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

ANAYASA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

Berat DUMAN

DOKTORA TEZİ

Danışman

Prof. Dr. Faruk BİLİR

Konya - 2020

T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

Öğrencinin		
	Adı Soyadı	Berat DUMAN
	Numarası	134134001006
	Ana Bilim / Bilim Dalı	Kamu Hukuku Ana Bilim Dalı Kamu Hukuku Bilim Dalı
	Programı	Tezli Yüksek Lisans ☐ Doktora ■
	Tezin Adı	ANAYASA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

ÖZET

Çalışmamızda Türk hukukunda ve Türk anayasa hukukunda önemi son yıllarda gittikçe artan "Kişisel Verilerin Korunması Hakkı"nı anayasal temel bir hak olarak ele alacağız.

Kişilerin, kişisel verilerinin korunması, temelde, bireylerin hak ve özgürlüklerinin korunmasının temelini, gövdesini oluşturur. Zira bireylere ilişkin bilgiler -en basitinden en detaylısına kadar- uluslararası metinler, anayasa ve yasalarda yapılan düzenlemeler neticesinde kişilere tanınan hakların kullanılması ile iç içe geçmiş durumdadır. Dolayısıyla modern demokrasiler ve çağdaş hukuk devletlerinde, kamu ve özel hukuk tüzel kişileri ile gerçek kişilerin, bu hakkın korunmasında veya başka bir deyişle ihlal edilmesinden kaçınılmasında, bazı yükümlülüklere tabi olduğu açıktır. Buradan hareketle, kamusal ve özel organların ve kişilerin, bütün işlem ve fiillerini hukuk düzeninin kendisine tanıdığı kurallara uygun bir şekilde yürütmek mecburiyeti vardır. Bunun sonucu olarak, “Kişisel Verilerin Korunması Hakkı” nın her hukuk devletinin anayasasında temel hak olarak tanımlanması temayülü gün geçtikçe artan bir şekilde, dünya hukuk düzenini oluşturan hukuk sistemlerinde kendisini göstermektedir.

Bu bağlamda çalışmamızda Türk hukukunda ilk defa 2010 Anayasa değişikliği ile anayasal bir hak olarak bireylere tanınan "Kişisel Verilerin Korunması Hakkı"nın anayasal çerçevede korunmasının temellerini incelemeye çalışacağız. Anayasa temelinde söz konusu hakkı incelemenin yanında, hakkın anlaşılmasında önemli bir yer tutan uluslararası belgeleri, bu hakka ilişkin terminolojiye ve bunlara ek olarak gerek ceza gerekse hukuk alanında temel koruma alanları ile özellikle "Kişisel Verileri Koruma Kanunu"na değineceğiz.

Çalışmamız dört ana bölümden oluşmaktadır. İlk bölümde genel olarak kişisel verilerin korunması ile ne anlatılmak istendiğine, tarihçesine ve uluslararası temel metinlerde yer alma şekline değineceğiz. İkinci bölümde, kişisel verilerin korunması hukukunda bilinmesi gereken temel terimler ile ilkelere göz atacağız. Üçüncü bölümde, bu hakkın Türk anayasa hukukundaki temellerine ayrıntılı bir şekilde bakmaya çalışacağız. Son bölümde ise, anayasal bir hak olan "Kişisel Verilerin Korunması" hakkının kanun düzeyinde ceza ve hukuk alanında korunması ile özel bir kanun olan Kişisel Verileri Koruma Kanunu'nun sağladığı korumaya değineceğiz. Bunlarla beraber, esas olarak, kişisel verilerin korunması hakkını anayasal temel bir hak olarak bu çalışmamızda ortaya koymaya çalışacağız.

T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

Öğrencinin		
	Adı Soyadı	Berat DUMAN
	Numarası	134134001006
	Ana Bilim / Bilim Dalı	Kamu Hukuku Ana Bilim Dalı Kamu Hukuku Bilim Dalı
	Programı	Tezli Yüksek Lisans ☐ Doktora ■
	Tezin Adı	PERSONAL DATA PROTECTION in CONSTITUTIONAL LAW

ABSTRACT

In our study, we are going to consider the right to Protection of Personal Data as a constitutional fundamental right, which has gained importance in Turkish law and Turkish constitutional law in recent years.

The protection of personal data constitutes the basis and body of the protection of the rights and freedoms of individuals. Because information about individuals is intertwined with the exercise of the rights granted to individuals as a result of the arrangements made in international texts, constitution and laws - from the simplest to the most detailed. Thus, in modern democracies and contemporary states of law, it is clear that public and private legal entities and natural persons are subject to certain obligations in the protection of this right or in other words in the avoidance of this violation. From this point of view, public and private bodies and individuals are obliged to carry out all their transactions and acts in accordance with the rules recognized by the legal order. As a result, the tendency to define the Right to Protection of Personal Data as the fundamental right in the constitution is gradually increasing in the legal systems constituting the world legal order.

In this respect, we are going to try to examine the basics of the protection of the Hakkı Right to Protection of Personal Data tanınan granted to individuals as a constitutional right for the first time in 2010 with the 2010 constitutional amendment in Turkish law. Although we examine the right on the basis of the Constitution, we are going to tuch upon the international documents, which have an important place in the understanding of the right, the terminology related to this right, as well as the main areas of protection in both criminal and legal fields, and in particular the Personal Data Protection Law

Our study consists of four main sections. In the first part, personal data in general; protection, what is meant to be told, the history and the way we will refer to the main international texts. In the second part, we will look at the basic terms and principles that should be known in the law on the protection of personal data. In the third part, we will try to look at the foundations of this right in Turkish Constitutional Law in detail. In the last section, we will refer to the protection of the constitutional right of Personal Data Protection in the field of punishment and law at the law level and the protection provided by the Law on the Protection of Personal Data. In addition to this, we will try to put forward the right to protection of personal data as a constitutional, fundamental right in this study.

İÇİNDEKİLER

İÇİNDEKİLER..... Vİ

ÖZET..... İİ

ABSTRACT V

KISALTMALAR..... XİV

GİRİŞ..... XVİİİ

BİRİNCİ BÖLÜM

GENEL OLARAK KİŞİSEL VERİLERİN KORUNMASI HUKUKU, TARİHÇESİ, ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL METİNLER

1.1. GENEL OLARAK KİŞİSEL VERİLERİN KORUNMASI HUKUKU 1

1.2. TARİHÇE 6

1.3. ULUSLARASI METİNLER 17

1.3.1. OECD 17

1.3.2. BİRLEŞMİŞ MİLLETLER 19

1.3.3. AVRUPA KONSEYİ 21

1.3.3.1. Genel Olarak 21

1.3.3.2.108 SAYILI SÖZLEŞME 23

1.3.3.2.1. Tarihçesi 23

1.3.3.2.2.Sözleşmenin Amacı ve Kapsamı 25

1.3.3.2.3. Sözleşmede Belirtilen İlkeler 27

1.3.3.2.4.Sınır Ötesi Veri Akışı 29

1.3.3.3. AİHS 31

1.3.4. AVRUPA BİRLİĞİ 32

1.3.4.1. 95/46/AT Yönergesi 34

1.3.4.2. AB Temel Haklar Şartı 36

1.3.4.3. AB Genel Veri Koruma Tüzüğü (GDPR) 37

1.3.4.4- Elektronik Veriyi Korumaya İlişkin 2002/58/Ec Sayılı Avrupa Birliği Direktifi *44*
1.3.4.5- Avrupa Birliği Vatandaşlık Hakkı Direktifi (2009/136/Ec Sayılı Direktif) *44*
1.3.4.6. Europol Antlaşması ve Kişisel Verilerin Korunması *44*
1.3.4.7. Eurojust *45*
1.3.4.8. Schengen Antlaşması ve Kişisel Verilerin Korunması *46*

İKİNCİ BÖLÜM

KİŞİSEL VERİLERE İLİŞKİN TERMİNOLOJİ VE VERİLERİN KORUNMASINDA TEMEL İLKELER

2.1. TERMİNOLOJİ 47
2.1.1.KİŞİSEL VERİ 47
2.1.1.1. Kişisel Verinin Unsurları *52*
2.1.1.1.1.Bilgi 53
2.1.1.1.2.Kimliği Belirli veya Belirlenmesi Mümkün Kişi 54
2.1.1.1.3.Bilginin Kimliği Belirli veya Belirlenebilir Kişiye İlişkin Olması 55
2.1.2. KİŞİSEL VERİ TÜRLERİ 60
2.1.2.1. Hassas -Özel Nitelikli- Kişisel Veri *60*
2.1.2.1.1.Genel Olarak 60
2.1.2.1.2. Hassas Kişisel Veri Türleri 66
2.1.2.2. Anonim -Genel Nitelikli- Kişisel Veriler *74*
2.1.3. KİŞİSEL VERİLERİN HUKUKİ NİTELİĞİ 75
2.1.3.1. İnsan Onuru, Bireysel Özerklik Kavramı ve Verilerin Geleceğini Belirleme Hakkı Görüşü *75*
2.1.3.2. Özel Hayatın Gizliliği Hakkı Görüşü *77*
2.1.3.2.1. Ortak Alan 81
2.1.3.2.2. Özel Alan 82
2.1.3.2.3. Gizli Alan (Giz Alanı) 83

2.1.3.3. Mülkiyet Hakkı Görüşü *84*
2.1.3.4. Fikri Mülkiyet Hakkı Görüşü *86*
2.1.3.5. Görüşler Hakkında Değerlendirme *89*
2.1.4. İLGİLİ KİŞİ (VERİ ÖZNESİ, VERİ SAHİBİ, VERİNİN KONUSU) 92
2.1.5. RIZA 95
2.1.6. VERİ İŞLEYEN 99
2.1.7. VERİ SORUMLUSU 100
2.1.8. KİŞİSEL VERİLERİN İŞLENMESİ 102
2.1.8.1. Kesin İşlem Yasağı *105*
2.1.8.2. İşlem Yasağının İstisnaları *106*
2.1.8.2.1. İlgilinin Rızası 106
2.1.8.2.2. Hayati Çıkarların Korunması 107
2.1.8.2.3. Kamuya Yararlı Özel Hukuk Kişileri Tarafından İşlenme .108
2.1.8.2.4. İş Hukuku Kaynaklı Yükümlülüklere Uyulması 109
2.1.8.2.5.Verinin İlgili Kişi Tarafından Kamuya Açıklanması 110
2.1.8.2.6. Yargılama Sebebiyle İşlenme 111
2.1.8.2.7. Cezalara Yönelik İşlenme 112
2.1.8.2.8. Sağlık Gerekleri 113
2.1.8.2.9. Ek İstisnalar 114
2.2. VERİLERİN KORUNMASINDA TEMEL İLKELER 116
2.2.1. ESASA İLİŞKİN TEMEL İLKELER 116
2.2.1.1. Kişisel Verilerin Hukuka ve Dürüstlük Kuralına Uygun İşlenmesi *116*
2.2.1.2. İlgilinin Rızasının Alınması İlkesi *118*
2.2.1.3. Belirli Bir Amacın Bulunması *120*
2.2.1.4. Amaca Bağlılık İlkesi *121*
2.2.1.5. Orantılılık ve Gereklilik İlkesi *124*
2.2.1.6. Verilerin Doğruluğu ve Güncelliği İlkesi *126*
2.2.2. USULE İLİŞKİN İLKELER 128
2.2.2.1. Veri Güvenliği İlkesi *128*
2.2.1.2. İlgili Kişilerin Bilgilendirilmesi İlkesi *129*

2.2.1.3. Bilgi Edinme, Kişisel Verinin Düzeltilmesi ve Kaldırılması, Kişisel Veriyi Sildirme, Engelleme ve İtiraz Haklarının Garanti Edilmesi İlkesi 131
2.2.1.3. 1. Bilgi edinme hakkı 131
2.2.1.3. 2.Düzeltme, sildirme, engelleme ve itiraz etme hakkı 134
2.2.1.4. İşlem Aleniyeti 135
2.2.1.5. İşlemin Gizliliği ve Güvenliği.....138
2.2.1.6.Ön Denetim.....139
2.2.1.7. Zararın Giderilmesi İlkesi 140

ÜÇÜNCÜ BÖLÜM

ANAYASA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASININ TEMELLERİ

3.1. BİREYİN KİŞİSEL VERİLERİNİN KORUNMASI HAKKI.....143

3.1.1. GENEL OLARAK.....143
3.1.2. T.C. ANAYASASI'NDAKİ DÜZENLEME.....145
3.1.2.1. Anayasa'nın 20. Maddesindeki Düzenleme.....145
3.1.2.1.1. Anayasanın 20/ 3. Fıkrasının Eklenmesinden Önce Kişisel Verilerin Korunması.....146
3.1.2.1.2. Anayasanın 20/3. Fıkrasının Eklenmesinden Sonra Kişisel Verilerin Korunması.....149
3.1.2.2. Anayasa'nın 20. Maddesindeki Düzenlemenin Genel Bir Değerlendirmesi 150

3.2. KİŞİSEL VERİLERİN KORUNMASI HAKKI İLE GETİRİLEN KORUMA ALANI VE BU ALANIN SINIRLARI 152

3.2.1. KİŞİSEL VERİLERİN KORUNMASI HAKKI İLE GETİRİLEN KORUMA ALANI.....153
3.2.2. KİŞİSEL VERİLERİN KORUNMASI HAKKINA GETİRİLEN SINIRLAR.....154
3.2.2.1. Genel Olarak Özgürlük 154
3.2.2.2. Hak ve Özgürlüklere İlişkin Başlıca Güvence Ölçütleri 155

3.2.2.2.1. Kamu düzeni ilkesi 157
3.2.2.2.2. Demokratik toplum düzeni ilkesi 158
3.2.2.2.3.Ölçülülük ilkesi 159
3.2.2.2.4. Sınırlamanın "kanun" ile düzenlenmesi ilkesi 162
3.2.2.2.5. Hakkın özü kavramı 165

3.3. KİŞİSEL VERİ HUKUKUNDA İNSAN ONURU 169

3.3.1. GENEL OLARAK İNSAN ONURU.....169
3.3.2. T.C. ANAYASASI'NDA İNSAN ONURU 171
3.3.3. İNSAN ONURU, KİŞİNİN MADDİ VE MANEVİ VARLIĞINI GELİŞTİRME HAKKI VE KİŞİSEL VERİLERİN KORUNMASI HAKKI.....173

3.4. KİŞİSEL VERİLERİN KORUNMASI HAKKINI KORUYAN DİĞER TEMEL HAK VE ÖZGÜRLÜKLERİN KISMİ GARANTİLERİ……. ….....177

3.4.1. DİN, VİCDAN, İNANÇ ÖZGÜRLÜĞÜ VE KİŞİSEL VERİLERİN KORUNMASI.....177
3.4.2. ÖZEL HAYATIN GİZLİLİĞİ İLKESİ VE KİŞİSEL VERİLERİN KORUNMASI.....179
3.4.2.1. Genel Olarak.....179
3.4.2.2. Avrupa İnsan Hakları Mahkemesi Uygulamasında Özel Hayatın Gizliliği Hakkı 181
3.4.2.3. Özel Hayatın Gizliliği ve Kişisel Verilerin Korunması Hakkı Arasındaki Temel İlişki.....182
3.4.3. BİLGİ EDİNME HAKKI VE KİŞİSEL VERİLERİN KORUNMASI.....186
3.4.3.1. Genel Olarak.....186
3.4.3.2. Bilgi Edinme Hakkının Sınırları.....190
3.4.3.3. Kişisel Verilerin Korunması ile Bilgi Edinme Hakları Arasındaki Temel İlişki 192
3.4.4. DÜŞÜNCEYİ AÇIKLAMA ÖZGÜRLÜĞÜ VE KİŞİSEL VERİLERİN KORUNMASI.....195

3.4.4.1. Genel Olarak *195*
3.4.4.2. Kişisel Verilerin Korunması Hakkı ile Düşünceyi Açıklama Özgürlüğü Arasındaki İlişki *199*
3.4.5. HABERLEŞME ÖZGÜRLÜĞÜ VE KİŞİSEL VERİLERİN KORUNMASI HAKKI 202
3.4.6. ÖZEL HABERLEŞMENİN GİZLİLİĞİ İLKESİ İLE KİŞİSEL VERİLERİN KORUNMASI HAKKI ARASINDAKİ İLİŞKİ 204
3.5. ANAYASA'NIN 90. MADDESİ YOLLAMASI İLE AİHS KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI VE AİHM'NİN ROLÜ 206
3.5.1. "8. MADDE: ÖZEL VE AİLE HAYATINA (YAŞAMINA) SAYGI HAKKI" 208
3.5.1.1. Kanuna uygun olarak *208*
3.5.1.2. Meşru amaç *209*
3.5.1.3. Demokratik bir toplumda gerekli olmak *209*
3.5.2. AİHM İÇTİHADI 209
3.5.2.1. Kişisel Verilerin Toplanması ve Saklanması *210*
3.5.2.2. Telefon dinleme-kaydetme, Ses-Fotoğraf-Görüntü Kaydı *215*
3.5.2.3. Tıbbi Verilerin Saklanması ve İfşa Edilmesi (Açıklanması) *223*
3.5.3. AİHM İÇTİHADININ DEĞERLENDİRİLMESİ 226
DÖRDÜNCÜ BÖLÜM
TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI
4.1. KİŞİSEL VERİLERİN KORUNMASI KANUNU 229
4.1.1. KANUNUN AMACI VE KAPSAMI 229
4.1.2. KİŞİSEL VERİLERİN İŞLENMESİNDE BENİMSENEN GENEL İLKELER 231
4.1.3. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI 231
4.1.4. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENME ŞARTLARI 235
4.1.4.1. Kapsam *235*

4.1.4.2. Özel Nitelikli Verileri İşleme Yasağının İstisnaları 235
4.1.5. KİŞİSEL VERİLERLE İLGİLİ İŞLEMLER.....236
4.1.5.1 Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi.....236
4.1.5.2. Kişisel Verilerin Aktarılması.....237
4.1.5.3. Kişisel Verilerin Yurt Dışına Aktarılması 238
4.1.5.3.1 Kurumsal Yapılandırmada Ülke Örnekleri: 239
4.1.6. VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ VE İLGİLİ KİŞİNİN HAKLARI. 244
4.1.6.1.Veri Sorumlusunun Aydınlatma Yükümlülüğü 244
4.1.6.2. İlgili Kişinin Hakları 244
4.1.6.3.Veri Güvenliğine İlişkin Yükümlülükler 245
4.1.6.4.Veri Sorumlusuna Başvuru.....247
4.1.6.5. Kurula Şikâyet.....248
4.1.6.6. Şikâyet Üzerine veya Resen Yapılacak İncelemenin Usul ve Esasları.....249
4.2. TÜRK MEDENİ KANUNU KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI.....251
4.2.1. GENEL OLARAK.....251
4.2.2. MEDENİ KANUN'DAKİ KORUMA 252
4.3. TÜRK CEZA KANUNU KAPSAMINDA KORUMA.....254
4.3.1.GENEL OLARAK 254
4.3.2. KİŞİSEL VERİLERE DOĞRUDAN KORUMA SAĞLAYAN SUÇ TİPLERİ 256
4.3.2.1. Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu.....256
4.3.2.2. Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu .263
4.3.2.3. Verileri Yok Etmeme Suçu.....268
4.4. CEZA MUHAHAKEMESİ KANUNU KAPSAMINDA KORUMA 275
4.5. DİĞER KANUNLAR KAPSAMINDA KORUMA.....277
SONUÇ 285

KAYNAKÇA 317

İNTERNET KAYNAKLARI 312

AİHM KARARLARI 315

KISALTMALAR

a.g.e. : Adı geçen eser

a.g.m. : Adı geçen makale

ABAD : Avrupa Birliği Adalet Divanı

AB : Avrupa Birliği

ABTHŞ : Avrupa Birliği Temel Haklar Şartı

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sozleşmesi

AÜEHFD : Ataturk Üniversitesi (Erzincan) Hukuk Fakültesi Dergisi

AÜHFD : Ankara Üniversitesi Hukuk Fakültesi Dergisi

AÜSBF : Ankara Üniversitesi Siyasal Bilgiler Fakültesi

AÜSBFD : Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi

AYM : Anayasa Mahkemesi

AYMK : Anayasa Mahkemesi Kararı

B. : Bölüm

bas.no. : Başvuru no

BEHK : Bilgi Edinme Hakkı Kanunu

BK : Borçlar Kanunu

Bkz. : Bakınız

C. : Cilt

CCTV : Close Circuit Television (Kapalı Devre Televizyon)

CMK	: Ceza Muhakemesi Kanunu
Çev.	: Çeviren
DEÜHFD	: Dokuz Eylül Üniversitesi Hukuk Fakultesi Dergisi
DNA	: Deoksiribo Nükleik Asit
E.	: Esas sayısı
ECJ	: European Court of Justice (Avrupa Adalet Divanı)
EHK	: Elektronik Haberleşme Kanunu
EHSKVİY	: Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik
ETDK	: Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
FLSF	: Felsefe ve Sosyal Bilimler Dergisi
GPS	: Global Positioning System (Kuresel Yer Belirleme Sistemi)
HD	: Hukuk Dairesi
İHEB	: İnsan Hakları Evrensel Beyannamesi
İÜHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
İÜY	: İstanbul Üniversitesi Yayınları
K.	: Karar sayısı
k.t.	: Karar tarihi
KVKK	: Kişisel Verilerin Korunması Kanunu
m.	: Madde
MERNİS	: Merkezi Nüfus İdaresi Sistemi
MK	: Medeni Kanun

MÜHF : Marmara Üniversitesi Hukuku Fakültesi Dergisi

N.Y.U. L. Rev.: New York University Law Review

no. : Numara

OECD : Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)

PVSK : Polis Vazife ve Selahiyet Kanunu

RG. : Resmî Gazete

s. : Sayfa

S. : Sayı

SÜHFD : Selçuk Üniversitesi Hukuk Fakültesi Dergisi

SDÜHFD : Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi

T. : Tarih

TBB : Türkiye Barolar Birliği

TBBD : Türkiye Barolar Birliği Dergisi

TCK : Türk Ceza Kanunu

TDK : Türk Dil Kurumu

TMK : Türk Medeni Kanunu

TTK : Türk Ticaret Kanunu

vb. : Ve benzeri

vd. : Ve devamı

Y. : Yıl

yy. : Yüz yıl

GDPR : Avrupa Birliği Veri Koruma Tüzüğü

AB Veri Koruma Yönergesi : 95/46/AT sayılı Yönerge

AK 108 sayılı Sözleşmesi : Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

GİRİŞ

İnsanlığın eski çağlardan günümüze doğru toplumsal hareketleri, yeni toplum kurallarını doğurduğu gibi, hukukun giderek çerçevesinin daha da belirgin olmasını sağlamıştır. Tarih içerisinde toplumsal sınıfların oluşması, bu sınıfların birbirleriyle mücadeleleri, modern devletlerin giderek belirginlik kazanmasını sağlarken aynı zamanda kaotik düzenin azaltılıp bitirilmesi adına herkesi bağlayan temel kuralların kaçınılmaz bir zaruret olarak güçlenmesini sağlamıştır. Sınırların güvenliği kadar artık kişilerin bireysel sınırlarının güvenliği de güvence altına alınmaya başlamıştır. Kamu güvenliği modern devletlerin temel bir faaliyet alanı olurken, bireysel haklar da bu çerçevede her geçen zaman önem kazanmıştır. Modern devlet mekanizması, kendi güvenliğini yöneten yönetilen dengesine yaslamıştır. Eski devletlerin krallık perspektifi yönetime katılmayı mümkün hatta mecbur kılan bir boyut kazanarak değişmiş, temel haklar ekseninde yönetilenler yani bireyler haklar bağlamında güvenceler kazanmıştır. Bu haklar olağan ve meşru bir güç haline gelmiştir.

Anayasalar ve bu anayasa metinlerinde yer alan temel hak ve hürriyetler uzun soluklu siyasal ve sosyal çabaların eseri olarak hukuk hayatında yerini almıştır. Genel anlamda anayasalar devletlerin siyasal yapılarını, bu siyasal sistem içerisinde görev alan kurum ve mekanizmaların görev ve salahiyet alanlarını belirleyen en üst normları içeren metinler olarak tanımlanabilir. Anayasalar, devleti oluşturan kurum ve kuruluşların yeknesak bir şekilde işlemesi yanında aynı zamanda başta iktidar olmak üzere bu kurum ve mekanizmaların hukuki sınırlarını da belirlemiştir.

Tarihsel süreçte, anayasacılık hareketlerinin temelinde iktidarın sınırlandırılması ile birlikte bireylere sağlanan temel hak ve hürriyetlerin garanti altına alınması gayesi olduğunu görüyoruz. Anayasalar bir yandan devletin işleyişini düzenlerken diğer taraftan iktidarın nasıl kullanılacağını belirler. Bunlara ilaveten, anayasalar, temel hakları, insan odaklı kodifiye ederek onları birey lehine yorumlayarak devletin müdahalesine sınırlamalar getirir.[1] En üstün norm olan anayasalar, bu bahsedilen alanların düzenlenmesi ile kanunlara ve diğer düzenleyici

[1] Kaya, Semih Batur, "Hukuk Devleti, Demokrasi ve Anayasacılık Ekseninde Anayasa Yargısı ve Yargısal Aktivitizm", Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XIX, Y. 2015, S. 3, s.359.

işlemlere göre değiştirilmesi çok daha zor olan hükümler halini alırken, hem devlet mekanizmasına ve onu kullanan iktidarlara hem de bireylere yönelik bağlayıcı hal almaktadır.

Anayasacılık hareketlerinin devamlılığı ve günümüz modern anayasalarına evirilmesinin neticesinde, devletler, bireyleri önceleyen ve onlara tanınan temel hakları anayasa ile teminat altına alan modern hukuk devleti olma yolunda ilerlemişlerdir. Düşünce ve ifade hürriyeti, özel hayatın gizliliği, haberleşme özgürlüğü gibi klasik temel haklar geçmişten günümüze anayasalarda yer alan temel haklar arasında görülmektedir. Kişisel verilere ilişkin hakların ise temelini bu klasik hakların oluşturduğu görülmektedir.

Devletler, tabiiyetinde bulunan kişilere ilişkin bilgi elde etme, onları tanıma ihtiyacı duyarlar. Devlet mekanizmalarının oluşmasından başlayarak günümüze kadar bu ihtiyaç hep var olmuştur. Bu gereksinimdeki motivasyonun kaynağı; kamu güvenliği ve düzeninin tesisinin yanı sıra suç işlenmesinin önlenmesine yönelik olabileceği gibi devletlerin bazı ticari ve ekonomik kaygılarından da kaynaklanabilmektedir. Gün geçtikçe bu ihtiyaç kamu sektörünün yanı sıra ticari kaygılardan ekonomik kaygılara kadar uzanan bir ihtiyaç listesi içerisinde özel sektöre de sirayet etmiştir. İlk başlarda geleneksel şekilde kişilere ilişkin verilerin manuel olarak tutulması şeklinde başlayan işleme faaliyetleri; teknolojinin akıl almaz bir biçimde ilerlemesi, verilere ulaşmadaki ve verileri depolamadaki kolaylıklar ile birlikte git gide otomatize edilmiş sistemler üzerinde veri işlenmesi ile günümüzdeki halini almıştır. Böylelikle genel manada, doğrudan veya dolaylı olarak gerçek kişiler ile irtibatlandırılabilen her türlü bilgi kişisel veri olarak günümüz hukuk literatüründe yerini almıştır

20. yy.'nin özellikle ortalarından itibaren teknoloji ve bilişim sektöründe yaşanan hızlı gelişmelerle birlikte kişiler hakkındaki bilgilerin toplanarak depolanması, diğer kişiler, özel veya kamu kurumları hatta diğer ülkeler arasında paylaşılması iyiden iyiye kolaylaşmıştır. Kişisel verilerin işlenmesi olarak adlandırabileceğimiz bu faaliyetlerin, özellikle teknolojik araçlar sayesinde hızlı ve kolay yapılabilmesi, kişisel verileri oluşturarak elinde tutan kişilerle söz konusu veri

sahipleri arasındaki çıkar dengesini, veri sahipleri aleyhine bozmuştur. Bu durum karşısında, verilerin ait oldukları kişilerin maddi ve manevi varlıkları zarar görmeye başlayınca, veri sahiplerinin çıkarlarının korunması ihtiyacı doğmuştur. Gün geçtikçe kişisel verilerin kötüye kullanımına yönelik artan endişeler, kişisel verilerin korunması alanındaki hukuki sorunların çözümünü gerekli kılmıştır.

1970'lerden sonra uluslararası platformlarda bu hususta fikirler üretilmeye başlamış ve anayasacılık hareketlerinin temel motivasyonuna paralel merkezde çeşitli uluslararası düzenlemeler ile kişisel verilerin işlenmesi karşısında kişilerin temel hak ve hürriyetlerinin korunması sağlanmaya çalışılmıştır. Hatta bazı ülkeler anayasalarına kişisel verilerin korunması hakkını temel hak olarak dercetmek suretiyle bu hakka anayasal hak statüsü kazandırarak koruma altına almıştır. Zira kişisel verilere yönelik, kamu sektörü ve özel sektör kişilerin verilerini elde etme hatta gerektiğinde kullanma temayülünde olmuştur.

Ülkemizde ise, kişisel verilerin korunması hukukunun çok köklü bir geçmişi olmamasına rağmen, Avrupa Konseyi'nin kurucu üyesi olan ülkemiz açısından 108 sayılı sözleşmenin imzaya açılmasından bu yana, kişisel verileri koruma hukukunun ülkemiz gündeminde olduğu görülmektedir. Avrupa Konseyi'nin 108 sayılı sözleşmesinin yanı sıra özellikle AB düzenlemeleri olan 95/46/AT sayılı Yönerge ve GDPR'nin, KVKK üzerindeki etkisi değerlendirildiğinde, kişisel verileri koruma alanında Türk hukukunda yapılan her atılımda Avrupa hukukun katkısı ve etkisi göz ardı edilemeyecek bir gerçektir.

Biz de bu çalışmamızın birinci bölümünde; genel olarak kişisel verileri koruma hukuku ile ne kast edilmek istendiğini ve bu alana ilişkin tarihçesini inceleyerek "kişisel veri" kavramının uluslararası metinlerde düzenleniş şekillerini ortaya koymaya çalıştık. Özellikle uluslararası zeminde kronolojik sırayı gözeterek bu hakkın nasıl doğduğuna, teknolojik gelişmelerin bu hakkın oluşmasına nasıl bir katkıda bulunduğuna ve bu hakka yönelik sağlanan korumanın hukuki yönelimlerine değindik. Özellikle uluslararası metinlerde kişisel verileri koruma hukukunun; ortaya konuluş şekli, amacı, ilkeleri ve bu metinlerin bağlayıcılık eksenli olmak üzere ayırt edici yönlerini ele aldık. Bu bağlamda OECD ve BM başta olmak üzere esasen ülkemizin

kurucu üyesi olması ve uluslararası alanda ilk bağlayıcı sözleşme olan 108 sayılı sözleşmeyi kabul etmesi nedeniyle AK; köklü deneyime sahip olması ve ülkemizin de üye adayı olmasından ötürü AB hukukuna ayrıntılı bir şekilde değinmiş olduk.

Çalışmamızın 2. bölümünde; "kişisel veri" kavramı, bu kavramın unsurları, özellikle "hassas veri", "anonim veri" kavramları etrafında kişisel veri türleri ele alındı. Ayrıca kişisel verilerin hukuki niteliğine ilişkin ortaya atılan; insan onuru, özel hayatın gizliliği, mülkiyet ve fikri mülkiyet hakkı görüşleri ekseninde hukuki nitelendirilmesine ilişkin teorilere değinilmiştir. Öte yandan, kişisel veri hukukuna ilişkin temel terminoloji incelenerek, veri sahibi, veri işleyen, veri sorumlusu, rıza ve veri işleme faaliyeti gibi kişisel verileri koruma hukukunun önde gelen terimlerinin hukuki tanımlamalarını uluslararası ve ulusal metinler ile doktrin çerçevesinde ortaya konulmuştur. Ayrıca kişisel verilerin korunmasında gözetilecek ilkelerin neler olduğunu esas ve şekli ilkeler olarak ikiye ayrılmak suretiyle aynı usulde açıklanmaya çalışılmıştır.

Çalışmamızın ana gövdesini ve temelini oluşturan üçüncü bölümde ise; anayasa hukuku ve anayasal bağlamda kişisel verilerin korunması hukuku incelenmiştir. Bu minvalde, uluslararası metinlerde yer alan kişisel verilerin korunması hakkı ile ilgili düzenlemeler daha eski tarihli olsa da, iç hukukumuza 2010 Anayasa değişikliği ile Anayasa'nın 20. m.'sine eklenen 3. fıkra ile kişisel verilerin korunması hakkı, anayasal temel bir hak statüsüne kavuşmuştur. Bu bağlamda, özelde kişisel verilerin korunması konusuna getirilen anayasal koruma ile bu hakka sağlanan anayasal korumanın hukuki temelleri; genel olarak ise anayasada teminat altına alınmış diğer bazı temel haklar etrafında kişisel verilere sağlanan korumalar ile bu hakka yönelik yapılabilecek olan müdahalelerin anayasal sınırları incelenmiştir. Bu inceleme yapılırken özellikle AYM kararları ile anayasa yargısının bu konudaki içtihatları çalışmamızda kendisine yer bulmuştur. Yine bu bölümde Anayasa m. 90 atfı ile normlar hiyerarşisinde kendisine en üst düzeyde yer bulan AİHS'ye ve onun yargısal denetimini yapan ve başta AYM olmak üzere Türk yargı makamlarının içtihatına yön veren AİHM'nin kararlarına ve bu kararlarda AİHM'nin dikkat ettiği kriterlere etraflıca çalışılmıştır.

Çalışmamızın son bölümünde ise; yasa yapım çalışmaları çok daha eski tarihe dayansa da 2016 yılında yürürlüğe girmiş olan 24/3/2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile kişisel veriler hakkındaki yasal düzenleme ve korumalar incelenmeye çalışılmıştır. Yine burada kişisel verileri koruma konusunda yetkilendirilmiş otorite olan kurumlara yönelik mukayeseli hukukta bir karşılaştırma yapılmıştır. Yine anayasamızın da kendilerine dayanak olduğu ve iç hukukumuzda kişisel verilerin korunması konusunda hükümler içeren kanunlardan hukuk ve ceza alanında başlıca yasalarımız olan Türk Medeni Kanunu'ndaki, Türk Ceza Kanunu'ndaki ve Ceza Muhakemesi Kanunu'ndaki kişisel verilerin korunmasına ilişkin düzenlemeler ile ilgili yasal mevzuat -çalışmamızın konu başlığı gözetilerek- incelenmiştir.

BİRİNCİ BÖLÜM

GENEL OLARAK KİŞİSEL VERİLERİN KORUNMASI HUKUKU, TARİHÇESİ, ULUSLARARASI HUKUKTA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL METİNLER

1.1. GENEL OLARAK KİŞİSEL VERİLERİN KORUNMASI HUKUKU

Kişisel verilerin toplanmasından başlamak suretiyle, işlenmesi, muhafaza edilmesi ve belli alanlarda kullanılması gibi birtakım işlem ve eylemlere dair usul ve esasların belirlenmesi, kişisel verilerin korunması hukukunun esas konusunu oluşturmaktadır. Kişisel verilerin korunması hukuku, *-eşyanın tabiatı gereği-*, pek çok hukuk dalı ile iç içe geçmiş durumdadır. Hukukun sınıflandırılmasında, kamu hukuku-özel hukuk ayrımı, Roma Hukukunun oluşmasından bu yana genel geçer kabul gören sınıflandırma biçimi olarak karşımıza çıkmaktadır.[2] Fakat tarihin olağan akışı içinde ve teknoloji alanında kaydedilen gelişmelere paralel olarak, toplumsal yapıların yanı sıra devlet yapılanmalarının değişmesi ve gelişmesi, özellikle teknolojik gelişme içerisinde sayılan dijital[3], bilişim[4], yazılım[5] alanındaki ilerlemeler ile birlikte bilgisayar[6] sistemlerindeki son gelişmeler göz önüne alındığında artık bu ayrımın yetersiz olduğu kanaati doktrinde kendisine yer bulmaya başlamıştır. Bu ayrımın yetersiz kaldığı savından hareketle, bazı yazarların, kamu hukuku ve özel hukuk

---

2 Gözübüyük, Şeref, "Hukuka Giriş ve Hukukun Temel Kaynakları", 35. Baskı, Ankara, 2013, s. 23.

3 Köken itibarıyla Fransızca bir kelime olup "sayısal", "*verileri bir ekran üzerinde otomatik olarak gösteren*" demek olan sıfat türünde bir kelimedir. http://sozluk.gov.tr/, Erişim tarihi, 10.01.2018.

4 "*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik*", http://sozluk.gov.tr/, Erişim tarihi, 10.01.2018.

5 "*Bir bilgisayarda donanıma hayat veren ve bilgi işlemde kullanılan programlar, yordamlar, programlama dilleri ve belgelemelerin tümü*", http://sozluk.gov.tr/, Erişim tarihi, 10.01.2018.

6 "*Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin*", http://sozluk.gov.tr/, Erişim tarihi, 10.01.2018.

unsurlarını bünyesinde barındıran karma hukuk adında yeni bir alanı bu ayrıma eklemledikleri görülmektedir.[7]

Türk hukukuna genel olarak baktığımızda, kişisel verileri koruma hukuku, 1982 Anayasasının 20. m.'sinde yani temel haklar kısmının, kişi hakları bölümünde kendisine yer bulmasının bir gereği olarak kamu hukuku süjesi gibi görünse dahi kişiler hukuku ile olan ilgisi göz önüne alındığında, bu bağlamda, dar anlamda medeni hukuktan geniş anlamda -özel hukuktan- izler taşıdığı görülmektedir. Hatta TMK'da kişisel verilere ilişkin düzenlemelere yer verildiği görülmektedir. Aynı şekilde TCK (m. 135 vd.) ve TTK'da (m. 24 vd.) kişisel verilere ilişkin hükümler bulunmaktadır. Gerek anayasal bir kamu hakkı olarak tali kurucu iktidar tarafından anayasaya eklenmesi, gerekse TCK ile bu hakka riayet edilmemesinin belli başlı yaptırımlara bağlanması, diğer taraftan, 6698 sayılı Kanun ile *"Kişisel Verilerin Korunması Kurumu"* nun kamu gücünü kullanan bağımsız idari otorite şeklinde örgütlenmesi gibi hususlar göz önünde bulundurulduğunda, kişisel verileri koruma hukukunun kamu hukuku alanına yaklaştığını söylemek mümkündür.[8]

Devletlerin yurttaşları ile olan ilişkilerinin yanı sıra devlet kurumlarının birbirleri ile olan ilişkilerini düzenleyen hukuk dalı, kamu hukuku olarak adlandırılmaktadır. Bu ayrımı ortaya koymaya yönelik teorilere başka bir ifade ile bir hukuk dalının kamu hukuku mu yoksa özel hukuk mu olduğunu belirlemek için ortaya atılan görüşlere baktığımızda: *"çıkar teorisi"* ne göre uyuşmazlık konusu kamuyu ilgilendiriyor ise; *"alt-üst ilişkisi"* teorisine göre uyuşmazlığın taraflarından biri devlet otoritesinin gücünü kullanıyor ise; *"özel hukuk"* teorisine göre, mevzuat sadece devlet otoritesine birtakım sorumluluk ve yetkiler yüklüyor ise, bu durumlarda kamu hukukunun varlığından söz edildiği görülmektedir.[9] Kanaatimizce, kişisel verileri koruma hukukunu kamu hukuku alanında değerlendirmek gerekmektedir. Şöyle ki yukarıda bahsettiğimiz üzere, bu hakkın, anayasaların temel haklar kısmında kendisine yer bulması, birçok temel hak ile iç içe geçme durumunun yanı sıra devletlerin hukuk

---

7 Atay, Ender Ethem, "Hukuk Başlangıcı", 1.Baskı, Ankara, 2013, s. 123.

8 Karma Hukuk alanına girdiğine ilişkin görüş için ayrıca bkz. Taştan, Furkan Güven "Türk Sözleşme Hukukunda Kişisel Verilerin Korunması", 1. Baskı, İstanbul, 2017, s. 8.

9 https://www.turkcebilgi.com/kamu_hukuku, Erişim tarihi 22/12/2019.

sistemlerini oluşturan temel ceza yasalarında devlet veya başka kişilerce bu hakka müdahale edilmesinin kamu adına yaptırımlara bağlanması hususları bu görüşümüzün temelini oluşturmaktadır. Öte taraftan, yukarıda açıkladığımız teorilerin temel kabullerinden hareketle, kişisel verileri koruma hukuku alanında çıkabilecek uyuşmazlıkların en azından bir tarafında devlet mekanizması veya bu mekanizmayı oluşturan kurum ve kuruluşların olması dikkate alındığında, kişisel verileri koruma hukukunun, kaynağını anayasal haktan alan ve temel kanunlarda kendisine düzenleme alanı bulan bir kamu hukuku dalı olduğu kabul edilmelidir.

Anayasa hukuku bağlamında, özellikle, sosyal devlet olmanın gerektirdiği faaliyetlerin yanı sıra güvenliğin tesisinin ve yönetime ilişkin kararların alınabilmesinin bir gereği olarak, devlet otoritesi, hükümranlığı altında bulunan kimselerin ayırt edici özellik taşıyan verilerine ulaşma, bunları derleme ve sınıflandırma ihtiyacını hissetmektedir. Bu hususlar, esasen, anayasa hukuku bakımından, kişisel verilerin korunmasının bir anayasal hak olarak tanınmasındaki meşruluğun da temelini oluşturmaktadır.[10] Başka bir deyişle, anayasa hukuku açısından, kişisel verilerin korunması kavramının temeli, devletlerin belirli anayasal ve kanuni şartlar altında, hukuki öngörülebilirlik çerçevesinde, vatandaşlarının kişisel bilgilerine erişme isteği ve/veya bunları tasnif etme mecburiyetinden kaynaklanmaktadır. Bir hukuk devletinden bahsedilebilmesi için, kişilerin kendilerine ait bilgilerin toplanması ve kullanılması gibi hususlarda hukuki öngörülebilirliğe sahip olmaları gerekmektedir. Esasen bu temel ilkenin doğal bir sonucu olarak 1982 Anayasası'nda kişisel verilerin korunmasını isteme hakkı, temel kişi hak ve hürriyetleri kapsamında değerlendirilmiştir.

