin c bendinde, veri sorumlusunun tabi olduğu yasal bir yükümlülüğe uyması amacıyla veri işlemenin gerekli olması; d bendinde, veri sahibinin hayati menfaatlerini korumak için işlemenin gerekli olması; e bendinde, kamu yararına yürütülen bir görevin yerine getirilmesi veya veri sorumlusuna veya verilerin açıklandığı üçüncü bir tarafa verilen resmi yetkinin kullanılması için işlemenin gerekli olması; f bendinde, veri sahibinin temel hak ve özgürlüklerine ilişkin menfaatlerin bu menfaatlerin önüne geçtiği durumlar haricinde veri işlemenin veri sorumlusunun ya da verilerin açıklandığı üçüncü tarafın meşru menfaatleri için gerekmesi halinde kişisel verilerin işlenmesinin mümkün olacağı hükme bağlanmıştır.

Direktif ile düzenlenen bir başka konu ise hassas verilere ilişkindir. Hassas veriler, Direktif'in 8. maddesinde düzenlenmiştir. İlgili hükümde dikkat çeken husus, hassas verilere ilişkin getirilen düzenlemenin 108 sayılı Sözleşme hükümlerine kıyasla daha detaylı düzenlenmiş olduğudur¹⁷¹. Hükmün birinci fıkrasında üye devletlerin, etnik köken, ırk, dini ve felsefi inançlar, sendika üyeliği, siyasi görüş, sağlık ve cinsel yaşamla ilgili verilerin işlenmesini yasaklayacakları ifade edilmiştir. Hemen ardından aynı maddenin ikinci fıkrasında birinci fıkrada yer alan bu yasağa istisnalar getirmiştir. Ancak istisna getirilmesi, istisna kapsamındaki hassas verilerin Direktif koruması dışında kaldığı şeklinde anlaşılmamalıdır. Aksine hükümde istisna kapsamındaki hassas verilerin işlenebilmesinin tüm güvenlik önleminin alınması ve işleme sürecinin denetim altında tutulması ile mümkün olabileceği özellikle vurgulanmıştır¹⁷². Hükmün ikinci fıkrasının a bendinde getirilen ilk istisna veri sahibinin hassas verilerinin işlenmesi konusunda vereceği açık rızasıdır. Diğer bir deyişle, veri sahibi hassas verilerinin işlenebileceğine ilişkin açık rıza veriyor ise o kişinin hassas verilerinin işlenmesi mümkün olabilecektir¹⁷³. Ayrıca 8. maddenin beşinci fıkrasında, suçlar, ceza mahkumiyeti veya güvenlik önlemleri ile ilgili verilerin işlenmesi bakımından, altıncı fıkrasında ise ulusal kimlik numaraları ve kamusal öneme sahip tanıtıcı işaretler bakımından özel bir koruma öngörülmüştür¹⁷⁴.

¹⁷¹ Korkmaz, Kişisel Veriler, s. 219.

¹⁷² Göçmen Uyarer, ss. 59,60.

¹⁷³ Başar, s. 176.

¹⁷⁴ Korkmaz, Kişisel Veriler, s. 219; Başar, s.177.

Direktif, üye ülkelerden üçüncü ülkelere gerçekleştirilecek olan veri aktarımları bakımından kritik bir düzenleme getirmiştir. Direktif'te üçüncü ülkelere veri aktarımına ilişkin kurallar 25. ve 26. maddelerde düzenlenmiş olup Avrupa Birliği dışına veri aktarımının ancak üçüncü ülkelerde verilerin yeterli düzeyde bir korumaya tabi tutulması halinde olanaklı olacağı ifade edilmektedir. Bir başka ifade ile AB'ye üye bir ülkeden AB üyesi olmayan ülkeye veri aktarımı yapılabilmesi için aktarımın yapılacağı ülkede kişisel verilerin yeterli düzeyde korunuyor olması şartı aranır. Koruma düzeyinin yeterliliği bakımından ölçüt ise bütün unsurların birlikte değerlendirilmesi suretiyle belirlenmektedir. Bu çerçevede aktarımı yapılan verinin niteliği, işlenme amacı ve süresi, aktarımın yapılacağı üçüncü ülkede yürürlükteki hukuk kuralları, o ülkede uygulanan güvenlik önlemleri gibi hususlar “*yeterli düzeyde koruma*” değerlendirmesi bakımından özel olarak önem taşımaktadır¹⁷⁵.

Direktif'in “*Denetim Otoritesi*” başlıklı 28. maddesine de değinmekte fayda vardır. Zira bu maddede üye devletlere, ülke sınırları içerisinde kişisel verilerin korunmasına ilişkin hükümlerin uygulamasını takip etmek ve denetlemekle sorumlu bir veya birden çok, bağımsız veri koruma otoritesinin kurulması yükümlülüğü getirilmektedir¹⁷⁶.

Direktif'in 29. maddesinde kişisel verilerin işlenmesine ilişkin olarak bireylerin korunması hakkında bir Çalışma Grubunun, Direktif ile kurulduğu belirtilmektedir. Çalışma Grubunun görevlerine Direktif'in 30. maddesinde yer verilmektedir. Çalışma Grubu, danışma fonksiyonuna sahip bağımsız bir organ niteliğinde olup, veri koruma alanına ilişkin olarak görüş bildirmektedir¹⁷⁷. Örneğin, Komisyonda ve üçüncü ülkelerdeki veri koruma düzeyi hakkında Komisyon'a görüş bildirmek, Çalışma Grubunun görevleri arasında yer almaktadır.

Avrupa Birliği Direktifleri üye devletlerde doğrudan uygulanamazlar. Üye devletlerin direktifleri kendi iç hukuklarına aktarmaları gerekmektedir. “95/46/EC sayılı Veri Koruma Direktifi”, AB üyesi devletler arasında veri koruma düzenlemelerine ilişkin bir yeknesaklık sağlama amacı taşısa da üye devletlerin bu alanda kendi ulusal hukuklarında yapmış oldukları düzenlemeler birbirinden farklı

¹⁷⁵ Küzeci, Kişisel Verilerin, ss. 192-194.

¹⁷⁶ Başar, s. 178.

¹⁷⁷ Başar, s. 167.

olmaya devam etmiştir. Başka bir ifade ile, bir AB üyesi ülkede veri işleme alanında gerçekleştirilen faaliyet, başka bir AB üyesi ülkedeki özel veri işleme uygulamaları sebebiyle hukuka aykırı olarak kabul edilebilmektedir¹⁷⁸. Bu nedenin de dahil olduğu birtakım nedenler silsilesi içerisinde AB, 95/46/EC sayılı Veri Koruma Direktif’ini kaldırmış, onun yerine “2016/679 sayılı Genel Veri Koruma Tüzüğü” kabul edilmiştir. Son olarak belirtmek gerekir ki, 95/46/EC sayılı Direktif’in kabul edilmesinin ardından “2016/679 sayılı Genel Veri Koruma Tüzüğü’nün” kabul edildiği tarihe kadarki geçen süreçte Avrupa Birliği, veri koruma alanında yaşanan gelişmelerin de etkisiyle birtakım düzenlemeler yapmaya devam etmiştir. 15 Aralık 1997 tarihinde kabul edilen “*Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Özel Hayatın Korunmasına İlişkin 97/66/EC sayılı Direktif*”, 12 Temmuz 2002 tarihinde kabul edilen “*2002/58/EC sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliği Korunmasına İlişkin Direktif*”¹⁷⁹, 15 Mart 2006 tarihinde kabul edilen “*2006/24/EC sayılı İletişim Trafik Verilerinin Saklanması Direktifi*” bu düzenlemelere örnek olarak gösterilebilir¹⁸⁰.

(3) Genel Veri Koruma Tüzüğü

Teknolojide yaşanan devrimsel nitelikteki gelişmelerin etkisiyle kişisel verilerin korunması alanında ortaya çıkan yeni sorunlar, 95/46/EC sayılı Direktif’in bu yeni sorunlarla mücadele etmedeki yetersizliği ve yine Direktif’in beklentinin aksine uzun yıllar geçmesine rağmen AB üyesi ülkelerde yeknesak bir veri koruma standardı oluşturamaması, Avrupa Birliği’ni kişisel verilerin daha etkin korunabilmesini sağlamak üzere yeni bir düzenleme yapmaya yönlendirmiştir. Konuya ilişkin 2009 yılında başlayan çalışmalar zaman içerisinde olgunlaşmış ve 2016/679 sayılı Genel Veri Koruma Tüzüğü, Avrupa Parlamentosu ve Avrupa Konseyi tarafından 27 Nisan 2016 tarihinde kabul edilmiştir. Tüzüğün uygulanmaya başlaması bakımından iki senelik bir geçiş süreci öngörülmüş ve Tüzük 25.05.2018’den itibaren uygulanmak üzere 24 Mayıs 2016’da yürürlüğe girmiştir¹⁸¹.

¹⁷⁸ Dülger, Kişisel Veriler Hukuku, s. 59.

¹⁷⁹ Hayrunnisa Özdemir, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin Yayıncılık, Ankara, 2009, ss. 34,36.

¹⁸⁰ Korkmaz, Kişisel Veriler, s. 230.

¹⁸¹ Göçmen Uyarer, ss. 65-67; Küzeci, Kişisel Verilerin, s. 221; Dülger, Kişisel Veriler Hukuku, s. 65.

Tüzüğün hazırlanma sürecinde iki temel soruna yanıt aranarak çalışmalara yön verildiği söylenebilir. İlk sorun, 95/46/EC sayılı Direktif'in süratle gelişen teknoloji karşısında yetersiz kalması; ikinci sorun Avrupa Birliği ve Birlik üyesi ülkelerin mevzuatında bireysel mahremiyetin etkili bir biçimde korunamamasıdır. Gerçekten de Direktif'in uygulandığı süreçte, amaçlananın aksine Birlik üyesi ülkelerin mevzuatlarında veri korumaya ilişkin düzenlemeler bakımından farklılıklar oluşmuş ve hatta veri aktarımlarında veri koruma seviyesi daha düşük devletler üzerinden veri aktarımlarının gerçekleştirilmesi gibi fiili durumlar yaşanmaya başlamıştır¹⁸². Bu ise kişisel verilerin korunmasını temel insan haklarından bir tanesi olarak gören ve köklerini de insan hak ve özgürlüklerine dayandıran Avrupa Birliği için kabul edilebilir değildir. Ayrıca yukarıda izaha konu edilen problemler, Birlik içerisinde ticari engellerin kaldırılması suretiyle nihai olarak oluşturulması hedeflenen tek pazarın gerçekleştirilme sürecini de baltalar niteliktedir¹⁸³. Tüm bu sebeplerle Avrupa Birliği'nde, 95/46/EC sayılı Direktif'i kaldıran ve kişisel verilerin korunması alanında Birlik üyesi ülkeler arasında bir yeknesaklık oluşturacak 2016/679 sayılı Genel Veri Koruma Tüzüğü uygulanmaya konmuştur. Bununla birlikte Tüzük, yaşanan teknolojik gelişmeler karşısında kişisel verilerin korunması hakkının temini bakımından da aşağıda detaylıca incelenecek önemli düzenlemeler barındırmaktadır.

“2016/679 sayılı Genel Veri Koruma Tüzüğü” ile gelen yeniliklerden ilki metnin türüne ilişkindir. Zira Avrupa Birliği mevzuatında tüzükler ile direktifler farklı etkilere sahip hukuki metinler olarak karşımıza çıkmaktadır. Direktifler, belirli konularda, belirli ilke ve amaçlar doğrultusunda üye devletlerin mevzuatını birbirine yaklaştırmak üzere düzenlenmektedir. Üye devletlerde Direktif hükümleri doğrudan uygulama alanı bulmaz, üye devletlerin Direktif hükümlerini kendi mevzuatlarına ayrıca aktarmaları gerekmektedir. Avrupa Birliği nezdinde yürürlüğe konulan Tüzükler bakımından ise üye devletlerin Tüzük hükümlerini ayrıca kendi iç hukuklarına aktarmalarına gerek kalmamaktadır. Çünkü Tüzük hükümleri genel kapsama sahip olup, Birlik üyesi ülkelerde doğrudan uygulanabilir niteliktedir.

¹⁸² Başar, s. 180.

¹⁸³ İpek Çimen Bulut, “Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları”, *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, Cilt:20, Sayı:2, 2020, s. 129.

Tüzükler, Avrupa Birliği'nde yürürlüğe girmeleri ile tüm üye devletler bakımından bağlayıcı hale gelmektedirler¹⁸⁴. Hiç şüphesiz, yeni düzenlemenin Tüzük şeklinde oluşturulması Avrupa Birliği tarafından özellikle tercih edilmiş bir yöntemdir. Zira Direktif'in Birlik üyesi ülkelerin mevzuatları arasında uyumlaştırmayı sağlayamamasının en önemli sebeplerinden bir tanesi de üye ülkelerde doğrudan uygulama alanı bulamıyor olmasıydı. Ancak Genel Veri Koruma Tüzüğü ile bu sorun tamamen ortadan kalkmıştır. Tüzük uygulanmaya konduğu tarih itibarıyla bütün üye ülkeleri hukuken bağlamaktadır.

“2016/679 sayılı Genel Veri Koruma Tüzüğü'nün”, Direktifle kıyaslandığında çok önemli yenilikler getirdiği görülmektedir. Özellikle daha önce Avrupa Birliği Adalet Divanı kararlarında yer vermeye başlayan “*unutulma hakkı*”na Tüzük çerçevesinde yer verilmesi, geliştirilen teknolojilerin daha geliştirilme aşamasında veri koruma ilke ve uygulamalarına uygun bir şekilde geliştirilmesine özen gösterilmesi hususu (*privacy by default - privacy by design*), veri koruma otoritelerinin güçlendirilmesi, veri ihlalleri söz konusu olduğunda ihlal bildiriminde bulunma yükümlülüğü, veri sahiplerinin veri sorumlusundan işlenmiş verilerinin bir kopyasını isteyebilmesi ve bununla birlikte ayrıca elektronik ortamda başka bir sisteme aktarabilmesi (*data portability*)¹⁸⁵, IP adresleri ve site çerezlerinin kişiyi belirlenebilir kılan çevrimiçi veriler olması sebebiyle kişisel veri olarak kabul edilmesi¹⁸⁶ öne çıkan yeniliklerin bazılarıdır.

Tüzüğün birinci bölümünün “*Konu ve hedefler*” başlıklı 1. maddesinin ilk fıkrasında, Tüzük ile gerçek kişilerin kişisel verilerinin işlenmesiyle ilgili olarak korunmasına ve kişisel verilerin serbest dolaşımına ilişkin kuralların düzenlendiği ifade edilmiştir. İkinci fıkrasında ise Tüzüğün, gerçek kişilerin temel hak ve özgürlüklerini, bilhassa da kişisel verilerin korunması hakkını koruduğu vurgulanmıştır. Maddenin üçüncü ve son fıkrasında, Birlik içerisinde serbest veri dolaşımının teminine ilişkin ifadeler yer almaktadır. Hükme göre, Birlik içerisinde kişisel verilerin serbest dolaşımı, Birlik üyesi ülkeler tarafından gerçek kişilerin kişisel verilerinin korunmasıyla bağlantılı sebepler öne sürülerek kısıtlanamayacaktır. Görüldüğü üzere

¹⁸⁴ Murat Volkan Dülger, “Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması”, **Yaşar Hukuk Dergisi**, Cilt:1, Sayı:2, 2019, (Genel Veri Koruma Tüzüğü Bağlamında), s. 84.

¹⁸⁵ Küzeci, *Kişisel Verilerin*, s. 225; Göçmen Uyarer, s. 67.

¹⁸⁶ Dülger, *Genel Veri Koruma Tüzüğü Bağlamında*, s. 87.

Genel Veri Koruma Tüzüğü, Tüzüğün konu ve amaçlarını düzenlediği hükümde, 95/46/EC sayılı Direktif ile paralel nitelikte bir düzenleme getirmektedir. Nitekim tam da burada ifade etmek gerekir ki, her ne kadar Genel Veri Koruma Tüzüğü çok sayıda önemli yenilik getirmiş olsa da 95/46/EC sayılı Direktif'in düzenlemelerine paralel olan yahut düzenlemelerin güçlendirilmiş olduğu birçok hükmü de ayrıca bünyesinde barındırmaktadır¹⁸⁷.

Tüzüğün “*Kapsam*” başlıklı 2. maddesinin ilk fıkrasında ise yine 95/46/EC sayılı Direktif'e paralel bir biçimde Tüzük hükümlerinin, kişisel verilerin tamamen veya kısmen otomatik araçlarla işlenmesine ve otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya oluşturması amaçlanan araçlarla işlenmesine uygulanacağı belirtilmiştir. Görüldüğü üzere Tüzük, tıpkı Direktif'de olduğu gibi veri işleme usulünün kapsamını oldukça geniş tutmak suretiyle hemen hemen bütün kişisel verileri koruma altına almayı hedeflemiştir. Maddenin ikinci fıkrasında Tüzük hükümlerinin uygulanma alanına getirilen istisnalar ifade edilmektedir. Hüküm uyarınca, birlik hukukuna girmeyen bir faaliyet esnasında, üye devletler tarafından Avrupa Birliği Antlaşması'nın V. başlığının 2. bölümü kapsamına giren faaliyetler gerçekleştirilirken, tamamen kişisel veya ev yaşamı içerisinde gerçek bir kişinin gerçekleştirdiği veri işleme faaliyetlerinde, kamu güvenliğinin korunması ve kamu güvenliğine yönelik tehditlerin önlenmesi de dahil olmak üzere, suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai yaptırımların infazı amacıyla kişisel verilerin işlenmesine yönelik olarak yetkili makamlar tarafından gerçekleştirilen faaliyetler bakımından Tüzük hükümleri uygulanmayacaktır.

Tüzüğün “*Bölgesel Kapsam*” başlıklı 3. maddesinde Tüzüğün yer bakımından uygulanmasına ilişkin düzenlemeler yer almaktadır. Madde hükümleri incelendiğinde Tüzüğün uygulama bulacağı yerlerin kapsamının oldukça geniş tutulduğu dikkatlerden kaçmamaktadır¹⁸⁸. Maddenin birinci fıkrasında Tüzüğün, işleme faaliyetinin Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın Birlik içerisindeki bir veri sorumlusu veya veri işleyenin faaliyetleri bağlamında kişisel verilerin işlenmesine uygulanacağı ifade edilmiştir. Bu çerçevede örneğin, Birlik üyesi ülkelerden birinde kurulmuş ve faaliyet yürüten bir veri sorumlusunun, Birlik üyesi olmayan bir başka

¹⁸⁷ Başar, s. 182.

¹⁸⁸ Korkmaz, Kişisel Veriler, s. 240.

ülkede gerçekleştirmiş olduğu veri işleme faaliyetlerine Genel Veri Koruma Tüzüğü uygulanabilecektir¹⁸⁹. Yine aynı maddenin ikinci fıkrasında, Genel Veri Koruma Tüzüğü ile getirilen önemli yeniliklerden bir diğeri bulunmaktadır. Hükümde Tüzüğün uygulama alanının, yalnızca Avrupa Birliği içerisinde gerçekleştirilen veri işleme faaliyetleriyle sınırlı olmadığı ifade edilmektedir. Anlatım kolaylığı sağlaması açısından öncelikle hükme doğrudan yer vermek ve ardından hükümde sayılan durumlara açıklık getirmek daha faydalı olacaktır. Söz konusu hüküm, *“Bu tüzük, işleme faaliyetlerinin aşağıdaki hususlarla alakası olması durumunda, Birlik içerisinde bulunan veri sahiplerinin kişisel verilerinin Birlik içerisinde kurulu olmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesine uygulanır: (a) Veri sahibine bir ödeme yapılmasına gerek olup olmadığına bakılmaksızın, Birlik içerisindeki söz konusu veri sahiplerine mal ya da hizmetlerin sunulması veya (b) Davranışları birlik içerisinde gerçekleştiği ölçüde, davranışlarının izlenmesi”* şeklindedir¹⁹⁰. Hükümde özetle, veri sorumlusu veya veri işleyenlerin AB dışında faaliyet gösteriyor olmaları halinde bile belli şartlar var ise Genel Veri Koruma Tüzüğü’nün uygulama alanı içerisinde kalabilecekleri ifade edilmektedir. Söz konusu şartlardan ilki, veri sorumlusu veya veri işleyen AB dışında merkezi bulunsa ve faaliyet alanı AB dışında olsa dahi Birlik sınırları içerisinde mal ve hizmet sunuyor ve bu çerçevede Birlik topraklarında bulunan kişilerin verilerini işliyor olmasıdır. Bu halde ilgili veri sorumlusu/veri işleyen Genel Veri Koruma Tüzüğü ile muhatap olacaktır. Üstelik veri sahiplerine bir ödemede bulunup bulunulmadığı bir önem teşkil etmemektedir. AB dışında kurulu veri sorumlusu/veri işleyen veri işleme faaliyetlerinin Tüzük kapsamında değerlendirilebilmesi için ikinci şart ise, Birlik toprakları içerisinde gerçekleştiği ölçüde veri sahiplerinin davranışlarının AB dışında bulunan veri sorumluları/veri işleyenler tarafından izlenmesi halidir. Bu hükümle özellikle AB dışında kurulu sosyal medya şirketleri, arama motorları şirketleri ve diğer şirketlerin birtakım teknolojik imkanlardan ve AB müşteri tabanlarından faydalanmak suretiyle gerçekleştirdikleri faaliyetlerde, veri koruma prensiplerine uygun olarak hareket etmelerini sağlamak hedeflenmiştir¹⁹¹. Tüzüğün 3.maddesinin üçüncü ve son fıkrasında ise Tüzük hükümlerinin, Birlik içerisinde bulunmayan ancak uluslararası

¹⁸⁹ Dülger, Genel Veri Koruma Tüzüğü Bağlamında, s. 96.

¹⁹⁰ Genel Veri Koruma Tüzüğü, m. 3/2.

¹⁹¹ Dülger, Genel Veri Koruma Tüzüğü Bağlamında, ss. 96,97.

kamu hukuku vasıtasıyla Birlik üyesi devletlerden birinin hukukunun uygulandığı bir yerde kurulu bulunan veri sorumlusunun gerçekleştirdiği kişisel veri işleme faaliyetlerine uygulanabileceği ifade edilmiştir.

Tüzüğün “*Tanımlar*” başlıklı 4. maddesinde kişisel veri, işleme faaliyeti, işleme kısıtlaması, kontrolör, veri sahibinin rızası, genetik veri gibi birçok kavramın tanımına yer verilmiştir. Tüzükte kişisel veri kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi olarak belirtilmiştir. Yine kişisel verinin tanımının yapıldığı hükmün devamında belirlenebilir gerçek kişinin, doğrudan veya dolaylı olarak, özellikle kimlik numarası, isim, konum verileri, çevrimiçi tanımlayıcı ya da söz konusu gerçek kişinin fizyolojik, genetik, fiziksel, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir yahut daha fazla sayıda etkene atıfta bulunulmak suretiyle tanımlanabilen kişi olduğu ifade edilmiştir. İşleme faaliyeti ise aynı maddede, otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri kümeleri üzerinde gerçekleştirilen, toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, hizalama ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisi olarak ifade edilmiştir. Direktif hükümleri ile karşılaştırıldığında Tüzüğün, kişisel veri kavramına ve veri işleme faaliyetine getirdiği tanımlamaların büyük ölçüde benzerlik taşıdığı görülmektedir¹⁹². Tüzüğün 4. maddesinde yer verilen kavramlardan kontrolör ve işleyici kavramlarına da özel olarak değinmek ve aralarındaki farkı izah etmekte yarar vardır. Zira bu sıfatları taşıyan kişilerin Genel Veri Koruma Tüzüğü’nün getirdiği yeni düzenlemeler bağlamında sorumlulukları bir hayli arttırılmıştır¹⁹³. Kontrolör kavramı hükümde, “*Kişisel verilerin işleme amaçlarını ve yöntemlerini tek başına veya başkalarıyla birlikte belirleyen gerçek veya tüzel kişi, kamu otoritesi, kurum veya diğer organ anlamına gelir.*” şeklinde belirtilmiştir. İşleyici ise, “*Kontrolör adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu otoritesi, kurum veya diğer organ anlamına gelir*” Tüzükte veri kontrolörü olarak belirtilen kavram hukukumuzda veri sorumlusu olarak da adlandırılmaktadır.

¹⁹² Başar, s. 186.

¹⁹³ Çimen Bulut, s. 130.

Tüzükte kişisel verilerin işlenmesi faaliyetlerinin hukuka uygun olabilmesi için gerekli şartlar 6. maddede yer almaktadır. Madde hükmü detaylı bir şekilde incelendiğinde, Direktif'te yer alan hukuka uygunluk sebeplerinin ufak bir farkla, benimsendiği görülmektedir. Bu farklılık ise Tüzük ile artık yalnızca veri sahibinin yaşamsal çıkarlarının korunması için değil, bir başka gerçek kişinin hayati menfaatlerinin korunması bakımından da veri işleme ihtiyacının doğması durumunda, o işleme faaliyetinin hukuka uygun kabul edileceği düzenlemesine yer verilmesidir¹⁹⁴.

Tüzük, veri sahibinin rızasına dayalı veri işleme faaliyetlerinde rızanın koşullarına da detaylı bir şekilde değinmiştir. Nitekim Tüzüğün bu konudaki 7. maddesi, Tüzüğün veri sahibinin rızasına attığı önemi göstermekte, rızanın alınması koşullarında veri sahibini güçlendiren düzenlemelere yer vermektedir. Bu çerçevede rıza talebinin açık, anlaşılır ve kişisel verinin işlenme amacını bildiren basit bir dil kullanılmak suretiyle veri sahibine iletilmesi gerektiği, rızanın geri çekilmesinin mümkün olduğu öne çıkan başlıca hususlardır¹⁹⁵.

Tüzük kapsamında, veri kontrolörü ve veri işleyicisinin sorumluluklarının genişletildiğini daha önce belirtmiştik. Tüzüğün 32. maddesi, kişisel veri işleme süreçlerinde, veri kontrolörü ve veri işleyicisinin bir veri ihlali ortaya çıkmadan önce önleyici tedbirler alınmasına ve veri güvenliği faaliyetlerini makul seviyede tutmasına ilişkin sorumluluklarını düzenlemektedir. Burada özellikle alınması gerekli teknik ve örgütsel tedbirler bakımından veri işleyicisinin de veri kontrolörü ile birlikte sorumlu tutulması öne çıkan hususlardan bir tanesidir. Yine aynı maddede, veri kontrolörü ve veri işleyicisinin kişisel verilerin işlenmesi sürecinin güvenliğini sağlayabilmesi adına alacağı takma ad kullanılması ve şifreleme yapılması, veri işlemeye ilişkin sistem ve hizmetlerin ihlal girişimlerine karşı, gizliliğinin, bütünlüğünün, kullanılabilirliğinin ve dayanıklılığının sürekliliğinin sağlanması gibi uygulamalara değinilmektedir¹⁹⁶.

Genel Veri Koruma Tüzüğü, kişisel verilerin korunmasının etkili bir şekilde sağlanabilmesi bakımından 77-84. maddeleri arasında yaptırım mekanizmalarını düzenlemektedir. Söz konusu hükümler incelendiğinde, kişisel verilerin işlenmesine ilişkin olarak meydana gelen hukuka aykırılık hallerinde veri işleyen ile veri sorumlusunun yükümlülüklerinin eşit düzeylere getirildiği, veri ihlali durumunda

¹⁹⁴ Başar, s. 189.

¹⁹⁵ Korkmaz, Kişisel Veriler, ss. 240, 241.

¹⁹⁶ Çimen Bulut, s. 130.

uygulanacak idari para cezalarının miktarlarının arttırıldığı, içerik ve kapsamlarının oldukça genişletildiği görülmektedir. Bunun yanında, bağımsız olmalarına özellikle vurgu yapılan denetim makamlarına veri sahibi tarafından yapılacak şikayetlerde veri sahibinin denetim makamları tarafından sürece ilişkin olarak bilgilendirilmesi gerektiği, denetim makamlarınca şikayetin ele alınmaması veya süreç hakkında veri sahibinin bilgilendirilmemesi hallerinde veri sahibinin etkili hukuk yollarına başvurabileceği, yine denetim makamlarının şikayet üzerine vermiş olduğu kararlara karşı da veri sahibinin denetim makamının bulunduğu üye devlet mahkemelerinde yargısal yollara başvurma hakkının bulunduğu, kişisel verilerinin korunması hakkı ihlal edilen veri sahibinin bu durumdan ötürü uğramış olduğu maddi-manevi zarar var ise veri sorumlusu ve veri işleyene karşı tazminat isteminde bulunabileceği, veri sorumlusu ve veri işleyenin Tüzük’den doğan sorumluluklarına uygun hareket etmiş olmaları ve ihlalde kusurlarının bulunmadığını ispat etmeleri halinde tazminat yükümlülüklerinin doğmayacağı gibi düzenlemelere Tüzük’de yer verilmiştir¹⁹⁷.

Hiç şüphesiz ki, Tüzük’de sayılabilecek daha birçok önemli düzenleme ve yenilik bulunmaktadır. Örneğin, Tüzükte düzenlenen “*Unutulma Hakkı*” da bu kapsamda yer almaktadır.

Bilişim teknolojilerinde yaşanan gelişmeler, kişisel verilerin işlenmesi ve aktarılmasını kolaylaştırdığı gibi bu işleme ve aktarımlara bağlı olarak kişisel verilerin bir daha ortadan kaldırılmasının güçleşmesi gibi bir sonucun doğmasına da sebebiyet vermiştir. Bunun karşısında insan onuruna yaraşır bir yaşam çerçevesinde bireyin başkalarının gözetimi altında hissetmeden, özgürce bir yaşam sürdürebilmesi, bireysel özerkliğini gerçekleştirebilmesi gerekmektedir. İşte tüm bu süreç “*unutulma hakkı*” na duyulan ihtiyacı ortaya koymuştur¹⁹⁸. Unutulma hakkının tarihine kısaca değinmek gerekirse, bu kavrama ilişkin çalışmaların 2010’lu yıllarda Avrupa’da başladığı görülmektedir. Özellikle bu konudaki tartışmaların yürürlükten kalkan 95/46/EC sayılı Tüzük için planlanan revizyon hareketi kapsamında yoğunlaştığı söylenebilir. Nitekim 2010 yılında Komisyon, sunmuş olduğu teklif ile bireylerin internet ortamında yer alan ve artık işletilmesi yahut tutulmasına gerek duyulmayacak nitelikteki kişisel verilerini

¹⁹⁷ Çimen Bulut, s. 135-138.

¹⁹⁸ Aydın Akgül, “Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı”, **TBB Dergisi**, Sayı: 116, 2016, (Unutulma Hakkı), s. 15.

sildirebilmesi doğrultusunda unutulma hakkı olarak ifade ettiğimiz hakkın kabulüne öncülük etmiştir¹⁹⁹. Yine Avrupa Birliği Komisyonu 95/46/EC sayılı Direktif’de köklü değişiklikler yapılmasını içeren bir öneri hazırlamış ve bunu 25 Ocak 2012 tarihinde yayımlamıştır. Komisyon adına öneri ile ilgili açıklamalarda bulunan, dönemin Komisyon Başkan Yardımcısı Viviane Reading, Avrupa’da 17 yıl önce internet kullanımının %1’lerde olduğunu ifade etmiş, bugün ise verilerin saniyeler içerisinde çok uzak noktalara aktarılabilirdiğini ve söz konusu öneri ile sektörün sağlıklı bir şekilde büyümesinin yanında bireylerin de dijital ortamda kişisel verilerinin daha etkili bir biçimde korunmasının amaçlandığını belirtmiştir²⁰⁰. Unutulma hakkının tarihsel gelişimi içerisinde özel öneme sahip gelişmelerden bir diğeri ise 13 Mayıs 2014 tarihinde Avrupa Birliği Adalet Divanı tarafından verilen C-131/12 sayılı Google İspanya kararıdır. Karara konu olayda, Mario Costejo Gonzales isimli İspanya vatandaşı, 1998 yılında sosyal güvenlik borçları nedeniyle satışa çıkarılan evinin bir İspanyol gazetesinde yayımlanan açık artırma ilanına, olayın üzerinden yıllar geçmesine ve ilana sebep olan hususların sona ermesine rağmen halen, Google arama motorları üzerinden erişilebilmesi durumunun, özel hayatın gizliliği hakkının ihlaline sebebiyet verdiğini ileri sürmüştür²⁰¹. Mario Costejo Gonzales’e göre, ismi ile Google’da yapılan aramalarda halen bu ilanın çıkıyor olması onun saygınlığına zarar vermektedir. Bu sebeplerle Gonzales, Google’dan bu kişisel verilerinin kaldırılmasını talep etmektedir. ABAD önüne gelen bu olaya ilişkin vermiş olduğu kararda özetle, Google’ın kişisel veri işleme faaliyeti gerçekleştirdiğinde şüphe bulunmadığını, aynı zamanda Google’ın veri kontrolörü (veri sorumlusu) sıfatını taşıdığını ve bu sebeple AB hukuku çerçevesindeki sorumluluklardan kaçınamayacağını, arama motorlarının bir yapılandırma işlemi suretiyle ekrana getirdiği sonuçların söz konusu bilgiler doğru olsa dahi üzerinden bir süre geçmesinin ardından toplanma ve işleme amaçlarından kopar hale geldiğini, bu nedenle söz konusu verilerin arama motorları sonuçlarında yer almasının bir süre sonra verilerin işleme amacı ile ilgisiz veya ölçüsüz hale dönüşebileceğini, ayrıca tüm bunların yanında olaydaki verilerin bireyin özel yaşamının gizliliği, şirketin ekonomik çıkarları ve toplumun bilgiye erişme hakkı

¹⁹⁹ Akgül, (Unutulma Hakkı), ss. 23-25.

²⁰⁰ Tamer Soysal, Unutulma Hakkının Avrupa Birliği’nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi, **Uyuşmazlık Mahkemesi Dergisi**, Sayı: 13, 2019, s. 350.

²⁰¹ Küzeci, Kişisel Verilerin, s. 257

çerçevesinde değerlendirilmesi gerektiğini, şirketin ekonomik menfaatlerinin bireyin özel yaşamının gizliliği hakkı karşısında üstün tutulamayacağını, özellikle toplumun bilgi edinme hakkına ilişkin özel bir çıkar söz konusu değilse özel yaşamın gizliliği hakkının ticari çıkarlar karşısında korunması gerektiğini ifade etmiştir²⁰².

Geçen sürede ve geline noktada ise, her ne kadar o güne kadar kendisinden önceki düzenlemelerde münhasır bir hak olarak kendisine yer verilmemiş olsa da²⁰³ unutulma hakkı, 95/46/EC sayılı Direktif'i ilga eden Genel Veri Koruma Tüzüğü'nün 17. maddesinde doğrudan düzenlenmiştir. “*Silme hakkı (unutulma hakkı)*” başlığını taşıyan 17. maddenin ilk fıkrasında veri sahibinin, veri sorumlusundan kendisi ile ilgili verilerin gecikmeksizin silinmesini talep etme hakkına sahip olduğu ifade edilmiştir. Hükmün devamında ise, birazdan sıralanacak sebeplerin somut olayda bulunması halinde veri sorumlusunun yine herhangi bir gecikme olmaksızın kişisel verileri silme yükümlülüğü bulunduğu belirtilmiştir. Bu sebepler Tüzük hükmünde şu şekilde ifade edilmiştir: kişisel verilerin toplanma veya başka bir şekilde işleme amaçlarıyla ilgili olarak artık gerekli olmaması, veri sahibi madde 6(1)'in (a) bendi veya 9(2)'nin (a) bendine göre işlemenin dayandığı onayı geri çeker ve işleme için başka yasal bir dayanak kalmazsa, veri sahibi madde 21(1) uyarınca işlemeye itiraz eder ve işleme için ağır basan meşru bir gerekçe bulunmazsa veya veri sahibi madde 21(2) uyarınca itiraz ederse, kişisel veriler kanuna aykırı olarak işlenmişse, kişisel verilerin veri sorumlusunun tabi olduğu Birlik ve üye devlet ulusal hukukundaki yasal bir yükümlülüğe uygun olması için silinmesinin gerekmesi halinde ve kişisel verilerin madde 8(1)'de atıfta bulunulan bilgi toplumu hizmetlerinin sunulması kapsamında toplanması durumlarında kişisel verileri veri sorumlusu silmek zorundadır. Tüzüğün 17. maddesinin 2. fıkrası, veri sorumlusunun, kişisel verileri kamuya açıkladığı ve 1. fıkrada sayılan sebeplerle silmekle yükümlü olduğu durumlarda, mevcut teknoloji ve uygulama maliyetini dikkate alarak, söz konusu kişisel verilere ilişkin her türlü bağlantının veya bu verilerin her türlü kopyasının ya da çoğaltmasının silinmesi konusunda söz konusu kişisel verileri işleyen diğer veri sorumlularına bilgilendirmede bulunma yükümlülüğü getirmiştir. 17. maddenin son fıkrası olan 3. fıkrasında ise işleme faaliyetinin amacının, ifade ve bilgi edinme hakkının kullanılması, veri

²⁰² Soysal, ss. 352, 353; Küzeci, Kişisel Verilerin, s. 258.

²⁰³ Dülger, Genel Veri Koruma Tüzüğü Bağlamında, s. 155; 95/46/EC sayılı Direktif.

sorumlusunun tabi olduđu Birlik hukuku veya üye devlet ulusal hukuku tarafından işlemeyi gerektiren yasal bir yükümlülüğe uygunluk veya kamu yararı için yürütülen bir görevin ifası ya da veri sorumlusuna verilen resmi yetkinin kullanılması için verilerin işlenmesi, madde 9(2)'nin (h) ve (i) bentleri ve ayrıca madde 9(3) uyarınca halk sağlığı alanındaki kamu yararı nedenleriyle verilerin işlenmesi, 1. fıkrada atıfta bulunulan hakkın, söz konusu amaçlara ulaşılmasını imkansız kılacağı veya ciddi şekilde bozacağı ölçüde madde 89(1) uyarınca kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları veya istatistiksel amaçlar için verilerin işlenmesi ve son olarak yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması amaçlarıyla verilerin işlenmesi olduđu durumlarda 1. ve 2. fıkra hükümlerinin uygulanmayacağını düzenlemiştir. Başka bir deyişle, 17. maddenin 3. fıkrasında düzenlenen amaçlarla gerçekleştirilen veri işleme faaliyetlerinde unutulma hakkı uygulanmayacaktır²⁰⁴.

3. Türkiye’de Kişisel Verilerin Korunmasına İlişkin Temel Düzenlemeler

a. Genel Olarak

Günümüzde gerek kamuda gerekse özel sektörde kişisel verilere duyulan ihtiyaç bir hayli artmış, yaşanan teknolojik gelişmelerin etkisiyle bireylerin kişisel verilerinin toplanması, saklanması ve aktarılması ise bir hayli kolay hale gelmiştir²⁰⁵. Kişisel verilerin işlenmesi süreçlerinin bu denli kolaylaşmış olması, bireylerin temel hak ve hürriyetlerinin ihlale uğraması riskini beraberinde getirmektedir. Bu risk karşısında bireylerin temel hak ve özgürlüklerinin korunması amacıyla kişisel verilerin korunmasına yönelik uluslararası ve ulusal alanda çeşitli hukuki düzenlemeler yürürlüğe konulmuştur.

Kişisel verilerin korunması, ülkemiz bakımından da bilhassa son senelerde üzerinde sıklıkla durulan ve çeşitli düzenlemeler yapılan konular arasında yer almaktadır. Bu durumun sebebi ise şüphesiz başta Kıta Avrupa’sı olmak üzere dünyanın birçok yerinde konuya ilişkin yaşanan ve yaşanmaya devam eden süratli

²⁰⁴ Başar, s. 195.

²⁰⁵ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, Ankara, 2019, s. 11.

gelişmelerdir. Zira Kıta Avrupası’nda kişisel verilerin korunması hakkı bireyin kişilik hakkının bir uzantısı şeklinde görülmüş ve bu çerçevede kişilerin mahremiyet hakkı ile birlikte temel hak ve özgürlüklerinin korunması hedeflenmiştir²⁰⁶. Kıta Avrupası’nda kişisel verilerin korunmasına yönelik ulusal ve uluslararası birçok düzenleme yapılmıştır. Ülkemiz, bu düzenlemelerden biri olan Avrupa Konseyi’nin 108 sayılı Sözleşmesini ilk imzalayan devletlerdendir. Ancak hal böyle olmasına rağmen uzun yıllar Türk hukuk sisteminde kişisel verilerin korunmasına yönelik kapsamlı düzenlemeler gerçekleştirilememiştir.

Teknolojide yaşanan değişim ile kişisel verilerin korunması bakımından doğan tehlikelerin boyutları ve bunun yanında ülkemizin Avrupa ülkeleri ile olan ilişkileri, Türk hukuk sisteminde kişisel verilerin başta Anayasal olmak üzere çeşitli hukuki düzenlemelerle güvence altına alınması gerekliliğini doğurmuştur²⁰⁷. Bu doğrultuda ülkemizde, normlar hiyerarşisinin en tepesinde yer alan Anayasada değişiklik yapmak suretiyle kişisel verilerin korunmasına yönelik kapsamlı adımlar atılmaya başlanmıştır. 1982 Anayasası’nda 2010 yılında gerçekleştirilen değişiklik ile “*Özel Hayatın Gizliliği*” başlıklı 20. maddenin 3. fıkrasına “*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*” hükmü eklenmiştir. Böylelikle kişisel verilerin korunması hakkı ülkemizde Anayasal bir hak olarak güvence altına alınmıştır.

Ülkemizde yasal düzlemde ise kişisel verilerin korunması kanunu çıkartılmasına yönelik çeşitli dönemlerde girişimlerde bulunulmuştur. Bu girişimlerin temel amaçlarından bir tanesi de özellikle tarafı olunan 108 sayılı Sözleşme ve o dönemde Avrupa Birliği’nin başta 95/46/EC sayılı Direktif’i olmak üzere sair mevzuatına uyum sağlamaktır. Söz konusu girişimler ancak 24/03/2016 tarihinde TBMM Genel Kurulu’nda kabul edilerek kanunlaşan tasarı ile sonuç vermiş ve 07/04/2016 tarihinde “*6698 sayılı Kişisel Verilerin Korunması Kanunu*” Resmi

²⁰⁶ Aksoy, s. 56.

²⁰⁷ Dülger, Kişisel Veriler Hukuku, s. 69.

Gazete’de yayımlanarak yürürlüğe girmiştir²⁰⁸. 6698 sayılı Kişisel Verilerin Korunması Kanunu ile ilgili detaylı açıklamalara, çalışmanın devamında ayrı bir başlık altında değinilecektir.

b. Anayasamız

Ülkemiz kişisel verilerin korunmasına ilişkin uluslararası alandaki gelişmeleri takip etmektedir. Türkiye, Avrupa Konseyi’nin 1981 tarihli ve 108 sayılı “*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunması Sözleşmesi*”ni imzalayan devletler arasında yer almaktadır²⁰⁹. Türkiye Cumhuriyeti Anayasası’nda 2010 yılında gerçekleştirilen değişiklik ile kişisel verilerin korunmasını isteme hakkına yer verilmiştir. Ancak bu durum 2010 yılından önce kişisel verilerinin korunmasının Anayasal bir temeli bulunmadığı anlamına gelmemektedir²¹⁰. Zira kişisel verilerin korunması hakkının birçok temel hak ve özgürlükle yakından ilişkili olması sebebiyle Anayasa’da düzenlenen temel hak ve özgürlükler çerçevesinde kişisel verilerin korunması mümkün olabilmekteydi. Bu haklara örnek olarak, özel hayatın gizliliği, kişinin dokunulmazlığı, maddi ve manevi varlığı, düşünce ve kanaat özgürlüğü verilebilir²¹¹. Anayasamızın “*Özel Hayatın Gizliliği*” başlıklı 20. maddesinin 3. fıkrasına getirilen düzenleme ile kişisel verilerin korunması hakkı ülkemizde açıkça Anayasal temele kavuşturulmuştur. İlgili hüküm uyarınca “*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*”. Hüküm incelendiğinde, hakkın süjesi olarak herkesin gösterildiği ve hakkın içeriği konusunda birtakım açıklamalara yer verildiği görülmektedir. Hükümde dikkat çeken önemli bir husus, bireyin kişisel verilerinin geleceğini belirleme ve bunlar üzerindeki denetimi konusunda sahip olduğu yetkilere

²⁰⁸ Alaattin Bük, **Bilişim Alanında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, Ankara, 2018, s. 74.

²⁰⁹ Doğan, s. 88.

²¹⁰ Küzeci, *Kişisel Verilerin*, s. 318.

²¹¹ Doğan, s. 87.

ilişkin ifadelerdir. Yine söz konusu hükümde kişisel verilerin korunması konusundaki esas ve usullerin kanunla düzenleneceği belirtilmiştir. Başka bir deyişle, kişisel verilerin korunması hakkının kullanılmasının, bu hakkı somutlaştıracak kanuni düzenlemelerin yapılmasına muhtaç olduğu belirtilmektedir²¹². Fakat ne yazık ki, Anayasada öngörülen kanunun yürürlüğe girmesi yaklaşık altı yıl sürmüştür.

c. Kanunlar

(1) 6698 Sayılı Kişisel Verilerin Korunması Kanunu

(i) Genel Olarak

6698 sayılı “*Kişisel Verilerin Korunması Kanunu*” 24 Mart 2016 tarihinde TBMM Genel Kurulunda kabul edilmiş ve 7 Nisan 2016 tarihinde Resmî Gazetede yayımlanarak yürürlüğe girmiştir. Bu yasadan önce de çeşitli kanunlarda kişisel verilerin korunmasına ilişkin hükümler yer almaktaydı. Türk Ceza Kanunu’na 2005 yılında eklenen kişisel verilere karşı işlenen suçlar hakkındaki düzenlemeler bunlara örnek olarak verilebilir²¹³. Ancak konuya ilişkin kapsamlı bir kanunun bulunmayışı söz konusu düzenlemelerdeki teknik terimlerin yorumlanması noktasında tereddüt yaşanabilecek durumlara sebebiyet verebilmekteydi²¹⁴. Nitekim “*Kişisel Verilerin Korunması Kanununun*” tasarı metnindeki “*Genel Gerekçe*” başlıklı bölümde, kanuna duyulan ihtiyacın dayanak noktaları arasında bu durum da ifade edilmiştir. Tasarının genel gerekçesinde özetle, kişisel verilerin gerek kamu gerekse özel sektörde sıklıkla kullanıldığı, söz konusu kullanımın her ne kadar kolaylık ve avantajlar sağlasa da bilgilerin istismarı ve bireylerin temel haklarının ihlali riskini de beraberinde taşıdığı, insan haklarının korunması bilincinin gelişmesiyle beraber kişisel verilerin korunmasının öneminin de giderek arttığı, buna karşılık ülkemizde konuyu bütüncül olarak düzenleyen bir kanunun bulunmadığı, yine kişisel verilerin işleme sürecini düzenleyen ve denetleyen bir kurumun da ülkemizde bulunmadığı, tüm bunların

²¹² Çekin, ss. 8,9.

²¹³ Onur Baskın, **Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, Ankara, 2021 s. 39.

²¹⁴ Dülger, *Kişisel Veriler Hukuku*, s. 182.

sonucu olarak kişisel verilerin haksız kullanımından kaynaklı bazı hak ihlallerinin yaşandığı, ceza kanunundaki kişisel verilere ilişkin suç hükümlerinin yorumlanmasında özel bir kanun bulunmaması sebebiyle tereddütlerin olduğu belirtilmiştir. Ayrıca yine genel gerekçe bölümünün devamında, uluslararası alanda güvenlik birimleri arasındaki bilgi alışverişi ve işbirliğinin etkin bir şekilde sağlanabilmesi, sağlık kuruluşlarında işlenen özel nitelikli verilerin korunması noktasında yaşanan zafiyetlerin AİHM önünde ülkemiz aleyhine özel hayatın gizliliğinin ihlali kararlarına konu olması, AB’ye üyelik sürecinin gereklilikleri ve veri aktarımlarının doğurduğu sorunların ekonomik alandaki olumsuz etkilerinin ortadan kaldırılmak istenmesi gibi sebepler, Kişisel Verilerin Korunması Kanununa duyulan ihtiyaca dayanak teşkil eden sebepler arasında sayılmıştır²¹⁵.