Devlet tüzel kişisi, kamu tüzel kişileri, özel hukuk tüzel kişileri ve gerçek kişilerin; kişilere ait verileri, sistematik bir şekilde, otomatize[11] edilmiş mekanik veya

---

10 Şimşek, Oğuz, "Anayasa Hukukunda Kişisel Verilerin Korunması", 2008, Beta yayınları s. 4.

11 Kişisel Verilerin Korunması Kanununda otomatik işleme kavramı tanımlanmamış olmasına rağmen, Kanun gerekçesinde kapsam ifade edilirken, "*Günümüzde bu veriler, gerek özel sektör ve gerekse kamu sektörü tarafından bilişim sistemleri üzerinden otomatik yollarla sıkça kullanılmaktadır.*" denilmek suretiyle doğrudan olmasa da, bilişim sistemleri üzerinden yapılan faaliyetlerin otomatik işleme olduğunu ifade etmiştir. https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-SorulanSorular, Erişim tarihi, 12.01.2018.

dijital yazılımlar ile kayda alması, bu kayıtları kendi alanında menfaatlerine uygun olarak kullanması ile kişisel verilerin korunması konusu ve bu hukuk dalı teori ile beraber uygulamada önemli ölçüde alan kazanmıştır. Başka bir anlatımla; kişilerin bilgilerine, verilerine erişim meselesi ve bunların kötüye kullanılmasına ilişkin kaygılar, hiç şüphesiz dünyamızın teknolojik olarak modernleşmesinin neticesinde; hayatımıza doğrudan dahil olan internet, sosyal medya, verilerin depolanmasındaki yazılımsal kolaylıklar ile gitgide artmıştır. Bu alan kazanmaya paralel olarak kişilerin bilgilerine ve bireylerin verilerine erişim meselesi ile bu bilgilerin ve verilerin kötüye kullanılmasına ilişkin kaygıların yükseldiği görülmektedir.

Devlet otoritesinin ve özel hukuk kişilerinin belli başlı yazılımları ve otomatize edilmiş mekanik ve dijital sistemleri kullanmaya başlaması ile birlikte kişilerin verilerine ulaşmadaki kolaylığın artması beraber değerlendirildiğinde, kamu ve özel hukuk kişilerinin bu verileri işlemesi -kullanması- sırasında hukuki ve yasal olarak sınırlandırılmaları gerekliliği ortaya çıkmıştır. Böylelikle geniş anlamda veri koruma hukukunun, dar anlamda ise kişisel veriler hukukunun modernleşme ve teknolojik gelişme sürecinin içerisinde günümüz hukukunda kendine yer bulduğu alana doğru evrildiği görülmektedir.

Otomatik işlem deyiminden maksat, 108 sayılı sözleşmenin[12] 2. m.'sinde, "*tamamen veya kısmen otomatik[13] yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal[14] ve/ veya aritmetik[15] işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılır*." şeklinde düzenlenmiştir. Buradan hareketle, geniş anlamda otomatik sistemi tanımlayacak olursak; en üst derecede, elektronik veya dijital ortamda bilgisayar yazılımı ile üretilen ve yapay zekaya haiz bir sistem, program veya bu kadar üst düzey teknoloji ürünü

---

12 Avrupa Konseyi Sözleşmesi hakkında ayrıntılı bilgi için bkz.. "*Avrupa Konseyi'ndeki Kişisel Verilerin Korunması*" başlığı, s. 12 vd.

13 "*Mekanik yollarla hareket ettirilen veya kendi kendini yöneten (alet)*", http://sozluk.gov.tr/, Erişim tarihi, 12.01.2018.

14 "*Doğru düşünme sanatı ve bilimi. Düşüncenin ve düşüncenin varlık biçimlerinin, ögelerinin, türlerinin, olanaklarının, yasalarının ve düşünce bağlamlarının bilimi, lojik*", http://sozluk.gov.tr/, Erişim tarihi, 12.01.2018.

15 "*Matematiğin, konusu sayılar, bunların özellikleri ve işlemler olan kolu, hesap*", http://sozluk.gov.tr/, Erişim tarihi, 12.01.2018.

olmamakla beraber verilerin oluşturulması ve kaydı için tamamen veya kısmen insan gücüne ve zekasına ihtiyaç duyan sistem, program diyebiliriz. Örneğin, bu bağlamda MERNİS[16] üst düzey teknoloji ile donatılmış, verileri kaydetmeye, bulmaya yarayan elektronik, otomatize olmuş bir sistem olarak karşımıza çıkmaktayken; bir bakkalın veresiye defteri kendi içinde müşterilerin alışveriş yaptıkları ürünleri, müşterilerin ekonomik durumlarını sınıflandıran ancak otomatize edilmemiş manuel bir veri kayıt sistemi olarak karşımıza çıkmaktadır. Fakat veri koruma hukuku bakımından, hakkın özü itibarıyla iki sistemden kaynaklanan hukuki tecavüzlerin aynı şekilde Türk hukukunda korunduğunu söyleyebiliriz.[17]

Günümüzde, elektronik ortamda yapılan işlem sayısı gün geçtikçe artmakta ve kişisel verilerin korunmasına yönelik olarak bu alanda alınacak önlemlere ilişkin hukuki düzenlemeleri yapma zorunluluğu doğmaktadır. Bu bağlamda, günümüzde, geniş anlamı ile kişisel verilerin korunmasından kasıt, salt olarak o verinin korunmasını temin etmek değil, bu verinin korunmaması nedeniyle ortaya çıkabilecek temel hak ve özgürlük ihlallerinin önüne geçmeye çalışmak olduğu görülmektedir.[18] Buradan hareketle, kişinin, kişisel verilerinin korunması talebi ve hakkı ve bu hakkın kamu otoritesi tarafından korunması demokratik, özgür ve en önemlisi hukuki güvenliğe sahip bir toplumun oluşmasında küçümsenmeyecek bir role sahip olduğunu belirtebiliriz.

Hukuki olarak verilerin korunması terimi, veri işlemenin tüm aşamalarını; yönetme, depolama, biriktirme, paylaşma vb. hususları işaret etmektedir. Verilerin korunmasına ilişkin yapılan düzenlemeler gerek uluslararası gerekse ulusal bazda olsun özel hayat, ifade özgürlüğü, uluslararası ticaret ve kamu düzeni ile ilişkili olarak

---

16 Mernis, tüm kişisel bilgilerin elektronik ortama aktarılmasını sağlayan ve kişisel bilgilerde ortaya çıkan bütün değişikliklerin ülkenin her yerine dağıtılmış bulunan 970 merkezden anlık olarak güncellenerek oluşturan bir ağ üzerinden güvenli bir şekilde paylaşımını sağlayan projenin adıdır. https://www.icisleri.gov.tr/merkez-nufus-idare-sistemi-mernis, Erişim tarihi, 12.01.2018.

17 Türkiye Cumhuriyeti, 108 sayılı sözleşmeye ilişkin vermiş olduğu beyanlarda, Sözleşme madde 3/2-c gereğince, "*sözleşmenin otomatik olmayan yollar ile işlenmiş olan kişisel verilere de uygulayacağını*" beyan etmiştir.

18 Şimşek, a.g.e, s. 4.

giderek önem kazanmıştır.[19] Diğer bir deyişle, kişisel verilerin koruması, kişisel bilgilerin, bir bilgisayar ortamında saklanan elektronik veya el ile yazılmış materyaller gibi şeyler ile nelerin yapılabileceğini veya yapılamayacağını ifade eder. Veri korumaya ilişkin düzenlemeler; vatandaş, müşteri ve çalışan bağı ile bir otoriteye bağlı olan kişilerden kişisel verilerin toplanmasına ve hatta başka bir ülkeye gönderilmesi için kişisel bilgilerin kısıtlanması, kullanımı, depolanması, aktarılması, sınırlandırılması ile ilgili kuralların uygulanmasını amaçlar.[20]

Genel olarak, veri koruma hukukundaki yaklaşımın, 108 sayılı Sözleşme, 95/46/AT sayılı Yönerge, GDPR (2016/ 679/ AT sayılı Genel Veri Koruma Tüzüğü), Almanya, Belçika, Birleşik Krallık, Hollanda ve Yunanistan gibi bazı AB ülkelerindeki yasal düzenlemeri göz önünde bulundurarak tüzel kişiden daha çok, gerçek kişiyi korumak olduğu kabul edilebilir. Bununla birlikte, giderek artan bir şekilde, bu türden bir korumanın tüzel kişilere teşmil edilmesi yönünde bir talep olduğu görülmektedir. Bunun sonucu olarak ise Avusturya, İtalya ve Lüksemburg gibi bazı ülkelerin iç hukuklarında, bu türden tüzel kişiliklerin korunmasını sağlama yoluna gittikleri görülmektedir.[21] Türk hukukunda ise, ileride açıklayacağımız üzere, gerçek kişilerin anayasal ve yasal çerçevede korunduğu görülmektedir.

1.2. TARİHÇE

Eski çağlardan beri devletler, devlet olmanın bir gereği olan hizmetleri icra edebilmek için kendi tabiiyetinde veya hükümranlığı altında olan kimseleri subjektif olarak bilmek ve bu kimselere yönelik özellikle kamusal hizmetleri yürütmek maksadıyla belli başlı verilere ulaşmak istemişlerdir. Böylelikle ilk olarak devlet otoritesi ile gerçek kişiler arasında, gerçek kişilerin kişisel verilerine ulaşabilmek ihtiyacından kaynaklanan birtakım hukuki nitelik içeren meselelerin oluşmaya başladığını görüyoruz. Zira devletlerin oluşturulması ve yapılandırılması ile birlikte

19 Steven, S. McCarty-Snead; Anne, Titus Hilby, "Research Guide to European Data Protection Law", 42 Int'l J.Legal Info. 2014, s. 350.

20 Peter, Carey, "Privacy and Data Protection", 2009, Volume 10, Issue 1, November, Articles/Data Protection: Backto Basics, s. 2.

21 Aksoy, Hüseyin Can "Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması", Ankara 2010, s. 19.

devletler, ülkelerinde yaşayan insanları tanımak için verileri kendi imkânlarıyla kayıt altına almışlardır. [22]

İlk çağlarda belirli meslek gruplarına yönelik sır saklama yükümlülüğü adı altında, daha doğrusu, bir kişiye ait bilinmesi istenmeyen bir şeyin yayılmasının engellenmesi amacıyla -günümüzdeki anlamı ile olmasa bile- kişisel verilerin korunması kavramı kullanılmaya başlanmıştır. Belli meslek gruplarına tanınan "susma hakkı", "sır saklama yükümlülüğü" gibi kavramlarda bu hakkın tohumlarını görüyoruz. Özellikle doktorların ilk çağlardan beri hastalarına ilişkin elde ettikleri bilgileri saklama ve bunları açığa vurmama gibi yükümlülükleri hep var olmuştur. Sır saklama ile ilgili ilk bilgi, "Hipokrat Yemini" nde bulunmaktadır. Adı geçen yeminde sır saklamaya ilişkin olarak *"tedavi sırasında veya tedavi dışında insan hayatında görüp işittiklerim hakkında sessiz kalacağım ve bu tür şeyleri konuşmayacağım."* ifadesine yer verilmiştir.[23] Yine ilk çağlardan beri rahiplerin meslekleri icabı elde ettikleri kişisel bilgileri kullanmama ve saklama durumları ortaya çıkmıştır. Zira, Hristiyanlıkta günah çıkarma müessesesinin işlemesi sırasında kişilere ait pek çok bilgi ve verinin din adamları tarafından öğrenilmesi kuvvetle muhtemeldir.[24]

Esasen bu meslek mensuplarının elde ettikleri bilgiler ve kişisel veriler alelade bir veriden ziyade, günümüz hukuku anlamında hassas veri kategorisinde değerlendirilebilecek tarzda veriler olmaktadır. Örneğin; bir doktorun hastasının mahrem hastalığını bilmesi, yine bir din adamının kendisine gelen kişinin bir kabahatini hatta belki işlediği bir suçu bilmesi imkan dahilindedir. Dahası bu imkanın, o çağların teknolojik alt yapısı ve sosyolojisi düşünüldüğünde çok değerli bir statüde konumlandığını söylemek yanlış olmaz. Dolayısıyla, bu meslek mensuplarının gerek dini gerekse "yemin" gibi normatif sayılabilecek düzenlemeler ile sınırlamalara tabi tutuldukaları dikkate alındığında, insanların doğal olarak ilk çağlarda kendilerine ait bilgilerin elde edilmesi, kullanılması ve yayılması hususlarına temkinli yaklaşarak bu

---

22 Şimşek, a.g.e., s. 3.

23 Törenli Çakıroğlu, Maral, "Hekimin Borçlarından Özel Olarak Sır Saklama Borcu", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 12, Sayı: 2, Yıl: 2010, s. 159.

24 Şimşek, a.g.e, s. 3-7.

bilgilere sahip olanları hukuki düzenlemeler ile sınırlamak istedikleri içgüdüsel bir yaklaşım olarak karşımıza çıkmaktadır.

Öte yandan "Kişisel veri" kavramı yazı ile başlamış ve tarihsel süreç içerisinde kil taşlarından dijital ortama kadar çeşitli şekillerde değişime uğrayarak günümüze kadar ulaşmıştır. Örneğin, Eski Asur Ticaret Kolonileri Devri'nden (M.Ö 2000-1750) günümüze Asurca kil tabletler üzerine yazılmış 2.500 civarında çivi yazılı tablet kalmış ve bu tabletlerde Asur'dan Anadolu'ya ticaret yapmak için gelen tüccarların ticari ve hukuki sorunlarıyla ilgili kişisel verilerin tutulduğu ilk kayıt ve belge örneklerine rastlanılmıştır.[25]

Yine, Anadolu'da yapılan tarihi eserlere baktığımızda, özellikle Selçuklu dönemi eserlerinde, taş malzeme üzerine yapıyı yapan hükümdar, mimar ve eserde çalışan sanatçı isimlerine yer verilmiştir. Örneğin; Divriği Ulu Cami ve Darüşşifasının, Mengücekoğlu Ahmet Şah ve karısı Turan Melek tarafından, kuzey taç kapısındaki kitabeye göre, 1228-1229 tarihinde tamamlandığı; mimarının, Tiflisli Ahmed Bin İbrahim olduğu ve ahşap minberi yapanın ise ahşap üzerine yazılı kitabeye göre Tiflisli İbrahim oğlu Ahmet olduğu belirtilmektedir.[26] Aynı şekilde Ahlat mezar taşları, isimleri ve tarihleri belirtmesi açısından veri niteliğindeki belgeler olarak değerlendirilebilir.

Osmanlılar zamanında ise defterler tutulmak suretiyle tüm kurum birimlerinde veriler kayıt altına alınmıştır. Bunlara örnek olarak; nüfus ve şeriye sicilleri, hurufat defterleri gösterilebilir. Yine "ruznamçe defterleri" adı verilen kadı ve müderrislerin tayin, terfi, azil ve yer değiştirme vb. gizli bilgilerinin (kişisel veri olarak) ve her türlü işlemlerinin kaydedildiği defterlerin tutulduğu görülmektedir.[27]

"Hipokrat Yemini" nin kişisel verilerin elde edilmesi ve kullanılmasına yönelik sınırlama içeren bu bağlamda sır saklama yükümlülüğünü tıp doktorlarına yükleyen ilk tarihi metinlerden olduğunu yukarıda belirtmiştik. Günümüzde ise, 1973 yılında

---

25 Çayır, Murat, "Kültepe'den Yerli Bir Tüccara Ait Beş Belge", Archıvum Anatolıcum 7/1, 2004, s. 45-57.

26 http://www.sivas.gov.tr/divrigi-ulu-camii-ve-darussifasi, Erişim Tarihi, 30.11.2019.

27 Alan, Ercan, "Kadıasker Ruznamce Defterlerine Göre XVII. Yüzyılda Rumelide Kaza Teşkilatı ve Kadılar", Güneydoğu Avrupa Araştırmaları Dergisi, Yıl: 2013-1, Sayı: 23, s. 53.

gerçekleştirilen 27. Dünya Tıp Birliği toplantısında da hasta ile doktor arasındaki ilişkideki gizliliğin en temelinde doktorların özel olarak sır saklama borcu ile bireylerin kişisel dokunulmazlığının yattığı ortaya konulmuştur. BM tarafından, dünyada bireylerin insan olmaları dolayısıyla kazandığı en temel haklardan birisi olan mahremiyet hakkını temin etmenin bir gereği olarak "sırların korunması" hakkı kabul edilmiştir.[28]

ABD ve Avrupa Hukuku[29], kişisel verilerin korunması konusunda 1960'lardan beri dünya çapında önde gelen hukuk düzenleri, sistemleri olarak bilinmektedir. Özel hayatın gizliliğinin korunması minvalinde kişisel verilerin korunmasına ilişkin haklar sırasıyla AİHS ve Temel Haklar Şartında güvence altına alınmıştır.[30] Bununla beraber, esas olarak kişisel verilerin korunmasına ilişkin uyuşmazlıkların ve bu alandaki hukuki meselelerin, tarihsel süreç içersinde teknolojinin gelişimine paralel olarak kişisel verilerin otomatik olarak işleme tabi tutulabilmesi aşamasına geldikten sonra ortaya çıkmaya başladığı görülmektedir. Başka bir deyişle, modern dünyada, hem kamu sektörünün hem özel sektörün; bilginin ve verinin toplanması, işlenmesi ve değerlendirilmesinde sağladığı avantajlar nedeniyle otomatik veri işleme kolaylığı sağlayan, sistematik olarak kullanılabilen dijital platformlardan yararlandığı açıktır. Bu sistemler aracılığıyla hem kamu hem özel tüzel ve gerçek kişilerinin elinde, bir çeşit kişileri tanımaya yarayan, onların ayırt edici yönlerini ortaya koyan veri bankası oluştuğu bilinmektedir. Bu verilerin ise günümüz dünyasında kolaylıkla erişilebilir olmaları ve sağlanan bilgiler dikkate alındığında çok yönlü olarak her ortamda kullanılabildikleri müşahede edilmektedir. Özellikle bu veri işleme veya kullanma faaliyetlerine ilişkin endişeler; yetkisiz veri işlenmesi, verilere erişim ve verilerin kötüye kullanılmasına karşı yükselmektedir.[31]

---

28 Başbuğ, Aydın, "Hekimin Yükümlülükleri ve Hukuki Sorumluluğu", Kuzey Kıbrıs Türk Cumhuriyeti, Lefke Avrupa Üniversitesi, 17-18 Mayıs 2010, II. Sağlık Hukuku Sempozyumu, s. 132.

29 Avrupa Hukuku deyiminden: Kıta ve Kara Avrupası devletleri hukuku sistemlerinin yanı sıra AB, AK düzenlemeleri kastedilmektedir.

30 Steven S. McCarty-Snead; Anne TitusHilby, a.g.m., s. 350.

31 Edwards, Lilian, "The Problem with Privacy: A Modest Proposal", International Review of Law Computers&Technology, Volume 18, 2004, s. 316.

Günümüzdeki anlamı ile kişisel verilerin korunması kavramı, 1960 yılından başlayarak ilk olarak ABD'de kendisini göstermiştir. Buradaki kişisel verilere ilişkin tartışmaların temelinde, vatandaşların kredi notunun hesaplanabilmesi amacıyla belli başlı verilerinin bir otomatik sisteme kaydı ile mantıksal sınıflandırma yapabilen bir yazılım vasıtasıyla kredi notunun öğrenilmesine ilişkin veri bankasının oluşturulması yatmaktaydı. Ancak bu alanda itirazlar, toplanan verilerin kimler tarafından işleneceği ve hangi amaçlar için kullanılabileceği hususlarının sabit olmaması nedeniyle yükseldi. Sonuç olarak, büyük bir proje olarak görülen "Ulusal Veri Merkezi" kurma çalışmaları insan haklarının ihlali minvalinde yükselen kamuoyu baskısı ile akamete uğradı.[32]

Yine aynı yıllarda İsveç'te kişilerin nüfus ve vergi bilgilerine ilişkin kapsamlı bir sicil çalışması yapılarak kişilere ilişkin nüfus ve vergi bilgileri ile alakalı bir sicil oluşturulmuştur. Ancak bu çalışmanın yasalaşması 1973 yılında gerçekleşmiştir.[33]

1970 yılına gelindiğinde ise, o zamana dek, dünyada kişisel verilerin korunması hukuku bakımından ilk adımın atıldığı görülmektedir. İlk olarak 1970'te Federal Almanya'da bulunan Hessen eyaleti, verilerin korunması konusunda bir kanun kabul etmiştir. Bu kanunun eyalet seviyesinde kabul edilmesiyle birlikte federal düzeyde tartışmalar başlamıştır. Bu gelişmenin akabinde, 1977 yılında, Almanya'da "Veri Koruma Yasası" kabul edilmiştir.[34] İleride de değineceğimiz üzere, Almanya Anayasa Mahkemesi tarafından 15 Aralık 1983 tarihinde verilen bir kararla, Almanya'da kişisel verilerin korunması hakkı ilk kez anayasal bir hak olarak tanınmıştır. Gelişen teknoloji ve toplumun ihtiyaçları karşısında 2009 ve 2010 yıllarında değişikliğe uğrayan "Veri Koruma Yasası" Almanya'da veri koruma hukukuna yön vermiştir.[35] [36]

---

32 Şimşek, a.g.e., s. 8.

33 Şimşek, a.g.e., s. 10.

34 Kuşkonmaz, Elif Mendos "Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması", Yayınlanmamış Yüksek Lisans Tezi, İstanbul 2013, s. 44.

35 Uyarer, Göçmen Sinem, "6698 Kişisel Verilerin Korunması Kanunu ve 5237 sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması", Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2019, s. 60.

36 Uyarer Göçmen, a.g.e., s. 60.

Bununla birlikte, ulusal düzeyde veri koruma kanununu kabul eden ilk devlet 1973 yılında İsveç olmuştur. Daha sonra kronolojik olarak, 1974 yılında ABD, "Privacy Act" olarak bilinen kişilerin özel alanlarının korunmasına dair kanunu kabul etmiştir. 1977 yılına gelindiğinde ise Kanada veri koruma yasasını çıkarmıştır. 1974 yılında Fransa'da "Safari"[37] adı altında kişilerin bilgilerine otomatik bir sistem vasıtasıyla ulaşmayı, bunları depolama ve tasniflemeyi öngören bir proje ortaya atılmıştır. Bu projenin gün yüzüne çıkmasının akabinde oluşan kamuoyu baskısı ile beraber 1978 yılında ise Fransa ulusal düzeyde, veri korunması konusunda uygulanacak olan Elektronik Veri İşlenmesi, Veriler ve Özgürlük Haklarına ilişkin Kanunu yürürlüğe koymuştur. Fransa'da kişisel verilerin korunması konusu, Türkiye'de olduğu gibi, Fransız Ceza Kanunu çerçevesinde de korunmaktadır. Bu konu ile ilgili ilk olarak, içerisinde kişisel verilerin korunmasına ilişkin maddeler içeren, 6 Ocak 1978 tarihli, "*Bilgi Teknolojisi, Veri Dosyaları ve Sivil Özgürlükler Kanunu"* yürürlüğe girmiştir.[38] Avrupa Birliği Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesi ile birlikte kabul edilen kanun büyük ölçüde değiştirilerek GDPR'ye uyumlu hale getirilmiştir.[39]

Yine aynı yıllarda İsviçre ve İskandinav ülkelerinde yasalaştırma çalışmalarının bir sonucu olarak Danimarka ve Norveç'te bu alanda yasalar kabul edilmiştir. 1979 yılında Luxemburg'da yine aynı şekilde yasa çıkarılmıştır.[40] İsviçre'de kişisel verilerin korunmasına iilişkin ilk düzenleme 1976 yılında, devlet kurumları ve bağlı kuruluşlar arasında verilerin korunması amacıyla "Anayasal Veri Koruma Yönetmeliği" ile yapılmıştır.[41] 1992 yılında ise verilerin korunmasına ilişkin kanun çıkarılmıştır.[42]

---

37 Taştan, a.g.e., s. 2.

38 Uyarer Göçmen, a.g.e., s. 54.

39 Uyarer Göçmen, a.g.e., s. 54.

40 Evans, A.C. "European Data Protection Law", American Journal of Comparetive Law, Cilt:29, Yıl: 1981, s. 572.

41 Özdemir, Hayrunisa, "Elektornik Haberleşme Alanında Kişesel Verilerin Özel HukukHükümlerine Göre Korunması", Ankara Üniversitesi Sosyal Bilimler Enstitüsü,Yayınlanmamış Doktora Tezi, Ankara, 2009, s. 91.

İtalya'da kişisel verilerin korunmasına ilişkin olarak ilk adım 31 Aralık 1996 tarihinde yürürlüğe giren, "Bireylerin ve Diğer Veri Öznelerinin Kişisel Verilerinin İşlenmesine İlişkin Olarak Korunma Kanunu" ile atılmıştır.[43] GDPR'nin de yürürlüğe girmesi ile birlikte, tıpkı Almanya ve Fransa'da olduğu üzere mevcut kanun bir kez daha güncellenmiştir.

İngiltere'de, "Veri Koruma Kanunu" 1984 yılında kabul edilmiş ve 95/46/AT sayılı AB Yönergesine dayalı olarak yapılan değişiklikler sonucu 1998 yılında güncellenmiştir.[44] İngiltere'de kişisel verilerin korunması ile ilgili kurum, ICO (The Information Commissioner's Office/Bilgi Komiserliği Ofisi) Adalet Bakanlığına sadece mali yönden bağlı-ilişkili bir kurumdur.[45]

1983 yılında Kanada'da yürürlüğe giren ve federal hükümet organlarının elinde bulunan kişisel verilerin korunmasına yönelik hükümler içeren "Özel Yaşamın Gizliliği Yasası"nda Federal Veri Koruma Denetçisinin (Privacy Commissioner) görev ve yetkilerini de belirlemektedir. Buna göre Veri Koruma Denetçisi, bu yasa uyarınca yapılan şikayetleri araştırmak ve sonuca bağlamak, federal kurumları denetlemek, hükümetin veri yönetimi uygulamalarına ilişkin değişiklikler ve önerilerde bulunmak; bunlara ilaveten parlamentoya yıllık rapor sunmak konularında yetkili kılınmıştır.[46]

Ancak devletlerin çıkarmış oldukları yasaların yıllar içerisinde toplumun ve bireyin ihtiyaçlarına cevap vermediği görülmektedir. Buradaki temel sebep ise, teknolojinin modernleşmesi ve kişisel verilerin artık rahatça ulaşılabilir hale gelmesi

---

42 Gürpınar, Damla, "Kişisel Verilerin Korunmasından Doğan Hukuki Sorumluluk", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan, Cilt: 19, Özel Sayı: 2017, s. 688.

43 Uyarer Göçmen, a.g.e., s. 68.

44 Habip, Oğuz, "Elektornik Ortamda Kişisel Veriilerin Korunması Bazı Ülke Uygulamaları ve Ülkemizdeki Durum", Uyuşmazlık Mahkemesi Dergisi. 2013;0(3): 1-38.

45 Habip, a.g.m., s. 13.

46 Küzeci, Küzeci, Elif, "Kişisel Verilerin Korunması", Doktora Tezi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilimdalı, Ankara 2010. (Doktora Tezi olarak anılacak), s. 111.

ile birlikte devletlerin yanı sıra özel kurum ve kuruluşların veri depolama sistemlerini kullanmaya başlamasıdır.[47]

Yeni gelişen, dijital platformlar ve otomatik veri işleme sistemleri, şüphesiz, kişisel verilerin korunması sorununu beraberinde getirmiştir. Özellikle yetkisiz veri işlenmesi, verilere erişim ve verilerin kötüye kullanılmasına karşı bu sistemlerden ve internet kullanımından kaynaklanan kaygılar günümüz dünyasında giderek yükselmiştir. Bu kaygı ve endişelere paralel olarak, uluslararası örgütler ve devletler, kişisel verilerin korunmasına ilişkin olarak tarih içerisinde birtakım düzenlemeleri yürürlüğe koymaya başladılar. Bunu yaparken özellikle kişisel verilerin ne olduğu, onları toplamak için kimlerin nasıl yetkilendirilebileceği, verilerin toplanma amacı, sınırlama ve istisnalar gibi bazı kişisel verileri koruma hukukuna özgü müesseselerin ortaya çıktığı görülmektedir.

1980'li yıllara gelindiğinde ise, devletlerin yukarıda bahsedilen, bu tek taraflı kişisel verileri koruma çabalarının yerini artık yavaş yavaş uluslararası kuruluşların çabalarının aldığı ve bu alanda uluslararası kuruluşların hukuki metin ortaya koyduklarını görmekteyiz. Bu bağlamda uluslararası kuruluşların[48] kişisel verilerin korunmasına yönelik şu kronolojik sıra göze çarpmaktadır:

- **23 Eylül 1980** tarihinde → OECD tarafından çıkartılan Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri,
- **28 Ocak 1981 tarihinde**→ Avrupa Konseyi'nin 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi,
- **14 Aralık 1990 tarihinde**→ BM tarafından çıkartılan Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri

47 Küzeci, Elif, Kişisel Verilerin Korunması, 3. Baskı, Seçkin Yayınevi, Ankara, 2019, s. 111.

48 Bu kuruluşların çalışmalarına ilişkin ayrıntılı açıklama bir sonraki bölümde yapılacağından burada yüzeysel olarak değinilmiştir. Ayrıca AİHS, 1950 yılında kabul edilmekle beraber doğrudan kişisel veriler ile ilgili bir düzenleme içermediğinden bu kronolojik sıralamaya dahil edilmemiştir.

- **25 Ekim 1998 tarihinde→** 95/46/AT sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi,
- **8 Kasım 2001 tarihinde→** Avrupa Konseyi'nin 181 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol,
- **Nisan 2016 tarihinde→** AB'nin 2016/679 AB VKD; Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR olarak anılacaktır.).

20. yy. teknoloji ve iletişim alanında birçok yenilik getirdi. Bu yüzyılda iletişim konularını içeren bilişim (enformatik) ve bilgisayar sistemleri açısından baş döndürücü bir şekilde teknolojik gelişme yaşandı. Teknolojinin bu hızlı gelişim ve dönüşümü, kişilere ait olan verilerin toplanması, derlenmesi ve bunların analiz edilerek ilgili kişi hakkında bir kanaate varılmasını -GDPR'de belirtildiği üzere profil çıkarma[49] işlemi- kolaylaştırmıştır. Bu gelişmelerin insanlara kolaylık sağlamasının yanı sıra olumsuz etkilerinin bulunduğu yadsınamaz bir gerçek halini almıştır. Dijital bilgisayar sistemlerinin, yapay zekâ içeren yazılımların ortaya çıkması ve bunların kişisel verilere ihtiyaç duyan kamu ve özel sektör otoritelerinde kullanılması ile birlikte, kötü niyetli kişilerin başkalarının verilerine erişmeleri çok kolay bir hal aldı. Aynı şekilde, sosyal medya dahil olmak üzere otomatik bilişim sistemi ve dijital platformların hızlı bir şekilde büyümesi ve insanoğlunu kuşatması, üçüncü kişiler açısından, doğum tarihi-yeri ve kimlik numarası gibi video, ses, fotoğraf ya da daha fazla kişisel verileri içeren bilgiye kolayca ulaşmayı artık mümkün kılmaktadır.[50]

Görüldüğü üzere ilk çağlarda basit bir yemin veya teolojik kurallara, dolayısıyla toplumsal ve yaptırımı olmayan kurallara bağlanan kişisel verileri koruma hukukunun,

---

49 GDPR'de profil çıkarma kavramı: "*bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere söz konusu gerçek kişiye ilişkin belirli kişisel özelliklerin değerlendirilmesi için kişisel verilerin kullanımını ihtiva eden her türlü otomatik kişisel veri işleme biçimi*" şeklinde ifade edilmiştir.

50 Kılıç, Doğan, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 61, Sayı:3, Yıl: 2012, s. 1090-1092.

tarihsel süreç içersinde, özellikle 1980'li yıllardan sonra uluslararası ve ulusal alanda devletleri ve kişileri ilzam eden hukuk kuralları oluşturulması yoluna gidilerek bu kuralların ihlal edilmesi halinde uygulanacak yaptırımlar belirlenmiştir.

Ülkemizde ise, kişisel verilerin korunması hukukunun çok köklü bir geçmişi olmamasına rağmen, Avrupa Konseyi'nin kurucu üyesi olan ülkemiz açısından 108 sayılı sözleşmenin imzaya açılmasından bu yana, kişisel verileri koruma hukukunun gündemde olduğunun kabulü gerekir. Avrupa Konseyi'nin 108 sayılı sözleşmesinin yanı sıra Türkiye'nin, üye olmamasına rağmen AB tarafından çıkartılan 95/46/AT sayılı Yönergenin ve GDPR'nin, KVKK üzerindeki etkisi olduğu genel kabul gören bir gerçektir. Ayrıca kişisel verilerin korunmasını isteme hakkı, 2010 anayasa değişikliği ile anayasal bir hak olarak 1982 Anayasası'na dercedilmiştir. Bu bağlamda ülkemizdeki kişisel verilerin korunmasına ilişkin kronolojik sıraya bakacak olursak;

- 12 Ekim 2004 tarih ve 5237 sayılı Türk Ceza Kanunu'nda yapılan düzenlemeler,
- 12 Eylül 2010 tarihinde özel hayatın gizliliğine ilişkin hakkın devamına kişisel verilerin korunması ile ilgili hükmün 1982 Anayasası'na eklenmesi,
- 17 Mart 2016 tarihinde 108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin TBMM tarafından onaylanarak Türk hukukuna dahil edilmesi,
- 7 Nisan 2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun Cumhurbaşkanı tarafından 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmesi,
- 05 Mayıs 2016 tarihinde 181 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınıraysan Veri Akışına İlişkin Protokolün TBMM tarafından onaylanarak Türk hukukuna dahil edilmesi,

olarak göze çarpmaktadır.[51]

[51] Esasen Türk hukukunda kişisel veriler ile alakalı pek çok düzenleme bulunmasına rağmen burada doğrudan kişisel verileri koruma hakkına yönelik olan düzenlemeler kronolojik sıralamaya dahil edilmiştir.

Bunlara ek olarak; ülkemizde 1136 sayılı Avukatlık Kanunu'nda *"sır saklama"* başlığını taşıyan 36. madde ile avukatlara, kendilerine tevdi edilmiş olan ya da hem avukatlık görevleri hem de TBB ve baroların hizmet birimlerindeki diğer görevleri nedeniyle öğrenmiş oldukları bilgileri açığa vurmama yasağı getirilmiştir.[52]

1512 sayılı Noterlik Kanunu'nda *"meslek sırrı"* başlığını taşıyan 54. m.'de ise gerek noterin gerekse noterlik katiplerinin görevleri nedeniyle öğrenmiş oldukları sırları, yasaların açıkça emrettiği durumlar haricinde açıklayamayacakları kuralı getirilmiştir.[53]

213 sayılı Vergi Usul Kanununa göre *"Vergi muameleleri ve incelemeleri ile uğraşan memurlar, vergi mahkemeleri, bölge idare mahkemeleri ve Danıştay da görevli olanlar, vergi kanunlarına göre kurulan komisyonlarına iştirak edenler ve vergi işlerine kullanılan bilirkişiler, görevleri dolayısıyla vergi mükellef ve sorumlularının veya onlarla ilgili kişilerin şahıslarına, muamele ve hesaplarına, işlerine, işletmelerine, servetlerine veya mesleklerine dair olmak üzere öğrendikleri sırları veya gizli kalması lazım gelen diğer hususları açıklayamazlar ve kendilerinin veya üçüncü şahısların yararına kullanamazlar."* hükümlerine yer verilerek vergi mahremiyetine uymaya mecbur olanlar sıralanmıştır.[54]

1211 sayılı Türkiye Cumhuriyeti Merkez Bankası Kanunu'nun 35'inci m.'si ile Merkez Bankası mensuplarının, sıfat ve görevleri nedeniyle hem Bankaya hem de Banka ile ilişkisi bulunan kişi ile kurumlara ilişkin bilinen sırların gizliliğine uygun davranmak ve söz konusu sırları yasaların yetkili kıldığı makamlardan başkasına herhangi bir şekilde açıklamama yükümlülüğü getirilmiştir.[55]

---

52 Avukatlık Kanunu (1969), 07/04/1969 tarihli ve 13168 sayılı Resmi Gazete.

53 Noterlik Kanunu (1972), 05/02/1972 tarihli ve 14090 sayılı Resmi Gazete.

54 Vergi Usul Kanunu (1961), 10/01/1961 tarihli ve 10703 sayılı Resmi Gazete.

55 Türkiye Cumhuriyeti Merkez Bankası Kanunu (1970), 26/01/21970 tarihli ve 13409 sayılı Resmi Gazete.

Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik'in 17'nci maddesinde, kurul üyeleriyle, kurul başkanının lüzum görmesi hallerinde, kurul toplantısına yahut hazırlık faaliyetlerine katılan kişiler için, faaliyetler esnasında gerek ilgililere gerekse üçüncü kişilere dair öğrenilen sırlara ilişkin, bu konuda yasa ile yetkilendirilen merciler hariç, açıklama yasağı öngörülmekte ve hatta söz konusu yükümlülüğün bu kişilerin görevlerinden ayrılmasının ardından da devam edeceği belirtilmektedir.[56]

1.3. ULUSLARARASI METİNLER

1.3.1. OECD

Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) sözleşmesi 1960 yılında imzalanmıştır. OECD; finansal istikrar, ekonomik iş birliği, demokrasi ve insan hakları kavramları üzerine inşa edilmiş bir kuruluştur.[57] Ülkelerin birbirleri ile olan entegrasyonunu ve uluslararası ticaretin gelişmesini savunan bir kuruluş olarak hiç şüphesiz kişisel verilerin korunması OECD için kaçınılmaz olarak ele alınması gereken konuların başında gelmektedir.

Bu bağlamda, OECD'nin 1980 yılında yayımladığı, **"Kişisel Verilerin Sınır Aşan Trafiği ve Kişisel Verilerin Korunmasına İlişkin Kılavuz İlkeler"**, veri koruması hukuku alanında ilk uluslararası metindir. Belgenin hukuki niteliğine baktığımızda bir tavsiye kararından öteye gidemediği görülmektedir. Bu bakımdan belgenin hukuki olarak bağlayıcılığından söz etmek mümkün değildir. Ama yine de bu belgenin ayırt edici özelliği, temel ilkeleri içermesi nedeniyle veri koruma konusunda hiçbir düzenlemenin bulunmadığı ülkeler için bir kılavuz niteliğinde

---

56 Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik, 16/11/2017 tarihli ve 30242 sayılı Resmi Gazete.

57 OECD demokratik bir yapıya sahip ve piyasa ekonomisine önem veren 36 devlet tarafından dünyada hızlı bir şekilde gerçekleşen küreselleşmenin ekonomik, sosyal ve idari problemlerine çözüm üretmek ve bu sürecin sunduğu fırsatlardan yararlanmak üzere oluşturulan devletlerarası bir uluslararası örgüttür. Avrupa Birliği ile ABD, Kanada bu örgüte üyedir. Türkiye de bu örgütün kurucu üyelerinden birisidir. http://www.oecd.org/ , Erişim tarihi, 02.02.2018.

olmasıdır.[58] Diğer bir deyişle, bu rehberin, kişisel verilerin korunması hukuku alanıda çerçeve metni oluşturarak, dünya çapında bu hukuki alanın kodifiye edilmesi sürecinde bir köşe taşı vazifesi gördüğünü söyleyebiliriz.

OECD, ilgili rehberin 7. ve 14. maddeleri arasında toplam sekiz adet temel ilke belirlemiştir. Bu ilkeler[59];

- Veri toplama işleminin sınırlı olması ilkesi,
- Açıklık (şeffaflık) ilkesi,
- Verilerin kaliteli olması ilkesi,
- Veri kullanımın sınırlanması ilkesi,
- Veri güvenliğini sağlama ilkesi,
- Amacın belirliliği ilkesi,
- Bireyin katılımı ilkesi,
- Hesap verilebilirlik ilkesi,

Bu ilkelerin, pek çok ülkeye ilham kaynağı olduğunu söylemek mümkündür. Söz konusu ilkeler, kişisel veri hukukunun ulusal alandan çıkarak uluslararası alanda tartışılmaya başlandığının göstergesidir. Öte yandan kuruluşa üye olan devletler göz önünde bulundurulduğunda, bu ilkelerin saptanmasında tüm dünya genelinde ekonomik refah ve demokrasi açısından ileri gitmiş olan ülkelerin katılımı ile yani geniş tabanlı bir katılım ile objektif ilkelerin belirlendiği görülmektedir. Bu husus kuşkusuz belgenin niteliğini ve saygınlığını artıran bir unsur olarak karşımıza çıkmaktadır.

Teknolojideki ve iletişimdeki hızlı büyüme ile birlikte, bu düzenlemenin, yüksek düzeyde korumaya ihtiyaç duyan günümüz dünyasına uyarlanması kaçınılmaz hale gelmiştir. Bu nedenle OECD, bu belgeyi 2013 yılında güncellemiştir. OECD

---

58 Gürsel, İlke, "Protection of Personal Data in International Law and The General Aspects of TheTurkish Data Protection Law", DEÜHF Dergisi, C. 18, S. 1, 2016, (Basım Yılı: Ekim 2016), s. 4.

59 https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.html, Erişim tarihi, 02.02.2018.

kılavuzları bugün bile OECD üyesi olan ya da olmayan ülkeler için özel ve dikkate değer etkiler yaratmaktadır.[60]

Sonuç olarak, uluslararası alanda, OECD gibi geniş katılımlı ve ülkelerin birbirleri ile olan entegrasyonunu ekonomik ve özellikle ticari alanda savunan bir kuruluşun, kişisel verileri koruma hukukuna ihtiyaç olduğunu bildiren, bu alana ilişkin genel bir çerçeve çizerek belli başlı prensipleri belirleyen tavsiye niteliğinde dahi olsa rehber ilkeleri yayımlaması, bu alana olan ilginin hem küresel çapta hem de devletlerin iç hukukunda artmasına sebebiyet vermiştir.

1.3.2. BİRLEŞMİŞ MİLLETLER

Bilindiği üzere ikinci dünya savaşının dünya toplumları üzerinde yarattığı tahribatın tekrar yaşanmaması için 24 Ekim 1945 tarihinde Birleşmiş Milletler kuruldu. Bu uluslararası kuruluşun halihazırda 190'ı aşkın üyesi bulunmaktadır.[61]

Başkalarının tecavüzüne karşı -ki buna Devlet de dahil olmak üzere- bireyin özel alanının korunması konusu, kuruluşundan bu yana BM için önemli konuların başında gelmektedir. Bu nedenle BM, 1948 tarihli İnsan Hakları Evrensel Beyannamesi'ni (İHEB) yürürlüğe koymuştur. Bu evrensel metnin 12. maddesinde, özel yaşamın gizliliği düzenlenilmek suretiyle özel hayat ile birlikte aile hayatının da korunmasına net bir şekilde vurgu yapılmıştır. Bu maddeye göre, hiçbir kimsenin, özel yaşamı, ailesi, konutu ya da haberleşmesi gibi çekirdek alanlarına keyfi olarak müdahalede bulunulmamalıdır. Ayrıca kimse onur ve şöhretine yönelik saldırılara maruz bırakılmamalı ve bu tür saldırılara karşı herkes korunmalıdır. Bu tür müdahale ve saldırılara karşı korumanın yasal güvence altına alınması devletler açısından bir yükümlülüktür. Ayrıca belirtmek gerekir ki bu maddenin temel ayırt edici özelliği, bireyin korunması gereken alanlarına ilişkin uluslararası ve ulusal alanda düzenlenmesi gereken yasal metinlerin gerekliliğini ortaya koymak olmuştur. Başka bir deyişle, BM'nin insan hakları ile ilgili bu düzenlemeleri devletler ve uluslararası

60 http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, Erişim tarihi, 05.02.2018.

61 https://www.un.org/en/about-un/, Erişim tarihi, 05.02.2018.

kuruluşlar başta olmak üzere tüm dünya kurumlarını temel haklar alanında düzenleme yapma konusunda etkileyerek teşvik etmiştir.[62]

1966 yılına gelindiğinde Birleşmiş Milletler tarafından Medeni ve Siyasi Haklar Sözleşmesi hazırlanarak imzaya açılmıştır. Adı geçen 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."*

denilmek suretiyle insan hakları beyannamesine paralel bir düzenleme getirildiği görülmektedir. Burada kişisel verilerin korunması hukuku açısından önemli olan husus ise, BM İnsan Hakları Komitesinin getirmiş olduğu içtihat ile kişisel verilerin gizliliği hususunun özel yaşamın korunması hakkına eklemlenerek koruma alanına alınması yönünde görüş bildirmesi olmuştur.[63]

BM tarafından kişisel verilerin korunması hukuku alanında atılan en önemli adım ise 1990 yılında, Genel Kurul *"**Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesi Rehber İlkeleri**"* adlı BM kılavuzunu kabul etmesi olmuştur. Bu kılavuz, tavsiye niteliğinde olan dokuz temel ilkeyi kapsamaktadır. Bu ilkeler şunlardır:

- hukuka uygun ve dürüst yollardan verilerin toplanması ve işlenmesi ilkesi,
- doğruluk ilkesi,
- amaç-özellik ilkesi,
- ilgili kişinin erişiminin sağlanması ilkesi,
- bireyler arasında ayrımcılık yapılmaması ilkesi,

---

62 Council of Europe, "Handbook on European Data Protection Law", European Union Agency for Fundamental Rights, 2014, s. 14.

63 Gemalmaz, Mehmet Semih, "Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş", 2013, Cilt:1, s. 434.

- istisna yapma yetkisi,
- güvenlik ilkesi,
- denetim ve yaptırımlar,
- sınır ötesi veri akışı, şeklinde belirlenmiştir.[64]

Bu ilkelerin uygulamasını denetlemek üzere bağımsız yapıya haiz yetkili bir veri koruma kuruluşunun oluşmasını öngören ilk belge olması açısından bu rehber ilkeler kılavuzu ayrı bir öneme sahiptir.[65]

Kişisel verilerin korunması hukukuna ilişkin olarak, 1940'lı yıllardan 2000'li yıllara kadar evrilen süreç içerisinde, kuşkusuz uluslararası diplomasi ve politikalara yön veren kuruluşların başını çeken BM'nin özel hayatın gizliliği, kişilik haklarının korunması ve bilgisayarlı sistemlere geçirilmiş olan bireylere ilişikin verileri koruma hususlarında gösterdiği hassasiyetin teknolijk gelişmelere endeksli olarak arttığını görmekteyiz. BM'nin bu alana ilişkin en kayda değer katkısının ise özerk bir yapıya sahip olan denetim kuruluşunun üye devletlerce ihdas edilmesini öngörmesi olmuştur.

1.3.3. AVRUPA KONSEYİ

1.3.3.1. Genel Olarak

1949 yılında kurulan Avrupa Konseyi; insan hakları, demokrasi ve hukukun üstünlüğü kavramlarının üzerine bina edilmiş olan uluslararası bir kuruluştur. Türkiye, AK'nın kurucu üyeleri arasında bulunmaktadır. 1950 yılında, AK, kişilerin özel yaşamı ve aile hayatı, evi ve çevresine ilişkin hakları tanımlayan düzenlemeleri barındıran, muadillerinden ve önceki uygulamalara göre hukuki koruması daha yüksek olan Avrupa İnsan Hakları Sözleşmesi'ni (AİHS) kabul etmiştir.[66]

AİHS'nin 8. maddesinde "*özel yaşam ve aile hayatına saygı*" hakkı düzenlenmektedir. Belirtmek gerekir ki, "kişisel verilerin korunması" hakkı konusunda sarih bir düzenleme sözleşmede bulunmamaktadır. İlk bakışta

64 http://www.refworld.org/docid/3ddcafaac.html, Erişim tarihi, 06.02.2018.

65 Küzeci, a.g.e., s. 136.

66 McKay, Cunningham, "Complying with International Data Protection Law", 84 University of Cincinnati Law Review, 421, 2016, s. 426.

(primafacie), bu bir eksiklik olarak görülebilir. Ancak, veri koruma alanında artan endişeleri dikkate alan AİHM, kişisel verilerin kötüye kullanılmasına yönelik şikâyetlerin engellenmesi amacıyla bu maddeyi geniş yorumlayarak kişisel verilerin korunması hususunda bu maddeyi, meşru zemin, sözleşmedeki dayanak noktası haline içtihatı ile getirmiştir.[67]

1980'li yıllarda, Avrupa Konseyi Bakanlar Komitesi tarafından verilerin korunmasına ilişkin olarak pek çok tavsiye kararı alınmıştır. Bu tür gelişmeler, 1981 yılında, ***"108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireyin Korunması"*** adı verilen sözleşmenin tanzim edilmesine ve imzaya açılmasına yol açtı. Günümüzde bu sözleşme, hukuki olarak bağlayıcılığı olan tek uluslararası belge olması nedeniyle veri koruma hukuku alanındaki hayati rolünü korumaktadır. Bu sözleşmenin yürürlüğe konmasındaki amacın, AİHS'nin 8. maddesinde belirtilen ana hatları uygulamak ve veri koruma hukuku alanında daha spesifik güvenceler sağlamak olduğunu söyleyebiliriz. Genel olarak sözleşmeye baktığımızda, sözleşmede belirlenen hakların uygulanmasına yönelik kısıtlamalar, ancak devletin güvenliği, kamu düzeni gibi genel geçer menfaatlerin tehlikeye maruz kalması durumunda gündeme gelebilecektir.

Sözleşmenin uygulanmasına gelince, AB'nin tüm üyeleri 108 sayılı sözleşmeyi kabul etmişlerdir. Bununla beraber sözleşme AK'ya üye olmayan devletlerin de imzasına yani katılımına açıktır. Bu sözleşmeye ek olarak, 2001 yılında, AK üyesi olmayan ülkelere sınır ötesi veri akışını düzenleyen ve buna ek olarak ülkeler bazında bağımsız idari otorite kurularak ülke içindeki kişisel verilerin korunmasını izleyen ve denetleyen kurumların kurulması zorunluluğunu içeren 108 sayılı Sözleşmeye 181 sayılı Ek protokol düzenlenmiştir.[68]

108 sayılı sözleşmenin temel amacı, gerçek kişilerin korunmasıdır. Ancak, sözleşme, her devletin hukuk düzeninde gerçek kişilerin yanı sıra tüzel kişilere teşmil

---

67 AİHM Kararı, M.S. v. Sweden, Başvuru No: 20837/92, Tarih: 27.08.1997. Kararın İngilizce tam metni için bkz. http://www.hrcr.org/safrica/privacy/ms_sweden.html, Erişim tarihi, 06.02.2018.

68 https://www.kisiselverilerinkorunmasi.org/mevzuat/kisisel-verilerin-otomatik-isleme-tabi tutulmasi-karsisinda-bireylerin-korunmasi-sozlesmesine-ek-denetleyici-makamlar-ve sinirasan-veri-akisina-iliskin-protokol-181 sayili-ek-protokol/, Erişim tarihi, 06.02.2018.

edilmesine engel değildir.[69] Zira verilerin korunmamasından kaynaklanan sorunlara yalnızca gerçek kişilerin düçar olacağının ileri sürülemeyeceği gibi bu korumanın sadece gerçek kişiler ile sınırlandırılması düşünülemez. Bu hususta, doktrinde, bazı yazarlar tarafından, örneğin, tek kişilik şahıs şirketi gibi bazı tüzel kişilikler düşük koruma gerektirirken; bazı politik ve dini yapıya haiz oluşumların ve sendikal örgütlenmelerin daha fazla korumaya ihtiyaç duyduklarını ileri sürmüştür.[70] Öte yandan, özel yaşamın sadece gerçek kişilerle ilgili olması nedeniyle, tüzel kişiliğe ilişkin bilgilerin, veri olarak kabul edilmemesi gerektiğine ilişkin bazı görüşler bulunmaktadır. Bu görüşlerin temelinde, bu türden tüzel kişilere ilişkin bilgilerin ticari sır olarak kabul edilebileceği yatmaktadır.[71]

1.3.3.2. 108 SAYILI SÖZLEŞME

1.3.3.2.1. Tarihçesi

Kişisel verilerin korunması konusu, AK'nın gündemine 1960'lı yıllarda gelmiştir. AK'da bilişim alanında gelişmekte olan teknolojiye karşı verilerin korunması alanında mevcut hukuk düzeninin yetersizliği hususunda giderek artan bir endişe vardı. Bu kaygının temel sebebi ise kişisel verilerin kapsamlı bir şekilde hem kamu sektörü hem özel sektör tarafından otomatik olarak işlenmesinden kaynaklanıyordu.[72] Bu tür gelişmelerin bir sonucu olarak, ilk olarak Bakanlar Komitesi, 1968[73] yılında kişisel verilerin korunmasını[74] ele almak üzere toplanmıştır. Bahse konu tarihten itibaren Bakanlar Komitesi, özel hayatı ve kişisel verileri korumak için çaba sarf etmeye başlamıştır. Bu çabaların bir sonucu olarak, kişisel verilerin daha

---

69 CoE, "Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personaldata, regarding supervisory authorities and transborder data flows", CETS No. 181, 2001.

70 Douwe, Korff, "Study On The Protection Of The Rights And İnterests Of Legal Persons With Regard To The Processing Of Personal Data Relating To Such Persons" Commission of The European Communities (StudyContract ETD/97/B5-9500/78), Final Raporu, s. 42-44, https://poseidon01.ssrn.com/delivery.php?ID, pdf, Erişim tarihi, 06.02.2018.

71 Tezcan, Durmuş, "Bilgisayar Karşısında Özel Hayatın Korunması", Anayasa Yargısı, S. 8, 1991, s. 389.

72 Graham, Pearce/Nicholas, Platten, "Achieving Personal Data Protection in the European Union", Journal of Common Market Studies, S. 36, December 1998, s. 531.

73 A.C. Evans, a.g.m., s. 572.

74 Fritz H. Grupa/William Kuechler/ScottSweeney, "Dealing with Data Privacy Protection: An Issue for the 21st Century", LawInvestigations andEthics, January/February 2002, s. 46.

iyi bir şekilde nasıl korunacağı konusunda tavsiyelerde bulunması planlanan bir uzmanlar komitesi oluşturulmuştur. Uzmanlar komitesinin çalışmaları neticesinde, Bakanlar Komitesi 1973 ve 1974 yıllarında arka arkaya ***"Özel Sektörde Elektronik Veri Bankalarına Karşı Kişisel Mahremiyetin Korunması Hakkında 73/22 sayılı Karar"*** ile ***"Kamu Sektöründe Elektronik Veri Bankalarına Karşı Bireylerin Korunması Hakkında 74/29 sayılı Karar"*** olmak üzere iki düzenleyici kararı kabul etmiştir. Bu kararların esas konusu dijital banka işlemlerini asgari standartlarda korumak olmuştur. Ancak bu kararların 108 sayılı Sözleşme için hazırlayıcı metin niteliğinde oldukları da kabul edilmektedir.[75]

1981 yılına kadar uzmanlar komitesi tarafından hazırlanan taslak sözleşme metni Bakanlar Komitesi tarafından kabul edilmiş ve yukarıda belirtildiği şekilde, **"*Kişisel Verilerin Otomatik İşlenmesine İlişkin 108 sayılı Sözleşme*"** olarak adlandırılmış ve imzaya açılmıştır. Sözleşmenin 22/2[76] maddesine göre, sözleşmenin yürürlüğe girmesi için sözleşmenin en az 5 ülke tarafından onaylanması gerekiyordu. Bu nedenle, Federal Almanya'nın onay beyanını takiben, 108 sayılı sözleşmenin yürürlüğe girmesi 1985 yılında gerçekleşti. Her ne kadar sözleşme etkili bir koruma içermese de, ayırt edici özelliği uluslararası düzeyde ilk bağlayıcı hukuki metin olmasıdır.[77]

Söz konusu sözleşmenin yürürlüğe girmesinin ardından, Bakanlar Komitesi, bu sözleşmeye katılması için Avrupa Konseyi üyesi olmayan herhangi bir Devleti davet etmeye yetkili kılınmıştır. Ancak, bunu gerçekleştirmek için, davet hususunda, sözleşmedeki taraf devlet temsilcilerinin oybirliği ile almış olduğu bir karar olması gerekmektedir.[78]

---

75 Colin J. Bennett/Charles D. Raab, "TheGovernance of Privacy Policy Instruments in Global Perspective", Ashgate Publishing Company, England, 2004, s. 72.

76 108 s. söz., m. 22.

77 Sözleşmenin kabul tarihi 28 Ocak, Avrupa Konseyi tarafından "veri koruma günü" olarak ilan edilmiştir. https://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/Default_DP_Day_en.asp#TopOfPa.g.e, Erişim tarihi, 08.02.2018.

78 108 s. söz., m. 20-23.

Bugüne kadar, AK üyesi tüm ülkeler sözleşmeyi onaylamış bulunmaktadır. Ayrıca, üye olmamasına rağmen, dört ülke -Mauritius, Senegal, Tunus ve Uruguay- sözleşmeyi imzalamıştır.[79]

Öte yandan sözleşme ile ilgili önemli bir diğer husus ise, 2001 yılında sözleşmeye ek protokolün taraf devletlere imzaya açılması olmuştur. Bu protokole uygun olarak, tüm taraf devletlerin, kişisel verilerin sözleşmenin öngördüğü seviyede korunduğunu denetlemek üzere kendi ulusal hukukları kapsamında bir otorite ihdas etmeleri gerekmektedir. Aksi takdirde, protokol, o ülkeden başka herhangi bir ülkeye veya uluslararası kuruma veri akışı oluşturmasını yasaklamaktadır. Diğer bir ifadeyle, artık 108 sayılı sözleşme denetleme kurumlarını zorunlu kılmıştır. Bu otoriteler, 108 sayılı sözleşme uyarınca aynı ilkeler ve standartlar etrafında faaliyet göstermelidir.[80] Protokol 2004 yılında yürürlüğe girmiştir ve şu ana kadar, 40 ülke bu protokole onay vermiştir.[81] Nitekim bu ek protokole taraf olmanın bir gereği olarak Türkiye Cumhuriyeti, "Kişisel Verileri Koruma Kurumu"nu Adalet Bakanlığının ilgili kuruluşu olarak hayata geçirmiştir.[82]

1.3.3.2.2. Sözleşmenin Amacı ve Kapsamı

Sözleşmenin esas amacı; vatandaşlık veya mukim olma hususunu gözetmeksizin, her bir taraf devletin hükümranlığındaki bireylerin, hem kamu sektörü hem özel sektör tarafından işlenen verilerini güvence altına almanın yanı sıra; kişisel verilerin otomatik bir şekilde işlenmesi temelinde temel hak ve hürriyetlere özellikle de mahremiyetlerine saygı göstermek şeklinde sözleşmede tanımlanmıştır.[83] Sözleşme, taraf ülkelerde ikamet eden herkese otomatik işlemlerde kişisel verilerin korunması alanında güvence sağlamaktadır. Bu itibarla, sadece insan unsuru kullanılarak ve otomatik bir sistem veya herhangi bir elektronik, dijital sistem kullanmadan işlenen veriler kapsam dışında kalmaktadır. Fakat ileride değinileceği

---

79 https://www.coe.int/en/web/conventions/full-list/-conventions/treaty/108/signatures?p_auth=gXtFjq5a,Erişim tarihi, 08.02.2018.

80 Handbook on European Data Protection Law, a.g.e., s.115.

81 https://www.coe.int/en/web/conventions/full-list/ /conventions/treaty/181/signatures?p_auth=gXtFjq5a, Erişim tarihi, 08.02.2018.

82 https://kvkk.gov.tr/ Erişim tarihi, 08.09.2018.

83 108 s. söz. m.1.

üzere sözleşme, otomatik olarak işleme kavramından verinin işlemesine ilişkin herhangi bir safhanın otomatik işleme metotlarından biri ile yapılmasını yeterli görmektedir.[84]

Başka bir anlatımla, netice itibarıyla, sözleşmenin, biri özel yaşamı korumak diğeri ticaret ve ticarete yönelik dezavantajlarını ortadan kaldırılmasını gerektiren sınır ötesi serbest veri akışını sağlamak olan iki ana amacının olduğunu söylemek yanlış olmayacaktır.[85]

Sözleşmenin bir diğer amacı olarak görülebilecek bir husus m. 4'te belirtildiği üzere, taraf devletlerin bu sözleşmede belirtilen temel ilkeleri gözeterek kendi iç hukuklarında yasalaşma sürecini tamamlamaları ve bağımsız bir idari denetim mekanizmasının kurulmasının temini olarak belirtilebilir.[86] Kanaatimizce, bu hususlar, hem bir amaç hem de yükümlülük olarak görülebilir. Nitekim Türkiye'nin bu yükümlülüğün bir gereği olarak bağımsız idari otorite olarak KVKK'yı ihdas ettiğini belirtmiştik.

Genel olarak sözleşme, verilerin toplanması ve işlenmesinden başlayarak kişisel verilerin akışının düzenlenmesini, verilerin yanlış kullanılmasına karşı korunmasını amaçlamaktadır. Yine sözleşme hukuki olarak verilerin toplanması ve otomatik işleme tabi tutularak saklanmasında dikkat edilecek hususları belirlemektedir. Ayrıca, kişisel verilerin toplanmasını gerektiren hukuki bir sebep ve bu sebebe uygun bir şekilde toplanan verilerin kullanılması usul ve esaslarını düzenlediği görülmektedir. Diğer taraftan, sözleşme, yasal güvencelerin yokluğunda hassas kişisel verilerin toplanmasını açıkça yasaklamaktadır. Yine sözleşme kişinin kendisine ait toplanmış bir verinin düzenlenmesi ve düzeltilmesini isteme hakkını bireye tanımaktadır.[87]

---

84 Atak, Songül "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", TBBD, S.87, 2010, s. 95.

85 A.C. Evans, a.g.m, s.578.

86 Bkz.. 108 s. söz. m.4.

87 Handbook on European Data ProtectionLaw, a.g.e., s.16.

108 sayılı sözleşme, kişisel verilerin işlenmesi konusunda, gerçek kişilere ait kişisel verilerin gerek özel sektörde gerekse kamu sektöründe işlenmesi işlemlerini içermektedir. Buradan anlaşıldığı üzere, uygulama alanı tüzel kişilere veya kuruluşlara uygulanmasına izin vermeyecek şekilde dar tutulmuştur. Yine, otomatik olarak işlenmeyen kişisel veriler, korunması gereken bilgiler olarak ele alınmamaktadır. Bununla beraber, taraf devletler, sözleşmeden daha kısıtlayıcı ve geniş bir koruma içeren hükümler kendi iç hukuklarında uygulayabilirler.[88] Yani gerçek kişilerin yanı sıra, kendi iç hukuklarında tüzel kişilere ait verilerin korunmasını da hüküm altına alabilirler. Sözleşmede bu hususta herhangi bir kısıtlayıcı hüküm bulunmamaktadır.[89]

1.3.3.2.3. Sözleşmede Belirtilen İlkeler

Kişisel verilerin toplanmasına ilişkin temel ilkeler, 108 sayılı sözleşmenin 5. m.'sinde belirtilmiştir. Bu maddeye göre otomatik işlem gören kişisel veriler;

- adil ve hukuka uygun olarak elde edilerek işlenmeli,
- belirtilen meşru amaçlar doğrultusunda saklanmalı ve söz konusu amaçlarla bağdaşacak şekilde kullanılmalı,
- elde edilen veri, toplanmasını gerektiren amaç ile ilgili olmalı ve bu amaç ile ölçülü olacak şekilde toplanmalı,
- veri, doğru ve güncel olmalı,
- veriler depolandığı amaç için gerekli olduğu kadar muhafaza edilmiş olmalıdır.

Özel veri kategorilerinde sayılan hassas verilerle ilgili olarak, 6. m. uyarınca ırk, köken, siyasi görüş, dini inanç, sağlık, cinsel yaşamla ilgili verilerin yanı sıra cezai mahkumiyetlerle ilgili verilerin toplanmaması ve saklanmaması hükmünü amirdir.[90] Bununla birlikte, ülkelerin kendi iç hukukları, hassas veriler açısından hukuki olarak yeterli koruma sağlıyorsa, o zaman hassas veriler işlenebilir. Öte yandan, otomatik veri dosyalarında saklı bulunan kişisel verilerin yanlışlıkla veya yetkisiz bir şekilde imha

88 108 s. söz., m.11.

89 Tapper, Colin, "New European Directions in Data Protection", Journal of Law, Information and Science, Sayı: 9, 1992, s.11.

90 108 s., söz. m. 6.

edilmesine veya kazayla kaybedilmesine ve yetkisiz erişime, değiştirilmeye veya yayılmaya karşı korunması için gerekli önlemler alınmak zorundadır. Buradan anlaşılacağı üzere, alınabilecek önlemler iç hukuka, başka bir deyişle taraf devletlere bırakılmıştır.

Sözleşmenin getirdiği güvencelerle ilgili istisnalar ve kısıtlamalar, AİHS'nin 8. maddesiyle benzerlik göstermektedir. Zira ilgili taraf devletin iç hukuku ile demokratik toplumun gereklerine uygun olarak kamu düzeni, devletin güvenliği, devletin iktisadi çıkarları ve her türlü suçla mücadele veya başkalarının hak ve hürriyetlerini tecavüzlere karşı korumak için kişisel veriler konusunda kanunlarla sınırlama getirilebilecektir. Öte yandan, herhangi bir mahremiyeti bulunmayan, anonim şekilde istatistik tutma ya da bilimsel araştırma yürütme gibi amaçlarla kullanılan otomatik kişisel veri dosyalarının kullanılması da taraf devletler tarafından kendi yasaları ile uygun görülebilecektir. Taraf devletler, temel ilkelerin uygulanması alanında 108 sayılı sözleşme ile uyumlu olan verilerin korunmasından da sorumludur. Bu nedenle, her devlet, bir hukuk ihlali olduğunda iç hukuk düzeninin sağladığı yaptırımlar ve telafi yolları için gerekli düzenlemeleri yapmak zorundadır.[91]

Sözleşmeye göre, sözleşmeye taraf devletlerin, kendi iç hukuklarında kişisel verilerin korunması rejimi konusunda yasal bir düzen oluşturmaları gerekliliği ve zorunluluğu göze çarpmaktadır. Esasen sözleşmenin taraf devletlerin iç hukukunda doğrudan doğruya uygulanabilmesi imkânı bulunmamaktadır. Bu nedenle, taraf devletlerin 108 sayılı sözleşmeyi çerçeve kabul ederek, bu sözleşmenin her bir hükmünü tafsilatlı bir şekilde düzenleyerek yasalaştırması gerekmektedir.[92] Ayrıca, bu tür bir yasanın çıkarılması ile sözleşme taraf devletlerin iç hukukunda daha etkili olacak ve verilerin korunmasında ortak temel güvencelerin oluşmasına zemin hazırlayacaktır.[93] Nitekim, Türkiye Cumhuriyeti, 6698 sayılı Kişisel Verilerin

---

91 108 s., söz. m.10.

92 Akıllıoğlu, Tekin "İdari Usul ve Kişisel Verilerin Korunması", www.idare.gen.tr/akillioglu-idariusul.htm, s. 6, Erişim tarihi, 09.02.2018.

93 Schwartz, Paul M. "European Data Protection Law and Restrictions on International Data Flows", IOWA LawReview, S. 80, March 1995, s. 477.

Korunması Kanununu bu sözleşmenin getirmiş olduğu yükümlülüğün neticesinde yürürlüğe koymuştur.

1.3.3.2.4. Sınır Ötesi Veri Akışı

Öncelikle, sınır ötesi veri akışının tanımı yapılmalıdır. Genel olarak, bu kavramın, kişisel verilerin yabancı bir devletin yargı yetkisine tabi kılınan bir alıcıya aktarılması şeklinde açıklanması mümkündür.[94] Günümüz dünyasında, daha fazla kişinin internet ortamına, sosyal medyaya ve dijital dünyaya katılması nedeniyle, kişisel verilerin korunması hukukunda sınır ötesi veri akışı da kaçınılmaz olarak ele alınması gereken konulardan olmuştur.[95]

Taraf devletler arasında verilerin serbest dolaşımı kabul edilmiştir. Bunun neticesinde, taraf devletler özel hayatın gizliliğinden bahisle birbirlerine veri aktarımını sınırlayamayacaklardır. Fakat, sözleşme, bu hususta iki istisna öngörmüştür. Bu istisnalar, taraf devletlerin birinde belli başlı veriler için getirilen özel koruma tedbirlerinin olması halinde, veri transferi yapılacak diğer devletin iç hukukunda bu koruma tedbirleri benimsenmemesi halinde, veri transferi yapmama seçeneği seçimlik bir hak olarak veri transferi yapmakla yükümlü bulunan devlete tanınmıştır. Yine Ek Protokol ile getirilen 2. m.'de, sözleşmenin tarafı olmayan bir uluslararası örgüte veya devlete veri gönderilmesinin şartı olarak, yalnızca bu devletin veya uluslararası örgütün veri koruma konusunda eşit düzeyde bir koruma sağlaması durumunda izin verilebileceği hususu sarih bir şekilde belirtilmiştir.[96]

Sınır ötesi transfere ilişkin ana kural; bir tarafın, yalnızca mahremiyetinin, özel yaşamın korunmasına yönelik olarak, kişisel verilerin aktarımının sınırlanamayacağı sözleşmenin 12/2 m.'sinde tanımlanmıştır. Elbette, her kuralda olduğu gibi, bazı istisnalar vardır. Sözleşmenin 12/3. m'sine göre:[97]

---

94 ETS 181 – Automatic Processing of Personal Data (Protocol), 8.XI.2001; Handbook on European Data Protection Law, a.g.e., s. 130.

95 Cunningham, McKay, a.g.m., s. 422.

96 108 s. söz. m.12, Atak, Songül, a.g.m., s. 98.

97 108 s. söz., m. 12.

- Devletlerin kendi mevzuatlarının, bazı kişisel veri ya da otomatik kişisel veri dosyası kategorileri açısından, söz konusu verilerin ya da dosyaların doğasının gereği birtakım özel düzenlemeler içermesi ve diğer taraf devletin yasal düzenlemelerinin eş değer bir koruma içermemesi,
- Söz konusu transferin sözleşmeye taraf bir devletin ülkesinden, diğer bir taraf devlet üzerinden sözleşmeye taraf olmayan üçüncü bir devlet ülkesine gerçekleştirilmesi halinde, sözleşmeye taraf devletin ilgili mevzuatındaki boşluklardan yararlanmak için yapılacak her türlü transferi engellemek amacıyla,

devletler veri aktarımına sınırlama getirilebilir:[98]

Bu nedenle, 108 sayılı sözleşmenin, alıcı devlet veya kuruluşun, veri aktarımı için yeterli bir koruma seviyesini temin etmesi koşuluyla, iç hukukun, sözleşmeye taraf olmayan devletlere serbest veri akışına izin verdiği açıkça görülmektedir. Bu husus, taraf devletlerin, hukuk düzeni tarafından, yabancı bir ülkede veri koruma seviyesinin nasıl ve kim tarafından değerlendirileceğine karar verilebileceği anlamına gelmektedir.[99]

Sonuç olarak, AK'nın kişisel verileri koruma hukukuna yönelik serüvenine baktığımızda, AK bakımından kişisel verilerin korunması meselesinin 1960'lı yıllarda başladığı görülmektedir. 1973 yılına gelindiğinde ise bu meseleye bir yön verilmeye başlandığı göze çarpmaktadır. Ancak, esas olarak, 1981 yılında 108 s. sözleşmenin kabulü ile AK için günümüz anlamında verileri koruma hukukunun oluştuğunun kabulü gerekir. Fakat burada AK'nın yaratmış olduğu katma değeri yani kişisel verilerin korunması konusundaki farkındalığı, sadece AK üyesi devletler ile sınırlı tutmamak lazım gelir. Şöyle ki, AK adı geçen sözleşmeyi üye devlet olmayanların da tanıyabileceğini kabul etmiştir. Bu yönüyle AK üyesi devletler bünyesinde ve AK'nın kendi uhdesinde oluşan bilgi ve tecrübenin, sınırları Avrupa'da olmayan birtakım devletlere ve başkaca hukuk sistemlerine ulaşması imkanı tanınmıştır. Özellikle

98 108 s. söz., m. 12.

99 Handbook on European Data Protection Law, a.g.e., s. 133.

uluslararası alanda akid devletleri yükümlülük altına sokarak kişisel verilerin korunması hukuku alanında bağlayıcı bir sözleşme olması ve 2001 yılında ek protokol ile bağımsız denetim otoritelerin ulusal düzeyde kurulmasını temin etmesi bunlara ilaveten kişisel verileri koruma alanında tafsilatlı bir genel çerçeveyi belirlemesi ve AİHS ile eş güdümlü bir koruma mekanizmasını belirlemesi hasebiyle 108 s. sözleşme çok önemli bir yer tutmaktadır.

1.3.3.3. AİHS

Avrupa Konseyi'nin amaçlarından birisi de Avrupa devletlerini, insan haklarını kurumsal ve korunması gereken bir hukuk alanı olarak kendi iç hukuklarında ilgili düzenlemeleri yapmak ve insan hakları ihlallerini engellemek için bir araya getirmektir. Bu amaca yönelik olarak, 1953 yılında yürürlüğe giren 1950 tarihli Avrupa İnsan Hakları Sözleşmesi'ni kabul etmiştir. Altı yıl sonra, imzacı devletlerin AİHS kapsamındaki yükümlülüklerini yerine getirmelerini garanti altına almak için, Strasburg'da Avrupa İnsan Hakları Mahkemesi kurulmuştur.[100]AİHS, insan hakları hukuku ve bu hakların korunması mekanizması içerisinde dünyada en önemli uluslararası metinlerin başında gelmektedir.

Esasen AİHS'de, kişisel verilerin korunmasına ilişin herhangi bir hakkın özel olarak sayılmadığı görülmektedir. Gerçekten de, uygulama, içtihat ve sözleşmelere bakıldığında, AİHS'de kişisel verilerin haksız müdahalelerden korunması için özel bir hüküm olmadığı açıktır. AİHM, bu hakkı özel hayat hakkı olarak 8. m. kapsamında ele almıştır. Bu nedenle, bu genişletici yorumların yardımıyla, hem kişisel veriler alanında yasa çıkaran hem de yasa çıkarmayan devletler aynı koruma kapsamında kalmaktadır. AİHM, kişisel verilerin korunması hakkına müdahalenin 8. m. kapsamında olup olmadığını değerlendirmektedir. Mahkeme bu değerlendirmeyi yaparken, hakka yönelik yapılan müdahalelerin, iç hukuka ve 108 sayılı sözleşmeye uygun olarak yapılıp yapılmadığını 8. m. şemsiyesi altında incelemektedir.

Kanaatimizce, 8. m. kapsamında yapılan denetimden ziyade, kişisel verilerin korunması hukukunun uygulama alanının giderek genişlemesi, her devletin kendi iç

[100] Handbook on European Data Protection Law, a.g.e., s. 14.

hukukunda özellikle anayasalarında bu hakka temel hak olarak yer vermeleri dikkate alındığında, ayrı ve özel bir m. AİHS'ye eklenerek bu hakkın koruma altına alınması isabetli olacaktır. Özellikle de sınırlama rejiminde, veri koruma hukuku ile özel yaşamın korunması arasında farklılıklar ortaya çıkabilmektedir.[101] Bu bağlamda, ek bir hükmün kabul edilmesine ilaveten bu hakka getirilecek sınırlamaların açık şekilde bu hakkın gereksinimlerine uygun olarak sözleşmeye eklenmesinin uygun olacağı tarafımızca değerlendirilmektedir.

1.3.4. AVRUPA BİRLİĞİ

Berlin Duvarının yıkılmasının ardından 3 Kasım 1990'da Doğu ve Batı Almanya'nın birleşmesi ve Aralık 1991'de Sovyetler Birliği'nin çözülmesi ile birlikte Avrupa'nın siyasi yapısı baştan aşağı değişmiştir. Avrupa devletleri, temel kriterleri 1991 yılında Maastricht'te gerçekleştirilen Avrupa Birliği Zirvesi ile belirlenen yeni bir andlaşma yapılması için müzakerelere başlamışlardır. Bu müzakereler sonucunda Avrupa Birliği Antlaşması olarak da anılan Maastricht Antlaşması, 1 Kasım 1993 tarihinde yürürlüğe girmiştir.[102] Esasen, 1995'te siyasi ve ekonomik bir birlik olarak anılan AB'nin amacı, üye devletlerde doğrudan uygulanabilecek yasama faaliyetlerinde bulunabilmektedir. Fakat her üye devletin bağımsız olması ve dış politikada kendilerini temsil edebilmeleri dikkate alındığında tipik federal devletten ayrıldığı görülmektedir.

Avrupa'da 1960'ların başından itibaren kişisel verilerin korunması hususu bir tartışma alanı haline gelmiştir ve aslında bu tarihlerde, kişisel verilerin korunmasını düzenlemeye yönelik önemli adımlar atılmıştır. Örneğin, Almanya'nın Hessen eyaleti, 1970 yılında dünyada ilk olarak veri koruma yasasını kabul etmiştir.[103] İsveç, Avusturya, Danimarka ve Fransa da aynı yolu izleyerek 1970'li yıllarda iç

---

101 Juliane Kokott / Christoph Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", International Data Privacy Law, 2013, S. 3, s. 222.

102 https://www.ab.gov.tr/avrupa-birliginin-tarihcesi_105.html, Erişim tarihi, 11.02.2018.

103 Tapper, Colin, a.g.m., s.10; Sandra C. Henderson, Charles Asynder, "Personal Information Privacy: Implicationsfor MIS Mana.g.ers", Information & Mana.g.ement, S. 36, 1999, s. 214.

hukuklarında verilerin korunmasına ilişkin yasalar çıkardılar.[104] Bu doğrultuda, kişisel verilerin korunması hakkı 1976 tarihli Portekiz Anayasasında, 1978 tarihli İspanya Anayasasında ve ayrıca 1983 tarihli Hollanda Anayasasında kendisine yer bulmuştur.[105] Aynı zamanda, Alman Anayasa Mahkemesi, kişisel verilerin korunması hukukunda Kıta Avrupa'sına olağanüstü katkıda bulunduğu kabul edilen ve "Nüfus Sayımı Kararı" olarak bilinen kararında, Alman yasalarında veri koruması için yasal bir referans noktası olarak, kişilerin kendisi hakkında tutulan bilgilere erişimine ek olarak kişinin kendisine ait olan veriler üzerinde tasarruf yetkisini kabul eden -kişilerin verilerinin kaderini tayin hakkı- karara imza atmıştır.[106] Dolayısıyla; Avrupa Hukukunda, 95/46/AT sayılı AB Yönergesinin yürürlüğe konulmasından önce, verilerin korumasının öneminin farkına varıldığı ve pek çok anayasada bir anayasal hak olarak tanındığı görülmektedir.

Avrupa hukukunun genel anlamda veri koruma hukukuna, daha özelde ise kişisel verilerin korunması hukukuna yaptığı katkı inkar edilemez bir gerçektir. Özellikle 1960'lı yıllarda başlayan süreç ile ilk olarak, Avrupa'daki ulus devletlerin bu meseleye eğildiği bilinmektedir. Bu aşamadan sonra, bu devletlerlerden bazılarının bu hakka anayasalarında yer vermeye başladığı görülmektedir. Yine bu gelişmelere paralel olacak şekilde, Avrupa merkezli olan AK ve onun peşi sıra AB'nin bu alanda düzenlemeler yaptığını görmekteyiz. En nihayetinde kişisel verilerin korunması hukuku alanında muazzam katkısı olan 95/46/AT sayılı Yönerge ve onun hemen akabinde yine GDPR'nin bu alanda en ileri seviyede koruma içeren ve diğer devletlere ve uluslararası kuruluşlara ilham kaynağı olabilecek evrensel bir metin halinde AB tarafından yürürlüğe konulduğunu görmekteyiz.

---

104 Krause, Rüdiger, "New Developmentsin Data Privacy for Employees in German Law", The Law in the Information and Risk Society, (Ed. GunnarDuttge/SangWon Lee), Universitäts verlag Göttingen, 2011, s. 89.

105 Kuner, Christopher "European Data Protection Law, Corporate Compliance and Regulation", Second Edition, Oxford University Press, United Kingdom 2007, s. 18.

106 Lothar Determann / Robert Sprague: "Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States", Berkeley Technology Law Journal, S.26, 2011, s. 1025.

1.3.4.1. 95/46/AT Yönergesi

Kişisel verilerin korunması konusunda en temel metinlerden birisinin de ***"Kişisel verilerin işlenmesi ve bu türdeki verilerin serbest dolaşımı bağlamında bireylerin korunmasına ilişkin 24 Ekim 1995 tarihli ve 95/46/AT sayılı Avrupa Parlamentosu ve Konseyi Yönergesi"*** olduğu söylenebilir. Yönerge, 1990'ların başında şekillendirilerek 24 Ekim 1995'te resmi olarak onaylandı.[107] Bu metin, doktrin tarafından o zamana kadar olan en etkili uluslararası belge olarak değerlendirildi. Bunun nedeni, belgenin, esasen Avrupa Birliği ülkelerindeki veri akışını düzenlemek için hazırlanmış olmasına rağmen, o dönemde dünyanın her yerinde referans alınan bir metin haline gelmiş olmasıdır. Öte yandan, yönergeye ayırt edici özelliğini veren bir diğer husus ise AB üye ülkelerinde bu yönergenin bağlayıcı ve zorlayıcı bir hukuksal metin olmasıdır.[108] Yönerge, aynı zamanda dünya genelinde etkisini artıran sınır ötesi veri transferleri için sağladığı mekanizma ile ön plana çıkmıştır. Kesin olarak söylenebilir ki, yönerge, AB üyesi olmayan ülkeleri, AB üyesi ülkeler ile olan ticari ve benzeri faaliyetleri nedeniyle düzenleme yapmak suretiyle kişisel veri güvenliğini sağlamaları bakımından itici güç olarak teşvik etmiştir. Bu tür bir kapsayıcı yaklaşım, 95/46/AT sayılı Yönergeye olan yönelimi dünya çapında artırmıştır.[109]

Yönergenin amacı, tüm AB üyelerinde koordineli olarak yüksek veri koruma standartları oluşturmak ve AB üyeleri arasında veri koruma açısından uygulamayı uyumlu hale getirmek suretiyle, AB içindeki kişisel verilerin serbest dolaşımını kolaylaştırmaktır.[110] Zira, üye devletler arasındaki serbest -kişisel veriler dahil- veri ve bilgi akışının, gelişmiş ortak Avrupa pazarı hedefine hiçbir engel teşkil etmemesi AB için hayati önem taşımaktadır.[111] Kısacası, yönergenin amaçlarını, kişisel bilgilerin işlenmesiyle ilgili olarak bireylerin mahremiyetinin korunması ve buna ek olarak, üye

---

107 Daniel J. Solove / Marc Rotenberg / Paul M. Schwartz, "Information Privacy Law", Apsen Publishers, New York, 2006, s. 900.

108 Cunningham, McKay, a.g.m., s. 427.

109 Cunningham, McKay, a.g.m, s. 427.

110 Solove / Rotenberg/ Schwartz a.g.e., s. 900.

111 Bainbridge, David, "Introduction to Informaion Technology Law", Six Edition, Pearson Longman, 2007, s. 499.

devletlerin iç hukuklarında verilerin korunmasına dair yasalarının AB mevzuatı ile uyumlaştırılması olarak özetleyebiliriz.[112]

Yönergenin 3. maddesinde belirtilen kapsama göre, otomatik olarak oluşturulan veya otomatik olarak oluşturulmasa dahi bir dosyalama sisteminde depolanan veriler bakımından yönerge uygulama alanı bulacaktır. Modern dünyada neredeyse verilerin tamamı bilgisayar sistemleri kullanılmak suretiyle otomatik olarak kaydedilmektedir. Diğer taraftan eskiden var olan birtakım elle tutulan kişisel verilerin ise süratle otomatik veri işletim sistemlerine taşındığı görülmektedir. Bu nedenle, yönergenin kapsamının neredeyse -*otomatik yollar ile tutulan veriler olsun veya klasik metotlar ile tutulmasına rağmen otomatik sistemlere aktarılan veriler dahil*- tüm verileri kapsayacak şekilde geniş yorumlanması mümkündür.[113]

Yönergede ifade edilen temel ilkeleri şu şekilde sıralamak mümkündür: [114]

- verinin kaynağını bilme hakkı,
- yanlış verilerin düzeltilmesi hakkı,
- hukuka aykırı işlemelere karşı başvuru hakkı,
- doğrudan pazarlama hususlarında kişisel verilerin kullanılmasına izin vermeme hakkı.