(ii) 6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı

“6698 sayılı Kişisel Verilerin Korunması Kanunu’nun” 1. maddesinde Kanunun amacı düzenlenmektedir. Hükümde kanun ile amaçlananın başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin korunması ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlenmesi olduğu belirtilmiştir. Hükümden açıkça anlaşıldığı üzere Kanunun temel hedefi hak ve özgürlüklerin koruma altına alınmasıdır²¹⁶. Nitekim söz konusu düzenlemeye ilişkin tasarı metnin madde gerekçesinde, kanunun amacının kişisel verilerin işlenmesinin disiplin altına alınması, özel hayatın gizliliği, mahremiyet hakkı ve bilgi güvenliği hakkının da içerisinde bulunduğu temel hak ve özgürlüklerin korunması olduğu belirtilmiştir²¹⁷. Gerçekten de veri koruma düzenlemeleri, kişisel verilerin fazla sayıda saldırı ve suistimale maruz kaldığı günümüz koşullarında, bireylerin mahremiyetlerini güvence altına almak açısından son derece önemli ve gereklidir.²¹⁸

²¹⁵ Türkiye Büyük Millet Meclisi, **Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu**, Yasama Dönemi: 26, Yasama Yılı: 1, Sıra Sayısı:117, https://www5.tbmm.gov.tr/develop/owa/tasari_teklif_sd.onerge_bilgileri?kanunlar_sira_n2o=193635 (03.01.2022), ss.4,5.

²¹⁶ Küzeci, *Kişisel Verilerin*, s. 356.

²¹⁷ TBMM, “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 6.

²¹⁸ Öztürk ve diğerleri, s. 18.

(iii) 6698 sayılı Kişisel Verilerin Korunması Kanununun Kapsamı

Kanunun 2. maddesinde kapsamı düzenlenmektedir. Madde metnine göre, “*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 veya tüzel kişiler hakkında uygulanır*”. Kanunun kapsamına, kişisel verileri işlenen gerçek kişilerin girdiği hükümde açıkça belirtildiğinden, tüzel kişilerin verilerinin bu kanunun koruma kapsamı dışında kalacağını ifade etmekte yarar vardır. Hukukumuzda tüzel kişilerin verilerinin korunup korunmayacağına ilişkin tartışmaya da ilgili hüküm ile son verilmiştir. Ayrıca yine madde metninde, veri işleyen olarak kanunun kapsamına, tamamen veya kısmen otomatik yollarla veri işleyen gerçek ve tüzel kişiler ile otomatik veri işleme yöntemi kullanılsa da veri kayıt sisteminin parçası olan verileri işleyen gerçek ve tüzel kişilerin girdiği belirtilmiştir. Otomatik olmayan yöntemlerle işlenen ve veri kayıt sisteminin parçası olmayan kişisel veriler ise 6698 sayılı Kanunun kapsamında yer almamaktadır²¹⁹.

Tamamen otomatik veya kısmen otomatik yollarla veri işleme ayırımında kullanılan kriter, sistemin tamamen kendi başına mı yoksa bir insan müdahalesi ile mi verileri işlediği sorusunun yanıtına göre belirlenmektedir. Günümüzde bilgisayar temelli gerçekleştirilen her türlü veri işleme faaliyetinin, tamamen veya kısmen otomatik yollarla veri işleme yöntemi olduğuna dair bir şüphe bulunmamaktadır. Bu çerçevede, her türlü bilgisayar, gözetleme sistemi, kamera, dron, dijital tarama cihazı, akıllı araç, akıllı ev sistemleri, akıllı saat gibi kişisel veri toplamaya hizmet eden bütün teknolojik ürünler 6698 sayılı Kanun kapsamında olup Kanunun gerekliliklerinin bu araçlarca gerçekleştirilen veri işlemlerinde uygulanması gerekmektedir. Kanunda belirli bir veri toplama yöntemi belirtilmeyerek Kanunun dolanılması önlenmek istenmiştir. Zira veri işleme araç ve yöntemlerinden hangisi kullanılırsa kullanılsın, eğer kullanılan yöntem tamamen veya kısmen otomatik yollarla veri işlemesine hizmet ediyorsa bu Kanun kapsamındadır²²⁰. Otomatik olmayan ancak herhangi bir veri kayıt sisteminin parçası olacak şekilde gerçekleştirilen veri işleme faaliyetlerine de ayrıca

²¹⁹ Göçmen Uyarer, s. 104.

²²⁰ Çekin, ss. 22,23.

değnilmelidir. Veri kayıt sistemi ifadesi ile ne anlaşılması gerektiği Kanunun “*Tanımlar*” başlıklı 3. maddesinin 1/h fıkrasında belirtilmiştir. Buna göre veri kayıt sistemi, kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir. Bir dosyalama sistemi olarak da ifade edilebilecek olan veri kayıt sistemi elektronik veya fiziki ortamda oluşturabilir. Veri kayıt sisteminde kişisel veriler, ad, soyad ya da kimlik numarası üzerinden sınıflandırılabilceği gibi örneğın kredi borcunu ödemeyenler hakkında bu kriter üzerinden yapılan bir sınıflandırmaya ilişkin veri topluluğu da Kanun kapsamında değlendiriilebilecektir²²¹. Herhangi bir ortak özelliğı olmayan ve belli kriterlere göre yapılandırılmamış, sistemsiz, gelişigüzel işlenen veriler Kanunun kapsamında olmayacaktır²²². Konuyu örneklerle açıklamak gerekirse, personel dosyaları, hastanede tutulan hasta kayıt dosyaları, mahalle bakkalınca tutulan ve kişilerin ad, soyad ve borç durumlarını gösteren bir veresiye defteri dahi veri kayıt sistemi olarak kabul edilebilecek ve Kanunun uygulama kapsamında sayılacaktır. Ancak örneğın, bir mağazada alışveriş yapan müşterinin ad, soyad ve numarasını yazdığı bir kağıdı mağazaya bırakması durumunda burada veri kayıt sisteminin varlığından bahsedilemeyecektir²²³. Burada önemli bir nokta, madde gerekçesini içeren tasarı metninde de belirtildiğı üzere, otomatik olmayan yollarla ve herhangi bir veri kayıt sisteminin parçası olmaksızın işlenen kişisel veriler, her ne kadar 6698 sayılı Kanunun uygulama kapsamı dışında kalsa da kişisel veri vasfını taşımaya devam edecek ve söz konusu verilere yönelik hukuka aykırı eylemler 5237 s. Türk Ceza Kanununca yaptırıma tabi tutulacaktır²²⁴.

Kanunun 28. maddesinde, Kanun kapsamı dışında kalan haller ayrıca zikredilmiştir. Hükümde, kişisel verilerin üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlölöklere uyulmak kaydıyla gerçek kişilerin tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi, kişisel verilerin resmi istatistik ile anonim hale getirilmek suretiyle araştırma, istatistik gibi amaçlarla işlenmesi, yine kişisel verilerin milli güvenlik, milli savunma, kamu güvenliği, kamu düzeni, ekonomik güvenlik, özel hayatın gizliliğı

²²¹ Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular**, Ankara, 2019, www.kvkk.gov.tr, (05.01.2023), s. 30.

²²² Dölger, Kişisel Veriler Hukuku, s. 16.

²²³ Çekin, s. 23.

²²⁴ TBMM, “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 7.

veya kişilik hakları ihlal edilmemek ya da suç teşkil etmemek şartıyla sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi, kişisel verilerin milli savunma, milli güvenlik, kamu güvenliği, kamu düzeni veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi, kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemleriyle ilgili olarak yargı veya infaz mercilerince işlenmesi halleri 6698 sayılı Kanunun kapsamı dışında tutulmuştur. 6698 sayılı Kanunun 28. maddesinin 2. fıkrasında ise ilgili yasanın bir kısmından istisna tutulan haller düzenlenmiştir. Hükme göre, kişisel veri işleme faaliyetlerinin suç işlenmesinin önlenmesi veya suç soruşturması sebebiyle gerekli olması, ilgili kişinin kendisi tarafından alenileştirilmiş vaziyetteki kişisel verilerinin işlenmesi, kişisel verilerin işlenmesinin kanunun vermiş olduğu yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları tarafından düzenleme veya denetleme görevlerinin yürütülmesi ile disiplin soruşturması veya kovuşturması için gerekli olması ve son olarak kişisel verilerin işlenmesinin bütçe, vergi ve mali konulara ilişkin olarak Devletin mali çıkarlarının ve ekonomik çıkarlarının korunması amacıyla gerekli olması hallerinde 6698 sayılı Kanunun belirli bazı hükümlerinin uygulanmayacağı düzenlenmiştir. Bu hükümler, veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10'uncu, zararın giderilmesini talep etme hakkı hariç olmak üzere ilgili kişinin haklarını düzenleyen 11'inci ve veri sorumluları sicili sistemine kayıt yükümlülüğünü düzenleyen 16'ncı madde hükümleridir. Ancak maddede, bu istisnaların söz konusu olduğu durumlarda dahi, Kanunun amacına ve Kanunda yer verilen temel ilkelere uygun olmak şartıyla veri işleme faaliyeti gerçekleştirilmesi gerektiği ifade edilmiştir.

6698 sayılı Kanunun 28. maddesinde sayılan istisnaların son derece geniş tutulduğu ve özellikle Devletin veri işleme etkinlikleri bakımından yasanın uygulama alanının daraltılmış olduğu dikkat çekmektedir. Her ne kadar günümüzde özel sektörün veri işleme etkinlikleri bir hayli artmış olsa da bu durum devletin veri işleme etkinliklerinin zayıfladığı anlamına gelmemektedir. Kaldı ki kişisel verilerin korunması hakkı en başta, Devletin veri işleme etkinlikleri karşısında bireyin aleyhine bozulan dengenin tekrar sağlanması amacıyla ortaya konulmuştur. Bu sebeplerle

Devletin veri işleme etkinliklerinde de hukuka uygun olma, yalnızca meşru amaçlara yönelmiş olma ve o amacın gerektirdiği oranda işlenmesi ilkelerine sıkı sıkıya bağlı kalınmalıdır²²⁵.

(2) Diğer Kanunlar

Türk hukuk sistemi bakımından kişisel verilerin korunması alanında atılan kapsamlı ve ivme kazandırıcı adımların miladını 1982 Anayasası'nda 2010 yılında gerçekleştirilen değişiklik ve devamında yasalaşan “6698 sayılı *Kişisel Verilerin Korunması Kanunu*” olarak görmek mümkün ise de bu tarihlerden önce de hukukumuzda, çeşitli hükümlerde kişisel verilerin korunmasına ilişkin düzenlemelerin yer aldığını ifade etmek gerekir. Nitekim 26.09.2004 tarihli “5237 sayılı Türk Ceza Kanunu'nun” 135-139. maddeleri, kişisel verilerin korunmasına yönelik cezai düzenlemeler olup hala yürürlüktedir. Yine 05.11.2008 tarih ve “5809 sayılı Elektronik Haberleşme Kanunu'nun” 4. maddesi ile aynı kanunun 12. ve 51. maddeleri, hukukumuzda adeta kişisel verilerin korunması alanına kaynak teşkil edebilecek niteliği haiz düzenlemelerdir²²⁶.

Kişisel verilerin korunması hakkının kişilik hakkı ile olan sıkı bağlantısı, kişilik hakkının korunmasına yönelik temel düzenlemelerin kişisel verilerin özel hukuk yönüyle korunması bakımından da uygulanmasına olanak sağlamaktadır. Bu çerçevede Türk Medeni Kanunu'nun 23, 24 ve 25. maddeleri ile Türk Borçlar Kanunu'nun 58. maddesi kişilik hakkının bir uzantısı olan kişisel verilerin korunması hakkını özel hukuk boyutuyla koruma altına almaktadır. Bahsedilen korumanın kişisel verilerin korunması alanının kendine has özellikleri sebebiyle etkili bir güvence sağlayamayacağı ve bu sebeple özel hukukun çeşitli alanlarında ayrıca kişisel verilerin korunmasına ilişkin düzenlemeler gerçekleştirilmesi gerektiği söylenebilir. Nitekim bu doğrultuda 4857 sayılı İş Kanunu, 5490 sayılı Nüfus Hizmetleri Kanunu ve 213 sayılı Vergi Usul Kanunu gibi yasal metinlerde dolaylı da olsa düzenlemeler bulunduğu görülmektedir²²⁷.

²²⁵ Küzeci, *Kişisel Verilerin*, s. 383.

²²⁶ Öztürk ve diğerleri, s. 55.

²²⁷ Bük, s. 79.

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN İŞLENMESİ, DENETİM SİSTEMİ VE KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN İDARENİN UYGULAMA ÖRNEKLERİ

I. KİŞİSEL VERİLERİN İŞLENMESİ

A. Genel Olarak

Günümüzde kişisel verilere duyulan ihtiyaç hem kamu sektörü hem de özel sektör bakımından had safhada olup gerek kamu kurum ve kuruluşları gerekse özel sektör aktörleri tarafından her an kişisel veriler toplanmakta, depolanmakta ve aktarılmaktadır. Bunun yanında teknolojiye yaşanan devrimsel nitelikteki gelişmeler, kişisel verilerin toplanma, depolanma ve aktarılma gibi süreçlerini oldukça kolay hale getirmiştir. Tüm bu durumlar karşısında kişilerin temel hak ve özgürlükleri ise büyük bir tehdit altında bulunmaktadır. Bu tehdidin bertaraf edilmesi ise ancak kişisel verilerin korunmasına yönelik hukuki düzenlemeler ve bu düzenlemelerle uyumlu etkin uygulamalarla mümkün olabilecektir. Nitekim Anayasamızın 20. maddesinin 3. fıkrasında kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebileceğini belirtilmektedir. Görüldüğü üzere normlar hiyerarşisinin en üstünde yer alan Anayasamıza göre kişisel verilerin işlenmemesi kural iken belirli şartların bulunması halinde işlenmesi hukuka uygun kabul edilmektedir.

İzah edilen hususlar çerçevesinde kişisel verilerin mutlak ve sınırsız bir hak olmadığı ve Anayasamızın 13. maddesi hükmü uyarınca burada yer alan esaslar çerçevesinde ancak kanun ile sınırlandırılabilceği söylenebilir²²⁸. 6698 sayılı Kanunun 5. maddesi kişisel verilerin işlenme şartlarına ilişkin bir düzenleme olup bu konuya detaylıca değinmeden önce kişisel verilerin işlenmesi ile ilgili bazı kavramlara açıklık getirmenin faydalı olacağı kanaatini taşıyoruz.

²²⁸ Başar, s. 29.

1. Veri İşleme Faaliyeti

Kişisel verilerin işlenmesi kavramı, içeriği oldukça geniş bir kavramdır. Zira bu kavram, verilerin toplanmasından silinmesine kadar olan süreci ifade eder²²⁹. 6698 sayılı Kanunun “*Tanımlar*” başlıklı 3. maddesinde, kişisel verilerin işlenmesinin, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade ettiği belirtilmektedir. Görüldüğü üzere kişisel verilerin korunması hakkının etkin bir şekilde sağlanabilmesi amacıyla veri işleme kavramı oldukça geniş tutulmuştur. Bu düzenlemeden, ayrıca, veri sorumlusunun sorumluluğunun oldukça geniş tutulduğu da kolaylıkla anlaşılabilmektedir²³⁰. Düzenlemede yer alan ifade, kişisel verileri üzerinde gerçekleştirilecek her türlü işlemin istisnasız bir veri işleme faaliyeti olarak değerlendirilmesine olanak sağlar niteliktedir²³¹. Zira madde hükmünün gerekçesinde de kişisel verilerin oldukça geniş bir alanı kapsadığı ve kişisel verilerin işlenmesi kavramından verilerin ilk defa elde edilmesinden itibaren bu veriler üzerinde gerçekleştirilen her türlü işlemin anlaşılması gerektiği belirtilmiştir. Bu çerçevede yine, elle veya bilgisayar vasıtasıyla kişisel veriler üzerinde gerçekleştirilen her türlü sürecin, işleme olarak kabul edilebileceğini belirtmek gerekir²³². 6698 sayılı Kanunda kişisel verilerin işlenmesine getirilen tanımın, “95/46/EC sayılı Direktif” ve onu kaldıran “2016/679 sayılı Genel Veri

²²⁹ Özdemir, s. 135.

²³⁰ Çekin, s. 38.

²³¹ Başar, s. 32.

²³² Korkmaz, Kişisel Veriler, s. 63.

Koruma Tüzüğü” gibi söz konusu alan bakımından önem arz eden uluslararası metinlere benzer şekilde düzenlendiği fark edilmektedir²³³.

2. Veri Kayıt Sistemi

6698 sayılı Kanunun 3. maddesinde veri kayıt sistemi, belirli kriterlere göre yapılandırılarak kişisel verilerin işlendiği kayıt sistemi olarak tanımlanmıştır. Kanunun gerekçesinde söz konusu sistemlerin elektronik veya fiziki ortamda oluşturulabileceği belirtilmektedir. Bu kavrama ilişkin detaylı açıklamalara kanunun kapsamına ilişkin kısımda yer vermiş olmamız sebebiyle tekrara düşmemek adına ilgili kısma atıf yapmakla yetiniyoruz.

3. Veri Sorumlusu, Veri İşleyen ve İlgili Kişi

a. Veri Sorumlusu

6698 sayılı Kanunda veri sorumlusu kavramından, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişinin anlaşılması gerektiği ifade edilmiştir. Söz konusu tanımda dikkate değer hususlardan bir tanesi, veri sorumlusu sıfatını taşıyabilecek olanların gerçek kişiler ile sınırlı tutulmayıp tüzel kişilerin de bu kapsama dahil edilmiş olmasıdır. Kişisel verileri işlenen gerçek kişilerin, işlenen kişisel verilerinin akıbeti hakkında bilgi sahibi olabilmesi, yine bu verileri üzerinde denetim sahibi olabilmesi ve karşısında sorumlu bir muhatap bulabilmesi açısından veri sorumlusu, kişisel verilerin korunması hukukunun başlıca aktörleri arasında yer

²³³ 95/46/EC sayılı Direktifin “Tanımlar” başlıklı 2.maddesinde kişisel verilerin işlenmesi kavramı, otomatik olan veya olmayan yöntemlerle “toplama, elde etme, kaydetme, depolama, düzenleme, uyarılma veya değiştirme, kullanım, danışma, sıraya koyma veya birleştirme, yayma veya başka şekilde kullanılabilir hale getirme, iletim yoluyla ifşa etme, silme, engelleme veya imha vb. bütün işlem veya işlem dizileri” olarak tanımlanmıştır. Yine “2016/679 sayılı Genel Veri Koruma Tüzüğü” de ufak değişiklikler ile benzer bir tanıma yer verilmiştir. Söz konusu Tüzüğün “Tanımlar” başlıklı 4. maddesi uyarınca “işleme faaliyeti, kişisel veri veya kişisel veri dizileri üzerinde gerçekleştirilen otomatik yöntemlerle olsun veya olmasın toplama, elde etme, düzenleme, kaydetme, saklama, yapılandırma, uyarılma veya değiştirme, kullanma, danışma, yayma veya kullanıma sunma, iletim yoluyla açıklama, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha vb. herhangi bir işlem veya işlem dizisidir”.

alır²³⁴. Özellikle veri işleme sürecine dahil olan üçüncü kişilerden ayırt edebilmek amacıyla veri sorumlusuna bu sıfatı kazandıran özelliklerini tespit etmek gerekir. Nitekim Kanunun 3. maddesinde de bu özellikler belirtilmektedir. Hüküm uyarınca en genel tabiriyle veri sorumlusunu, kişisel verilerin nasıl işleneceği hususunda tasarruf yetkisine sahip kişi olarak ifade edebiliriz. Bu bakımdan verileri sadece işleyen kişi ile verilerin nasıl işleneceği konusunda tasarruf yetkisine sahip kimsenin ayırt edilebilmesi, yükümlülük ve sorumlukların belirlenmesi yönüyle de önem taşımaktadır²³⁵. Her ne kadar kanun hükmünde kamu kurumlarının da veri sorumlusu olduğuna ilişkin ayrıca bir düzenleme bulunmasa da, Kanun hükümlerinin gerek özel hukuk tüzel kişilerini gerekse kamu hukuku tüzel kişilerini bağlaması sebebiyle kamu kurumları da veri sorumlusu olarak kabul edilmektedir²³⁶. Veri sorumlusunun tespiti çok önemli olmakla birlikte günümüzde gerçekleşen bazı teknolojik gelişmeler bu tespitin yapılmasını zorlaştırmaktadır. Zira buna en önemli örnek blockchain teknolojisidir. Blockchain sisteminde, sistemin bir yöneticisinin bulunmayışı ve merkeziyetsiz bir işlem ağına sahip olması veri sorumlusunun tespitini güçleştirmektedir²³⁷.

b. Veri İşleyen

Kişisel verilerin işleme sürecine dahil olan ancak veri sorumlusu sıfatını taşımayan kişiler de bulunmaktadır. Bu kişilerden bir tanesi de veri işleyendir. Hak ve yükümlülüklerin tespiti ve sorumluluğun isnadı bakımından veri sorumlusu ve veri işleyen kavramlarının ayrımını yapabilmeyen çok önemli olduğunu yukarıda belirtmiş idik. Zira 6698 sayılı Kanundaki genel yaklaşım, kişisel verilerin işlenmesine ilişkin yükümlülüklerin yerine getirilmesinden büyük oranda veri sorumlusunun sorumlu tutulması yaklaşımıdır. Bu çerçevede 6698 sayılı Kanun veri işleyeni, 3. maddenin 3. bendinde veri sorumlusunun yetkilendirmesiyle veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlamıştır. Veri işleyen, veri sorumlusunun vermiş olduğu yetkinin sınırları dahilinde hareket edebilen kişiyi ifade etmektedir.

²³⁴ Göçmen Uyarer, s.118.

²³⁵ Çekin, s. 41.

²³⁶ Küzeci, Kişisel Verilerin Korunması, ss. 364,365.

²³⁷ Çekin, ss. 41,42.

Veri işleyen, veri sorumlusundan aldığı yetkiye dayanarak, kişisel verilerin toplanılmasında kullanılacak teknolojilerin ve yöntemlerin ne olduğuna, verilerin güvenliğinin sağlanması amacıyla alınacak tedbirlere, verilerin nasıl saklanacağına, silme veya yedeklemeye karar veren kişidir²³⁸. Başka bir ifadeyle veri işleyen, veri sorumlusunun kendisine vermiş olduğu talimatlar çerçevesinde kişisel verileri işleyen ayrı bir gerçek veya tüzel kişidir²³⁹. Veri işleyenin veri sorumlusuna bağlı bir birim olma zorunluluğu bulunmamaktadır. Veri sorumlusu ile aralarında kişisel verilerin işlenmesi faaliyeti bakımından hukuki bir ilişki mevcuttur²⁴⁰. O halde veri işleyenin veri sorumlusunun doğrudan bir çalışanı olması mümkün olduğu gibi, veri sorumlusu ile sözleşme ilişkisi içerisindeki bir üçüncü kişi olması da mümkündür²⁴¹. Sorumluluk hususunda ise veri işleme etkinlikleri bakımından temel sorumluluğun veri sorumlusuna ait olduğu, onun verdiği yetkiye dayanarak onun adına veri işleme faaliyetinde bulunan veri işleyenin ise belirli açılardan sorumluluğunun bulunduğu söylenebilir²⁴². Nitekim 6698 sayılı Kanunun 12. maddesinin 2. fıkrasında veri sorumlusunun, kendisi adına başka bir gerçek veya tüzel kişi tarafından kişisel verilerin işlenmesi durumunda veri güvenliğine ilişkin aynı hükmün 1. fıkrasında yer alan tedbirleri almada o gerçek veya tüzel kişi ile müştereken sorumlu olduğu ifade edilmektedir. Görüldüğü üzere Kanun, veri sorumlusunun veri işleme faaliyetini, veri işleyen sıfatındaki başka bir kişiye gördürmesi halinde, veri güvenliğinin sağlanmasına ilişkin tedbirlerin alınması bakımından hem veri sorumlusunu hem de veri işleyeni müşterek olarak sorumlu kabul etmiştir. Yani veri işleme faaliyeti ayrıca bir veri işleyen tarafından gerçekleştiriliyor olsa dahi veri sorumlusunun yükümlülükleri ortadan kalkmamaktadır²⁴³.

²³⁸ Başar, s. 40; Öztürk ve diğerleri, s. 42.

²³⁹ Kişisel Verileri Korunma Kurumu, Veri Sorumlusu ve Veri İşleyen, www.kvkk.gov.tr, (18.01.2023), s. 1.

²⁴⁰ Dülger, Kişisel Veriler Hukuku, s. 20.

²⁴¹ Baskın, s. 65.

²⁴² Küzeci, Kişisel Verilerin Korunması, s. 366.

²⁴³ Başar, s. 41.

c. İlgili Kişi

İlgili kişi en genel tabiriyle, verileri işlenen gerçek kişiyi ifade etmektedir²⁴⁴. Nitekim 6698 sayılı Kanun 3. maddesinin ç) bendinde ilgili kişiyi, kişisel verisi işlenen gerçek kişi olarak tanımlamıştır. 95/46/EC sayılı Direktif ile 2016/679 sayılı Tüzükte kişisel verisi işlenen gerçek kişi “*veri öznesi*” olarak isimlendirilmiştir. Kanunumuzda ise veri öznesi kavramının karşılığını “*ilgili kişi*” kavramı oluşturmaktadır. 6698 sayılı Kanun kişisel verilerin korunması hakkında yararlanacak kişilerin kapsamını gerçek kişilerle sınırlı tutmuştur. Gerçekten de, kişisel verilerin korunması, niteliği itibarıyla başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin korunmasını ve yine insanın sadece insan olmasından kaynaklı sahip olduğu kişilik haklarının güvence altına alınmasını amaçlayan bir alandır²⁴⁵. Bu noktada tüzel kişilerin verilerinin kişisel verilerin korunması çerçevesinde değerlendirilmesi mümkün değildir. Konuya, birinci bölümde kişi kavramına getirdiğimiz açıklamalarda detaylı bir biçimde değinmiş olduğumuzdan tekrara düşmemek adına ilgili başlığa atıf yapmakla yetiniyoruz.

B. Kişisel Verilerin İşlenmesi Sürecine Hâkim Olan Genel İlkeler

6698 sayılı Kişisel Verilerin Korunması Kanununun 4. maddesi, kişisel verilerin işlenmesine ilişkin genel ilkeleri düzenlemektedir. İlgili hükmün birinci fıkrasında, kişisel verilerin ancak 6698 sayılı Kanunda ve diğer kanunlarda öngörülen usul ve esaslara göre işlenebileceği ifade edilmiştir. İkinci fıkrada ise kişisel verilerin işlenmesinde uyulması gereken ilkeler belirtilmiştir.

Kişisel verilerin işlenmesinde uyulması gerekli olan ilkeler insan onuru ve değerlerinin korunması amacıyla belirlenmiş ortak ilkelerdir. Verilerin işlenme sürecinde bu ilkelere aykırı hareket edilmesi bizleri, kişisel verilerin iyi niyetle ve hukuka uygun olarak işlenmediği, ortada bir kötüye kullanım hali bulunduğu sonucuna ulaştıracaktır²⁴⁶. Başka bir deyişle, Kanunun 4. maddesinde düzenlenen temel ilkeler başlı başına bir hukuka uygunluk sebebi sayılmamakla birlikte her türlü veri işleme

²⁴⁴ Dülger, Kişisel Veriler Hukuku, s. 17.

²⁴⁵ Küzeci, Kişisel Verilerin Korunması, s. 363.

²⁴⁶ Korkmaz, Kişisel Veriler, s. 323.

faaliyetinde dikkate alınması mutlak surette zorunlu olan ilkelere aykırı davranılması durumunda söz konusu veri işleme faaliyetinin hukuka aykırı olduğundan bahsedilebilecektir²⁴⁷. Kişisel verilerin işlenmesine ilişkin ilkeler, sınırları katı ve net kurallar bütünü niteliğinde olmayıp verilerin işlenmesinde genel bir çerçeve çizer niteliktedirler²⁴⁸. Genel ilkelere, kişisel verilerin işlenmesi sürecinin başından sonuna kadar uyulması gerekmektedir²⁴⁹.

1. Hukuka ve Dürüstlük Kurallarına Uygun Olma İlkesi

Kişisel verilerin işlenmesi kavramı gerek 6698 sayılı Kanunda ve bu kanuna kaynak teşkil eden 95/46/EC sayılı Direktif'te gerekse daha sonra yürürlüğe giren Tüzükte, kişisel veriler üzerinde gerçekleştirilen bütün süreçleri kapsayacak şekilde oldukça geniş tanımlanmıştır²⁵⁰. Kişisel verilerin işlenmesinin hukuka ve dürüstlük kurallarına uygun olması ilkesi ise verilerin işlenmesinde birincil ve temel ilke olarak ifade edilebilir. Zira bu ilke diğer birçok ilkenin kaynağını oluşturmaktadır²⁵¹. Hukuka uygun olma ile veri işleme faaliyetlerinde gerek usul gerekse esas bakımından mevzuata, hukukun evrensel ilkelerine ve içtihatlarla uygun hareket edilmesi anlaşılmalıdır. Dürüstlük kurallarına uygun olma ise kavram itibariyle etik değerlere riayet edilmesini vurgular. Nitekim dürüst kelimesi, Almanca ve İngilizcede adil kelimesini karşılamakta, adil ise hukuku ve ahlakı da içerisinde barındıran etik değerlerden bir tanesi olarak karşımıza çıkmaktadır²⁵². Bu ilke kapsamında belirtilen dürüstlük kurallarına uygun olma ile Medeni Kanun m. 2/2'de yer alan dürüstlük kuralının eş anlamlı olmadığını ifade etmemiz gerekir. İlke yer alan dürüstlük ile daha çok “*adil kullanım*” kastedilmektedir. Veri işleme sürecine katılan veri işleyen ve veri sorumlusu dahil herkesin ilgili kişiye adil davranma yükümlülüğü bulunmaktadır. Ayrıca yine burada belirtilen dürüstlük kuralı, tarafların haklı çıkar ve menfaatlerinin dengelenmesinde bir hayli önem taşımaktadır²⁵³. Kişisel verilerin

²⁴⁷ Çekin, s. 42.

²⁴⁸ Öztürk ve diğerleri, s. 58.

²⁴⁹ Akgül, Verilerin Korunması, s. 154.

²⁵⁰ Korkmaz, Kişisel Veriler, ss. 121,122.

²⁵¹ Küzeci, Kişisel Verilerin Korunması, s. 228.

²⁵² Öztürk ve diğerleri, s. 58.

²⁵³ Çekin, s. 45.

hukuka ve dürüstlük kurallarına uygun olarak işlenmesi ilkesi ile bir bütün olarak genel itibariyle, kişisel verilerin işlenmesi sürecinin tamamında hukuka uygun hareket edilmesi, ilgili kişinin çıkarlarının korunması, maddi-manevi bütünlüğünün ve bireysel özerkliğinin makul olmayan sebeplerle ihlal edilmemesi, sürecin şeffaf yönetilerek veri sorumlusunca ilgili kişinin bilgilendirilmesi, ilgili kişinin de dilediğinde veri işlemeye ilişkin bilgilere erişebilmesi sağlanmaktadır²⁵⁴.

2. Doğru ve Gerekliğinde Güncel Olma İlkesi

Kişisel verilerin doğru ve gerektiğinde güncel olması ilkesi hem ilgili kişinin hem de veri sorumlusunun çıkarları ile yakından ilişkili bir ilkedir. Zira işlenen verilerin doğru ve güncel olmaması halinde ilgili kişinin temel hak ihlalleri, maddi ve manevi zararlarla karşı karşıya kalması söz konusu olabileceken; veri sorumlusunun da verilerin işlenmesi ile hedeflediği sonuca ulaşması mümkün olmayacaktır²⁵⁵. Kişisel verilerin kimliği belirli ya da belirlenebilir kılan, kişiyi tanımlayabilme işlevine sahip her türlü bilgi olduğunu daha önce ifade etmiştik. Ancak kişisel verilerin gerek bu işlevinin yerine getirilebilmesi gerekse genel anlamda kişisel verilerin korunmasının sağlanabilmesi bu verilerin doğru ve güncel olmasına bağlıdır²⁵⁶.

İlkenin veri sorumlusunu ve veri ilgisini ilgilendiren yönleri bulunmaktadır. Şöyle ki en başta, veri sorumlusunun, işlediği kişisel verilerin hatasız, doğru ve güncel olmasının sağlanması bakımından özenli davranması gerekmektedir²⁵⁷. Veri sorumlularının kişisel verilerin doğru ve güncel olarak tutulması yükümlülüğü olup, bu yükümlülük devredilemez niteliktedir²⁵⁸. Bu çerçevede veri sorumluları, veri işleme faaliyetini gerçekleştirirken gerekli tedbirleri almalı²⁵⁹, verilerin elde edildiği kaynağın doğruluğunu tespit etmeli, verilerin doğru olmadığına yönelik başvurular var ise bunları göz önünde bulundurmalı ve gerekli incelemeleri gerçekleştirerek makul

²⁵⁴ Küzeci, *Kişisel Verilerin Korunması*, s. 230.

²⁵⁵ Küzeci, *Kişisel Verilerin Korunması*, s. 243.

²⁵⁶ Dülger, *Kişisel Veriler Hukuku*, ss. 130,131.

²⁵⁷ Sefer Oğuz, “Kişisel Verilerin Korunması Hukukunun Genel İlkeleri”, **Bilgi Ekonomisi ve Yönetimi Dergisi**, Cilt:13, Sayı:2, 2018, s. 133.

²⁵⁸ Küzeci, *Kişisel Verilerin Korunması*, s. 244.

²⁵⁹ Baskın, s. 60.

önlemleri almalıdır²⁶⁰. Verilerin doğru ve gerektiğinde güncel tutulmasının sağlanmasında, veri sorumlularını, her durum bakımından sorumlu tutmanın hakkaniyete aykırı sonuçlar doğurabileceğini belirtmek gerekir. Nitekim verilerin doğruluğu bakımından, örneğin kişisel verinin toplanması doğrudan veri ilgisinden oluyorsa, burada en başta veri ilgisinin verisini doğru olarak veri sorumlusu ile paylaşması kendisinden beklenmektedir. Veri ilgisi kendisine ilişkin bilgiyi doğru bir şekilde vermiş olmasına rağmen bilinçli veya bilinçsiz olarak bu verilerin hatalı yorumlanması veya yanlış işlenmesi halinde ise yine veri sorumlusunun sorumluluğuna gidilebilecektir²⁶¹. Verilerin güncelliği bakımından ise veri sorumlusunun sürekli olarak verilerin güncelliğini araştırmasının kendisinden beklenemeyeceğini öncelikle ifade etmek gerekir. Veri ilgisinin var ise bilgilerinde oluşan değişiklikleri veri sorumlusuna bildirmesi gerekmektedir. Ancak burada veri sorumlusunun yükümlülüğünü doğuran nokta, bu hususun sağlanması amacıyla ilgili kişilerin bilgilerine ulaşabileceği ve onları denetleyebileceği makul kanallar oluşturması yönüyledir²⁶². Başka bir deyişle veri sorumlularının, ilgililere bilgilerini doğrulayabileceği ve güncelleyebileceği imkanları sağlama yükümlülüğü bulunmaktadır²⁶³. Örneğin veri sorumlusu, 6 ay veya 1 yıllık sürelerle, veri ilgisine bilgilerinde bir değişiklik var ise bunun kendisine bildirilmesini belirten bildirimlerde bulunabilir²⁶⁴. Yine web sitelerinde kullanılan ve veri ilgililerinin kendilerine ait şifreleri ile kendi bilgilerine ulaşp düzeltibildikleri sistemler de bu yükümlülüğün yerine getirilebileceği başka bir örnektir²⁶⁵.

3. Belirli, Açık ve Meşru Amaçlar İçin İşlenme İlkesi

Kişisel verilerin belirli, açık ve meşru amaçlarla işlenmesi ilkesine göre, kişisel verilerin işlenmesinde işlenme amacının belirli olması ve yine işlemenin meşru

²⁶⁰ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, s. 67.

²⁶¹ Dülger, Kişisel Veriler Hukuku, s. 131.

²⁶² Küzeci, Kişisel Verilerin Korunması, s. 244.

²⁶³ Baskın, s. 60.

²⁶⁴ Dülger, Kişisel Veriler Hukuku, s. 133.

²⁶⁵ Küzeci, Kişisel Verilerin Korunması, s. 244.

amaçlarla gerçekleştirilmesi gerekmektedir²⁶⁶. Başka bir deyişle bu ilke ile hedeflenen, veri sorumlusunun veri işleme amacını açık ve kesin olarak belirlemesini ve bu amacın da meşru bir amaç olmasını sağlamaktır. Bu çerçevede veri sorumlusu, ilgili kişiyi kişisel verilerinin işlenme amacı hakkında bilgilendirmeli, bu bilgilendirmeyi ise anlaşılır ve açık bir dil kullanarak yapmalıdır²⁶⁷. Belirtilen amaçlar dışında bir veri işleme faaliyetinde bulunulması hukuka aykırı olacak ve veri sorumlusunun sorumluluğunu doğuracaktır²⁶⁸. Meşru amaç ile kastedilen verilerin toplanma amacının yasal bir temele sahip ve bütün hukuki gereklilikleri sağlıyor olmasıdır²⁶⁹. Bununla birlikte veri sorumlusu tarafından işlenen veriler, veri sorumlusunun yaptığı iş veya sunduğu hizmetler bakımından bağlantılı ve gerekli olmalıdır. Örneğin, bir giyim mağazasının, müşterilerinin ad-soyad ve iletişim bilgilerini işlemesi, meşru bir amaca dayalı veri işleme olarak kabul edilebiliyor iken aynı giyim mağazasının müşterilerinin kan grubu bilgilerini işlemesi meşru amaç kapsamında sayılmayacaktır²⁷⁰.

İlkenin genel itibarıyla özünü, veri işleme faaliyetlerinde “*bir gün lazım olur*” mantığıyla hareket edilmesini engellemek oluşturur. Aksi durumda, her veri sorumlusu tarafından belirsiz ve açık olmayan amaçlarla verileri işlenen bireyler, kişisel verileri üzerindeki denetimini kaybetme, dolayısıyla bireysel özerkliğin ve kişiliği geliştirme hakkı gibi temel değerlerinin ihlali tehlikesiyle de karşı karşıya kalacaklardır²⁷¹.

4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma İlkesi

Kişisel verilerin korunması hukukuna hâkim olan ve 6698 sayılı Kanunda da yer verilen ilkelerden bir diğeri, kişisel verilerin, işlenme amaçlarıyla bağlantılı, amaçla sınırlı ve ölçülü olması ilkesidir. Kanunun tasarı metninde yer alan gerekçe uyarınca bu ilke, sadece belirlenen amaçların gerçekleştirilmesi bakımından elverişli olan verilerin işlenmesini, belirlenen amacın gerçekleştirilmesi bakımından ihtiyaç

²⁶⁶ Göçmen Uyarer, s. 125.

²⁶⁷ Kişisel Verileri Koruma Kurumu, Kanunun Uygulanmasına İlişkin Rehber, s. 47.

²⁶⁸ Baskın, s. 61.

²⁶⁹ Korkmaz, Kişisel Veriler, s. 123.

²⁷⁰ Kişisel Verileri Koruma Kurumu, Kanunun Uygulanmasına İlişkin Rehber, s. 47.

²⁷¹ Göçmen Uyarer, s. 126; Küzeci, Kişisel Verilerin Korunması, s. 231.

duyulmayan, amaçla ilgisi bulunmayan verilerin ise işlenmesinden kaçınılmasını gerektirmektedir²⁷². Bu ilke ile temel olarak bireylere ait kişisel verilerin mümkün olduğunca asgari ölçüde işlenmesi, diğer bir deyişle veri minimizasyonunun sağlanması amaçlanmaktadır²⁷³.

Verilerin işlendikleri amaçla bağlantılı ve sınırlı olması, belirlenen amacın gerçekleştirilmesi bakımından ihtiyaç duyulan verilerin veri işleme faaliyetine konu edilmesi anlamını taşımaktadır. O anda mevcut olmayan ya da daha sonra mevcut olabileceği düşünülen muhtemel amaçlar için veri işlenmesi yoluna gidilmemelidir²⁷⁴. Başka bir ifade ile işlenecek olan verilerin niteliği ile işleme amacının birbiriyle uyumlu olması ve yalnızca amaç bakımından ihtiyaç duyulan verilerin işlenmesi gerekmektedir²⁷⁵. Daha sonra ortaya çıkabilecek muhtemel ihtiyaçlara dayalı veri işleme faaliyeti ayrı bir veri işleme faaliyeti olarak değerlendirilecek ve burada Kanunun 5. maddesindeki veri işleme şartlarından birinin gerçekleşmesi aranacaktır²⁷⁶. Veri sorumlusundan, amaca bağlılık ilkesi çerçevesinde yapması gereken değerlendirmeyi kişisel verileri topladığı her durumda tekrarlaması beklenir. Örneğin iş başvuru formları, internet kayıt sayfaları gibi veri toplama araçları hazırlanırken amaca bağlılık ilkesine riayet edilmeli ve amaç için gerekli olanların haricinde kişisel veri istenmemelidir²⁷⁷. Ölçülülük ilkesi ise belirtilen amaca kişisel verilerin işlenmesinden başka araçlarla ulaşılabilir olması ve bu araçların korunması hedeflenen temel hak ve hürriyetlere hiç müdahalede bulunmuyor veya daha az müdahalede bulunuyor olması hallerinde veri işlenmesi yerine bu araçların tercih edilmesi anlamına gelmektedir²⁷⁸. Ancak elbette belirtilen amaca yönelik bir veri işleme faaliyeti mutlak surette gerekiyor ise bu durumda da ölçülülük ilkesi gereği amaç bakımından mutlak surette gerekli olanlarla sınırlı bir veri işleme faaliyeti gerçekleştirilmelidir. Ölçülülük ilkesine ilişkin olarak Kişisel Verileri Koruma Kurulu'nun vermiş olduğu bir kararında yer alan değerlendirmelerin, bu ilkenin daha iyi anlaşılması bakımından kolaylık sağlayacağı kanaatindeyiz. Söz konusu karar, ses

²⁷² TBMM, “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 8.

²⁷³ Korkmaz, Kişisel Veriler, s. 125; Küzeci, Kişisel Verilerin Korunması, s. 237.

²⁷⁴ Kişisel Verileri Koruma Kurumu, Kanunun Uygulanmasına İlişkin Rehber, s. 47.

²⁷⁵ Göçmen Uyarer, ss. 126,127.

²⁷⁶ Kişisel Verileri Koruma Kurumu, Kanunun Uygulanmasına İlişkin Rehber, s. 47.

²⁷⁷ Küzeci, Kişisel Verilerin Korunması, s. 237.

²⁷⁸ Çekin, s. 53.

kayıt özelliği bulunan güvenlik kameraları ile ilgilidir. Kurul kararında ölçülülük ilkesini, veri işleme faaliyeti ile ulaşılmak istenen amaç arasında makul bir denge kurulması olarak ifade etmiş, kararın devamında ise somut olay bakımından, kayıt ile beklenen faydanın ses kaydına ihtiyaç duyulmaksızın yalnızca görüntü kaydı ile elde edilebilecek olması durumunda ayrıca ses kaydının da yapılmasının kişisel veri işleme faaliyeti ile ulaşılmak istenen amaç arasındaki dengeyi bozacağını ve ölçülülük ilkesine aykırılık teşkil edeceğini belirtmiştir²⁷⁹.

İlkenin genel itibarıyla, belirlenen amaçla ilgisi bulunan kişisel verilerin, yine amacın gerektirdiği miktarda işlenmesini öngördüğünü ifade edebiliriz. Bununla birlikte ilke, bir gün lazım olacağı düşüncesiyle belirlenen amaçla ilgisi bulunmayan verilerin işlenmesinden kaçınılmasını gerektiren bir ilkedir. Eğer muhtemel ihtiyaçlar için bir veri işleme faaliyetine girişilecekse bu, yeni bir veri işleme faaliyeti olarak değerlendirilecek ve Kanunun veri işleme şartlarını düzenleyen 5. maddesinin dikkate alınması zorunluluk teşkil edecektir.

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

Kişisel verilerin işlenmesi sürecinde uyulması gereken temel ilkelerden bir tanesi de işlenen verilerin mevzuatta öngörülen süre veya işlendiği amaç için gerekli olan süre ile sınırlı olarak muhafaza edilmesidir. 6698 sayılı Kanunun 4. maddesinde de yer verilen bu ilkenin amacı, kişisel verilerin hukuka uygun gerekçelere bağlanarak işlenmiş olsalar dahi sınırsız bir süre boyunca muhafaza edilmesini önlemektir. Nitekim aksinin kabulü, daha önce de ifade ettiğimiz üzere, bir kez kişisel verisi işlenmiş olan kişinin artık bu verilerinin yaşamı boyunca bir yerlerde kayıt altında bulundurulduğunu ve yeri geldiğinde kullanılmak üzere bekletildiğini düşünmesine neden olacaktır²⁸⁰.

Eğer veri sorumlusu mevzuattan kaynaklı bir veri işleme gerekçesine dayanarak kişisel veri işleme faaliyeti yürütüyor ve mevzuatta da kişisel verilerin

²⁷⁹ Kişisel Verileri Koruma Kurulunun 12.03.2020 tarihli ve 2020/212 sayılı karar özeti, <https://www.kvkk.gov.tr/>, (13.01.2023).

²⁸⁰ Küzeci, Kişisel Verilerin Korunması, s. 245.

saklanması için bir süre öngörülüyor ise veri sorumlusunun belirtilen süre tamamlanınca işlemiş olduğu verileri yok etmesi, silmesi veya anonim hale getirmesi gerekir²⁸¹. Zira Ceza Muhakemesi Kanunu'nun 80. maddesi bu konuya verilebilecek örnek bir mevzuat düzenlemesidir. Ancak her durumda, kişisel verilerin saklanma süresi mevzuatta öngörülmemektedir. Kaldı ki, kişisel veri olarak kabul edilebilecek verileri saymanın mümkün olmaması da her kişisel veri bakımından mevzuatta bir süre öngörülmesini olanaksız kılmaktadır²⁸². Bu sebeple mevzuatta kişisel verilerin saklanması ile ilgili bir süre öngörülmemiş ve bu konuda verilmiş Kurul kararı da bulunmuyor ise veri sorumlusunun işlemiş olduğu kişisel verileri, işleme amacı gerçekleşikten sonra yok etmesi, silmesi yahut anonim hale getirmesi gerekmektedir²⁸³. İleri zamanlarda, kişisel verilerin tekrar kullanılabilceği düşünülerek veya başka herhangi bir gerekçe ile kişisel verilerin muhafaza edilmesi mümkün olmayacaktır²⁸⁴.

Kurumun yayımlamış olduğu Rehberde söz konusu ilkenin amaçla sınırlılık ilkesinin bir gereği olduğu belirtilmekle birlikte, bu ilke kapsamında kişisel verilerin amaç için gerekli olan süreye uygun muhafaza edilmesi ve veri sorumlusunun da bu konuda gerekli bütün teknik ve idari tedbirleri alması gerektiği ifade edilmektedir²⁸⁵. Nitekim 6698 sayılı Kanunun 12. maddesi veri sorumlusunun işlemiş olduğu verilerin güvenliğini sağlaması noktasında birtakım yükümlülükler öngörmektedir. Hüküm uyarınca veri sorumlusu, işlemiş olduğu kişisel verilerin, hukuka aykırı işlenmesini önlemek, muhafazasını sağlamak ve yine bu verilere hukuka aykırı erişilmesini önlemek amacıyla veri güvenliğini sağlamaya yönelik gereken bütün teknik ve idari tedbirleri almak zorundadır. İşlenme amacı ortadan kalkan verilerin veri sorumlusu tarafından saklanmaya devam edilmesi, hukuka aykırı olmasının yanında mevcut verilerin her an güvenlik riski ile karşı karşıya kalmasına da neden olacaktır. Zira günümüzde, bilişim teknolojilerindeki gelişmeler bu alanda yüzde yüz güvenlikten söz edilemeyeceğini göstermektedir²⁸⁶.

²⁸¹ Göçmen Uyarer, s. 128.

²⁸² Anayasa Mahkemesi'nin 28.09.2017 tarih ve 2016/125 E. 2017/143 K. sayılı Kararı

²⁸³ Baskın, s. 63.

²⁸⁴ Kişisel Verileri Koruma Kurumu, Kanunun Uygulanmasına İlişkin Rehber, s. 70.

²⁸⁵ Kişisel Verileri Koruma Kurumu, Kanunun Uygulanmasına İlişkin Rehber, s. 69.

²⁸⁶ Dölger, Kişisel Veriler Hukuku, s. 134.

Özet itibariyle, veri sorumlusu öncelikle işleme amacını ve sürecini aşamalandırarak hangi verileri hangi amaç için işlediğini net bir şekilde belirlemeli, bu amaç çerçevesinde işlemiş olduğu veriler için mevzuatta bir saklama süresi belirtilmiş ise bu süreye uygun olarak ve bütün veri güvenliği tedbirlerini alarak verileri muhafaza etmeli, belirtilen süre sona erdiğinde ise kişisel verileri silmeli yahut anonim hale getirmelidir. Mevzuatta belirlenmiş bir süre yok ise veri sorumlusu belirlenen amacın gerçekleşmesi için öngördüğü makul süre boyunca bu verileri tüm veri güvenliği tedbirlerini sağlayarak muhafaza etmelidir. Amacın ortadan kalkması, gerçekleşmesi yahut da o amaç için gerekli olduğu zannedilen verinin aslında gerekli olmadığına anlaşılmaması anında²⁸⁷; başka bir ifade ile veriler saklanma amaçları açısından gereksiz hale geldiği anda veri sorumlusu tarafından derhal silinmeli veya anonimleştirilmelidir²⁸⁸.

C. Kişisel Verilerin İşlenme Şartları

1. Genel Olarak

Kişisel verilerin korunması hakkının hukukumuz bakımından temel dayanak düzenlemesi olan Anayasa m. 20/3 hükmü uyarınca “*kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir*”. Söz konusu düzenleme ile esasında kişisel verilerin korunmasının bir temel hak niteliği taşıdığına ve bu temel hakkın ise kişinin açık rızası yahut kanunda öngörülen hallerde sınırlandırılabilmesine vurgu yapılmaktadır²⁸⁹. Veri koruma hukukunda kural, kişisel verilerin işlenmesinin yasak olmasıdır. Ancak 6698 sayılı Kanunun 5. ve 6. maddelerinde kişisel verilerin hangi koşullarda işlenebileceği düzenlenmiştir. Bu düzenlemeler kişisel verilerin işlenmesi yasağının hukuka uygunluk halleridir²⁹⁰. Belirtmekte fayda var ki, sadece Kanunun 5.ve 6. maddelerindeki koşullara uygun hareket etmek, gerçekleştirilecek veri işleme faaliyetini hukuka uygun kılmaya yetmeyecektir. Zira bu hükümlerdeki

²⁸⁷ Dülger, Kişisel Veriler Hukuku, ss. 135,136; Küzeci, Kişisel Verilerin Korunması, s. 245.

²⁸⁸ Oğuz, s. 12.

²⁸⁹ Çekin, s. 54.

²⁹⁰ Dülger, Kişisel Veriler Hukuku, s. 214.

koşulların varlığı ile birlikte Kanunun 4. maddesinde yer alan veri koruma hukukun temel ilkelerine riayet edilmesi de aranmaktadır²⁹¹. Özetle, kişisel verilerin korunmasının temel bir hak olması gerekçesiyle, söz konusu verilerin işlenmesinde Anayasanın 13. ve 20. maddelerine ve 6698 sayılı Kanunun bu alanın temel ilkelerini düzenleyen 4. maddesi ile veri işleme koşullarını düzenleyen 5 ve 6. maddelerine uygun hareket edilmesi gerekmektedir²⁹². Ayrıca son olarak, kişisel verilerin işlenme şartlarının kanunda yazanlarla sınırlı olduğunu, bu şartların veri sorumlusu tarafından genişletilemeyeceğini belirtmek yararlı olacaktır²⁹³.

Kişisel verilerin işlenme koşulları konusunda Kanun, özel nitelikli olmayan kişisel veriler için 5. maddede “*kişisel verilerin işlenme şartları*” başlıklı; özel nitelikli kişisel veriler için ise 6. maddede “*özel nitelikli kişisel verilerin işlenme şartları*” başlıklı iki ayrı düzenleme ihtiva etmektedir. Konunun anlaşılmasında kolaylık sağlaması açısından, biz de özel nitelikli kişisel veriler ile özel nitelikli olmayan kişisel verilerin işlenme koşullarını ayrı başlıklar altında ele almayı uygun buluyoruz.

2. Özel Nitelikli Olmayan Kişisel Verilerin İşlenme Şartları (m.5)

a. İlgili Kişinin Açık Rızası (m.5/1)

6698 sayılı Kanunun 5. maddesinin ilk fıkrasında “*Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez*” hükmü yer almaktadır. Kanunun 3. maddesinin a bendinde ise açık rıza, “*Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza*” olarak tanımlanmıştır. 6698 sayılı Kanunun gerekçesinde, kural olarak kişisel verilerin, ilgili kişinin açık rızası yahut maddede belirtilen diğer istisnalar dışında işlenmesinin yasak olduğu belirtilmekle birlikte 95/46/EC sayılı direktife atıf yapılarak rıza kavramı açıklanmıştır. Gerekçeye göre rıza, 95/46/EC sayılı direktif esas alınarak, ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanıdır. Bu açıklamalar ışığında 6698 sayılı kanunun, kişisel verilerin işlenmesinde hukuka uygunluk hallerinden biri olarak

²⁹¹ Çekin, s. 54.

²⁹² Öztürk ve diğerleri, s. 67.

²⁹³ Dülger, Kişisel Veriler Hukuku, s. 214.

düzenlediği ilgili kişinin açık rızası hususunun, 95/46/EC sayılı direktife paralel olduğu anlaşılmaktadır.

İlgili kişinin açık rızasının olmasının, kişisel verilerin işlenmesinde hukuka aykırılığı ortadan kaldıran başlıca etmenlerden bir tanesi olduğu söylenebilir²⁹⁴. Ancak ilgili kişinin açık rızasının, diğer hukuka uygunluk sebepleri karşısında bir üstünlüğü bulunmadığını da ayrıca ifade etmek gerekir²⁹⁵. Kişisel verilerin işlenmesinde, her durumda açık rızanın alınması gerektiği algısı yanlış bir algıdır²⁹⁶. Veri sorumlusu kişisel verilerin işlenmesi sırasında somut olay bakımından aşağıda detaylıca incelenecek olan diğer hukuka uygunluk sebeplerinden birine dayanabiliyorsa, ilgili kişinin açık rızasını almasına gerek kalmayacaktır²⁹⁷. Zira veri sorumlusunun diğer hukuka uygunluk sebeplerinden birine dayanarak kişisel veri işlemesi mümkün iken ilgili kişinin açık rızasını alması ilgili kişide, bu rızanın geri alınabileceği ve geri alınma neticesinde veri işleme faaliyetine son verilebileceği şeklinde aldatıcı bir düşünceye sebebiyet verecektir. Halbuki, zaten somut olay bakımından yapılan veri işleme faaliyeti kanundaki diğer hukuka uygunluk sebeplerinden birine dayanmaktadır²⁹⁸. Başka ifade ile, ilgili kişinin, bilgilerinin geleceğini belirleme hakkına istinaden açık rıza vererek verilerinin işlendiğini ve bu rızasını geri çektiğinde veri işlemeye son verileceğini düşünmesine karşın aldatıcı mahiyette, veri işlemenin devam ediyor olması dürüstlük kuralına aykırıdır²⁹⁹.

Konuya ilişkin Kurumun yayımlanmış olduğu rehberde, açık rızanın ilgili kişinin olumlu irade beyanını içermesi gerektiği, diğer mevzuat düzenlemeleri saklı kalmak kaydıyla açık rızanın herhangi bir şekil şartına bağlı olmadığı, yine açık rızanın elektronik ortam, çağrı merkezi vb. yollarla alınabileceği ve açık rızanın alındığına dair ispat külfetinin veri sorumlusunun üzerinde bulunduğu ifade edilmiştir³⁰⁰. Gerçekten de kişinin temel hak ve hürriyetlerine müdahaleyi meşru kılma işlevi gibi önemli bir görev gören açık rızanın, ilgilisi tarafından aktif bir şekilde verilmesi şartı

²⁹⁴ Başar, s. 44.

²⁹⁵ Dülger, Kişisel Veriler Hukuku, s. 215.

²⁹⁶ Göçmen Uyarer, s. 131.

²⁹⁷ Çekin, s. 64.

²⁹⁸ Dülger, Kişisel Veriler Hukuku, s. 215.

²⁹⁹ Küzeci, Kişisel Verilerin Korunması, s. 395.

³⁰⁰ Kişisel Verileri Koruma Kurumu, Açık Rıza, www.kvkk.gov.tr, (24.01.2023), s. 3.

aranmalıdır³⁰¹. Diğer ifade ile ilgili kişinin sükutu ikrar olarak değerlendirilemeyecek, örtülü rıza beyanının varlığı halinde açık rızanın bulunduğu sonucuna ulaşamayacaktır³⁰².

6698 sayılı Kanunun kabul ettiği açık rızada, üç unsur birlikte aranmaktadır. Bunlar belirli bir konuya ilişkin olarak açık rızanın verilmesi, rızanın bilgilendirmeye dayalı olması ve yine açık rızanın özgür, serbest iradeyle açıklanmasıdır. Açık rızanın geçerli olabilmesi için belirli bir konuya ilişkin ve o konu ile sınırlı olması mutlak surette aranmaktadır. Eğer birden fazla kategori için veri sorumlusu tarafından açık rıza alınacaksa bu açık rızanın, hangi kişisel veriler için ve ne amaçla verildiğinin belirli olması ve her kategori bakımından ayrı ayrı alınmış olması gerekir³⁰³. Yine ilgili kişinin, veri işleme faaliyetinin konusu hakkında, açık rıza vermesi durumunda bunun sonuçları hakkında ve veri işleme faaliyetinin tüm yönlerine ilişkin olarak açık ve anlaşılır biçimde bilgilendirilmesi gerekmekte olup bu bilgilendirme mutlaka veri işlenmesinden önce yapılmalıdır³⁰⁴. İlgili kişinin özgür iradesiyle açık rıza göstermesi Kanunda aranan açık rızaya ilişkin niteliklerden bir diğeridir. İlgili kişinin iradesini sakatlayan tehdit altında olma veya başkalarınca rıza göstermeye zorlanma gibi hallerde verilen açık rıza, özgür iradeye dayanmayacağından burada hukuka uygun bir açık rızadan söz edilemeyecektir³⁰⁵. Tarafların eşit konumda olmadığı veya birinin diğeri üzerinde etkide bulunduğu örneğin işçi-işveren ilişkisi gibi ilişkilerde kişisel verilerin işlenmesine yönelik verilen açık rızanın özgür iradeye dayanıp dayanmadığı da dikkatle incelenmelidir³⁰⁶. Yine bir ürünün teslimi yahut da bir hizmetin sunulması gibi hallerde, gerekli olmamasına rağmen bu teslim veya hizmet sunumu kişisel verilerin işlenmesi şartına bağlı kılınıyorsa burada kişisel verilerin işlenmesine yönelik verilen açık rızanın özgür iradeyle verilmediği sonucuna ulaşılır. Zira somut olayda bir bağlantı yasağı söz konusudur³⁰⁷.

Son olarak, ilgili kişinin açık rızası alınmadan gerçekleştirilen bir veri işleme faaliyetinde daha sonradan ilgili kişinin icazetinin alınması, başta gerçekleştirilen veri

³⁰¹ Çekin, ss. 58,59.

³⁰² Başar, ss. 46,47.

³⁰³ Kişisel Verileri Koruma Kurumu, Açık Rıza, s. 4.

³⁰⁴ Kişisel Verileri Koruma Kurumu, Açık Rıza, s. 5.

³⁰⁵ Çekin, s. 59.

³⁰⁶ Kişisel Verileri Koruma Kurumu, Açık Rıza, s. 6.

³⁰⁷ Çekin, s. 60.

işleme faaliyetinin hukuka aykırı olduğu gerçeğini değiştirmeyecektir. Ayrıca ilgili kişi kişisel verilerinin işlenmesine ilişkin olarak vermiş olduğu açık rızayı her zaman ve herhangi bir gerekçe göstermeden geri alabilir. Ancak bu durum, geri almadan önceki kişisel veri işleme faaliyetinin yasallığını etkilemez³⁰⁸.

b. İlgili Kişinin Açık Rızası Aranmadan Kişisel Verilerin İşlenebileceği Haller

6698 sayılı Kanunun m. 5/2’de, ilgili kişinin açık rızası aranmadan kişisel verilerin işlenebileceği durumlar düzenlenmiştir. Yukarıda, açık rıza başlığı altında da ifade ettiğimiz üzere, eğer veri sorumlusu kişisel verilerin işlenmesine ilişkin olarak açık rıza dışındaki hukuka uygunluk sebeplerinden birine dayanabiliyorsa, ilgili kişinin açık rızasını alma yoluna gitmemeli, veri işleme faaliyetini o hukuka uygunluk sebebi çerçevesinde gerçekleştirmelidir. Kanunun m. 5/2 hükmünde yer alan, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenebileceği hukuka uygunluk sebepleri şunlardır: Kanunlarda açıkça öngörülmesi, ilgili kişi tarafından alenileştirilmiş olması, sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması şartıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, fiili imkansızlık sebebiyle rızasını açıklayamayacak durumda olan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin veya başkasının hayatı/beden bütünlüğünün korunması için zorunlu olması, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

(1) Kanunlarda Açıkça Öngörülmesi (m.5/2-a)

Kişisel verilerin işlenmesine ilişkin olarak, 6698 sayılı Kanun dışındaki kanunlarda açıkça düzenleme bulunması halinde, ilgili kişinin açık rızasına

³⁰⁸ Başar, s. 48.

başvurulmaksızın kişisel verileri işlenebilir³⁰⁹. Öğretide, hükümde belirtilen “açıkça” ifadesine dikkat edilmesi ve yasal düzenlemelerden açıkça anlaşılamayan yahut dolaylı bir şekilde kişisel verilerin işlenebileceği sonucu çıkarılan hallerde kişisel verilerin işlenmesi yoluna başvurulmaması gerektiği belirtilmektedir³¹⁰. Başka ifade ile, kanunlarda genel bir yetki ile kişisel verilerin işlenmesini öngören düzenlemeler var ise o düzenleme meşru bir işleme sebebi teşkil etmeyecektir³¹¹. Kanunun gerekçesinde örnek olarak iki yasal düzenleme gösterilmiştir. Bunlar, bir suç soruşturmasına istinaden şüphelilerin parmak izlerinin alınması hakkındaki 2559 sayılı Polis Vazife ve Salahiyet Kanunun 5. maddesi ile Adalet Bakanlığı’nın kişilerin ceza mahkumiyetlerine ilişkin verilerini işlemesi hakkındaki 5352 sayılı Adli Sicil Kanunu hükümleridir. Bu örnekleri çoğaltmak mümkündür. Nitekim 5271 sayılı Ceza Muhakemesi Kanunu’nun 137. maddesinde telekomünikasyon hizmeti veren kurum ve kuruluşların yetkililerinden iletişimin tespiti, dinlenmesi veya kayda alınması işlemlerinin yapılması istendiğinde bu istemin derhal yerine getirileceği belirtilmektedir. Söz konusu düzenleme uyarınca gerçekleştirilecek olan kişisel verileri işleme faaliyeti, yasal dayanağı bulunması sebebiyle hukuka uygun sayılacaktır³¹². Kişisel Verileri Koruma Kurumu tarafından verilerin bir Kurul Kararının da konuyu örneklendirme bakımından faydalı olacağını düşünüyoruz. Kararda avukatların, icra takip dosyalarında yer alan kişisel verilere vekaletname olmaksızın erişimleri bakımından yapılan inceleme ve değerlendirmeler neticesinde, bu yetkinin 1136 sayılı Avukatlık Kanununun 46. maddesi uyarınca avukatlara tanındığı ve 6698 sayılı Kanunun m.5/2-a hükmü uyarınca da alacaklı vekili avukatlar tarafından borçlunun alacaklı olduğu icra dosyalarına ilişkin kişisel veri işleme faaliyeti yürütebileceği ifade edilmiştir³¹³.

Hükümde geçen kanun ifadesinden yasama işlemi olan kanunu anlamak yani şekli kanun anlayışını benimsemek gerekir³¹⁴. Nitekim kişisel verilerin korunması temel bir hak olarak Anayasada düzenlenmiştir. Anayasada düzenlenen temel hakkın

³⁰⁹ Küzeci, Kişisel Verilerin Korunması, s. 395; Göçmen Uyarer, s. 131.

³¹⁰ Dülger, Kişisel Veriler Hukuku, s. 216.

³¹¹ Küzeci, Kişisel Verilerin Korunması, s. 395.

³¹² Başar, s. 56.

³¹³ Kişisel Verileri Koruma Kurulu’nun 20.05.2021 tarih ve 2021/511-512-513 sayılı Karar Özeti, www.kvkk.gov.tr, (25.01.2023).

³¹⁴ Başar, s. 57.

sınırlandırılması ancak Anayasa m. 13 çerçevesinde diğer şartları da taşımak koşuluyla kanunla gerçekleştirilebilecektir³¹⁵. Ayrıca belirtmek gerekir ki, usulüne göre yürürlüğe girmiş uluslararası sözleşme hükümlerinin de Anayasa m. 90 uyarınca kanun hükmünde sayılması sebebiyle örneğin kişisel verilerin işlenmesi konusundaki uluslararası sözleşmelerin getirebileceği düzenlemeler uygulanabilir nitelikte olacaktır³¹⁶.

(2) Kişinin Kendisinin veya Bir Başkasının Hayatı veya Beden Bütünlüğünün Korunması İçin Zorunlu Olması (m.5/2-b)

Açık rızası olmaksızın ilgili kişinin kişisel verilerinin işlenebileceği hallerden bir diğeri olan bu hukuka uygunluk sebebinde iki şartın varlığı birlikte aranmaktadır. Birinci şart, ilgili kişinin fiili imkânsızlık sebebiyle rızasını açıklayamayacak durumda bulunması veya hukuki olarak rızasına geçerlilik tanınmayan bir kişi olması durumudur. Örneğin kişinin geçirmiş olduğu kaza sebebiyle bilincinin kapanmış olması yahut da kişinin tam ehliyetsiz olması, birinci şartın gerçekleştiği örneklerdir³¹⁷. İkinci şart ise ilgili kişinin kendisinin veya bir üçüncü kişinin hayatının veya beden bütünlüğünün korunması bakımından veri işleme faaliyetinin zorunluluk teşkil etmesidir³¹⁸. Hükümün gerekçesinde verilen örnekler konunun daha iyi anlaşılması bakımından faydalı olacaktır. Gerekçede, kişinin şuurunun yerinde olmadığı veya akıl hastası olması sebebiyle rızasının geçerli olmadığı durumlarda, hayatının ve beden bütünlüğünün korunması amacıyla, tıbbi müdahale esnasında kişisel verilerinin işlenebilecek olması konuya verilen ilk örnektir. Gerekçede verilen diğer bir örnek ise, hürriyeti sınırlandırılmış bir kişinin kurtarılması amacıyla, kendisinin veya şüphelinin taşımakta olduğu telefon, kredi kartı vb. teknik araçlar üzerinden yerinin belirlenebilmesi için bu verilerin işlenebilmesidir.

³¹⁵ “Anayasanın 13. Maddesi uyarınca Özel hayatın gizliliği ve kişisel verilerin korunması hakları, yalnızca kanunla ve demokratik bir toplumda gerekli olduğu ölçüde sınırlanabilir.” Anayasa Mahkemesi’nin 28.12.2017 tarih ve 2016/179 E., 2017/176 K. sayılı kararı.

³¹⁶ Başar, s. 58,59.

³¹⁷ Öztürk ve diğerleri, s. 75.

³¹⁸ Dülger, Kişisel Veriler Hukuku, s. 216.

Hükmün özündeki hukuka uygunluk nedeni kişinin üstün nitelikli özel yararının korunmasına denk gelmektedir³¹⁹. Gerçekten de somut şartlar düşünüldüğünde, kişinin hayatı veya beden bütünlüğünün korunması amacıyla bir başka temel hak ve hürriyetinin kısıtlanması zorunluluk teşkil etmekte ve kişinin üstün nitelikli özel yararı lehine hareket edilmesi gerekmektedir. Aksi halde, yaşamsal durumlarda kişisel verilerin işlenmesi prosedürlerine takılı kalınması, bireylerin yaşamları veya beden bütünlükleri üzerinde telafisi imkânsız sonuçlara sebebiyet verebilecektir³²⁰.

(3) Sözleşmenin Taraflarına Ait Kişisel Verilerin İşlenmesinin Gerekli Olması (m.5/2-c)

6698 sayılı Kanunda, kişisel verilerin açık rıza olmaksızın işlenebildiği hallere sözleşmesel ilişkiler bakımından da bir düzenleme getirilmiştir. Buna göre bir sözleşmenin kurulması veya ifasıyla ilgili olması kaydıyla taraflara ait kişisel veriler, tarafların açık rızası aranmaksızın işlenebilecektir. Hükmün gerekçesinde, bir sözleşme ilişkisine istinaden paranın ödenmesi amacıyla borçlunun alacaklının hesap numarasını alması hali, bir bankanın akdedilecek kredi sözleşmesine istinaden tapu kaydı, icra borcu olmadığını gösteren belge, maaş bordrosu gibi evrakları edinmesi hali konuya örnek olarak gösterilmiştir.

Sözleşme, tarafların karşılıklı ve birbirine uygun irade beyanlarından oluşan ve hukuki sonuç doğurmaya yönelmiş hukuki bir işlemdir³²¹. Sözleşmede tarafların arzu etmiş olduğu hukuki sonuca ulaşabilmeleri çoğu zaman bazı kişisel verilerin işlenmesini gerektirmektedir³²². Bu hükümde kanun koyucunun, en az ilgili kişi kadar veri sorumlusunun da haklı menfaatlerini gözettiğini belirtmek faydalı olacaktır. Ayrıca yine kanun koyucunun, hükmün lafzında yalnızca sözleşme ifadesini kullanmış olması, sebepsiz zenginleşme ve haksız fiilden doğan borçlar bakımından bu hukuka uygunluk sebebinin uygulanamayacağı anlamını taşımaktadır³²³. Hükümde,

³¹⁹ Başar, s. 60.

³²⁰ Göçmen Uyarer, s. 132.

³²¹ Küzeci, Kişisel Verilerin Korunması, s. 397.

³²² Dülger, Kişisel Veriler Hukuku, s. 217.

³²³ Çekin, ss. 65-67.

sözleşmenin kurulması veya ifasıyla doğrudan ilgili olan kişisel verilerin işlenebileceğine vurgu yapılmıştır. Sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olma, o sözleşmenin kurulması veya ifası için zorunlu olan bilgileri ifade etmektedir³²⁴. Dolayısıyla amaçlanan veri işleme süreci ile o sözleşmenin kurulması yahut ifası arasında doğrudan bir bağlantı bulunması gerekmektedir. Başka bir deyişle kişisel verilerin işlenmesi, o sözleşmenin kurulması yahut ifası bakımından gerekli ve alternatifsiz olmalıdır³²⁵.

(4) Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirebilmesi İçin Zorunlu Olması (m.5/2-ç)

Veri sorumlusunun 6698 sayılı Kanun dışında, başka hukuki düzenlemelerden kaynaklı da birtakım yükümlülükleri bulunabilmektedir. Bu yükümlülükleri doğrultusunda veri sorumlusunun kişisel veri işleme gerekebilir. Ancak veri işlemenin meşruiyetini yalnızca kişinin rıza göstermesinde aramak veri sorumlusunun hukuki yükümlülüğünü yerine getirememesine sebep olabilecektir³²⁶. Bu nedenle 6698 sayılı Kanun m. 5/2-ç’de, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi bakımından zorunlu olan kişisel verileri, ilgili kişinin açık rızasına ihtiyaç duyulmaksızın işleyebileceği düzenlenmiştir. Söz konusu hükmün uygulanabilmesi için en başta, hukuki yükümlülüğün veri sorumlusuna yüklenmiş olması gerekmektedir. Ayrıca hukuki yükümlülüğün mutlaka bir kanunla öngörülmüş olması gerekmekte, ikincil düzeydeki mevzuat düzenlemeleri de bu kapsama girmektedir. Önemli olan, veri sorumlusunun tercih olanağı bulunmaksızın ilgili hukuki yükümlülüğe uymasının zorunlu olmasıdır³²⁷.

Konuya örnek olarak 2577 sayılı İdari Yargılama Usul Kanununun (İYUK) 20. maddesi verilebilir. Hükümde, re’sen araştırma ilkesi düzenlenmiş olup, örneğin, mahkeme kararı ile veri sorumlusu sıfatındaki idari bir kurumdan belge talep edilmesi

³²⁴ Nafiye Yücedağ, “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”, **İÜHF Mecmuası**, Cilt: 75, Sayı:2, 2017, s. 777.

³²⁵ Çekin, s. 68.

³²⁶ Küzeci, Kişisel Verilerin Korunması, s. 397.

³²⁷ Yücedağ, ss. 778,779.

halinde bu belgenin mahkemeye sunulması amacıyla kişisel verilerin işlenmesi, 6698 sayılı Kanunun m. 5/2-ç hükmü çerçevesinde kabul edilen hukuka uygun bir veri işleme faaliyetidir³²⁸. Konuya bir başka örnek ise 1774 sayılı Kimlik Bildirme Kanunundan verilebilir. Kimlik Bildirme Kanununun 2. maddesi, otel, motel, tatil köyü gibi konaklama yerlerinde konaklayacak kişilerin kimliği ile geliş- ayrılış kayıtlarını, örneğine ve usulüne uygun olarak günü gününe tutması, bu kayıtları her zaman genel kolluğun incelemesine hazır bulundurması gerektiğini ve talebi halinde Devlet İstatistik Enstitüsüne vermek zorunda olduğunu belirtmiştir. Veri sorumlusu sıfatındaki konaklama işletmeleri, konaklayan kişilere ilişkin işledikleri kişisel verileri, 1774 sayılı Kanuna ve bu kanunun veri sorumlusuna getirdiği hukuki yükümlülüğe dayanarak gerçekleştirmektedir³²⁹. Son olarak belirtmek gerekir ki, bu hukuka uygunluk sebebi somut olaylarda kimi zaman sözleşmesel ilişkiler hakkındaki hukuka uygunluk sebebi ile³³⁰, kimi zaman ise kanunlarda açıkça öngörülme hali ile birlikte bulunabilmektedir³³¹.

(5) İlgili Kişi Tarafından Alenileştirilmiş Olması (m.5/2-d)

Kişisel verilerin işlenmesinde hukuka uygunluk sebeplerinden bir diğeri, Kanunun m. 5/2-d'de, ilgili kişi tarafından alenileştirilmiş olması olarak ifade edilmiştir. Hükmün gerekçesinde, ilgili kişi tarafından alenileştirilen, başka bir ifadeyle herhangi bir şekilde kamuoyuna açıklanan kişisel verilerin işlenebileceği, ilgili kişi tarafından alenileştirilmek suretiyle herkes tarafından bilinebilir hale gelen kişisel verilerin işlenmesinde, korunması gerekli hukuki yararın ortadan kalktığı belirtilmektedir. Gerekçede dikkat çeken husus, diğer hukuka uygunluk sebeplerinin aksine bu hükme ilişkin herhangi bir örneklendirmenin yapılmamış olmasıdır.

Kişisel Verileri Koruma Kurumunun alenileştirilmiş olma hususunda yayımlamış olduğu kamuoyu duyurusunda bu hukuka uygunluk sebebinde dikkate alınması gereken iki temel ölçüte dikkat çekmiştir. Bunlardan ilki ilgili kişinin kişisel verilerini alenileştirme iradesi ile kamuoyu ile paylaşmış olması; diğeri ise

³²⁸ Başar, s. 62.

³²⁹ Öztürk ve diğerleri, s. 76.

³³⁰ Dülger, Kişisel Veriler Hukuku, s. 217.

³³¹ Öztürk ve diğerleri s. 76.

alenileştirme amacıdır. İlgili kişinin kişisel verilerinin aleni olmasını istemesi gerekmektedir. Başka ifadeyle, ilgili kişinin alenileştirme iradesi olmaksızın kişisel verilerin kamuoyuna açık hale gelmesi alenileştirme olarak kabul edilemeyecektir. Ayrıca ilgili kişinin alenileştirme amacının da tespiti gereklidir. Çünkü alenileştirme, ilgili kişinin kişisel verilerini kamuoyu ile paylaşma amacı ile sınırlıdır. Veri sorumlularının bu alenileştirme amacı dışında kişisel verileri işlemleri, Kanuna aykırılık teşkil edecektir. Örneğin, ikinci el araç satışı yapılan bir internet sitesinde aracını satmak isteyen ilgili kişinin paylaşmış olduğu iletişim bilgileri, yalnızca aracı satın almak veya ilan hakkında bilgi edinmek için kullanılmalıdır. Bunun haricinde bir amaca dayanarak verilerin kullanılması halinde kanuna aykırılık söz konusu olacaktır³³². Yine örneğin, özel muayenehanesi olan bir hekimin üzerinde ad, soyad ve iletişim bilgilerinin yer aldığı bir kart bastırarak dağıtması o verilerini alenileştirdiğini göstermektedir. Ancak elbette ki bu durum, hekimin kart üzerindeki kişisel verilerinin her türlü amaç için kullanılabileceği anlamına gelmemektedir. Kart üzerinde yer alan iletişim bilgisinin hekime muayene için randevu almak isteyen kişi tarafından işlenmesi hukuka uygun kabul edilebilecek iken; ilaç şirketleri tarafından pazarlama amacıyla kullanılması alenileştirilme amacı dışında kullanılması nedeniyle hukuka aykırılık taşıyacaktır³³³. Kişisel Verileri Koruma Kurulunca bu örneğe benzer verilmiş bir karar da bulunmaktadır³³⁴. Ayrıca belirtmekte fayda var ki, ilgili kişi tarafından alenileştirilen kişisel verilerin işlenmesinde her halükârda 6698 sayılı Kanunun 4. maddesindeki genel ilkelere uygun hareket edilmesi bir zorunluluktur³³⁵.

Son olarak, ilgili kişi tarafından kişisel verilerin alenileştirilmiş olması hukuka uygunluk sebebine ilişkin Kanunda yer alan düzenlemenin, oldukça soyut olduğunu

³³² Kişisel Verileri Koruma Kurumu’nun 16.12.2020 tarihli “Alenileştirme” Hakkında Kamuoyu Duyurusu, www.kvkk.gov.tr, (31.12.2023)

³³³ Dülger, Kişisel Veriler Hukuku, ss. 217,218.

³³⁴ Kurulun, ilgili kişi tarafından alenileştirilen cep telefonu numarasının bir sigorta şirketi tarafından alenileştirme amacı dışında işlenmesi hakkındaki 07.11.2019 tarihli ve 2019/331 sayılı Karar özetinde, “Şikayetçinin kişisel verilerine kendisi tarafından daha önce alenileştirilen internet sitesinden ulaşılması halinde dahi Şirket tarafından Şikayetçinin bu bilgilerinin internet sitesinde bulunma ve alenileştirilme amacıyla kullanılmadığı, diğer bir deyişle Şikayetçinin mesleki yetkinliğinden faydalanmak için kendisine ulaşılmaya çalışılmadığı, aksine Şirket faaliyetlerine ilişkin randevu talebi ile Şikayetçinin arandığı anlaşıldığından, Şirket tarafından gerçekleştirilen veri işleme faaliyetinin 6698 sayılı Kişisel Verilerin Korunması Kanunun 5’inci maddesinin (2) numaralı fıkrasının (d) bendi çerçevesinde değerlendirilemeyeceği kanaatine varılmış olup...” şeklinde bir değerlendirmede bulunmuştur, www.kvkk.gov.tr, (31.01.2023).

³³⁵ Küzeci, Kişisel Verilerin Korunması, s. 399.

belirtmemiz gerekir. Zira öğretide de bu durum eleştirilmiş ve kişisel verilerin açık rıza olmaksızın işlenebildiği istisna hallerden biri olan alenileştirmenin, kanunda soyut ifadelerle düzenlenmesinin kişisel verilerin korunması hakkının ihlaline sebebiyet verebileceği, olması gerekenin esnek yorumlara mahal vermeyen, net bir düzenleme olduğu ifade edilmiştir³³⁶.

(6) Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Veri İşlemenin Zorunlu Olması (m.5/2-e)

6698 sayılı Kanun m. 5/2-e’de, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olduğu hallerde gerçekleştirilen veri işleme faaliyetinin hukuka aykırı olmayacağına yer verilmiştir. Düzenlemenin gerekçesinde bu hukuka uygunluk sebebi örneklerle açıklanmıştır. Gerekçeye göre, veri işlemenin hakkın tesisi, kullanılması veya korunması için zorunlu olması halinde veriler işlenebilecek, örneğin bir şirkete çalışanı tarafından yöneltilen bir davada şirket ispat faaliyeti için çalışanına ilişkin bazı verileri kullanabilecek veya kısıtlının haklarının korunması amacıyla vasisinin veya kayyımın kısıtlıya ilişkin mali bilgileri saklaması hukuka uygun sayılacaktır. Konuya başka bir örnek daha vermek gerekirse örneğin, eşlerin boşanma davasında evlilik birliğinin temelden sarsıldığına ilişkin olarak Mahkemeye sunacakları delilleri diğer eşin rızası olmaksızın işleyebilmesi bu hukuka uygunluk sebebi kapsamında değerlendirilecektir³³⁷. Hükümde yer verilen hak kavramına ilişkin olarak söz konusu hakkın kaynağının, sözleşmesel veya kanuni bir yükümlülüğten yahut da özel hukuk veya kamu hukukundan doğabileceğini belirtmemiz gerekir. Kısaca bir hakkın tesisi, kullanılması veya korunması için gerekli olan bütün işlemler bakımından bu hükmün uygulanması mümkündür³³⁸. Hüküm açısından dikkate değer noktalardan bir tanesi ise hakkın kötüye kullanılması yasağıdır³³⁹. Bu çerçevede Kurul vermiş olduğu bir kararında özetle, ödenmemiş alacakları temlik alan bir bankanın, borçluya alacağı temlik aldığını ve ödemeyi eski alacaklıya değil kendisine yapması

³³⁶ Başar, s. 65.

³³⁷ Esra Tepe, **Özel Hukuk Açısından Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, Ankara, 2021, s. 59.

³³⁸ Yücedağ, s. 782.

³³⁹ Öztürk ve diğerleri, s. 80.

gerektiğini bildirir bir kısa mesaj yollamak amacıyla kişisel veri olan cep numarasını işlemlerini hukuka uygun saymış, ancak aynı bankanın, bu bilgilendirme mesajlarını farklı zamanlarda ve mükerrer defa iletmesini hakkın kötüye kullanılması olarak değerlendirmiştir³⁴⁰. Son olarak Kanunda yer alan düzenleme bakımından, bir hakkın tesisi, kullanılması veya korunması hususları bir yana hükmün son kısmında yer verilen veri işleminin zorunlu olması halinin her durumda mutlak surette aranması gerekmektedir³⁴¹.

(7) Veri Sorumlusunun Meşru Menfaatleri İçin Veri İşlenmesinin Zorunlu Olması (m.5/2-f)

6698 sayılı Kanunun 5. maddesinin f fıkrasında meşru menfaatlerin korunmasına yönelik bir hukuka uygunluk sebebi getirilmiştir. Söz konusu düzenlemede yer alan hukuka uygunluk sebebinin uygulanması için başlıca iki hususun tespiti gerekmektedir. Bunlardan ilki, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olup olmadığıdır. İkincisi ise, bu veri işleme faaliyetinin ilgili kişinin temel hak ve özgürlüklerine zarar vermediğinin tespiti³⁴². Diğer bir deyişle salt meşru menfaatin varlığı kişisel verilerin işlenmesinde hukuka uygunluk sebebi teşkil etmemekte, aynı zamanda veri öznesinin temel hak ve hürriyetlerine de zarar verilmemelidir³⁴³. Hükmün gerekçesinde konu bir örnekle açıklanmıştır. Çalışanlarının temel hak ve özgürlüklerine zarar vermemek koşuluyla, bir şirket sahibi, çalışanlarının terfileri, maaş zamları gibi birtakım hak edişleri yahut sosyal haklarının düzenlenmesi noktasında ya da işletmenin yeniden bir yapılandırılmaya tabi tutulması sürecinde görev ve rol dağıtımında esas alınmak üzere çalışanların kişisel verilerini işliyorsay bu hukuka uygun bir veri işleme faaliyeti olacaktır. Gerekçede, veri sorumlusu sıfatını haiz şirket sahibi bakımından, işletmenin yeniden yapılandırılması ya da ehliyetli ve liyakatli çalışanların terfi almaları hususlarının, meşru menfaat kapsamında olduğuna dikkat çekilmiştir. Hükmün gerekçesinin son cümlesinde ise oldukça kritik bir ölçüte yer verilmiştir. Şöyle ki, bu hukuka uygunluk sebebinin

³⁴⁰ Kişisel Verileri Koruma Kurulu'nun 31.05.2019 tarihli ve 2019/159 sayılı Karar Özeti, www.kvkk.gov.tr, (01.02.2023).

³⁴¹ Küzeci, Kişisel Verilerin Korunması, s. 400.

³⁴² Öztürk ve diğerleri, s. 81.

³⁴³ Başar, s. 67.

varlığının tespitinde, kişisel verilerin korunmasına ilişkin temel ilkelere uyulması ve veri sorumlusu ile ilgili kişi arasındaki menfaat dengesinin sağlanması gerekliliğidir.

Kanunun tartışmalı konularından bir tanesi olan³⁴⁴ bu hükümde, tartışmanın odağını “meşru menfaat” kavramının nasıl yorumlanması gerektiği oluşturmaktadır. Zira meşru menfaat kavramının geniş bir şekilde yorumlanması halinde hakkın özü zarar görme tehlikesiyle karşı karşıya kalacaktır³⁴⁵. Kurul bu konuda vermiş olduğu bir kararında değerlendirmenin nasıl yapılması gerektiğine ilişkin önemli bilgilere yer vermiştir. Kararda, 6698 sayılı Kanunun 5. maddesinin ikinci fıkrasının f bendinde yer alan hukuka uygunluk sebebinin tespitinde veri sorumluları tarafından, “*kişisel verilerin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması, söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi, meşru menfaatin halihazırda mevcut, belirli ve açık olması, ilgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması, meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kar elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin, bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması, bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması, kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması, kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması, bu kapsamda kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması hususlarının*” değerlendirilmesi gerektiği ifade edilmiştir³⁴⁶. Kurumun yayımlamış olduğu rehberde ise, gerçekleştirilecek olan denge testinde veri sorumlusunun meşru

³⁴⁴ Göçmen Uyarer, s. 134.

³⁴⁵ Küzeci, Kişisel Verilerin Korunması, s. 401.

³⁴⁶ Kişisel Verileri Koruma Kurulunun 25.03.2019 tarih ve 2019/78 sayılı kararı, www.kvkk.gov.tr, (01.02.2023).

menfaatinin ilgili kişinin temel hak ve özgürlükleri karşısında çok güçlü ve etkin olmaması halinde, ilgili kişinin temel hak ve özgürlüklerinin veri sorumlusunun daha az öneme sahip meşru menfaatinden üstün tutulacağı, denge testinde kavramsal olarak meşru menfaat ve veri işleme amacı kavramlarının karıştırılmamasına dikkat edilmesi gerektiği, veri işleme amacının verinin işlenme sebebi ile ilgili olması söz konusu iken meşru menfaatin daha geniş yorumlanmak suretiyle veri sorumlusunun veri işleme gerçekleştirildikten sonra elde edeceği faydaya ilişkin bir kavram olduğu, meşru menfaat hukuka uygunluk sebebinin diğer hukuka uygunluk sebeplerine başvurulamıyorsa başvurulacak son çare olarak görülmemesi gerektiği, yine bu düzenlemenin her türlü veri işleme faaliyetini kanuna uygun hale getirecek bir düzenleme de olmadığı vurgulanmıştır³⁴⁷.

Konuya bir başka örnek olarak, örneğin bir şirket binasının içerisi ve dışarısının güvenliğinin sağlanması amacıyla binaya güvenlik kamerası sistemi kurulmasında o şirketin meşru menfaati olduğu söylenebilir. Ancak bu tek başına söz konusu veri işleme faaliyetini hukuka uygun kılmaya yetmeyecektir. Veri sorumlusu şirket, binada güvenlik kamerası ile görüntü kaydı alındığına ilişkin ilgili kişileri aydınlatma yükümlülüğünü yerine getirmeli ve ilgili kişilerin temel hak ve özgürlüklerini korumak amacıyla görüntü kayıtlarına yetkisiz erişimi önleyecek idari ve teknik tedbirleri almalıdır³⁴⁸.

3. Özel Nitelikli Kişisel Verilerin İşlenme Şartları (m.6)

Kişisel veri türleri arasında öyle bazı veriler bulunur ki, bunlar gerek temel hak ve özgürlüklere yakınlık düzeyleri gerekse başkaları tarafından öğrenilmeleri halinde doğuracakları zararlı sonuçların ağırlığı bakımından özel bir koruma sistemine tabi tutulmayı gerektirir. Bu veri türleri literatürde sıklıkla kullanılan tabiriyle özel nitelikli kişisel veriler veya hassas veriler olarak adlandırılmaktadır. Çalışmamızda, literatürdeki sık kullanış biçimleri olmaları sebebiyle her iki kavrama da yer vermek suretiyle konular açıklanmaya çalışılacaktır.

³⁴⁷ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenme Şartları, www.kvkk.gov.tr, (02.02.2023), ss. 14-16.

³⁴⁸ Öztürk ve diğerleri, s. 82.

Gerçekten de özel nitelikli kişisel veriler nitelikli bir korumayı gerektirmektedir³⁴⁹. Zira bu veri kategorisinde yer alan bilgilerin nitelikleri sebebiyle başkaları tarafından öğrenilmesi ilgili kişi üzerinde ağır mağduriyetler doğurabilecek ve ayrımcılığa maruz kalmasına neden olabilecektir³⁵⁰. Burada akla gelen ilk soru, hangi veri türlerinin hassas kişisel veri olarak adlandırılacağı sorusudur. Bu konuda gerek uluslararası gerekse ulusal hukuk düzenlemelerinde ortak bir yaklaşım bulunmamaktadır. Kaldı ki, “95/46/EC sayılı Direktif”, “108 sayılı Avrupa Konseyi Sözleşmesi”, “BM Rehber İlkeleri” gibi bazı uluslararası belgelerde özel nitelikli verilere yer verilmekte iken; APEC Çerçeve Belgesi ve OECD Rehber İlkeleri gibi bazı düzenlemelerde ise özel nitelikli verilere yer verilmediği görülmektedir³⁵¹. Özel nitelikli verilere içeriğinde yer veren düzenlemeler arasında da kapsam itibarıyla farklılıklar söz konusu olabilmektedir. Kimi düzenlemelerde hassas veriler kapsamında değerlendirilecek verilerin kapsamı oldukça geniş tutulurken kimi düzenlemelerde daha dar kapsamlı bir sayıma gidilmiştir³⁵².

6698 sayılı Kanunun özel nitelikli kişisel verilerin işleme şartlarını düzenleyen 6. maddesinin ilk fıkrasında “*kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir*” demek suretiyle hangi verilerin Kanun nazarında hassas veri olarak değerlendirileceği tahdidi bir şekilde sayılmıştır. Bu veri türleri dışındaki verileri, yorum yoluyla hassas veri kategorisine dahil etmek olanaksızdır. Ancak burada dikkat edilmesi gereken bir nokta vardır ki o da özel nitelikli kişisel verilerin etkin bir şekilde korunması ve kişilerin özel hayatının gizliliği ile diğer temel hak ve özgürlüklerinin güvence altına alınması amacına ulaşabilmek için bu verilere erişim olanağı sunabilecek nitelikteki verilerin de 6698 sayılı Kanunun 6. maddesi çerçevesinde değerlendirilmesi gereğidir. Bu çerçevede örneğin, bir siyasi partinin yayınlarına ilişkin abone listesi, bireylerin siyasi

³⁴⁹ Küzeci, Kişisel Verilerin Korunması, s. 403.

³⁵⁰ Başar, s. 72.

³⁵¹ İbrahim Korkmaz, “Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme”, **TBB Dergisi**, Cilt: Mayıs-Haziran 2016, Sayı:124, (Kanun Hakkında Değerlendirme), ss. 111,112.

³⁵² Başar, ss. 83,84.

eğilimleri hakkında dolaylı bir veri olabileceğinden 6. madde kapsamında korunmalıdır³⁵³. 6. maddenin ikinci fıkrasında ise ilgilinin açık rızası olmaksızın özel nitelikli kişisel verilerin işlenmesinin yasak olduğu belirtilmiştir. Özel nitelikli kişisel verilerin işlenmesinde kanun koyucu özellikle açık rıza ifadesini kullanmıştır. Bu çerçevede örtülü olarak verilen bir rızaya dayanarak gerçekleştirilecek özel nitelikli veri işleme faaliyeti hukuka aykırı olacaktır. Örneğin, bir klinikte tedavi görecektir hastaya itiraz etmediği müddetçe tıbbi dosyasının araştırmacıya aktarılacağı bilgisinin verilmesi, olayda açık rıza şartı sağlanmadığından hukuka aykırı olacaktır³⁵⁴. Görüldüğü üzere özel nitelikli kişisel verilerin veri sorumluları tarafından işlenmesinde kural, açık rıza olmadan veri işleme faaliyetinin yasak olmasıdır.

Kanunun 6. maddesinin 3. fıkrasında ise açık rıza aranmaksızın hassas verilerin işlenebileceği istisna haller düzenlenmektedir. Hükümde ilk tahlilde, ikili bir ayrıma gidildiği göze çarpmaktadır. Buna göre ilk olarak, sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebileceği belirtilmiştir. Örneğin, 4857 sayılı İş Kanunu'nun 75. maddesi uyarınca işveren, çalıştırdığı her işçi için bir özlük dosyası hazırlamakla ve bu dosya içerisinde 4857 sayılı İş Kanunu ve diğer Kanunlarda hazırlanması zorunlu tutulan belgeleri saklamakla yükümlü kılınmıştır. Özlük dosyasında bulunması gerekli olan ve fakat özel nitelikli veriler içermeyen evrakların işlenmesinde 6698 sayılı Kanunun 5. maddesinin uygulanacağı hususunda tereddüt bulunmamaktadır³⁵⁵. Ancak işçi hakkında bir ceza mahkumiyeti veya güvenlik tedbiri olup olmadığını gösteren adli sicil bilgisinin özlük dosyasına eklenmesi mevzuatta öngörülüyorsa, bu durumda Kanunun 6. maddesinin üçüncü fıkrasının ilk cümlesindeki hukuka uygunluk sebebine dayanılarak ilgili kişinin açık rızası aranmaksızın bu hassas verileri işverence işlenebilecektir. Örneğin, 5187 sayılı Basın Kanunu'na göre sorumlu müdür olarak istihdam edilebilmek için aday işçinin kamu hizmetinden yasaklanmamış olması ve yüz kızartıcı bir suçtan mahkum olmaması koşulları aranmaktadır. 2219 sayılı Hususi Hastaneler Kanunu uyarınca hastanenin mesul müdürünün herhangi bir suçtan ötürü ağır hapse veya şeref ve haysiyeti bozan suçlardan kaynaklı hapis cezasına mahkûm

³⁵³ Başar, ss. 76,77.

³⁵⁴ Başar, ss. 92,93.

³⁵⁵ Öztürk ve diğerleri, s. 84.

olmaması gerekmektedir. Görüldüğü üzere bu konudaki yasal düzenlemelerin varlığı halinde, veri sorumlusu işveren, işçinin özel nitelikli verisi olan adli sicil kayıtlarını işçinin açık rızasına ihtiyaç duymaksızın özlük dosyasına kaydedebilecektir³⁵⁶. Yine işçinin bağlı olduğu sendika bilgisinin işveren tarafından özlük dosyasında tutulması da 6698 sayılı Kanunun 6. maddesinin üçüncü fıkrası kapsamında değerlendirilecektir³⁵⁷. Sağlık ve cinsel hayat dışında kalan özel nitelikli verilerin ilgili kişinin açık rızasına ihtiyaç duyulmadan işlenebilmesine ilişkin getirilen istisna düzenlemesinde dikkat çeken husus, salt “*kanunlarda öngörülme*” ifadesine yer verilmiş olmasıdır. Oysa özel nitelikte olmayan kişisel verilerin ilgili kişinin açık rızası olmaksızın işlenebileceği istisna halleri düzenleyen 5. madde hükmünde “*kanunlarda açıkça öngörülme*” kriteri aranmaktaydı. Daha sıkı bir koruma rejimi gerektiren özel nitelikteki kişisel veriler bakımından “*kanunlarda açıkça öngörülme*” ifadesine yer verilmemiş olması, hükmün amacına zarar veren bir niteliğe sahiptir. Hassas veriler için kanunlarda açıkça öngörülme hali evleviyetle geçerli olmalıdır³⁵⁸.