Ayrıca 95/46/AT madde 3/2'ye göre, yönerge kamu güvenliği, milli savunma, devletin güvenliği ve ceza hukuku alanında devletin faaliyetlerinde işlediği kişisel verilere ilişkin uygulama alanı bulamayacaktır.[115] Yine ikinci bir istisna, gerçek kişiler tarafından salt kişisel ya da kişilerin ailelerine yönelik etkinlikleri ile alakalı veri işlenmesinde yönerge hükümleri uygulanmayacaktır. Yönerge profesyonel ve belli bir ticari amaca matuf olmayan veri işlemeleri bu kategoride değerlendirmiştir. Mesela,

---

112 Carey, Peter, "Data Protection, A Practical Guide to UK and EU Law", Oxford University Pres, 2004, s. 6.

113 Şimşek, a.g.e., s. 43.

114 https://kisiselveri.com/9546ec-turkce, Erişim tarihi, 13.03.2018.

115 "Bu istisna, özellikle Europol ve Schengen Antlaşmalarının uygulanmasına ilişkin olarak kişisel verilerin korunmasına yönelik saldırılarda çeşitli tartışmaların alevlenmesine neden olmuştur. Yine bu konuya ilişkin bir diğer önemli tartışma konusu ise Havayolu şirketlerinin yolcu kayıtlarını ABD'nin yetkili mercilerine aktarmasına ilişkindir.", Küzeci, a.g.e., s. 181.

bir kişinin sahip olduğu telefon defteri yönerge kapsamında tutulamayacaktır. Burada tartışma konusu olan alanın ise sosyal medya ağları üzerinde kişilerin hesaplarında tuttukları verilere ilişkin olduğu görülmektedir. Zira facebook, twitter, instagram gibi uygulamalarda, hesap sahibi, pek çok kişi ile alakalı resim, görüntü, ses, adres ve konum bilgisini bu hesapları üzerinde tutmakta hatta paylaşım yaparak bu bilgileri alenileştirmektedir.[116]

95/46/AT sayılı Yönergenin 29. maddesine göre, kişisel verilerin işlenmesi ile ilgili olarak çalışma grubu kurulmuştur. Bu çalışma grubu danışman bir komisyon gibi hizmet sunacak ve bağımsız olarak hareket edecektir. Çalışma Grubu, her üye devlet tarafından belirlenen denetim yetkilisi veya yetkilileri ile AB organlarının bir temsilcisi ve bir Komisyon temsilcisinden oluşur. Bu Çalışma Grubu, kişisel bilgilerin işlenmesi, gerçek kişilerin hak ve özgürlüklerini korumak için alınacak tedbirler ve bu yönergeye yönelik olarak önerilen herhangi bir değişiklik hakkında Komisyona tavsiyede bulunur.[117] Bu çalışma grubunun ihdasının bir sonucu olarak, özel hayatın korunması hakkı AB tarafından temel bir hak olarak dikkate alınmış, AB'nin Temel Haklar Şartı'nda verilerin korunması hakkı olarak bu şart üzerine dercedilmiştir.[118]

Yönerge ile bir yandan kişisel bilgilerin serbest dolaşımının sağlanması diğer yandan bireylerin temel haklarının korunması anlayışının bir araya getirilmesi bu yönergeye ilişkin yapılan olumlu eleştiriler arasında bulunmaktadır.[119]

1.3.4.2. AB Temel Haklar Şartı

AB Temel Haklar Şartı 07 Aralık 2000 yılında imzalanarak AB devletlerinde - vatandaş olmasa dahi- mukim olan ve AB vatandaşlığına sahip olan kimselerin; kişisel, siyasi ve ekonomik hakları ilk defa olmak üzere tek bir metinde bir araya getirilmiştir.

---

116 Küzeci, "Doktora Tezi", s. 181-182.

117 Art. 29-30 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such datahttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, Erişim tarihi, 14. 03.2018.

118 Bergkamp, Lucas, "EU Data Protection Policy, The Privacy Fallacy: Adverse Effects Of Europe's Data Protection Policy İn An Information-Dirven Economy", Computer Law and Security Report, Sayı: 18, Yıl: 2002, s. 33.

119 Poullet, Y./Gutwirth S., "The Contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of reflexive governance?", Brussels, 2008, s. 570-580.

2009 yılında bu şart Lizbon Antlaşmasının imzalanması ile bağlayıcı bir metin halini almıştır. AB Temel Haklar Şartı'nın *"Kişisel verilerin korunması"* başlıklı 8. maddesi şu şekildedir:[120]

1) *"Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir.*
2) *Bu veriler, dürüst bir şekilde belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanılarak işlenir. Herkes kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir.*
3) *Bu kurallara uyulması bağımsız bir makam tarafından denetlenir."*

Burada dikkati çeken husus "*herkes*" kelimesinin tercih edilmesi olmuştur. Doktrinde, bu ifadenin tercih edilmesine rağmen, burada korunacak olan kişilerin gerçek kişiler olduğuna dair yorumların bulunduğu müşahede edilmektedir.[121] Bu şartın kabulünden önce yürürlüğe giren 95/46/AT sayılı Yönergede gerçek kişi ifadesi açık bir şekilde kullanılmıştır. Ancak burada herkes ifadesinin tüzel kişileri de maddenin lafzi yorumundan kapsayabileceği kanaatinde olmamıza rağmen sistematik ve tarihsel yorum perspektifinden baktığımızda korumanın sadece gerçek kişiler ile sınırlı olduğunu söylemek daha makul görülmektedir.

Sonuç olarak, Lizbon Antlaşmasının 01/12/2009 tarihinde yürürlüğe girmesi ile Temel Haklar Şartı bağlayıcı bir araç haline gelmiştir.[122] Yine bu antlaşma ile kişisel verilerin işlenmesini hukuki ve idari yönden denetleyecek olan bir bağımsız kuruma ihtiyaç teyid edilmiştir.

1.3.4.3. AB Genel Veri Koruma Tüzüğü (GDPR)

2012 yılının başında, Avrupa Komisyonu tarafından, teknoloji ve küreselleşmenin geldiği nokta dikkate alınarak mevcut düzenlemelerin gözden geçirilmesi gerektiğini vurgulayan bir reform önerisi sunuldu. Bu teklifte, komisyon

120 Küzeci, a.g.e., s. 172-vd.

121 Şimşek, a.g.e., s. 73.

122 Kacrorowska, Alina "European Union Law", Routledge.Cavendish, Taylor and Francis Group, London and New York, 2009, s. 43.

tarafından, Genel Veri Koruma Tüzüğünün (GDPR olarak anılacak), kolluk yetkisinin kullanımı ve adli iş birliği konularında 95/46/AT sayılı Yönergenin yerini alması amaçlandı.[123] 2015 Aralık ayı sonunda, bu yeni tüzük hakkında Avrupa Parlamentosu, Konsey ve AB Komisyonu arasında bir anlaşmaya varıldı. Nisan 2016'da GDPR'nin son versiyonu, sırasıyla, Avrupa Birliği Konseyi ve Avrupa Parlamentosu tarafından onaylandı. Daha sonra, resmî belge 04 Mayıs 2016 tarihinde yayınlandı. 24 Mayıs 2016'dan itibaren, tüzüğün üye ülkelerde yürürlüğe konulması açısından yapılacak olan hazırlıkların tamamlanması amacıyla, üye ülkelere iki yıllık bir geçiş dönemi öngörüldü.[124]

Tüzüğün temel amacının, kişisel verilerin korunması alanında, daha yüksek ölçütler belirleyerek AB ülkelerinin bu alanda entegrasyonunu hızlandırmak ve AB üyesi olmayan ülkelerde faaliyet gösteren ancak AB ile ticari ilişkileri bulunan şirketlerin bu düzenlemelere uyumunu sağlamak olduğu görülmektedir.[125] AB'nin yönergeden vazgeçerek veri koruma hukukunu tüzük ile tanzim etmesinin ana sebepleri olarak tüzüklerin üye devletlerde aynen uygulanması gerektiği ve hukuken bağlayıcı bir metin olmasından kaynaklanmaktadır.[126] Böylelikle, AB, tüm üye ülkeler arasında kişisel verilerin korunması hukuku bakımından yeknesaklığı sağlamış olacaktır. Özellikle AB ile ticaret yapan ancak AB üyesi olmayan ülkeler menşeli şirketlerin tek bir hukuki metne tabi olması tüzükle getirilen önemli bir yenilik olarak göze çarpmaktadır. Başka bir deyişle, GDPR'nin kapsamı, yönergeye göre bir adım ileriye götürülerek, Tüzüğün 3/2 maddesine göre AB hukukuna tabi kuruluşların yanı sıra tabi olmayan fakat AB vatandaşlarına mal ve hizmet sunan kuruluşların da kapsam dahiline alındığı görülmektedir.

---

123 European Commission (2012), "Proposal For A Regulation Of The Europeanparliament And Of The Council On The Protection Of İndividuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data (General Data Protection Regulation)", COM(2012) 11 Final, Brussels, 25 January 2012.

124 GDPR, m. 99.

125 Taştan, a.g.e., s. 15.

126 Baykal, Sanem/ Göçmen, İlke,"Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi" Prof. Dr. Erdal Onar'a Armağan, Cilt- II, Ankara – 2013, s. 325; Ayrıca bkz. AB İşleyişine Dair Anlaşma, m. 288.

Kişisel verilerin işlenmesine ilişkin ilkeler ise GDPR'nin 5. maddesinde şu şekilde belirtilmiştir;

- Hukuka uygunluk ilkesine göre, veri sahibiyle alakalı kişisel verilerin hukuka uygun, adil ve şeffaf bir şekilde işlenmesi gerekir.

- Amacın belirli olması ilkesine göre, kişisel verilerin belirtilen, açık ve meşru amaçlar doğrultusunda toplanması ve söz konusu amaçlara uygun şekilde işlenmesi gerekir. Ayrıca veri işlenmesinde gözetilecek amaçlar şunlardır;
  - kamu yararı amacıyla arşivleme,
  - bilimsel amaçla veri işleme,
  - tarihi araştırma amacıyla veri işleme,
  - istatistiki amaçlarla veri işleme.

- Güncel, yeterli ve gerekli olma ilkesinin gereği olarak, kişisel veriler işlendikleri amaçlarla ilgili olmalıdır. Bununla birlikte veri işlemenin yeterli, yerinde ve gerekli olanla sınırlı olması gerekmektedir. Ayrıca veri işlemenin doğru olması ve gereken şekilde yapılması; verilen güncel tutulması büyük önem taşır. Dahası veriler işlendikleri amaçlar da göz önünde bulundurularak doğru olmayan kişisel verilerin derhal silinmesi ya da düzeltilmesinin sağlanmasıyla konularında gerekli tedbirlerin alınması gerekmektedir.

- Belirli süre saklama ilkesinin bir sonucu olarak, veri sahibi bireylerin sadece kişisel verilerin işlenme amaçlarının zorunlu kıldığı süre zarfında teşhis edilmesi gerekmektedir. Fakat GDPR'de belirtildiği üzere, veriler sadece kamu yararına arşivleme, bilimsel veya tarihi araştırma ya da istatistiki faaliyetler kapsamında işlendikleri sürece ve veri sahibinin hakları ve hürriyetlerini korumaya yönelik gerekli teknik tedbirlerin alınması şartıyla, kişisel verilerin uzun süreler boyunca saklanması mümkündür.

- Gizlilik ve bütünlük ilkesi gereği, yetkisiz ya da hukuka aykırı veri işlemelerine karşı ve kazara veri kaybına, verilerin imha edilmesine ya da tahrip olmasına karşı koruma da dahil olmak üzere, teknik ve uygun tedbirler kullanılarak kişisel veriler güvenli bir şekilde işlenmelidir.

Tüzüğün 7. maddesi "*ilgilinin rızası*"nı düzenlemektedir. Burada ilgili kişi daha önceden kişisel verilerinin toplanmasına dair vermiş olduğu rızayı istediği zaman geri alabilmektedir. Yine bu maddeye göre, kişisel verileri tutmak ve onları muhafaza etmek ile görevli olan veri sorumluları veriyi rızaya uygun olarak topladıklarını ispat ile mükelleflerdir. 8'inci m.'ye göre, önleyici ve rehberlik hizmetleri istisna olmak koşulu ile 16 yaşından küçüklerin verilerinin toplanması ve internet üzerinde profil oluşturmada kullanılması için velilerinin rızasına ihtiyaç vardır. Üye ülkelere, bu yaşı 13'e kadar indirebilme yetkisi tüzükte tanınmıştır.

GDPR'nin getirdiği öncü yeniliklerden biri de hiç şüphesiz "unutulma hakkı"nın[127] tanınması olmuştur. Artık üye devletler, bu hakkı tanımak durumunda kalmışlardır.[128] Verisi işlenen kişi, kendisiyle alakalı kişisel verilerin gecikmeksizin silinmesini işleyenden (controller: kontrolör) talep etme hakkına sahiptir. Esasen tüzüğün kabulünden önce ABAD'ın vermiş olduğu bir kararla unutulma hakkı gündeme gelmişti.[129] İlgili kararda internet arama motoru Google'a "Costeja Gozalez" adlı bir avukatın ismi girildiğinde, arama sonuçlarının aranan kişinin sosyal güvenlik borçlarını ödemek için mal varlığını icra yoluyla satmak mecburiyetinde kaldığına ilişkin bilgiler çıkmaktaydı. Bunun üzerine ilgili kişi İspanya'da, Google arama motorunda çıkan bu bilgilerin silinmesi talebi ile dava açmıştır. Açılan dava ABAD aşamasına kadar gelmiş ve bu aşamada ABAD; kişilik haklarının, kamunun bilgiye erişimi hakkından üstün tutarak kararında "*kişinin ismine dayalı olarak üçüncü kişiler tarafından internet ortamında yasal olarak işlenmiş ve yayınlanmış kişisel veriler,*

127 "Unutulma hakkı", kişinin kendisi ile ilgili olarak dijital hafızada yer alan, foto, kimlik, adres vb. bilgilerinin talebi ile geri dönüşümü olmayacak şekilde silinmesini ifade eder. Akgül, Aydın "Kişisel Verilerin Korunmasında Yeni Bir Hak: Unutulma Hakkı ve ABAD'ın Google Kararı", TBBD, 2015, C. 27. S. 116, s. 16.

128 Taştan, a.g.e., s.17.

129 ABAD, C-11/12 sayılı T.13/05/2014 kararı, https://rm.coe.int/ozelyasam-aile-ceza/16808e940d, Erişim Tarihi, 29.05.2019.

geçersiz, eksik, tamamen ilgisiz veya sonradan ilgisiz hale gelmiş ise işlenmesi amacını aşan ve arama motorları tarafından internet ortamına yüklenen söz konusu kişisel verilerin ve buna ilişkin sonuç listesinde yer alan bilgilerin silinmesi" gerektiğini belirtmiştir.[130] Netice itibarıyla, ABAD, "*Google kararı*"nda; bireyin ismi ile arama yapılarak link verilmesi durumunda ilgili kişinin bu linkin kaldırılması hakkının bulunduğuna hükmetmiştir. İstisna olarak ise anılan kararda *"üstün kamu yararı"*, *"kişilerin yoğun ilgisi"*, *"verinin kamu hayatındaki önemi"* gibi hususları belirtmiştir. ABAD bu kararında 95/46/AT sayılı Yönergesini esas alarak karar vermiştir.

GDPR'nin 17. maddesine göre;[131](silme işlemi-unutlma hakkı)

(a) kişisel verilerin toplanma veya işlenme amaçlarıyla ilişkili olarak artık gerekli olmaması;

(b) veri sahibinin 6(1) maddesinin (a) bendi veya 9(2) maddesinin (a) bendine göre işleme faaliyetinin dayandığı izni geri çekmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması;

(c) veri sahibinin 21(1) maddesi uyarınca işleme faaliyetine itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması ya da veri sahibinin 21(2) maddesi uyarınca işleme faaliyetine itirazda bulunması;

(d) kişisel verilerin yasa dışı biçimde işlenmiş olması;

(e) kontrolörün tabi olduğu Birlik veya üye devlet hukukundaki bir yasal yükümlülüğe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması;

(f) kişisel verilerin 8(1) maddesinde atıfta bulunulan bilgi toplumu hizmetlerinin sağlanması ile ilgili toplanmış olması."

---

130 https://curia.europa.eu/jcms/jcms/j_6/en/ Erişim tarihi, 20.04.2018; Akgül, a.g.m., s. 30 vd.

131 https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf, Erişim tarihi, 20.04.2018.

durumunda ilgili kişisel verilerin herhangi bir gecikmeye mahal verilmeksizin silinir. Ancak bunun istisnası olarak, kamu yararı, kamu düzeni, genel sağlık gibi sebeplerin varlığı durumunda silme talebi ilgili Tüzüğün 17/3. maddesi uyarınca reddolunur.[132] Yukarıda sayılan bentlerden birinin gerçekleşmesi silme işlemi için yeterli olacaktır. Kanaatimizce buradaki silme işlemine ilişkin sayım tahdidi bir sayımdır. Yani veri sorumlusu veya kontrolörü bu sayılan bentlerin dışındaki gerekçelerle gelen silme talebini reddedecektir.

GDPR'nin getirdiği en önemli yeniliklerin bir diğeri ise "Tasarımla Veri Koruma" (Privacy by design) ve "Varsayılan Ayarlarla Veri Koruma" (Privacy by Default) ilkelerinin benimsenmesi olmuştur. Tasarım ile veri koruma deyiminden kasıt, veri işleyen veyahut bu hususa ilişkin teknoloji üreten-kullanan kimselerin ürünlerinin tasarım aşamasındayken yüksek güvenlikli olması gerekliliğidir.[133] Varsayılan ayarlar ile korumadan kasıt ise, alınan ürün ve hizmetin kişisel verilerin korunmasına ilişkin gerekli olabilecek şekilde gizlilik politikalarına ve ayarlarına riayet etmesini kastetmektedir. Örneğin, Facebook adlı sosyal paylaşım sitesine üye olunduğunda ilgili sitenin, yani şirketin varsayılan ayarlarında, üyenin her türlü bilgisinin üçüncü kişilerin müdahalesine ve erişimine kapalı olması gereklidir. Üye eğer ayarları değiştirirse bu "rıza" kapsamında değerlendirilerek ihlal oluşmayacaktır.[134] Örneğin, Apple, güvenlik rehberinde[135] kişisel verilerin korunmasına ilişkin azami ölçüde dikkat edildiğini belirtmiştir. Burada hukuk tekniği bakımından adı geçen ilkelerin kabulünde bir beis olmasa dahi bu ilkelerin pratikte, yani hayatın içinde, nasıl uygulanacağına ilişkin ciddi sorunlar olduğu

---

132 Ayrıntılı bilgi için bkz. GDPR, m. 17/3.

133 Başalp, Nilgün "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri" MÜHF, Cilt: 21, Sayı: 1, s. 92.

134 Taştan, a.g.e., s. 19.

135 "Güvenli önyükleme zinciri, kod imzalama bir aygıtta yalnızca güvenilir kod ve uygulamaların çalışmasını sağlamaya yardımcı olur. iOS, güvenlik altyapısının diğer bölümlerinin tehlikeye girdiği durumlarda bile (örneğin, yetkisiz değişikliklere sahip bir cihazda) kullanıcı verilerini korumak için ek şifreleme ve veri koruma özelliklerine sahiptir. Bu, hem kullanıcılar hem de BT yöneticileri için önemli avantajlar sağlar, kişisel ve kurumsal bilgileri her zaman korur ve cihaz çalınması veya kaybolması durumunda anında ve eksiksiz uzaktan silme yöntemleri sağlar". https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf s.19, Erişim tarihi, 01.05.2018.

görülmektedir.[136] Zira bu sistemlerin kurulumu, denetimi hukuk tekniğinden ziyade bilişim teknolojisi ile çözülebilecek bir sorun olarak göze çarpmaktadır. Ancak yine de GDPR'nin, günümüz teknolojisinin geldiği noktayı gözeterek almış olduğu bu tedbirler olumlu mütalaa edilmelidir. Gündelik hayatımızda ve rutin eylemlerimizde, kişisel verilerimizin rızamız dahilinde olsun veya olmasın en çok kaydedildiği, kullanıldığı alan olarak internet bazlı uygulamaların olduğunu söylemek yanlış olmayacaktır. Bu nedenle facebook, youtube, twitter ve instagram gibi bazı popüler sosyal medya uygulamalarının GDPR'de kendisine yer bulan "varsayılan ayarlar" ile kullanıcılarına asgari düzeyde kişisel verilerinin korunduğuna dair taahhütte bulunması gerekmektedir. Böylelikle kişisel verileri daha kaynağında iken bir sözleşme ile kişiler koruma altına almaktadır.

GDPR'nin 35. m.'sinde veri koruma etki değerlendirmesi tanımlanmıştır. Buna göre; "*Özellikle yeni teknolojiler kullanıldığında ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçları dikkate alındığında bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından* ***yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde****, kontrolör, işleme faaliyetinden önce, öngörülen işleme faaliyetlerinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapar. Tek bir değerlendirmede benzeri yüksek riskler taşıyan bir dizi benzer işleme faaliyeti ele alınabilir.*" denilmektedir. Özellikle profil çıkarma dahil gerçek kişilerle alakalı kişisel verilerin otomatik işlemeye dayanan ve gerçek kişi ile ilgili hukuki sonuçlar doğuran veya gerçek kişiyi kayda değer şekilde etkileyen kararların varlığı halinde sistematik ve kapsamlı bir değerlendirme yapılmalıdır. Yine benzer bir değerlendirmenin yapılması durumu; hassas kişisel verilerin, mahkûmiyet kararlarının ve ceza gerektiren suçlara ilişkin kişisel verilerin işlenmesi veya kamunun erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlenmesi durumlarında bir zorunluluktur.[137]

---

136 Hornung, Gerrit, "A general data protection regulation for Europe? Light and Shade in the Commission's Draft of 25th January 2012.", Script-ed 9, No:1, s. 75.

137 GDPR, m. 35.

"Veri koruma görevlisi" yine GDPR ile kişisel verileri koruma hukuku literatürüne kazandırılmıştır.[138] Veri koruma görevlisi unvanı ile kastedilen, kişisel verilerin, ne için işlendiği hususlarında ve bu işleme faaliyeti gerçekleştirilirken hangi vasıtaların kullanılacağına ilişkin takdir hakkı bulunan kimseyi ifade eder. Bu kimse hukuken gerçek veya tüzel kişi olabilir. Bu kişilere hukuken birtakım yükümlülükler getirilebilir. Bunlar; aydınlatma, gizlilik vs. yükümlülükler şeklinde sayılabilir. [139]

1.3.4.4. Elektronik Veriyi Korumaya İlişkin 2002/58/Ec Sayılı Avrupa Birliği Direktifi

Avrupa Konseyi ve Avrupa Parlamentosu 12 Temmuz 2002 tarihinde "Elektronik Veriyi Kullanmaya İlişkin İlişkin Direktifi" kabul etmiştir. 2002/58/EC sayılı bu direktifin amacı elektronik telekomünikasyon alanında temel hak ve özgürlükleri korumaktır.[140]

1.3.4.5. Avrupa Birliği Vatandaşlık Hakkı Direktifi (2009/136/Ec Sayılı Direktif)

Avrupa Birliği Vatandaşlık Hakkı Direktifi olarak da bilinen 2009/136/EC sayılı direktif, 2002/58/EC sayılı Elektronik Veri Koruma Direktifindeki kişisel verilerin güvenirliliği konusundaki eksiklikleri tamamlamak için kabul edilen bir direktiftir.[141]

1.3.4.6. Europol Antlaşması ve Kişisel Verilerin Korunması

Avrupa Birliği'nin resmi kolluk birimi olarak kurulan ve merkezi Hollanda'nın Lahey şehri olan Europol 1998 yılında faaliyetlerine başlamıştır. Europol'ün görevi, iki veya daha fazla üye devleti etkileyen ve Europol Kararı'nın ekinde listelenmiş olan organize suç, terörle mücadele ve diğer ağır suç türlerinin önlenmesi, soruşturulması ve kovuşturulması konularına destek vermek şeklinde açıklanmıştır.[142] Yeni gelişme

---

138 Taştan, a.g.e., s. 20.

139 https://www.kvkk.gov.tr/Icerik/2032/Veri-Sorumlusu-Kimdir, Erişim Tarihi: 15.11.2019

140 Özdemir, a.g.e., s. 43.

141 Uyarer Göçmen, a.g.e., s. 44.

142 https://kpveri.com/wpcontent/uploads/2017/07/avrupa Veri Koruma Hukuku El Kitabi.pdf,s.108, Erişim Tarihi: 26/11/2019.

ve oluşumlar sonucu, 1 Ocak 2013 tarihinde Europol'de Avrupa Siber Suç Merkezi kurulmuştur.[143]

Europol Antlaşması'nın 13-25 arasındaki maddelerinde verilerin işlenmesi konusunda önemli düzenlemelere yer verilmiş ve ayrıca üye devletlerin veri değişim sistemine dahil olabilmesi için Avrupa Konseyi'nin 108 sayılı Sözleşmesi'ni uygun bulmak suretiyle ulusal hukuklarında verilerin korunmasına dair bir standart oluşturması gerektiği belirtilmiştir. [144]

1.3.4.7. Eurojust

Merkezi Lahey'de olan ve 2002 yılında kurulan Eurojust, AB'ye üye olan en az iki devletle ilgili ağır nitelikli suçların kovuşturma ve soruşturma evrelerinde adli işbirliği yapılmasını teşvik eden bir AB organıdır.[145]

Eurojust'ın, hedeflerine ulaşmak amacıyla durumun gerektirdiği ölçüde kişisel verileri işlemesi mümkündür. Fakat işlemenin birtakım sınırları vardır. Buna göre Europol, yetki alanına giren bir suçu işleyen ya da bu tarz bir suça karıştığından şüphelenilen veyahut hüküm giyen kişilere dair bilgilere erişebilecektir. Yine aynı şekilde Eurojust'ın, yetki alanındaki suçlara tanıklık eden veya söz konusu suçların mağduru olan kişilerle ilgili bazı bilgileri işlemesi de mümkündür.[146]

Belirtmek gerekir ki veri alışverişi gerçekleştirilecek hallerde gerek Eurojust Konsey Kararları gerekse Eurojust Veri Koruma Kuralları göz önünde bulundurularak yürürlüğe giren iş birliği andlaşmaları ile çalışma düzenlemeleri içinde yer alan özel kurallarla sınırlamalara uygun hareket edilmesi gerekir.[147]

---

143 Avrupa Veri Güvenliği Gözetmeni (EDPS), Veri Güvenliği Gözetmeni'nin Avrupa Komisyonundan Konseye Ve Avrupa Parlamentosuna, Avrupa Siber Suç Merkezi'nin Kurulmasına İlişkin Bildirimin Üzerine Verdiği Görüş, Brüksel, 29 Haziran 2012.

144 Şimşek, a.g.e, s. 75.

145 Avrupa Birliği Konseyi (2002), Ağır suçlarla mücadeleyi güçlendirme amacıyla Eurojust'i kuran 28 Şubat 2002 tarihli ve 2002/187/JHA sayılı Konsey Kararı.

2003/659/JHA Sayılı Konsey Kararı ve 2009/426/JHA sayılı, m. 15 (2) Konsey Kararı ile değiştirilen 2002/187/JHA Konsey Kararının konsolide versiyonu, https://kpveri.com/wpcontent/uploads/2017/07/avrupa VeriKorumaHukukuElKitabi.pdf, s. 108.

147 Kişisel Verilerin İşlenmesine ve Korunmasına İlişkin Usul Kuralları Eurojust, 19 Mart 2005, https://kpveri.com/wpcontent/uploads/2017/07/avrupa Veri Koruma Hukuku El Kitabi., Erişim Tarihi; 20/11/2019, pdf, s. 110.

1.3.4.8. Schengen Antlaşması ve Kişisel Verilerin Korunması

Temelinde taraf olan devletler arasında geçerli olan sınır kontrollerinin kaldırılmasını amaçlayan Schengen Anlaşması 1986 tarihinde yürürlüğe girmiştir.

Antlaşma'ya üye tüm devletlerin SIS II adlı otomatik sisteme, parmak izi ve fotoğraf gibi biyometrik verileri veya çalıntı tekneler, uçaklar, konteyner veya ödeme araçları şeklinde yeni uyarı kategorilerini, kişilere ve nesnelere ilişkin gelişmiş uyarıları; tutuklama, teslim veya iade için aranan kişilere ait kopyalarını sisteme girme gibi kişisel verilere ilişkin yetkileri ve görevleri bulunmaktadır. Sözleşmeye taraf olan her devlet bu bilgi sistemine giriş yapabilecektir. Sistem içerisinde yer alan verilerin korunması konusunda ise söz konusu verileri sisteme kaydeden ulusal makamların sorumluluğu söz konusudur.[148]

148 https://kpveri.com/wpcontent/uploads/2017/07/avrupaVeriKorumaHukukuEl Kitabi.pdf, s. 11, Erişim Tarihi: 29.11.2019

İKİNCİ BÖLÜM

KİŞİSEL VERİLERE İLİŞKİN TERMİNOLOJİ ve VERİLERİN KORUNMASINDA TEMEL İLKELER

2.1. TERMİNOLOJİ

2.1.1.KİŞİSEL VERİ

Kişisel verinin tanımını yapmadan önce, *"veri"* kavramından ne anlaşılması gerektiği üzerinde durulmalıdır. Sözlük anlamı itibarıyla veri[149], "*bilgi – data"* ve *"olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi"* şeklinde tanımlanmaktadır. Veri (data) sözcüğü köken itibarıyla Latince olup anlamı "verilen bir şey" demektir.[150] Bu verilen şey bir sözcük, eşya olabileceği gibi rakamlardan oluşan bir dizi de olabilir. Dolayısıyla verilen şeyin bir bilgi ile irtibatı esas olarak tespit edilebiliyorsa veri olarak kabul edilebilir.[151] Diğer bir deyişle, veriler soyut olarak bilgi kırıntısının en düşük seviyesi olarak tanımlanabilir. Veriyi takip eden aşamalar ise sırasıyla bilgi ve üst düzey bilgidir.[152] Buradan hareketle kabaca, kişisel veriler, yaşayan bir bireyi tanımlayan, elektronik veya manuel bilgi olarak tanımlanabilir. Örneğin, bir kişinin ismi, telefon numarası, adresi, mesleği, inancı, e-posta adresi, DNA örneği, doğum tarihi, sağlık sorunları, CCTV görüntüsü, kredi kartını kullanma tarihi ve saati, maaşı ve benzeri kişisel bilgiler "*irtibatlandırılabilen bilgi*" olarak sayılabilir.[153] Bununla beraber verilerin sadece bilgisayar sistemi üzerinde otomatik olarak işlenmesi gerekmez. Aynı zamanda konuşma tanıması ve kapalı devre video sistemleri gibi bilgisayar dışı sistemlerde de veri otomatik ve sistemsel olarak

---

149 TDK'da veri kavramı, "Bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done; bir sanat eserine veya bir edebî esere temel olan ana ilkeler; bir problemde bilinen, belirtilmiş anlatımlardan bilinmeyeni bulmaya yarayan şey; olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi" şeklinde matematik, edebiyat ve bilişim gibi çeşitli alanlarda farklı şekillerde tanımlanmıştır. Ancak biz çalışmamızda genel tanımlarından ikisine yer verdik. http://sozluk.gov.tr/, Erişim Tarihi, 27.08.2019.

150 Van Belle, Gerald /Ruiter, Leslie, "Data and Law: Beyond the Sweat of the Brow: Who Owns Published Data? And What Is Data?", April, 2014, Journal of Significance, S.11, s. 28.

151 Gordon, Keith,"Principles of Data Mana.g.ement, Facilitating Information Sharing, BCS Learning Development", Second Edition, November 2013, s. 3.

152 Van Belle, Gerald /Ruiter, Leslie, a.g.m., s. 29.

153 Carey, a.g.e., s. 2 ; Şimşek, a.g.e., s. 120.

işlenebilmektedir.[154] İngiliz Temyiz Mahkemesince "kişisel veri", *"bireylerin kişisel ya da aile yaşantıları, iş veya meslekî kapasiteleri yönünden özel hayatını etkileyen bilgi"* olarak tanımlanmıştır.[155]

Kişiler hakkındaki veriler, kişiye dair hayatın her alandaki bilgi kırıntılarının bir araya gelmesi suretiyle kişiyi tanımamıza, ayırt etmemize yardımcı olan bilgileri oluşturur. Bu bakımdan, günümüzde internet kullanımının yaygınlaşması, e-ticaret ya da elektronik ve çevrimiçi işlemlerde meydana gelen olağanüstü artış, bireyin "çevrim içi" ve "çevrim dışı" kimliklerinin oluşmasına yani bir gerçek hayattaki esas kimliğinin yanı sıra profilinin çıkarılmasına zemin hazırlamıştır. Bir kişinin internet üzerinde gezinirken, sosyal medya hesaplarında paylaşım yaparken veyahut bu hesaplar aracılığıyla beğenide bulunurken aslında bu nitelikli verilerin bilgi hatta üst düzey bilgi halini alarak ilgili kişiyi işaret ettiği günümüzün yadsınamaz bir gerçeğidir. Gerçekte, her insanın kişiliği kendisine özgüdür. Ancak günümüzde basit bir şekilde bazı kişisel özelliklerin filtrelenmesi suretiyle kişilikler birbirinden ayırt edilebilir hale gelmiştir. "Çevrim içi kimlik", kişinin internet ve sosyal medya üzerinde geçirdiği zaman ve yönelimleri neticesinde, kişinin genel tavrı, internet ortamında gezindiği internet siteleri, dikkatini çeken mal ve hizmetler, satın alma geçmişi hakkında bilgi verirken, "çevrim dışı kimlik" diye tabir edilen kimlik, esasta o kişinin gerçek kimliğidir. Örneğin, web sitelerinden arama yaptıktan sonra internet üzerinden bir şeyler satın almak, çevrim içi kişilik eylemi tarafından gerçekleştirilen işlemdir ve bu, kimlik bilgilerini ve IP adresini izleyerek çevrim içi kimlik tespitini ortaya çıkarır. Öte yandan, internet üzerinden kredi kartı numarası ile alışverişin sona erdirilmesi aşamasında, kredi kartı numarasının gerçek olması ve gerçek bir kişiye bağlı olması nedeniyle, gerçekte çevrim dışı kimliğin devreye girmesine neden olur.[156] Çünkü çevrim içi ve çevrim dışı kişilik, sağlanan veri koruma kapsamını belirlemek için büyük bir önem taşımaktadır.

---

154 Carey, a.g.e., s. 26.

155 Oğuz, a.g.m., s. 13.

156 https://www.heinz.cmu.edu/~acquisti/papers/acquisti_eis_refs.pdf, Erişim tarihi, 01.02.2018.
Acquısti, Alessandro, "Privacyand Security of Personal Information-Economic Incentives and Technological Solutions", Economics of Information Security Advances in Information Security, s. 3.

Genel ve sözlük anlamından sıyrılarak hukuki açıdan kişisel verilerin tanımını yapacak olursak; kişisel veriler, tanımlanmış ya da tanımlanması mümkün bir gerçek kişiye göre karakterize edilen bilgiler anlamına gelir. Başka bir deyişle, kimliği açıkça belli olan ya da en azından bir şekilde belirlenebilen, tamamlayıcı bilgiler elde edilerek bir kişi hakkında oluşturulan bilgiler, kişisel verilerdir. Sonuç olarak, kişisel verilerin üçüncü bir kişiye, veri konusunun kim olduğunu kolay bir şekilde anlamaya ya da daha fazla araştırma yapmak suretiyle imkân tanıdığı açıkça söylenebilir.[157] Örneğin, IP adresleri ve davranışsal reklam profilleri, veri ve kişiler arasında bir bağlantı yapılmasa bile, kişiyi tanımlamaya yardımcı bilgiler olarak kabul edilir.[158]

Kişilerin konu olduğu bilgiler olarak adlandırılan kişisel veri, belirli ya da belirlenebilir özellikteki bir kişiyle ilgili dolaylı veya doğrudan bağlantısı olan her türlü bilgiyi ifade etmektedir[159]. Kişiyle ilintili isim, yaş, medenî durum, mail adresi, telefon numarası, pasaport bilgileri, resim ve ses, parmak izi, aile bilgileri, sağlık durumu gibi bilgiler kişisel veri niteliğindeki bilgilerdir.[160]

Kişisel verilerin resmi yürürlük kazanmış metinler üzerinde yapılmış olan tanımlara baktığımızda; ulusal ve uluslararası birçok belgede kişisel verinin tanımının yapıldığını görmekteyiz. Uluslararası düzenlemelerden, Avrupa Birliği'nin 95/46/AT sayılı Yönergesinin 2/a m.'sinde kişisel veri: *"Bir gerçek kişinin belirli veya belirlenebilir olması, şifre numarasına göre ya da psişik, psikolojik, fiziksel, ekonomik, kültürel veya sosyal benliği ifade eden bir veya birden fazla unsura, aidiyeti aracılığıyla doğrudan veya dolaylı olarak teşhis edilebilmesi anlamına gelmektedir"* şeklinde tanımlanmaktadır. Bununla birlikte, 95/46/AT sayılı Yönergenin 29. maddesi gereğince kurulan "Verilerin Korunması Çalışma Grubu" verinin kişisel veri olarak adlandırılabilmesi için "tanımlanabilir kişi" terimi üzerinde durulması gerektiğinin altını çizmiştir. Örneğin, bütün bir ülke göz önünde bulundurulduğunda bir isim

157 Handbook on European Data Protection Law, a.g.e., s. 36.

158 DeHert, Paul / Papakonstantinou, Va.g.elis"The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection of Individuals", 2012, S. 28, Computer Law & Security Review, s. 133.

159 Başalp, Nilgün, "Kişisel Verilerin Korunması ve Saklanması", Ankara 2004, Yetkin Yayınevi, s. 33.

160 Aksoy, Hüseyin Can "Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması", Ankara, Çakmak Yayınları, 2010, s. 12.

uygun bir tanımlayıcı olarak kabul edilemez, ancak bu isim, bir sınıftaki bir öğrenciyi tanımlamak için kullanılıyorsa bir tanımlayıcı olabilecektir.[161] Sonuç olarak, bir gruptaki bir kişiyi tanımlamak için veriler yeterliyse, bu kişi tanımlanmış bir kişi olarak kabul edilecektir. Ancak, veriler tanımlamak için yeterli değilse, bu kişi tanımlanabilir bir kişi olacaktır.[162] Bu nedenle, bir bireyle ilişkilendirilemedikçe, nesnelerle ilgili bilgilerin kişisel veri olarak görülmediği açıktır.[163]

Kişisel veri, "*Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi"*nin 2. m.'sinin (a) fıkrasında ve 1980 yılında OECD'nin yayımladığı *Kılavuz İlkeler'*in 1. m.'sinin (b) fıkrasında ise, *"belirli ya da kimliği belirlenmesi mümkün ilgili gerçek kişi hakkındaki tüm bilgiler"* şeklinde tanımlanmaktadır.

GDPR'de, kişisel veriler yerine, veri konusunun tanımı belirlenir ve kişisel veriler, veri konusunun tanımına atıfta bulunarak kısaca belirtilir.[164]

Bir bireyin kimliğini yansıtan herhangi bir bilgi, bir bankaya müşterisi tarafından verilen talimatlara ilişkin telefon kayıtları, video gözetim sistemi tarafından çekilen bir bireyin görüntüleri veya bir çocuğun nöro-psikiyatrik bir testte kullanılan ailesine ait bir resim gibi şeyler kişisel veri olarak değerlendirilebilir.[165]

Ulusal mevzuatta ise, Kişisel Verilerin Korunması Kanunu'nun[166] 3. m.'sinde uluslararası belgelerdeki kişisel veri tanımının tekrar edildiği görülmektedir. Buna göre kişisel veri, "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmıştır. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi

---

161 Article 29, Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP136, 20 June 2007, Brussels.

162 Olteanu, Florina Mariana / Olteanu, Mihalena, "Protection of Personal Data–Actual and Proposed Issues", 2012, The 7th Edition of the International Conference European Integration Realities and Perspectives, s. 303

163 Ticher, Paul, "Data Protection vs Freedom of Information, Access and Personal Data", IT Governance Publishing Ely 2008, s. 33.

164 Bkz.. Veri Öznesi Başlığı, GDPR. m.12, veri sahibi olarak da çeviriler mevcuttur. Ayrıca bkz. https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf, Erişim Tarihi, 09.03.2018.

165 Article 29, Working Party, 8.

166 RG. 7/4/2016 Sayı: 29677.

ve Gizliliğinin Korunması Hakkında Yönetmelik'in 3. maddesinde ise kişisel veri, "*belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgileri"* şeklinde ifade edilmiştir. Bu yönetmelikte gerek uluslararası kuruluşların gerekse KVKK'nın yaklaşımından farklılaşarak tüzel kişilere ilişkin verilerin de kişisel veri olarak değerlendirildiği dikkat çekmektedir. Başka bir deyişle, adı geçen yönetmelikte, gerçek kişilere ait bilgiler kişisel veri olarak kabul edildiği gibi tüzel kişilere ilişkin bilgilerin dahi kişisel veri olarak kabul edildiği müşahede edilmektedir. Daha önce belirtildiği üzere, uluslararası belgelerdeki düzenlemelerde, kişisel veri kapsamına tüzel kişilere ait bilgiler girmemektedir. Bunun nedeni ise, kişisel verilerin korunması kavramının, temel hakların ve özgürlüklerin korunması amacına yönelik olmasıdır.[167] Dolayısıyla, öyle görülmektedir ki, bir tüzel kişinin manevi varlığı olmadığı düşünüldüğünden tüzel kişilere yönelik koruyucu bir düzenleme yapılmasına gerek duyulmamıştır.

Kişisel veri, Federal Almanya Verilerin Korunması Kanunu'nda; "*Belirli ya da belirlenmesi mümkün bir gerçek kişinin, şahsi ya da maddi ilişkilerine ilişkin münferit veriler*", şeklinde tanımlanmışken, Avusturya Verilerin Korunması Kanunu'nda ise; "*Kimliği belirli ya da belirlenmesi mümkün bireyler hakkındaki bilgiler*" olarak tanımlanmaktadır.[168]

Ulusal ve uluslararası belgelerdeki tanımlamalar ışığında, kişisel verinin, bir gerçek kişinin, diğer gerçek kişilerden ayırt edilmesini sağlayan niteliklerini göstermesine imkân veren her türlü bilgi olarak tanımlanması mümkündür.[169] Doktrinde daha geniş kapsamlı tanımlamalar da yapılmaktadır. Buna göre, kişisel veri, belli veya belirlenmesi mümkün olan bir kişinin kimliği, etnik kökeni, cinsel tercihi, fiziki özellikleri, sağlık durumu, genetik bilgileri, eğitim veya istihdam bilgisi, ikamet bilgisi, banka bilgileri, ekonomik durumu ile ilgili bilgiler, emniyet makamları

---

167 Ayözger, Ayşe Çiğdem, "Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması, Yayımlanmamış Doktora Tezi, İstanbul, 2016. s. 14.