6698 sayılı Kanunun 6. maddesinin üçüncü fıkrasında, ikinci ayırım olarak, sağlık ve cinsel hayata ilişkin verilerin işlenme esaslarına ilişkin ayrı bir düzenleme getirilmiştir. Buna göre, sağlık ve cinsel hayata ilişkin kişisel verilerin ilgili kişinin açık rızasına ihtiyaç duyulmaksızın işlenebilmesinde, kanun koyucunun, diğer özel nitelikli verilere kıyasla daha da hassas davrandığı dikkat çekmektedir. Zira maddede, sağlık ve cinsel hayata ilişkin verilerin hem işlenebileceği haller bakımından hem de bu verileri işleyebilecek kişiler bakımından özel bir sayım ve sınırlandırmaya gidilmiştir. Bahse konu hüküm uyarınca, sağlık ve cinsel hayata ilişkin kişisel veriler, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgili kişinin açık rızası aranmaksızın işlenebilir. Kanun koyucu, sağlık ve cinsel hayata ilişkin verilerin, ilgili kişinin rızası aranmaksızın işlenebilmesi hususunda iki koşulun varlığını birlikte aramaktadır. Bunlardan ilki, kanunda belirtilen kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi

³⁵⁶ Neslihan Emre İlhan, “Kişisel Verilerin Korunması Kanunu Kapsamında İşverenin Özlük Dosyası Oluşturma Yükümlülüğü”, **İstanbul Barosu Dergisi**, Cilt:94, Sayı:1, 2020, s.82.

³⁵⁷ Dülger, *Kişisel Veriler Hukuku*, s. 221.

³⁵⁸ Küzeci, *Kişisel Verilerin Korunması*, ss. 405,406.

ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi veri işleme amaçlarından en az birinin somut olayda bulunması, ikincisi ise yine kanun hükmünde belirtilen sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından veri işleme faaliyetinin gerçekleştirilmesi koşuludur³⁵⁹. Sır saklama yükümlülüğü altında bulunan kişilere örnek olarak hekimler verilebilir. Zira hekimlerin sır saklama yükümlülüğü eskiden beri var olan bir yükümlülüktür. Bu yükümlülük hekim ile hastası arasındaki güvene dayalı tedavi ilişkisinin doğal bir sonucudur³⁶⁰. Nitekim Hekimlik Meslek Etiği Kurallarının 9. maddesinde hekimin hastasından mesleğini uygularken öğrendiği sırları açıklayamayacağı, hastanın ölmesi veya hekimle ilişkisinin sona ermesi halinde dahi bu yükümlülüğün ortadan kalkmayacağı ifade edilmektedir³⁶¹. Bununla birlikte hekimlerin, 6698 sayılı Kanunun 6. maddesinde belirtilen amaçlardan en az birinin var olduğu durumlarda sır saklama yükümlülüğü altında bulunan kişilerden sayılması sebebiyle hastanın sağlık ve cinsel hayata ilişkin verilerini onun açık rızasına ihtiyaç duymaksızın işlemesi mümkün olacaktır. Konuya mevzuat temelinde verilebilecek münferit bir örnek 1593 sayılı Umumi Hıfzıssıhha Kanunun 58. maddesi hükmüdür. Hüküm uyarınca aynı Kanunun 57. maddesinde belirtilen hastalıkların vuku bulduğu anlaşılır yahut bulacağından şüphe duyulursa hekimler 24 saat içerisinde sağlık müdürlüğü başta olmak üzere hükümde belirtilen yerlere hastanın isim ve adresini bildirmekle yükümlüdür. Kanunun 6. maddesinde yer verilen, sağlık ve cinsel hayata ilişkin verileri işleyebilecekler arasında sayılan yetkili kurum veya kuruluşlara ise örnek, madde hükmünün gerekçesinde verilmiştir. Gerekçeye göre, Sağlık Bakanlığı ile her türlü sağlık kuruluşunun ve Sosyal Güvenlik Kurumunun hükümde yazılı amaçlarla tuttıkları veriler ve kayıtlar, 6. maddenin üçüncü fıkrasındaki sağlık ve cinsel hayata ilişkin özel nitelikli verilerin işlenmesi kapsamında değerlendirilecektir. Sağlık Bakanlığının bu çerçevede gerçekleştirmiş olduğu veri işleme faaliyetine güncel bir örnek “*Hayat Eve Sığar*” mobil uygulamasıdır. 2020 yılında dünyayı etkisi altına alan Kovid-19 virüsü salgını, birçok devleti kamu sağlığını koruyabilmek amacıyla çeşitli önlemler almaya itmiştir. Bu çerçevede Sağlık Bakanlığı da vakıa

³⁵⁹ Öztürk ve diğerleri, s. 85.

³⁶⁰ Yusuf Büyükay, “Hekimin Sır Saklama Yükümlülüğü”, **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:7, Sayı:1-2, 2004, ss. 383,384.

³⁶¹ Hekimlik Meslek Etiği Kuralları, www.ttb.org.tr, (01.03.2023).

sayılarının tespit edilebilmesi, salgının yayılmasını engelleyici çeşitli önlemlerin alınması ve alınan önlemlerin denetlenebilmesi gibi amaçlarla ismi yukarıda zikredilen mobil uygulamayı geliştirmiştir. Uygulamada yer alan Hes kodu, ilgili kişinin sağlık verisi başta olmak üzere bazı kişisel verilerini barındırmakta olup bu kod ile özellikle toplu alanlarda salgının yayılması kontrol altında tutulmaya çalışılmıştır. Ayrıca mobil uygulamada, Kovid-19 hastalığı geçirmekte olan kişilerin tespiti yapılarak bu kişilerin kişisel verileri anonimleştirilmek suretiyle hastalığın bulaşma riski çeşitli renklendirmelerle bir harita üzerinde kullanıcıların bilgisine sunulmaktadır. Söz konusu haritalandırmada noktasal bir gösterim kullanılmamış, hastalık taşıyan yahut temaslı kişilerin bulunduğu adres mevkileri yoğunluk haritası biçiminde renk işaretlemeleriyle belirtilmiştir³⁶². Sağlık Bakanlığı tarafından geliştirilen bu uygulamada gerçekleştirilen veri işleme faaliyeti, 6698 sayılı Kanunun 6.maddesinin üçüncü fıkrasında yer alan kamu sağlığının korunması, tıbbi teşhis ve tedavi hizmetlerinin yürütülmesi, sağlık hizmetlerinin planlanması gibi amaçlarla yetkili kurum ve kuruluşlar tarafından sağlık verilerinin, ilgilinin açık rızasına ihtiyaç duyulmaksızın işlenmesi hususuna güncel bir örnek oluşturmaktadır. Burada Kanunun 28/1-ç maddesine değinmekte yarar vardır. Anılan hükümde 6698 sayılı Kanun hükümlerinin uygulanmayacağı istisna hallerden birine yer verilmektedir. Hükme göre, kamu düzeninin sağlanmasına yönelik olarak kanunla görev ve yetki verilmiş kamu kurumlarınca yürütülen önleyici, koruyucu faaliyetler çerçevesinde kişisel verilerin işlenmesi halinde 6698 sayılı Kanun uygulanmayacaktır. İlgili hükümden hareketle, kamu sağlığının korunması da kamu düzeninin bir unsuru olarak nitelendirilebileceğinden, bunun sağlanmasına yönelik idarenin önleyici kolluk faaliyetleri çerçevesinde kişisel verileri işleme 6698 sayılı Kanunun hükümlerinin uygulanmayacağı şeklinde bir değerlendirme yapmaya da müsaittir³⁶³. Haliyle kamu sağlığı söz konusu olduğunda kamu kurumlarının gerçekleştirdiği önleyici faaliyetler çerçevesindeki veri işleme uygulamaları, m.28/1-ç'deki istisna kapsamında değerlendirilebileceğinden Kanunun 6. maddesinin üçüncü fıkrasındaki koşulların aranmasına gerek kalmayacağı yorumu da yapılabilecektir.

³⁶² Murat Özdemir ve diğerleri, “Kişisel Sağlık Verilerinin 6698 Sayılı Kanun Çerçevesinde Korunması”, **19 Mayıs Sosyal Bilimler Dergisi**, Cilt:3, Sayı:1, 2022, s. 92.

³⁶³ Başar, ss.102,103.

6698 sayılı Kanunun m. 6/4’de özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınmasının şart olduğu ifade edilmiştir. Yine Kanunun “*Kurulun görev ve yetkileri*” başlıklı 22. maddesinin birinci fıkrasının 4 bendinde, özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemekle Kurul görevli kılınmıştır. Bu doğrultuda Kurul tarafından 31/01/2018 tarihli ve 2018/10 Sayılı “*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*” isimli karar³⁶⁴ 07/03/2018 tarihli Resmî Gazete’de yayımlanmıştır³⁶⁵. Böylelikle özel nitelikli kişisel verilerin işlenmesinde veri sorumlularının alması gereken önlemler detaylı bir biçimde ele alınmıştır. Kararda, özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara, kanun ve buna ilişkin yönetmelikler ile özel nitelikli kişisel veri güvenliği hususlarında düzenli olarak eğitimler verilmesi, gizlilik sözleşmelerinin yapılması, özel nitelikli kişisel verilerin güvenliğine ilişkin kuralları net şekilde belli, yönetilebilir, sistemli ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi, verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net bir şekilde tanımlanması, yetki kontrollerinin periyodik aralıklarla gerçekleştirilmesi, görev değişikliği olan ya da işten ayrılan çalışanlar söz konusu ise yetkilerinin derhal kaldırılması, ayrıca bu kapsamda veri sorumlusu tarafından tahsisli envanterin iade alınması gerektiği ifade edilmektedir. Bununla birlikte Kurul özel nitelikli kişisel verilerin saklandığı ortamlar bakımından da alınması gereken önlemlere değinmiştir. Şayet özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması, bu ortamların fiziksel güvenliğinin sağlanması suretiyle yetkisiz giriş çıkışların önlenmesi şarttır. Kararda özel nitelikli kişisel verilen aktarımına ilişkin olarak da alınması gerekli görülen tedbirlere yer verilmiştir. Ayrıca Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır. Görüldüğü üzere Kurul tarafından özel nitelikli kişisel verilerin işlenmesinde veri sorumlularınca alınması

³⁶⁴ Karar metni için bkz. <https://www.kvkk.gov.tr/Icerik/4110/2018-10>, (01.03.2023).

³⁶⁵ İlgili R.G. için bkz. <https://www.resmigazete.gov.tr/eskiler/2018/03/20180307.htm>, (01.03.2023).

gereken yeterli tedbirler, bu verilerin işlenmesinde görev alan kişilerden verilerin tutulduğu ortama ve hatta aktarım süreçlerine kadar geniş bir yelpazede düzenlenmiştir. Özel nitelikli kişisel veri işleyen veri sorumlularının veri işleme süreçlerinde mutlaka bu önlemleri almaları gerekmektedir.

Son olarak, özel nitelikli kişisel verilerin hukuka aykırı işlenmesinin önüne geçilmesi ve bireylerin temel hak ve özgürlüklerinin korunması bakımından önemli gördüğümüz bir başka hususa değinmek istiyoruz. Şöyle ki, bazı kişisel veri işleme faaliyetlerinde somut olaya hangi veri işleme şartının uygulanması gerektiği tereddüde sebebiyet verebilir. Zira örneğin, güvenlik kamerası kaydı alınması faaliyetinde bu kayıtlarda yer alan görüntüler hem kişilere ait biyometrik veri, kılık-kıyafet verisi gibi hassas verileri içermekte hem de hassas olmayan kişisel verileri barındırmaktadır. Böyle bir durumda veri sorumlusunun hangi veri işleme şartına uygun hareket etmesi gerektiği veri işlemenin amacına göre belirlenmelidir. Eğer veri sorumlusunun amacı yalnızca güvenliğin sağlanması ise Kanunun 5. maddesinin; biyometrik veri gibi özel nitelikli verileri toplamak amaçlanıyorsa Kanunun 6.maddesinin uygulanması gerekmektedir³⁶⁶.

D. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi

1. Genel Olarak

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi hakkının dayanağı en başta Anayasamızın 20/3. maddesidir. Zira daha önce de belirtmiş olduğumuz üzere ilgili hükümde, kendisi ile ilgili kişisel verilerin korunmasını herkesin isteme hakkına sahip olduğu belirtilmektedir. Hiç şüphesiz ki, kişisel verilerinin silinmesini ilgili kişinin talep etme hakkı da bu kapsamdadır³⁶⁷. 6698 sayılı Kanunun 7. maddesinin birinci fıkrasında 6698 sayılı Kanun ve ilgili diğer Kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebebin ortadan kalkması halinde kişisel verilerin re'sen veya ilgili kişinin talebi üzerine veri

³⁶⁶ Öztürk ve diğerleri, s. 84.

³⁶⁷ Hilal Tuğba Öksüzöğlu, “6698 Sayılı Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Hukukunda Kişisel Verilerin Silinmesi ve Düzeltilmesi”, **Bilişim Hukuku Dergisi**, Cilt:1, Sayı:2, 2019, ss. 192,193.

sorumlusu tarafından silinmesi, yok edilmesi veya anonim hale getirilmesi gerektiği ifade edilmektedir. Kişisel verilerin işlenmesini gerektiren sebebin ortadan kalkması hallerine örnek vermek gerekirse, sınırlı bir sayım teşkil etmemekle birlikte, verilerin işlenmesine dayanak yasa hükümlerinin değişmesi yahut kaldırılması, sözleşmesel ilişkilere bağlı veri işleme faaliyetlerinde bu sözleşmenin geçersizliği, feshi veya sözleşmeden dönülmesi, yalnızca açık rıza şartına dayalı gerçekleştirilen veri işleme faaliyetlerinde ilgili kişinin rızasını geri alması, Kanunun 5. ve 6. maddelerindeki kişisel veri işleme koşullarının somut olayda ortadan kalkması, verilerin saklanma süresinin geçmesine rağmen verileri daha uzun süre saklamayı haklı kılacak bir nedenin bulunmaması gibi durumlar örnek verilebilir. Bu hallerde kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi gerekecektir³⁶⁸.

6698 sayılı Kanunun 7. maddesinin ikinci fıkrasında ise kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu belirtilmiştir. Örneğin, veri sorumlusu tarafından kişisel verilerin aktarıldığı tüzel kişiliğin bir devlet kurumu olması ve kanundan kaynaklı bir istisnanın bulunması halinde silme, yok etme veya anonim hale getirmenin şekli ve süresi bu kanun hükümlerine göre belirlenecektir³⁶⁹. Yine hükmün gerekçesinde de belirtildiği üzere örnek olarak Adli Sicil Kanunu'ndaki verilerin silinmesi veya yok edilmesine ilişkin düzenlemeler 6698 sayılı Kanuna göre öncelikli olarak uygulanır.

6698 sayılı Kanunun 7. maddesinin son fıkrasında ise yönetmelikle kişisel verilerin yok edilmesine, silinmesine veya anonim hale getirilmesine ilişkin usul ve esasların düzenleneceği öngörülmüştür. Nitekim Kanunun 22. maddesinin e bendinde, Kurulun görev alanına giren konularda gerekli düzenleyici işlemleri yapmakla görevli olduğu hükmü yer almaktadır. Bu doğrultuda Kurulun hazırlamış olduğu “*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik*” 28 Ekim 2017 tarihli Resmî Gazetede yayımlanmış ve 1 Ocak 2018 tarihinde yürürlüğe girmiştir. Görüldüğü üzere kanun koyucu kişisel verilerin yok edilmesi, silinmesi veya anonim hale getirilmesi hususunda genel kurala değinmekle yetinmiş, konunun detaylarına ilişkin ise yönetmeliğe atıfta bulunmuştur. Ayrıca Kişisel Verileri Koruma Kurumu tarafından yönetmeliğe dayanarak yapılacak

³⁶⁸ Çekin, ss. 93, 94.

³⁶⁹ Dülger, Kişisel Veriler Hukuku, s. 253.

işlemlerin nasıl yapılacağı konusunda açıklık sağlanması ve iyi uygulama örnekleri oluşabilmesini amacıyla³⁷⁰ “*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi*” isimli bir rehber de yayımlanmıştır.

2. Kişisel Verilerin İmhası

“Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelikte” (Yönetmelik) sıklıkla zikredilen “*imha*” kavramı aynı Yönetmeliğin “*Tanımlar*” başlıklı 4. maddesinin (c) bendinde kişisel verilerin yok edilmesi, silinmesi veya anonim hale getirilmesini ifade eden üst kavram olarak tanımlanmıştır. Biz de bu konu başlığı altında silinme, yok edilme veya anonim hale getirme kavramları ile birlikte yer yer “*imha*” kavramını da kullanacağız.

Yönetmeliğin birinci bölümünde yer verilen ve Yönetmeliğin amacı ile kapsamını düzenleyen hükümler uyarınca özetle, tamamen veya kısmen otomatik yollarla yahut bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine kısaca kişisel verilerin imhasına ilişkin usul ve esaslar söz konusu Yönetmelikle düzenlenmekte ve işbu Yönetmelik hükümleri veri sorumluları hakkında uygulanmaktadır.

Yönetmeliğin “*Kişisel Veri Saklama ve İmha Politikası*” başlığını taşıyan ikinci bölümü kapsamında 5. maddede 6698 sayılı Kanunun 16. maddesi uyarınca Veri Sorumluları Siciline kayıt yükümlülüğü bulunan veri sorumlularının³⁷¹ kişisel veri saklama ve imha politikası hazırlama yükümlülüğü bulunduğu, 6. maddede ise kişisel

³⁷⁰ Kişisel Verileri Koruma Kurumu, “*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi*”, 2018, s. 2.

³⁷¹ 6698 sayılı Kanunun 16/2. maddesi çerçevesinde Kurul, Veri Sorumluları Siciline kayıt yükümlülüğünden istisna tutulacak veri sorumlularına ilişkin bazı kararlar almıştır. Örneğin 15.05.2018 tarih ve 30422 sayılı Resmî Gazetede yayımlanan, 02.04.2018 tarih ve 2018/32 sayılı Kurul kararında, herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler, noterler, dernekler, vakıflar, sendikalar, siyasi partiler, avukatlar ve mali müşavirlerin Veri Sorumluları siciline kayıt yükümlülüğünden istisna tutulmuştur. Yine 18.08.2018 tarihinde 30513 sayılı Resmî Gazete yayımlanan, 19.07.2018 tarih ve 2018/87 sayılı Kurul kararında, yıllık çalışan sayısı 50’den az ve yıllık mali bilanço toplamı 25 milyon TL’den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanların Veri Sorumluları Siciline kayıt yükümlülüğünden istisna tutulduğu ifade edilmiştir.

veri saklama ve imha politikasının kapsamına ilişkin detaylı düzenlemeler yer almaktadır. Kişisel verileri saklama ve imha politikası, Yönetmeliğin 4. maddesinde, tanımlanmıştır. Burada Kişisel Verileri Koruma Kurumu için hazırlanan kişisel veri saklama ve imha politikası metnine de değinmek gerekir. Zira Kurumun resmi internet sitesinde belirtildiği üzere veri sorumlularına örnek ve yardımcı olması amacıyla hazırlanan kişisel veri saklama ve imha politikası, uygulamada veri sorumlularına faydalı ve yol gösterici niteliktedir³⁷². Yönetmeliğin 5. maddesinin 3. fıkrasında ise kişisel veri saklama ve imha politikası hazırlama yükümlülüğü altında olmayan veri sorumlularının da kişisel veri yok etme, saklama veya anonim hale getirme yükümlülüğünün Kanun ve bu yönetmelik uyarınca devam ettiği ayrıca belirtilmiştir. Görüldüğü üzere kişisel veri saklama ve imha politikası hazırlama yükümlülüğü bakımından Yönetmelik, veri sorumluları arasında, Veri Sorumluları Siciline Kayıt yükümlülüğü bulunma durumuna göre bir ayrıma gitmiştir. Ancak kişisel veri silme, saklama, yok etme veya anonim hale getirme yükümlülüğü bakımından Kanun ve Yönetmelik hükümlerinin, herhangi bir ayırım olmaksızın, bütün veri sorumluları bakımından uygulanması esası öngörülmüştür.

Kişisel verilerin yok edilmesi, silinmesi veya anonim hale getirilmesi işlemlerinde en başta kavramların içeriğinin doldurulması gerekmektedir. Nitekim bu doğrultuda gerek 6698 sayılı Kanun gerekse Yönetmelikte bu kavramlara ilişkin tanımlara yer verilmiştir. Yönetmeliğin “*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi*” başlığını taşıyan üçüncü bölümünde, 8. maddede kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar³⁷³ için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi olarak ifade edilmiştir. Kişisel verilerin yok edilmesi ise, Yönetmeliğin 9. maddesinde, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi olarak belirtilmiştir. İki kavrama ilişkin tanımlar ilk bakışta aynı gibi görünse de aralarında temel farklılıklar bulunmaktadır. Kişisel verilerin silinmesi işleminde bu verilerin geri dönüştürülmesinin imkânsız olması aranmaz. Yalnızca ilgili

³⁷² İlgili metne ulaşmak için bkz. <https://www.kvkk.gov.tr/Icerik/5387/KVKK-Kisisel-Veri-Saklama-ve-Imha-Politikasi>, (13.03.2023).

³⁷³ İlgili kullanıcı kavramı Yönetmeliğin 4.maddesinde, verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler olarak tanımlanmıştır.

kullanıcıların bir daha bu verilere erişememesi ve kullanamaması gerekir. Bunlar dışında örneğin bir suç soruşturmasında görevli adli kolluk memuru gibi üçüncü kişilerin bu verileri geri dönüştürerek verilere tekrar erişmesi ve verileri kullanması mümkündür. Oysa yok etme işleminde kişisel veriler, hiç kimse tarafından hiçbir şekilde, adli bilişim ve veri kurtarma yazılımları dahil geri getirilemez, erişilemez ve kullanılamaz hale gelmektedir³⁷⁴. Anonim hale getirme kavramı ise Yönetmelikte ve Kanunda düzenlenmiştir. 6698 sayılı Kanunun 3. maddesinde anonim hale getirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi olarak ifade edilmiştir. Diğer bir ifadeyle, anonim veriler, gerçek kişiyle ilişkisi tamamıyla kesilmiş verilerdir³⁷⁵. Bu çerçevede kişisel veri anonimleştirme işlemi, kişisel verilerin başka verilerle eşleştirilse, aralarında bir bağ kurulsa dahi o verinin hiçbir surette ilgili kişiyi belirlenebilir kılamayacak duruma getirilmesi işlemidir. Kişisel verilerin maskelenmesi, verinin ait olduğu gerçek kişiyi başka verilerle eşleştirme yapılmak suretiyle belirlenebilir kıldığından anonimleştirme için yetmemektedir³⁷⁶. Günümüzde gelişen teknolojik araçlar ile anonim verilerle dahi kişilerin kimliğinin tespitinin yapıldığı örnekler bulunmaktadır. AOL (America Online) ve Netflix firmalarının anonim hale getirip yayımlamış olduğu müşteri verileri buna örnektir. Nitekim New York Times gazetecileri AOL'nin yayımlamış olduğu anonim verileri başka veriler ile eşleştirerek bazı kullanıcıların kimliğini tespit etmiştir. Yine kişisel verilerin anonimleştirilmesi noktasında güncel bir sorun blockchain teknolojisinde söz konusudur. Zira bu teknolojiye bir işlem zinciri oluşturulmakta ve her yeni işlem adeta bu zincirin halkasını oluşturmaktadır. Böylelikle tüm işlemler en baştaki işleme kadar takip edilebilmektedir. Ayrıca bahse konu işlem zinciri, bütün ağ kullanıcıları ile paylaşılmakta ve zincirin herhangi bir halkasında yapılması muhtemel değişiklik diğer katılımcıların zincirle bağlantısının kopmasına neden olabilecek niteliktedir. Başka ifade ile zincirin bir halkasında (hash'de) yapılacak herhangi bir değişiklik bütün zinciri geçersiz hale getirmektedir. Haliyle ilgili kişinin blockchain sisteminde işlenen

³⁷⁴ Dülger, Kişisel Veriler Hukuku, ss. 256,257.

³⁷⁵ Furkan Güven Taştan, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, (Yayımlanmış Yüksek Lisans Tezi) , www.tez.yok.gov.tr, (11.03.2023), s. 56.

³⁷⁶ Dülger, Kişisel Veriler Hukuku, s. 257.

kişisel verileri hakkında veri sorumlusuna yönelteceği silme talebi diğer tüm işlemler üzerinde etki doğuracağından bu taleplerin, blockchain sisteminde karşılanması pek mümkün görünmemektedir³⁷⁷. Ezcümle, kişisel verilerin anonimleştirilmesi işlemi günümüzün teknolojik olanakları göz önünde bulundurulduğunda, veri sorumlusunun oldukça titiz hareket etmesini gerektiren bir faaliyettir. Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemlerinin açıklandığı Yönetmelikte söz konusu işlemleri gerçekleştiren veri sorumlusunun açıklamalardaki amaca ulaşılmasını sağlamak adına gerekli bütün teknik ve idari tedbirleri alacağı ifade edilmiştir. Zira Yönetmelikte, kişisel verilerin silinmesi bakımından, ilgili kullanıcıların silinen kişisel verilere tekrar erişememesi ve kullanamaması için; verilerin yok edilmesi ve anonim hale getirilmesi işlemleri bakımından da bu işlemlerle ilgili gereken her türlü teknik ve idari tedbirin veri sorumlusu tarafından alınması yükümlülüğü öngörülmüştür.

Yönetmeliğin 7. maddesinde kişisel verilerin imhası konusunda uygulanacak ilkeler düzenlenmektedir. Hükmün birinci fıkrasında temel kurala yer verilmiş ve Kanunun 5. ve 6. maddelerindeki veri işleme koşullarının hepsinin ortadan kalkması durumunda veri sorumlusu tarafından kendiliğinden yahut ilgili kişinin talebiyle kişisel verilerin yok edilmesi, silinmesi veya anonimleştirilmesi gerektiği belirtilmiştir. Maddenin üçüncü fıkrasında ise kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesiyle ilgili bütün işlemlerin veri sorumlusu tarafından kayıt altına alınması ve diğer hukuki yükümlülükler hariç olmak üzere bu kayıtların üç yıl süreyle saklanması yükümlülüğü getirilmiştir.

Kişisel verilerin imhasına ilişkin sürelerde Yönetmelik, “*periyodik imha işlemi*” yaklaşımını benimsemiştir. Gerçekten de bir taraftan sürekli olarak kişisel verileri kaydetme, aktarma vb. gibi işlemler yapan veri sorumlusunun aynı zamanda bu verilere ilişkin bir taraftan imha işlemi gerçekleştirmesi, bunların takibini yapması ciddi bir zaman ve emek harcamasına neden olabilecektir. Durumun farkında olan Kurum sürecin periyodik bir sürece bağlanmasını uygun görmüştür³⁷⁸. Bu çerçevede Yönetmeliğin 11. maddesinde Kurum, kişisel veri saklama ve imha politikası hazırlama yükümlülüğü bulunan ve böyle bir yükümlülüğü bulunmayan veri

³⁷⁷ Çekin, ss. 95,96.

³⁷⁸ Dülger, Kişisel Veriler Hukuku, s. 258.

sorumluları bakımından imha periyodu süreleri ile ilgili ayrıma gitmiştir. Hükümün birinci fıkrasında kişisel veri saklama ve imha politikası hazırlayan veri sorumlusunun, kişisel verileri yok etme, silme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi izleyen ilk periyodik imha işleminde bu verileri yukarıda sayılan üç işlemde birini kullanarak imha etmesi gerektiğini ifade etmiştir. İkinci fıkra imhanın gerçekleştirileceği zaman aralığının belirlenmesinde veri sorumlusunun hazırlayacağı politikada belirlenen sürelerin esas alınacağı ancak bu sürenin her halde altı ayı geçemeyeceği belirtilmiştir. Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü bulunmayan veri sorumluları bakımından ise Kurum, 11. maddenin üçüncü fıkrasında, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün doğmasından itibaren üç ay içinde söz konusu imha işlemlerinin gerçekleştirilmesi yükümlülüğünü düzenlemiştir.

İlgili kişinin kendisine ait kişisel verilerin silinmesi veya yok edilmesi talebine ilişkin olarak ise Yönetmeliğin 12. maddesinde düzenlemeler bulunmaktadır. Hükme göre, ilgili kişinin Kanunun 13. maddesine dayanarak veri sorumlusuna yönelttiği kişisel verilerinin silinmesi veya yok edilmesi hakkındaki talep, söz konusu kişisel verilerin işleme şartları ortadan kalkmış ise, veri sorumlusunca kişisel verilerin yok edilmesi, silinmesi veya anonim hale getirilmesi suretiyle yerine getirilir. Hükümde ayrıca bu talebin gereğinin en geç otuz günlük süre içerisinde veri sorumlusu tarafından sonuçlandırılacağı ve ilgili kişinin bilgilendirileceği ifade edilmiştir. Talebe konu veriler başkalarına aktarılmış ise veri sorumlusu, durumu bu kişilere bildirerek onların Yönetmelik hükümleri uyarınca gerekli işlemleri gerçekleştirmesini temin eder. Ancak, ilgili kişinin talebi olmasına karşın kişisel verileri işleme şartları henüz ortadan kalkmamış ise ilgili talep, veri sorumlusu tarafından Kanunun 13. maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilir. Bu ret cevabı ise ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamdan bildirilir. Elbette Yönetmeliğin bu hükümlerinin yanında somut olaya göre var ise diğer mevzuat hükümleri de göz önünde bulundurulmalıdır³⁷⁹. Örneğin Kurul bir kararında, devlet memurlarının memurluk döneminde haklarında yürütülmüş inceleme-soruşturma evraklarının imha edilmesi talebinin veri sorumlusu kamu kurumu tarafından yerine getirilmemesi nedeniyle kendisine yapılan bir başvuruya istinaden söz konusu

³⁷⁹ Göçmen Uyarer, s. 170.

evraklardaki kişisel bilgilerin, 657 sayılı Devlet Memurları Kanunu gereğince, memurların özlük dosyalarında saklanması gerektiği, Kamu Personeli Genel Tebliğine (Seri No:2) göre görevi sona eren memurların özlük dosyalarının kurumları tarafından saklanacağı ve Devlet Arşiv Hizmetleri Yönetmeliği uyarınca son işlem tarihi üzerinden yüz bir yıl geçmemiş memuriyet sicil dosyaları içerisinde yer aldığı hususlarından hareketle, 6698 sayılı kanunun 7. maddesinde belirtilen kişisel verilerin işlenmesini gerektiren nedenlerin ortadan kalkmadığını, başvurunun ilgili kamu kurumu tarafından karşılanmamasının uygun olduğunu ifade etmiştir³⁸⁰.

Son olarak kişisel verilerin imhası yöntemlerine ilişkin açıklamalarda bulunmakta yarar vardır. Zira bilindiği üzere gelişen teknolojinin etkisiyle kişisel veriler yalnızca fiziki ortamlarda değil aynı zamanda dijital ortamlarda da işleme tabi tutulmaktadır. Kişisel verilerin silinmesi işleminin ilgili kullanıcılar bakımından; kişisel verilerin yok edilmesi işleminin ise kimse tarafından söz konusu verilere hiçbir şekilde tekrar erişilememesi, geri getirilememesi ve yeniden kullanılamaması anlamını taşıdığını daha önce belirtmiştik. Kişisel verilerin silinmesi yahut yok edilmesi gereken hallerde bu işlemler, kişisel verilerin kayıt altında tutulduğu ortamın türüne göre farklı yöntemlerle gerçekleştirilebilmektedir. Nitekim bu hususlara da yer veren Kişisel Verileri Koruma Kurumu'nun yayımlamış olduğu Rehberde, kişisel verilerin yok edilmesi veya silinmesi gereken durumlarda hangi yöntemlerin kullanılması gerektiği, verilerin kaydedildiği ortam türüne göre detaylı bir biçimde açıklanmıştır. Rehberde göre, kişisel verilerin silinmesine ilişkin olarak, eğer veriler hizmet olarak uygulama türü bulut çözümlerinde yer alıyor ise sistemdeki veriler silme komutu ile silinmeli ve silme işleminin gerçekleştiği esnada ilgili kullanıcının bulut sistemindeki verileri geri getirme yetkisi bulunmamalıdır. Kâğıt ortamında bulunan kişisel verilerin silinmesinde ise karartma yöntemi kullanılmalıdır³⁸¹. Merkezi sunucuda yer alan ofis dosyalarında kişisel verilerin silinmesi işlemi, silme komutu ile gerçekleştirilmeli veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekmektedir. Veri tabanlarında söz konusu işlem, kişisel verilerin bulunduğu satırların veri tabanı komutları kullanılmak suretiyle gerçekleştirilmelidir. Gerek merkezi sunucuda yer alan ofis dosyalarındaki gerekse veri tabanlarındaki

³⁸⁰ Kişisel Verileri Koruma Kurumunun 28.06.2018 tarih ve 2018/69 sayılı kararı, www.kvkk.gov.tr, (13.03.2023).

³⁸¹ Kişisel Verileri Koruma Kurumu, "Kişisel Verilerin Silinmesi", 2018, s. 7.

kişisel verilerin silinmesi işlemlerinde, bu işlemler gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmamasına dikkat edilmelidir. Yine Rehberde, USB bellek gibi taşınabilir medyada bulunan kişisel verilerin bu ortamlara uygun yazılımlar vasıtasıyla silinmesi gerektiği ifade edilmektedir³⁸². Kişisel verilerin yok edilmesine ilişkin olarak ise Rehber, yerel sistemler söz konusu olduğunda bu sistemler üzerindeki kişisel verilerin, de-manyetize etme, fiziksel olarak yok etme veya üzerine yazma gibi yöntemler kullanılarak yok edilebileceğini, kağıt ve mikrofiş ortamlar söz konusu olduğunda ana ortamın kendisi olan kağıt imha veya kırpma makineleriyle anlaşılabilir ve geri birleştirilemeyecek biçimde küçük parçalara bölünmesi gerektiğini, bulut ortamı söz konusu olduğunda bulut bilişim sistemindeki söz konusu kişisel verilere erişimi olanaklı kılan bütün şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerektiğini, çevresel sistemler söz konusu olduğunda ise yine Rehberde detayları belirtilen birtakım teknik işlemler uygulanmak suretiyle kişisel verilerin yok edilebileceğini belirtmiştir. Kişisel verilerin anonim hale getirilmesi işleminde kullanılacak yöntemlere ilişkin olarak Rehber, verilerin bulunduğu kayıt sistemindeki kayıtlara uygulanan ve otomatik olan yahut olmayan grupta, rastgele hale getirme, türetme, genelleştirme, maskeleye gibi yöntemlerle yürütülen bağ koparma işlemlerinin tamamına anonim hale getirme yöntemleri adının verildiğini ifade etmiştir. Burada Rehberin “*bağ koparma*” ile kastetmiş olduğu husus, verilerin anonim hale getirilmesindeki amaç olan kişisel veri ile o kişisel verinin tanımladığı gerçek kişi arasındaki bağın kopartılması olup artık ilgili kişi ile söz konusu kişisel verilerin ilişkilendirilemeyecek duruma getirilmesidir³⁸³. Son olarak kişisel verilerin anonim hale getirilmesi ile takma isim vermek suretiyle kimliğin gizlenmesi hususlarının birbirinden farklı olduğunu belirtmekte yarar görüyoruz. Zira kişisel verilerin anonimleştirilmesi işleminde veri ile veri sahibi arasındaki ilişki herkes için, kalıcı ve bir daha geri döndürülemez bir biçimde kesilmekte iken; takma isim verilerek kimliğin gizlenmesi halinde kişisel veri, üçüncü kişilere karşı korunmakta ancak veri ile veri sahibi arasındaki bağ mutlak olarak kesilmemektedir. Konuya örnek olarak bir üniversitenin sınav sonucu açıklama sisteminde öğrencilerinin kimlik bilgilerinden olan isim ve soy isimlerinin baş harflerine yer

³⁸² Kişisel Verileri Koruma Kurumu, “Kişisel Verilerin Silinmesi”, s.9; Göçmen Uyarer, s. 171.

³⁸³ Kişisel Verileri Koruma Kurumu, “Kişisel Verilerin Silinmesi”, s. 16.

vererek geri kalan harfleri “****” şeklinde maskeleyerek göstermesi verilebilir. Bu durumda her ne kadar üçüncü kişilere karşı anonimleşme sağlansa da üniversite tarafından veri ve veri sahibi arasındaki ilişki bilinir olduğundan üniversitenin veriler üzerindeki sorumluluğu devam etmektedir³⁸⁴.

E. Kişisel Verilerin Aktarılması

1. Genel Olarak

Aktarım faaliyeti, her ne kadar 6698 sayılı Kanunun 3. maddesinin 1.fıkrasının e) bendinde tanımlanan veri işleme türlerinden biri ise de kanun koyucu bu faaliyeti kendi içerisinde ikili bir ayrıma tabi tutarak ayrı maddelerde düzenleme ihtiyacı hissetmiştir³⁸⁵. Nitekim 6698 sayılı Kanunun 8. maddesi kişisel verilerin yurt içinde aktarılmasını; 9. maddesi ise kişisel verilerin yurt dışına aktarılmasını düzenlemektedir. Kişisel verilerin hukuka uygun olarak aktarılabilmesi için belirtilen maddelerdeki şartlara uygun bir aktarım faaliyeti gerçekleştirilmesi gerekmektedir³⁸⁶.

2. Yurt İçinde Aktarım

Kanunun kişisel verilerin yurt içinde aktarılmasını düzenleyen 8. maddesinin ilk fıkrasında, ilgili kişinin açık rızası olmaksızın kişisel verilerin aktarılamayacağı ifade edilmektedir. Aynı maddenin ikinci fıkrasında ise kişisel verilerin, 5. maddenin ikinci fıkrasında ve yeterli önlemlerin alınması kaydıyla 6. maddenin üçüncü fıkrasında belirtilen şartlardan birinin bulunması durumunda ilgili kişinin açık rızası aranmaksızın aktarıma tabi tutulabileceği belirtilmektedir. Görüldüğü üzere, kişisel verilerin işlenmesi bakımından Kanunun 5. ve 6. maddelerinde aranan hukuka uygunluk sebepleri, bir veri işleme faaliyeti türü olan aktarım konusunda da benzer şekilde aranmaktadır³⁸⁷. Göze çarpan tek farklılık 8. maddede, özel nitelikli kişisel

³⁸⁴ Öztürk ve diğerleri, ss. 92,93; Dülger, Kişisel Veriler Hukuku, s. 257.

³⁸⁵ Küzeci, Kişisel Verilerin, s. 410.

³⁸⁶ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, s. 87.

³⁸⁷ Çekin, s. 75.

verilerin aktarımı hususunda yeterli önlemlerin alınması şartının düzenlenmiş olmasıdır³⁸⁸. Kanunun 22. maddesinin birinci fıkrasının ç) bendi uyarınca özel nitelikli kişisel verilerin işlenebilmesi için aranan yeterli önlemlerin belirlenmesi görevi Kişisel Verileri Koruma Kuruluna verilmiştir. Nitekim bu doğrultuda Kurul “yeterli önlemler” ifadesinden ne anlaşılması gerektiği konusunda uygulamaya yol gösterici nitelikte olan, 31/01/2018 tarih ve 2018/10 sayılı “*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*” isimli kararı yayımlamıştır³⁸⁹.

Kanunun yurt içinde kişisel verilerin aktarılmasını düzenleyen 8. maddesinin üçüncü ve son fıkrasında ise, kişisel verilerin aktarılmasına ilişkin olarak diğer kanunlarda yer alan hükümlerin saklı olduğu belirtilmektedir. Nitekim elektronik haberleşme, sağlık ve bankacılık gibi sektörlerle ilişkin mevzuatta da kişisel verilerin korunması hakkında çeşitli hükümler bulunmaktadır. Bu düzenlemelerin önemli bir kısmında veri aktarımı bakımından Kişisel Verilerin Korunması Kanununun getirmiş olduğu sistem ile büyük ölçüde paralellik bulunduğu gözlemlenmektedir. Diğer kanunlarda kişisel verilerin aktarılmasına ilişkin yer verilen düzenlemelere örnek olarak Bankacılık Kanununun 73. maddesi gösterilebilir. Hükümde, diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğini haiz bilgilerin, yine 73. maddede belirtilen istisnai haller dışında, 6698 sayılı Kanun çerçevesinde müşterinin açık rızası alınmış olsa da yurt içinde veya yurt dışındaki üçüncü kişilerle müşteriden gelen bir talep yahut talimat olmaksızın paylaşılamayacağı ve onlara aktarılamayacağı ifade edilmektedir³⁹⁰.

Uygulamada örneklerine sık rastlandığı üzere kimi veri sorumlularınca, veri işleme faaliyeti, veri işleyen sıfatındaki bir üçüncü gerçek veya tüzel kişiye gördürülebilmektedir. Nitekim, Kanunun 3. maddesinde veri sorumlusu, “*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*” olarak tanımlanmaktayken; veri işleyen, “*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*” olarak ifade edilmiştir. Veri

³⁸⁸ Küzeci, Kişisel Verilerin Korunması, s. 410.

³⁸⁹ Bahsi geçen karar özetine ulaşmak için bkz. [https://www.kvkk.gov.tr/Icerik/4110/2018-10,\(10.07.2023\).](https://www.kvkk.gov.tr/Icerik/4110/2018-10,(10.07.2023).)

³⁹⁰ Sevgi Ünsal Özden ve diğerleri, “Kişisel Veri Aktarımı ve Bankacılık Kanunu Madde 73 Değişikliği”, **Kişisel Verileri Koruma Dergisi**, Cilt:3, Sayı:1, 2021, ss. 26,32.

sorumlusu ve onun adına kişisel verileri işlemekle yetkilendirilen veri işleyen arasındaki veri aktarım faaliyetinin, 8. madde kapsamında değerlendirilip değerlendirilmeyeceğine ilişkin ise Kanunumuzda bir netlik söz konusu değildir. Bu çerçevede, bahsi geçen durumun ortaya koyabileceği iki muhtemel sonuca değinmekte fayda vardır. Bunlardan ilki, veri sorumlusunun verdiği yetkiye dayanarak ve onun adına veri işleme faaliyetinde bulunan veri işleyene, veri sorumlusu tarafından gerçekleştirilecek kişisel veri aktarımında 8. maddenin uygulanması, buradaki hukuka uygunluk sebeplerinin veri sorumlusu ile veri işleyen arasındaki veri aktarımlarında da aranması gerektiğine ilişkindir. Bir diğer muhtemel sonuç ise, veri sorumlusu ile onun yetkilendirmesiyle ve onun adına veri işleyen kişi arasındaki veri aktarımlarının, 8. maddedeki şartlardan muaf tutulması gerektiğidir. Zira kişisel verilerin işlenmesinin kapsamına Kanunun 3. maddesindeki tanımdan hareketle kişisel verilerin devralınması da girmekte ve kişisel verileri devralan kişi veri sorumlusu sıfatını haiz olmaktadır. Burada, bilhassa devralan konumuna veri işleyenin konulması, onun veri sorumlusu olarak nitelendirilmesine sebep olabilecektir. Oysa veri işleyen sadece veri sorumlusunun yetkilendirmesiyle ve onun adına verileri işlemekte, veri sorumlusu sıfatı taşımamaktadır. Haliyle veri sorumlusu tarafından veri işleyene gerçekleştirilen aktarımlar teknik anlamda kişisel verilerin aktarılması olarak değerlendirilemeyecektir³⁹¹. Böyle bir kavram karışıklığına yer vermemek amacıyla ortaya konulmaya çalışılan iki değerlendirme ve sonuç içerisinde daha isabetli olanın, ikinci yaklaşım olduğu kanaatini taşıyoruz. Böylelikle Kanunun tamamında korunmaya çalışılan veri sorumlusu ve veri işleyen kavramları arasındaki temel farklılığın bu yaklaşım tercih edilerek korunmaya devam edilebileceğini düşünüyoruz. Ayrıca veri sorumlusu sıfatını haiz bir tüzel kişinin kendi bünyesi içerisinde gerçekleşecek olan kişisel veri aktarımının da 8. madde kapsamında kişisel verilerin aktarılması olarak değerlendirilmemesi gerektiğini ifade etmek yararlı olacaktır. Örneğin aynı veri sorumlusu tüzel kişinin çalışanları yahut birimleri arasında gerçekleştirilecek veri aktarımı, 8. madde kapsamında bir kişisel veri aktarımı değildir³⁹². Buna karşılık, bir şirketler topluluğu bünyesi içerisinde yer alan birden

³⁹¹ Çekin, ss. 76,77.

³⁹² Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, s. 89.

fazla sayıdaki veri sorumlusu şirketler arasında gerçekleştirilen kişisel veri aktarımı, Kurul kararında 8. madde kapsamında, üçüncü kişiye kişisel veri aktarımı olarak değerlendirilmiştir³⁹³.

3. Yurt Dışına Aktarım

6698 sayılı Kanunun 9. maddesinde kişisel verilerin yurt dışına aktarılması hususu ayrıca düzenlenmektedir. Maddenin birinci fıkrasında, kişisel verilerin yurt dışına aktarılabilmesi bakımından temel kural olarak ilgili kişinin açık rızasının arandığı görülmektedir. Buna göre, ilgili kişinin açık rızası olmaksızın kişisel veriler yurt dışına aktarılamayacaktır. Maddenin ikinci fıkrasında ise ilgili kişinin açık rızası aranmaksızın kişisel verilerin aktarılabilmesine ilişkin şartlar düzenlenmiştir. Hükme göre ilgili kişinin açık rızası olmaksızın kişisel verilerin yurt dışına aktarılabilmesi için ilk olarak, Kanunun 5. maddesinin ikinci fıkrası ile 6. maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığının bulunması gerekmektedir. Ancak bu şartlardan birinin bulunması, ilgili kişinin açık rızası olmaksızın kişisel verilerin yurt dışına aktarılabilmesi için yeterli değildir. Bunun yanında, ayrıca kişisel verilerin aktarılacağı yabancı ülkede yeterli korumanın bulunması; yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması şartları aranmaktadır (Kanun, m. 9/1,2). Kanunun 9. maddesinin dördüncü fıkrasında, Kurulun yabancı ülkede yeterli koruma bulunup bulunmadığına ilişkin değerlendirmesini yaparken Türkiye'nin taraf olduğu uluslararası sözleşmeleri, kişisel veri talebinde bulunan ülke ile Türkiye arasında veri aktarımı hususundaki karşılıklılık durumunu, her somut kişisel veri aktarımı yönünden kişisel verinin niteliği ile işleme amaç ve süresini, kişisel verilerin aktarılacağı ülkenin konu ile ilgili mevzuat ve uygulamalarını, kişisel verilerin aktarılacağı ülkede bulunan veri sorumlusunun taahhüt ettiği önlemleri göz önünde bulundurarak ve hatta ihtiyaç duyması halinde ilgili kurum ve kuruluşların görüşünü de alarak karar vereceği ifade edilmektedir. Şu anki uygulama bakımından belirtmekte fayda var ki, henüz Kurul tarafından yeterli

³⁹³ İlgili karar özeti için bkz. <https://www.kvkk.gov.tr/Icerik/5262/Kisisel-Verileri-Koruma-Kurumu-Karar-Ozetleri#>, (10.07.2023).

korumanın bulunduğu ülkeler listesi yayımlanmamıştır. Bu sebeple halihazırda yurt dışına veri aktarımında bulunulabilmesi için taraflar arasında yeterli koruma sağlanmasına dair bir taahhütname yapılması ve Kurul'un izninin alınması gerekmektedir³⁹⁴. Kurul, hazırlanan taahhütnameyi inceleyerek yurt dışına veri aktarımına izin verip vermeyeceğine ilişkin bir karara varmaktadır³⁹⁵. Ayrıca kişisel verilerin yurt dışına aktarımına ilişkin olarak veri sorumluları tarafından hazırlanacak taahhütnamede yer alacak asgari unsurlar Kişisel Verileri Koruma Kurumunun internet sitesinde “*veri sorumlusundan veri işleyene aktarım*” ile “*veri sorumlusundan veri sorumlusuna aktarım*” olmak üzere ikili bir ayrıma tabi tutularak taahhütname örnekleri de verilmek suretiyle yayımlanmıştır. Yine Kurumun internet sitesinde “*Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru*” yayımlanmak suretiyle yurt dışına veri aktarımında bulunacak veri sorumlularının hazırlayacağı taahhütnamelerin usulü ve içeriğinin nasıl olması gerektiği detaylı olarak izah edilmiştir³⁹⁶.