168 Şimşek, Oğuz, "4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu ve Kanunun 4. Maddesine Göre "Kayıt ve Verilerin İncelenmesi" ve Kişisel Nitelikli Verilerin Korunması", İzmir Barosu Dergisi, 2001/1, s. 94 vd.

169 Şen, Ersan, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", İstanbul Barosu Dergisi, C. 83, S. 3, 2009, s. 1197.

nezdindeki bilgileri, düşünce ve inanç dünyası, alışveriş eğilimleri, fotoğrafları, bilgisayarının IP adresi, parmak izi, sms'leri, e-mailleri, sosyal medya bilgileri ve geçmişte yaşadığı olaylara ilişkin bilgilere kadar uzayan, her türlü bilgidir.[170] Kişiyi, diğer kişilerden ayırt etmeye yarayan spesifik, özel bilgiler kişisel veri kapsamında kalmaktadır.[171] Dolayısıyla şunu kesin olarak ifade edebiliriz ki, hangi yöntem ile elde edildiği veya kayıt altına alındığına bakılmaksızın, kişiyi diğer kişilerden ayırt etmeye yarayan her türlü bilgi kişisel veridir. Bu bilgiler, kişinin sosyal, fiziksel, duygusal ve ekonomik durumuyla ilgili bilgiler olabilmektedir.[172]

Kişiye ait her türlü bilgi olduğundan mütevellit kişinin sahip olduğu kişisel veriler üzerinde hak sahibi olduğu kabul edilmektedir. Federal Alman Anayasa Mahkemesi'nin, "Nüfus Sayımı Kararında", kişilerin, kişisel özellikteki verileri üzerinde haklarının varlığına hükmettiği görülmektedir. Bu hakkın, kişisel veriler üzerinde tasarrufta bulunma ve akıbetini tayin etme hakkı olduğu vurgulanmaktadır.[173]

2.1.1.1. Kişisel Verinin Unsurları

Ulusal ve uluslararası düzenlemeler ve yukarıda yer vermeye çalıştığımız doktrindeki kişisel veri tanımlarından yola çıkarak, kişisel veri kavramının esasen üç temel unsurdan teşekkül ettiği görülmektedir. Bu çerçevede, kişisel verinin unsurlarını *"bilgi"*, "*kimliği belirli veya belirlenebilir bir kişi*" ve bu *"bilginin kişiye ilişkin olması*" olarak sıralamak mümkündür.[174] Aşağıda bu unsurları açıklamaya çalışacağız.

---

170 Akgül, Aydın "Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması", İstanbul, Beta Yayınları, 2014, s. 97; Küzeci, a.g.e., Elif, "Kişisel Verilerin Korunması, Seçkin Yayınevi, 3. Baskı Ankara 2019, s. 1; Aksoy, Kişisel Verilerin Korunması, s. 1.

171 Arslan, Çetin, "Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması" Kazancı Hakemli Hukuk Dergisi, Mart-Nisan 2011. s. 33; Dinkçi, Fatih,"Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye Örneği", Yayımlanmamış Yüksek Lisans Tezi, Çanakkale, 2014, s. 3.

172 Kaya, Cemil, "İdare Hukukunda Bilgi Edinme Hakkı", Seçkin Yayınları, Ankara 2005, s. 87.

173 Kaya, a.g.e., s. 88.

174 Tasnif için bkz.. Aksoy, Kişisel Verilerin Korunması, s. 13.

2.1.1.1.1.Bilgi

Kişisel veri kavramının unsurlarından ilki bilgidir.[175] Hem AB 95/46/AT sayılı Yönergesi hem de KVKK 3. maddesinde, kişisel veri, "*belirli veya kimliği belirlenebilir olmak şartıyla -gerçek- bir kişiye ilişki her türlü bilgi*"[176] şeklinde tanımlanmıştır. İçeriğinden bağımsız olarak, belirli veya belirlenmesi mümkün bir şahsa ait olan objektif veya sübjektif nitelikli her türlü bilgi, kişisel verinin unsurunu oluşturur[177] ve kişisel veri niteliğini taşır.

Bilginin, kişisel veri sayılabilmesi için alenî ya da gizli olmasının bir önemi yoktur.[178] Bu kapsamda kişinin ad-soyadı, fiziksel özellikleri, arabasının plakası gibi alenî bilgilerinin yanında; kredi kartı veya elektronik posta adresinin şifresi, kişisel sırları gibi gizli bilgileri de kişisel veri kapsamındadır.[179] Ayrıca, bilginin; nesnel ya da öznel nitelikte olması, biçimi, saklanma şekli ve işlenme yöntemi de bir bilginin veri olarak değerlendirilmesi bakımından herhangi bir önem arz etmez.[180] Örneğin, kişinin hem kan testi sonuçları gibi nesnel bilgileri hem de karakterine ilişkin olarak toplumda yarattığı kanı gibi öznel bilgileri kişisel veri niteliğindedir. Veri, biçimsel olarak alfabetik, sayısal, çizgisel, akustik ya da fotografik olabilir. Kâğıt üzerinde, elektronik ortamda veya bilgisayar ortamında saklanabilir. Bu konudaki bir diğer

---

175 TDK da bilgi, *"insan aklının erebileceği olgu, gerçek ve olguların bütünü, malumat; öğrenme, araştırma veya gözlem yoluyla elde edilen gerçek, malumat, vukuf; insan zekâsının çalışması sonucu ortay çıkan düşünce ürünü; genel olarak zihnin kavradığı temel düşünceler, malumat; bilim; kurallardan yararlanarak kişinin veriye yönelttiği anlam*" olmak üzere birden çok şekilde tanımlanmıştır. http://sozluk.gov.tr, Erişim tarihi, 15.06.2018.

176 Kişisel veri kavramının kapsamının çok geniş olması sebebiyle ortaya çıkabilecek karışıklıkların önüne geçilebilmesi için, 95/ 46/ AT sayılı Yönergenin 29. maddesi gereğince bağımsız bir danışma kurulu olarak kurulan "Working Party" tarafından, kişisel veri tanımı ve unsurları hakkında ayrıntılı bilgi veren, "kişisel veri kavramı" başlıklı bir rapor hazırlanmıştır. Söz konusu rapor için bkz.. ARTICLE 29 DATA PROTECTION WORKING PARTY; Opinion 4/ 2007 on the concept of personal data, http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, Erişim tarihi, 15.06.2018; Mayıs 2018 itibariyle 2016/ 679/ AT sayılı Tüzüğün 68'inci maddesiyle kurulan Avrupa Veri Koruma Kurulu, 94/ 2 maddesi gereğince Madde 29 Veri Koruma Çalışma Grubunun yerini almıştır.

177 ARTICLE 29 DATA PROTECTION WORKING PARTY, s. 6.

178 Aksoy, "Kişisel Verilerin Korunması", s. 14.

179 Üçüncü, Sümeyye Hilal, "Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması", Yayınlanmamış Doktora Tezi, Ankara, 2018, s. 6.

180 Akgül, "Kişisel Veri", s. 13; Aksoy, "Kişisel Verilerin Korunması", s. 14-16.

husus ise, bilginin gerçek olması ve doğruluğunun ispatlanması da bilgi olarak nitelendirilebilmesi için gerekli değildir.[181]

Genellikle hangi verilerin kişisel olduğunu saptamakta bir sorun bulunmamakla birlikte, doktrinde "veri" ve "bilgi" kavramları birbirlerinin yerine kullanılmaktadır ve bu kavramlar arasında fark olup olmadığı hususlarında tam görüş birliği de yoktur.[182] Kanaatimizce, veri, "bilgi kırıntısı" olarak nitelendirilmelidir. Buradan hareketle bir veriden yola çıkılarak bir bilgiye ulaşılabilir, bu bilgiden yola çıkılarak ise bir kişiye ulaşılabilir. Dolayısıyla bilgi, veriye göre daha üst düzeyde ayırt edici özellikler sunar ki bu ayırt edici özellikler bir gerçek kişi ile irtibatlandırılabilirse bu bilgi kişisel veri halini alır. Dolayısıyla veriden, bilgiye; bilgiden ise üst düzey biligiye ulaşılabileceği konusundaki görüşe biz de katılıyotuz.[183]

Öte yandan, Türk Dil Kurumu sözlüklerinde yapılan tanımlara bakıldığında, bilgi ve verinin neredeyse eş anlamlarda kullanıldığı görülmektedir. Her iki kavramın karışık ve belirsiz yapısı ve birden çok tanımlama yapılması dikkate alındığında, her iki kavram arasında farklılıklar olduğu kabul edilse de kişisel verilerin korunması konusunda birbirlerinin yerine kullanılmalarında herhangi bir sorun olmayacağı değerlendirilmektedir.[184]

2.1.1.1.2. Kimliği Belirli veya Belirlenmesi Mümkün Kişi

Bilginin kimliği belirli veya belirlenmesi mümkün bir kişiye ilişkin olması kişisel verinin ikinci unsurudur. Veri, kimliği belirli veya belirlenmesi mümkün bir kişi ile ilişkilendirilemediğinde "kişisel veri" olarak değerlendirilemez. Kimliği belirli olmaktan maksat, o kişinin bulunduğu topluluktaki diğer kişilerden ayırt edilebilir olmasıdır. Kimliğin belirlenebilir olması ise, henüz kişinin ayırt edilmemiş olmasıyla birlikte, ayırt edilebilmesinin mümkün olması halidir.[185]

---

181 ARTICLE 29 DATA PROTECTION PARTY, s. 6.

182 Küzeci, a.g.e., s. 9.

183 Van Belle, Gerald /Ruiter, Leslie, a.g.m., s.29.

184 Küzeci, a.g.e., s.12.

185 INFORMATION COMMISSIONER'S OFFICE; Data Protection Technical Guidance-Determining What İs Personal Data, s,7, https://ico.org.uk/media/fororganisations/documents/1554/determining-what-is-personal-data.pdf, Erişim tarihi, 06.09.2019.

Kişisel veya maddî ilişkiler hakkındaki veriler, belirli bir kişi ile doğrudan doğruya ilişkilendirilebildiğinde kimliği belirli bir kimsenin kişisel verisi olarak nitelendirilir. Buna karşın, verinin ek bilgiler veya zamansal, kişisel, maddî çaba ve imkânlar kullanılarak belirlenebilir bir kişi ile ilişkilendirilebilmesi halinde ise kimliği belirlenebilir bir kimsenin kişisel verisinin varlığından bahsedilir. Kimlik numarası vasıtasıyla ya da psikolojik, fizyolojik, ekonomik, sosyal veya kültürel özellikleriyle kullanılarak kişi belirli veya belirlenebilir olabilir. Bir kişinin ismi kaydedilmese bile, 60 yaşında olduğu, üç çocuk sahibi olduğu, mühendis olduğu, Ankara'da çalıştığı gibi verilerin kaydedilmesi gibi bir örnekte, bu kişinin özellikleri vasıtasıyla belirlenebilir kılınması söz konusudur[186]

Bir kişinin "belirli veya belirlenebilir olma"sı, GDPR'de kişinin özellikle isim, yer bilgisi, kimlik numarası, çevrim içi tanımlayıcı gibi belirleyiciler yardımıyla veya fizikî, fizyolojik, mental, genetik, ekonomik, sosyal ve kültürel kimliğine has bir ya da birden çok faktörle dolaylı olarak ya da doğrudan belirlenebilir olması şeklinde açıklanmıştır.[187]

Ancak istatistiksel bilgiler, yani herhangi bir kişiyle ilişkili olmayan, herhangi bir kişi ile ilişkilendirilmesi mümkün olmayan verilerin, "*kişisel veri"* şeklinde nitelendirilmesi mümkün değildir.[188]

2.1.1.1.3. Bilginin Kimliği Belirli veya Belirlenebilir Kişiye İlişkin Olması

Bilginin kimliği belirli veya belirlenmesi mümkün kişiye ilişkin olması konusunda, bilginin veya verinin isnat edilebilir olması, gerçek kişi ile arasında bir nedensellik bağının olması hususlarından söz edilmektedir. Kişisel verinin unsurlarından olan "bilginin kimliği belirli veya belirlenmesi mümkün kişiye dair olması" hususu açıklanırken "kişi" kavramının incelenmesi gerekmektedir. Kişi kavramı; hak ve borçlara sahip olma anlamına gelir ve gerçek ve tüzel kişileri kapsar. Ancak, kişisel verilerin korunması kapsamında sadece gerçek kişilerin mi kaldığı

186 Şimşek, a.g.e., s. 143

187 Üçüncü, a.g.e., s. 7.

188 Arslan, Çetin, a.g.e., s. 33-34.

yoksa gerçek kişiler ile birlikte tüzel kişilerin de mi kapsamda olduğu konusunda ulusal ve uluslararası düzenlemelerde farklılıklar vardır.

Kişisel verilerin korunmasına ilişkin uluslararası metinlerin esas olarak, gerçek kişilerin, kişisel verilerini korumaya yönelik düzenlemeler içerdiği görülmektedir. Bu kapsamda 108 sayılı sözleşmenin geçerlilik alanı gerçek kişilerle ve gerçek kişilere ait kişisel verilerle sınırlanmıştır.[189] Buna karşılık, 108 sayılı sözleşmeye taraf olan devletler, doğrudan ya da dolaylı olarak gerçek kişilerden oluşan kişi gruplarının, dernekler ve vakıfların, toplulukların, kurumların ve öteki organların hakkında da sözleşmenin uygulanabileceği şekilde iç hukuklarında düzenlemeler yapabileceklerdir.[190] Aynı şekilde OECD'nin Verilerin Korunmasına ilişkin Rehber İlkeleri de geçerlilik alanını belirli veya belirlenebilir gerçek kişiler ile sınırlamış (m. 1), tüzel kişilerin ve kişi gruplarının uygulama alanına dâhil edilmesi üye devletlerin takdirine bırakılmıştır (m. 6).

Avrupa Birliğinin Kişisel Verilerin Korunması Yönergesi de (95/46/AT) sadece gerçek kişileri koruma kapsamına almıştır. Yönergenin uygulama alanının düzenlendiği 3. maddesinde, adı geçen yönergenin gerçek kişilere ilişkin veri işleme faaliyetlerinde uygulanacağı belirtilmektedir. Buna karşılık; Danimarka, İtalya ve Lüksemburg ile Avrupa Birliğine üye olmayan İsviçre, İzlanda, Norveç gibi bazı devletler verilerin korunmasına ilişkin kanuni düzenlemelerde tüzel kişileri de koruma kapsamına almışlardır.[191]

Türk hukukuna gelince, gerek anayasal düzlemde 1982 Anayasasının 20. m'si gerekse kişisel verilerin korunması konusunda temel ulusal düzenleme olan Kişisel Verilerin Korunması Kanunu'nda yalnızca gerçek kişiler korunma altına alınmıştır.[192] Zira, kişisel verilerin korunması hakkının temel haklardan olup, özünde insanın kişiliği ile onun özel alanını korumayı amaçladığı göz önüne alındığında, kişisel verilerin korunması hakkının tüzel kişiler hakkında uygulama alanı bulamayacağı sonucuna

189 Bkz.. AK 108 nolu Söz., m. 2/ a

190 Bkz.. AK 108 nolu Söz., m. 3/ 2-b.

191 Şimşek, a.g.e., s. 122.

192 KVKK m. 2.

varılarak bu düzenlemelerin yapıldığını görüyoruz. Buna karşılık tüzel kişiler nezdinde doğrudan veya dolaylı olarak bireyler hakkındaki kişisel verilerin bulunması (örneğin, bir işletmenin ticari ilişkilerinde işletmecinin kişisel verilerin bulunması gibi) da mümkündür. Yani tüzel kişilere ilişkin verilerin, aynı zamanda gerçek kişiye ilişkin kişisel verileri de içermesi halinde bu veriler de kişisel verilerin korunması hakkı kapsamında korunurlar.[193]

O halde hukukumuza ve yaygın olan uygulamaya göre kişisel verilerin korunması temel hakkının sahibi gerçek kişilerdir. Yani kişisel verilerin korunması hakkının sahibi "herkes" olarak belirtilmesinden mütevellit ve burada herkes deyiminden gerçek kişilerin anlaşılması gerektiğinden bahisle, bu hakkın temel bir insan hakkı olduğunda şüphe yoktur. Bu bağlamda, hak sahibinin yaşayan gerçek bir kişi olması gerekliliği, kişisel verilerin korunması hakkının esas olarak bireyin, kendi kişisel verilerinin geleceğini belirleme hakkını korumasından da kaynaklanır. Bu nedenle insan öldükten sonra kişisel verilerin korunması hakkının doğrudan sahibi olamayacaktır.[194]

Özel hukuk tüzel kişilere ait verilerin korunması noktasında kişisel verileri koruma hukukundan ziyade ticaret hukukunun alanına girmesi hasebiyle ticari sır kapsamında verilerinin korunabileceği ileri sürülmektedir.[195] [196] Kanaatimizce bu görüş, tüzel kişilerin verilerinin korunması açısında son derece yetersizdir. Zira gerek kamu gerekse özel hukuk tüzel kişisi olsun, tüzel kişilerin faaliyet alanlarının sadece ticari hayatla sınırlı olmaması nedeniyle bu görüşe katılmak mümkün görülmemektedir.

---

193 Başalp, a.g.e., s. 35; Şimşek, a.g.e., s. 123.

194 Şimşek, a.g.e., s. 123.

195 Yargıtay 11. Hukuk Dairesi tarafından verilen 2004/7827 Esas ve 2007/5755 Karar sayılı kararı ile "*ticari sır kavramının en önemli unsurunun toplumun bilgisi dâhilinde olmama veya ilgili alanda rakip firmalarca bilinmeme şartının olduğu*" ifade edilmiştir. Mali projeler, işletme ve stratejik planları, makine çizimleri, müşterilerin listesi, maliyet ve fiyatlandırma konusunda bilgiler ve finansal raporlar, iş metotları, pazarlama teknikleri, detaylı proje ve planlar ile mühendislik raporlarının ticari sırra örnek olarak verilmesi mümkündür.

196 Korkmaz, İbrahim, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", Türkiye Barolar Birliği Dergisi, Sayı: 124, Yıl: 2016, s. 89.

Yine kişisel verinin son unsuru açıklanırken incelenmesi gereken bir diğer husus, verinin, kimliği belirli veya belirlenmesi mümkün kişiye "*ilişkin olması*"dır.

Genel olarak bir bilgi, bir kişi hakkında olduğunda o kişiye ilişkin addedilir. Bilgi ile kişi arasındaki ilişki, çeşitli şekillerde ortaya çıkabilir. Yani bilgi; içerik, amaç veya sonuç yönünden kişiye ilişkin olabilir.[197]

Kişi ile bilgi arasındaki bağ açıkça tespit edilebiliyorsa, bilginin içerik olarak kişiye ilişkin olduğu kabul edilir. Ancak bazı durumlarda bilginin kişiye ilişkin olduğu açıkça anlaşılamayabilir. Bazı hallerde de veri, ilk bakışta bir kişiye ilişkin değil, bir nesneye ilişkin olabilir.[198] Benzer şekilde, veri ilk aşamada bir kişi ile değil, kişinin faaliyetiyle, bir süreçle veya olayla ilişkilendirilebilir.[199] Kişi ile bilgi arasında bağlantı varsa, bilginin kişiye ilişkin olduğu açıkça anlaşılmasa da veri, kişisel veri kapsamında değerlendirilebilir. Örneğin; bir iş ilanında işe ilişkin olarak verilen maaş bilgisi kişisel veri niteliğinde değildir ancak, bu maaş bilgisinin bir kişiyle bağlantılı olduğu durumlarda, mesela söz konusu pozisyonda hâlihazırda çalışan bir kişinin olması durumunda, bilgi bu kişinin yani çalışanın, kişisel verisi sayılabilir.[200] Bilginin amaç itibariyle de bir kişiye ilişkin olması mümkündür. Somut olayın tüm koşulları göz önüne alındığında; veriler bir kişinin durumu veya davranışları hakkında değerlendirme yapabilmek veya bunları etkilemek ya da bu kişiye belirli bir şekilde davranmak için kullanılıyor veya kullanılabiliyorsa, bilginin amaç itibarıyla kişiye ilişkin olduğu kabul edilebilir.[201] Örneğin; bir şirketin çalışanlarına verdiği şirket telefonlarının arama kayıtları, şirkete dair ve/veya telefonun tahsis edildiği çalışana, aranan kişiye veya temizlik görevlisi gibi şirkete girme yetkisi olup telefona ulaşabilen kişilere ilişkin bilgi içerebilir. Bu bilgi söz konusu kişilere, bu kişilerin iş yerinden

197 ARTICLE 29 DATA PROTECTION WORKING PARTY, s. 9.

198 ARTICLE 29 DATA PROTECTION WORKING PARTY, s. 9.

199 Örneğin, kişisel banka ekstreleri veya ayrıntılı telefon faturaları gibi veriler, banka ve telefon operatörü bakımından sözleşme yapan kişiyle ilgili kişisel veri olarak kabul edilir. INFORMATION COMMISSIONER'S OFFICE, s. 10.

200 ARTICLE 29 DATA PROTECTION WORKING PARTY, s. 9; INFORMATION COMMISSIONER'S OFFICE, s. 10.

201 Aksoy, "Kişisel Verilerin Korunması", s. 29.

çıkış saatinin belirlenmesi gibi farklı amaçlar için kullanılabilir.[202] Bu gibi durumlarda bu kişisel verilerin amaç itibarı ile kişiye ilişkin olduğu kabul edilebilir.

Bilginin sonuç itibariyle de kişiye ilişkin olması mümkündür. Somut olayın özelliklerine göre, verinin kullanımı halinde kişinin hak ve menfaatleri etkileniyorsa, bilgi sonuç itibariyle kişiye ilişkin kabul edilebilir. Fakat, bunun için ortaya çıkacak muhtemel sonucun büyük bir etkiye sahip olması gerekmemektedir. Verinin işlenmesi sonucunda, kişiye diğer kişilerden farklı muamelede bulunulması yeterlidir. Örneğin; bir taksi firmasının taksilerin hareketlerini izlemek veya müşteriye en yakın taksiyi göndermek gibi amaçlarla araç takip sistemi kurması halinde, elde edilen veriler aslında sürücülere ait olmayıp otomobillere ilişkindir. Her ne kadar sistem taksi şoförlerine ilişkin bilgi toplama amacı taşımasa bile, taksi şoförlerinin performanslarını izleme, hız limitlerine uyup uymadıklarını tespit etme ve hangi saatte nerede olduklarını belirleme gibi imkânlar da sağlar. Bu sebeple, taksi konumuna ilişkin veriler sonuçları itibarıyla, taksi şoförlerine ilişkin kişisel veri niteliğinde değerlendirilebilir.[203]

Bu kapsamda göz önüne alınması gereken bir diğer husus da verinin kişiye ilişkin olup olmadığının belirlenmesinde kullanılan içerik, amaç ve sonuç unsurlarının birbirlerine alternatif olarak aranacağıdır. Yani bilgi içerik olarak kişiye ilişkinse, aynı zamanda amaç ve sonuç olarak da o kişiye ilişkin olması gerekmez. Bir bilgi; içerik, amaç ve sonuç itibariyle farklı kişilere ilişkin olabilir.[204] Bu gibi durumlarda, somut olayın özelliklerine göre bilginin ilgili kişiyi belirli veya belirlenebilir kılıp kılmadığına dikkat edilmelidir.[205]

Sonuç itibarıyla bir bilgi kırıntısının, en küçük hali ile aslında bu kırıntı dahi bir veridir, kişisel veri olarak kabul edilmesi kıstaslarından en önemlisi gerçek bir kişiye ait olması ile beraber o gerçek kişinin diğer kişilerden ayırt etmesini sağlaması; başka bir anlatımla o veriden, bilgiden hareketle veri sahibine ulaşılabilmesi gerekmektedir.

---

202 ARTICLE 29 DATA PROTECTION WORKING PARTY, s. 10.

203 Aksoy, "Kişisel Verilerin Korunması", s. 29; ARTICLE 29 DATA PROTECTION WORKING PARTY, s. 11; INFORMATION COMMISIONER'S OFFICE, s. 22.

204 ARTICLE 29 DATA PROTECTION WORKING PARTY, s. 12.

205 Üçüncü, a.g.e., s. 10.

Yani bir verinin kişisel olup olmadığının tespitinde, verinin çeşidinin ve niteliğinin önemi yoktur. Bu veri hassas bir veri olabileceği gibi alelade, ulaşılması kolay bir veri de olabilir. Aslolan o verinin sahibi ile eşleşmesi somut bir kişide tecessüm etmesidir.

2.1.2. KİŞİSEL VERİ TÜRLERİ

Kişisel veriler etki alanları göz önüne alındığında "hassas" özel nitelikli ve "anonim" genel nitelikli olmak üzere iki gruba ayrılır.

2.1.2.1. Hassas -Özel Nitelikli- Kişisel Veri

2.1.2.1.1. Genel Olarak

Bazı veri türleri, doğal yapıları gereği, hassas veriler olarak adlandırılır. Bu tür veriler, etnik köken, cinsel eğilim ve siyasi görüş gibi veri öznelerinin yani ilgili kişilerin özel yaşam tarzları hakkında önemli bir bilgi vermektedir. Uluslararası sözleşmeler ve belgelerde hassas verilere ilişkin bazı düzenlemeler olmasına rağmen, hassas verilerin neler olduğunu tam manasıyla belirlemek tartışmalı bir alan olarak görülmektedir. Doktrinde, özellikle hassas verilere yönelik bazı görüşlerde, tahdidi bir sayım ile bu veri türlerinin belirlenmesi gerektiği belirtilmektedir. Karşıt görüş olarak; verilerin hassas olup olmamasının, neden toplandıklarına ve hangi amaçla kullanıldığına bağlı olarak somut olayın özelliklerine göre belirlenmesi gerektiğidir. Bu nedenle, belli bir şekilde, bu sayılan faktörlere, başka bir deyişle somut olayın özelliklerine bakmadan, verilerin hassas oldukları ya da olmadıkları söylenemez. [206] Sürekli değişen ve dinamik bir hukuk alanı olan kişisel verilerin korunması hukukunda bunun pek uygun bir yaklaşım olmadığı ileri sürülebilir ise de; hukuki öngörülebilirlik, yargı ve idare makamlarının uygulamalarında yeknesaklık sağlanması, hassas verilerin içeriğine ve işlenmesine ilişkin yapılabilecek olan değerlendirmelerin objektif bir şekilde yapılabilmesi ve en azından idari ve adli anlamda asgari standartların sağlanması nedeniyle biz de verilere ilişkin tahdidi bir sayım yapılabileceği kanaatindeyiz.

---

206 McCULLAGH, Karen, "Data Sensitivity: resolving the conundrum", Journal of International Commercial Law and Technology C. 2, S. 4, 2007, s. 12.

Bu konuda yapılan çeşitli tanımlardan da anlaşıldığı üzere, hassas kişisel verilerin kapsamlarına girdikleri temel hak ve hürriyetlere yakınlıkları göz önüne alınarak özel bir koruma gerektiren veriler olarak kabul edildikleri söylenebilir.[207] Bu nedenle, hassas kişisel veriler Avrupa Konseyi'nin Ocak 1981 tarih ve 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme ve 95/46/AT sayılı Yönerge kapsamında özel olarak koruma altına alınmıştır. Hassas kişisel veriler GDPR'nin 9. m.'sinde düzenlenirken 95/46/AT Yönergesinin 8. m.'si temel alınmıştır.[208]

Uluslararası metinlere baktığımızda; 108 sayılı Sözleşme, 95/46/AT sayılı Yönerge, BM Kılavuzu (Yönergesi) ve GDPR'nin, hassas verilerin düzenlenmesi ve korunması bakımından daha nitelikli bir koruma sağladığı ancak OECD rehber ilkelerinin bu alanda yetersiz kaldığı görülmektedir. Örneğin; 108 sayılı sözleşmeye göre, özel yasal rejimi gerektiren özel bir veri kategorisi bulunmakla beraber bu tür veriler, doğaları gereği, işlenecek ilgili kişiler için bir tehdit oluşturabilir denmiştir. Bu nedenle, özel kategoride sayılabilecek olan hassas verilere ilişkin fazladan korumaya gerek duyularak bu tür verilerin işlenmesi özel rıza ve şartlara bağlanmıştır.[209] Sözleşmenin 6. maddesinde, hassas veriler aşağıda belirtildiği şekilde sıralanmıştır;

- ırksal veya etnik kökenleri açığa vuran kişisel veriler,
- siyasi görüşleri, dini ya da diğer inançları açığa vuran kişisel veriler,
- sağlık ya da cinsel yaşamla ilişkili kişisel bilgiler,
- mahkumiyetler.[210]

95/46/AT sayılı Yönerge uyarınca hassas veriler, doğalarının bir gereği olarak, özel yaşama ilişkin oldukları için, diğer veri türlerine göre ihlal edilmeye daha

207 Akgül, "Kişisel Veri", s. 18.

208 Ayözger, a.g.e., s. 27.

209 Handbook on European Data ProtectionLaw,a.g.e., s. 43.

210 108 s. söz., m. 6.

müsaittir. Bu nedenle de Yönerge'de bu verileri daha fazla koruma gerektiren veriler olarak tanımlanmışlardır.[211]

GDPR'nin 9. m.'si uyarınca, şu verileri hassas veriler kategorisine sokmak mümkündür;

- ırk ya da etnik kökene ilişkin veriler,
- siyasi görüşlere ilişkin veriler,
- dini veya felsefi inançlara ilişkin veriler,
- sendika üyeliğinin gösterildiği kişisel veriler,
- gerçek kişilerin kimlik tespitinin yapılması için ortaya konan genetik veriler ile biyometrik veriler,
- sağlıkla alakalı veriler,
- gerçek kişilerin cinsel hayatı ya da cinsel eğilimine dair veriler.

95/46/AT sayılı Yönerge ile karşılaştırıldığında, Yönergede genetik ve biyometrik veriler bulunmadığı için hassas veriler kavramı genişletilmiştir. Günümüzde hassas veriler; yaşam hakkının koruması, bireyin seçimlerinin kamuoyuna karşı ve sosyal yönden lekelenmeme hakkı ile temelden ilişkili olması sebebiyle bu kavramsal genişleme olumlu karşılanmalıdır.[212]

Başka bir anlatımla; Yukarıda da belirtildiği üzere GDPR m. 9'da *"ırk veya etnik kökeni, siyasî düşünceleri, dinî veya felsefî inançları ya da sendika üyeliğini açığa çıkaran kişisel veriler ile genetik verilerin, bir gerçek kişiyi benzersiz şekilde tanımlama amacıyla işlenen biyometrik verilerin, sağlığa veya cinsel hayata ya da cinsel yönelime ilişkin verilerin işlenmesi yasaklanmalıdır."* hükmüyle genetik ve biyometrik veriler de hassas veri türleri kapsamına dahil edilmiştir. 95/46/AT sayılı Yönergenin 8. m.'sinin 1. fıkrasında, üye devletlerin, bireylerin sağlık durumu ya da cinsel hayatına dair verilerin işlenmesini ve sendika üyeliği, dini inançları ile felsefi

211 Reed, Chris /Angel, John "ComputerLaw, The Law and Regulation of Information Technology", Sixth Edition, Oxford University Press 2007, s. 476.

212 Rodota, Stefano "Data Protection As a Fundamental Right" in Serge Gutwirth, Yves Poullet, Paul De Hert, Cecile De Terwangne, Sjaak Nouwt (eds) Reinventing Data Protection, Springer Science Business Media B.V. 2009, s. 78.

inançları, siyasi görüşleri, ırk veya etnik kökeni belirten kişisel verilerin işlenmesini yasaklamak suretiyle hassas veri tanımı yapılmıştır.[213] İlgili Yönergenin 10. m.'sinde de, dolaylı olarak ya da doğrudan kişilerin ten rengini, etnik kökeni ve ırkını, felsefi ve dini inançlarını, siyasi görüşlerini, sağlık ve cinsel yaşamını ve bağımlılıklarını, sendika üyeliğini, mahkûmiyet ve güvenlik tedbirlerine dair kararları, genetik ve biyometrik verilerini ortaya çıkarabilecek türden olan veriler hassas veriler olarak kabul edilmiş ve bu tanımda güvenlik tedbirleri ve mahkûmiyetler de hassas kişisel veri olarak kabul edilmiştir.[214]

Genel olarak, uluslararası belgeler ve doktrinde, hassas veriler konusunda bir fikir birliği bulunmasa da eğer veriler, özel yaşam alanı ile ilgili olarak diğer kişilerin düşüncesini, arzusunu, fantezisini ve bilgilerini tespit etmesini sağlıyor ise, bu tür veriler hassas, özel nitelikli olarak adlandırılabilir.[215]

Özleri itibarı ile kişisel veri niteliğinde olmalarına rağmen, daha fazla koruma ihtiyacı duyulan küçük bir kişisel veri grubu "hassas kişisel veri" olarak adlandırılır.[216] Hassas veriler, açıklanmaları halinde ilgili oldukları kişinin zarar görmesine ya da bu kişi aleyhine ayrımcılık yapılmasına yol açabilecek nitelikte olan kişisel verilerdir. Hassas verilerin kapsamında, politik ve dini düşüncelere dair veriler, etnik kökene dair veriler gibi bireyin hayatının dar alanına ait olan veriler bulunmaktadır.[217] Zira, bu veri grubuna dahil edilen verilerin, yüksek risk faktörü olarak değerlendirilen "ayrımcılık tehlikesi" bulundurmaları, bu verilerin ortak özelliği olarak belirtilmektedir.[218]

Hassas veri olarak nitelendirilen ve daha fazla korunan bu değerler, daha ziyade kişilik değerleri içinde yer aldığından ve işlenmeleri durumunda ait oldukları kişi hakkında ayrımcılık yapılmasına neden olma riski taşıdıklarından, hassas verilerin diğer verilere oranla daha özel olarak korunmaları, gerçekten de aynı zamanda kişilerin

213 Kaya, "Hassas Veriler", s. 318.

214 Kaya, "Hassas Veriler", s. 318.

215 Bloustein, Edward J., "Privacyas an Aspect of Human Dignity: An Answer to Dean Prosser", 39 N.Y.U. L. Rev. 962 (1964), s. 1023.

216 Kaya, Cemil, "Avrupa Birliği 1995/46/EC Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", İÜHFM, C. LXIX, S. l -2, 2011, s. 318.

217 Şimşek, a.g.e., s. 121.

218 Başalp, a.g.e., s. 23.

kişilik haklarının da korunmasına yardım etmektedir.[219] [220] Nitekim bu verilerin başkaları tarafından öğrenilmeleri gibi durumlarda, bu verilerin özellikleri icabı ilişkili oldukları kişinin mağdur olmalarına neden olabilme ihtimalleri vardır. Mesela, bir kişinin etnik kökeni veya ırkına ait kişisel verilerin öğrenilmeleri halinde, bu kişi ırkçı saldırılara maruz kalma tehlikesi ile karşı karşıya kalabilir.[221]

Öte yandan dünya hukuk sistemlerine baktığımızda, veri koruma hukuku alanında yasal düzenleme yapan, neredeyse bütün ülkeler, bazı veri türlerinin hassasiyet gösterdiğini kabul ederek bu yönde düzenleme yapma yoluna gitmişlerdir.[222] Kişisel verilerden bazılarının *"hassas veri"* olarak gruplandırılıp ayrıma tabi tutulması, bu verilerin diğer verilere oranla sıkı bir denetimden geçirilmesinin gerekli olduğu düşüncesinden kaynaklanmaktadır.[223] Örneğin; nüfus kayıtlarının ayrıntılı olarak tutulmasından sonra gerçekleşen Yahudi Soykırımı gibi travma yaratan tarihi bazı olaylar da göz önüne alındığında, kişilerin etnik kökenine veya ırkına ilişkin verilerin, diğer kişisel verilerden farklı kurallara tabi tutulmasının, söz konusu verilerin devlet kurumlarınca kötüye kullanılabileceği kaygısıyla alakalı olduğu da söylenebilir.[224]

Ulusal düzeydeki hukuk düzenlemeleri bakımından bir kişisel verinin hassas veri niteliğine sahip olup olmadığı yönündeki değerlendirme, veri koruma konusundaki yetkililerin ve son olarak mahkemelerin değerlendirmelerine bağlıdır.[225] [226] Bununla birlikte genel olarak, veri sahibinin, ırk veya etnik kökenine, dini ve politik

---

219 Şimşek, a.g.e., s. 88.

220 Zira T.C. Anayasası'nda kişisel verilerin korunması ile ilgili düzenlemenin Kişinin Hak ve Ödevleri Başlıklı İkinci Bölümünde yer alması, ülkemizde de kişisel veriler ile ilgili düzenlemelerde aynı amacın güdüldüğünü göstermektedir.

221 Başalp, a.g.e., s. 43.

222 Lloyd, Ian J., "İnformation Tecnology Law", Fifth Edition, Oxford University Pres, Oxford, 2008, s.42 (Aktaran: Kaya, Hassas Veriler, s. 317).

223 Küzeci, a.g.e., s. 230.

224 Ringelheim, Julie, "Processing Data On Racial or Ethnic Origin For Antidiscrimination Policies: How to Reconcile the Promotion of Equality with the Right to Privacy", New York, Newyork Universitiy, School of Law, 2006.

225 Küzeci, a.g.e., s. 232.

226 ABAD, hassas kişisel verilerin geniş kapsamlı yorumlanması gerektiğinin vurgulandığı Lindquivist kararında, 95/46/AT sayılı Yönergenin 8/1. maddesinin hükmünü geniş bir şekilde yorumlayarak; sağlıkverilerinin, kişinin ruhsal ve fiziksel sağlığına dair her türlü bilgiyi kapsıyor olması nedeniyle, başvurucunun ayağının incinmesi ile ilgili bilginin de sağlık verisi olmasından

düşüncelerine veya başka inançlarına, cinsel hayatına, ticari herhangi bir birliğe üyeliğine, zihinsel ya da fiziki sağlığına ya da şartlarına, kamu idaresi tarafından isnat edilmiş suça dair bilgileri içeren verilerin hassas nitelikte veri olduğu değerlendirilmektedir.[227]

Kişilerin ırki kökenleri, felsefî düşünceleri, siyasî görüşleri, dini inançları, mezhep ayrılıkları veya bunun dışında kalan inançları; sendika, dernek ve vakıf üyeliği, sağlığına veya vücuduna ilişkin özellikleri ve özel hayat ve her türlü mahkûmiyet kararları vb. şeyler ile alakalı olan kişisel veriler "özel niteliği olan" veya "hassas" kişisel veriler olarak kabul edilir. Bu verilerin işlenmesinin yasak olarak kabul edilmesi genel kabul gören bir yaklaşımdır.[228] Fakat, kamu yararının gerekli kılması gibi istisnai hallerde veya kişinin rızasının alınması gibi durumlarda bu verilerin işlenmesine izin verilebilmektedir.[229]

Kişisel Verilerin Korunması Kanunu, hassas veriler terimi yerine özel nitelikli veriler terimini benimsemiştir. Kişisel Verilerin Korunması Kanunu'nun "*Özel Nitelikli Kişisel Veriler*" başlığını taşıyan 6. m.'sinin 1. fıkrası hükmü gereğince, şu veriler *"*özel nitelikli kişisel veri" olarak adlandırılır:[230]

---

dolayı hassas veri kategorisi içinde kabul edilmesi gerektiğine karar vermiştir. Küzeci, a.g.e., s. 232 vd.

227 Room, Stewart, "Data Protection and Compliance in Context", British Computer Society, Swindon 2007, s. 40.

228 Kaya, "Hassas Veriler", s. 317-334.

229 Döner, "Kişisel Verilerin Korunması Hakkında Federal Kanun", s. 1-16.

230 Kişisel veri türlerinin bazıları, uluslararası düzeydeki düzenlemelerde ve ulusal veri koruma kanunlarında genellikle başta "*hassas veri*" olmak üzere farklı isimler ile adlandırılmışlardır. Örneğin Hollanda kişisel verilerin korunması için çıkardığı kanununda "*special personal data*"-"*özel kişisel veri*" kavramını kullanmış. http://www.dutchdpa.nl/Pa.g.es/en_wetten_wbp.aspx,E.T.29.03.2018),Yunanistan(http://www. lawandtech.eu/nea-eidiseis/data-protection-lawinGreece.html, Erişim tarihi, 11.06.2019. İsviçre (http://www.government.se/content/1/c6/01/55/42/b451922d.pdf, Erişim tarihi, 13.06.2019) ve İngiltere kişisel verilerin korunması için çıkardıkları kanunlarında (http://www.legislation.gov.uk/ukpga/1998/29/section/2, Erişim tarihi, 13.06.2019) ise "*sensitive personal data*", yani "*hassas veri*" kavramı tercih etmişlerdir. Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi'nin 6. maddesinde ise "*özellikli veri kategorileri*" kavramı kullanılmıştır (http://www.avrupakonseyi.org.tr/antlasma/aas_108.htm, Erişim tarihi, 13.06.2019). Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde de "*hassas kişisel veri*" kavramı yerine "*özel niteliği olan kişisel veriler*" kavramı kullanılmıştır. KVKK'nın 6. maddesinde "*hassas veriler*" "*özel nitelikli kişisel veriler*" olarak adlandırılmış ise de mukayeseli

- kişilerin ırkı,
- etnik kökeni,
- siyasî düşüncesi,
- felsefî inancı,
- dini, mezhebi veya diğer inançları,
- kılık ve kıyafeti,
- dernek, vakıf ya da sendika üyeliği,
- sağlığı,
- cinsel hayatı,
- ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri,
- biyometrik ve genetik verileri.

Demokratik bir hukuk devletinden bahsedilebilmesi için, bireylerin hassas nitelikli verilerinden olan siyasi görüşleri, felsefi ve dini inançları ve ahlaki eğilimlerine yönelik herhangi bir müdahalede bulunulması, tamamen kişi dokunulmazlığının ihlal edilmesi olarak nitelendirilecektir. Çünkü, hukuk devletinin temel unsurlarından birisi olan temel hakların, yalnızca mutlak zorunluluk hallerinde ve kanunla sınırlandırılabileceği ilkesinin gereği olarak, vatandaşların dini inanç, siyasi düşünce ve özel yaşamlarına müdahale edilmesinin söz konusu olmaması gerekmektedir.[231]

2.1.2.1.2. Hassas Kişisel Veri Türleri

Kişisel verilerin korunmasına dair uluslararası platformdaki ve ulusal düzenlemelerde, genellikle kişisel veri türleri arasında ayrım yapılması yoluna

hukukta genellikle "*hassas kişisel veri*" kavramı kullanıldığı için biz de çalışmamızda hassas kişisel veri kavramını kullanmayı tercih ediyoruz.

231 Şen, Ersan, "Verilerin Korunması Kanunu Tasarısı'nın Anayasa...", a.g.m., 2009, s. 1206.

gidilerek, hassas kişisel verilerin işlenmesi, hassas olmayan kişisel verilerin işlenmesine nazaran daha katı şartlara bağlanmıştır.[232]

95/46/AT sayılı Yönergenin m. 8/1'de, kişilerin etnik kökeni ve ırkına, ifade ve düşünce özgürlüğüne ve sağlığına dair verileri, hassas kişisel veri türü olarak kabul edilmiştir. Adı geçen yönergede, hassas kişisel veriler sınırlı sayıda sayılmıştır. Ancak, yönergenin 8. maddesinin 5. fıkrasında getirdiği *"üye devletler, hukuk davalarındaki kararlar veya idari müeyyidelere ilişkin verilerin de resmi makamın kontrolü altında işlenmesini sağlayabilirler."* şeklindeki düzenleme ile mahkûmiyet ve güvenlik tedbirleri kararları hakkındaki verilerin de hassas kişisel veri olarak kabul edildiği söylenebilir.[233] GDPR, m. 9.'da biyometrik ve genetik veriler de hassas kişisel veri kapsamda kabul edilmiş, mahkûmiyet ve güvenlik tedbirleri ile ilgili verilerden ise 10. m.'de ayrıca bahsedilmiştir. Aynı maddede, mahkûmiyetler ve güvenlik tedbirlerine ilişkin verilerin, bu konuda yetkili olanların kontrolü altında yapılması şartıyla, ayrıca veri sahibinin temel haklarının ve özgürlüklerinin ihlal edilmesine yol açılmadan işlenebileceği belirtilmiştir. 108 sayılı sözleşmenin 6. m.'sinde ise; siyasi görüşler, ırki köken, sağlık ve cinsel yaşam, din ve diğer inançlar ve mahkûmiyetler ile ilgili veriler hassas kişisel veri olarak kabul edilmiştir.[234]

Doktrindeki bazı görüşler, kişisel verilere ilişkin ulusal ve uluslararası hukuki metinlerde hassas verilerin sınırlı sayıda sayılmasına karşı çıkmaktadır. Bu tür düzenlemeye karşı çıkan görüşler "bağlamsal" ve "amaçsal" olmak üzere iki farklı görüşü savunmaktadırlar. Bu kapsamda *"bağlamsal yaklaşım"* görüşünü destekleyenlere göre, kişisel verilerin kendi aralarında gruplandırılması suretiyle bazılarının mutlak şekilde hassas veri olarak değerlendirilmesi söz konusu olamaz.[235] Zira bir verinin işlenmesi suretiyle veya somut durumun şartlarına göre, hassas kişisel

---

232 Deryck, Beyleveld/ David Towned, Segolene/ Rouille- Mirza and Jessica Wright, "*The Data Protection Directive and Medical Research Across Europe*", Burlington: Ashgate Publishing Limited, 2004, s. 28.

233 Kaya, "Hassas Veriler", s. 318.

234 Ayözger, a.g.e., s. 27.

235 Aksoy, "Kişisel Verilerin Korunması", s. 33.

veri haline dönüşmesi mümkündür.[236] Bu görüşe göre, bir veri hakkında hassas veri olup olmadığına dair karar vermeden önce, o verinin ait olduğu kişinin çıkarları ve bu verinin muhtemel alıcıları, toplanmasındaki amaç, işlenme şartları ve ilgili kişiler açısından doğabilecek muhtemel sonuçlar bir arada değerlendirilirek bir verinin hassas veri olup olmadığı değerlendirilmelidir. 95/46/AT sayılı Yönergeye uyum sağlamak için gerekli yasal düzenlemeleri yapmadan önce Avusturya ve Alman hukukunda bu görüş benimsenmişti. Her ne kadar haklarında veri işlenen kişilerin çıkarları yönünden bu görüşün uygulanması daha uygun ise de; bu görüş benimsendiğinde sektörel düzenlemeler yapılması gerekli olacağından, bu görüşün uygulanmasının zor olacağı ve yüksek maliyet gerektireceği nedenleriyle bu görüş eleştirilmektedir.[237]

Bu konudaki bir diğer yaklaşım olan *"amaçsal yaklaşım"* görüşünü savunanlara göre ise; bir verinin hassas veri olup olmadığına dair değerlendirme, o verinin işlenme amacı göz önüne alınarak yapılmalıdır. Yani, verinin işlenmesinin amacı ortaya konulmalı, bu amacın hassas türden bir veriyi açığa vurma olup olmadığı tespit edilmelidir. Bu görüş, sadece ve direkt olarak hassas türden verileri kasten açığa vurma amacını taşıyanları hedef alarak, bu konuda açılabilecek dava sayısında biraz azalmaya neden olacağı savunuluyorsa da açığa çıkarılan verinin hassas veri olup olmadığı yönündeki değerlendirmeyi somut olayda kimin yapacağı sorununun gündeme geleceği gerekçesiyle eleştirilmektedir.[238]

Bağlamsal yaklaşımda; bir verinin, hassas veri tayin edilerek o kategoride değerlendirilmesi reddedilerek kişisel verinin tetkik edilmesi, bu tetkik yapılırken veri sahibinin sübjektif durumu ile beraber somut olayın özellikleri göz önünde bulundurularak verinin hassas veri olup olmadığının tayin edilmesi gerektiği ileri sürülmüştür. Buradan hareketle bir kimse için alelade veri sayılan bir bilginin başka bir kimse için hassas sayılması mümkün görünmektedir. Amaçsal yaklaşımda ise; verinin işlenme amacı ön plana çıkarılarak verinin işlendiği amaç, kişi için hassas ve alelade olmayan bir nitelikte ise, o veriyi hassas veri sayma eğiliminde olduğu

---

236 Cammilleri Anne/ Clarie Levallois, "Data Protection in the European Union", Bruxelles, 2007, s. 26.

237 Aksoy, "Kişisel Verilerin Korunması", s. 33.

238 Aksoy, "Kişisel Verilerin Korunması", s. 34.

görülmektedir. Kanaatimizce hukuki öngörülebilirlik, veri işleme faaliyetlerinde yeknesaklık sağlanması ve işleme faaliyetlerinde tereddüt oluşmaması bakımından hassas verinin tayini hususunda geliştirilen teorilerden amaçsal yaklaşım teorisinin daha avantajlı ve uygulanabilir olduğunu söyleyebiliriz. Diğer taraftan hassas verilere ilişkin yapılan düzenlemelerde, bu verilerin ne olduğunun objektif kriterlere göre belirlenmesi ve her olayda farklı uygulamanın önüne geçilmesi açısından, amaçsal yaklaşımın daha isabetli olduğunu belirtmeliyiz. Böylelikle hem uygulayıcılar hem de denetleyici makamda bulunan otoriteler ve yargı erki için hassas verinin tespitinin yapılmasının daha kolay ve objektif şekilde yapılabileceğini düşünmekteyiz.

Avrupa Hukukunda, AK ve AB, kişisel verileri farklı gruplara ayırarak bu türleri birbirinden ayrı tutmaktadır. Avrupa Birliği kişisel veri türleri içinde *"hassas kişisel veri"* adıyla tamamen yasal olan bir sistem kurmuştur.[239] [240]

AB tarafından hazırlanan 95/46/AT sayılı Yönergenin "*Özel Veri Kategorilerinin İşlenmesi*" başlığını taşıyan 8. maddesi üye Devletlere, ırk, etnik köken, politik düşünce, din ya da felsefi inanç, ticari birlik üyeliği ve sağlık ya da cinsel yaşamla alakalı verileri açığa vuracak şekilde kişisel verilerin işlenmesini yasaklamak suretiyle hassas verileri korumaya almıştır.[241] Yönergenin, hassas verilerin belirlenmesi için benimsediği yaklaşım, 8. maddesinde "hassas veri" olarak kabul edilen veri türlerinin, daha ziyade 2. Dünya Savaşından sonra baş gösteren ayrımcılık karşıtı ve insan onurunu korumaya çalışan görüşlerin bir yansıması olduğu noktasında eleştirilmektedir. Çünkü, bilhassa teknolojik alandaki gelişmelerle birlikte 21.yy ihtiyaçları da farklılık göstermekte ve bununla birlikte son zamanlarda, yönergede hassas veri olduğu belirtilen verilerden bazılarının önemini yitirdiği, buna karşın hassas veri olarak yer verilmeyen bazı veri türlerinin ise daha fazla korunması gerekliliğinin zamanla arttığı değerlendirilmektedir. Bu bağlamda, mesela, yönergede

---

239 Cammilleri and Levallois, a.g.e., s. 7.

240 Avrupa Birliğinin bütünleşme projesinde en temel 2 hedefin ortak pazarın gerçekleşmesi ile vatandaşların temel hak ve hürriyetlerinin korunması olduğunu söylemek mümkündür. Birliğin bu hedeflere ulaşmak amacıyla kişisel verilerin korunması hukuku içerisinde "*hassas kişisel veri*" adı verilen hukuki bir sistem kurduğu görülmektedir. Cammilleri and Levallois, a.g.e., s. 7.

241 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT/, Erişim tarihi, 14.06.2019.

hassas veri kategorisinde görülmeyen mali veriler Finlandiya, Hollanda Danimarka, Portekiz, Yunanistan ve Fransa gibi ülkeler tarafından ulusal veri koruma kanunlarında özel korumaya alınmışlardır.[242]

Hassas kişisel veriler hakkında AB ile AK'nın yaptığı yasal düzenlemelerden, bu iki örgütün hangi verilerin hassas veriler olduğu konusunda farklı yaklaşım içinde oldukları anlaşılmaktadır. Kişilerin politik düşüncelerine, dini inanışlarına, ırkına, sağlığına ve cinsel yaşamına ait veriler hem 108 sayılı sözleşmede hem de 95/46/AT sayılı Yönergede hassas veri türleri olarak sayılmıştır. Ancak her iki örgütün hassas veriler ile ilgili düzenlemeleri; kişilerin etnik unsurları, felsefi düşünceleri, diğer inançları ve ticari birliğe üyelikleri gibi hususlarda farklılık göstermektedir. 95/46/AT sayılı Yönergede felsefi düşünceler, etnik unsur ve ticari birlik üyeliği hassas veri olarak nitelendirilmişken, diğer inançlar ise 108 sayılı Sözleşme'de hassas veri olarak kabul edilmiştir.[243] [244]

Üye devletlerin, 95/46/AT sayılı Yönergede belirlenen asgari düzenlemeyi sağlamaları halinde, kendi ulusal mevzuatlarında yönerge ile düzenlenenden daha kapsamlı bir şekilde hassas veri düzenlemesi yapmaları mümkündür. Bu nedenle üye olan devletlerin kendi ulusal mevzuatlarında hassas veri kategorisinde kabul ettikleri veriler de farklılık gösterebilmektedir. Örneğin; üye devletler, kişilerin suç veya ceza

---

242 Aksoy, "Kişisel Verilerin Korunması", s. 33.

243 Cammilleri and Levallois, a.g.e., s. 18.

244 Avrupa Birliği ülkelerinde kişisel verilerin korunması hakkındaki yasal düzenlemelere bakıldığında, hassas kişisel verilerle ilgili belirlemeler arasında farklılıklar olduğu görülmektedir. AB ülkelerinden Çekya, Estonya, Yunanistan, Avusturya, İtalya ve İngiltere'de kişisel veriler hakkındaki kanunlarında "hassas kişisel veri" kavramı tanımlanmışken, Almanya, Finlandiya, Fransa, Polonya, İsveç ve Hollanda gibi devletlerin yasalarında ise, "hassas kişisel veri" herhangi bir tanıma yer vermeden, Yönergede olduğu gibi söz konusu verilerin işlenmesi yasaklanmıştır. Ancak 95/46/AT sayılı Yönergenin uygulamasında, ülkeler arasındaki terim farklılığının sözlük farklılıkları nedeniyle ortaya çıktığı da dile getirilmektedir. Bu farklılıklara örnek vermek gerekirse; Çekya Kişisel Verilerin Korunması Kanunu'nda Yönergedeki "*political opinions (siyasal düşünceler)*" ifadesi yerine, *"political attitudes (siyasal davranışlar)*" kavramına yer vermiştir. Benzer şekilde, Fransız Kişisel Verilerin Korunması Kanunu'nda "dini ve felsefi inançlar" yerine "dini ve felsefi düşünceler (religious and philosophical opinions)" teriminin kullanıldığı görülmektedir. İngiltere'ye ait Kişisel Verilerin Korunması Kanunu'nda ise, Yönergedeki "*religious and philosophical beliefs*" ifadesi yerine "*beliefs of a similar nature (insan tabiatının inançları)*" terimi tercih edilmiş; bunun sebebi olarak da "*felsefi düşünceler*" ifadesinin muğlak bir kavram olması nedeni ile kanun koyucu tarafından uygun görülmemiş olması gösterilmiştir. Cammilleri and Levallois, a.g.e., s.25; Mullock, James Piers Leigh- Pollit, "*The 1998 Data Protection Act. 2*", the United Kingdom, 2000, The Stationery Office Limited, s. 29.

bilgilerinin hassas kişisel veri olarak kabul edilip edilmeyeceği konusunda farklı yaklaşım sergilemişlerdir.[245]

Kişisel Verilerin Korunması Kanununda "*hassas kişisel veri*" kavramı yerine "*özel niteliği olan kişisel veriler*" kavramının kullanıldığını daha önce belirtmiştik. KVKK'nın 6. maddesinde *"kişilerin ırkı", "etnik kökeni", "siyasi düşüncesi", "felsefî inancı", "dini, mezhebi veya diğer inançları", "kılık ve kıyafeti", "dernek, vakıf ya da sendika üyeliği", "sağlığı", "cinsel hayatı", "ceza mahkumiyeti ve güvenlik tedbirleri", "biyometrik ve genetik"* verileri hassas veri olarak sayılmıştır.[246]

Öte yandan, kişinin sağlığı hakkında bilgiler hassas veri türünden kabul edilerek yüksek düzeyde koruma altına alınmıştır. Bu nedenle kişinin sağlığı hakkındaki verilerin işlenmesine diğer verilerin işlenmesinden daha çok sınırlama getirilmiştir.[247] Kişilerin sağlık verileri geçmişi, şimdiki zamanı ve geleceğine ilişkin ya da fiziksel veya zihinsel sağlığı ile ilgili olabilir.[248] Genel anlamda sağlık bilgileri kapsamına özür durumuna ilişkin veriler (ör: Estonya), alkol ve uyuşturucu bağımlılıklarına ilişkin veriler (ör: Polonya ve İzlanda), tıbbi ilaç kullanımına ilişkin, cinsel yaşam ve cinsel davranışlara ilişkin veriler (ör: İzlanda), cinsel yaklaşımları ve cinsel hayatı, hastalık sağlık, tedavi ve diğer benzer tedbirlere ilişkin veriler (ör: Finlandiya), zihinsel ve fiziksel sağlık ve duruma ilişkin veriler (ör: İngiltere) girebilir.[249]

---

245 Aksoy, "Kişisel Verilerin Korunması", s. 31.

246 Mukayeseli hukukta genel olarak benzer nitelikli veriler hassas kişisel veri olarak kabul ediliyorsa da başka yaklaşımlar da söz konusu olabilmektedir. Mesela; Estonya İzlanda, Bulgaristan ve Polonya'da "genetik bilgiler", Slovakya, Slovenya, ve Çekya'da "biyometrik bilgiler", İtalya'da "dernek üyeliği", Finlandiya'da "sosyal refah ihtiyaçları ve kapsamda alınan yararlanmalar, destek ve diğer sosyal refah yardımları," Danimarka,Yunanistan, Finlandiya, Portekiz, Fransa ve Hollanda'da "mali veriler", İngiltere'de "işlenilen ya da işlendiği iddia edilen suçlara, bu suçlar için yürütülen kovuşturmalara, bu kovuşturulmaların sonlandırılmasına ve bu kovuşturmalar sonucunda bir mahkeme tarafından verilen mahkûmiyetlere"dair veriler, hassas kişisel veri olarak sayılmıştır. Cammilleri/ Levallois, a.g.e., s.25; Room, s. 30. Ulusal kimlik numarası Estonya, Fransa, Finlandiya, Polonya, İsveç ve Yunanistan kanunlarında hassas kişisel veri olarak kabul edilmiş ve bu numaranın kullanımı ile ilgili katı düzenlemeler yapmıştır. Cammilleri and Levallois, a.g.e., s. 27.

247 Edwars Charlie/ Catherine Fieschi, "UK Confidental", United Kingdom, 2008, s. 192.

248 Cammilleri and Levallois, s. 18

249 Cammilleri/Levallois, a.g.e., s. 25; Akgül, "Kişisel Veri", s. 22 vd. ; Kaya, "Hassas Verile"r, s. 319.

Adli sicil kayıtlarına ilişkin veriler[250], bireylerin ekonomik durumları ve sosyal hayatları yönünden ciddi sonuçlara yol açabildiği için, bu verilerin kaydedilip işlenmesi de ceza hukuku kurallarının uygulanması için hassas veri olarak kabul edilip özel nitelikte korunabilir.[251]

Adli amaçla ve kimlik tespiti için DNA[252] örneklerinin alınması, bu örnekler üzerinde çeşitli analizler yapılabilmesi, bunlara ait verilerin saklanması gibi hususlar, insanın genetik yapısına ilişkin bilgilerin elde edilmesi ve bu bilgilerin incelenerek değerlendirilmesi, depolanarak saklanması ya da kullanılması ile yakından ilişkilidir. Bu nedenle DNA[253] örneklerinin alınması temel insan hakları ve özgürlükleri açısından çok ciddi öneme sahiptir.[254] Çünkü insanlar üzerinde gelişen teknolojinin yardımıyla yapılan gen analizleri, kişilerin özel yaşamlarına ve kişilik haklarına hukuki açıdan tecavüz anlamına gelebilir.[255] DNA işlemleri ve gen analizleri neticesinde elde edilen bilgilerin, kişiye ait hassas veriler olarak kabul edilmesi ve bu verilerin önemine binaen[256], bu işlemlerin herhangi bir yanlışlığa mahal bırakmadan ve gizlilik ilkelerine riayet edilerek yapılmaları gerekir.[257]

---

250 Bkz., "diğer kanunlar kapsamında koruma" başlığı.

251 Küzeci, a.g.e., s. 237

252 Bkz., "CMK kapsamında koruma" başlığı.

253 "*İnsanın genetik yapısının 30 bin kadar gene sahip büyük bir DNA molekülünden teşekkül ettiği bilimsel araştırmalarla belirlenmiştir. Gen bilimindeki ve teknolojideki hızlı gelişmeler, DNA'da bulunan şifredeki tek bir harf değişikliğinin dahi ortaya konulabileceği seviyeye gelmiştir. Günümüzde gen analizleri sayesinde insanlardaki pek çok hastalığın teşhis edilip tedavi edilebilmesi olanaklı hale gelmiştir*.", Büyükay, Yusuf, "Gen Analizleri ve Mukayeseli Hukuktaki Düzenlemeler", EÜHFD, 2005, C.IX, S. 3-4, s. 355 vd.

254 Çınar, Ülkü, "DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı Üzerine Bir Değerlendirme ve Öneriler". Terazi Hukuk Dergisi, 2008, Sayı. 21, s. 149.

255 Büyükay, a.g.m., s. 355. vd.

256 DNA profillerinin saklanması dolayısıyla Avrupa İnsan Hakları Sözleşmesi'nin ihlal edildiği iddiasıyla S. ve Marper tarafından Birleşik Krallık aleyhine AİHM'ye bireysel başvuru yapılmıştır. Başvuruyu inceleyen AİHM, DNA profili, parmak izi ve hücre örnekleri gibi verilere ilişkin kayıtların "*belirli ya da belirlenmesi mümkün bir kişi*" ile ilişkilendirilebilmesi hallerinde "kişisel veri" olarak kabul edileceğini ifade etmiştir. Fakat Mahkeme, aralarındaki niteliksel farklılıklardan dolayı bu kayıtların ayrı ayrı değerlendirilmesi gerektiği vurgulamış; "*ilgili kişinin hücre örneklerinin ve DNA profilinin bir veri bankasında tutulmasının sonuçlarının, parmak izi kayıtlarının tutulmasına göre çok daha ağır*" olduğu yönünde karar vermiştir. Bu bakımdan AİHM, yol açabileceği zararın niteliği göz önünde bulundurularak kişisel veriler arasında da bir ayrım yapılmasının mümkün olduğunu kabul etmiştir. Karar için bkz.. Küzeci, a.g.e., s. 237.

257 Çınar, a.g.m., s. 149.

Hassas kişisel veri kapsamında değerlendirilen etnik kökene ait ırki veriler, daha ziyade yakın tarihte yaşanmış olan travmatik olaylar ve günümüzde bile zaman zaman ortaya çıkabilen marjinal tepkiler nedeni ile özel olarak koruma altına alınmıştır.[258]

Kişinin ait olduğu dine, siyasi görüşlere, inanç ve felsefi düşüncelere ilişkin veriler, düşünce ve ifade özgürlüğü kapsamında değerlendirebilecek verilerdendir ve bu veriler de özel koruma ihtiyacı nedeni ile hassas kişisel veri olarak kabul edilmiştir.[259] Zira bu veriler öğrenilmeleri durumunda ilişkin oldukları kişinin farklı mağduriyetlere maruz kalmasına yolaçabilir.[260]

Bir işyerinde çalışanların sendika üyelikleri, bir müşteri için tekerlekli sandalyenin gerekli olduğuna dair otel rezervasyon bilgisi, uçakta bir yolcunun dini inancının gereği olarak yaptığı yemek seçimine ilişkin bilgi, bir çalışanın belirli bir hastalık nedeniyle ameliyat için hastaneye gittiğini gösteren bilgi, bir kişinin cinayet suçunu işlediğini gösteren bilgi, bir kişinin uyuşturucu madde bağımlısı olduğuna dair hastane kayıtları, hassas kişisel verilere örnek olarak verilebilirler.[261]

Bazı durumlarda hassas kişisel verileri doğrudan tespit etmek çok da kolay olmayabilir. Bu zorluğun aşılması için "dolaylı hassas kişisel veri" ifadesi geliştirilmiş ve bu problem çözülmeye çalışılmıştır. Bu bağlamda, mesela -*bir kişi doğrudan siyasi fikrini açıklamasa dahi*- siyasi (politik) bir dergi abonelerinin internet ortamında yayınlanması siyasi görüşlere ilişkin hassas kişisel veri niteliğinde kabul edilerek, üst düzey bir koruma sağlanmak istenmiştir.[262]

---

258 Özdemir, Hayrunnisa, "Haberleşmenin Gizliliği ve Kişisel Veriler", Erzincan Üniversitesi Hukuk Fakültesi Dergisi, C.13, Sayı: 1-2, Yıl: 2009, s. 126.

259 Henkoğlu, Türkay, "Bilgi Güvenliği ve Kişisel Verilerin Korunması", Ankara, 2015, s. 126,

260 Kaya, "Hassas Veriler", s. 319.

261 Carey, Peter,"Data Protection: A Practical Guide to UK and EU Law", 3. Edition, Oxford University Press, Oxford 2009, s. 83.

262 Murray, Andrew, "Information Technology Law (The Law and Society)", Oxford University Press, 2010, s. 475-476; Özdemir H, a.g.m., s. 127.

2.1.2.2. Anonim - Genel Nitelikli- Kişisel Veriler

Kişisel veri tanımının tersinden yola çıkarak anonim kişisel veri tanımı yapılabilir. Buna göre, bir kişi ile irtibatlandırılamayan veya bu veriden yola çıkarak bir kişiye ulaşılamayan veya kaynağı belirlenemeyen veya belirlenemez hale gelmesi veya getirilmesi neticesinde oluşan bilgiye "anonim veri" denilebilir.[263]

Anonim bilgiler genellikle; araştırma, planlama, istatistik vb. amaçlar için tutulan ve herhangi bir kişiyi belirtmeyen, kitlesel bilgi yığını şeklindeki verilerdir. Bu tür verilerin, sahibi olan kişilerle irtibatlandırılabilme ihtimalleri söz konusu olmadığından, kişisel veri olarak kabul edilmeleri mümkün değildir. Bu durumda verinin ait olduğu kişi ile veri arasındaki irtibat koptuğundan, bu tarz veriler hakkında yapılacak herhangi bir işlem kişilerin hak ve hürriyetlerinin ihlaline yol açmayacaktır.[264]

Kişisel verilerin korunması kapsamında değerlendirilen kişisel bilgilerin en önemli özelliklerinden biri, ait oldukları kişiyle birlikte geçerliliklerini devam ettirmeleridir. Bu nedenle bu verilere sağlanan koruma ilgili kişinin hayatta olduğu zaman ile sınırlıdır ve bu kişinin hayatının son bulması ile birlikte bu verilere sağlanan koruma önlemleri de belli ölçüde kalkacaktır.[265] Bunun yanında, hayatı son bulan bireyin kişisel verileri tamamen korumasız da değildir. Çünkü kişisel verilerin korunması insana tanınan temel haklardan biri olduğu için kişilerin ölmesi halinde bile bu değerler belli ölçüde koruma altında olacaklardır. Türk ve İsviçre Hukukunda, hayatını kaybeden kişilere ait olan kişisel verilerin ihlal edilmesi halinde ölen kişinin mirasçılarının kişilik haklarının zarar göreceği kabul edilerek TMK'nın 25. maddesinde düzenlenen haklara, ilgili mirasçıların sahip olduğu kabul edilmiştir.

---

263 Ersoy, Uğur, "Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması", YayımlanmamışYüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2009, s. 20.

264 Başalp, a.g.e., s. 16.

265 Boz, Ahmet, "Kişisel Verilerin Korunması; Türkiye, ABD ve AB Örnekleri", Yayımlanmamış Yüksek Lisans Tezi, Ankara: Polis Akademisi, Güvenlik Bilimleri Enstitüsü, 2014, s. 7-10.

2.1.3. KİŞİSEL VERİLERİN HUKUKİ NİTELİĞİ

Teknolojinin hızlı bir şekilde gelişmesi ile insan kişiliğine yönelik tehditler artmış ve bununla beraber, kişileri bu tehditlere karşı en üst düzeyde koruma yolları hukuk düzenleri tarafından aranmıştır.[266] Bu arayışın temelinde, teknolojik gelişmelere paralel şekilde artış gösteren veri işleme faaliyetleri karşısında, kişilerin kişisel verilerinin kolayca elde edilebilmesi, bu kişisel verilerin yine hiçbir sınırlama olmadan toplanması, kullanılması ve başka kişilere aktarılması ihtimalleri karşısında bireyin korunması yatmaktadır.[267]

Kişilere bu korumanın hangi hukuki gerekçe kapsamında sağlanacağı önemli olmakla birlikte, bu konuda görüş birliği sağlanabilmiş değildir. Kişisel verilerin özellikleri göz önüne alınarak ileri sürülen görüşleri aşağıda inceleyeceğiz.

2.1.3.1. İnsan Onuru, Bireysel Özerklik Kavramı ve Verilerin Geleceğini Belirleme Hakkı Görüşü

Kişisel verilerin korunması ile, günümüzde hızlı bir şekilde gelişen bilişim teknolojileri aracılığı ile kişisel bilgileri hiçbir sınırlama olmadan toplanan, bu verileri çeşitli şekillerde ve amaçlarla kullanılan, devredilen bireylerin korunmasını amaçlamaktadır. Bu kapsamda kişisel verilerin korunması hakkının ilkin insan onuru

266 Şimşek, a.g.e., s. 115.

267 Şimşek, a.g.e., s.,112.

ve bununla ilintili olarak da bireylerin kişiliklerini serbestçe geliştirebilmesi hakkına[268] dayandırıldığı gözlemlenmektedir.[269]

Federal Almanya Anayasa Mahkemesi'nin 1983 yılında kişisel verilere ilişkin vermiş olduğu "Nüfus Sayımı" kararında, Alman Anayasası'nın insan onurunun korunmasına dair 1/1m.'sini ve kişiliğin korunması hakkına dair 2/1. m.'sini bir arada değerlendirerek, *"bilgilerin geleceğini belirleme hakkı*" kavramını literatüre sokmuştur.[270] Çünkü, mesela, toplantı ve gösteri yürüyüşü yapmasının ya da çeşitli sivil toplum örgütlerine üye olmasının resmi makamlar tarafından kaydedildiğini ve bunun bazı mağduriyetler yaşanmasına yol açabileceğini düşünen bir kişi, bu durumdan çekinerek bu haklarını kullanmak istemeyebilir. Bu durum, *"bireyin kendi kişiliğini geliştirme hakkı"*nı zedeleyeceği gibi, bunun yanında kamu çıkarlarının zarar görmesine de yol açabilir. Zira, "özgürlükçü" bir demokrasinin gereği gibi işlemesi, bireyin topluma katılması ve toplum içinde işlev görme becerisi ile bağlantılıdır. Bundan dolayı, kişiliğin özgürce geliştirilebilmesi ve demokratik toplum yapısının sürekliliğinin sağlanması için, devlet tarafından yapılan kişisel verilerin toplanma, kaydedilme, kullanılma ve devredilme işlemlerine karşı kişinin korunması gerekmektedir. Bireyin kurmuş olduğu çeşitli ilişkilerin açığa çıkacağı zamanı ve açığa çıkmanın sınırı konusunda kişinin kendisi karar verebilmelidir. Sonuç olarak,

---

268 Federal Almanya Anayasa Mahkemesi 1983 yılında verdiği "Nüfus Sayımı" kararında bu duruma işaret ederek, parlamentoda oy birliği ile kabul edilen Nüfus Sayımı Kanununu Anayasaya aykırı bulmuştur. Mahkeme bu kararında "*Toplumun özgür bir üyesi olan bireylerin onuru hukuk devletlerinde anayasal düzenin merkezindedir. Günümüzde yaşanan hızlı teknolojik ve teknik gelişmelerin ve bu değişimlere bağlı ortaya çıkan tehdit ve tehlikeler karşısında, bireylerin kişiliğinin hukuk sistemince korunması büyük bir önem arz etmektedir. Bireylerin kendilerine ilişkin hangi bilgilerin edinildiği ve söz konusu bilgilerin kimlerin elinde olduğunu öğrenebilme imkânına sahip olamaması, bireyin kendi kararlarını verme özgürlüğünebüyük ölçüde zarar vermektedir. Özellikle teknolojik gelişmeler sonucunda otomatik veri işleme araçlarının yaygınlaşması ile verilerin sınırsız bir şekilde kaydedilebilmesi, kaydedilen verilerin her zaman ulaşılabilir olması ve kişilerindetaylı kişilik profilinin oluşturulabilme ihtimali de göz önünde bulundurulduğunda, bu durumun bireyler üzerinde psikolojik baskı yaratması ve bireylerin kamusal hayata katılımasını etkilemesi mümkün görünmektedir*." şeklinde tespitlerde bulunmuştur. Aksoy, Hüseyin Can, "The Right to Personality and Its Different Manifestations As the Core of Personal Data", Ankara Law Rewiev, Cilt: 5, Sayı: 2, Yıl: 2008, s. 241-242; "*Söz konusu Yasa ile 1983 yılında görevlilerin ev ev dolaşarak yapacakları sayımda vatandaşların sayılmasının yanında başka bazı bilgilerin öğrenilmesi de öngörülerek vatandaşlara kapsamı geniş bilgileri açıklama zorunluluğu getirilmişti, bu zorunluluğu yerine getirmeyenler için ise bazı yaptırımlar öngörülmüştür.*" Elif, Küzeci, a.g.e., s. 68

269 Şimşek, a.g.e., s. 111.

270 Akgül, "Kişisel Veri", s. 87; Küzeci, a.g.e., s. 69.

"bilgilerin geleceğini belirleme hakkı", kural olarak kişinin kendisine ait kişisel verileri üzerinde tasarrufunu sağlamayı amaçlamaktadır.[271]

Diğer taraftan kişisel verileri toplanarak sürekli izlenen ve yaşamına ilişkin bilgiler kayıt altına alınarak adeta şeffaflaşan kişinin, kişiliğini serbestçe geliştirebilmesi çok mümkün olmayabilir. Bir kişinin kendinden beklenen davranış tarzına göre hareket etmesi nedeni ile toplumsal yaşamda kişiliğini özgürce belirleyememesi hususu da söz konusu olabilir. Bu kapsamda; kişisel verilerin korunması hakkı, kişiye kendisine ait kişisel verilerin hukuka aykırı olarak hiçbir sınırlama olmadan kaydedilmesi, bu verilerin işlenmesi, paylaşılması ihtimallerine karşı bir temel hak vererek onu sıradan bir *"veri nesnesi"* olma tehlikesine karşı korumaktadır. Yani kişilerin bilgilerin geleceğini belirleme hakkı, kişiye verilerinin kullanılması üzerinde karar verme hakkını sağlamaktadır.[272]

Kişilik hakkının bir görünümü olarak ortaya çıkan *"insan onuru"*, *"bireysel özerklik"* gibi kavramlar ve *"bilgilerin geleceğini belirleme hakkı"*nın, kişisel verilerin korunmasının temellerinden birini, hatta en önemlisini oluşturduğu söylenebilir. Çünkü, kişisel verilerin korunması, sadece verilerin toplandığı andan değil, verilerin elde edilmesinden silinmesine kadar geçen tüm aşamalarda kişinin korunmasını amaçlamaktadır. Böylece, kişisel verilerin elde edilmesinden silinmesine kadar geçen süreç içinde veri sahibi olan kişiye verileri üzerinde belirli hakları kullanabilme imkânı sağlanmaktadır.[273]

2.1.3.2. Özel Hayatın Gizliliği Hakkı Görüşü

Kişisel verilerin korunması hakkının hukuki niteliğine ilişkin bir diğer görüş de özel hayatın gizliliği hakkı görüşüdür. Özel hayat[274] demokratik bir hukuk

---

271 Küzeci, a.g.e., s. 69.

272 Şimşek, a.g.e., s. 112.

273 Çokmutlu, Metin, "Türk Ceza Hukukunda Kişisel Verilerin Korunması", Yayımlanmamış Doktora Tezi, Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilimdalı, Kocaeli, 2014, s. 54 vd.

274 "*Özel hayat tüm insan hakları içinde anlaşılması en zor olanıdır. Özel hayat mahremiyet kavramı ile bağlantılı olup, mahremiyet ise; kişi, grup veya kurumlara ait olan verilerin nasıl, ne zaman ve hangi ölçüde başkalarına aktarılabileceğini belirleyebilme hakkıdır. Mahremiyetin, mekansal mahremiyet, kişi mahremiyeti ve veri mahremiyeti olmak üzere üç niteliğinin olduğu kabul edilmekte ve mahremiyetin kişi özgürlüğünün bir parçası olması nedeni ile mahremiyetin ihlal edilmesinin özgürlüğün ihlal edilmesi sonucunu doğuracağı kabul edilmektedir. Mahremiyet kişi*

devletinde vazgeçilmez nitelik taşıyan ve kişilik hakları içinde özel bir öneme sahip olan bir unsur olarak değerlendirildiği için özel hayat bireylerin kişiliğinin "*en temel çekirdeği*" olarak görülmektedir. Modern hukuk düzenlerinde, kişi tüm yönleriyle bir bütün olarak değerlendirilip, özel hayatın da bu bütün resmin bir parçası olarak kabul edilmesi mümkündür. Bu nedenle, kişiye kişiliğini özgürce geliştirmesi için yalnız ve kendi yakınları ile baş başa kalabileceği, diğer kişiler veya devlet tarafından rahatsız edilmeyeceği "özerk bir alan"ın sağlanması gerekmektedir.[275] Kişisel verilerin korunması ile kişiye içerisinde başkaları tarafından gözetlenmeksizin yalnız kalabileceği, istediği kişilerle iletişim kurabileceği, kendisini geliştirmesine olanak veren özel bir alanın korunmasına yönelik güvence verilmektedir.[276] Bununla beraber, gerek iç hukukumuzda gerekse uluslararası metinlerde özel hayat ile ilgili olarak bir tanımın yapılmasından kaçınıldığını gözlemlemek mümkündür. Bu bağlamda kesinlikle şunu ileri sürebiliriz ki, özel hayat, mahremiyet hakkının ziyadesiyle ilerisinde ve tanımlanması zor bir kavram olarak göze çarpmaktadır.

Kişisel veriler, Kıta Avrupası ülkelerinde genellikle kişilik hakkının bir parçası olarak görülmüştür. Zira, 95/46/AT sayılı Yönergesinin bazı düzenlemelerinde kişisel veriler, genellikle mahremiyet hakkıyla irtibatlandırılarak temel kişi haklarının korunması amaçlanmıştır.[277] Bu kapsamda, "mahremiyet hakkı" olarak ifade edilen hak, Türk hukukundaki "özel hayat hakkı"na karşılık gelmekte olup, hukukumuzda, özel hayat hakkı, kişilik hakkının bağımsız görünüm şekillerinden birisi olarak karşımıza çıkmaktadır.[278] Her ne kadar, özel hayatın gizliliği hakkı kişisel verilerin

gelişimi için önemli bu unsurdur.", Korkmaz Ali, "İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması", KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi, 16, (Özel Sayı), 2014, s. 99; "Mahremiyet hakkı kişilik hakkının bir görünümüdür ve bu yolla kişisel verilerin korunmasına yardım etmektedir. Kişinin ailevi durumu, sağlığı, inancı ile ilgili bilgiler gibi kişisel bilgiler o kişinin "özel alanı"na ait olup, bu bilgilerin başka kişilere verilmesi gibi, başka kişilere verilmesi riskini barındırdığı için de başka birisi tarafından saklanması, "özel alan"a müdahale etme anlamına gelecektir.", Karahisar, Tuba, "Özel Hayatın Gizliliği ve İnternette İşlenen Suçlar", II. Medya ve Etik Sempozyumu, Medya Kültür İlişkisinde Etik, s. 599.

275 Eker, Behiye Kazancı, "Kişilerin İzinsiz Görüntülerinin Alınmasının TCK m. 134 Çerçevesinde Değerlendirilmesi", DEÜHFD, C. 9, S. 1. 2007, s. 131.

276 Uncular, Selen, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", Ankara, Seçkin Yayıncılık, 2014, s. 28.

277 Ayrıntılı bilgi için ayrıca bkz. Korff, Douwe, "EC Study on Implementation of Data Protection Directive – Comparative Summary of National Laws", Cambridge, 2002.

278 Ketizmen, Muammer, "Kişisel Verilerin Korunması" Tebliğ, http//www.tbd.org.trusr_imgcdkamubib14raporlarPDFRP2-2008.pdf, Erişim tarihi, 27.06.2019.

korunması hakkından daha kapsamlı bir alanı ifade etmekte ise de kişisel verilerin korunması hakkının günümüzde kazandığı önem nedeni ile, bu hak temel ilkelerini özel hayatın gizliliğinden alsa bile ondan büyük oranda ayrılmış[279] ve kişisel verilerin korunması için farklı yasal düzenlemeler yapılmıştır.[280]

AİHS'nin denetleyicisi olan AİHM, özel hayatın tanımını yapmaktan özellikle kaçınmış, ancak "özel hayatın", kişinin "giz alanı"ndan daha geniş bir alan olduğunu vurgulamıştır. AİHM, özel hayatı tanımlamanın çok mümkün ve -aslında gerekli de olmadığını- Niemietz v. Almanya kararında: *"Mahkeme "özel hayat" ifadesinin tam tanımının yapılmasının mümkün olduğu ya da bu şekilde bir çabanın gerekli olduğu kanaatinde değildir. Ayrıca "özel hayat" kavramını, bireyin kişisel yaşamını istediği tarzda yaşayabileceği bir "giz alanı" ile sınırlamanın ve bu alanın haricinde kalan dış dünyanın bu alandan bütünüyle ayrılmasının onu aşırı sınırlandıran bir yaklaşım olacağını söylemek mümkündür. Özel hayata saygı diğer insanlarla ilişki kurmak ve bu ilişkileri geliştirmek hakkını da bir dereceye kadar kapsamalıdır…"* şeklinde ifade etmiştir. Diğer benzer davalarda da aynı anlayışı sürdüren Mahkeme, Niemietz v. Almanya kararına[281] atıflar yaparak özel hayat kavramının tam olarak tanımlanamayacağını tekrarlamıştır.[282]

AİHM yine Niemietz - Almanya kararında *"…Özel hayat kavramını, bireyin kişisel hayatını istediği gibi yaşayabileceği bir iç alanla kısıtlamak ve bu alanın dışında kalan dış dünyayı bu alandan tamamen hariç tutmak aşırı sınırlayıcı bir yaklaşımdır. Özel hayata saygı, başka insanlarla ilişki kurmak ve söz konusu ilişkileri geliştirmek hakkını da bir dereceye kadar içermelidir…"*[283] diyerek özel hayatla ilgili

279 Kişisel verilerin korunması hakkı özel yaşamın gizliliği hakkının "özellik" taşıyan bir türü ise de, kişisel verilerin korunmasına özgü bazı gereklilikler yüzünden ayrı bir alan olarak değerlendirilmeye başlanmıştır. Zira, özel hayatın gizliliğine dair benimsenen ilkeler ve geleneksel yaklaşımların teknolojinin gelişmesiyle kişisel verilerin korumasında yetersiz kalınmasına neden olduğu, tarihsel süreç içinde kişisel verilerin korunmasının özel yaşamın gizliliği hakkından ayrılmaya başladığı ifade edilmiştir. Küzeci, a.g.e., s. 70.

280 Küzeci, a.g.e., s. 74.

281 AİHM Kararı: Niemietz v Almanya, Başvuru No: 13710/88, Tarih: 16.12.1992. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-57887, Erişim tarihi, 27.06.2019.

282 Salihpaşaoğlu, Yaşar, "Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme", GÜHFD, C. 17, Yıl: 2013, Sayı: 3, s. 234.