Halihazırda hukukumuzda, Türkiye’de bulunan veri sorumlusunca, yeterli veri koruması olmayan ülkelere yerleşik veri sorumlusuna yahut veri işleyene yapılacak veri aktarımlarında Kurulun onayına sunulmak üzere taraflarca taahhütname hazırlanması yöntemi uygulanmaktadır. Ancak bu durum çok uluslu şirket toplulukları arasında yapılacak veri aktarımları bakımından pratik bir uygulama değildir. Bu sebeple Kişisel Verileri Koruma Kurumu tarafından, çok uluslu şirket toplulukları arasında gerçekleştirilecek uluslararası veri aktarımlarında, alternatif bir yöntem olarak “*Bağlayıcı Şirket Kuralları*” yöntemi belirlenmiştir. Söz konusu şirketlerin, Kurumun internet sitesinde yer alan bağlayıcı şirket kuralları formunu doldurmak ve belirtilen talimatları uygulamak suretiyle “*Kişisel Verileri Koruma Kurumuna*

³⁹⁴ Öztürk ve diğerleri, s. 95.

³⁹⁵ Örneğin Kurul, Veri Sorumlusu Turksport Spor Ürünleri San. Tic. Ltd. Şti. (Decathlon Türkiye) tarafından yurt dışına kişisel veri aktarımı yapılması hususunda gerçekleştirilen Taahhütname başvurusunu 6698 sayılı Kişisel Verilerin Korunması Kanununun 9.maddesinin 2.fıkrasının b) bendi kapsamında değerlendirmiş ve veri aktarımına 22.06.2021 tarihinde izin vermiştir. İlgili duyuruya ulaşmak için bkz. <https://www.kvkk.gov.tr/Icerik/6985/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU>, (11.07.2023).

³⁹⁶ İlgili duyuru için bkz. <https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU>, (11.07.2023).

Bağlayıcı Şirket Kuralları” başvurusunda bulunması gerekmektedir³⁹⁷. Kişisel verilerin yurt dışına aktarılmasında kullanılan “*Taahhütnameler ve Bağlayıcı Şirket Kuralları*” yöntemlerinin, büyük ölçüde 95/46/EC sayılı Direktif kapsamında oluşturulan çalışma grubunun yayımlamış olduğu metinlerle benzerlik gösterdiği dikkat çekmektedir. Söz konusu yöntemlerin içeriğinin kurul tarafından yayımlanan çeşitli dokümanlar yerine yasal bir düzenleme kapsamında ele alınması ve kurul tarafından çıkartılacak uygulama rehberleri ile bu düzenlemelerin açığa kavuşturulması daha faydalı olacaktır³⁹⁸.

Kanunun 9. maddesinin beşinci fıkrasında kişisel verilerin, uluslararası sözleşme hükümleri saklı kalmak kaydıyla Türkiye’nin veya ilgili kişinin menfaatinin ciddi bir biçimde zarar göreceği durumlarda ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak kurulun izniyle yurt dışına aktarılabilceği ifade edilmektedir. Söz konusu düzenleme, Türkiye’nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar görebileceği durumların belirlenmesinde objektif bir ölçütün bulunmaması, hangi hallerin ciddi bir zarara sebep olabileceği, bu konuda bir tespit yapılırken hangi kamu kurum veya kuruluşunun görüşünün alınacağını ve yurt dışına her veri aktarımında veri sorumlusunun buna ilişkin bir değerlendirme yapmasının gerekli olup olmaması bakımından herhangi bir belirliliğin bulunmaması yönleriyle sorunlar doğurmaya müsaittir³⁹⁹. Kanunun 9. maddesinin altıncı fıkrasında ise, tıpkı yurt içinde kişisel veri aktarımını düzenleyen 8. maddede olduğu gibi, kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu belirtilmiştir.

Türk hukuku bakımından kişisel verilerin yurt dışına aktarılması birçok yönden soruna yol açmakta olup Kurul tarafından güvenli ülkeler listesinin halen yayımlanmamış olması dahi bu sorunların doğmasına etki eden başlıca etkenler arasında yer almaktadır. Anılan eksikliğin ivedilikle giderilmesi ve Türk hukukunda

³⁹⁷ Konuya ilişkin detaylı açıklama ve dokümanlara ulaşmak için bkz. <https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU>, (11.07.2023).

³⁹⁸ Sevgi Eraslan, “Türk Hukukunda Kişisel Verilerin Yurt Dışına Aktarılması Sorunu: Açık Rıza Kapsamında Bir Değerlendirme”, *Kırıkkale Hukuk Mecmuası*, Cilt:1, Sayı:1, 2021, s. 112.

³⁹⁹ Küzeci, *Kişisel Verilerin Korunması*, s. 413.

yurt dışına veri aktarımının yasal bir zemine oturtulması büyük önem arz etmektedir⁴⁰⁰.

II. İLGİLİ KİŞİNİN HAKLARI VE VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ

A. İlgili Kişinin Hakları

6698 sayılı Kanunun 11. maddesinde ilgili kişinin hakları düzenlenmektedir. İlgili kişiye tanınan haklar, kişisel veri işleme sürecinin meşruiyetini denetleme noktasında veri sahibine önemli bir imkân sunmaktadır. Zira ilgili kişi, kendisine tanınan bu imkân sayesinde, veri sorumlusunun Kanuna uygun hareket edip etmediğini tespit edebilecek, gerekli görmesi halinde kişisel veri işleme faaliyetinin hukuka uygun hale getirilmesini yahut veri sorumlusunun hukuka aykırı eylemi sebebiyle doğan zararın tazminini yine veri sorumlusundan talep edebilecektir⁴⁰¹.

Kanun koyucu ilgili kişinin haklarını düzenlerken “herkes” ifadesini kullanmak suretiyle bu haklardan yararlanacak olanlar bakımından vatandaş olma veya olmama ayırımına gitmemiştir. Ancak ilgili kişinin yalnızca kendisine ilişkin kişisel veriler hakkında başvuru yapabileceğini belirtmek gerekir⁴⁰². Hükmün a) bendinde, ilgili kişiye, kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenme hakkına yer verilmiştir. Burada kişiye üçüncü kişilerin kişisel verilerinin ya da soyut nitelikte kişisel verilerin işlenip işlenmediği hususunda bilgi alma yetkisi tanınmadığını ifade etmek gerekir. Zira hüküm, ilgili kişi hakkında kişisel veri işlenip işlenmediği hususuna ilişkindir⁴⁰³. Hükmün b) bendinde ilgili kişinin, kişisel verilerinin işlenmiş olması halinde buna ilişkin veri sorumlusundan bilgi talep etme; c) bendinde, kişisel verilerinin işleme amacı ile bu verilerin amacına uygun kullanılıp kullanılmadığı hakkında bilgilendirilme; ç) bendinde ise yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme hakkı düzenlenmiştir (Kanun, m.11/a,

⁴⁰⁰ Eraslan, s. 112.

⁴⁰¹ Çekin, s. 88.

⁴⁰² Öztürk ve diğerleri, s. 118.

⁴⁰³ Çekin, s. 89.

b, c, ç). Kişisel veriler her ne kadar üçüncü kişiler nezdinde hukuka uygun olarak tutuluyor ise de veri sahibi bakımından erişilebilir, denetlenebilir ve gerektiğinde müdahale edilebilir olmalıdır⁴⁰⁴. Verilere erişim hakkının, bilgilendirme yükümlülüğü ile de yakından ilişkili olduğunu ifade etmek gerekir. Zira kişisel verileri işleyen veri sorumlusunun, ilgili kişiye bu konuda bilgi vermemesi halinde ilgili kişinin kişisel verilerinin işlendiğinden haberi olmayacaktır. Hal böyle iken ilgili kişinin, kişisel verilerine erişim, bunlar üzerinde düzeltme, silme, yok etme ve üçüncü kişilere aktarılmasını engelleme gibi konularda haklarını kullanması söz konusu olmayacaktır⁴⁰⁵. Özü itibarıyla, etkin bir şekilde kişisel verilerin korunması hakkının korunabilmesi için, veri sorumlusunun yükümlülükleri ile ilgili kişinin haklarını birbirini tamamlayan parçalar olarak nitelendirmek yanlış olamayacaktır. 6698 sayılı Kanunun 11. maddesinin birinci fıkrasının d) bendinde kişisel verilerin eksik veya yanlış işlenmesi halinde bunların düzeltilmesini isteme; e) bendinde 7. maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme hakkı, ilgili kişinin veri sorumlusuna yöneltebileceği hakları arasında sayılmıştır. Kişisel verilerin eksik veya yanlış işlenmiş olduğuna hangi kriterler esas alınarak karar verileceği önem taşımaktadır. Burada işlevsel yoruma göre, verinin işleniş amacına göre kişi hakkında yanlış bir tablo ortaya çıkıyorsa verinin yanlış olduğu sonucuna varmak gerekir. Ayrıca verinin yanlış olmamakla birlikte muğlak, yanıltıcı yahut da yanlış anlaşılmaya elverişli olması durumunda da düzeltme hakkı gündeme gelir⁴⁰⁶. Kanaatimizce de verinin eksik veya yanlış olup olmadığına ilişkin yapılacak yorumlamada en somut ölçüt bu yaklaşımda yer almaktadır. Kişisel verilerin mevcudiyetini etkileyen nitelikteki kişisel verilerin silinmesini isteme hakkı, ise 7. maddede öngörülen şartlar çerçevesinde ilgili kişinin veri sorumlusuna yöneltebileceği bir hak olarak tanınmıştır. Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi konusuna daha önce detaylı bir şekilde değinmiştik. Bu yüzden burada genel bir açıklamada bulunmakla yetineceğiz. Kişisel verilerin silinmesini talep etme hakkı, unutulma hakkı olarak da tanımlanabilir. Bu hakkın içeriği, hukuka aykırı olarak işlenen kişisel verilerin silinmesini gerektirdiği gibi; yasal düzenlemelere uygun olarak işlenen kişisel verilerin de işlenme amacının ortadan kalkması üzerine

⁴⁰⁴ Dülger, Kişisel Veriler Hukuku, s. 156.

⁴⁰⁵ Korkmaz, Kanun Hakkında Değerlendirme, s. 131.

⁴⁰⁶ Çekin, s. 42.

silinmesini gerektirmektedir. Zira işlenme amacı ortadan kalkan kişisel veriler, artık gereksiz veri haline gelmektedir. Günümüz gelişmeleri ışığında, “*belki bir gün lazım olur*” düşüncesiyle çok sayıda kişisel veri işlenebilmektedir. İşlenme amacı ortadan kalksa dahi veri sorumlularınca bu verilerin saklanmaya devam etmesi ise “*veri kirliliğine*” sebebiyet vermektedir. İlgili kişiye tanınan, belli şartlar çerçevesinde kişisel verilerinin silinmesini talep etme hakkının ve veri sorumlusuna bu konuda öngörülen yükümlülüğün amacı, bu kirliliği ortadan kaldırmaktır⁴⁰⁷. İlgili kişilerin haklarına ilişkin Kanundaki düzenlemede yer alan bir diğer hak, 10. maddenin birinci fıkrasının d) ve e) bentleri uyarınca kişisel verilerin aktarıldığı üçüncü kişilere yapılan işlemlerin bildirilmesini isteme hakkıdır (Kanun, m.10/1-f). Bu hak ilgili kişiyi, kişisel verinin aktarıldığı üçüncü kişileri ayrı ayrı tespit etme ve onlara başvurma külfetinden kurtarmaktadır. Hak çerçevesinde ilgili kişinin veri sorumlusuna başvurması üzerine veri sorumlusu, eğer kişisel veriler üçüncü kişilere aktarıldıysa bu kişilere gerekli bildirimleri yapacaktır⁴⁰⁸. Kanunun 11. maddesinin birinci fıkrasının g) bendinde ilgili kişinin “*itiraz hakkı*” düzenlenmektedir. Kanunun gerekçesinde söz konusu hak, münhasıran otomatik sistemler aracılığıyla işlenen verilerin analiz edilerek aleyhe bir sonucun oluşmasına itiraz hakkı olarak ifade edilmiştir. Gerekçede konunun daha iyi anlaşılması açısından bir de örneğe yer verilmektedir. Bu örnekte, bir çalışanın çalışma performansının, yapmış olduğu işlerin, otomatik bir sisteme işlenerek analiz sonucuna göre değerlendirilmesine çalışanın itiraz edebilmesinin bu hak kapsamında değerlendirileceği ifade edilmiştir⁴⁰⁹. İlgili kişinin haklarına yönelik olarak Kanunda düzenlenen hükmün son bendinde, kanuna aykırı şekilde kişisel verilerin işlenmesi sebebiyle ortaya bir zarar çıkması durumunda bu zararın giderilmesini isteme hakkı düzenlenmiştir (Kanun, m.11/1-ğ). Burada dikkat edilmesi gereken husus, 6098 sayılı Türk Borçlar Kanunun genel hükümleri uyarınca haksız fiil koşullarının oluşması gerektiğidir. Başka bir ifadeyle, bu hükme dayanılarak tazminat hakkının kullanılabilmesi için, veri işleme faaliyeti hukuka aykırı olmalı, bu veri işleme faaliyetinden ötürü ilgili kişi zarar görmüş olmalı ve doğan zarar ile veri işleme faaliyeti arasında illiyet bağı bulunmalıdır. Söz konusu koşulların varlığı halinde ilgili

⁴⁰⁷ Dülger, s. 166.

⁴⁰⁸ Öztürk ve diğerleri, s. 118.

⁴⁰⁹ TBMM, “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 12.

kiři, maddi veya manevi tazminat davası açabileceđi gibi açık rıza şartı aranmaksızın özel nitelikli kişisel verilerin işlendiđi hallerde ifa davası açabilecek, cebri icra yollarına başvurabilecek, ihlalin durdurulması, önlenmesi yahut tespit edilmesi taleplerinde bulunabilecektir. Ayrıca Kişisel Verileri Koruma Kurumuna da başvuruda bulunabilecektir⁴¹⁰.

Bu başlık altında son olarak, ilgili kişinin yukarıda değinilen haklarını kullanmak üzere veri sorumlusuna başvuru sürecini ele almanın faydalı olacağını düşünüyoruz. Söz konusu sürecin detayları Kanunun “*Veri sorumlusuna başvuru*” başlıklı 13. maddesinde yer almaktadır. Madde hükmünün ilk fıkrasında, ilgili kişinin veri sorumlusuna, Kanunun uygulanmasına dair taleplerini yazılı olarak yahut kurulun belirleyeceği diğer yöntemlerle ileteceđi belirtilmiştir. İkinci fıkrada ise veri sorumlusunun, kendisine yöneltilen talebi, talebin niteliğine göre, en kısa süre içerisinde ve en geç otuz gün içinde ücretsiz olarak sonuçlandırması gerektiđi, işlemin ayrıca maliyet gerektirmesi durumunda ise kurulca belirlenen tarifiedeki ücretin ilgili kişiden alınabileceđi ifade edilmiştir. Maddenin üçüncü ve son fıkrasında ise veri sorumlusunun talebi kabul edebileceđi gibi gerekçesini açıklayarak reddedebileceđi, cevabını ilgili kişiye yazılı şekilde veya elektronik ortamda bildireceđi düzenlenmiştir. Veri sorumlusuna yapılacak başvurulara ilişkin olarak, Kişisel Verileri Koruma Kurumu tarafından “*Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ*” isimli bir tebliğ de yayımlanmıştır⁴¹¹. Tebliğde veri sahiplerinin veri sorumlusuna yapacağı başvuruların ve veri sorumlularının da bu başvurulara vereceđi cevapların usulü detaylı bir şekilde izah edilmektedir. Özellikle Tebliğ’de yer alan, veri sorumlusunun hukuka ve dürüstlük kuralına uygun şekilde başvuruları cevaplama yükümlülüğü, ilgili kişinin haklarını etkin bir biçimde ve süreç zorlaştırılmadan kullanabilmesi açısından oldukça önemlidir⁴¹².

⁴¹⁰ Dođan, s. 71.

⁴¹¹ 10.03.2018 tarih ve 30356 sayılı Resmî Gazetede yayımlanan Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, <https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm>, (31.07.2023).

⁴¹² Göçmen Uyarer, s. 177.

B. Veri Sorumlusunun Yükümlülükleri

1. Genel Olarak

Demokratik ülkelerde bireylerin temel hak ve özgürlükleri anayasalar tarafından güvence altına alınmıştır. Kişisel verilerin korunması hakkının da temel hak ve özgürlüklerden bir tanesi olması sebebiyle güvence altına alınması, temel hak ve özgürlüklerin korunması açısından büyük önem arz etmektedir⁴¹³. Veri sorumlusunun, kişisel verilerin işleme amaç ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olduğunu⁴¹⁴ daha önce ifade etmiştik. Bu çerçevede temel hak ve özgürlüklerden bir tanesi olan kişisel verilerin korunması hakkının etkin bir biçimde güvence altına alınabilmesi amacıyla mevzuatımızda veri sorumlusuna yönelik çeşitli yükümlülükler öngörülmektedir. 6698 sayılı Kişisel Verilerin Korunması Kanununda, veri sorumlusunun yükümlülüklerinin dağınık bir şekilde düzenlendiği, bununla birlikte söz konusu düzenlemelerin Kurul'un düzenlemeleri ile desteklendiği görülmektedir⁴¹⁵.

Veri sorumlusunun, her ne kadar 6698 sayılı Kanun ve diğer mevzuatta, hemen her alanda yükümlülükleri bulunan ana aktör konumuna sahip olduğu açıkça ortaya konulmuş ise de bir diğer aktör olan veri işleyenin de bazı yükümlülüklerinin bulunduğunu belirtmekte yarar vardır⁴¹⁶. Zira veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak, veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişidir⁴¹⁷. Kanunun veri güvenliğine ilişkin yükümlülükleri içeren 12. maddesinin ikinci fıkrasında, birinci fıkrada belirtilen tedbirlerin alınması hususunda veri işleyen ile veri sorumlusunun müştereken sorumlu olduğu ifade edilmiştir. Veri işleyen, kişisel verilerin hukuka aykırı işlenmesinin engellenmesi bakımından veri sorumlusunun yanında konumlandırılmaktadır. Bununla birlikte ilgili hükümde yer

⁴¹³ Doğan, s. 166.

⁴¹⁴ Kişisel Verilerin Korunması Kanunu, m.3/1-1.

⁴¹⁵ Öztürk ve diğerleri, s. 97.

⁴¹⁶ Elif Küzeci, “Veri Sorumlusunun Yükümlülükleri”, **II. Kişisel Verilerin Korunması Sempozyumu**, İstanbul, 07.02.2019, www.academia.edu, (18.07.2023), (Veri Sorumlusunun Yükümlülükleri), ss.1,2.

⁴¹⁷ Kişisel Verilerin Korunması Kanunu, m.3/1-ğ.

alan “*müştereken sorumludur*” ifadesi ile veri sorumlusu ve veri işleyenin kusurları oranında mı yoksa her birinin bütünüyle sorumlu olmasını mı amaçladığı hususu, ayrıca bir değerlendirmeye tabi tutulmalıdır. İkinci durumun kabulü halinde kanunda “*müteselsilen*” ifadesinin kullanılması daha doğru olacaktır⁴¹⁸.

Veri sorumlusunun mevzuat tarafından öngörülen yükümlülüklerine aykırı davranması halinde maruz kalacağı yaptırımların neler olduğunu ise yükümlülüğün türüne göre üç kategori altında değerlendirmek mümkündür. Bunlar, 6698 sayılı Kanunun 18. maddesi bakımından idari yaptırım, Türk Ceza Kanunun 135. ve devamı maddelerindeki suçlar bakımından cezai yaptırım ve son olarak ilgili kişinin zararının doğmuş olması halinde doğan zarar bakımından tazmin borcu şeklinde ifade edilebilir⁴¹⁹.

2. Veri Sorumlusunun Aydınlatma Yükümlülüğü

6698 sayılı Kanun uyarınca veri sorumlusuna yüklenen yükümlülüklerin en başında ilgili kişiyi aydınlatma yükümlülüğü gelmektedir. Bu yükümlülük genel olarak kişisel verileri işlenen ilgili kişinin, hangi verilerinin, ne amaçla, nasıl bir yöntemle işleneceği ve kişisel verilerinin işlenmesi sürecinde veri sorumlusuna yönelik haklarının neler olduğu gibi hususlarda bilgilendirilmesi esasına dayanmaktadır. Söz konusu yükümlülüğün Anayasamız tarafından da güvence altına alındığını belirtmek gerekir⁴²⁰. Zira Anayasamızın 20. maddesinin üçüncü fıkrasında, kişisel verilerin korunmasını isteme hakkının kişinin kendisiyle ilgili kişisel verilere erişme, bu veriler hakkında bilgilendirilme, bu verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme ile bunların silinmesini veya düzeltilmesini talep etmeyi de kapsadığı belirtilmektedir⁴²¹. 6698 sayılı Kanunun veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10. maddesinde “*Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerinin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçlarla aktarılabileceği, ç)*

⁴¹⁸ Küzeci, (Veri Sorumlusunun Yükümlülükleri), s. 2.

⁴¹⁹ Öztürk ve diğerleri, s. 98.

⁴²⁰ Şehriban İpek Aşıkoğlu, “Veri Sorumlularının Aydınlatma Yükümlülüğü-Avrupa Birliği ve Türk Hukukunda”, **Kişisel Verileri Koruma Dergisi**, Cilt: 1, Sayı:2, 2019, s. 43.

⁴²¹ Türkiye Cumhuriyeti Anayasası, m.20/3.

Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11'inci maddede sayılan diğer hakları konusunda bilgi vermekle yükümlüdür” düzenlemesine yer verilmiştir. Kanunun veri sorumlusunun aydınlatma yükümlülüğünü genel hatlarıyla ifade etmiş olması birçok açıdan belirsizliğe sebebiyet vermektedir. Bu belirsizliklerin giderilmesi ve aydınlatma yükümlülüğü yerine getirilirken veri sorumlusu tarafından uyulması gereken usul ve esasların belirlenmesi amacıyla Kişisel Verileri Koruma Kurumu tarafından “*Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ*” (“*Aydınlatma Yükümlülüğü Tebliği*”) 10.03.2018 tarih ve 30356 sayılı Resmî Gazetede yayımlanmıştır⁴²². Ayrıca Kurul tarafından, bu yükümlülüğün veri sorumluları tarafından uygulamada doğru bir şekilde yerine getirilebilmesi amacıyla “*Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi*” yayımlanmıştır.

Aydınlatma yükümlülüğünün hukuka uygun bir şekilde gerçekleştirilebilmesi için en başta, 6698 sayılı Kanunun 4. maddesinde belirtilen genel ilkelere uygun hareket edilmesinin bir zaruret teşkil ettiğini belirtmekte yarar görüyoruz⁴²³. Zira örneğin, aydınlatma yükümlülüğü yerine getirilirken ilgili kişilere eksik veya yanıltıcı bilgiler verilmesi, hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırıdır. Söz konusu durum, diğer bir taraftan Aydınlatma Yükümlülüğü Tebliğinin 5. maddesinin birinci fıkrasının j bendine de aykırılık teşkil etmektedir⁴²⁴. Yine örneğin, ilgili kişiye bildirilen veri işleme amacı belirli, açık ve meşru değil ise bu durum da yine belirli, açık ve meşru amaçlar için işleme ilkesine aykırılık teşkil etmektedir. Dolayısıyla ilgili kişiye yönelik olarak bu örneklerdeki gibi bir bilgilendirme gerçekleştirilmesi halinde aydınlatma yükümlülüğünün hukuka uygun olarak yerine getirildiğinden bahsedilemeyecektir⁴²⁵.

Aydınlatma Yükümlülüğü Tebliğinin, aydınlatma yükümlülüğünün kapsamını düzenleyen 4. maddesinde, Kanun 10. maddesine atıf yapılmakla birlikte kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişilerce, ilgili

⁴²² Dülger, Kişisel Veriler Hukuku, s. 297.

⁴²³ Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Ankara, 2019, s. 9.

⁴²⁴ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin 5.maddesinin birinci fıkrasının j bendi uyarınca “Aydınlatma Yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir.”

⁴²⁵ Serdar Çelikel, **Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri**, Seçkin Yayıncılık, Ankara, 2022, s. 94.

kişilerin bilgilendirilmesi gerektiği ve bu bilgilendirme sırasında asgari olarak: veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, kişisel veri toplamanın yöntemi ve hukuki sebebi, kişisel verilerin kimlere ve hangi amaçla aktarılabilceği ve ilgili kişinin Kanunun 11'inci maddesinde sayılmış olan diğer hakları konularında bu kişilere bilgilendirilme yapılması gerektiği ifade edilmektedir⁴²⁶. Veri sorumlusunun, veri işleme faaliyetinin gerçekleştirildiği her durumda ilgili kişiyi aydınlatma yükümlülüğü bulunmaktadır⁴²⁷. Nitekim Aydınlatma Yükümlülüğü Tebliğinin 5. maddesinde bu hususa ilişkin olarak, ilgili kişinin açık rızasına veya Kanundaki diğer veri işleme şartlarına dayanılarak yapılan her kişisel veri işleme faaliyetinde, aydınlatma yükümlülüğünün yerine getirilmesi gerektiği ifade edilmektedir. Yine kişisel veri işleme amacının değiştiği durumda ilgili kişiye, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü yerine getirilmelidir. Ayrıca sicile kayıt yükümlülüğü bulunması halinde, aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilen bilgiler ile sicile açıklanan bilgilerin uyumlu olması da gerekmektedir. Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı kılınmış olmayıp aydınlatma yükümlülüğünün yerine getirilmiş olduğunun ispatı da veri sorumlusuna yüklenmiştir⁴²⁸. Veri sorumlusunun aydınlatma yükümlülüğünü yerine getirmiş olduğuna dair ispat külfeti, kötü niyetli ilgili kişiler karşısında veri sorumlusunu tedbir almaya sevk edebilecek türden bir külfettir. Zira eğer aydınlatma yükümlülüğü veri sorumlusu tarafından sözlü olarak yerine getirildiyse, bunun daha sonra ilgili kişi tarafından inkâr edilmesi, veri sorumlusunu ispat bakımından zor bir duruma sokabilecektir. Buna karşın yazılı veya elektronik ortamda ilgili kişiden alınan aydınlatma yükümlülüğünün yerine getirildiğine dair beyan veri sorumlusuna ispat kolaylığı sağlayabilecektir⁴²⁹. Kişisel verilerin ilgili kişinin açık rızasına dayanılarak işlendiği hallerde, aydınlatma yükümlülüğü ile açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir⁴³⁰. Kurul konuya ilişkin olarak vermiş olduğu bir kararında, online platform üzerinden iş

⁴²⁶ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, m.4/1.

⁴²⁷ Öztürk ve diğerleri, s. 99.

⁴²⁸ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, m.5/1-a,b,ç,d,e.

⁴²⁹ Dülger, Kişisel Veriler Hukuku, ss. 301.

⁴³⁰ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, m.5/1-f

başvurusu alan şirketler topluluğu şeklindeki veri sorumlusunun, iş başvurularının yapılabilmesi için üyelik kaydını zorunlu tuttuğunu ve üyelik kaydı işleminin gerçekleştirildiği sırada aynı kutucuğun işaretlenmesi suretiyle hem aydınlatma metninin okunduğu hem de kişisel verilerin işlenmesine açık rıza verildiğine ilişkin onay alınması yoluna başvurulduğunu tespit etmiş ve bu durumu 6698 sayılı Kanunun amacına ve tebliğ'in 5.maddesinin birinci fıkrasının f bendinde yer verilen hükme açıkça aykırı olarak değerlendirmiştir. Nitekim ilgili kararda Kurul, aydınlatma yükümlülüğünün yerine getirilmesinin herhangi bir onaya bağlı olmadığını, aydınlatma yükümlülüğünün yerine getirilmesindeki amacın ilgili kişinin kişisel verilerin işlenmesi hususunda bilgilendirilmesi olduğunu, açık rıza alınmasındaki amacın ise veri sorumlusu tarafından kişisel verilerin işlenmesinin hukuki bir gerekçeye dayandırılması olduğunu, aydınlatma metni sayesinde ilgili kişinin kişisel verilerinin işlenmesi hususunda bilgi edindiğini ancak söz konusu metinde yazılanlara açık rıza vermek zorunda olmadığını ifade etmiştir⁴³¹. Kurul yine konuyla ilgili vermiş olduğu bir başka kararda ise açık rıza şartına dayalı olarak gerçekleştirilen veri işleme süreçleri bakımından aydınlatmanın yapılması ile açık rızanın alınması işlemlerinin birlikte gerçekleştirilmesinin yürürlükteki mevzuata aykırılık teşkil ettiği, karara konu olayda web sitesinde veri sorumlusunca yayımlanan “*Gizlilik Bildirimi*” metninin birçok bilgi içermesiyle birlikte veri işlemeye ilişkin olarak genel bir bilgilendirme niteliğinde olması nedeniyle ilgili kişilere, kişisel verilerin işlenmesine ilişkin olarak aydınlatma yapıldığı ve açık rıza alındığı anlamına gelmediği değerlendirmesinde bulunmuştur⁴³². Gerçekten de açık rıza metni, ilgili kişiye kişisel verilerinin işlenmesine ya da bunun tam tersine karar verme olanağı sunmakta iken, aydınlatma metni hangi veri işleme sebebine dayanılarak olursa olsun ilgili kişinin bilgi sahibi kılınmasına yönelik veri sorumlusu yükümlülüğüdür⁴³³.

Aydınlatma Yükümlülüğü Tebliğinin 5. maddesinin birinci fıkrasının g bendinde, aydınlatma yükümlülüğü çerçevesinde ilgili kişiye açıklanacak veri işleme amacının belirli, açık ve meşru olmasının arandığı, aydınlatma yükümlülüğünün

⁴³¹ Kişisel Verileri Koruma Kurulunun 26.07.2018 tarihli ve 2018/90 sayılı karar özeti, <https://www.kvkk.gov.tr/>, (24.07.2023).

⁴³² Kişisel Verileri Koruma Kurulunun 27.02.2020 tarihli ve 2020/173 sayılı karar özeti, <https://www.kvkk.gov.tr/>, (24.07.2023).

⁴³³ Küzeci, Kişisel Verilerin Korunması, s. 421.

yerine getirilmesi sırasında genel nitelikte ve muğlak ifadelerle yer verilmemesi gerektiği belirtilmiştir. Bununla birlikte aynı bentte, gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaati uyandıran ifadelerin de kullanılamayacağı ifade edilmektedir⁴³⁴. Örneğin, bir şirket çalışanına ait kişisel verilerin o şirketin insan kaynakları sürecinin planlanması için işleneceğinin açıkça belirtilmesi bu anlamda usule uygun bir aydınlatma olarak değerlendirilebilir. Ancak “*kişisel verilerinizi araştırma amaçlı kullanabiliriz*” yahut da “*kişisel verilerinizi yeni hizmetler geliştirmek amacıyla kullanabiliriz*” şeklindeki muğlak ifadelerin bulunduğu bir aydınlatma metni hukuka uygun kabul edilemeyecektir⁴³⁵. Aydınlatma Yükümlülüğü Tebliğinin 5. maddesinin birinci fıkrasının g bendi hükmü uyarınca, aydınlatma yükümlülüğünün ilgili kişiye yönelik olarak açık, anlaşılır ve sade bir dille yerine getirilmesi gerekmektedir⁴³⁶. Aydınlatma metninin öz, şeffaf ve anlaşılır olması gerekliliği şeklinde de ifade edilebilecek olan bu hüküm, aydınlatma metninde ağırlıklı bir dilin kullanılmaması, kişisel verilerin işlenmesi ve korunması süreci ile herhangi bir ilgisi bulunmayan, gereksiz ifadelerden kaçınılması anlamına gelmektedir⁴³⁷. Aydınlatma Yükümlülüğü Tebliğinin 5. maddesinin birinci fıkrasının h bendinde ise 6698 sayılı Kanunun 10. maddesinin birinci fıkrasının ç bendinde yer alan ve aydınlatma yükümlülüğü kapsamında ilgili kişilere bilgi verilmesi gereken hususlar arasında sayılan, kişisel verileri toplamanın “*hukuki sebebi*” hakkında açıklamalar getirilmektedir. Aydınlatma Yükümlülüğü Tebliğinin ilgili hükmüne göre “*hukuki sebep*” ifadesinden, kişisel verilerin Kanunun 5. veya 6. maddesinde sayılan hukuka uygunluk sebeplerinden hangisine dayanılarak işlendiği anlaşılmalıdır. Hukuki sebebin aydınlatma yükümlülüğü yerine getirilirken açıkça belirtilmesi gerektiğine de Aydınlatma Yükümlülüğü Tebliğinin ilgili hükmünde özel olarak yer verilmiştir⁴³⁸. Bu noktada akıllara, Kanunun 5. maddesinin 2. fıkrasının a bendinde yer alan ve açık rıza şartı aranmaksızın, kişisel verilerin kanunlarda açıkça öngörülmesi halinde

⁴³⁴ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, m.5/1-g.

⁴³⁵ Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Ankara, 2019, s. 10.

⁴³⁶ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, m.5/1-ğ.

⁴³⁷ Aşıkoglu, s. 45.

⁴³⁸ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, m.5/1-h.

işlenebileceğini öngören hukuka uygunluk sebebi gelmektedir. Zira aydınlatma yükümlülüğü kapsamında veri sorumlusu tarafından ilgili kişiye yapılacak bilgilendirmede, sadece “*kanunlarda açıkça öngörülme*” hukuki sebebine dayanıldığı bilgisine yer verilmesinin yeterli olup olmayacağı konusunda bir tereddüt doğması mümkündür. Ancak salt bu ifadenin kullanılması bir hukuki sebep olarak değil, o hukuki sebebin dayanağı olarak değerlendirilmelidir. Dolayısıyla aydınlatma yükümlülüğü yerine getirilirken, veri işlemeyi hukuka uygun kılan kanun hükmü hangisiyse o hükmün bilgisi ilgili kişiye verilerek bu yükümlülüğün yerine getirilmesi gerekir⁴³⁹. Aydınlatma Yükümlülüğü Tebliğinin 5. maddesinin birinci fıkrasının 1 bendinde, kişisel verilerin aktarılma amacı ve aktarılacağı alıcı gruplarının da aydınlatma yükümlülüğü kapsamında ilgili kişiye belirtilmesi gerektiği ifade edilmiş, i bendinde ise kişisel verilerin tamamen veya kısmen otomatik olan yahut veri kayıt sisteminin parçası olmak suretiyle otomatik olmayan yöntemlerden hangisiyle elde edildiğinin de aydınlatma yükümlülüğü kapsamında ilgili kişinin bilgisine açık şekilde sunulması gerektiği belirtilmiştir. Aydınlatma Yükümlülüğü Tebliğinin 5. maddesinin birinci fıkrasının son bendi olan j bendinde ise aydınlatma yükümlülüğünün yerine getirildiği sırada eksik, yanlış ve kişileri yanıltabilecek nitelikteki bilgilere yer verilmemesi gerektiği açıkça düzenlenmiştir⁴⁴⁰.

Aydınlatma yükümlülüğü, 6698 sayılı Kanunun 10. maddesi uyarınca kişisel verilerin elde edilmesi sırasında gerçekleştirilmesi gereken bir yükümlülüktür. Ancak her zaman, kişisel verilerin elde edilmesi anında aydınlatma yükümlülüğünün bir bütün halinde yerine getirilmesi mümkün olmamaktadır. Böyle durumlarda katmanlı aydınlatma yöntemi kullanılabilecektir. Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi’nde katmanlı aydınlatma, kişisel verilerin elde edildiği sırada ilgili kişiye, kişisel verilerin elde edildiği hususunda ön bilgilendirme yapılarak, ilgili kişinin Kanunun 10. maddesine uygun aydınlatmaya yönlendirilmesi olarak tanımlanmıştır⁴⁴¹. Örneğin, bir şirket binasına, binanın iç ve dış güvenliğinin sağlanması amacıyla, görüntü kaydı alacak güvenlik kameraları yerleştirilebilir. Böyle bir durumda güvenlik kameralarının taktırılmasında şirketin meşru menfaati olduğu

⁴³⁹ Dülger, Kişisel Veriler Hukuku, s. 302.

⁴⁴⁰ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, m.5/1-1,i,j.

⁴⁴¹ Kişisel Verileri Koruma Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Ankara, 2019, s. 8.

söylenbilir. Ancak yalnızca bu unsur, işlenen verilerin hukuka uygun olarak işlendiği anlamını taşımamaktadır. Firmanın ayrıca, ilgili kişilere görüntü kaydı alınacağına dair aydınlatma yükümlülüğünü de yerine getirmesi gerekir. Ancak görüntü kaydı alınan her bir kişiye, ayrıntılı bir şekilde aydınlatma yükümlülüğünün yerine getirilmesi mümkün olmayacağından, katmanlı aydınlatma yöntemi uygulanması daha makul olabilir. Buna yöneme göre, herkes tarafından görülebilecek bir yere bir kamera ikonu eklenerek güvenlik kamerası kaydı alındığı hakkında ilgili kişilere bir ön bilgilendirme yapılabilir. İşlenen kişisel verilerin hangi amaç, hukuki sebep ve yöntemle işlendiği, ilgili kişilerin haklarının neler olduğu gibi hususlara ise ilgili kişilerin yönlendirilecekleri çevrimiçi bir dokümanda yer verilebilir⁴⁴².

Aydınlatma Yükümlülüğü Tebliğinin 6. maddesinde, kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüğünün ne zaman yerine getirilmesi gerektiği düzenlenmiştir. Buna göre, kişisel verilerin ilgili kişiden elde edilmemesi halinde, kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde; kişisel verilerin ilgili kişi ile iletişim kurulması amacıyla kullanılacak olması durumunda ilk iletişimin kurulacağı esnada; kişisel verilerin aktarılması söz konusu ise en geç kişisel verilerin ilk defa aktarımı yapılacağı sırada ilgili kişiyi aydınlatma yükümlülüğünün yerine getirilmesi gerektiği belirtilmektedir⁴⁴³.

Bu başlık altında son olarak, değinmekte fayda var ki, Kanunda aydınlatma yükümlülüğünün ne şekilde yerine getirileceği konusuna ilişkin olarak sınırlayıcı bir yöntem veya şekil şartı öngörülmemiştir⁴⁴⁴. Nitekim Aydınlatma Yükümlülüğü Tebliğinin 5. maddesinin birinci fıkrasında, kullanılacak yöntemlerin bazılarına ilişkin örnekler verilmiştir. Hükme göre, veri sorumlusu veya yetkilendirdiği kişi tarafından sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle aydınlatma yükümlülüğü yerine getirilebilir⁴⁴⁵.

⁴⁴² Öztürk ve diğerleri, ss. 101,102.

⁴⁴³ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, m.6.

⁴⁴⁴ Çelikel, s. 95.

⁴⁴⁵ Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, m.5/1.

3. Veri Güvenliğine İlişkin Yükümlülükler

Kişisel verilerin korunması ile temel olarak kişisel verileri işlenen bireylerin temel hak ve özgürlüklerinin korunması ve veri işleme faaliyetlerine ilişkin hukuki sınırlar ifade edilmekte iken; veri güvenliği ile verilerin bizzat kendisinin korunmasına yönelik alınması gerekli olan teknik ve idari tedbirlerin anlaşılması gerekmektedir⁴⁴⁶. Ancak söz konusu veriler, gerçek kişiye ilişkin ise veri güvenliğinin sağlanması, kişisel verilerin korunması açısından bir hayli önem arz eder hale gelmektedir⁴⁴⁷. 6698 sayılı Kanunun 12. maddesinde veri güvenliğine ilişkin yükümlülükler düzenlenmiştir. Maddenin birinci fıkrasında, veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu ifade edilmektedir. Görüldüğü üzere kanun koyucu, kişisel verilerin güvenliğini sağlamakla yükümlü tuttuğu veri sorumlusunun gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğunu genel ifadelerle düzenlemiştir. Teknik ve idari tedbirlerin detaylarına ise ilgili hükümde değinilmemiştir. Kanun koyucunun bu yaklaşımı bir eksiklik değil, 6698 sayılı Kanunun genel kanun olma niteliğinin bir görünümüdür⁴⁴⁸. Kaldı ki tedbirlerin detaylarına Kişisel Verileri Koruma Kurumu tarafından yayımlanan Kişisel Veri Güvenliği Rehberi'nde yer verilmektedir⁴⁴⁹.

Kişisel verilerin güvenliğini sağlanması noktasında Kanunun 12. maddesinin ikinci fıkrasında, birinci fıkradaki tedbirlerin alınması bakımından veri sorumlusu, onun adına verileri işleyen ile birlikte müştereken sorumlu tutulmuştur. Müştereken sorumluluk, kusurlar oranında sorumluluğu ifade eden bir kavramdır. 6698 sayılı Kanun kapsamında veri ihlali sebebiyle zarara uğrayan gerçek kişinin, zararının tazmini amacıyla kusurları oranında veri sorumlusu ve veri işleyene ayrı ayrı başvurusu gerekecektir⁴⁵⁰. Veri işleyenlerin de veri işlemeden kaynaklı riskleri, işlenen verilerin niteliğini ve teknolojik gelişmeleri dikkate almak suretiyle yeterli

⁴⁴⁶ Şimşek, s. 95.

⁴⁴⁷ Küzeci, Kişisel Verilerin Korunması, s. 414.

⁴⁴⁸ Çelikel, s. 110.

⁴⁴⁹ Kişisel Verileri Koruma Kurumu, **Kişisel Veri Güvenliği Rehberi**, Ankara, 2018.

⁴⁵⁰ Öztürk ve diğerleri, s. 107.

teknik ve idari tedbirleri almaları gerekmektedir⁴⁵¹. Ayrıca belirtmekte fayda var ki, veri sorumluları ve veri işleyenler, işlemiş oldukları kişisel verilerin güvenliğini, bu verileri elde ettikleri ilk andan itibaren, her aşamada, yeterli düzeyde sağlamalı ve gerekli önlemleri almalıdır. Bu çerçevede veri güvenliğinin sağlanmasının tek seferlik değil sürekli bir sorumluluk olduğu ve değişen-gelişen teknolojik gelişmeler doğrultusunda alınan tedbirlerin yenilenmesi gerektiği belirtilebilir⁴⁵².

Veri güvenliği, yalnızca doğru yazılım ve donanım gibi teknik hususlarla sağlanamaz. Aynı zamanda iç organizasyon kurallarının uygulamaya konulması da gerekmektedir. Özellikle veri gizliliğinin korunması amacıyla çalışanlara veri koruma hukuku kapsamındaki yükümlülüklerle ilişkin olarak düzenli eğitimler verilmesi bu kapsamda değerlendirilebilecektir⁴⁵³.

Kanunun 12. maddesinin üçüncü fıkrasında veri sorumlusunun, kendi kurum veya kuruluşunda, 6698 sayılı Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorunda olduğu belirtilmiştir. Görüldüğü üzere hükümden, veri sorumlusunun, söz konusu denetimi bizzat yapmak zorunda olmadığı, dışarıdan hizmet alma yoluyla da bu denetimi sağlayabileceği açıkça anlaşılmaktadır⁴⁵⁴. Ayrıca her ne kadar hükümdeki ifadeden, veri sorumlusuna kendi kurum ve kuruluşlarıyla sınırlı olarak bu denetim yükümlülüğünün getirildiği anlamı çıkarılsa da veri sorumlusunun, müşterek sorumluluğun bir gereği olarak aynı şekilde veri işleyen üzerinde de denetim yapma yükümlülüğü bulunmaktadır⁴⁵⁵.

Kanunun 12. maddesinin dördüncü fıkrasında, hükmün gerekçesinde de ifade edilmiş olduğu üzere veri sorumluları ve veri işleyenlerin sır saklama yükümlülüğü düzenlenmektedir⁴⁵⁶. Kişisel verilerin korunması hukukunda sır saklama yükümlülüğü öğrenilen kişisel verilerin bir başkasına açıklanmaması anlamına gelmektedir⁴⁵⁷. Nitekim ilgili hükümde, veri sorumlusu ve veri işleyen kişilerin, öğrenmiş oldukları

⁴⁵¹ Küzeci, Kişisel Verilerin Korunması, s. 415.

⁴⁵² Dülger, Kişisel Veriler Hukuku, s. 176.

⁴⁵³ Çelikel, ss. 110,111.

⁴⁵⁴ Tuba Kendir Tunalı, “Veri Sorumlularının Yükümlülükleri”, **Kişisel Verilerin Korunması Alanında Yeni Gelişmeler Sempozyumu**, Anadolu Üniversitesi Hukuk Fakültesi-İktisadi ve İdari Bilimler Fakültesi-Kişisel Verileri Koruma Kurumu-Eskişehir Sanayi Odası, 05.12.2019, Adalet Yayınevi, Ankara, 2019, ss. 37,38.

⁴⁵⁵ Çelikel, s. 112.

⁴⁵⁶ TBMM, “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 12.

⁴⁵⁷ Kendir Tunalı, s. 38.

kişisel verileri, 6698 sayılı Kanun hükümlerine aykırı olarak başkasına açıklayamayacakları ve işleme amacı dışında kullanamayacakları belirtilmiştir. Ayrıca hükmün devamında, bu yükümlülüğün görevden ayrılımları sonrasında da devam edeceği ifade edilmiştir (Kanun, m.12/4). Bu düzenleme ile yalnızca veri sorumlusuna değil veri sorumlusunun bünyesinde çalışan kişilere de sır saklama yükümlülüğü getirilmektedir. Ayrıca yine bu yükümlülük, yalnızca çalışılan süre boyunca değil, kişisel verilerin öğrenildiği çalışma ortamından ayrılınca dahi hayat boyu devam eden bir yükümlülüktür⁴⁵⁸.

Kanunun 12. maddesinin beşinci fıkrasında Kurula bildirim yükümlülüğü düzenlenmektedir. Hükme göre, işlenmiş kişisel verilerin, kanuni olmayan yollarla başkaları tarafından ele geçirilmesi halinde, ilgili kişilere ve Kurula veri sorumlusu tarafından en kısa sürede bildirimde bulunulması zorunluluktur. Kurul, gerekmesi halinde durumu, kendi internet sitesi üzerinden ya da uygun göreceği başka bir yöntem ile ilan edebilecektir. Veri ihlaline ilişkin bildirimin veri işleyen tarafından değil her durumda veri sorumlusu tarafından yapılacağını belirtmek gerekir⁴⁵⁹. Veri işleyen nezdinde veri ihlali gündeme gelmesi ve veri işleyenin bunu veri sorumlusuna geç bildirmesi halinde sorumluluk yine veri sorumlusu üzerinde doğacak ancak iç ilişkide veri sorumlusu, veri işleyene rücu edebilecektir⁴⁶⁰. Söz konusu hüküm, günümüzde sıklıkla yaşanan “veri sızıntıları” karşısında büyük önem arz etmektedir. Zira veri sızıntısının yaşanmasını takiben, 12. maddenin beşinci fıkrası uyarınca, ilgili kişilerin ve yetkili kurumların bilgilendirilmesi, bir taraftan soruna ilişkin olarak kendilerini koruyacak tedbirler almalarını ve zararın asgari düzeyde tutulmasını sağlar. Diğer taraftan ise ilerleyen zamanda yeni veri sızıntılarının önüne geçilmesine yardımcı olur⁴⁶¹. Kurulun veri ihlaline ilişkin durumu kendi internet sitesinde ilan etmesi, veri sorumlularınca ilgili kişilere ulaşılamayan ve yaşanan veri ihlali hakkında bilgilendirilmeleri mümkün olmayan durumlarda ilgili kişileri bilgilendirme işlevi görmektedir. Böylelikle ilgili kişiler, yaşanan veri ihlalinden asgari düzeyde

⁴⁵⁸ Kendir Tunalı, s. 38.

⁴⁵⁹ Öztürk ve diğerleri, s. 108.

⁴⁶⁰ Çekin, s. 112; Çekin’e göre “Veri sorumlusu ile veri işleyen arasında yapılacak sözleşmeye, “data breach” halinde veri sorumlusuna derhal bildirimde bulunulacağına, aksi takdirde belirli bir miktar ceza ödeneceğine dair hüküm konulması faydalı olacaktır. İlgili açıklama için bkz. Çekin, s. 112.