283 Üzeltürk, Sultan, "1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı", İstanbul, 2004, Beta Yayınevi.

başka önemli tespitlerde de bulunmuştur. Bu kararda, kişinin özel hayatının, hayatın iç alanıyla sınırlandırılmaması gerektiği, dış dünyanın iç alandan tamamen ayrılamayacağı vurgulanarak, bireyin çeşitli ilişkiler kurabilmesi ile bu ilişkileri geliştirme hakkının da özel hayat kavramı içinde olduğu değerlendirilmiştir.

Bir bireyin, cinsel ilişkileri de dâhil olmak üzere, farklı ilişkiler içine girebilmesi ve cinsel kimliğini belirleyip bu kimliği benimseme, telefon görüşme içerikleri, özel olarak yapılan haberleşmeye müdahale etme amacıyla gizli teknolojik cihazların kullanılması, kişiler hakkında, kişilerin rızası alınmadan devlet eliyle bilgi toplanması, mecburi olan tıbbî tedaviler, diğer kişilerle ilişki kurup bu ilişkileri geliştirebilme özel hayat kapsamında kabul edilebilir.[284]

Özel hayatın doktrinde *"herkes tarafından bilinmeyen, özel araştırma ve bilgi edinmeyle sağlanan kişiye ait hususlar", "kişinin sadece kendisi için saklı tuttuğu ve başkalarının bilgisinden uzak kalmasını istediği yaşam görünümleri", "bireyin kişiliğini geliştirmek ve manevi değerlerine güvence sağlamak için başkaları tarafından bilinmesini istemediği hususların oluşturduğu ve korunması hukuken gerekli görülen hayat üzerindeki hakkı", "kişilerin gizli hayat alanlarında yapmış oldukları faaliyetlerin başkaları tarafından bilinmemesini istedikleri taraflar"* şeklinde çeşitli şekillerde tanımlaması yapılmış olup, bu tanımların ortak noktası ise sadece kişiye ait olan bir alan bulunması ve bu alanın başkaları tarafından bilinmemesidir.[285]

AİHM'nin, çeşitli kararlarında, özel hayatın tanımının yapılmasının mümkün ve gerekli olmadığını belirterek genel bir tanım yapmaktan kaçındığını yukarıda ifade etmiştik. Bununla birlikte, AİHM çeşitli içtihatlarında, doğum yeri, medeni durum, cinsiyet ve diğer kişisel veriler ile ilgili bilgileri toplamaya ilişkin uygulamaların, fotoğraf, parmak izi veya bunlar gibi kişisel bilgilerin kaydedilmesinin; tıbbi verilerin toplanmasının veya tıbbi gerekçelerle kayıtlarının tutulmasının, sağlık hizmetleri ile

284 Kılınç, a.g.m., s. 1100.

285 Kılınç, a.g.m., s. 1100.

sosyal hizmetler ve vergi benzeri idari nitelikli konuların düzenlendiği "*bireysel kimlik belirleme sistemi*"nin kişisel veriler niteliğinde olduğuna dair tespitler yapmıştır.[286] [287]

Burada, özel hayat kapsamında yer almayan bazı verilerin kişisel veri kapsamında değerlendirilip değerlendirilemeyeceği sorunu gündeme gelmektedir. Kişisel veri kavramının, özel hayat alanında yer almadığı için üçüncü kişilerden gizlenmesi beklenmeyen şeyleri de kapsayabileceği ileri sürülmüştür. Mesela, kişinin herhangi bir sendikaya üye olduğu bilgisi, üçüncü kişiler açısından, gizli tutulması gereken bir özel hayat olayı olarak kabul edilemeyecekken, bu hususun, hukuka aykırı bir şekilde kaydedilmesi durumunda bu bilgi kişisel veri niteliğine dönüşecektir.[288] Zira, AİHM Rotaru / Romanya kararında[289] *"Ayrıca kamuya açık bilgiler, düzenli olarak toplandığında ve yetkili makamlar tarafından dosyalarda saklandığında da özel hayat kapsamına girebilir. Bu durum özellikle söz konusu bilgiler kişinin geçmişine aitse daha da geçerlidir…"*[290] demek suretiyle aslında özel hayatın gizliliği kapsamında değerlendirilmeyecek verilerin, kişi hakkında düzenli olarak toplanıp dosyalanması halinde özel hayat kapsamına gireceği kabul edilmiştir.

Özel hayatın korunmasının kapsamı hakkında her ne kadar görüş birliği yok ise de özel hayatın birbirinden farklı koruma dereceleri bulunan üç alanının olduğu kabul edilmektedir. Bu alanlar ise, "*ortak alan", "özel alan"* ve "*gizli alan"* dır.

2.1.3.2.1. Ortak Alan

Ortak hayat alanı, topluma açık olan, başka kişiler tarafından bilinmesinde herhangi bir sakınca bulunmayan, başkalarının girebildiği genel alandır. Kişiler bu hayat alanlarında yaşarken bu alana dair şeyleri gizleme gereği duymazlar. Örnek vermek gerekirse, ortak alan, bir kimsenin çeşitli yerlerde kültürel faaliyetlerde bulunması, alışveriş merkezi gezileri, toplu ulaşım araçlarını kullanması gibi, kamuya

---

286 Salihpaşaoğlu, a.g.m., s. 234.

287 Ayrıntılı bilgi için bkz..çalışmamızın "AİHM İçtihadı" bölümü.

288 Keklik, Ramazan, "Özel Hayatın Gizliliğini İhlal Suçları", 2012, Ankara, Adalet Yayınevi, s. 27.

289 AİHM Kararı: Rotaru v Romania, Başvuru No: 28341/95, Tarih: 04.05.2000. Kararın İngilizce tam metni için bkz.. http://hudoc.echr.coe.int/eng?i=001-58586, Erişim tarihi, 27.06.2019.

290 Keklik, a.g.e., s. 27.

açık olan alanlarda gerçekleştirilen faaliyetlerden oluşan alandır.[291] Ortak alan kapsamının belirlenmesinde kişinin statüsü de belirleyici bir etken olabilmektedir. Yani, kamuoyunca tanınan resmi kişilerin veya sanatçıların ortak yaşam alanı ile normal bir kişinin ortak yaşam alanı pek tabii birbirinden farklıdır. Bu kapsamda kamuoyunca tanınan kişilerin özel hayatlarının sınırları normal insanlara göre daha dar olabilir ve hatta bazen ortadan kalkmış bile olabilir.[292]

2.1.3.2.2. Özel Alan

Özel alan, kişinin istemesi halinde ancak, en yakın kişilerle paylaşabildiği, aslında gizli olan ve birtakım sırlar barındıran bir alandır. Bir diğer deyişle, kişinin aile bireyleri, arkadaşları veya dostları, akrabaları veya iş arkadaşları ile paylaşmayı seçtiği yaşam alanı özel alandır. Bu nedenle, tüm bireyler, özel alanı kapsamında kalan şeylerin gizli kalmasını isteme hakkına sahiptir. Yani, bireyler özel yaşam alanında kalan konuların başka kişiler tarafından bilinmesini istemeyebilirler. Özel alan, aşağıda açıklayacağımız, gizli alana nispeten daha aleni ise de bu alenilik, toplum gözü önünde bir aleniliği gerektirmemektedir. Bu alenilik sadece, olayların meydana geliş şekilleri itibarı ile belirli vasfa sahip ve belirli sayıda kişiyle paylaşımın söz konusu olmasını ifade eder. Yani bir kişinin nişanlandığı kişi, arkadaşının kim olduğu, çeşitli ailevi sorunları gibi konular sadece kişinin kendisini ve belirli kişileri ilgilendirir. Kişinin özel alana ait olayları sadece istediği kişilerle paylaşması nedeniyle, özel alana giren olayların üçüncü kişiler tarafından yayılması halinde, kişinin özel yaşam alanı ihlal edilmiş olacaktır.[293]

Kişinin özel hayatının hukuken korunması kapsamına; kişinin itibar, şöhret ve onurunun, haksız fiiller karşısında korunması, zihinsel ve fiziksel dokunulmazlığının korunması, kişinin adı, kimliği ve fotoğrafının haksız kullanımlar karşısında korunması, kişinin izlenme, gözetlenme ve tacizlere karşı korunması, meslek sırrı kapsamına dahil olan bilgilerin açıklanmasına karşı korunması gibi konular girer.[294]

---

291 Kılınç, a.g.m., s. 1101.

292 Kılınç, a.g.m., s. 1102.

293 Özbek, Veli Özer, "Yeni Türk Ceza Kanunun Anlamı (Açıklamalı, Gerekçeli, İçtihatlı)", C. 2 (Özel Hükümler), Ankara, 2008, Seçkin Yayınevi, s. 916.

294 Üzeltürk, a.g.e., s. 169 vd.

Kişinin özel hayatının korunması kapsamına giren konulardan yola çıkarak bireylerin kişisel verilerinin hayatın özel alanı kapsamına girdiği söylenebilir.[295]

2.1.3.2.3. Gizli Alan (Giz Alanı)

Hayatın özel alanı kapsamında derecelendirilen üçüncü alan sır alanı da olarak ifade edilen gizli alandır.[296] Kişi, gizli alanda başkalarının bilmesini istemeyeceği bir hayat sürdürmekte ve bu alanda yaşanan olayları, sadece kendisine yakın hissettiği kişilerle özel olarak paylaşmaktadır. Çünkü; gizli hayat alanı, bir kişinin yaşamının en gizli ve özel kısmını oluşturmaktadır. Kişilerin sırları, düşünce ve duyguları, ümit ve korkuları, kişisel tercihleri gibi konular gizli alan kapsamında değerlendirilir. Gizli alan her türlü müdahaleye karşı hukuki koruma altında ve dokunulmaz olup, bu alan kapsamında olduğu değerlendirilen bilgiler basın ve yayına kapalıdır. Bu yüzden kişinin, felsefi veya dini inançları ve siyasi görüşleri, sağlığı ve cinsel hayatı ile ilgili, hassas nitelikteki verilerin bu alan kapsamında kaldığı söylenebilir.[297]

Hayatın gizli alanı olarak kabul edilen alana girilmesi ağır bir hak ihlali olduğundan, bu alan her türlü müdahaleye karşı mutlak bir şekilde korunmaktadır. Gizli alan her türlü müdahaleye karşı "mutlak" bir şekilde korunmuşsa da hayatın özel alanı "kural olarak" üçüncü kişilere ve devlet müdahalesine karşı korunmuş, ancak bu alan dokunulmaz olarak kabul edilmemiştir. Bu hakka, yani alana, suçla etkin mücadele veya başka kişilerin hak ve özgürlüklerinin korunması gibi nedenlerle müdahale edebilmek mümkün olduğundan, bu alanda sağlanan korumanın nisbi koruma olduğu ifade edilmiştir. Yine kural olarak, hayatın ortak alanı korumasız olarak görülse de normal bir kişinin umumi bir yerde otururken haber değeri olmamasına rağmen, kişinin rızası olmadan fotoğrafının çekilmesi gibi bir örnekte, kişinin fotoğrafının bu şekilde çekilmesi haksızlık teşkil edecek, hukuka aykırı olacaktır.[298]

---

295 Çokmutlu, a.g.e., s. 58.

296 Aksoy, "Kişisel Verilerin Korunması", s. 52.

297 Kılınç, a.g.m., s. 1102.

298 Özbek, a.g.e., s. 917.

2.1.3.3. Mülkiyet Hakkı Görüşü

Kişisel verilerin korunmasının hukuki niteliğine ilişkin görüşlerden bir diğeri olan mülkiyet hakkı görüşü, özellikle Amerika hukuk sistemi ve kaynaklarında öne sürülen görüştür. Buna göre, kişisel veriler hem kişiliğin bir uzantısı hem de kişiliğin bir ürünüdür. Bu kapsamda; kişinin, kendisi hakkındaki kişisel verilerin sahibi olduğu kabul edilip, kişilerin, mülkiyetindeki bu verilerin hangi şartlar altında kullanılacağını kontrol etmesine olanak sağlanmalıdır.[299] Bu görüşe göre, mülkiyet hakkının temeline dayanan bir korumanın kişisel verilere sağlanması halinde, mülkiyet hakkı ile tanınan geniş yasal korumalardan veri sahibi kişi yararlanarak, kendisine ait olan bilgiler üstünde kapsamlı bir denetim hakkına sahip olması mümkün olabilecektir.[300]

Kişisel verilerin mülkileştirilmesi gerektiğini ileri süren bu görüşe göre kişisel veri öznesi çeşitli anlaşmalar yaparak, kendisine ait verilerin kullanımının maddi ve manevi karşılığını alabilecektir. Yani bu görüşe göre bireyler, istemeleri halinde kişisel bilgilerini satabilmeli -ki böyle bu pazarın daha adaletli bir şekilde işlemesi sağlanacaktır ya da açıklayabilmelidirler. Ayrıca bu yolla, şirketlerin kişisel verilerin toplanması ve işlenmesi nedeni ile ortaya çıkan maliyetleri benimsemek zorunda kalarak, özel hayatın gizliliğinin daha güçlü bir şekilde korunacağı da savunulmuştur.[301] Kişisel verilerin kötüye kullanılması durumunda, bu görüşe göre, veri sahibine doğrudan mahkemeye dava açma yahut uğradığı zararın giderilmesini talep hakkının verilmesi bu teorinin en güçlü yanını oluşturmaktadır. Ayrıca kişilere kendine ait profil üzerinde bir denetim olanağı ve bu hakkını mahkeme önünde savunma imkânı da sağlanırsa, ilgili kişi izni olmadan kişisel bilgilerinin paylaşımını önleyebilecektir.[302]

Bu görüşte kişisel verilerin ticari değerleri ön plana çıkmaktadır. Yani, bazı teşebbüsler, topladıkları kişisel verilerden yararlanarak, müşterilerine sundukları hizmetin kalitesini artırabilecekleri gibi, bu verileri pazarlama stratejilerini belirlerken kullanabilecek veya bu verileri üçüncü kişilere devrederek ticari kazanç

299 Küzeci, a.g.e., s. 62.

300 Akgül, "Kişisel Veri", s. 73.

301 Küzeci, a.g.e., s. 62.

302 Küzeci, a.g.e., s. 62.

sağlayabileceklerdir. Fakat geniş çaplı olarak kişisel veri toplayan, bu verileri kullanan ve üçüncü kişilere satan işletmelerin bu uygulamalarının olası olumsuz sonuçları, direkt olarak veri sahipleri üzerinde etkisini gösterebilecektir.[303]

Kişisel verileri işlenen kişilerin de verilerinin kullanımları karşılığında, birtakım kurum ve kuruluşlar para kazandığında, bu kurum ve kuruluşlardan uygun ve adil bir karşılık talep etme hakları vardır. Ayrıca, kişisel verilerinin başka kişiler tarafından kullanılmasının olumsuz sonuçlarına katlanmak durumunda kalan bireyler, bir işletme ile belli bir amaç doğrultusunda paylaşmış oldukları kişisel verilerinin, söz konusu amacın dışında kullanıldığında, bunu genellikle öğrenemedikleri için herhangi bir hak iddiasında da bulunamamaktadırlar. Fakat, mülkiyet hakkı görüşü benimsendiğinde, kişiler kendi kişisel verileri üzerinde mülkiyet hakkına sahip olacakları için, kendisine ait veri türlerinden hangilerini hangi işletmelerle paylaşacağına karar verebilecekken bu paylaşım karşılığında talep edeceği bedel konusunda da pazarlık yapabilecektir.[304]

Mülkiyet hakkı görüşünü savunanlar bu görüşün kabul edilmesi halinde aynı zamanda uygulama açısından da kolaylık sağlanacağını ileri sürmektedirler. Çünkü, bu görüşün kabul edilmesi halinde, başka herhangi bir sistem oluşturulmasına ihtiyaç kalmadan, mülkiyet hakkının korunması kapsamında kişisel verilerin korunması da sağlanabilecektir.[305]

Bununla birlikte, kişisel verilere ticari değer kazandıran mülkiyet hakkı görüşü, birçok açıdan eleştirilmiştir. Bu eleştirilerden ilki, mülkiyet hakkı kavramının niteliğinin kişisel verilerin niteliği ile uyumlu olmayacağı yönündedir. Mülkiyet hakkının en önemli niteliklerinden birinin, malın ilk sahibi tarafından satılmasından sonra, mal üzerinde yeni hak sahibi olanın bunu dilediği gibi kullanabileceği veya satabileceği göz önüne alındığında, malın malikine mülkiyet hakkının sağladığı en

303 Prins, Corien,"When Personal Data, Behavior And Virtual Identities Become A Commodity: Would A Property Rights Approach Matter? (personal data)", Scripted, Cilt: 3, Sayı: 4, Yıl: 2006, s. 274-275. (Aktaran: Aksoy, Kişisel Verilerin Korunması, s. 57).

304 Prins, "Personel Data", s. 279 (Aktaran: Aksoy, Kişisel Verilerin Korunması, s. 58).

305 Clarke, Roger, "Internet Privacy Concerns Confirm the Case for Intervention", (Internet), Comminication of the ACM, Cilt: 42, S: 2, Yıl: 1999, s. 63 (Aktaran: Aksoy, Kişisel Verilerin Korunması, s. 60).

temel yetkilerden biri olan *tasarruf yetkisinin*, kişisel veriler açısından söz konusu olabileceğinin kabulü oldukça zor olacaktır. Mülkiyet hakkı görüşüne göre, kişisel veriler yönünden tasarruf yetkisinin söz konusu olduğunun kabul edilmesi durumunda, kişisel verileri veri öznesinden bir kere rızası ile satın alan kimse, artık bu verileri veri öznesinin rızasını aramadan üçüncü kişilere devredebilmelidir. Ancak, kendi kişisel verilerini bir işletme ile paylaşan kişinin aynı veriyi başka bir kişi veya işletme ile paylaşmak istememesi söz konusu olabilir. Bu kapsamda, kişisel verilerini bir başkasına devreden veri sahiplerini, kendisine ait olan bu verilerden mutlak bir şekilde soyutlayacak olması nedeni ile mülkiyet hakkı görüşünün kişisel verilerin niteliği ile bağdaşmadığı ifade edilmektedir.[306]

Mülkiyet hakkı görüşüne getirilen bir diğer eleştiri, mülkiyet hakkının işlevine dairdir. Yani mülkiyet hakkının doğuş nedeni, doğadaki sınırlı kaynakların daha doğru dağılımının sağlanması olduğuna, doğada ise kişisel veriler bakımından herhangi bir kıtlık söz konusu olmadığına göre; bu çerçevede kişisel verilerin hukuki niteliğinin mülkiyet hakkı kapsamında değerlendirilmesi mümkün olmayacaktır.[307]

Mülkiyet hakkı görüşüne yapılan başka bir eleştiri ise, mülkiyet hakkı görüşünün uygulamadaki yani pratik sonuçlarına dairdir. Mülkiyet hakkı görüşünün kabul edilmesi halinde, veri sahiplerinin kendi kişisel verilerini üçüncü kişilere devri işlemi masraf ve süre yönünden elverişsiz olacaktır. Çünkü; kişisel verileri toplayan işletmenin toplamak istedikleri her bir veri için, o verinin malikinden izin almaları ekonomi üzerinde olumsuz etkiler yapacaktır. Zira kişilerin kendilerine ait kişisel verilerin toplanmasını, kullanılmasını ve el değiştirmesini kontrol edebilmelerinin kabul edilmesi halinde, bilginin serbest dolaşımı sekteye uğrayacağından modern ticaretin zarar görmesi söz konusu olabilecektir.[308]

2.1.3.4. Fikri Mülkiyet Hakkı Görüşü

Kişisel verilerin hukuki niteliğine ilişkin ortaya atılan son görüşün fikri mülkiyet hakkı görüşü olduğu söylenebilir. Bu görüşü savunanlar, kişisel verilerin

306 Aksoy, Kişisel Verilerin Korunması, s. 64-65.

307 Aksoy, "Kişisel Verilerin Korunması", s. 66.

308 Aksoy, "Kişisel Verilerin Korunması",s. 65.

korunmasıyla fikri mülkiyet hakkının korunmasındaki temel amacın; bilginin korunup, kontrollü dağılımının sağlanması olduğundan yola çıkarak, bu iki hak arasında amaçları yönünden bir benzerlik bulunduğunu ileri sürmektedirler.[309] Diğer taraftan, fikri mülkiyet hukukunda eser sahibinin meydana getirdiği eser üzerindeki hakları ile kişisel veri öznesinin kendisine ait olan kişisel verileri üzerindeki hakları arasında bir benzerlik bulunmasından yola çıkarak bu görüşü ileri sürmüşlerdir.[310] Yani, bu görüşte, kişisel verilerin veri öznesine, kişiye sağladığı haklar ile eser sahibine tanınan manevi haklardan olan "*eseri umuma arz yetkisi* [311] ve "*eserde değişiklik yapılmasını yasaklama yetkisi"*[312] arasında bir benzerlik bulunduğu ileri sürülmektedirler. Fikri mülkiyet hakkından kaynaklanan bu bahsedilen haklara, benzer şekilde, ilgili kişinin de sahip olduğu verileri hangi şartlar altında ve kimlerle paylaşacağına karar verme yetkisi ve üçüncü kişilerin elinde bulunsa bile kendisi ile ilişkili verilerin bütünlüğünün ve doğruluğunun korunmasını isteme yetkisi olmalıdır. Kişisel verilerin ait oldukları kişiye sağladığı haklar ile eserin sahibine sağladığı haklar arasındaki bu benzerlik esas itibariyle, fikri mülkiyet hakkı görüşünün temelini oluşturmaktadır.[313]

Bu görüş de çeşitli nedenlerden dolayı eleştiriye uğramıştır. Bu eleştirilerden biri, fikri mülkiyet hakkının bilgiyi temel alan bir hak alanı olarak nitelendirilmesi nedeni ile fikri mülkiyet hakkı ile kişisel verilerin korunamayacağına dairdir. Çünkü fikri ürünlerle ortaya çıkabilecek sorunların üstesinden gelmek, fikrî mülkiyet

---

309 Prins, "Personel Data", s. 1146 (Aktaran, Aksoy, Kişisel Verilerin Korunması, s. 60).

310 Akgül, "Kişisel Veri", s. 74.

311 "*Umuma arz yetkisi: Eser sahibinin manevi haklarından biri eserin umuma arz edilmesidir. Umuma arz, sadece bir kez gerçekleştirilebilen, eser sahibinin iradesi ile eserin tamamının veya bazı kısımlarının ilk defa olarak aleniyete sunulmasıdır. Eserin sahibinin rızası olmadan umuma sunulmuş olması halinde aleniyet gerçekleşmemiş olacaktır. Yani umuma arz, bir eserin ülkenin bütününde veya bir yöresinde aleniyete kavuşturulmasıdır. Eserin umuma arz yetkisi, eser sahibine veya yetkilendirdiği kişiye ait olup, bu yetki eserin kamuya sunulup sunulmaması hakkında karar verilmesini, kamuya sunulma zamanının belirlenmesi, sunuluş şeklini belirlemeyi ve eserin içeriği hakkında bilgi vermeyi kapsayan manevi bir haktır*.", Ateş, Mustafa, "Fikir ve Sanat Eserleri Üzerindeki Hakların Kapsamı ve Sınırlandırılması", Ankara, 2003, s. 135.

312 FSEK m. 67/4 de eserde değişiklik yapılmasının yasaklanması yetkisinin ihlal edilmesi halinde durdurma davasında eser sahibinin neleri talep edebileceği ve verilecek kararın kapsamı tespit edilmiştir. Ayrıntılı bilgi için bkz. Kılıçoğlu, Ahmet, "Fikri Hakların İhlalinde Koruma Yolları (Sınai Haklarla Karşılaştırmalı Olarak)", Türkiye Barolar Birliği Dergisi, Sayı: 54, Yıl: 2004.

313 Aksoy, "Kişisel Verilerin Korunması", s. 61.

hukukunun ekonomik temelini oluşturmaktayken, kişisel veriler, fikir ürünü olarak nitelendirilemeyecektir.[314]

Her iki hakkın korunması amacına yönelik getirilen eleştiriler ise, fikri mülkiyet hakkına yöneltilen diğer eleştirilerdendir. Bu görüşü savunanlara göre, bilgi ekonomisine katkı sağlamak, fikri mülkiyet haklarının ve kişisel verilerin korunmasının amacını oluşturmaktadır. Fakat, fikri mülkiyet görüşüne dayanak olarak görülen bu ortak amaca karşı, her iki kurum arasında doğaları itibariyle önemli farklılıklar söz konusudur. Kişinin bilinçli bir şekilde sarf ettiği emeğin ürünü olarak fikri mülkiyete konu olan değerler meydana geldiği için, fikri mülkiyette asıl korunan şey kişinin emeğidir. Buna karşın, kişisel verilerin meydana gelmesi için kişinin sarf ettiği herhangi bir emek veya çaba söz konusu olmadan, kişisel veriler, kişinin bazı tercihleri kapsamında yaşamını sürdürmesi esnasında, kişinin tabii varlığından doğmaktadır.[315]

Bu konudaki diğer bir eleştiri ise, kişisel verilerin korunması ile fikri mülkiyet hakkının varlık amacına ilişkindir. Gelişimin teşvik edilmesi, fikri ve sınaî haklar alanında kalkınmanın sağlanması amaçlarıyla fikri mülkiyet hakkı geliştirilmiştir. Bu kapsamda, kişinin fikri çabası sonucunda meydana gelen eserlerin, bir tür mülkiyet hakkı çerçevesinde korunması ile kişiye çabasının ticari semerelerinden faydalanma imkânı tanımaktadır. Bununla birlikte, kişisel verilerin korunmasında bu türden bir teşvik amacı güdülmemektedir. Yani, kişisel verilerin oluşturulmasını ya da kapsamlı şekilde dağılımını sağlayabilmek için kişisel veriler üzerinde mülkiyet hakkı kurulması zorunlu değildir. Zira, kişisel veriler herhangi bir çaba sarf edilmeden, kişinin belirli tercihleri çerçevesinde yaşamını sürdürmesi esnasında varlık kazanmaktadırlar. Bundan dolayı, veri sahiplerine bu verilerin yaratılmasını teşvik etmek için bu veriler üzerinde bir tür mülkiyet hakkı tanınmasına ihtiyaç yoktur.[316]

Bu konudaki doktrinde dile getirilen bir diğer eleştiri ise, her iki hakkın korunmadığı durumlarda doğacak sonuçlara dairdir. Zira kişisel verilerin

314 Küzeci, a.g.e., "Doktora Tezi", s. 64.

315 Prins, "Personal Data", s. 296 (Aktaran, Aksoy, Kişisel Verilerin Korunması, s. 66).

316 Prins, "Personal Data", s. 296 (Aktaran: Aksoy, Kişisel Verilerin Korunması, s. 66).

korunmaması ile fikri mülkiyet hakkının korunmaması kıyaslandığında çok daha büyük ve ağır zararlar ortaya çıkabilmektedir.[317] Örnek vermek gerekirse, hassas nitelikteki bir verinin korunmaması halinde, veri sahibi kişi ayrımcılığa maruz kalabileceği gibi bu nedenle işini kaybetme ihtimali doğabilecek, toplum içinde bazı özelliklerinin bilinmesi nedeniyle belki aşağılanabilecek ve bu suretle ağır insan hakkı ihlallerine muhatap olması söz konusu olabilecektir. Bunun yanında, fikri mülkiyet hakkının korunmadığı bir durumda, kişinin uğradığı zarar genellikle maddi zarar olarak ortaya çıkmaktadır.[318]

2.1.3.5. Görüşler Hakkında Değerlendirme

Yukarıda bahsettiğimiz kişisel verilerin hangi hukuki temele dayandırılarak koruncağı hukuk âleminde oluşturacağı neticeler bakımından muazzam önem arz etmektedir. Zira temel teori oluştuktan sonra kişisel verilerin korunması hukukundaki ana müesseseler, diğer hukuk dallarında olduğu gibi, bu teori etrafında şekillenecektir.

Görüşlerin hepsi kendi içerisinde belirli bir hukuki gerekçelendirmeye ve hukuki temele dayanmaktadır. Bu gerekçelerin maddi alanda öne çıkanları olduğu gibi manevi alanda da öne çıkan yanları olduğu görülmektedir.

İlk olarak **bireysel özerklik, insan onuru ve kişisel verilerin geleceğini belirleme** teorisini ele aldığımızda; kişilerin sıradan birer veri nesnesi olarak kabul edilmemesi gerektiğinin vurgulandığını görüyoruz. Zira demokrasilerde ve hukuk devletlerinde, kişilerin kendisi ile ilgili bilgilerin toplanması, tasnif edilmesi ve gerektiğinde ortaya çıkarılması hususlarında tam bir yetki ve denetiminin olması gerektiği ortaya konulmuştur. Diğer taraftan kişiler, salt insan olması nedeniyle insanlık onuruna sahiptirler. Bu hak devredilemez ve vazgeçilemez bir hak olarak karşımıza çıkmaktadır. Öte yandan, kişilerin verinin toplanmasından başlayarak işleme faaliyetinin her bir aşamasında kendileri ile alakalı verileri üzerinde tasarruf hakkı ve özellikle bu verilerin ne yönde kullanılabileceğine yönelik geleceklerini belirleme hakkı bulunduğu bu teoride savunulmuştur. Teori genel anlamda insan

317 Aksoy," Kişisel Verilerin Korunması", s. 66.

318 Çokmutlu, a.g.e., s. 52.

hakları odaklı bireyin manevi varlığını ön plana çıkaran ve bireyi önceleyen hukuki temele dayanmaktadır. Bu yönüyle esasen bir temel hak olan kişisel verileri korunma hakkına makul bir hukuki gerekçelendirme yaptığı görülmekle beraber çağdaş bireyci yaklaşıma daha uygun olduğu görülmektedir.

Özel hayatın gizliliği temelinde kişisel verilerin korunmasına baktığımızda, özel hayatın ne demek olduğu konusunda net bir tanım yapılmasından kaçınıldığını hem uluslararası metinler hem de özellikle AİHM kararlarından anlıyoruz. Fakat bunun bilinçli bırakılan bir boşluk olduğunu görmekteyiz. Çok genel bir biçimde, özel hayatı; kişinin kendisini geliştirebilmesi için müdahale edilmemesi gereken, bireyi devletten, toplumdan sıyıran özerk bir alan olarak tanımlayabiliriz. Kişisel verilerin hukuki temeli, bu görüşte kişinin bu özerk alanında dayandırılmaktadır. Kaynağını bu alandan almaktadır. Tabi özel hayat kişisel verilerden çok daha fazlasını ifade eder. Yukarıda da belirttiğimiz üzere özel hayat; ortak, özel ve giz alanlarından oluşmaktadır. Hassas verilerin giz alanında kaldığı değerlendirilebilir. Giz alanı mutlak olarak korunmakta iken özel alan kural olarak korunmaktadır. Ortak alan ise hususi bir koruma altında olmamasına rağmen bu korumasız bırakılacağı anlamına gelmez. Bu teoride, kişilerin bilgileri kişisel veri kapsamında özel hayatlarında kaldığı mütalaa edilerek bu görüş çerçevesinde korunduğu belirtilmiştir. Teori insan hakları temelli olması nedeniyle insan onuru ve bireysel özerklik teorisine yaklaşmaktadır. Ama sağlanan korumanın gerekçesi ve kişisel verilerin özel hayatı oluşturan unsurların sadece bir parçası olması hasebiyle yetersiz kaldığı ileri sürülebilir.

Mülkiyet hakkı görüşü ise; temelde kişisel verilerin esasen kişinin kendisine ait olan bir mal, ürün statüsünde değerlendirilmesi fikrine dayanmaktadır. Böylelikle kişiler kendisine ait veriler üzerinde tasarruf ederek maddi ya da manevi gelir sağlayarak aynı zamanda mülkiyet hakkının geniş koruma perspektifinden yararlanacaklardır. Bir zarara uğradıkları vakit ise yargı makamlarından bu zararların giderilebilmesini doğrudan isteyebileceklerdir. Teorinin, kişisel verileri bir meta olarak ticari kaygılar üzerinde değerlendirdiği görülmektedir. Zaten bu görüşün materyalist olması hasebiyle eleştirildiğini yukarıda belirtmiştik. Ayrıca kişisel verisini satan bir bireyin bu veri elinden çıktıktan sonra tasarruf edemeyeceği bir gerçektir. Bu nedenle bu görüş bireyi metalaştırdığı, insan onuru ve insan hakları ile

bağdaşmadığı yönünden eleştirilmelidir. Bunlara ilaveten, kanaatimizce, kamu gücü kullanılarak verilerin elde edilmesi durumlarında yani kanun ile bazı yetkilerin tanınması veya mahkeme kararı ile kişisel verilerin sahibinin rızası hilafına elde edilmesi hallerinde teorinin yetersiz kaldığı görülmektedir.

Fikri mülkiyet hakkı görüşüne baktığımızda, verilerin korunarak kontrollü bir şekilde dağıtılmasının, eserlere sağlanan telif hakkındaki hukuki gerekçelendirme ile aynı mantıkta savunulduğunu görüyoruz. Burada, eser sahibinin manevi haklarından olan eserin umuma arz yetkisi ile eserde değişiklik yapılmasının yasaklanma yetkileri ile bir benzerlik kurulmuştur. Fikri mülkiyette esasen eserin fikri korunmaktadır. Ancak kişisel verilerin bir fikir olmadığı gerçeği bulunmaktadır. Fikri mülkiyet daha ziyade bir maddi hakkın korunması iken kişisel verilerin korunması hakkı manevi hakka yöneliktir. Bu yönlerden bu görüşün zayıf olduğu göze çarpmaktadır.

Hukuk devletlerinde, anayasacılık hareketlerinin başlatılmasına paralel olacak şekilde, bireyin salt insan olmasından kaynaklanan haklarının olduğunun kabulü ile bu haklara müdahale edilememesi veya müdahale edilse bile anayasal çerçevede belli başlı üst düzey koruma mekanizmaları öngörülerek müdahale edilebilmesi öngörülmüştür.

Diğer bir anlatımla; günümüz çağdaş demokrasilerinde kişilerin münhasır, dokunulamaz alanlara sahip olduğu ve bu alanlara ilişkin kendi tercihlerini rahatlıkla yapabilecekleri bir ortamın devletler tarafından pozitif yükümlülükler çerçevesinde sağlanması gerektiği yönünde bir hukuk sisteminin tesis edildiğini görüyoruz. Bu hususların doğal sonucu olarak, prensipte, kişilerin kendileri ile alakalı konularda mutlak tasarruf hakkı olduğu, hukuki öngörülebilirliğe sahip olmaları gerektiği, hukuki güvenlik ve geleceklerini kendi serbest iradelerinin seçimleri neticesinde şekillendirebilecekleri artık inkâr edilemez bir gerçektir. Bu minvalde, "insan onuru, bireysel özerklik ve kişisel verilerin geleceğini belirleme" teorisine dayanan görüşün, gerek kişisel verilerin korunması hakkının özüne gerekse bireyi meta olarak görmeksizin salt insan olmasından kaynaklanan birtakım ayrıcalıklara sahip olması fikri temelinde daha isabetli ve uygulanabilir olduğu kanaatindeyiz.

2.1.4. İLGİLİ KİŞİ (VERİ ÖZNESİ, VERİ SAHİBİ, VERİNİN KONUSU)

108 sayılı sözleşme, 2. m.'sinde kimliği belirli veya belirlenebilir *"ilgili kişi"* hakkındaki tüm bilgileri kişisel veri olarak üstü kapalı bir şekilde belirtmiştir. Buradan anlaşılacağı üzere, ilgili kişi verilerin öznesi konumundaki gerçek kişiyi ifade etmektedir.

Diğer yandan, bu terimin 96/45/AT sayılı Yönergede de spesifik bir tanımı yoktur. Ancak ilgili yönergede veri öznesi *-data subject-* olarak kişisel verileri işlenen ve/veya kişisel verilerle ilgili hakları ihlal edilen kişi olarak metin içerisinde geçmektedir. Yine öte yandan, GDPR'de m.4/1'de veri sahibi olarak bir tanım yapılarak veri sahibinin "*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 kişi"* olduğu ifade edilmiştir.

KVKK'da m. 3/ç fıkrasında ilgili kişi kavramı *"kişisel verisi işlenen gerçek kişiyi ifade eder"* şeklinde ilgili kişi tanımlanmıştır.

Yukarıda ifade edildiği üzere kişisel veriler, tanımlanmış ya da tanımlanabilir bir bireyle[319] ilgili herhangi bir bilgi anlamına gelmektedir. Burada birey teriminden, verileri işlenen bir kişinin veri konusunu oluşturduğu anlaşılmalıdır. Veri konusu, kişisel verilerin konusu olarak kabul edilen gerçek bir kişidir.[320] Geniş anlamda, ilgili kişi, veri öznesi veya veri sahibi herhangi bir kişisel veriye konu olan gerçek kişidir.[321] Veri konusu kişi, veri koruma mevzuatı tarafından korunan kişidir. Kişisel veriler, tanımlanabilir gerçek bir kişi ile ilgili herhangi bir bilgi olarak tanımlanmıştır. Dolayısıyla, veri konusu kişi, dolaylı olarak veri koruma kanunu ile korunan ilgili kişiler olarak tanımlanır.[322]

---

319 108 s., söz., m. 2/a.

320 Rogers, Kevin M., "The Internet and The Law" (1stedn, Palgra ve Macmillan 2011), s . 149.

321 Carey, a.g.e., s. 3.

322 Kuner, Christopher, "European Data Privacy Law and Online Business", Oxford University Press, 2003, s. 54.

Netice itibarıyla, kişisel verilerin korunması ile ilgili uluslararası ve ulusal metinlere baktığımızda verileri işlenen gerçek kişilere terimsel olarak yaklaşımda bir bütünlük olduğunu söyleyemeyiz. Ancak bununla beraber işin esası gereği, her hukuk düzeninde bu terimin ya doğrudan tanım olarak ya da dolaylı olarak düzenleyici metinlerde yer aldığı görülmektedir. Genel olarak bir tanım yapılması gerekirse, geniş anlamda, ilgili kişi ya da diğer ifade ile veri öznesi; *"kişisel verisi işlenen gerçek kişiyi"* ifade etmektedir. Eğer hukuk düzeni, tüzel kişilerin de kişisel verilerini koruma hakkını kabul ederse *-ki çalışmamızın ilk bölümlerinde bazı Avrupa ülkelerin de bu yönde düzenlemelerin mevcut olduğunu belirtmiştik-* tüzel kişiler de ilgili kişi olarak anılabilecektir. Bununla beraber gerek iç hukukumuzda gerekse iç hukukumuza doğrudan kaynak olan AK ve AB hukuk sistemlerinde sadece gerçek kişilerin kişisel verileri korunmaktadır. Dolayısıyla ancak gerçek kişiler ilgili kişi, veri öznesi, veri konusu olabilir. Bu kapsamda vakıflar, dernekler, sendikalar ve şirketler gibi tüzel kişilikler ilgili kişi sayılmıyorken; işçiler, tüketiciler, gerçek kişi olan tacirler gibi gruplar kişisel veri hukuku bağlamında veri sahibi olarak nitelendirilmektedir. Ancak şunu da belirtmeliyiz ki, eğer tüzel kişiye ait bir veri, belli ya da belirlenmesi mümkün bir gerçek kişiyi tanımlıyor veya tanımlanabilir kılıyorsa tüzel kişiye ait bu veriler de koruma kapsamında kalacaktır. Mamafih, burada ilgili kişi sıfatı yine gerçek kişiye ait olacaktır.[323]

Gerçek kişilerin kişisel verilerinin korunmasını isteme hakkı olduğu tartışmasız kabul edilmesine, bu verilerin ne olduğuna yönelik çokça düzenleme yapılmasına ve doktrin üretilmesine karşılık, ters orantılı olarak, tüzel kişilere ait kişisel verilerin olup olamayacağı *-zira tüzel kişilerin manevi varlıklarının bulunmadığı yönünde savların ortaya atıldığı-* ve bunların ne şekilde korunacağına ilişkin kafa karışıklığının hem doktrin hem de pozitif hukuk bağlamında olduğu görülmektedir.

Uluslararası ve ulusal hukuk otoriteleri tarafından tüzel kişilere ait verilerin, gerçek kişilere ait veriler ile aynı kategoride ele alınmadığı bu konu ile alakalı olan metinlerin tetkikinden anlaşılmaktadır. Küreselleşen ve gitgide iletişimin, ulaşımın, ticaretin bunlarla beraber devletler ve bireyler arasında her alanda yapılan işbirliğinin

[323] https://verikorumahukuku.org/veri-sahibi-nedir/, Erişim tarihi: 08/09/2019

kolaylaşarak arttığı dünyamızda, yapay zekanın ön plana çıktığı sistemsel özelliklere haiz yapıların markalaştığı ve uluslararası bir boyut kazandığı dikkate alındığında *-ki bunların çoğu tüzel kişilik altında örgütlenen kamusal veya özel firmalardır-* bazı dev tüzel kişiliklerin oluştuğu gözden kaçırılmaması gereken bir gerçekir. Bu tüzel kişilikler öyle bir konuma gelmiştir ki sadece ticari sır kapsamında veri ve bilgilerinin korunması mümkün görülmemektedir. Zira bu tüzel kişilikler toplum nezdinde takip edilen, açıklamalarına itibar edilen kurumsal yapılar haline gelmişlerdir. Bunlara Apple, Huawei ve bazı büyük savunma şirketleri örnek olarak verilebilir.

Başka bir anlatımla, devletlerin ve uluslararası kuruluşların belli başlı temel kanunlarını tekrar tekrar ele alarak düzenleme yaptıkları görülmektedir. Bu düzenlemelerin temelinde gelişen teknoloji ile uyumlu olacak birtakım mekanizmaların ceza kanunu, medeni kanun ve ticaret kanunu gibi düzenlemelere eklemlendiği müşahade edilmektedir. Bunlara ek olarak, tüzel kişilerin kurumsal itibarının olduğu ve bu itibarın korunmasının tüzel kişilerin faaliyetlerinin devamı açısından hayati olduğu herkesçe malumdur. İşte bu noktada tüzel kişilerin menfaatlerine karşı işlenen haksız fiillere ve suçlara ceza kanunlarında yer verildiği bilinmektedir.