⁴⁶¹ Küzeci, Kişisel Verilerin Korunması, s. 416.

etkilenmek adına şahsi olarak alabilecekleri gerekli tedbirleri bizzat alabileceklerdir⁴⁶². Hükümde yer alan “*en kısa sürede*” ifadesinden ne kadarlık bir sürenin anlaşılması gerektiği hususunda Kurulun vermiş olduğu karar, konuya netlik kazandırmaktadır. Kararda, “*en kısa sürede*” ifadesinin 72 saat olarak yorumlanmasına ve veri sorumlusunun durumu öğrendiği andan itibaren gecikme olmaksızın ve en geç 72 saat içerisinde Kurula bildirimde bulunmasına karar verildiği ifade edilmektedir. Veri ihlali yaşanan durumlarda uygulamada standartlaşmayı sağlamak amacıyla verilmiş bulunan bu kararda ayrıca, veri sorumlusunca veri ihlalinin etkilenen kişilerin belirlenmesini müteakip ilgili kişilere makul olan en kısa süre içerisinde bildirim yapılması, veri sorumlusunca haklı bir gerekçe ile 72 saat içerisinde bildirim yapılamaması halinde yapılacak bildirimde bu gecikme nedenlerinin de Kurula izah edilmesi, Kurula yapılacak bildirimde Kurul’un internet sitesinde bulunan “*Kişisel Veri İhlal Bildirim Formu*”nun kullanılması, formda yer verilecek bilgilerin tamamının aynı anda sağlanması mümkün değilse söz konusu bilgilerin aşamalı olarak sağlanması, veri sorumlusunca veri ihlallerine ilişkin bilgilerin, alınan önlemlerin ve ihlalin etkilerinin kayıt altında tutularak Kurulun incelemesine hazır halde bulundurulması, veri işleyen nezdinde bulunan kişisel verilerin veri ihlaline maruz kalması halinde, veri işleyenin gecikmeksizin veri sorumlusuna bildirimde bulunması, veri ihlalinin yurt dışında yerleşik veri sorumlusu nezdinde yaşanması halinde bu ihlalin Türkiye’de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan hizmet ve ürünlerden Türkiye’de faydalıyor olmaları durumunda bu veri sorumlusunun da Kurula bildirimde bulunması, veri ihlali gerçekleşmesi halinde veri sorumlusu bünyesinde kimlere raporlama yapılacağı, kanun kapsamında gerçekleştirilecek bildirimler ve veri ihlalinin olası neticelerinin değerlendirilmesi hususunda, kendi bünyesindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları ihtiva eden bir veri ihlali müdahale planı hazırlanması ve bu planın aralıklarla gözden geçirilmesi gerektiği belirtilmektedir⁴⁶³.

Kişisel verilerin güvenliğinin sağlanmasına ilişkin olarak alınacak tedbirler bakımından önemli bir konu da veri minimizasyonudur. Veri sorumlusu, kişisel verilerin işleme amacının gerçekleşmesine yetecek düzeyde, en az miktarda veriyi

⁴⁶² Çelikel, s. 104.

⁴⁶³ Kişisel Veri İhlali Bildirim Usul ve Esaslarına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararına İlişkin Duyuru, www.kvkk.gov.tr, (25.07.2023).

işleme yolunu tercih etmelidir. Zira işlenen veri sayısı arttıkça ve çeşitlendikçe veri güvenliği ile ilgili riskler ve doğması muhtemel zararlar da artmaktadır. Yine işlenmiş bulunan kişisel verilerin, artık işlenme amacı bakımından muhafazasının zorunluluk teşkil etmediği durumlarda derhal silinmesi yahut anonimleştirilmesi gerekir⁴⁶⁴. Nitekim Kurumun yayımlamış olduğu Kişisel Veri Güvenliği Rehberinde, özellikle uzun bir süredir faaliyet gösteren veri sorumlularının bu süre zarfında çok fazla kişisel veri toplamasından ötürü bu verilerden bazılarının güncelliğini yitirmiş, işlenme amacı ortadan kalkmış ve artık doğru olmayan veriler haline dönüşebileceği, veri sorumluları tarafından işlenme amaçları bakımından anılan verilere ihtiyaç duyulup duyulmadığı konusunda bir değerlendirmede bulunulması ve verilerin doğru bir yerde muhafaza edildiğinden emin olunması gerektiği ifade edilmiştir⁴⁶⁵.

4. Veri Sorumluları Sicili'ne (VERBİS'e) Kayıt Yükümlülüğü

6698 sayılı Kanunun 16. maddesinin birinci fıkrası uyarınca “*Kurulun gözetiminde, Başkanlık tarafından kamuya açık olarak Veri Sorumluları Sicili tutulur*”. Veri sorumluları sicili, kişisel verilerin korunması sürecini şeffaf ve hesap verilebilir hale getirmeyi amaçlayan, veri sahiplerinin haklarının korunmasına yardımcı olan kişisel veri koruma yöntemlerinden bir tanesidir⁴⁶⁶. Kanunun 16. maddesinin ikinci fıkrasında kişisel verileri işleyen gerçek ve tüzel kişilerin, kişisel veri işleme faaliyetine başlamadan önce veri sorumluları siciline kaydolmak zorunda oldukları ifade edilmiştir. Hükmün devamında, işlenen kişisel verilerin niteliği, sayısı, veri işlemenin kanundan kaynaklı gerçekleştiriliyor olması yahut üçüncü kişilere aktarılması durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından veri sorumluları siciline kayıt zorunluluğu konusunda istisna getirilebileceği ayrıca belirtilmiştir (Kanun, m.16/2).

En başta belirtilmelidir ki, veri sorumluları siciline kaydolma zorunluluğu bulunan tüzel kişiler bakımından kanun herhangi bir ayırım yapmamıştır. Bu bağlamda hem özel hem de kamu tüzel kişileri için hüküm geçerlidir⁴⁶⁷. Kurul, yukarıda ifade

⁴⁶⁴ Çelikel, s. 111.

⁴⁶⁵ Kişisel Verileri Koruma Kurumu, Kişisel Veri Güvenliği Rehberi, s. 12.

⁴⁶⁶ Dilşat Yılmaz, “Yeni Bir İdari Faaliyet Alanı: “VERBİS””, **Yıldırım Beyazıt Hukuk Dergisi**, Sayı: 2, 2020, s. 83.

⁴⁶⁷ Küzeci, Kişisel Verilerin Korunması, s. 428.

edilen hüküm çerçevesinde veri sorumluları siciline kayıt zorunluluğundan istisna tuttuğu veri sorumlularına ilişkin bir dizi karar yayımlamıştır. Kurulun 02.04.2018 tarih ve 2018/32 sayılı kararında, herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler, noterler, yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı, Türkiye’de yerleşik dernek, vakıf ve sendikalardan sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler, siyasi partiler, avukatlar, serbest muhasebeci mali müşavirler ve yeminli mali müşavirler veri sorumluları siciline kaydolma zorunluluğundan muaf tutulmuştur⁴⁶⁸. Yine Kurulun, 28.06.2018 tarih ve 2018/68 sayılı kararı uyarınca gümrük müşavirlerine; 05.07.2018 tarih ve 2018/75 sayılı kararı uyarınca arabuluculara veri sorumluları siciline kayıt yükümlülüğü istisnası getirilmiştir⁴⁶⁹. Ayrıca Kurulun, 19.07.2018 tarih ve 2018/87 sayılı kararında, yıllık çalışan sayısı 50’den az ve yıllık mali bilanço toplamı 25 milyon TL’den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanların da veri sorumluları siciline kayıt zorunluluğundan istisna tutulmasına karar verilmiştir⁴⁷⁰. Bu son kararda değinilen kriterler yönünden Kurul tarafından, ülkemizde yaşanan ekonomik koşullar gerekçe gösterilerek yeniden bir değerlendirme yapılmış ve yeni bir karar yayımlanmıştır. 25.07.2023 tarihli 32259 sayılı Resmî Gazetede yayımlanan ve yayımlandığı tarihte yürürlüğe giren 06.07.2023 tarih ve 2023/1154 sayılı Kurul Kararında, 2018/87 sayılı kararda belirtilen yıllık mali bilanço toplamı tutarı güncellenmiş ve ifade “*yıllık çalışan sayısının 50’den az ve yıllık mali bilanço toplamı 100 milyon TL’den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanların*” şeklinde değiştirilmiştir. Görüldüğü üzere artık veri sorumluları siciline kayıt yükümlülüğünden istisna tutulan veri sorumluları, yıllık çalışan sayısı 50’den az ve yıllık mali bilanço toplamı 100 milyon TL’den az olan ve ana faaliyet konusu özel

⁴⁶⁸ İlgili Kurul Kararı için bkz. <https://www.kvkk.gov.tr/Icerik/4233/2018-32>, (26.07.2023).

⁴⁶⁹ Gümrük müşavirleri hakkında verilen karara ulaşmak için bkz. <https://www.kvkk.gov.tr/Icerik/5269/2018-68>, (26.07.2023); Arabulucular hakkında verilen karara ulaşmak için bkz. <https://www.kvkk.gov.tr/Icerik/5270/2018-75>, (26.07.2023).

⁴⁷⁰ İlgili karara ulaşmak için bkz. <https://www.kvkk.gov.tr/Icerik/5271/2018-87>, (26.07.2023).

nitelikli kişisel veri işleme olmayan veri sorumlularıdır⁴⁷¹. Veri sorumluları siciline kayıt yükümlülüğünden muaf tutulan veri sorumlularının 6698 sayılı Kanuna uygun davranma yükümlülüğü ortadan kalkmamaktadır. Diğer bir deyişle, veri sorumluları, veri sorumluları siciline kayıttan muaf tutulmayı, Kanunun kendilerine yüklediği diğer yükümlülüklerden ve Kanundan muaf tutulmak olarak anlamamaları gerekmektedir⁴⁷².

6698 sayılı Kanunun 16. maddesinin üçüncü fıkrasında veri sorumluları siciline kayıt başvurusu yapılırken başvurunun içeriğinde yer alması gereken bilgilere yer verilmiştir. Aynı maddenin dördüncü fıkrasında ise, bildirimde yer alan bilgilerde değişiklik meydana gelmesi halinde bunun derhal Başkanlığa bildirilmesi gerektiği ifade edilmiştir. Maddenin son fıkrası olan beşinci fıkrasında ise veri sorumluları siciline ilişkin diğer usul ve esasların yönetmelikle düzenleneceği belirtilmiştir.

Veri sorumluları siciline yapılması öngörülen kayıtlara ilişkin usul ve esasları belirlemek ve uygulanmasını sağlamak amacıyla “*Veri Sorumluları Sicili Hakkında Yönetmelik*” yayımlanmıştır⁴⁷³. Yönetmelikte veri sorumluları siciline kayıt sürecine ilişkin detaylı açıklamalar yer almaktadır. Aynı zamanda Yönetmelikte tanımlı yapılan “*kışisel veri işleme envanteri*” kavramına da ayrıca değinmek gerekir. Yönetmeliğin 4/1-h maddesinde kişisel veri işleme envanteri tanımlanmıştır. Kışisel veri envanterinin doğru, kapsamlı ve veri sorumlularının kendine özgü yapılarının dikkate alınması suretiyle çeşitli parametreleri içerecek biçimde oluşturulması, başta veri

⁴⁷¹ Yıllık çalışan sayısının ve yıllık mali bilanço toplamının nasıl hesaplanması gerektiği Kışisel Verileri Koruma Kurumunun internet sitesinde yer alan “Sorularla Veri Sorumluları Sicil Bilgi Sistemi” isimli dökümanda yanıtlanmıştır. Dökümanda yıllık çalışan sayısının hesaplanmasında, en başta tamamlanmış bir yıl olması gerektiği ve bu tamamlanmış yıl içerisindeki 12 ayın en az 7’sinin (aynı yıl içerisinde olması gereken bu 7 ayın ardışık olması gerekmemektedir.) her birinde veri sorumlusu tarafından yetkili kurum ve kuruluşlara aylık verilmekte olan Muhtasar ve Prim Hizmet beyannamesinde bildirilen çalışan sayısının esas alınacağı ifade edilmektedir. Yıllık mali bilanço toplamının hesaplanmasında ise yine öncelikle tamamlanmış bir yıl bulunması gerektiği ve o yıl içerisinde veri sorumlusunca yetkili kamu kurumuna yıllık olarak verilmekte olan gelir veya kurumlar vergisi beyanname ekindeki mali tablolarda yer alan mali bilanço bilgisinin dikkate alınacağı belirtilmektedir. Açıklama için bkz. Sorularla Veri Sorumluları Sicil Bilgi Sistemi, https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERB%C4%B0S.pdf, (26.07.2023), ss. 13,14.

⁴⁷² Çelikel, s. 107; Öztürk ve diğerleri, s. 112.

⁴⁷³ Veri Sorumluları Sicili Hakkında Yönetmelik 30.12.2017 tarihli ve 30286 sayılı Resmi Gazetede yayımlanmıştır.

sorumluları siciline kayıt olmak üzere sicile ilişkin diğer iş ve işlemlerde sorun yaşanmaması bakımından bir hayli önem arz etmektedir⁴⁷⁴.

5. Diğer Yükümlülükler

6698 sayılı Kanun kapsamında veri sorumlusunun yukarıda aktarılanlar dışında da çok sayıda yükümlülüğü bulunmaktadır. Çalışmamızda çeşitli konu başlıkları altında ve yeri geldikçe, veri sorumlularının Kanun tarafından öngörülen yükümlülüklerine değinilmektedir. Veri sorumlularına yönelik kanunda öngörülen diğer yükümlülükler: verileri imha etme yükümlülüğü, Kurul kararlarını yerine getirme yükümlülüğü, ilgili kişinin başvuru sürecine ilişkin düzenleme yapma ve başvurulara en kısa sürede cevap verme yükümlülüğü⁴⁷⁵, veri koruma etki değerlendirmesi yapma yükümlülüğü ve veri sorumlusunun zararı tazmin yükümlülüğü örnek gösterilebilir⁴⁷⁶.

III. DENETİM SİSTEMİ

A. Genel Olarak

Kişisel verilerin korunması hakkının bir temel hak ve özgürlük olarak güvence altına alınabilmesi, ancak bu hak üzerinde gerçekleşen veya gerçekleşmesi muhtemel ihlallere yönelik denetimlerin etkin bir şekilde sağlanması yoluyla mümkündür. İlgili kişi, kişisel verilerinin hukuka aykırı işlenmesi halinde hukuk düzeninin kendisine tanıdığı hak arama yollarına başvurma ve dolayısıyla yine kendisine bu hak arama yolları vesilesiyle tanınan korumalardan faydalanma hakkına sahiptir⁴⁷⁷. Nitekim bu doğrultuda mevzuatımızda kişisel verilerin hukuka uygun olarak işlenmesini denetlemek ve hukuka aykırı veri işleme faaliyetlerini yaptırma bağlamak amacıyla çeşitli düzenlemeler yapılmıştır. Bu düzenlemeleri, denetim sistemi başlığı altında incelemek yerinde olacaktır. Çalışmamızda, denetim sistemine ilişkin açıklamalar,

⁴⁷⁴ Dülger, Kişisel Veriler Hukuku, s. 266.

⁴⁷⁵ Öztürk ve diğerleri, ss. 110,111,117.

⁴⁷⁶ Çelikel, ss.113,115.

⁴⁷⁷ Öztürk ve diğerleri, s. 131.

konunun anlaşılma kolaylığının sağlanabilmesi açısından yargı dışı denetim ve yargısal denetim olarak iki alt başlığa ayrılmak suretiyle ele alınmıştır.

B. Yargı Dışı Denetim

1. Genel Olarak

Kişisel verilerin hukuka aykırı şekilde işlenmesinin önlenmesi amacıyla 6698 sayılı Kanunun 13, 14 ve 15. maddelerinde yargısal olmayan bir denetim sistemi öngörülmüştür⁴⁷⁸. Bunlar özetle, veri sorumlusuna başvuru, Kurula şikâyet ve Kurulun ihlal iddiasını öğrenmesi üzerine re'sen harekete geçmesidir. Söz konusu hak arama yollarında dikkat edilmesi gereken husus, veri sorumlusuna başvurunun, Kurula şikâyet öncesinde tüketilmesi gereken bir yol olduğudur⁴⁷⁹. Başka bir ifadeyle kanun koyucu, kademeli bir yapı öngörerek, ilgili kişinin veri sorumlusuna başvuru yapmaksızın Kurula şikâyetinde bulunamayacağını düzenlemiştir⁴⁸⁰.

Belirtmekte fayda var ki, kişisel verileri hukuka aykırı işlenen ilgili kişilerin veri sorumlusuna başvuru ve ardından Kurula şikâyet yollarını kullanmaksızın, genel hükümlere göre doğrudan zararlarının tazmini amacıyla yargısal yollara başvurmaları da mümkündür. Veri sorumlusuna ve Kurula şikâyet başvurusunun amacı, veri sorumlularının veri işleme faaliyetleri üzerinde idari bir denetim sağlanmasıdır⁴⁸¹.

2. Veri Sorumlusuna Başvuru

Kişisel verilerin hukuka aykırı olarak işlenmesi halinde ilgili kişinin başvurabileceği yargısal olmayan ilk yol, 6698 sayılı Kanunun 13. maddesinde düzenlenen veri sorumlusuna başvuru yoludur. Anılan maddenin birinci fıkrasında, ilgili kişinin kanunun uygulanmasına dair taleplerini yazılı yahut da Kurulun

⁴⁷⁸ Bu çerçevede 6698 sayılı Kanunun 13.maddesinde “Veri Sorumlusuna Başvuru”, 14.maddesinde “Kurula Şikayet” ve 15.maddesinde Kurulun resen incelemede bulunma görev ve yetkisine yer verilmiştir.

⁴⁷⁹ Kişisel Verilerin Korunması Kanunun 14.maddesinin ikinci fıkrasında “13’üncü madde uyarınca başvuru yolu tüketilmeden şikâyet yoluna başvurulamaz.” şeklinde bir düzenleme yer almaktadır.

⁴⁸⁰ Başar, s. 225.

⁴⁸¹ Öztürk ve diğerleri, s. 131.

belirleyeceği diğer yöntemlerle veri sorumlusuna ileteceği ifade edilmektedir (Kanun, m. 13/1). Maddenin ikinci fıkrasında, veri sorumlusunun kendisine yöneltilen başvuruda yer alan talepleri, talebin niteliğini de dikkate almak suretiyle en kısa süre içerisinde ve en geç otuz gün içerisinde, ücretsiz bir şekilde sonuçlandırması gerektiği ancak işlem ayrıca bir maliyet gerektiriyorsa, veri sorumlusunun bunun için Kurulun belirlediği tarifede yer alan ücreti alabileceği öngörülmektedir (Kanun, m. 13/2). Maddenin üçüncü ve son fıkrasında ise, veri sorumlusunun ilgili kişi tarafından kendisine yöneltilen başvuruyu kabul yahut gerekçesini açıklamak suretiyle reddedebileceği ve bu cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildireceği belirtilmiştir. Ayrıca aynı fıkarda başvurunun veri sorumlusu tarafından kabulü halinde, gereğinin yerine getirileceği ve başvurunun veri sorumlusuna ait bir hatadan kaynaklanmış olması halinde alınan ücretin ilgili kişiye iade edileceği hükmüne yer verilmiştir (Kanun, m.13/3).

Veri sorumlusuna başvuruyu düzenleyen Kanunun 13. maddesine ek olarak bir de Kişisel Verileri Koruma Kurumu tarafından, veri sorumlusuna yapılacak başvuruların usul ve esaslarını düzenlemek amacıyla “*Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ*” (Tebliğ) kabul edilmiştir⁴⁸². Tebliğin 4. maddesinde kişisel verisi işlenen gerçek kişilerin veri sorumlusuna başvuru hakkına sahip oldukları belirtilmiştir⁴⁸³. Tüzel kişilerin, tıpkı 6698 sayılı Kanunda olduğu gibi Tebliğ’de de kapsam dışında tutulduğu görülmektedir. Tebliğin 5. maddesi ilgili kişinin, veri sorumlusuna başvuru usulüne; 6. maddesi ise veri sorumlusunun başvuruya cevabına

⁴⁸² Bahsi geçen Tebliğ, 10.03.2018 tarih ve 30356 sayılı Resmi Gazetede yayımlanmıştır.

⁴⁸³ Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, m.4.

ilişkindir⁴⁸⁴. İlgili kişinin veri sorumlusuna yapmış olduğu başvuru neticesinde, veri sorumlusu başvuruyu reddeder, herhangi bir yanıt vermez yahut verilen yanıt yeterli görülmezse ilgili kişi Kurul'a şikâyet başvurusu gerçekleştirebilir⁴⁸⁵.

6698 sayılı Kanunun 13. maddesinin ikinci fıkrasında veri sorumlusunun kendisine yapılan başvurudaki talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde sonuçlandırması gerektiği düzenlenmesi yer almaktayken; 14. maddenin birinci fıkrasında veri sorumlusunun başvuruya cevap vermemesi halinde ilgili kişinin Kurula şikâyetle bulunabileceği belirtilmiştir. İki madde hükmü birlikte değerlendirildiğinde bir çelişki ortaya çıktığı aşikardır. Zira bir taraftan veri sorumlusuna başvuruyu sonuçlandırması için azami bir süre öngörülmüş, diğer taraftan ise ilgili kişiye veri sorumlusu tarafından cevap verilmemesinden bahsedilmiştir⁴⁸⁶. Kurul bu konuya ilişkin vermiş olduğu bir kararında, veri sorumlusunun, kendisine 11. madde çerçevesinde başvuruda bulunan ilgili kişinin talep ettiği hususlarla ilgili olarak, Kanunun 15. maddesinin 5. fıkrasına istinaden

⁴⁸⁴ Tebliğin veri sorumlusuna başvuru usulünü düzenleyen 5. maddesi uyarınca, “(1) İlgili kişi, Kanunun 11’inci maddesinde belirtilen hakları kapsamında taleplerini, yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir. (2) Başvuruda; a) Ad, soyad ve başvuru yazılı ise imza, b) Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası, c) Tebligata esas yerleşim yeri veya iş yeri adresi, ç) Varsa bildirimde esas elektronik posta adresi, telefon ve faks numarası, d) Talep konusu, bulunması zorunludur. (3) Konuya ilişkin bilgi ve belgeler başvuruya eklenir. (4) Yazılı başvurularda, veri sorumlusuna veya temsilcisine evrakın tebliğ edildiği tarih, başvuru tarihidir. (5) Diğer yöntemlerle yapılan başvurularda; başvurunun veri sorumlusuna ulaştığı tarih, başvuru tarihidir”; Tebliğin veri sorumlusunun kendisine yöneltilen başvuruya cevabını düzenleyen 6. maddesi uyarınca, “(1) Veri sorumlusu bu Tebliğ kapsamında ilgili kişi tarafından yapılacak başvuruları etkin, hukuka ve dürüstlük kuralına uygun olarak sonuçlandırmak üzere gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür. (2) Veri sorumlusu, başvuruyu kabul eder veya gerekçesini açıklayarak reddeder. (3) Veri sorumlusu, cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. (4) Cevap yazısının; a) Veri sorumlusu veya temsilcisine ait bilgileri, b) Başvuru sahibinin; adı ve soyadını, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarasını, yabancılar için uyruğunu, pasaport numarasını veya varsa kimlik numarasını, tebligata esas yerleşim yeri veya iş yeri adresini, varsa bildirimde esas elektronik posta adresini, telefon ve faks numarasını, c) Talep konusunu, ç) Veri sorumlusunun başvuruya ilişkin açıklamalarını, içermesi zorunludur. (5) Veri sorumlusu başvuruda yer alan talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, işlemin ayrıca bir maliyet gerektirmesi hâlinde, 7’nci maddede belirtilen ücret alınabilir. Başvurunun, veri sorumlusunun hatasından kaynaklanması hâlinde alınan ücret ilgiliye iade edilir. (6) İlgili kişinin talebinin kabul edilmesi hâlinde, veri sorumlusunca talebin gereği en kısa sürede yerine getirilir ve ilgili kişiye bilgi verilir”.

⁴⁸⁵ Küzeci, Kişisel Verilerin Korunması, s. 435.

⁴⁸⁶ Başar, ss. 243,244.

kararın tebliğinden itibaren 30 gün içerisinde cevap vermesi gerektiği, aksi takdirde Kanunun 18. maddesi uyarınca hakkında idari yaptırım uygulanacağı hususunda talimatlandırılmasına karar vermiştir⁴⁸⁷. Görüldüğü üzere Kurul, veri sorumlusuna başvuruda bulunan ilgili kişiye, veri sorumlusunca mutlaka bir cevap verilmesi yönündeki iradesini ortaya koymaktadır. Bu bakımdan örneğin, veri sorumlusu, ilgili kişinin başvurusu neticesinde kendisinde o kişiye ait herhangi bir kişisel veri bulunmadığını tespit etmiş olsa dahi başvuru sahibine bu hususta cevap vermekle yükümlü olmaktadır⁴⁸⁸.

3. Kişisel Verileri Koruma Kurumu Tarafından Gerçekleştirilen Denetim

a. Kişisel Verileri Koruma Kurumu

Kişisel verilerin korunması alanında faaliyet gösteren ve bağımsız bir kamu tüzel kişiliğine sahip olan “*Kişisel Verileri Koruma Kurumu*” (Kurum), 6698 sayılı Kişisel Verilerin Korunması Kanununun 19-27’nci maddelerinde düzenlenmektedir. Kişisel Verileri Koruma Kurumu, idari teşkilat içerisinde düzenleyici ve denetleyici kurumlar arasında yer almaktadır⁴⁸⁹. Nitekim 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, (III) Sayılı Cetvelde düzenleyici ve denetleyici kurumlar belirtilmiş ve bu kurumlar arasında Kişisel Verileri Koruma Kurumuna da yer vermiştir. Kanunun “*Kişisel Verileri Koruma Kurumu*” başlıklı 19. maddesinde, Kişisel Verileri Koruma Kurumu’nun idari ve mali özerkliğe sahip ve kamu tüzel kişiliğini haiz olduğu belirtilmektedir (Kanun, m. 19/1). Burada kamu tüzel kişilerinin işlemleriyle ilgili bazı açıklamalarda bulunmak faydalı olacaktır. Kamu tüzel kişileri, faaliyetlerinde kural olarak idare hukukuna tabi olup faaliyetleri sebebiyle doğan uyuşmazlıklar kural olarak idari yargıda çözülür. Kamu tüzel kişileri, kamu gücü ayrıcalıklarından faydalandıkları için görev ve yetkileri kapsamında tek taraflı işlemler yapma yetkisine sahiptir. Yine kamu tüzel kişilerinin işlemleri icrailik özelliğine sahip olup hukuka

⁴⁸⁷ İlgili karar için bkz. <https://www.kvkk.gov.tr/Icerik/5414/Veri-Sorumlusu-Tarafindan-Kanunda-Belirlenen-Sure-Icerisinde-Ilgili-Kisiye-Cevap-Verilmemesi>, (23.08.2023).

⁴⁸⁸ Öztürk ve diğerleri, s. 132.

⁴⁸⁹ Başar, s. 206.

uygunluk karinesinden faydalanmaktadır. Ayrıca kamu tüzel kişilerinin aldıkları kararları re'sen icra yetkisi bulunmaktadır⁴⁹⁰.

6698 sayılı Kanunun 19.maddenin gerekçesinde Avrupa Konseyinin 108 sayılı Sözleşmesinde ve Avrupa Birliğinin 95/46/EC sayılı Direktifinde kişisel verilerin işlenmesine ilişkin ilkelerin uygulanmasını izlemek ve yönlendirmek üzere, bağımsız şekilde faaliyet yürütecek otoritelerin oluşturulmasının öngörüldüğü, Avrupa Birliği üyesi ülkelerin tamamında veri koruma kurullarının bağımsız denetim otoriteleri şeklinde yapılandırıldığı ve söz konusu uluslararası belgeler ve mukayeseli hukuk uygulamaları dikkate alınarak Kişisel Verileri Koruma Kurumunun kurulduğu belirtilmektedir⁴⁹¹. Kişisel verilerin korunması alanında faaliyet yürüten denetim organının bağımsızlığı yalnızca bir kural olarak belirlenmekle sınırlı kalmamalı, uygulamanın da bu yönde etkin bir şekilde gelişmesi gerekmektedir⁴⁹². Gerçekten de kişisel verilerin korunması hakkının etkin bir şekilde sağlanabilmesi açısından Kurumun kritik bir konuma sahip olduğunu belirtmekte ayrıca fayda vardır.

6698 sayılı Kanunun 19.maddesinin ikinci fıkrasında Kurum'un, Cumhurbaşkanının görevlendireceği Bakan ile ilişkili olduğu ifade edilmektedir. Bağımsız idari otoritelerin, bağlı veya ilgili kuruluşlardan farkını ifade etmek, idare ile arasındaki ilişkiyi kurmak ve bağımsızlıklarını temin etmek amacıyla bu kurumlar için ilişkili kuruluş kavramı kullanılmaktadır. Kurumun Bakanlık ile ilişkili olması idarenin bütünlüğü ilkesinin bir gereği olup bu yolla merkezi idare ile uyum sağlanması söz konusu olacaktır. Ancak bu husus bir idari vesayet ilişkisi doğduğu şeklinde anlaşılmamalıdır. Kaldı ki, böyle bir denetim de Kurumun amacıyla bağdaşmaz⁴⁹³. Kurumun ilişkili olduğu bakan ise Adalet Bakanısıdır.

Kurumun, görev alanı itibariyle uygulama ve mevzuat gelişmelerini takip etmek, araştırma ve incelemelerde bulunmak, kişisel verilerle ilgili uluslararası gelişmeleri izlemek, bunları değerlendirmek, görev alanında ulusal ve uluslararası kurum ve kuruluşlarla işbirliği yapmak gibi çok sayıda görevi bulunmaktadır (Kanun, m. 20/1). Kurum Kurul ve Başkanlıktan oluşan bir yapıya sahip olup karar organı ise

⁴⁹⁰ Başar, s. 209.

⁴⁹¹ TBMM, "Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu", ss. 14,15.

⁴⁹² Küzeci, Kişisel Verilerin Korunması, s. 424.

⁴⁹³ Başar, ss. 207,208.

Kuruldur (Kanun, m. 19/4). Kurumun karar organının kurul şeklinde yapılanmış olmasının kurumun özerk yapısını pekiştiren bir faktör olduğunu ayrıca belirtmek gerekir⁴⁹⁴.

b. Kişisel Verileri Koruma Kurulu

Kişisel Verileri Koruma Kurulu, Kurumun karar organı olup görevleri Kanunun 22. maddesinde düzenlenmektedir. Kurulun görevlerini açıklamadan önce Kanunun 21. maddesinin birinci fıkrasına değinmek gerekir. Zira Kişisel Verileri Koruma Kurumu ve Kurumun karar organı olan Kurulun ne kadar önemli bir görevi olduğunu, 21. maddede yer verilen ifadeler ortaya koymaktadır. İlgili hüküm uyarınca, Kurul kendisine 6698 sayılı Kanun ve diğer mevzuat düzenlemeleri ile verilen görev ve yetkileri, kendi sorumluluğu altında ve bağımsız şekilde yerine getirir. Ayrıca görev alanına giren konularla ilgili olarak Kurul’a hiçbir makam, merci, organ veya kişi emir ve talimat veremez. Yine hiçbir organ, makam, merci veya kişi Kurul’a telkin ve tavsiyede bulunamaz (Kanun, m. 21/1). Kurumun karar organı Kurul aracılığıyla bağımsız şekilde hareket etmesi iki biçimde karşımıza çıkar. Bunlardan ilki, üyelerinin süresi dolmadan görevden alınamaması anlamına gelen organ üzerinde bağımsızlıktır. İkincisi ise kararların hiçbir organ, makam yahut mercii tarafından müdahalede bulunulmaksızın bağımsız olarak alınması olan işlem üzerinde bağımsızlıktır⁴⁹⁵. Kurul, beş üyesi Türkiye Büyük Millet Meclisi, dört üyesi ise Cumhurbaşkanı tarafından seçilen toplamda 9 üyeden oluşmaktadır (Kanun, m. 21/2).

Kurulun görev ve yetkileri Kanunun 22. maddesinde düzenlenmektedir. Hükmün en başında da yer verildiği üzere, Kurulun başlıca görevi, kişisel verilerin temel hak ve özgürlüklere uygun bir şekilde işlenmesini sağlamaktır. Nitekim bu doğrultuda yine aynı hükmün devamında Kurulun görevleri, kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikayetlerini karara bağlamak, kendisine yapılan şikayet başvurusu veya ihlal iddiasını öğrenmesi üzerine re’sen kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde

⁴⁹⁴ Esin Gürsel ve Fatih Düğmeci, “Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu’na İlişkin Bir Değerlendirme”, **R&S- Research Studies Anatolia Journal**, Cilt:1, Sayı:2, 2018, s. 327.

⁴⁹⁵ Öztürk ve diğerleri, s. 127.

geçici önlemler almak, özel nitelikli kişisel verilerin işlenmesinde aranan yeterli önlemlerin neler olduğunu belirlemek, veri sorumluları sicilini tutmak, Kurulun görev alanı ve Kurumun işleyişi hakkında gerekli düzenleyici işlemleri yapmak, veri güvenliğine ilişkin yükümlülüklerin belirlenmesi amacıyla düzenleyici işlem yapmak, veri sorumlusunun ve temsilcisinin görev, yetki ve sorumlulukları hakkında düzenleyici işlem yapmak, 6698 sayılı Kanunda öngörülen idari yaptırımlara karar vermek, diğer kurum ve kuruluşlar tarafından hazırlanan ve kişisel verilerin korunmasına ilişkin hükümler ihtiva eden mevzuat taslakları hakkında görüş bildirmek, Kurumun stratejik planını karara bağlamak ve amaçlarını, hedeflerini, hizmet kalite ve standartlarını, performans kriterlerini belirlemek, Kurumun stratejik planı, amaç ve hedeflerine uygun şekilde hazırlanan bütçe teklifini görüşüp karara bağlamak, Kurumun performansı, mali durumu, yıllık faaliyetleri ile ihtiyaç duyulan konulara ilişkin hazırlanan rapor taslaklarını onaylamak ve yayımlamak, taşınmaz alımı, satımı ve kiralanması konularındaki önerileri görüşmek ve karara bağlamak, Kanunlarla verilen diğer görevleri yerine getirmektir⁴⁹⁶. Görüldüğü üzere Kurulun sahip olduğu geniş görev ve yetkiler yine Kurulun, bir anayasal hak niteliğinde olan kişisel verilerin korunması açısından ne kadar kilit bir konumda olduğunu ortaya koymaktadır⁴⁹⁷.

(1) Kişisel Verileri Koruma Kurulu'na Şikâyet

6698 sayılı Kanunun 14. maddesinde Kurula şikâyet hususu düzenlenmiştir. Buna göre, ilgili kişinin veri sorumlusuna başvuru gerçekleştirmesinin ardından veri sorumlusunun söz konusu başvuruyu reddetmesi, başvuruya verdiği cevabın yetersiz bulunması yahut süresinde başvuruya cevap vermemiş olması hallerinde ilgili kişiye, veri sorumlusunun cevabını öğrendiği tarihten itibaren 30 ve her halde başvuru tarihinden itibaren 60 gün içerisinde Kurula şikâyetle bulunma hakkı tanınmıştır (Kanun, m. 14/1). Kurul'a intikal eden şikâyetlerde, söz konusu sürelerin yorumlanmasına ilişkin farklılıklar bulunduğu tespit edilmesi üzerine bir karar yayımlanarak anılan yorum farklılıkların ortadan kaldırılması amaçlanmıştır. Kişisel

⁴⁹⁶ Kişisel Verilerin Korunması Kanunu, m.22.

⁴⁹⁷ Küzeci, Kişisel Verilerin Korunması, s. 426.

Verileri Koruma Kurulu'nun 24.01.2019 tarih ve 2019/9 sayılı anılan kararında, ilgili kişinin başvurusu üzerine veri sorumlusu, 30 gün içerisinde bir cevap vermiş ise ilgili kişinin veri sorumlusunun cevabını müteakiben 30 gün içerisinde Kurul'a şikayette bulunabileceği; şayet veri sorumlusu tarafından ilgili kişiye herhangi bir cevap verilmemiş ise ilgili kişinin veri sorumlusuna başvuru tarihinden itibaren 60 gün içerisinde Kurula şikayet yoluna gidebileceği; veri sorumlusu 30 gün geçtikten sonra cevap vermiş ise, ilgili kişinin Kanunda veri sorumlusuna tanınan 30 günlük süre sonrasında cevabı bekleme yükümlülüğünün bulunmadığı ve cevap verme süresinin dolduğu hususlarından bahisle ilgili kişinin veri sorumlusuna başvuru tarihinden itibaren 60 gün içerisinde şikayette bulunabileceği ifade edilmektedir⁴⁹⁸. Mevzuatta yer alan şikâyet süreleri ilgili kişi tarafından geçirildikten sonra Kurul'a şikâyetle bulunulursa ne olacağı hususunu da değerlendirmek faydalı olacaktır. Böyle bir durumda Kurul, 15. madde uyarınca şikâyet veya ihlal iddiasını öğrenmesi üzerine re'sen incelemelerde bulunabilir⁴⁹⁹.

6698 sayılı Kanunun Kurula şikâyeti düzenleyen 14. maddesinde ayrıca, daha önce de ifade ettiğimiz üzere, 13. madde uyarınca veri sorumlusuna başvuru yolu tüketilmeden Kurul'a şikâyet yoluna gidilemeyeceği ve kişilik hakları ihlal edilenlerin genel hükümlere göre tazminat haklarının saklı olduğu belirtilmiştir (Kanun, m. 14/2,3).

6698 sayılı Kanunun 15. maddesi ise Kurulun şikâyet üzerine veya re'sen yapacağı incelemenin usul ve esaslarını düzenlemektedir. Anılan maddenin birinci fıkrasında, daha önce de değindiğimiz üzere, Kurulun şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda re'sen, görev alanına giren konularda gerekli incelemeleri yapacağı ifade edilmektedir (Kanun, m. 15/1). Bu hükme göre Kurul, başta kendisine gelen ihbarlar olmak üzere örneğin yazılı yahut görsel basında kamuya açık şekilde yer alan ve 6698 sayılı Kanuna aykırı veri işleme faaliyeti gerçekleştirildiğine dair iddialar içeren haberleri dayanak göstererek re'sen inceleme başlatabilecektir⁵⁰⁰. Başka bir deyişle, Kurul'un inceleme yapması için illaki bir

⁴⁹⁸ Kişisel Verileri Koruma Kurulu'nun 24.01.2019 tarih ve 2019/9 sayılı Kararı, <https://www.kvkk.gov.tr/Icerik/5358/Kamuoyu-Duyurusu>, (23.08.2023).

⁴⁹⁹ Küzeci, Kişisel Verilerin Korunması, s. 436.

⁵⁰⁰ Öztürk ve diğerleri, s. 135.

şikâyet gerekmemekle birlikte bu, ortada hiçbir sebep yokken Kurul'un incelemede bulunabileceği şeklinde de anlaşılmamalıdır. Zira şikâyet bulunmasa da Kurul'un inceleme başlatabilmesi için ihlal iddiasının bir şekilde öğrenilmesi yahut makul bir ihlal şüphesinin bulunması gerekir⁵⁰¹. Maddenin ikinci fıkrasında Kurul'a intikal ettirilecek şikâyet başvurularının 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6. maddesinde belirtilen şartlara uygun olarak yapılması gerektiği aksi halde söz konusu ihbar veya şikâyetlerin incelemeye alınmayacağı belirtilmektedir⁵⁰². Maddenin 3. fıkrasında, devlet sırrı niteliğindeki bilgi ve belgeler hariç olmak üzere veri sorumlusunun, Kurul'un kendisinden inceleme konusuyla ilgili talep ettiği bilgi ve belgeleri 15 gün içerisinde Kurul'a göndermek ve gerektiği takdirde yerinde inceleme yapılmasına imkân sağlamak zorunda olduğu düzenlenmiştir (Kanun, m. 15/3). Maddenin dördüncü fıkrasında, kendisine yapılan şikâyet başvurusu üzerine Kurul'un, talebi incelemek suretiyle ilgililere bir cevap vereceği, şikâyet tarihinden itibaren 60 gün içerisinde ilgililere Kurul tarafından bir cevap verilmemiş ise talebin reddedilmiş sayılacağı hükmü yer almaktadır (Kanun, m. 15/4). Söz konusu düzenleme birçok yönden eleştirilmeye müsaittir. Zira 6698 sayılı Kanun, veri sorumlusuna kendisine yapılan başvuruya 30 gün içerisinde cevap verme yükümlülüğü yüklüyor ve buna uyulmamasını idari yaptırıma bağlarken, bu hususları denetleyen ve idari para cezası kesme yetkisini haiz Kurul'a suskun kalma hakkının verilmesi çelişki ortaya koymaktadır⁵⁰³.

Maddenin 5. fıkrasına göre, şikâyet üzerine veya re'sen yapılan inceleme sonucunda Kurul, bir ihlalin varlığını tespit etmişse, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine yönelik bir karar vererek bunu ilgililere tebliğ eder. Bu karar, tebliğden itibaren gecikmeye mahal verilmeksizin ve en geç 30 gün içerisinde veri sorumlusu tarafından yerine getirilir (Kanun, m. 15/5). Verilen kararın

⁵⁰¹ Dülger, Kişisel Veriler Hukuku, s. 246.

⁵⁰² 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun m.6 hükmü uyarınca "Türkiye Büyük Millet Meclisine veya yetkili makamlara verilen veya gönderilen dilekçelerden; a) Belli bir konuyu ihtiva etmeyenler, b) Yargı mercilerinin görevine giren konularla ilgili olanlar, c) 4' üncü maddede gösterilen şartlardan herhangi birini taşımayanlar, incelenemezler."; Kişisel Verileri Koruma Kurumu tarafından Kuruma yapılacak şikâyetlerin usul şartlarına ilişkin olarak da ayrıca bir kamuoyu duyurusu yayımlanmıştır. Söz konusu duyuruda 3071 sayılı Kanunun 6.maddesi hükmüne de yer verilmek suretiyle Kurul'a yapılacak şikâyetlerin taşınması gereken usuli şartlara değinilmiştir. İlgili duyuruya ulaşmak için bkz. <https://www.kvkk.gov.tr/Icerik/6938/Kurumumuza-Yapilan-Sikayetlerin-Usul-Sartlarina-Iliskin-Kamuoyu-Duyurusu>, (23.08.2023).

⁵⁰³ Dülger, Kişisel Veriler Hukuku, s. 245.

en geç 30 gün içerisinde yerine getirilmemesi üzerine verilen bir Kurul kararında, kamu kuruluşu olarak değerlendirilen veri sorumlusunun, Kurul kararının gereğini, 15. maddenin beşinci fıkrasında belirtilen 30 günlük yasal süre içerisinde yerine getirmediğinden bahisle şirket hakkında 18. maddenin üçüncü fıkrası çerçevesinde işlem tesis edilmesine karar vermiştir⁵⁰⁴.

Maddenin 6. fıkrasında, şikâyet üzerine yahut re'sen yapılan inceleme sonucunda, ihlalin yaygın olduğunun tespit edilmesi durumunda Kurul'un bu konuda ilke kararı alacağı ve söz konusu kararı yayımlayacağı belirtilmektedir. Fıkranın devamında, Kurul'un ihtiyaç duyması halinde, ilke kararı almadan önce, ilgili kurum ve kuruluşların görüşüne başvurabileceği ifade edilmiştir (Kanun, m. 15/6). Alınan ilke kararları Resmî Gazete'de ve Kurum'un internet sitesinde yayımlanmaktadır. İlke kararları, gelişen teknolojinin etkisiyle farklı şekillerde karşılaşılan hukuka aykırı veri işleme faaliyetlerine karşı önlemler alınmasını ve böylelikle kişisel verilerin korunmasını sağlayabilecektir⁵⁰⁵. Örneğin Kurul vermiş olduğu bir ilke kararında, e-ticaret, ulaşım, turizm gibi muhtelif sektörlerde faaliyet yürüten veri sorumlularınca fatura, ekstre, rezervasyon belgesi gibi kişisel veri içeren dökümanların sms ve/veya e-posta ile gönderimini teminen ilgili kişilerden telefon numarası ve/veya e-posta adreslerinin istenildiği ancak ilgili kişilerin bu bilgileri beyanında yanlışlıklar olabildiği ve böylelikle ilgili kişiye ait kişisel verilerin üçüncü kişilere iletildiği durumlar için ilgili kişiler üzerinde olumsuz sonuçlar doğmasının önlenmesi amacıyla ilgili kişilerce beyan edilen iletişim bilgilerinin doğrulanmasına yönelik makul önlemlerin (telefon numarası ve/veya e-posta adresine doğrulama kodu/linki gönderilmesi gibi) alınması gerektiğini ifade etmiştir⁵⁰⁶. Kanunun 15. maddesinin 7. fıkrasında ise Kurul'un, telafisi güç ve imkânsız zararların doğması ve açıkça hukuka aykırılıkların bulunması halinde veri işlenmesi ve verilerin yurt dışına aktarılmasının durdurulmasına karar verebileceği düzenlemesi yer almaktadır.

⁵⁰⁴ Kişisel Verileri Koruma Kurulu'nun 16.10.2018 tarih ve 2018/118 sayılı Kararı, <https://www.kvkk.gov.tr/Icerik/5422/2018-118>, (23.08.2023).

⁵⁰⁵ Başar, s. 258.

⁵⁰⁶ Kişisel Verileri Koruma Kurulu'nun 22/12/2020 tarih ve 2020/966 sayılı İlke Kararı, <https://www.kvkk.gov.tr/Icerik/6858/2020-966>, (24.08.2023).

(2) Kişisel Verileri Koruma Kurulunun İdari Yaptırım Yetkisi

6698 sayılı Kanunun 18. maddesinde kabahat türleri düzenlenmiştir. Madde gerekçesinde, ilgili maddede, Kanunda öngörülen yükümlülüklerle aykırı davranılması halinde uygulanacak idari yaptırımların düzenlendiği belirtilmektedir⁵⁰⁷. Başka bir deyiş ile, veri sorumlusunun yükümlülüklerine aykırı davranması halinde, 18. madde kapsamında belirtilen kabahatler oluşacak ve idari para cezaları uygulanması gündeme gelecektir. Kurul, 18. maddede yer verilen para cezalarına, ilgili kişinin şikâyeti üzerine veya re'sen yürüteceği inceleme üzerine karar verebilecektir⁵⁰⁸. Maddenin birinci fıkrasında, aydınlatma, veri güvenliğinin sağlanması, Kurul kararlarının yerine getirilmesi ve veri sorumluları siciline kayıt ve bildirim yükümlülüklerine aykırı davranılması kabahat olarak düzenlenmiş ve idari para cezası yaptırımına bağlanmıştır. Hükümde belirtilen idari para cezası miktarları, 5326 sayılı Kabahatler Kanunun 17. maddesinin 7. fıkrası uyarınca her takvim yılı başından itibaren geçerli olmak üzere o yıl için 213 sayılı Vergi Usul Kanunun mükerrer 298.maddesi hükümleri gereğince tespit ve ilan edilen yeniden değerlendirme oranında arttırılarak uygulanmaktadır⁵⁰⁹. İdari para cezaları açısından belirtmekte fayda var ki, kanun hükmünde öngörülen cezalar ihlal başına verilmektedir. Zira Türk Ceza Kanunu'nda kabul edilen zincirleme suç hükümlerinin Kabahatler hukukunda söz konusu olmaması sebebiyle her hukuka aykırılık bakımından yaptırımlar ayrı ayrı uygulanmaktadır⁵¹⁰. Kurulun vereceği idari para cezalarına karşı idari yargı yolunun açık olduğunu da ayrıca belirtmek gerekir⁵¹¹.

Kanun 18. maddesinin ikinci fıkrasında, öngörülen idari para cezalarının veri sorumlusu olan gerçek kişiler ve özel hukuk tüzel kişileri hakkında uygulanacağı ifade edilmektedir. Görüldüğü üzere Kanun, idari para cezası yaptırımına tabi tutulacak kişiler arasında gerçek kişiler ile özel hukuk tüzel kişileri arasında bir ayrım

⁵⁰⁷ TBMM, “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 14.

⁵⁰⁸ Öztürk ve diğerleri, ss. 119,120.

⁵⁰⁹ Nitekim anılan hükmün gerekçesinde, Kanunda, kabahatlerle ilgili hüküm bulunmayan hallerde genel kanun niteliğini haiz 5326 sayılı Kabahatler Kanunu hükümlerinin uygulanacağını açık olduğu belirtilmektedir. Bkz. TBMM, “Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu”, s. 14.

⁵¹⁰ Dülger, Kişisel Veriler Hukuku, s. 374.

⁵¹¹ Küzeci, Kişisel Verilerin Korunması, s. 437.

gitmemiştir⁵¹². Maddenin üçüncü fıkrasında ise, birinci fıkrada belirtilen eylemlerin, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi halinde, Kurulun yapacağı bildirim üzerine ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılacağı ve sonucunun Kurula bildirileceği ifade edilmiştir. Görüldüğü üzere 18. maddede yer verilen kabahatler kamu tüzel kişisi tarafından işlenirse, Kurul o kamu tüzel kişisine idari para cezası veremeyecektir. Ancak sorumlu kamu görevlilerinin disiplin sorumluluğuna gidilmesi mümkün olacaktır⁵¹³. Elbette, idarenin idari para cezası yaptırımına tabi tutulmaması makuldür. Ancak kişisel verilerin işlenmesindeki genel ilkelere idarenin uyumunu sağlayacak etkin bir sisteme ihtiyaç bulunduğu da aşıkardır⁵¹⁴.

C. Yargısal Denetim

1. Genel Olarak

6698 sayılı Kanun, kişisel verilerin etkin bir şekilde korunabilmesi adına kendi içerisinde veri sorumlusuna başvuru ve Kurula şikâyet şeklinde, yargısal nitelikte olmayan, bir başvuru mekanizması öngörmüştür. Ancak bu başvurular ilgili kişinin genel hükümler uyarınca dava açma imkânını ortadan kaldırmamaktadır. İlgili kişi, veri sorumlusunun niteliğine göre adli veya idari yargıya da başvurabilir. Başka bir deyişle, ilgili kişiler bir taraftan Kanundaki başvuru sürecini işletirken bir taraftan da veri sorumlusunun niteliğine göre adli yargıda veya idari yargıda dava açma imkanına sahiptirler⁵¹⁵. Nitekim bu doğrultuda, 6698 sayılı Kanunun 14. maddesinin üçüncü fıkrasında, “*kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır*” ifadesine yer verilmiştir. Yine Kurul kararlarına karşı dava açılabilir. Ancak buna ilişkin Kanun’da ayrıca bir düzenleme yer almamaktadır. Kişisel verilerin

⁵¹² Dülger, Kişisel Veriler Hukuku, s. 374.

⁵¹³ Öztürk ve diğerleri, s. 122.

⁵¹⁴ Küzeci, Kişisel Verilerin Korunması, s. 442.

⁵¹⁵ Samet Saygı, “6698 Sayılı Kanun’un Sistematığında Yargısal Başvuru Yolları”, **Kişisel Verileri Koruma Dergisi**, Cilt:2, Sayı:2, 2020, ss. 30,31.

işlenmesinde karşılaşılabilecek hukuka aykırılıkların cezai boyutu ise Kanunun 17. maddesinde düzenlenmektedir.

2. Adli Yargı Denetimi

a. Özel Hukuk Hükümleri Çerçevesinde Kişisel Verilerin Korunması

Özel hukuk hükümleri çerçevesinde kişisel verilerin korunmasını iki açıdan değerlendirmek mümkündür. Bunlardan birincisi, kişisel verilerin hukuka aykırı olarak işlenmesi neticesinde ilgili kişi lehine doğabilecek tazminat hakkıdır. Bu hak özellikle Türk Medeni Kanunu'nun ve Türk Borçlar Kanunu'nun ilgili hükümleri çerçevesinde ele alınabilir. İkinci olarak ise kişisel veri işleme faaliyetlerinin artarak yaygınlaşması neticesinde sözleşmeler hukuku, işçi-işveren ilişkileri, elektronik ticaret gibi hukukun bazı özel alanlarında özel hukuk hükümlerine gereksinim duyulması durumudur⁵¹⁶.

Veri sorumlusunun özel hukuk kişisi olması halinde, kişisel verilerin hukuka aykırı işlenmesine dair çıkacak uyuşmazlıkların en başında kişilik haklarının korunmasına yönelik genel hükümlere başvuru hususu gündeme gelmektedir⁵¹⁷. Kişilik hakkı, kişinin kişiliğini oluşturan, insanı insan yapan maddi manevi tüm değerlere, özel olarak ise insan onuruna, beden bütünlüğüne, sağlığına, saygınlığına, özel yaşamının gizliliğine, özgürlüğüne, adına, resmine, ekonomik hareket serbestliğine ilişkin hakkıdır⁵¹⁸. Başka bir deyişle, kişinin hukuk düzeni tarafından korunan ve kişi olmasına bağlı olarak sahip olduğu bütün kişilik değerlerini ifade eden hukuki bir kavramdır⁵¹⁹. Kişisel verilerin korunmasına ilişkin birçok husus aynı zamanda kişilik hakkını ilgilendirmekte ve hatta kişilik haklarıyla aynı değerleri korumaktadır⁵²⁰. Kaldı ki, çalışmamızın ilgili bölümünde de ifade ettiğimiz üzere, kişisel verilerin korunması hakkı kanaatimizce genel kişilik hakkı olarak nitelendirilmesi gereken bir haktır. Hal böyle iken, kişisel verilerin korunması hakkına

⁵¹⁶ Küzeci, Kişisel Verilerin Korunması, s. 445.

⁵¹⁷ Saygı, s. 32.

⁵¹⁸ Serozan, s. 93.

⁵¹⁹ Şaban Kayıhan, **Kişiler Hukuku**, Seçkin Yayıncılık, Ankara, 2022, s. 68.

⁵²⁰ Saygı, s. 32.

yönelik gerçekleştirilecek her ihlalin aynı zamanda kişilik hakkı ihlali olduğunu belirtmek de yanlış olmayacaktır⁵²¹. 6698 sayılı Kanunun 14. maddesinin üçüncü fıkrası uyarınca “*Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır*”. Hükümde sözü edilen genel hükümlerden anlaşılması gereken, 4721 sayılı Türk Medeni Kanunu’nun “*Kişiliğin korunması*” üst başlığı altında düzenlenen 24. ve 25. maddeleri ile 6098 sayılı Türk Borçlar Kanunu’nun “*Haksız Fiillerden Doğan Borç İlişkileri*” ana başlığını taşıyan ve ikinci ayırım altında düzenlenen 53, 54, 56 ve 58. maddeleridir⁵²². Medeni Kanun genel olarak, ilgili kişiye, haksız saldırının önlenmesi, saldırıya son verilmesi, saldırının tespiti gibi kişilik hakkının korunmasına yönelik hâkimden talepte bulunabileceği özel bazı yetkiler öngörmüş, ilgili kişinin haksız saldırıdan doğan maddi-manevi tazminat ve vekaletsiz iş görme hükümleri uyarınca varsa kazancın kendisine devri talebi hakkının saklı olduğunu belirtmiştir⁵²³.

Kişisel verileri hukukun özel alanlarından bir tanesi olan ve özel hukuk bağlamında bir koruma gerektirmesi söz konusu olabilen sözleşme ilişkileri bakımından ele almanın faydalı olacağı kanaatini taşıyoruz. Zira ilgili kişi ile veri sorumlusu arasında kişisel verilerin işlenmesine ilişkin bir sözleşme ilişkisi bulunması durumunda ilgili kişi sözleşmeden kaynaklanan haklarını kullanabilecektir⁵²⁴. Kişisel verilerin sözleşmesel sorumluluk çerçevesinde korunması, Culpa in Contrahendo sorumluluğu, genel işlem şartları, sözleşmeden doğan borçların ifa edilmemesi ve kişisel veri işleme sözleşmeleri gibi başlıklar altında ayrı ayrı ele alınmayı gerektiren bir konudur⁵²⁵. Örneğin, bir sözleşmede tarafların kişisel verileri, bunun işlenmesine ilişkin bir edim yükümlülüğü içermese dahi koruma yükümlülükleri kapsamında korunur. Ancak ister kişisel verilerin korunması koruma yükümlülüğü kapsamında; ister kişisel verilerin işlenmesi borcu asli edim yükümlülüğü kapsamında olsun somut olayda hukuka aykırı bir işleme var ise bu, sözleşmenin gereği gibi ifade edilmemesi anlamını taşır. Her iki durumda da Türk Borçlar Kanunu’nun borcun ifa edilmemesi

⁵²¹ Mehmet Oğuz Vuraloğlu, “Kişisel Verilerin İşlenmesi Suretiyle Kişilik Hakkı İhlalinde Kazancın Devri Talebi”, **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:15, Sayı:1, 2018, s. 184.

⁵²² Damla Gürpınar, “Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk”, **D.E.Ü Hukuk Fakültesi Dergisi**, Prof. Dr. Şeref Ertaş’a Armağan, Cilt:19, Özel-Sayı, 2017, ss. 689-690.

⁵²³ 4721 Sayılı Türk Medeni Kanunu, m.24,25.

⁵²⁴ Saygı, s. 33.

⁵²⁵ Taştan, s. 61.

sebebiyle zararın giderilmesini düzenleyen 112. maddesine başvurulabilecektir. Edim yükümlülüklerinin ihlali bağımsız şekilde talep ve dava edilmeye müsaitken, koruma yükümlülüğünün ihlali bağımsız şekilde talep ve dava edilemeyip yalnızca tazminat davasına konu edilebilmektedir⁵²⁶. Yukarıda anılan, Culpa in Contrahendo sorumluluğu, genel işlem şartları, sözleşmeden doğan borçların ifa edilmemesi ve kişisel veri işleme sözleşmeleri gibi hususların her birine ilişkin açıklamalarda bulunmak, çalışmamızın amaç ve kapsamının aşılmasına sebebiyet verebilecek derinliğe sahiptir. Bu sebeple çalışmamızda yalnızca sözleşme ilişkilerine dair genel değerlendirmelere yer verilmiştir.

b. Ceza Hukukunda Kişisel Verilerin Korunması

5237 sayılı Türk Ceza Kanunu'nun (TCK) "*Kişilere Karşı Suçlar*" başlıklı ikinci kısmının "*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*" başlıklı dokuzuncu bölümünde kişisel verilerin korunmasıyla ilgili suç tipleri düzenlenmiştir. TCK'nın 135. maddesinde "*Kişisel verilerin kaydedilmesi*", 136. maddesinde "*Verileri hukuka aykırı olarak verme veya ele geçirme*", 137. maddesinde cezaların arttırılmasını gerektiren nitelikli haller, 138. maddede ise "*verileri yok etmeme*" suçları düzenlenmiştir. TCK'nın 139. maddesinde "*(1) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikâyeteye bağlıdır*" hükmüne yer vermek suretiyle aynı bölümün 132. maddesinde yer verilen "*Haberleşmenin gizliliğini ihlal*", 133. maddesinde yer verilen "*Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması*" ve 134. maddesinde yer verilen "*Özel hayatın gizliliğini ihlal*" suçlarının soruşturulmasının ve kovuşturulmasının şikayete bağlı olduğu; buna karşılık kişisel verilerle doğrudan ilgili yukarıda zikredilen diğer suç tiplerinin soruşturulması ve kovuşturulmasının şikayete bağlı olmadığı ifade edilmektedir. 6698 sayılı Kanunun "*Suçlar ve Kabahatler*" başlıklı beşinci bölümünün "*Suçlar*" başlıklı 17. maddesinin birinci fıkrası hükmü uyarınca ise "*(1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140'ıncı madde hükümleri uygulanır*". Görüldüğü üzere 6698 sayılı Kanunun 17. maddesinin

⁵²⁶ Taştan, ss. 87,88.

birinci fıkrasında, Türk Ceza Kanunu'nda düzenlenen kişisel verilerin korunması ile ilgili suç tiplerine atıfta bulunmaktadır. Belirtmekte fayda var ki, teknolojide yaşanan gelişmelerin kişisel verilere müdahale olanaklarını arttırması ve insan hakları alanında yaşanan gelişmeler, kişisel verilerin korunması ihtiyacını giderek arttırmış ve kişisel verilerin korunmasına yönelik suç tiplerinin düzenlenmesine zemin hazırlamıştır⁵²⁷.

TCK'nın 135. maddesinde kişisel verilerin kaydedilmesi suçu düzenlenmiştir. Hükmün birinci fıkrasında, kişisel verilerin hukuka aykırı olarak kaydedilmesinin cezalandırılacağı ifade edilmektedir. 6698 sayılı Kanunda, kişisel verilerin hukuka aykırı olarak kaydedilip kaydedilmediği hususunun belirlenmesinde dikkate alınması gereken temel ilkelere yer verilmekte olup bununla birlikte zikredilen “*hukuka aykırılık*” ifadesinin pozitif hukuk düzenlemelerinin de ötesinde bir anlama sahip olduğunu ayrıca belirtmekte yarar vardır⁵²⁸. Hükmün ikinci fıkrasında ise birtakım veri türleri sayılarak söz konusu verilere özel bir önem atfedilmiş ve bu verilerin kaydedilmesi verilecek cezayı ağırlaştırıcı sebep olarak düzenlenmiştir. Maddenin ikinci fıkrasında yer verilen veri türleri dikkatle incelendiğinde, 5237 sayılı Türk Ceza Kanunu ile 6698 sayılı Kişisel Verileri Koruma Kanunu arasında, ek güvencelerle koruma altına alınmış kişisel veriler bakımından bazı farklılıklar olduğu görülmektedir. Her iki Kanunda da kişilerin siyasi, felsefi, dini görüşleri, ırksal kökenleri, sağlık durumları, cinsel yaşamları ve sendika üyelikleri hassas veri kapsamına alınmıştır. Ancak etnik köken, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek ve vakıf üyelikleri, ceza mahkumiyeti ve güvenlik tedbirleri hakkındaki kişisel veriler ile biyometrik ve genetik verileri, 6698 sayılı Kanunda hassas veri kategorisinde sayılmasına rağmen 5237 sayılı Türk Ceza Kanunu'nda hassas veri olarak sayılmayıp ek güvencelerle korumaya tabi tutulmamıştır. Buna karşılık, 5237 sayılı TCK ahlaki eğilimlere ilişkin kişisel verileri, hassas veri olarak değerlendirip ek güvencelerle koruma altına almış iken, 6698 sayılı Kanunda ahlaki eğilim hassas veri kategorisinde sayılmamıştır⁵²⁹. Bu suç tipine ilişkin son olarak, TCK

⁵²⁷ Şeyma Sert, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, 2.Baskı, Seçkin Yayıncılık, Ankara, 2023, s. 97.

⁵²⁸ Küzeci, s. 480.

⁵²⁹ Korkmaz, *Kişisel Veriler*, ss. 431,432.

m. 137 kapsamında düzenlenen nitelikli hallerde değinmekte yarar görüyoruz. Zira TCK'nın 137. maddesi, muhteviyatı gereği, kişisel verilerin kaydedilmesi suç bakımından cezayı ağırlaştırıcı neden olarak uygulama bulmaktadır⁵³⁰. Buna göre, kişisel verilerin kaydedilmesi suçunun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle yahut da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi hallerinde ceza ağırlaştırılarak verilecektir.

TCK'nın 136. maddesinde verileri hukuka aykırı olarak verme veya ele geçirme suçu düzenlenmektedir. Bahse konu hüküm uyarınca, *“(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır. (2) Suçun konusunun, Ceza Muhakemesi Kanununun 236'ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.”*. Bu madde metni bakımından belirtilmesi gereken ilk husus, böyle bir suç tipinin kişisel verilerin yetkisiz üçüncü kişilere aktarımın önlenmesi amacıyla düzenlenmiş olduğudur⁵³¹. Değinilmesi gereken bir diğer husus ise başkasına verilen, yayılan yahut da ele geçirilen kişisel verilerin, hukuka uygun olarak kaydedilmiş veriler olup olmasının suçun oluşması bakımından herhangi bir etkisinin bulunmamasıdır. Nitekim madde gerekçesinde bu durum açıkça ortaya konmuştur⁵³². Yargıtay da bir kararında⁵³³, TCK m. 136 gerekçesine de değinmek suretiyle şu ifadelerle yer vermiştir: *“TCK'nın 136/1. maddesinin, gerekçesinden de anlaşılacağı üzere, “kişisel verilerin, “verildiği”, “yayıldığı” veya “ele geçirildiği”nin kabul edilebilmesi için, kişisel verilerin kaydedilmiş halde bulunması, kaydedilmiş haliyle başkalarına verilmesi, yayılması ya da ele geçirilmesi gerekir”*. Maddenin ikinci fıkrasında suçun nitelikli haline yer verildiği görülmektedir. Buna göre, suçun konusunun çocuğun cinsel istismarı ve cinsel saldırı suçlarından mağdur olanların beyan ve görüntülerine ilişkin olması

⁵³⁰ TCK'nın 137. Maddesi uyarınca *“(1) Yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, işlenmesi halinde, verilecek ceza yarı oranında artırılır.”*

⁵³¹ Küzeci, Kişisel Verilerin Korunması, s. 484.

⁵³² Dülger, Kişisel Veriler Hukuku, ss. 347,348.

⁵³³ Yargıtay 12.Ceza Dairesi'nin 21.12.2016 tarih ve 2015/10737 E., 2016/13557 K. sayılı kararına ulaşmak için bkz. <https://karararama.yargitay.gov.tr/>, (19.09.2023).

halinde verilecek ceza bir kat arttırılacaktır⁵³⁴. Suçun nitelikli hallerini oluşturan bir diğer hüküm ise TCK'nın 137. maddesinde düzenlenmiştir. Tıpkı 135. maddede olduğu gibi bu suç tipi bakımından da, kişisel verileri hukuka aykırı olarak veren, yayan veya ele geçiren kişinin kamu görevlisi olması ve görevinin verdiği yetkiyi kötüye kullanmak suretiyle bu suçu işlemesi halinde yahut da bu suçun belli bir meslek ve sanatın sağladığı kolaylıktan faydalanmak suretiyle işlenmesi halinde ceza ağırlaştırılarak verilecektir.

TCK'da doğrudan kişisel verilerin korunması alanına ilişkin olarak düzenlenen suç tiplerinden bir diğeri 138. maddede yer almaktadır. Söz konusu maddede verileri yok etmeme suçunu düzenlenmektedir. Ayrıca 6698 sayılı Kanunun 17. maddesinin ikinci fıkrasında *“Bu kanunun 7'nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hale getirmeyenler 5237 sayılı Kanunun 138'nci maddesine göre cezalandırılır”* hükmüne yer verilmiştir. TCK'nın 138. maddesinde göze çarpan ilk detay, kişisel verileri yok etmekle yükümlü olanların görevlerini yerine getirmemesi halinde cezai yaptırıma tabi tutulacaklarının öngörülmesidir. Bu çerçevede, verileri yok etmeme suçunun bir özgü suç olduğunu belirtmek gerekir. Zira suç ancak ve ancak verileri yok etme yükümlülüğü altında bulunan kişilerce işlenebilecektir⁵³⁵. Öncelikle, 6698 sayılı Kanunun 3. maddesinin birinci fıkrasının ı) bendi uyarınca *“veri sorumlusu”* nun, verilerin yok edilmesinden sorumlu olduğunu ifade etmek gerekir⁵³⁶. Nitekim 6698 sayılı Kanunun 7. maddesinde *“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”* düzenlemesi yer almaktadır. Ayrıca verileri yok etme yükümlülüğü altındaki kişilerin, TCK'nın 6. maddesinde tanımı verilen *“kamu görevlisi”* sıfatını taşımak zorunda olmadığını ve bu suç açısından failin kamu görevlisi olmasının aranmadığını belirtmemiz gerekir⁵³⁷. Verilerin yok edilmesine ilişkin olarak süreler hususuna da değinmekte yarar vardır. Verilerin yok edilmesi hakkında özel bir süre söz konusu

⁵³⁴ Küzeci, Kişisel Verilerin Korunması, s. 484.

⁵³⁵ Sert, s. 157.

⁵³⁶ Uğur Orhan, “Kişisel Verilerin Korunmasına İlişkin Türk Ceza Hukuku Düzenlemeleri Üzerine Değerlendirmeler”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 70, Sayı: 4, 2021, s. 1373.

⁵³⁷ Dülger, Kişisel Veriler Hukuku, s. 361.

değilse 6698 sayılı Kanunun 7. maddesi uyarınca kişisel verilerin işleme sebeplerinin ortadan kalkmasıyla birlikte ilgili kişinin talebi üzerine ya da re'sen, veri sorumlusu tarafından, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi gerekmektedir. Ayrıca 6698 sayılı Kanunda, diğer kanunlarda yer alan hükümlerin saklı olduğu belirtilmektedir. Bu sebeple hukuken yok edilmesi gerekli olan kişisel verilerin mevzuat düzenlemelerinin de ayrıca incelenmesi faydalı olacaktır⁵³⁸. Örneğin, Ceza Muhakemesi Kanununun 81. maddesinin ikinci fıkrasında, aynı maddenin birinci fıkrası çerçevesinde sanığın kayda alınan kişisel verilerinin hükümde belirtilen hallerde “*derhal*” yok edilmesi gerektiği düzenlenmiştir. Bu suç tipi açısından son olarak, kişisel verileri yok etmeme suçu, yalnızca ihmal yoluyla işlenebilen bir suç olup, yasal yükümlülük altındakiler bu yükümlülüğünü ihmalen yerine getirmediklerinde söz konusu suç işlenmiş olmaktadır⁵³⁹.

Kişisel verilere ilişkin yukarıda zikredilen suçlar bakımından tüzel kişilerin durumu ise TCK'nın 140. maddesinde düzenlenmiştir. Söz konusu hüküm uyarınca, “*Yukarıdaki maddelerde tanımlanan suçların işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur*”.

3. İdari Yargı Denetimi

a. Kurul Kararlarının Yargısal Denetimi

Anayasamızın 2. maddesinde ifade bulan “*hukuk devleti*” kavramının bir gereği de idarenin yargısal denetimidir. Yine Anayasamızın 125. maddesinde “*İdarenin her türlü işlem ve eylemlerine karşı yargı yolu açıktır.*” hükmü yer almaktadır. İdarenin yargısal denetimi, bir yandan idarenin hukuka uygun hareket etmesini sağlarken diğer yandan bireylerin idarenin keyfi işlem ve eylemlerine karşı korunmasını sağlamaktadır⁵⁴⁰. Nitekim düzenleyici ve denetleyici kurumlardan birisi olan Kişisel Verileri Koruma Kurumu ve onun yönetim ve karar organı olan Kurul'un işlem ve eylemlerine karşı yargı yollarının öngörülmüş olması Türkiye Cumhuriyeti'nin bir

⁵³⁸ Orhan, ss. 1373,1374.

⁵³⁹ Küzeci, Kişisel Verilerin Korunması, s. 486.

⁵⁴⁰ Öztürk e diğerleri, s. 136.

hukuk devleti olmasından kaynaklanmaktadır⁵⁴¹. Kişisel Verileri Koruma Kurumunun kişisel verilerin korunması alanını düzenlemenin yanında bu alanda denetlemelerde bulunma ve gerektiğinde yaptırım uygulama görev ve yetkisi bulunmaktadır. İdari bir organ olan Kurumun bu görev ve yetkileri idari fonksiyon kapsamında değerlendirilmektedir. Dolayısıyla Kurumun vereceği kararlar idari niteliği haiz olması sebebiyle Anayasa m. 125 uyarınca yargı denetimine açık olacaktır⁵⁴².

Öncelikle, Kurumun karar organı olan Kurulun, yaptırımlar alanında verebileceği karar türlerine değinmekte yarar görüyoruz. Şöyle ki Kurul kendisine yapılan şikâyet başvuruları veya re’sen başlattığı incelemeler neticesinde bir ihlalin varlığını tespit ederse dört şekilde karar tesis edebilmektedir. Birincisi Kurulun, veri sorumlusunun ihlali ortadan kaldırmasına karar vermesi halidir. İkinci olarak ise Kurul, veri sorumlusunun fillerinin 6698 sayılı Kanunun 18. maddesinde düzenlenen kabahatleri oluşturduğuna karar vermesi halinde yine aynı hüküm uyarınca idari para cezasına hükmedebilecektir. Kurulun somut olayda ihlal tespit etmesi üzerine verebileceği üçüncü karar şekli ise veri işlemenin ve aktarımının durdurulması kararıdır. Dördüncü olarak Kurul, Resmî Gazete’de yayımlanmak üzere ilke kararı da alabilmektedir⁵⁴³. 6698 sayılı Kanunda, bu kanun uyarınca verilecek idari para cezalarına itiraz yolunu düzenleyen özel bir hüküm bulunmadığını ifade etmek gerekir⁵⁴⁴. Ancak buna karşılık, 5326 sayılı Kabahatler Kanununun 3.maddesinde “(1) *Bu Kanunun; a) İdari yaptırım kararlarına karşı kanun yoluna ilişkin hükümleri, diğer kanunlarda aksine hüküm bulunmaması halinde, ... uygulanır*” hükmü yer almaktadır. 5326 sayılı Kabahatler Kanunun 27. maddesinde ise, idarî para cezası ve mülkiyetin kamuya geçirilmesine ilişkin idarî yaptırım kararına karşı, sulh ceza mahkemesine başvurulabileceği düzenlenmiştir. Görüldüğü üzere 6698 sayılı Kanun çerçevesinde uygulanacak idari para cezalarına karşı, Kabahatler Kanununun 27. maddesi

⁵⁴¹ Yasin Aydoğdu, “Kamu idaresinde Kişisel Verilerin Korunması”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 29, Sayı: 1, 2021, ss. 283,284.

⁵⁴² Öztürk ve diğerleri, s. 136.

⁵⁴³ Salih İnan, “Kişisel Verilerin Korunması Kapsamında İhdas Edilen Yaptırım Kararlarına Karşı Yargısal Başvuru Yolları: Karşılaştırmalı Bir İnceleme”, **Kişisel Verileri Koruma Dergisi**, Cilt: 3, Sayı: 2, 2021, s. 53; Saygı, s. 43.

⁵⁴⁴ Öztürk ve diğerleri, s. 137.

doğrultusunda, kararın tebliği tarihinden itibaren en geç on beş gün içinde kabahatin işlendiği yerdeki⁵⁴⁵ Sulh Ceza Hakimliklerine itirazda bulunulabilecektir.

Kurul tarafından verilen ve veri sorumlusunun idari para cezasına tabi tutulması yaptırım dışındaki yaptırım kararları için yargısal denetim idari yargı denetimine tabidir. Örneğin, ilgili kişi tarafından Kurul’a yapılan şikâyet başvurusunun reddi kararına yahut da Kurulun veri aktarımının durdurulmasına ilişkin veri sorumlusunun talimatlandırılması gibi kararlarına karşı 2577 sayılı İdari Yargılama Usulü Kanunu kapsamında iptal davası açılabilir⁵⁴⁶. Tam da bu noktada, Kurul tarafından idari para cezası ile idari yargının görev alanına giren başka idari yaptırım kararlarının birlikte verilmesi halinde, bu kararlara karşı nasıl bir yargısal denetim sürecinin işletilebileceği hususuna değinmek yararlı olacaktır. Şöyle ki, Kabahatler Kanunun 27. maddesinin sekizinci fıkrası uyarınca, “*İdarî yaptırım kararının verildiği işlem kapsamında aynı kişi ile ilgili olarak idarî yargının görev alanına giren kararların da verilmiş olması halinde; idarî yaptırım kararına ilişkin hukuka aykırılık iddiaları bu işlemin iptali talebiyle birlikte idarî yargı merciinde görülür*”. Görüldüğü üzere Kurul tarafından idari para cezası ile idari yargının görev alanına giren idari yaptırım kararının birlikte verilmesi halinde, idari yargının görev alanına giren idari yaptırım kararına (örneğin, veri sorumlusu için veri aktarımının durdurulması kararına) ilişkin hukuka aykırılık iddiaları, idari para cezası ile birlikte idari yargı mercii önünde ileri sürülebilecek ve ayrıca idari para cezası için sulh ceza hakimliğine başvuru yapılması gerekmeyecektir⁵⁴⁷. Bu durumda idari işlemle birlikte idari para cezasına itiraz edilmek istendiğinde görevli ve yetkili mahkeme Ankara İdare Mahkemeleri olacaktır⁵⁴⁸.

6698 sayılı Kanunun Kurulun görev ve yetkilerinin düzenlendiği 22. maddesinin birinci fıkrasının e) bendinde “*Kurulun görev alanı ile Kurumun işleyişine*

⁵⁴⁵ 5326 sayılı Kabahatler Kanunun 22.maddesinin dördüncü fıkrası uyarınca “4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun yer bakımından yetki kuralları kabahatler açısından da geçerlidir.” Ceza Muhakemesi Kanunun 12.maddesinin birinci fıkrası uyarınca ise “Davaya bakmak yetkisi, suçun işlendiği yer mahkemesine aittir.” Bu iki düzenlemeden hareketle kişisel verilerin korunması bağlamında yetki hususu ele alındığında suçun işlendiği yer, kabahate konu fiili işleyen veri sorumlusunun yerleşim yeri olarak düşünülebilecek ve Kurulun idari para cezasına karşı veri sorumlusunun yerleşim yerindeki Sulh Ceza Hakimliğine itiraz edilebilecektir. Bu konu hakkında açıklamalar için bkz. Saygı, s. 49.

⁵⁴⁶ Öztürk ve diğerleri, s. 137.

⁵⁴⁷ İnan, s. 56.

⁵⁴⁸ Aydoğdu, s. 288.

ilişkin konularda gerekli düzenleyici işlemleri yapmak” ve f) bendinde “*Veri Güvenliğine ilişkin konularda gerekli düzenleyici işlemleri yapmak*” şeklindeki hükümler vasıtasıyla Kurula birtakım düzenleyici işlemler gerçekleştirme yetkisi de verilmektedir. 2575 sayılı Danıştay Kanunun 24. maddesinin birinci fıkrasının c) bendinde Bakanlıklar, kamu kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşlarının çıkarmış olduğu ve ülke çapında uygulanacak düzenleyici işlemlere karşı açılan davaları Danıştay’ın ilk derece mahkemesi olarak görüp karara bağlayacağını düzenlemektedir⁵⁴⁹. Buradan hareketle, kamu kurumu niteliğindeki Kişisel Verileri Koruma Kurumu ve onun yürütme ve karar organı niteliğini haiz organı Kurul tarafından çıkarılan ve ülke çapında uygulanacak düzenleyici işlemlerine karşı Danıştay’da dava açılabilir⁵⁵⁰; ülke çapında olmayan düzenleyici işlemleri bakımından ise 2577 sayılı İdari Yargılama Usulü Kanunun 32. maddesi⁵⁵¹ uyarınca Ankara İdare Mahkemeleri yetkili ve görevli olacaktır.

b. Kişisel Verilerin İşlenmesine İlişkin İdari Yargı Denetimi

Kişisel verilerin korunmasında yargısal denetimin bir yönü de idare ve idari yargılama hukuku ile yakından ilişkilidir. Zira 6698 sayılı Kanun veri sorumlusunu tanımlarken, özel hukuk kişileri ve kamu tüzel kişileri arasında bir ayrıma gitmemiştir. Bu çerçevede kamu tüzel kişiliğine sahip idari kurum ve kuruluşların da somut olayın muhteviyatına göre veri sorumlusu olabilmesi mümkündür. Gerçekten de kamu hizmetinin yerine getirilmesi, planlama, güvenliğin sağlanması, suçluluğun önlenmesi gibi çok önemli görevlere sahip olan idare, bu görevlerini etkin bir şekilde yerine getirebilmek amacıyla kişisel verilere ihtiyaç duymakta ve kişisel verileri işlemektedir⁵⁵². Kamu tüzel kişisi idari kurum ve kuruluşların veri sorumlusu sıfatını

⁵⁴⁹ 2575 sayılı Danıştay Kanunun 24.maddesinin birinci fıkrasının c) bendi uyarınca, “1.Danıştay ilk derece mahkemesi olarak: ... c) Bakanlıklar ile kamu kuruluşları veya kamu kurumu niteliğindeki meslek kuruluşlarınca çıkarılan ve ülke çapında uygulanacak düzenleyici işlemlere, ... Karşı açılacak iptal ve tam yargı davaları ile tahkim yolu öngörülme-yen kamu hizmetleri ile ilgili imtiyaz şartlaşma ve sözleşmelerinden doğan idari davaları karara bağlar.”

⁵⁵⁰ Aydoğan, ss.285, 286.

⁵⁵¹ İdari Yargılama Usulü Kanununun 32. maddesinin birinci fıkrası uyarınca, “1.Göreve ilişkin hükümler saklı kalmak şartıyla bu Kanunda veya özel kanunlarda yetkili idare mahkemesinin gösterilmemiş olması halinde, yetkili idare mahkemesi, dava konusu olan idari işlemi veya idari sözleşmeyi yapan idari mercinin bulunduğu yerdeki idare mahkemesidir”

⁵⁵² Küzeci, Kişisel Verilerin Korunması, s. 528.

haiz olabilmeleri, kişisel verilerin işlenmesi ve korunmasına ilişkin getirilen kurallara uygun davranmalarını gerektirmektedir. Başka bir ifade ile, idareden kişisel veriler söz konusu olduğunda hukuka uygun davranması beklenir. Aksi halde idarenin sorumluluğu gündeme gelecektir⁵⁵³.

İdari makamların kamu hukuku alanındaki faaliyetlerinden ortaya çıkan uyuşmazlıkların çözümlenmesi ise idari yargının görevidir⁵⁵⁴. Burada, bir kamu kurumunun, sunduğu hizmetler bakımından özel hukuk hükümlerine tabi olması tereddüt doğurabilecek bir husustur. Böyle bir durumda veri sorumlusu olan kuruma yönelik dava yollarının belirlenmesi açısından tercih edilmesi gereken yaklaşım, kurumun kuruluş ve işleyişinin niteliğidir. Eğer söz konusu kurum, kamusal işlemlerle kurulmuş ve kamusal kurallara göre işliyorsa kamu kurumu olarak değerlendirilmelidir⁵⁵⁵.

Yukarıda, 6698 sayılı Kanunda yer verilen veri sorumlusuna başvuru ve Kurula şikâyet başvuru usullerinin, ilgili kişinin dava açma hakkını ortadan kaldırmadığını ve kamu kurum ve kuruluşlarının kişisel verileri işlerken ilgili kişinin haklarını ihlal etmesi halinde idarenin sorumluluğunun doğacağını ifade etmiştik. Ayrıca 6698 sayılı Kanunda belirtilen başvuru usullerinin, veri sorumlusu kamu tüzel kişinin idari işlemlerine karşı dava açmadan önce tüketilmesi zorunlu idari başvuru yolları niteliğinde olmadığını da önemle belirtmek gerekir⁵⁵⁶. İdari yargıda yargısal denetim, iptal ve tam yargı davaları yoluyla sağlanmaktadır. İptal davasında idari işlemi meydana getiren unsurlardan herhangi birindeki hukuka aykırılık iddiası ileri sürülmekte ve söz konusu işlemin iptali istenmekte iken; tam yargı davalarında idarenin bir işlem, eylem yahut eylemsizliğinden ötürü doğan zararın tazmini

⁵⁵³ Saygı, ss. 37-40.

⁵⁵⁴ Başar, s. 270.

⁵⁵⁵ Saygı, s. 38; Kurul 02.05.2019 tarih ve 2019/122 Karar sayılı kararında, 6698 sayılı Kanunun 11. maddesinde yer alan hakları çerçevesindeki taleplerini içeren kayıtlı elektronik posta ile veri sorumlusu Ziraat Bankası A.Ş'ye başvuruda bulunan ancak bu başvurusuna otuz günlük süresi içerisinde cevap alamayan ilgili kişinin şikâyetini, "... banka nezdinde, Kanunun 18. maddesinin üçüncü fıkrası çerçevesinde ihlale sebebiyet veren sorumlular ile gerekli tedbirleri almak ve denetimleri yapmakla yükümlü kişiler hakkında disiplin hükümlerine göre işlem yapılmasına,...karar verilmiştir" şeklinde karara bağlayarak her ne kadar veri sorumlusu anonim şirket olsa da adı geçen bankayı somut başvuru yönünden kamu kurumu olarak değerlendirmiştir. İlgili karar için bkz. <https://www.kvkk.gov.tr/Icerik/5461/2019/122>, (15.09.2023).

⁵⁵⁶ Öztürk ve diğerleri, s. 140.

istenilmektedir⁵⁵⁷. Görüldüğü üzere, kişisel verilerin korunmasının idare hukuku çerçevesindeki yargısal denetimi konusu, 2577 sayılı İdari Yargılama Usulü Kanunu ile 6698 sayılı Kişisel Verilerin Korunması Kanununun birlikte değerlendirilmesi gerekliliğini ortaya koymaktadır.

Kişisel verilerin işlenmesindeki hukuka aykırılık, bir idari işlem vasıtasıyla gerçekleşiyorsa ilgili kişinin dava açma süresi içerisinde iptal davası açma hakkı bulunmaktadır. Bununla birlikte söz konusu idari işleminden doğan zararın tazmini için ilgili kişi, İYUK m. 12⁵⁵⁸ kapsamında tam yargı davası da açabilecektir. Tam yargı davası iptal davası ile birlikte, iptal davasından sonra veyahut da ayrıca doğrudan açılabilir⁵⁵⁹.

Kişisel verilerin işlenmesi hususunda gerçekleşen ihlal, idari bir eylemden kaynaklanıyorsa bu halde, zarar gören ilgili kişinin İYUK m. 13⁵⁶⁰ çerçevesinde öncelikle zarara konu eylemi gerçekleştiren idareye başvurması gerekmektedir. Aksi halde idari merci tecavüzü söz konusu olacaktır. İdari eylemlerden ötürü hakları ihlal edilenler, dava yoluna başvurmadan önce, ihlale konu eylemin kendilerine yazılı olarak bildirilmesi üzerine veya başka surette öğrendikleri tarihten itibaren bir yıl ve her halde eylemin gerçekleştiği tarihten itibaren beş yıl içerisinde idareye başvurarak tazminini istemelidirler. Bu isteklerin reddedilmesi halinde işlemin kendilerine tebliğini izleyen günden itibaren yahut da istek hakkında otuz gün içerisinde idarece

⁵⁵⁷ Başar, s. 282.

⁵⁵⁸ İdari Yargılama Usulü Kanununun 12.maddesi uyarınca “İlgililer haklarını ihlal eden bir idari işlem dolayısıyla Danıştaya ve idare ve vergi mahkemelerine doğrudan doğruya tam yargı davası veya iptal ve tam yargı davalarını birlik-te açabilecekleri gibi ilk önce iptal davası açarak bu davanın karara bağlanması üzerine, bu husustaki kararın veya kanun yollarına başvurulması halinde verilecek kararın tebliği veya bir işlemin icrası sebebiyle doğan zararlardan dolayı icra tarihinden itibaren dava süresi içinde tam yargı davası açabilirler. Bu halde de ilgililerin 11.madde uyarınca idareye başvurma hakları saklıdır.”

⁵⁵⁹ Saygı, s. 39.

⁵⁶⁰ İdari Yargılama Usul Kanununun 13. maddesi uyarınca “(1) İdari eylemlerden hakları ihlal edilmiş olanların idari dava açmadan önce, bu eylemleri yazılı bildirim üzerine veya başka suretle öğrendikleri tarihten itibaren bir yıl ve her halde eylem tarihinden itibaren beş yıl içinde ilgili idareye başvurarak haklarının yerine getirilmesini istemeleri gereklidir. Bu isteklerin kısmen veya tamamen reddi halinde, bu konudaki işlemin tebliğini izleyen günden itibaren veya istek hakkında otuz gün içinde cevap verilmediği takdirde bu sürenin bittiği tarihten itibaren, dava süresi içinde dava açılabilir. 2. Görevli olmayan adli yargı mercilerine açılan tam yargı davasının görev yönünden reddi halinde sonradan idari yargı mercilerine açılacak davalarda, birinci fıkrada öngörülen idareye başvurma şartı aranmaz.”

cevap verilmemesi halinde bu sürenin bitiş tarihinden itibaren dava süresi içerisinde tam yargı davası açılması söz konusu olacaktır⁵⁶¹.

IV. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN İDARENİN UYGULAMA ÖRNEKLERİ

A. Genel Olarak

Anayasamızın 2. maddesinde Devletimizin “sosyal bir hukuk devleti” olduğu belirtilmiştir. Bu çerçevede idarenin gerçekleştirmekle yükümlü olduğu çok sayıda görevi bulunmaktadır. İdarenin başlıca görevlerini beş ana başlıkta saymak mümkündür. Bunlar, kamu hizmetini yürütme, idari kolluk faaliyetleri, özendirme ve destekleme faaliyetleri, planlama faaliyetleri ve iç düzen (özyönetim) faaliyetleridir⁵⁶². İdare söz konusu görevlerini gerçekleştirmek için muhtelif işlem ve eylemlerde bulunmaktadır. Burada idari işlev kavramına da değinmekte yarar vardır. Nitekim idari işlev (idari fonksiyon), yasama fonksiyonu, yargı fonksiyonu ve yürütmenin salt siyasal nitelikli faaliyetleri dışında kalan, devletin gündelik toplumsal ihtiyaçlarını karşılamak amacıyla yürüttüğü bütün kamusal faaliyetlerden oluşmaktadır⁵⁶³. İdare işlevinin amacı, kamu yararını gerçekleştirmektir⁵⁶⁴. Kamu yararı kavramından ne anlaşılması gerektiğine ilişkin olarak Anayasa Mahkemesi’nin bir kararında yaptığı tanımlama yol gösterici olacaktır. Kararda, “*kamu yararı, genel bir ifadeyle, bireysel, özel çıkarlardan ayrı ve bunlara üstün olan toplumsal yararı ifade etmektedir*” şeklinde belirtilmiştir⁵⁶⁵.

⁵⁶¹ Emel Badur ve Nesibe Kurt Konca, “Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini ve Görevli Mahkeme”, **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 13, Sayı: 2, 2022, s. 485; Saygı, s. 41.

⁵⁶² Oğuz Sancakdar ve diğerleri, **İdare Hukuku Teorik Çalışma Kitabı**, Seçkin Yayıncılık, 5. Baskı, Ankara, 2015, s.45.

⁵⁶³ Sancakdar ve diğerleri, s. 46.

⁵⁶⁴ Ramazan Yıldırım ve Serkan Çınarlı, **Türk İdare Hukuku Dersleri Cilt: I**, Astana Yayınları, Ankara, 2018, s. 31.

⁵⁶⁵ Anayasa Mahkemesi’nin 23.05.2015 tarihli ve 29364 sayılı Resmi Gazetede yayımlanan 13.05.2015 tarih, 2015/34 E. ve 2015/48 K. sayılı kararına ulaşmak için bkz. <https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2015-48-nrm.pdf>, (20.09.2023).

O halde konuyu çalışmamız bakımından ele almak gerekirse, en temelde kamu yararının gerçekleştirilmesi, sosyal devletin yaşama geçirilebilmesi, güvenliğin sağlanması ve kamu hizmetlerinin etkin bir şekilde yürütülmesi gibi görevleri sebebiyle idarenin gerçekleştirmiş olduğu faaliyetlerde kişisel verileri işleminin gerekli olduğu açıktır⁵⁶⁶. İşlenen kişisel verilerin, hukuka uygun bir şekilde işleniyor olması hukuk devleti olmanın bir gereği olup, bu gereklilik idarenin keyfiliğini önleyerek idareyi hukuka bağlayacak ve bireylerin başta kişisel verilerinin korunması hakkı olmak üzere temel hak ve özgürlüklerini güvence altına almış olacaktır.

B. Elektronik Devlet (E-Devlet) Hizmeti Bakımından

Elektronik hizmetler yoluyla devlet ile vatandaş arasındaki ilişkilerin planlanması ve yönetimi günümüzde kamu yönetimlerinin yapılanma çalışmalarının odak noktasında yer almaktadır⁵⁶⁷. Ülkemizde elektronik devlet ya da yaygın kullanılan tabiriyle e-devlet hizmeti, kamu yönetimindeki her türlü faaliyetin, vatandaşlar, kamu çalışanları, işletmeler ve devletin diğer fonksiyonlarıyla ilgili etkileşimlerin elektronik ortam üzerinden sunulmasını ve aracısız olarak kullanılmasını sağlamaktadır⁵⁶⁸. E-Devlet hizmetinin genel olarak üç önemli amacı olduğu söylenebilir. Bunlar, kamusal hizmetleri daha yaygın ve erişilebilir kılmak, kamu hizmetlerinin üretimi ve yönetimi sürecinde vatandaşın talep ve eğilimlerini daha verimli değerlendirerek katılımcı vatandaşlığın önünü açmak ve devlet kurumlarının daha verimli ve rasyonel işleminin sağlamaktır. Bunların yanında e-devlet hizmeti sayesinde devlet, maliyet ve zaman tasarrufu sağlanmakta, vatandaşların kamu hizmetine erişiminde geleneksel devlet uygulamalarının çıkardığı zorluklar aşılmakta ve bürokrasi azalmaktadır. Ayrıca kamu hizmetlerinde hız artmakta ve bu hizmetlerin kesintisizliği sağlanmaktadır⁵⁶⁹.

Her ne kadar e-devlet hizmeti gerek idare gerekse vatandaşa çok önemli avantajlar sunuyor ise de bu hizmet çerçevesinde kişisel verilerin çeşitli kurumlarca

⁵⁶⁶ Küzeci, Kişisel Verilerin Korunması, ss. 528,529.

⁵⁶⁷ Zerrin Toprak Karaman, "E-Devletin Güvenlik Bağlantılı Sorumlulukları ve E-Vatandaşın Hakları", *Akademik İzdüşüm Dergisi*, Cilt:5, Sayı:1, 2020, s. 4.

⁵⁶⁸ Küzeci, Kişisel Verilerin Korunması, s. 530.

⁵⁶⁹ Murat Akçakaya, "E-Devlet Anlayışı ve Türk Kamu Yönetiminde E-Devlet Uygulamaları", *Yüzüncü Yıl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, Sayı:3, 2017, ss. 13,14.

işleniyor olması ve internet ortamında tutulması veri güvenliğine ilişkin bazı sorunlara sebebiyet verebilir. Daha önce de belirttiğimiz üzere, 6698 sayılı Kanun, kamu sektöründeki veri işleme faaliyetleri açısından da bağlayıcılık taşımaktadır. Kamu sektöründe gerçekleştirilen veri işleme etkinliklerinin 6698 sayılı Kanuna uyumlu bir şekilde gerçekleştirilmesi gerekir⁵⁷⁰. Bilhassa veri güvenliğine ilişkin önlemlerin bilişim teknolojilerindeki gelişmeler takip edilerek güncel ve etkin bir şekilde tutulması büyük öneme sahiptir.

E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelikte (E-Devlet Hizmetleri Yönetmeliği) kişisel verilerin korunmasına atfedilen öneme istinaden birçok düzenlemeye yer verilmiştir. Örneğin, E-Devlet Hizmetleri Yönetmeliğinin “İlkeler” başlıklı 5. maddesinde e-devlet hizmetlerinin hangi ilkeler çerçevesinde yürütüleceği belirtilmiştir: Bunlar arasında “c) Siber Güvenliğin Sağlanması”, “f) Kişisel verilerin korunması ve mahremiyet prensibinin de dikkate alınarak, temel hak ve özgürlüklere riayet edilmesi”, “g) Bilişim sistemlerinin güvenliğine yönelik ulusal ve uluslararası standartlara uyulması”, “ğ) Elektronik ortamda kamu kurum ve kuruluşlarının paylaşımına açık olan verilerin ayrıca kişilerden talep edilmemesi, yalnızca sunulan hizmetin gerektirdiği verilerin istenmesi”, “ı) Kamu kurum ve kuruluşlarınca oluşturulan ve işlenen elektronik ortamdaki verilerin, kaynakların verimliliğinin sağlanması ve mükerrerliğin önlenmesi ilkeleri çerçevesinde katma değerli hizmetler yaratmak üzere mer’i mevzuattan kaynaklanan istisnalar saklı kalmak kaydıyla paylaşılması” yer almaktadır. Hükmün başında yer verilen “Bu Yönetmelik kapsamındaki kamu kurum ve kuruluşları...” ifadesi ile hangi kurum ve kuruluşlarının kastedildiği, E-Devlet Hizmetleri Yönetmeliğinin “Kapsam” başlıklı 2. maddesinde belirtilmektedir. Yine E-Devlet Hizmetleri Yönetmeliğinin Bakanlığın görev ve sorumluluklarını düzenleyen 6. maddesinde, kişisel verilerin korunmasına ilişkin olarak “(1) e-Devlet hizmetlerinin kapsamı ve yürütülmesinde Bakanlığın görev ve sorumlulukları şunlardır:... ı) e-Devlet hizmetleri kapsamında, ulusal siber güvenliğin ve kişisel verilerin korunması konusunda farkındalık sağlamak ve bilişim sistemlerinde gerekli önlemlerin alınması için kamu kurum ve kuruluşlarıyla işbirliği yapar” düzenlemesi yer almaktadır. Bu

⁵⁷⁰ Küzeci, Kişisel Verilerin Korunması, s. 532.

metinde yer verilen “Bakanlık” ifadesi ile Ulaştırma ve Altyapı Bakanlığı kastedilmektedir⁵⁷¹. E-Devlet Hizmetleri Yönetmeliğinin 7. maddesinde kişisel verilerin korunmasına yönelik olarak “1) e-Devlet hizmetlerinin kapsamı ve yürütülmesinde kamu kurum ve kuruluşlarının görev ve sorumlulukları şunlardır: ... a) Kamu kurum ve kuruluşları, yürüttükleri e-Devlet projeleri veya sundukları e-Devlet hizmetleri kapsamında üretmiş oldukları verilerin elektronik ortama taşınmasından, doğruluğundan, güncelliğinden, veri bütünlüğü ve güvenliğinin sağlanmasından ve saklanmasından sorumludur. ... g) Kamu kurum ve kuruluşları kendilerine ait bilgi sistemleri üzerinde siber güvenlik önlemlerini alır, kullanıma ilişkin erişim kayıtlarını tutar ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlar. ... h) Kamu kurum ve kuruluşları e-Devlet uygulamalarının internet üzerinden sunumunda yetkisiz erişimi engelleyecek önlemleri alır” ifadelerine yer verilmiştir. E-Devlet Hizmetleri Yönetmeliğinde ayrıca E-Devlet Kapısı İşletmecisinin⁵⁷² görev ve sorumluluklarına yer verilen 8. maddesinde “a) e-Devlet Kapısı İşletmecisi, bireysel ve kurumsal tüm kullanıcıların kamu hizmetlerine elektronik ortamdan güvenli ve etkin bir şekilde erişebilecekleri, e-Devlet hizmetlerinin sunumunda tek adres olabilecek özelliklere sahip ortak bir platform kurar ve işletir. ... f) e-Devlet Kapısı İşletmecisi, kamu kurum ve kuruluşlarının e-Devlet hizmetlerinin e-Devlet Kapısına entegrasyon, e-Devlet Kapısının işletilmesi, kapı ile ilgili geliştirme, iletişim altyapısı, tanıtım, güvenlik, donanım, yazılım, erişim imkânlarının yaygınlaştırılması gibi e-Devlet Kapısı hizmetlerinin gerektirdiği faaliyetlerin yürütülmesinden görevli ve sorumludur” hükmü yer almaktadır.

⁵⁷¹ E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik, m. 2.

⁵⁷² E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 3.maddesi uyarınca “...ç) e-Devlet Kapısı: e-Devlet hizmetlerinin son kullanıcıya farklı erişim kanallarından tek noktadan bütünsel olarak sunulduğu ortak elektronik platformu, ... d) e-Devlet Kapısı İşletmecisi: 24/3/2006 tarihli ve 2006/10316 sayılı Bakanlar Kurulu Kararı ve 10/8/2006 tarihli ve 2006/22 sayılı Başbakanlık Genelgesi ile e-Devlet Kapısının kurulması ve işletilmesiyle yetkilendirilmiş, 4/2/1924 tarihli ve 406 sayılı Telgraf ve Telefon Kanununun Ek 33’üncü maddesi ile kurulan Türksat Uydu Haberleşme Kablo TV ve İşletme Anonim Şirketini, ... ifade eder.”

C. Sağlık Hizmetleri Bakımından

Sağlık hizmetleri alanı, kişisel verilerin ve özellikle de özel nitelikli kişisel verilerin sıklıkla işlendiği bir alandır. Kişinin sağlık hizmeti alabilmek amacıyla sağlık kuruluşlarında yaptığı hemen her işlemde kişisel verileri işlenmektedir. Öncelikle sağlıkla ilgili tüm tıbbi verilerin, arşiv ve kayıtların özel nitelikli kişisel veri kategorisinde olduğunu ve 6698 sayılı Kanunun 6. maddesinde öngörülen şartlar çerçevesinde işlenebileceğini hatırlamak gerekir. Nitelikleri gereği yeterli teknik ve idari tedbirler alınmaksızın sağlık verilerinin işlenmesinin mümkün olamayacağını ve bu veriler bakımından tüm koruma şartlarının yanında aynı zamanda güvenli ortamın oluşturulmasının gerekliliğini de belirtmekte fayda vardır⁵⁷³. 6698 sayılı Kanunun kamu kurum ve kuruluşları bakımından bağlayıcılığı da düşünüldüğünde idarenin sağlık hizmetlerini yürütürken işlediği kişisel veriler bakımından bu yasaya ve kişisel verilerin korunmasına dair yürürlüğe konmuş sair mevzuat düzenlemelerine uyum içerisinde hareket etmesi gerekmektedir.

Sağlık Bakanlığı'nın sağlık kamu hizmetinin ifası sürecinde elde etmiş olduğu tüm sağlık verilerini yine sağlık hizmetinin gerekleri için kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla işleme yetkisi bulunmaktadır⁵⁷⁴. İdare bu yetkisini hukuka uygun bir şekilde kullanmalıdır. Zira sağlık hizmetlerinin yürütülmesi sürecinde elde edilen kişisel verilerin hatalı veya eksik tutulması, yapılan tedavilerin kayıt altına alınmaması Danıştay tarafından hizmet kusuru olarak görülmektedir. Nitekim Danıştay 10. Dairesi, 27.12.2011 tarih ve 2009/9151 E., 2011/5976 K. sayılı kararında, hastanın röntgen grafilerinin, hastanın dosyasında muhafaza edilmemesi sebebiyle mahkemeye ibraz olunamaması neticesinde idarenin hizmet kusuru olduğuna ve tıbbi verileri kaybolan hastanın yaşanan belirsizlikten üzüntü duyduğunu, bu nedenle uğradığı manevi zararın

⁵⁷³ Sabire Sanem Yılmaz, **Tıp Alanında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, 6. Baskı, Ankara, 2022, ss. 66, 67.

⁵⁷⁴ Ayşe Aslı Alçın, "Türk Hukukunda Kişisel Sağlık Verileri ve İdarenin Kişisel Sağlık Verilerini Koruma Yükümlülüğü", **Türkiye Adalet Akademisi Dergisi**, Sayı: 51, 2022, s. 378; Aynı eserde Sağlık Bakanlığının bu yetkisi, 1 sayılı Cumhurbaşkanlığı Kararnamesinin Sağlık Bakanlığını düzenleyen on ikinci bölümünde yer verilen 378.maddenin birinci ve ikinci fıkrasındaki düzenlemelerinden kaynaklanmaktadır.

tazmininin gerektiğine hükmetmiştir⁵⁷⁵. Görüldüğü üzere idarenin hukuk kurallarının dışına çıkarak veri işleme faaliyetinde bulunması veya veri işleme etkinliklerinin denetimlerini gerektiği gibi yerine getirmemesi neticesinde bireyin bir zararı doğmuş ise bu zarar idare tarafından tazmin edilecektir. Söz konusu tazmin borcu ise, İdari Yargılama Usulü Hakkında Kanunun 2. maddesinin birinci fıkrasının b) bendinde yer alan tam yargı davası vasıtasıyla gerçekleşecektir⁵⁷⁶.

Sağlık hizmetleri bakımından kişisel verilerin korunmasına ilişkin olarak çıkartılan Kişisel Sağlık Verileri Hakkında Yönetmeliğe (Kişisel Sağlık Verileri Yönetmeliği) değinmekte fayda vardır. Kişisel Sağlık Verileri Yönetmeliği'nin amacı 1. maddesinde belirtilmiştir. Kişisel Sağlık Verileri Yönetmeliği, kişisel verilerin idarenin sunmuş olduğu sağlık hizmetlerinde korunması bakımından çok önemli düzenlemeler ihtiva etmektedir. Özellikle genel ilke ve esasların düzenlendiği 5. maddede 6698 sayılı Kanundaki genel ilkelere riayet edilmesi gerektiğinin belirtilmesi yanında bu alana özgü tedbirlerin alınması noktasında birçok esasa yer verilerek sağlık hizmetlerinde kişisel verilerin korunmasına ilişkin bir standart getirmektedir. Örneğin, Kişisel Sağlık Verileri Yönetmeliğinin 5. maddesinde “... (3) Hiç kimse, sağlık hizmeti sunumu için gerekli olan durumlar haricinde geçmiş sağlık verilerinin dökümünü sunmaya veya göstermeye zorlanamaz. ... (4) Sağlık hizmeti sunucuları tarafından; banko, gişe ve masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymalarını, görmelerini, öğrenmelerini veya ele geçirmelerini engelleyecek nitelikte gerekli fiziki, teknik ve idari tedbirler alınır. ... (5) Sağlık hizmeti sunucuları, tahlil ve tetkik sonuçları gibi hastaya ait kişisel sağlık verilerini içeren basılı materyal üzerinde gerekli kısmî kimliksizleştirme veya maskeleyme tedbirlerini uygular ve söz konusu materyalin yetkisiz kişilerin eline geçmesi hâlinde kime ait olduğunun tespit edilmesini zorlaştıracak diğer tedbirleri alır” gibi hükümlere yer verilmek suretiyle uygulamada kişisel verilerin korunması hakkının ihlaline sebebiyet verebilecek yaygın ve sorunlu uygulamaların önlenmesi amaçlanmıştır.

⁵⁷⁵ Veli Durmuş, “Kişisel Sağlık Verilerinin Korunmasında İdarenin Hukuki Sorumluluğu”, **Dokuz Eylül Üniversitesi Hemşirelik Fakültesi Elektronik Dergisi**, Cilt:14, Sayı: 1, 2021, s. 73.

⁵⁷⁶ Alçın, s. 396.

Günümüz gelişmeleri ışığında kişisel sağlık verilerinin artan oranda elektronik ortama taşındığı, pek çok sağlık kuruluşunda hastalara ait randevu, sağlık bilgisi geçmişlerinin, tahlil sonuçları, tanı ve uygulanan tedavilere ilişkin bilgilerin dijital ortamda yer aldığı görülmektedir⁵⁷⁷. İdare de sağlık hizmetlerinin sunumunda gelişen teknolojinin olanaklarından fazlasıyla yararlanmaktadır. Örneğin, Medula olarak bilinen sistem tüm sağlık verilerini tek bir sistemde birleştiren bir sistemdir. Yine MHRS, e-Nabız gibi programlar da kişisel sağlık verilerinin idare tarafından işlendiği programlardır⁵⁷⁸. Söz konusu verilerin özellikle elektronik ortam aracılığıyla işleniyor olması kamu hizmetinin verimliliği açısından birçok yararlı yöne sahip ise de veri güvenliğine ilişkin önemli sorunları da beraberinde getirmektedir. Çünkü kişilerin sağlık durumuna ilişkin bilgilerin yanlış kullanımı, ilgili kişinin sosyal alandan dışlanması ve sosyal ayrımcılığa uğraması, sağlık hizmeti almaktan kaçınması ve salgın hastalık riskinin doğması gibi ciddi sorunlara yol açabilecektir⁵⁷⁹. Bu bakımdan 6698 sayılı Kanun hükümlerinin yanında Kişisel Sağlık Verileri Yönetmeliği'nin 18-20. maddelerinde veri güvenliğine ilişkin uyulması gerekli olan esaslara yer verilmek suretiyle idarenin sağlık hizmetleri çerçevesinde işlediği kişisel verilerin etkin bir şekilde korunması amaçlanmıştır. Hekimlerin ve sağlık personelinin de kişisel verilerin korunmasına yönelik ilke ve esaslara uygun hareket etmesi bir hayli önemlidir. Elbette hekimler ve sağlık personelinin özellikle bilişim teknolojileri konusunda uzman olması mesleklerinin gerektirdiği bir durum değildir. Ancak hekimlere ve sağlık personeline konuya ilişkin bilgilendirilmeler yapılmalı ve bu konuda bir denetim mekanizması kurulması zaruret teşkil etmektedir. Son olarak sağlık verilerinin korunmasında birincil görevin kamu otoritelerinde olduğunu da ayrıca belirtmek gerekir. Zira kişisel sağlık verileri, nitelikleri gereği güvenlik de dahil olmak üzere kamu çıkarlarıyla doğrudan ilişkilidir⁵⁸⁰.

⁵⁷⁷ Küzeci, Kişisel Verilerin Korunması, s. 553.

⁵⁷⁸ Yılmaz, s. 68.

⁵⁷⁹ Küzeci, Kişisel Verilerin Korunması, s. 554.

⁵⁸⁰ Küzeci, Kişisel Verilerin Korunması, ss. 570, 571.

D. Kolluk Faaliyetleri Bakımından

Kolluk faaliyetleri bakımından kişisel verilerin korunması konusuna geçmeden önce kolluk faaliyetleri hakkında genel bir açıklamada bulunmak faydalı olacaktır. Bilindiği üzere, kamu düzenini koruyarak insanların güvenli bir ortamda ve huzur içerisinde yaşamasını sağlamak idarenin görevleri arasında yer almaktadır. İdarenin bu amaçla yürütmüş olduğu faaliyetler ise kolluk faaliyetleri olarak isimlendirilmektedir⁵⁸¹. Kolluk faaliyetleri, idari kolluk ve adli kolluk olarak ikiye ayrılmaktadır. İdari kolluk, kamu düzeninin sağlanması, korunması ve bozulduğunda geri getirilmesi amacıyla, bireylerin toplum içerisindeki davranışlarının düzenlenmesi, gözetilmesi ve aykırı eylem ve durumların gerekmesi halinde kuvvet kullanılmak suretiyle önlenmesi, engellenmesi ve kaldırılması faaliyeti olarak tanımlanabilir. İdari kolluk, bireylerle idarenin temel hak ve özgürlükler konusunda sık bir şekilde karşı karşıya geldiği ve çetin sorunlara sebebiyet veren bir kamusal faaliyet türüdür⁵⁸². Adli kolluk ise kamu düzenini bozan ve suç sayılan eylemlerin işlenmesi neticesinde failleri ve suça ilişkin delilleri araştırıp, bulmak ve bunları adli makamlara teslim etmekle görevli kolluktur⁵⁸³. Buradan hareketle, idari kolluğun önleyici, engelleyici; adli kolluğun ise bastırıcı olduğu ifade edilmelidir⁵⁸⁴. İdari kolluk ve adli kolluk her ne kadar işlevleri ve görevleri bakımından birbirinden ayrı kavramlar ise de organik açıdan ülkemizde birbirinden ayrılmamaktadırlar. Zira her iki kolluk faaliyeti de aynı kamu görevlileri tarafından yürütülmektedir⁵⁸⁵.

Kolluk faaliyetleri gerçekleştirilirken bireylerin kişisel verilerinin işlenmesi söz konusu olabilmektedir. Yasalarda suç sayılan eylemin gerçekleştirilmesinin ardından suç delillerinin elde edilmesi ve/veya suçluların yakalanması amacıyla kişisel verilerin işlenmesi gündeme gelebildiği gibi suç işlenmesinin önlenmesi veya istihbarat amacıyla da kişisel veriler işlenebilmektedir⁵⁸⁶. İlk durum adli kolluk faaliyetleri kapsamında kişisel verilerin işlenmesi iken, ikinci durum idari kolluk

⁵⁸¹ Küzeci, Kişisel Verilerin Korunması, s.494.

⁵⁸² Sancakdar ve diğerleri, ss. 677,678.

⁵⁸³ Halil Kalabalık, **İdare Hukuku Dersleri Cilt: II**, 5.Baskı, Seçkin Yayıncılık, Ankara, 2021, (İdare Hukuku), s. 271.

⁵⁸⁴ Sancakdar, s. 678.

⁵⁸⁵ Ramazan Yıldırım ve Serkan Çınarlı, **Türk İdare Hukuku Dersleri Cilt: II**, Astana Yayınları, Ankara, 2019, s. 167.

⁵⁸⁶ Küzeci, Kişisel Verilerin Korunması, s. 502.

faaliyetleri kapsamında kişisel verilerin işlenmesidir. Ceza Muhakemesi Kanunun 75. maddesinde yer verilen ve bir suça ilişkin delil elde etmek amacıyla uygulanan “*Şüpheli veya sanığın beden muayenesi ve vücudundan örnek alınması*”, 78. maddesindeki “*Moleküler genetik incelemeler*” ve 81. maddesindeki “*Fizik Kimliğinin Tespiti*” başlıklı hükümler, 135. maddesindeki “*İletişimin tespiti, dinlenmesi ve kayda alınması*” ve 140. maddesindeki “*Teknik araçlarla izleme*” başlıklı koruma tedbirleri, kişisel verilerin adli kolluk faaliyetleri çerçevesinde işlendiği durumlara verilebilecek örneklerdir. İdari kolluk faaliyetleri kapsamında kişisel verilerin işlendiği durumlara örnek teşkil edebilecek mevzuat düzenlemelerinden bir tanesi ise 2559 sayılı Polis Vazife ve Salahiyet Kanununun “*Parmak izi ve fotoğrafların kayda alınması*” başlıklı 5. maddesinde yer almaktadır. Söz konusu maddede hangi kişilerin parmak izi ve fotoğraflarının, hangi hallerde ve kimler tarafından kullanılabileceği belirtilmektedir. Bu maddenin düzenlemesinden hareketle kişisel verilerin polis tarafından işlenmesinin kanunla belirlenmiş sınırlarının olduğu ve bu sınırlar dahilinde polisin kişisel verileri işleyebileceği sonucuna ulaşılmaktadır⁵⁸⁷. Yine 2559 sayılı Polis Vazife ve Salahiyet Kanununun Ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun Ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanununun “*Yetkiler*” başlıklı 6. maddesi idari kolluk faaliyetleri çerçevesinde kişisel verilerin işlenmesine ilişkin diğer örnek düzenlemeler olarak sayılabilir. Burada 6698 sayılı Kanunun konuya ilişkin hükümlerine değinmekte yarar vardır. Zira 6698 sayılı Kanunun 28. maddesinin birinci fıkrasının ç bendinde “*(1) Bu Kanun hükümleri aşağıdaki hallerde uygulanmaz: ... 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*” hükmüne yer verilmiştir. Görüldüğü üzere 6698 sayılı Kanun, milli savunma, milli güvenlik, kamu güvenliği, kamu düzeni veya ekonomik güvenliği sağlamak amacıyla kanun tarafından görevli ve yetkili kılınmış kamu kurum kuruluşlarınca yürütülen önleyici, koruyucu ve istihbari faaliyetlerde 6698 sayılı Kanun hükümlerinin uygulanmayacağını düzenlemektedir. Bu bağlamda idari kolluğun suç oluşturabilecek

⁵⁸⁷ Turan Atlı, “Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi”, **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:2, Sayı:1, 2019, s. 12.

durumların önlenmesi amacıyla gerçekleştireceği faaliyetlerin istisna kapsamında olacağını söylemek yerinde olacaktır⁵⁸⁸. Ancak yukarıda örnekleri verildiği üzere idari kolluğun suç işlenmesinin önlenmesi amacıyla kişisel verileri işlemesine olanak tanıyan düzenlemelerin, bireylerin anayasal temel hak ve özgürlüklerinden bir tanesi olan kişisel verilerin korunması hakkını temin edebilecek şekilde düzenlenmesi hukuk devleti ilkesinin bir gereğidir. Ayrıca uygulama yönünden de gerek adli kolluk gerekse idari kolluk faaliyetlerinde kişisel verilerin işlenebilmesine olanak tanıyan düzenlemelerde yer verilen koşullara, usul ve esaslara uygun hareket edilmesi, görevli personelin bu konuda eğitime tabi tutulması ve faaliyetlerinin denetiminin sağlanması kişisel verilerin korunması hakkının güvence altına alınabilmesi bakımından son derece önem arz etmektedir.

Bu başlık altında son olarak yaygın bir kolluk faaliyeti örneği olan ve kamusal alanlarda güvenliğin sağlanması amacıyla görüntü kaydı alan “Mobil Elektronik Sistem Entegrasyonu” (MOBESE) uygulaması üzerinde durmak faydalı olacaktır. MOBESE sistemleri ile suç işlenmesinin önlenmesi, suç sonrasında ise şüphelilerin ve suç delillerinin tespiti kolayca mümkün olabilmektedir. Nitekim MOBESE uygulaması giderek artan suç sayısı karşısında gerek ülkemizde gerekse başka ülkelerde suçlulukla mücadelede mucize bir silah olarak algılanmakta ve kullanılmaktadır. Bu çerçevede kamera kullanımı, şehir meydanları, otogarlar, havalimanları, alışveriş merkezleri gibi çeşitli alanlarda yoğunlaşmıştır⁵⁸⁹. Ülkemizde kamusal alanların MOBESE ile izlenmesine ilişkin bir yasal düzenleme bulunmamaktadır⁵⁹⁰. Bu türdeki uygulamalar kişilerin temel hak ve özgürlüklerine müdahale oluşturabilmektedir. Söz konusu müdahalenin meşru bir müdahale olarak nitelendirilebilmesi için ise sınırlamanın yasayla ve ölçülü bir şekilde belirlenmesi, Anayasa’nın ilgili maddelerinde belirtilen sebeplere bağlı olması gerekmektedir⁵⁹¹. MOBESE uygulaması çerçevesinde yürütülen faaliyet bir önleyici tedbir niteliği taşımakta olduğundan amacı, kapsamı ve koşullarının yasada düzenlenmesi zorunluluk teşkil etmektedir. Özellikle, MOBESE uygulamasında çalışmamız bakımından önem arz eden husus, bu sistemlerde kişisel verilerin de izleniyor ve kayıt

⁵⁸⁸ Atlı, s. 11.

⁵⁸⁹ Veli Özer Özbek, **Polis Hukuku ve Ceza Muhakemesi Hukukunda Temel Haklara Müdahaleler**, Seçkin Yayıncılık, Ankara, 2021, ss. 255,256.

⁵⁹⁰ Küzeci, Kişisel Verilerin Korunması, s. 510; Özbek, s. 261.

⁵⁹¹ Küzeci, Kişisel Verilerin Korunması, s.511.

altına alınıyor oluşudur. Elbette günümüz koşullarında, suçlar ve terörizm ile mücadelede bu tür bir uygulamanın kullanılması gereklidir. Ancak hukuk devleti ilkesinin bir gereği olarak idarenin kişisel veri niteliğindeki görüntü ve sesleri hangi koşullarda izleyebileceği, kayıt altına alabileceği ve depolayabileceği yasal düzenlemeler ile belirlenmelidir⁵⁹².

E. Bilgi Edinme Hakkı Bakımından

Kamu yararını gerçekleştirme amacıyla faaliyetlerde bulunan idareye bu amacını gerçekleştirebilmesi için birtakım üstün ve ayrıcalıklı yetkiler tanınmıştır. İdare üstün ve ayrıcalıklı yetkileri sayesinde çoğu zaman muhatabın rızasına yahut herhangi bir katılımına ihtiyaç duymaksızın tek taraflı idari işlemler yapabilmektedir. Bilgi edinme hakkı demokratik hukuk devletlerinde bireylere, idarenin bu üstünlüğüne karşılık olarak, idari faaliyetlerin işleyişine ilişkin bilgi sahibi olma ve idare üzerinde denetim gücü oluşturabilmek amacıyla kabul edilmiş demokratik bir haktır⁵⁹³. Ülkemizde 24/10/2003 tarihli ve 25269 sayılı Resmî Gazete’de yayımlanan ve yayımlandığı tarihten itibaren altı ay sonra, 24/04/2004 tarihinde, yürürlüğe giren Bilgi Edinme Hakkı Kanunu ile demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak bireylerin bilgi edinme hakkını kullanmalarına ilişkin usul ve esaslar düzenlenmiştir⁵⁹⁴. Bu bağlamda Bilgi Edinme Hakkı Kanununun kişilere, idarenin elinde bulunan kişisel verileri hakkında bilgi sahibi olma hakkı verdiğini söylemek uygun olacaktır⁵⁹⁵. Ancak belirtmek gerekir ki, bilgi edinme hakkının da sınırları bulunmaktadır. Zira, bilgi edinme hakkından kaynaklanan yarar ile kamusal yarar ve diğer kişisel yararlar arasında çatışma doğurabilecek durumlar söz konusu olabilmektedir. Bu halde, bunlar arasında bir denge kurulması, üstün ve meşru bir yararın bulunması halinde bilgi edinme hakkının sınırlandırılması gerekmektedir⁵⁹⁶. Bilgi edinme hakkının sınırları ise Bilgi Edinme

⁵⁹² Özбек, ss. 256, 257.

⁵⁹³ Fatma Ebru Gündüz ve İsmail Yazıcıoğlu, “Bilgi Edinme Hakkı Çerçevesinde Kişisel Verilerin Korunması”, *Anayasa Yargısı*, Cilt:38, Sayı:1, 2021, s. 173.

⁵⁹⁴ Bilgi Edinme Hakkı Kanunu, m1.

⁵⁹⁵ Küzeci, *Kişisel Verilerin Korunması*, s. 580.

⁵⁹⁶ Ayhan Döner, “Bilgi Edinme Hakkının Sınırı Olarak Özel Hayatın Gizliliği ve Kişisel Veriler”, *Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi*, Cilt:26, Sayı:1, 2022, ss. 39,41.

Hakkı Kanunun dördüncü bölümünde yer alan 15 ila 28. maddeleri arasında belirtilmektedir.

Bilgi edinme hakkının irtibatlı olduğu haklardan bir tanesi de kişisel verilerin korunması hakkı olup bu iki hak arasında çift yönlü bir ilişki bulunmaktadır. Kişinin kendi kişisel verilerinin söz konusu olduğu bilgi edinme talebinde, bu iki hak birbirini tamamlar nitelikte iken; kişinin bilgi edinme hakkına dayanarak talep ettiği bilgi ve belgeler başka kişilere ait kişisel verileri içeriyor ise bu iki hak birbiri ile çatışma halinde olacaktır⁵⁹⁷. Kişisel verilerin korunması hakkı bakımından bilgi edinme hakkının sınırları ise çalışmamız bakımından önem taşıyan bir husustur. Kişisel verilerin korunması hakkı, doğrudan Bilgi Edinme Hakkı Kanununda yer verilen istisnalar arasında sayılmış olmasa da 21. maddede düzenlenen özel hayatın gizliliği kapsamında yer almaktadır⁵⁹⁸. Zira, özel hayat kavramının kişisel verileri de içine alan daha geniş bir kavram olması ve kişisel verilerin korunması hakkının birçok ülkede özel hayatının gizliliği başlığı altında düzenlenmesi bizi böyle bir sonuca götürmektedir⁵⁹⁹. Bilgi Edinme Hakkı Kanunun 21. maddesi uyarınca *“(1) Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, mesleki ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. (2) Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir”*. Ayrıca Bilgi Edinme Hakkı Kanununun 5. maddesinin birinci fıkrası uyarınca kurum ve kuruluşların kendisinden talep edilen bilgi veya belgeyi başvuranların yararlanmasına sunması, kişisel verilerin işlenmesi kavramı içerisinde kalan bir faaliyettir⁶⁰⁰. Yine bilindiği üzere 6698 sayılı kanunun 5. ve 6. maddelerinde kişisel verilerin ve özel nitelikli kişisel verilerin işlenme şartları düzenlenmektedir. Tüm bu hükümleri birlikte değerlendirmek, bilgi edinme hakkının, kişisel verilerin korunması hakkı yönüyle sınırlarının çizilmesine yardımcı olacaktır. 6698 sayılı Kanunun 6. maddesi ile Bilgi Edinme Hakkı Kanunun 21. maddesi birlikte değerlendirildiğinde, özel nitelikli kişisel

⁵⁹⁷ Gündüz ve Yazıcıoğlu, ss. 184,185.

⁵⁹⁸ Gündüz ve Yazıcıoğlu, ss.189.

⁵⁹⁹ Döner, ss. 45,46.

⁶⁰⁰ Gündüz ve Yazıcıoğlu, s. 192.

verilerin, kişinin rızası olmaksızın bilgi edinme hakkının konusunu oluşturamayacağı sonucuna ulaşılmaktadır. Özel nitelikli olmayan kişisel veriler bakımından durum değerlendirildiğinde ise Bilgi Edinme Hakkı Kanununun 5. maddesi, 6698 sayılı Kanunun 5. maddesinde yer verilen ve kişinin rızası olmaksızın kişisel verilerin açıklanmasına olanak tanıyan kanuni dayanak olarak anlaşılabilecektir. Ayrıca Bilgi Edinme Hakkı Kanununda yer verilen ve özel hayatın gizliliği istisnası kapsamında olmayan kişisel verilerin de bilgi edinme hakkının kapsamında kalacağı ifade edilebilir. Ancak bu denli geniş bir yorum kimi zaman kişisel verilerin korunması hakkına ölçüsüz bir müdahale oluşturabilecektir. Buna karşılık sadece kişisel verilerin korunması odaklı bir yaklaşımın da kişisel verilerin içeriğinin genişliği düşünüldüğünde bilgi edinme hakkını işlevsiz hale getirebilmesi söz konusudur⁶⁰¹.

Bilgi edinme hakkı ile kişisel verilerin korunması hakkı arasındaki ilişki, her iki alanın da gerek insan hakları gerekse demokratik yönetim açısından önemi göz önünde bulundurularak kurgulanmalıdır⁶⁰². Zira demokratik hukuk devleti, bir yandan bilgi edinme hakkını tanıırken bir yandan da özel hayatın gizliliğini güvence altına alacak gerekli kanuni ve idari tedbirler almak zorundadır⁶⁰³. Bu noktada benimsenmesi gereken yaklaşım, Anayasa'nın 13.maddesini esas alarak her iki hakka getirilen sınırlamaların ölçülü olması ve hakkın özüne dokunulmamasıdır. Ayrıca iki hak arasında dengenin sağlanması gerekmekte olup bilgi edinme hakkı kullanılırken kişisel verilerin korunması hakkı ihlal edilmemelidir⁶⁰⁴. Her kurum ve kuruluşun talepte bulunan kişilere verecekleri bilgi ve belgelerde söz konusu hassas dengeyi sağlaması güçtür. Bu sebeple Bilgi Edinme Değerlendirme Kurulu'na ve yargı mercilerine önemli görevler düşmektedir⁶⁰⁵. Nitekim örneğin, Bilgi Edinme Değerlendirme Kurulu 11.10.2004 tarihli ve 2004/128 sayılı kararında, başvuruçuların kendileri hakkında sicil ve soruşturma raporlarına ve özlük dosyalarına ulaşmak yönündeki talepleriyle ilgili olarak varsa üçüncü kişiye ait bilgilerin çıkartılmasından sonra talep edilen belgelerin onaylı suretlerinin kendilerine verilebileceğini belirtmiştir⁶⁰⁶.

⁶⁰¹ Gündüz ve Yazıcıoğlu, ss. 191-194.

⁶⁰² Küzeci, Kişisel Verilerin Korunması, s. 582.

⁶⁰³ Döner, s. 49.

⁶⁰⁴ Gündüz ve Yazıcıoğlu, ss.193, 194.

⁶⁰⁵ Döner, s. 52.

⁶⁰⁶ Gündüz ve Yazıcıoğlu, ss. 194,195.

SONUÇ

Oldukça eski tarihlerden bu yana kişilere ilişkin veriler gerek kamu gerekse özel sektör bakımından çok kıymetli olmuştur. Kamuda kişisel veriler, kamu hizmetinin etkili bir şekilde sunulması, kamu düzeni ve güvenliğinin sağlanması gibi sebeplerle işlenmekteyken; özel sektörde ise verimlilik ve karlılığın artırılması gibi amaçlarla kullanılmaktadır. Özellikle bilişim teknolojilerinde devrimsel nitelikte gelişmeler yaşanması ile birlikte kişisel verilere erişim, bunların aktarılması ve depolanması bir hayli kolay hale gelmiş ve böylesine kolaylaşan veri işleme faaliyetleri karşısında bireyin temel hak ve özgürlüklerinin güvence altına alınması gerek uluslararası gerekse ulusal alanda üzerinde sık durulan bir konu halini almaya başlamıştır.

Kişisel verilerin günümüzde taşıdığı önem, onun bağımsız bir temel hak olarak değerlendirilmesine sebep olmuştur. Oysa kişisel verilerin korunması hakkı, uzun yıllar özel hayatın gizliliğinin kapsamında kabul edilen bir hak idi. Ancak kişisel verilerin korunması hakkını özel hayat ve mahremiyet kavramlarına indirgemek hakkın özüne zarar verebilecek niteliktedir. Çünkü bireylerin kişisel verileri yalnızca özel hayatlarında değil kamusal yaşantılarında da büyük önem arz etmektedir. Kişisel verilerin ve bu verilerin korunmasının, bireylerin kişiliklerini geliştirme, özgürce karar verme ve kamusal yaşama katılım gibi birçok konuda kritik rolü bulunmaktadır. Kişisel verilerin korunması hakkının, günümüz gelişmeleri de dikkate alındığında temel insan hakkı yaklaşımı içerisinde genel kişilik hakkının özel bir görünümü olduğunu ve bağımsız bir hak olarak değerlendirilmesi gerektiğini düşünüyoruz.

Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu çerçevede gerçek kişiye ilişkin bilgi, doğrudan kişi ile bağlantı kurulması suretiyle o kişinin diğerlerinden ayırt edilmesini sağlıyor veya dolaylı olarak o kişi hakkındaki başka verilerle birlikte ilişkilendirilmek suretiyle o kişiyi diğerlerinden ayırt edilebilir kılıyor ise kişisel veri olarak nitelendirilebilecektir. Uluslararası düzenlemelerde “*kişisel veri*” kavramına getirilen tanımların büyük ölçüde paralellik arz ettiği görülmektedir. Aynı paralellik kişisel verilerin işlenmesine yönelik getirilen tanımlarda da mevcuttur. Zira kişisel verilerin işlenmesi, bu verilerin elde edilmesi, depolanması, değiştirilmesi, açıklanması, aktarılması, sınıflandırılması,

kullanılmasının engellenmesi, silinmesi gibi çok geniş bir faaliyet türünü kapsar niteliktedir. Bu sebeple kişisel veriler üzerinde gerçekleştirilen hemen her türlü eylemin kişisel verilerin işlenmesi olarak değerlendirilebileceğini de ifade etmek gerekir. Ülkemizde 6698 sayılı Kişisel Verilerin Korunması Kanunu bu alandaki temel yasal düzenlemedir. Kişisel verilerin işlenmesi sürecinde temel hak ve özgürlüklerin güvence altında tutulmasını sağlamak amacıyla hazırlanan Kanun kişisel verilerin ve özel nitelikli kişisel verilerin hangi koşullarla işlenebileceğine dair 5. ve 6. maddelerinde detaylı düzenlemeler içermektedir. Söz konusu Kanunun hükümleri, kişisel verileri işlenen gerçek kişiler hakkında uygulama alanı bulduğu gibi madalyonun diğer yüzü olan ve kişisel verileri tamamen veya kısmen otomatik olan yahut bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek veya tüzel kişiler hakkında da uygulanmaktadır. Ayrıca Kanun özel sektör üzerinde bağlayıcılığa sahip olduğu gibi kamu kurum ve kuruluşları üzerinde de bağlayıcılığa sahiptir. Hal böyle iken, kişisel verileri kamu düzeni, kamu güvenliği, kamu hizmeti ve suçluluğun önlenmesini sağlamak gibi amaçlarla sıklıkla işleyen idarenin de veri sorumlusu sıfatı bulunmakta ve bu alanda mer'î yasal düzenlemelere uygun hareket etmesi gerekmektedir. Özellikle idarenin faaliyetlerinde, 6698 sayılı Kişisel Verilerin Korunması Kanununa istisna teşkil eden durumlar da dahil olmak üzere, Anayasal bir hak olan kişisel verilerin korunması hakkını güvence altında tutma eğiliminde olması gerekir. Nitekim böyle bir yaklaşım, demokratik bir hukuk devletinden beklenen yaklaşımdır. İdare kişisel verileri işlerken özellikle kişisel verilerin korunması hukukunda yer alan amaçla bağlılık ilkesine riayet etmelidir. Bu ilke kişisel verilerin belirli ve meşru amaçlar doğrultusunda, gerektiği miktarda ve yerde kullanılmak üzere işlenmesini ve amaç için gerekli olan süreden daha uzun bir süre tutulmamasını gerektirmektedir. Son olarak, kamu kurum ve kuruluşlarında çalışan personellerin idare tarafından kişisel verilerin korunması alanındaki güncel gelişmeleri takip etmek suretiyle eğitimlere tabi tutulması ve denetimlerin sağlanması idari faaliyetlerde kişisel verilerin korunması hakkının güvence altına alınması amacına büyük katkı sağlayacaktır.

KAYNAKÇA

KİTAPLAR VE MAKALELER

Akad, Mehmet, Bihterin Vural Dinçkol ve Nihat Bulut. **Genel Kamu Hukuku**, 10.baskı, Der Yayınları, İstanbul, 2014.

Akçakaya, Murat. “E-Devlet Anlayışı ve Türk Kamu Yönetiminde E-Devlet Uygulamaları”, **Yüzüncü Yıl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Sayı:3, 2017, ss. 8-31.

Akgül, Aydın. “Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı”, **TBB Dergisi**, Sayı: 116, 2016, (Unutulma Hakkı), ss. 11-38.

Akgül, Aydın. **Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi**, (Yayımlanmamış Doktora Tezi), Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli, 2013, www.tez.yok.gov.tr/UlusalTezMerkezi/, (21.08.2022), (Verilerin Korunması).

Akkurt, Sinan Sami. Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış, **Kişisel Verileri Koruma Dergisi**, Cilt: 2, Sayı: 1, 2020, ss. 20-32.

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

Alçın, Ayşe Aslı. “Türk Hukukunda Kişisel Sağlık Verileri ve İdarenin Kişisel Sağlık Verilerini Koruma Yükümlülüğü”, **Türkiye Adalet Akademisi Dergisi**, Sayı: 51, 2022, ss. 365-410.

Aşıkoğlu, Şehriban İpek. “Veri Sorumlularının Aydınlatma Yükümlülüğü-Avrupa Birliği ve Türk Hukukunda”, **Kişisel Verileri Koruma Dergisi**, Cilt: 1, Sayı:2, 2019, ss. 41-65.

Atlı, Turan. “Kişisel Verilerin Önleyici, Koruyucu ve İstihbari Faaliyetler Amacıyla İşlenmesi”, **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:2, Sayı:1, 2019, ss. 4-22.

Aydoğdu, Yasin. “Kamu idaresinde Kişisel Verilerin Korunması”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 29, Sayı: 1, 2021, ss. 263,293.

Badur, Emel ve Nesibe Kurt Konca. “Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini ve Görevli Mahkeme”, **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 13, Sayı: 2, 2022, ss. 476-490.

Baskın, Onur. **Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, Ankara, 2021.

Başar, Cemal. **Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması**, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilimdalı Kamu Hukuku Programı Yayınlanmış Doktora Tezi, 2019, www.tez.yok.gov.tr, (10.06.2022).

Bük, Alaattin. **Bilişim Alanında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, Ankara, 2018.

Büyükkay, Yusuf. “Hekimin Sır Saklama Yükümlülüğü”, **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:7, Sayı:1-2, 2004, ss. 383-396.

Cankurt, Ayça. **Kişisel Verilerin Korunmasında İdarenin Etkisi**, (Yayımlanmamış Yüksek Lisans Tezi), Karabük Üniversitesi Lisansüstü Eğitim Enstitüsü, Karabük, 2021, <https://tez.yok.gov.tr/UlusalTezMerkezi/>, (15.12.2022).

Çekin, Mesut Serdar. **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu**, On İki Levha Yayıncılık, İstanbul, 2018.

Çelikel, Serdar. **Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri**, Seçkin Yayıncılık, Ankara, 2022.

Çimen Bulut, İpek. “Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları”, **Anadolu Üniversitesi Sosyal Bilimler Dergisi**, Cilt:20, Sayı:2, 2020, ss. 127-142.

Doğan, Bayram. **Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı**, Adalet Yayınevi, Ankara, 2022.

Döner, Ayhan. “Bilgi Edinme Hakkının Sınırı Olarak Özel Hayatın Gizliliği ve Kişisel Veriler”, **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 26, Sayı:1, 2022, ss. 23-60.

Duman, Berat. **Anayasa Hukukunda Kişisel Verilerin Korunması**, (Yayınlanmamış Doktora Tezi), Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2020, <https://tez.yok.gov.tr/UlusalTezMerkezi/>, (15.12.2022).

Durmuş, Veli. “Kişisel Sağlık Verilerinin Korunmasında İdarenin Hukuki Sorumluluğu”, **Dokuz Eylül Üniversitesi Hemşirelik Fakültesi Elektronik Dergisi**, Cilt:14, Sayı: 1, 2021, ss. 67-76.

Dölger, Murat Volkan. “Avrupa Birlięi Genel Veri Koruma Tüzüğü Baęlamında Kişisel Verilerin Korunması”, **Yaşar Hukuk Dergisi**, Cilt:1, Sayı:2, 2019, (Genel Veri Koruma Tüzüğü Baęlamında), ss. 71-174.

Dölger, Murat Volkan. İnsan Hakları ve Temel Hak ve Özgürlükler Baęlamında Kişisel Verilerin Korunması, **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:5, Sayı:1, 2018, (İnsan Hakları Baęlamında), ss. 71-144.

Dölger, Murat Volkan. **Kişisel Verilerin Korunması Hukuku**, Hukuku Akademisi Yayıncılık, İstanbul, 2019, (Kişisel Veriler Hukuku).

Eraslan, Sevgi. “Türk Hukukunda Kişisel Verilerin Yurt Dışına Aktarılması Sorunu: Açık Rıza Kapsamında Bir Deęerlendirme”, **Kırıkkale Hukuk Mecmuası**, Cilt:1, Sayı:1, 2021, s. 82-115.

Erdoğan, İhsan ve A. Dilşad Keskin, **Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku**, Gazi Kitabevi, Ankara, 2019.

Göçmen Uyarer, Sinem. **Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, 2. Baskı, Seçkin Yayıncılık, Ankara, 2020.

Gündüz, Fatma Ebru ve İsmail Yazıcıoęlu. “Bilgi Edinme Hakkı Çerçevesinde Kişisel Verilerin Korunması”, **Anayasa Yargısı**, Cilt:38, Sayı:1, 2021, ss. 171-204.

Güneş, Ahmet M.. “Bir Uluslararası Hukuk Süjesi Olarak Avrupa Birlięi”, **Türkiye Adalet Akademisi Dergisi**, Yıl: 5, Sayı:19, Ekim 2014, ss. 127-158.

Gürpınar, Damla. “Kişisel Verilerin Korunamamasından Doęan Hukuki Sorumluluk”, **D.E.Ü Hukuk Fakültesi Dergisi**, Prof. Dr. Şeref Ertaş’a Armaęan, Cilt:19, Özel-Sayı, 2017, ss. 679-694.

Gürsel, Esin ve Fatih Düğmeci. “Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu’na İlişkin Bir Değerlendirme”, **R&S- Research Studies Anatolia Journal**, Cilt:1, Sayı:2, 2018, ss. 318-329.

İbrahim Korkmaz, “Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme”, **Türkiye Barolar Birliği Dergisi**, Cilt: Mayıs-Haziran 2016, Sayı:124, (Kanun Hakkında Değerlendirme), ss. 81,152.

İlhan, Neslihan Emre. “Kişisel Verilerin Korunması Kanunu Kapsamında İşverenin Özlük Dosyası Oluşturma Yükümlülüğü”, **İstanbul Barosu Dergisi**, Cilt:94, Sayı:1, 2020, ss.68-86.

İnan, Salih. “Kişisel Verilerin Korunması Kapsamında İhdas Edilen Yaptırım Kararlarına Karşı Yargısal Başvuru Yolları: Karşılaştırmalı Bir İnceleme”, **Kişisel Verileri Koruma Dergisi**, Cilt: 3, Sayı: 2, 2021, ss. 34-49.

Kalabalık, Halil. **İdare Hukuku Dersleri Cilt: II**, 5.Baskı, Seçkin Yayıncılık, Ankara, 2021, (İdare Hukuku).

Kalabalık, Halil. **İnsan Hakları Hukuku**, 5.Baskı, Seçkin Yayıncılık, Ankara, 2017.

Kayıhan, Şaban. **Kişiler Hukuku**, Seçkin Yayıncılık, Ankara, 2022.

Kendir Tunalı, Tuba. “Veri Sorumlularının Yükümlülükleri”, **Kişisel Verilerin Korunması Alanında Yeni Gelişmeler Sempozyumu**, Anadolu Üniversitesi Hukuk Fakültesi-İktisadi ve İdari Bilimler Fakültesi-Kişisel Verileri Koruma Kurumu-Eskişehir Sanayi Odası, 05.12.2019, Adalet Yayınevi, Ankara, 2019, ss. 33-46.

Korkmaz, İbrahim. **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayıncılık, Ankara, 2019, (Kişisel Veriler).

Küzeci, Elif. “Veri Sorumlusunun Yükümlülükleri”, **II. Kişisel Verilerin Korunması Sempozyumu**, İstanbul, 07.02.2019, www.academia.edu, (18.07.2023), (Veri Sorumlusunun Yükümlülükleri).

Küzeci, Elif. İstatistiki Birimler ve Bilgilerin Geleceğini Belirleme Hakkı, **İnsan Hakları Yıllığı**, Cilt:32, 2014, (Bilgilerin Geleceğini Belirleme), ss. 53-75.

Küzeci, Elif. **Kişisel Verilerin Korunması**, 4.Baskı, On İki Levha Yayıncılık, İstanbul, 2021, (Kişisel Verilerin Korunması).

Oğuz, Sefer. “Kişisel Verilerin Korunması Hukukunun Genel İlkeleri”, **Bilgi Ekonomisi ve Yönetimi Dergisi**, Cilt:13, Sayı:2, 2018, ss. 121-138.

Orhan, Uğur. “Kişisel Verilerin Korunmasına İlişkin Türk Ceza Hukuku Düzenlemeleri Üzerine Değerlendirmeler”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 70, Sayı: 4, 2021, ss. 1359-1384.

Öksüzöğlü, Hilal Tuğba. “6698 Sayılı Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Hukukunda Kişisel Verilerin Silinmesi ve Düzeltilmesi”, **Bilişim Hukuku Dergisi**, Cilt:1, Sayı:2, 2019, ss. 185-242.

Özbek, Veli Özer. **Polis Hukuku ve Ceza Muhakemesi Hukukunda Temel Haklara Müdahaleler**, Seçkin Yayıncılık, Ankara, 2021.

Özdemir, Hayrunnisa. **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin Yayıncılık, Ankara, 2009.

Özdemir, Murat, Metin Yılmaz ve Hakan Kaya. “Kişisel Sağlık Verilerinin 6698 Sayılı Kanun Çerçevesinde Korunması”, **19 Mayıs Sosyal Bilimler Dergisi**, Cilt:3, Sayı:1, 2022, ss. 85-96.

Öztürk, Bahri, Elif Altınok Çalışan ve Serkan Seyhan. **Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı**, 2.Baskı, Seçkin Yayıncılık, Ankara, 2022.

Sancakdar, Oğuz, Eser Us, Mine Kasapoğlu Turhan ve Lale Burcu Önüt. **İdare Hukuku Teorik Çalışma Kitabı**, Seçkin Yayıncılık, 5. Baskı, Ankara, 2015.

Saygı, Samet. “6698 Sayılı Kanun’un Sistematiğinde Yargısal Başvuru Yolları”, **Kişisel Verileri Koruma Dergisi**, Cilt:2, Sayı:2, 2020, ss. 30-61.

Serozan, Rona. “Kişilik Hakkının Korunmasıyla İlgili Bazı Düşünceler”, **İstanbul Üniversitesi Mukayeseli Hukuk Araştırmaları Dergisi**, Cilt:11, Sayı:14, 1977, ss. 93-112

Sert, Şeyma. **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, 2.Baskı, Seçkin Yayıncılık, Ankara, 2023.

Soysal, Tamer. Unutulma Hakkının Avrupa Birliği’nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi, **Uyuşmazlık Mahkemesi Dergisi**, Sayı: 13, 2019, ss. 339-422.

Şimşek, Oğuz. **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Basım, İstanbul, 2008.

Taştan, Furkan Güven. **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, (Yayımlanmış Yüksek Lisans Tezi), www.tez.yok.gov.tr, (11.03.2023).

Tepe, Esra. **Özel Hukuk Açısından Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, Ankara, 2021.

Toprak Karaman, Zerrin. “E-Devletin Güvenlik Bağlantılı Sorumlulukları ve E-Vatandaşın Hakları”, **Akademik İzdüşüm Dergisi**, Cilt:5, Sayı:1, 2020, ss. 1-20.

Uyar, Lema. **Birleşmiş Milletler’de İnsan Hakları Yorumları**, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2006.

Ünsal Özden, Sevgi, Mert Karamustafaoğlu ve İdil Uz. “Kişisel Veri Aktarımı ve Bankacılık Kanunu Madde 73 Değişikliği”, **Kişisel Verileri Koruma Dergisi**, Cilt:3, Sayı:1, 2021, ss. 17-40.

Vuraloğlu, Mehmet Oğuz. “Kişisel Verilerin İşlenmesi Suretiyle Kişilik Hakkı İhlalinde Kazancın Devri Talebi”, **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:15, Sayı:1, 2018, ss. 181-203.

Yıldırım, Ramazan ve Serkan Çınarlı. **Türk İdare Hukuku Dersleri Cilt: I**, Astana Yayınları, Ankara, 2018.

Yıldırım, Ramazan ve Serkan Çınarlı. **Türk İdare Hukuku Dersleri Cilt: II**, Astana Yayınları, Ankara, 2019.

Yılmaz, Dilşat. “Yeni Bir İdari Faaliyet Alanı: “VERBİS””, **Yıldırım Beyazıt Hukuk Dergisi**, Sayı: 2, 2020, ss. 83-118.

Yılmaz, Sabire Sanem. **Tıp Alanında Kişisel Verilerin Korunması**, Seçkin Yayıncılık, 6.Baskı, Ankara, 2022.

Yücedağ, Nafiye. “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: 75, Sayı:2, 2017, ss. 765-789