Dolayısıyla bilgi ve teknoloji çağında; tüzel kişilere ve özellikle uluslararası firmaların kendilerine ait birtakım verilerin, hukuken koruma altına alınması gerekliliğinden bahsedilmesi kaçınılmazdır. Bu hususa ilişkin uluslararası alanda ve ulusal bazda düzenlemelere yer verilmesi ve tüzel kişilere ait verilere ilişkin düzenleme yapılması elzem görünmektedir. Bu düzenlemeler ve tartışmalar yapılırken tüzel kişilere ait kişisel verilerin korunmasına yönelik atılacak adımların ele alınmasının hukuki bir zaruret halini alacağı kanaatindeyiz.

2.1.5. RIZA

Gerek iç hukukumuzda gerekse uluslararası metinlerde ilgilinin rızasının,[324] kişisel verilerin işlenmesinde çok önemli bir rol oynadığı görülmektedir.[325] Bu nedenle, "rıza" kavramına, çalışmamızın kişisel verilerin korunmasına hâkim olan ilkeler kısmında değinilecek olsa bile, bu hukuk alanındaki terminolojideki önemine binaen terimler kısmında ayrıca yer verme gereği hasıl olmuştur.

Rıza, esasen sözlük anlamı ile "razı olma, isteme" anlamına gelmektedir.[326] Başka bir deyişle, bir şeyin gerçekleşmesi için izin verilmesi veya bir şeyin yapılması için uzlaşılması anlamına gelmektedir.[327] Yani, rıza, ilgili kişinin –kişisel veri koruma hukuku bakımından veri sahibinin- özel ve iyi bilgilendirilmiş durumuna işaret etmektedir.

Kişinin, verilerinin yetkili kamu ve özel hukuk organları tarafından işlenebilmesi için rıza, neredeyse tüm hukuk sistemlerinde aranmıştır. Buradaki amaç ise, bireyi korumanın yanında kişisel verilerinin geleceğini belirleme hakkının uygulamasını sağlamaktır.[328]

Uluslararası düzenlemelere baktığımızda, 108 sayılı sözleşmede, rızanın ne anlama geldiğine ilişkin bir tanım bulunmamaktadır. Bu husus, AK tarafından taraf devletlerin iç hukukunca düzenlenmesi gereken yasal bir boşluk olarak bırakılmıştır. Bu, ilgili kişinin, bir verinin ne anlama geldiğini belirten bir beyanı veya bir eylemi olabilir. Genel kural olarak, ilgili kişi tarafından herhangi bir zamanda geri alınabilir. Öte yandan, AK hukuku uyarınca, geçerli rıza unsurları, 108 sayılı sözleşmenin uygulamasına yön veren ve gösteren tavsiyelere de konu olmuştur.[329]

---

324 Çalışmamıza konu edilen rıza, kişisel verileri koruma hukuku kapsamında aranan rızadır. Diğer taraftan hukuk ve ceza alanında aranan rızaya baktığımızda, geçerlilik şartları farklılık arz edebilir.

325 Anı, Nevzat Ali, "Kişisel Verilerin İşlenmesi ve Açık Rıza", Yüksek Lisans Tezi, İstanbul Üniveristesi, SBE, 2018, s. 126.

326 https://sozluk.gov.tr/, Erişim tarihi, 20.09.2018.

327 https://en.oxforddictionaries.com/definition/consent, Erişim tarihi, 20.09.2018.

328 Anı, a.g.e., s. 127.

329 Handbook on European Data Protection Law, a.g.e., s. 55, Convention 108, Statistical Data Recommendation, point 6.

108 sayılı sözleşmede rıza kavramına yer verilmediğini belirtmiştik. Bununla beraber, 95/46/AT sayılı Yönerge[330] gerekse GDPR[331] ve KVKK'ya[332] baktığımızda "ilgilinin rızası" olmaksızın veri işleme faaliyetlerinden herhangi biri yapılamayacaktır.

AB hukuku kapsamında, meşru veri işlemenin temeli olarak rıza, Yönergenin 7/a m.'sinde tesis edilmiş olup, aynı zamanda GDPR'nin 8. m'sinde açıkça belirtilmiştir. GDPR'ye göre*, "Rıza, veri konusunun, kendisi ile ilgili kişisel verilerin işlenmesine ilişkin olarak, elektronik araçlar da dahil olmak üzere yazılı bir beyanat ya da sözlü ifade gibi, serbestçe verilmiş, spesifik, bilgili ve açık bir şekilde belirlenmesini sağlayan açık ve olumlu bir kararla verilmelidir. Bu, bir internet sitesini ziyaret sırasında bir kutuyu işaretlemeyi, bilgi toplumu hizmetleri için teknik ayarları seçmeyi veya bu bağlamda, veri konusundaki kişinin kendi kişisel verilerinin önerilen şekilde işlenmesini kabul ettiğini açıkça belirten başka bir açıklama veya davranışı içerebilir. Sessizlik, önceden işaretlenmiş kutular veya hareketsizlik bu nedenle onayı oluşturmamalıdır. Onay aynı amaç veya amaçlarla gerçekleştirilen tüm işlem faaliyetlerini kapsamalıdır. İşlemin birden fazla amacı olduğunda, hepsine onay verilmelidir. Eğer veri konusu kişinin onayı bir elektronik yola yapılan talebin ardından verilecekse, talep açık, özlü olmalı ve sağlanan hizmetin kullanılmasına gereksiz yere zarar vermemelidir."*[333] şeklinde tanımlanmıştır.

1982 Anayasasının 20. maddesine baktığımızda *"kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin **açık rızasıyla** işlenebilir."* hükmü bulunmaktadır. Buradan da anlaşılacağı üzere Türk hukuk sisteminde kişisel verilerin işlenmesinde "*açık rıza*" usulünün benimsendiğini söyleyebiliriz. Yine TCK'nın 26. m.'si ile kişinin üzerinde mutlak tasarruf yetkisi olan haklarda rızasının varlığı

330 Yönerge m. 7/1-a.

331 GDPR m. 6/1-a.

332 KVKK m. 5/1.

333 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en, Erişim tarihi, 20.09.2018.

durumunda işlenen eylem nedeniyle cezaya hükmolunamayacağı açıkça belirtilmiştir.[334]

KVKK'nın 3. m.'sinde "*açık rıza*" düzenlenmiştir. İlgili maddeye göre açık rıza, *"belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı"* ifade etmektedir. Yani bireyler, kendilerine ilişkin verilerin işlenmesine, tamamen kendi istekleri doğrultusunda ya da karşı tarafın talebine onay vermek suretiyle rıza göstermelidir. Rızanın açık olmasının diğer önemli bir yönü de veri işleyen kişiye gerçekleştireceği fiil hakkında yol gösterici olmasıdır.[335] Açık rızanın bu bakımdan, rıza sahibinin "*olumlu irade beyanı*"nı içermesi bir zorunluluktur. Hukuk düzenindeki diğer düzenlemeler saklı kalmak kaydıyla, rızanın alınmasında bu işlemin yazılı şekilde yapılması zorunlu değildir. Açık rızanın internet gibi gerek elektronik ortam yoluyla gerekse telefon görüşmesi gibi çağrı merkezi aracılığıyla da alınması mümkündür. İspata ilişkin yükümlülük veri sorumlusuna aittir.

Kişisel verileri koruma hukuku bakımından aranacak olan rızaya ilişkin;[336]

- belirli bir konuya ilişkin olmalı,
- ilgili kişi aydınlatılmalı yani rıza konusuna ilişkin kendisine bilgi verilmeli,
- ilgili kişi rızasını özgür iradesine dayanarak vermeli, rızanın bu şartları taşıması gerekmektedir.

Bunlarla beraber, rızanın alınmasına ilişkin herhangi bir şekil şartı gerek 95/46/AT sayılı Yönerge gerek GDPR gerekse KVKK'da belirtilmemiştir.[337]

Diğer taraftan, Türk hukukunda, ilgili kişi öncelikle aydınlatılmalı yani konuya ilişkin bilgilendirilmeli ardından ise rızası alınmalıdır. İki eylemin aynı anda yapılması hususu cari mevzuat bakımından tartışmalı görülmektedir. Şöyle ki; Aydınlatma

---

334 Anı, a.g.e., s. 127.

335 https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar, Erişim tarihi, 20.09.2018.

336 Ayrıntılı bilgi için Bkz. Anı, a.g.e., s. 136-145.

337 Anı, a.g.e., s. 145.

Tebliği[338] m. 5/1(f) hükmünde *"kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir."* denilmektedir. Kanaatimizce; bu hüküm gereği ilgili kişinin, kişisel verilerinin işlenmesi için gereken rıza, ilgili kişinin aydınlatılmasının akabinde ikinci bir eylem ile yazılı, sesli, görüntülü, mail yoluyla veya herhangi bir şekilde ispat yükü veri sorumlusuna ait olacak şekilde, kişisel verilerinin işlenmesine özgür irade beyanı ile icazet verdiği bir hukuki işlem şeklinde tanımlanabilir.

Tüm hukuk sistemlerinde rıza şartı kabul görmüş ise de ilgilinin rızasının aranmadığı istisna haller, aynı şekilde, her hukuk sisteminde mevcuttur. İç hukukumuz bakımından, rızanın aranmayacağı haller KVKK m. 5 gereğince şu şekilde sayılmıştır:

- Kanunlarda açık bir şekilde öngörülmesi,
- Fiili imkânsızlık sebebiyle rızasını açıklayamayacak halde bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

338 "*Bu Tebliğin amacı, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununun 10 uncu maddesi uyarınca veri sorumluları veya yetkilendirdiği kişilerce yerine getirilmesi gereken aydınlatma yükümlülüğü kapsamında uyulacak usul ve esasları belirlemektir*.", 10.03.2018 tarihli ve 30356 sayılı Resmî Gazete.

KVKK m. 5 ile ilgilinin rızasının aranmadığı haller sarih ve tahdidi bir şekilde belirtilmiştir. Kanaatimizce bu sarih ve tahdidi sayım, anayasal bir hak olan kişisel verilere yapılacak olan müdahalelerde meşruiyetin ve yasallığın sağlaması olarak görülebilse de AİHM içtihatları dikkate alındığında tahdidi sayım bile olsa konu başlıklarının çok geniş bırakılması AİHS kapsamında hak ihlallerini gündeme getirebilecektir.

Sonuç itibarıyla kişisel verileri koruma hukukunda "rıza" nın kişisel verilerin işlenmesine ilişkin çok önemli bir rolü olduğu görülmektedir. Öyle ki veri sahibinin rızası olmadan veri işleme faaliyetinin yapılamayacağı gerek uluslararası gerekse ulusal mevzuatlarda hüküm altına alınarak genel prensip olarak kabul görümüştür. Ancak her kuralın istisnası olduğu gibi kamu yararı, kamu güvenliği, yasallık gibi ilkeler benimsenerek rızanın bulunmadığı durumlarda dahi veri sahibinin kişisel verilerinin işlenebileceği görülmektedir. Burada idari ve adli makamlar tarafından dikkat edilmesi gereken nokta, rızanın aranmayacağı hallerin, yani genel kuralın istisnasını, bu hakkın işlevine halel getirmeyecek şekilde dar yorumlamaları gerekliliği olarak göze çarpmaktadır.

2.1.6. VERİ İŞLEYEN

108 sayılı sözleşmede bu terime ilişkin herhangi bir şekilde tanım bulunmamaktadır. Bununla beraber AB hukuku kapsamında yapılan tanımlamalar, sözleşme sonrası yürürlüğe giren tavsiye kararlarında da gösterildiği üzere, tamamen AK hukuku için de geçerli görünmektedir.[339]

AB hukukuna değinecek olursak; 96/45/AT sayılı Yönerge madde 2'de işleyici, *"denetleyici (sorumlu) adına kişisel verileri işleyen gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya diğer bir kuruluşu"* şeklinde tanımlanmıştır.

GDPR madde 4/8'de ise işleyici, *"kontrolör (sorumlu) adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır."* şeklinde ifade edilerek yönergedeki tanım tekrar edilmiştir.

339 Handbook on European Data Protection Law, a.g.e., s. 52-54.

AB hukuku kapsamında işleyen, bir sorumlu namına kişisel verileri işleyen bir kişi olarak tanımlanmıştır. Bir işleyene emanet edilen faaliyetler, çok özel bir görev veya bağlamla sınırlı olabilir veya oldukça genel ve kapsamlı olabilir. İşleyenler, başkaları için veri işlemenin yanı sıra, örneğin kendi çalışanlarının, satışlarının ve hesaplarının yönetimi gibi, kendi amaçları için gerçekleştirdikleri işlemlere ilişkin olarak kendi başlarına veri sorumlusu da olabileceklerdir.[340]

İç hukukumuzda ise, KVKK'da madde 3/ğ'de veri işleyen "*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* şeklinde tanımlanmıştır. Yukarıdaki tanımlar göz önünde bulundurulduğunda veri işleyenin faaliyetlerinin esasen veri elde etmenin teknik kısımları ile ilgili olduğu ve bu kişinin herhangi bir inisiyatifinin bulunmadığı anlaşılmaktadır. Veri işleyen kanunda sayılan işlemleri yapan bir kimse olarak tanımlanabilir ki onun bu yönü veri sorumlusundan ayrılmasına yardımcı olur.[341]

2.1.7. VERİ SORUMLUSU

Veri sorumlusu (controller), kişisel verilerin işlenmesini kontrol eden bir kişi veya kuruluş olarak tanımmlanabilir. Örneğin; bankalar, sigorta şirketleri, borsacılar, hukuk firmaları, süpermarketler, devlet daireleri vb. tüm organizasyonlar veri sorumlularıdır.[342]

AK hukuku kapsamında "veri sorumlusu", ulusal yasalar uyarınca otomatik veri dosyasının amacının ne olabileceğine, kişisel verilerin hangi kategorilerinin saklanacağına ve bunlara ne tür işlemler uygulanacağına karar veren gerçek veya tüzel kişi, kamu otoritesi, ajans veya diğer herhangi bir organı ifade eder.[343] Genel olarak bu işlem, özel sektörü dikkate aldığımızda gerçek veya tüzel kişi tarafından yapılmaktadır. Diğer taraftan, kamu sektöründe çoğunlukla bu süreci hayata geçirecek bir otorite (yetkili makam) bulunmaktadır. Aynı zamanda, sorumlunun tanımı, kimlerin kişisel verileri belirli bir amaç için yasal olarak işleyebileceklerine dair bir

340 95/46/AT sayılı Yönerge m.2-e.

341 https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen,Erişim tarihi,08.09.2019.

342 Carey, a.g.e., s. 3.

343 108 s. söz. m. 2/d.

yanıttır. Veri sorumlusu, gerçek kişi, tüzel kişi ve kurum ya da kuruluş olabilir. Ayrıca, denetleyicinin yani sorumlunun ayırt edici bir özelliği de depolanmasının yanı sıra hangi bilgilerin hangi kategoriye ait olduğunu belirleme yetkisinin ve görevinin bulunmasıdır.[344]

96/45/AT sayılı Yönerge madde 2/d'de denetleyici (sorumlu) *"kişisel verilerin işlenme araçlarını ve amaçlarını tek başına ya da diğerleriyle ortaklaşa belirleyen gerçek veya tüzel kişi, kamu makamı, devlet dairesi veya başka bir kuruluşu"* şeklinde tanımlanmıştır. Aynı maddenin devamında *"işleme amaçları ve araçları ulusal veya topluluk hukuku veya yönetmelikleriyle belirlendiğinde, denetleyici veya atanması için özel kriterlerin"* ulusal ya da topluluk hukukuyla belirlenebileceği düzenlenmiştir.

GDPR m. 4/7'de*"kontrolör' -sorumlu- yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır; söz konusu işleme amaçları ve yöntemlerinin birlik ya da üye devlet hukukuna göre belirlenmesi durumunda, kontrolör veya kontrolörün belirlenmesine özgü kriterler birlik ya da üye devlet hukukuna göre belirlenebilir"* şeklinde ifade edilmiştir. Dolayısıyla, veri sorumlusu, kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirleyen herhangi bir gerçek veya tüzel kişidir.

İç hukukumuzda ise, KVKK m. 3/ı'da veri sorumlusu *"kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* şeklinde ifade edilmiştir. Belirtmek gerekir ki tüzel kişilerin kişisel verileri işleme kapsamında yaptıkları faaliyetlerde bizzat kendileri "veri sorumlusu" olarak nitelendirilecek ve hukuki sorumluluk ilgili tüzel kişinin şahsında ortaya çıkacaktır. Gerek kamu hukuku tüzel kişilikleri gerekse özel hukuk tüzel kişilikleri açısından bu konuda herhangi bir farklılık öngörülmemiştir. Örneğin; bir şirket kapsamında bulunan birimlerin ayrı bir tüzel kişiliği olmadığı için, söz konusu birimlerin veri sorumlusu olarak nitelendirilmesi mümkün görünmemektedir. Fakat bir şirketler topluluğu söz

344 108 s. söz. m. 2/d.

konusuysa, her şirket ayrı tüzel kişiliği haiz olduğundan, söz konusu şirketlerin hepsinin ayrı veri sorumlusu olarak nitelendirilmesi mümkündür.[345]

Bunlara ilaveten, ulusal hukukumuzda, Veri Sorumluları Sicili Yönetmeliğinin yürürlük kazanması ile birlikte veri sorumlularının, kişisel verileri işlemeye başlamadan önce bir sicile kayıt olması gerekmektedir.[346] Kişisel Verileri Koruma Kurumu tarafından oluşturulan bir otomatik sistem olan "VERBİS (*Veri Sorumluları Sicil Bilgi Sistemi*)" vasıtasıyla bu kayıt işlemi gerçekleştirilecektir. Öte yandan, "*veri sorumlusu temsilcisi"* kavramı hukukumuza girmiştir. Adı geçen yönetmeliğin 4/1-p m.'sine göre veri sorumlusu temsilcisi, *"Türkiye'de yerleşik olmayan veri sorumlularını ... asgari temsile yetkili Türkiye'de yerleşik tüzel kişi ya da Türkiye Cumhuriyeti vatandaşı gerçek kişi"* olarak düzenlenmiştir.

Veri sorumlusu ve veri işleyen sıfatlarını karşılaştırdığımızda, veri sorumlusunun, kişisel verilerin işlenmesine ilişkin her aşamada karar veren makamda olduğunu belirtmeliyiz. Buna karşılık, veri işleyen ise, veri sorumlusunun kararları doğrultusunda işleme faaliyetini teknik olarak gerçekleştiren kimse olarak görülmelidir. Bir örnekle açıklamak gerekirse, veri işleyeni yapay zekaya sahip bir makineye, veri sorumlusunu ise bu makineyi tasarlayan mühendise benzetebiliriz. Bu makine, mühendisin yazmış olduğu yazılım ve kodlar çerçevesinde hareket edecek ve onun rızası hilafına bir faaliyette bulunamayacaktır.

2.1.8. KİŞİSEL VERİLERİN İŞLENMESİ

Kişisel verilerin elde edilmesi, toplanması, kaydedilmesi, saklanması, organize edilmesi, uyarlanması, düzenlenmesi, değiştirilmesi, birleştirilmesi, sorulması, okunması, açıklanması, kullanılması, erişilebilir hale getirilmesi, transfer edilerek başkalarına verilmesi, yayılması ya da hazır bulundurulması için yapılacak işlemler gibi, bu verilerin kombinasyonu, silinmesi ya da yok edilmesi, ilişkilendirilmesi veya bloke edilmesi için gerçekleştirilecek bütün işlem ya da

345 https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen, Erişim tarihi, 08.09.2019.

346 T. 30/12/2017, RG. 30286, Veri Sorumluları Yönetmeliği İstisna uygulanacak haller ve istisnai kriterler için Yönetmeliğin 15. ve 16. maddelerine bkz.

işlemlerin hepsi "kişisel verilerin işlenmesi" kapsamında kabul edilebilir.[347] Diğer bir ifade ile, kişisel verilerin elde edilmesi, saklanması, kopyalanması veya aktarılmasıyla ilgili herhangi bir aşamada gerçekleştirilebilecek herhangi bir iş/eylem olarak kabaca işlenme hususu tanımlanabilir.[348]

Söz konusu işlem, dijital bir ortamda gerçekleştirilebilen işlemleri kapsadığı gibi elektronik olmayan (kâğıt vb. gibi) bir araç ile de geçekleştirilebilen ve kişisel verilerle alakalı olabilecek tüm süreci içerebilir.[349] Bu kapsamda, kişisel veriler ile ilgili olarak "otomatik işleme" ile kast edilen, bu verilerin otomasyon sistemleri kullanmak sureti ile, örneğin bilgisayar aracılığı ile işlenmeleridir. Böylece kişisel verilerin toplanmasından başlanarak bu işlemlerin geçtiği bütün evreleri içine alan tüm işlem türleri koruma altına alınmış olmaktadır.[350] "*Otomatik Veri Dosyası*", otomatik işlemden geçirilen herhangi bir veri kümesi anlamına gelir. Otomatik işleme sadece otomatik uygulamaları değil aynı zamanda kişisel verilerin manuel kullanımının belirli aşamalarını da içerir. Bu nedenle, otomatik işlemler terimini, tam olarak hem otomatik hem de manuel şekilde kişisel veriler üzerindeki performans durumları olarak tanımlayabiliriz.[351]

95/46/AT sayılı Yönergenin 2. m.'sinde işleme eylemi "*toplama, kaydetme, organizasyon, depolama, uyarlama veya değiştirme, kurtarma, danışma, kullanma, yayma yoluyla açıklama, sıralama veya birleştirme, engelleme, silme veya tahrip etme gibi otomatik veya otomatik olmayan yöntemlerle kişisel verileri üzerinde yapılan faaliyet ya da faaliyetler"* olarak ifade edilmiştir.

GDPR'nin 4. maddesinde "*toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, erişme, başvurma, kullanma, yaymak, yayınlamak veya diğer şekillerde ulaşılır hale getirmek suretiyle açıklama, sıralama*

347 Başalp, a.g.e., s. 16.

348 Carey, a.g.e, s. 2.

349 Ersoy, " İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması", s.20.

350 Başalp, a.g.e., s. 16.

351 Handbook on European Data Protection Law, a.g.e., s. 47.

veya birleştirme, kısıtlama, silme veya imha etme gibi eylemler" olarak ifade edildiği müşahede edilmektedir.

KVKK m. 3'te işleme kavramı, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla şu faaliyetleri ifade etmektedir;

- otomatik olmayan yollarla elde edilmesi,
- kaydedilmesi,
- depolanması,
- muhafaza edilmesi,
- değiştirilmesi,
- yeniden düzenlenmesi,
- açıklanması,
- aktarılması,
- devralınması,
- elde edilebilir hâle getirilmesi,
- sınıflandırılması ya da
- kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.

Bu tanımdan da anlaşılacağı üzere, esasen işleme kavramı, kişisel verilerin elde edilmesi sürecinden başlayarak veri üzerinde yürütülen her türlü eylemi ifade etmektedir.[352]

Özet olarak verilerin işlenmesi; anayasa, uluslararası andlaşmalar ve yasaların belirlediği çerçevede, veri sorumlusunun tayin ettiği sınırlar içerisinde, veri işleyen tarafından kişisel veriye ulaşılıp topanmasından başlayarak depolanması ve kullanılmasına kadar tahdidi sayılmayan fiillerin iritkap edilmesi olarak tanımlanabilir.

352 TBMM Komisyon Raporu, s. 7.

2.1.8.1. Kesin İşlem Yasağı

Kesin işlem yasağı deyiminden anlaşılması gereken, genel bir kural ve prensip olarak, hiçbir koşul altında hassas kişisel verinin işlenememesi durumudur. Gerek uluslararası düzenlemeler gerekse iç hukukumuz bakımından hassas-özel nitelikli veriler açısından kesin işlem yasağı belli başlı alanlardaki istisnaları içermek kaydıyla kabul edilmiştir.

Hassas verilerin işlenmesi 95/46/AT sayılı Yönergenin 8. maddesi gereğince kural olarak yasaktır. Bu kural birçok ulusal veri koruma kanunu ve GDPR'de de göz önüne alınarak ilgili düzenlemeler yapılmış, kural olarak hassas veriler için kesin işlem yasağı getirilmiş, hassas verilerin işlenmesine ancak istisna bazı hallerde izin verilmiştir.

Yukarıda bahsedilen yönerge uyarınca, hassas verilerin işlenmesine izin verilen istisnai hallerde dahi, hassas kişisel veriler yönerge ile sağlanan "*genel koruma*" dan yoksun bırakılmamıştır. Ancak, 8. m. ile sağlanan hassas kişisel verilerin işlenmesine ilişkin kesin işlem yasağının sağladığı "*özel koruma*" dan, ilgili kişinin açık rızası alınmak suretiyle kişisel verilerinin işlenebileceğini söylemek mümkündür.[353]

KVKK, genel kural olarak ilgilinin açık rızası bulunmaksızın özel nitelikli kişisel verilerin işlenmesini yasaklamıştır. Bununla beraber; sağlıkla[354] (cinsel hayat dahil)[355] ilgili zorunluluklar hariç olmak üzere; ilgili kanunlarla -*hassas kişisel*

---

353 Özdemir, a.g.m., s. 127.

354 "*Sağlık verilerinin işlenmesine ilişkin bir diğer çelişki ise, İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği 98. maddesi gereğince işverene getirilen işyerinde gerçekleştirilen iş sağlığı ve güvenliği faaliyetleri konusunda tutulan bütün kayıtlar ve işten ayrılma tarihinden itibaren en az 15 yıl boyunca çalışanların kişisel sağlık dosyalarını saklama yükümlülüğüne ilişkindir. İlgili yönetmelik uyarınca, işverenin çalışanlarının sağlık verilerini 15 yıl süreyle saklama yükümlülüğü getirilmiştir. Ancak işveren bu yükümlülüğü yerine getirmesi halinde 6698 sayılı Kanun m. 6/3 hükmüne aykırı davranmış olacaktır. Zira sağlık verilerinin işlenmesi için kanunlarda açıkça öngörülme şartı getirilmemiştir. Bu nedenle 6698 sayılı Kanun uyarınca işveren, çalışanının sağlık verilerini saklayamayacaktır."*, Anı, a.g.e., s. 122.

355 " *...sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir*." KVKK m. 6/3.

verilerin işlenmesine yönelik meşru dayanak tesis eden kanunların cari olması durumunda- düzenlenen durumlarda hassas verilerin, ilgili kişinin açık rızası alınmadan dahi işlenebileceği istisnai olarak kabul edilmiştir. Ancak bu düzenlemeler, temel haklara ve özgürlüklere hukuka aykırı bir şekilde müdahale edilmesine imkân sağlayabilir. Özellikle çeşitli alanlarda çıkarılan kanunlarda amacın meşru, ölçülü ve belirli olup olmadığı yönündeki tartışmalar yoğunlaşacak ve bu durum yargının iş yükünü artıracaktır. Bir diğer yandan, KVKK sistematiğinde, hassas kişisel veriler hakkında yapılacak işlemlere ilişkin hem çok geniş hem de sınırları belli olmayan istisna getirilmesinden dolayı, kesin işlem yasağına dair getirilen istisnalar "hassas veriler" başlığı altında değil de hassas olsun veya olmasın tüm kişisel veriler hakkında uygulanabilecek bir şekilde "çeşitli hükümler" başlığı altında düzenlenmiştir. Bu iki nedenle hassas veriler başlığı altında ve bu verilere özgü istisnaların getirilmesinin daha yerinde bir düzenleme olabileceği öne sürülmüştür.[356]

2.1.8.2. İşlem Yasağının İstisnaları

2.1.8.2.1. İlgilinin Rızası

Hassas kişisel verilerin işlenmesi yasağının ilk istisnası veri sahibinin rıza göstermiş olmasıdır. Yani veri sahibi açıkça rıza göstermiş ise hassas kişisel veriler işlenebilecektir. 95/46/AT sayılı Yönergede, rızanın açık olması gerektiği vurgulanarak örtülü rıza kabul edilmemiştir. Bu nedenle hassas kişisel verilerin işlenmesi için veri sahibinin açık rızası gereklidir.[357] Ancak, ilgili yönergenin 8/2(a) m.'sinde veri sahibinin açık rızasının olması halinde bile, üye ülkelerin ulusal kanunlarında hassas verilerin işlenmesini yasaklayabileceği kabul edilmiş aynı durum GDPR'de m. 9/2(a)'da tekrar ifade edilmiştir.[358]

Hassas kişisel verilerin işlenebilmesi için veri sahibi tarafından verilecek rızanın kesin ve açık olması, rıza vermeye yönelik iradenin gönüllü ve özgür olması gerektiği gibi, bu rızanın iradi ve bilinçli bir şekilde açıklanarak ortaya çıkması gerekir.[359] Bunun yanında, rızasını beyan edecek veri sahibinin veri işlemesi

356 Ayözger, a.g.e., s. 30.

357 Küzeci, a.g.e., "Kişisel Veriler", s. 240.

358 Ayözger, a.g.e., s. 30.

359 Kaya, "Hassas Veriler", s. 326.

konusunda yeterli ölçüde bilgilendirilmiş olması da gereklidir. Aksi durumda açık rızanın bulunduğu söylenemeyecektir.[360] Ayrıca, veri sahibinin, açık rızasının spesifik yani belirli bir duruma ilişkin olması gerekir. Başka bir deyişle; açık rıza, hassas kişisel verilerin işlenmesi için genel olarak bir rıza verilmesi demek olmayıp, her bir durum için o duruma özgü belirlenmiş hassas kişisel verilerin işlenmesi için verilecek rızayı ifade etmektedir.[361]

Verilecek açık rızanın yazılı olması mutlaka gerekmemekle[362] birlikte, yazılı rızanın alınması ispat külfetinin yerine getirilmesi yönünden faydalı olur. Bu nedenle veri işleyenler için yazılı rıza alınması bir güvence ve rahatlık sağlayacaktır.[363]

1982 Anayasası ve KVKK'da ilgilinin rızasının aranacağı açıkça hükme bağlanmıştır.[364]

2.1.8.2.2. Hayati Çıkarların Korunması

Veri sahibinin veya başka birinin hayati ehemmiyeti olan menfaatlerini korumak için zorunlu olması halinde, veri sahibinin fiziki veya hukuki nedenlerle rızasını açıklayamaması halinde bile hassas verilerin işlenebileceği 95/46/AT sayılı Yönerge 8/2(c) maddesinde ve GDPR'nin 9/2(c) maddesinde düzenlenmiştir.[365] Bu istisna düzenleme ile, esas itibariyle insan hayatını tehdit eden durumların varlığının söz konusu olması halinde, hassas verilerin işlenebilmesi amaçlanmıştır.[366]

Ağır bir hastalık nedeni ile veya bir kaza geçirmesi sonucunda veri sahibinin bilincinin kapalı olması gibi haller fiili nedenlerle veri sahibinin rızasının

---

360 Carey, a.g.e., s. 84 vd.

361 Kaya, "Hassas Veriler", s. 326.

362 Carey, s. 85; "*Veri sahibinin açık rızası, hassas kişisel verilerin işleme amacının detaylı bir şekilde ortaya konulup, veri sahibinin veri işlemesine muvafakatini gösterme imkânının tanınması suretiyle elde edilebilir.Örnek olarak, veri sahibi açık rıza verilmesi yönündeki iradesini bir internet sitesindeki kutucuğu "opt-in (istek içi)" rıza şeklinde yani "katılmayı tercih ediyorum" şeklinde işaretlemekle gösterebilir."*, Room, a.g.e, s.127; "*Bu yolla elde edilen rızanın geçerli olabilmesi için, veri sahibinin imzalayacağı ya da işaretleyeceği forma söz konusu işleme faaliyetini ya da faaliyetlerini nitelendiren bir ibarenin konulmuş olması gerekir*.", Kaya, "Hassas Veriler", s. 326.

363 Carey, a.g.e, s. 85.

364 Bu hususta "rıza" başlığı altındaki değerlendirmelere bkz. çalışmamızın 91-95. sayfaları.

365 Küzeci, a.g.e., "Kişisel Veriler", s. 240.

366 Kaya, "Kişisel Veriler", s. 327.

alınamayacağı durumlara örnek olarak gösterilebilir.[367] Ancak, veri sahibi kişinin sağlığına kavuşmasından sonra rızasının geçmişe dönük olarak alınması gerekir.[368] Veri sahibinin küçük veya ayırt etme gücü olmayan bir kişi olması ve veli veya vasisine ulaşılamaması hali ise hukuki nedenlerle veri sahibinin rızasının alınamayacağı hallere örnek olarak gösterilebilir.[369]

Yukarıda bahsettiğimiz düzenleme sadece veri sahibinin hayati çıkarları söz konusu olduğunda değil, başka bir kişinin hayati çıkarlarının söz konusu olması halinde de hassas kişisel verilerin işlenebilmesine olanak sağlamaktadır.[370] Veri sahibinin tehlikeli bir bulaşıcı hastalığının olması durumunda veri sahibi ile ilişki halindeki diğer kişilerin hayati çıkarlarının korunması için sağlık görevlilerinin, veri sahibinin rızasını almadan onunla alakalı hassas verileri işleyebilmesi ise üçüncü bir kişinin hayati çıkarlarının söz konusu olmasına örnek olarak verilebilir.[371]

2.1.8.2.3. Kamuya Yararlı Özel Hukuk Kişileri Tarafından İşlenme

GDPR m. 9/2(d) ve 95/46/AT sayılı Yönergenin m. 8/2(d)'e göre, uygun güvenceler verilmesi halinde, hassas veriler, dini, siyasi, sendikal veya felsefi amaç taşıyan derneğin, vakfın ve buna benzer faaliyetlerde kâr amacı taşımayan diğer kuruluşların legal faaliyetleri için işlenebilecektir.[372]

Bu istisnanın geçerli olabilmesi için, sadece bu kuruluşlara üye olanların veya belli amaçları doğrultusunda bu gibi kuruluşlarla devamlı olarak irtibatlı olan kişilerin hassas kişisel verilerinin işlemeye konu olması, bir de bu kişisel verilerin, veri sahiplerinin rızası olmadan başka kişilere açıklanmaması gerekir. Bu gibi kuruluşlara düzenli olarak bağış yapan kişiler, amaçları için düzenli olarak bu kuruluşlarla irtibatlı olan kişilere örnek olarak verilebilir.[373]

---

367 Kaya, "Kişisel Veriler", s. 327.

368 Özdemir, H., a.g.m., s. 128.

369 Kaya, "Kişisel Veriler", s. 327.

370 Kaya, "Kişisel Veriler", s. 327.

371 Rosemary, Jay, "Data Protection Law and Practice", Fourth Edition, London, Sweet & Maxwell, 2007, s. 275

372 Ayözger, a.g.e., s. 33

373 Kaya, "Hassas Veriler", s. 327 vd.

Bu kuruluşlar tarafından hassas kişisel verilerin işlenmesinde önemli olan bir husus, bu kuruluşların kamu yararı güden kuruluşlar olması gerektiğidir. Bu nedenle *"ölüme bağlı tasarruflar ile kurulan dernek ve vakıflar"* bu istisna kapsamında değerlendirilemeyecektir. Bu istisna ile ilgili bir diğer önemli husus ise, kesin işlem yasağı konusunda düzenlenen bu istisna ile sadece kâr kazanmayı amaç edinmeyen bazı kuruluşlara, bu kuruluşların sadece faaliyet gösterdikleri alanlar ile sınırlı olmak üzere, hassas kişisel verilerin işlenmesi hakkında izin verilmesidir. Görüldüğü üzere bu istisna kâr kazanmayı amaç edinmeyen tüm kuruluşlar için geçerli olmayıp, sadece siyasi, felsefi, dini veya sendikal amaçlı olan ve aynı zamanda da kâr amacı gütmeyen kuruluşlar için geçerli olmasıdır.[374]

GDPR m. 9/2-d ve 95/46/AT Yönergenin m. 8/2-d ile kamu yararı güden bazı kuruluşlara kişisel veri işleme konusunda istisna tanıyan düzenleme KVKK da benimsenmemiştir. Ancak KVKK m. 28/1-a[375] m.'sinde başka kişilere verilmemesi ve veri güvenliği ile ilgili yükümlülüklere uyulması kaydıyla sadece gerçek kişilerin, tamamen kendisi veya aynı konutta yaşadığı aile fertleri ile ilgili faaliyetler kapsamında işleme yapılması veri işleme yasağına istisna olarak kabul edilmiştir.

2.1.8.2.4. İş Hukuku Kaynaklı Yükümlülüklere Uyulması

95/46/AT sayılı Yönerge m. 8/2-b'de ve GDPR m. 9/2-b' de ki düzenlemeye göre; ulusal hukuk tarafından yetki verilip yeterli güvenceler de sağlandığında, kişisel verileri işleyenin, iş hukukundan kaynaklanan ödevlerini ve birtakım haklarını yerine getirebilmesi için mecbur olması halinde hassas veriler işlenebilecektir. İşverenin vergi ödemelerini yapma veya engelli ayrımının önüne geçmek için çalıştırdığı engelli çalışanları kayıt etme gibi, ulusal hukuk tarafından veri işleyene yüklenen hukuki bir yükümlülüğü yerine getirmek için hassas verileri işlemenin zorunlu olduğu durumlar da söz konusu olabilir.[376] İşverenin kendi işçisiyle ilgili edindiği bilgileri dürüstlük kurallarına ve hukuka uygun bir şekilde kullanma, bu verilerin gizli tutulmasında

374 Korff, a.g.e., s. 47.

375 KVKK madde 28/1-a: "*Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz: Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.*".

376 Uncular, a.g.e., s. 57.

işçinin menfaatinin bulunması halinde ise bu verileri gizli tutma zorunluluğu vardır.[377] Burada kamu hukuku çalışma alanını da çalışma hukukunun kapsamında değerlendirmek gerekir. Bir başka ifadeyle, çalışma hukukunu sadece iş hukuku alanına özgülememek gerektiği gibi[378] veri öznesini veri işleyenin çalışanı olması da zorunlu değildir.[379]

4857 sayılı İş Kanunu'nun 75. m.'sinde *"İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermek zorundadır. İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür."* kanunun lafzından açıkça anlaşılacağı üzere işveren, işçiye ilişkin kişisel verileri tutmak ile görevli ve yetkilidir. Kanaatimizce, işçiye dair KVKK kapsamında hassas kişisel veri olabilecek veriler, İş Kanunu'nun bu açık hükmü gereği işlenebilse de bu bilgilerin gizli kalmasında işçinin haklı menfaati bulunduğundan mütevellit bunları işveren, ilgili kanundaki istisnalar saklı kalmak kaydıyla açıklayamayacaktır.

2.1.8.2.5. Verinin İlgili Kişi Tarafından Kamuya Açıklanması

İlgili kişinin (veri öznesinin) bizzat açıkça halka duyurduğu verilerin işlenmesine getirilen istisna GDPR m. 9/2-e ve 95/46/AT sayılı Yönergenin m. 8/2-e'de düzenlenmiştir. Buna göre, ilgili kişinin, veri öznesi tarafından açık bir şekilde kamuya açıklanan hassas kişisel verilerin işlenmesi mümkündür. Bu düzenleme, verinin ilişkin olduğu kişinin hassas kişisel verilerini kendi istek ve kendi uğraşı veya diğer sebeplerle kamuya açıklaması durumuna ilişkindir.[380] Bu istisnadan söz edebilmek için verinin sadece kamuya açıklanması yeterli olmayıp, veri sahibinin iradesiyle bu açıklamanın gerçekleşmiş olması gerekir.[381] Bu istisnaya, ilgili kişi bir

377 Uncular, a.g.e., s. 57.

378 Kaya, "Hassas Veriler", s. 327.

379 Room, a.g.e., s. 128.

380 Özdemir, H. a.g.m., s. 130; Kaya, "Hassas Veriler", s. 329.

381 Kaya, "Hassas Veriler", s. 329.

televizyon veya radyo kanalında HIV virüsü taşıdığını söylediğinde, bu hassas kişisel verinin işlenmesinin artık mümkün olması örnek olarak verilebilir.[382]

Bu konuda "kamuya açıklanma" kavramından ne anlaşılması gerektiği hususu dikkat edilmesi gereken önemli bir noktadır. İlgili kişinin, hassas kişisel verisini özel hayat alanında bulunan, sadece bazı arkadaşlarıyla paylaşması işlemi ile herkese açık bir alanda mesela bir televizyon programında ifade etmesi arasında pek tabii bir farklılık olacaktır. Veri sahibi kişinin, istemeden hassas bazı kişisel verilerini kamunun erişimine açık bir alanda paylaşması gibi bazı durumlarda, veri sahibinin iradesi ile hareket ettiğinden bahsedilemeyeceği için bu verilerin koruma kapsamında olması gerekebilir. Bu nedenle, hassas kişisel verilerin işlenmesine olanak sağlayan istisnai durumların gerçekleşip gerçekleşmediği somut olayın özellikleri göz önüne alınarak ayrı ayrı değerlendirilmelidir.[383]

Engelli olma veya başörtüsü takmak gibi bazı durumlar görsel olarak bir kişinin, etnik kökeni, dini inancı ya da sağlığına ilişkin hassas nitelikli kişisel veriler hakkında kamuoyuna bilgi verebilir.[384] Bu gibi durumlarda, somut olay göz önüne alınarak bu durumun bir kamuoyuna duyurma olarak değerlendirilmesi durumunda, bu verileri işlerken kişinin temel hak ve özgürlüklerinin ihlal edilmemesi gerektiği unutulmamalıdır.[385]

KVKK'nın m. 28/2-b düzenlemesinde, bireyin kendisinin alenileştirdiği hassas nitelikli kişisel verilerin işlenebileceği kural olarak benimsenmiş, bu gibi hallerde veri sorumlusuna herhangi bir aydınlatma yükümlülüğünün yüklenmediği ve bir zararın varlığı halinde veri sahibinin yalnızca tazminat talep edebileceği kabul edilmiştir.[386]

2.1.8.2.6. Yargılama Sebebiyle İşlenme

Hukuksal iddiaların uygulanması, tesisi ve savunma amacıyla hassas verilerin işlenmesinin gerekli olması halinde bu verilerin işlenebileceği GDPR madde 9/2-f'de

382 Kaya, "Hassas Veriler", s. 329.

383 Carey, a.g.e., s. 86.

384 Jay, a.g.e., s. 281.

385 Özdemir, H, a.g.m., s. 138.

386 Ayözger, a.g.e., s.36.

ve 95/46/AT sayılı Yönergenin 8/2-e m.'sinde düzenlenmiştir. Aynı konunun KVKK'nın 28/1-d maddesi ile de kabul edildiğini söylemek mümkündür.[387]

Müvekkillerinden aldıkları talimatları yerine getirmek için avukatların yaptıkları faaliyetlerin çoğu bu istisna kapsamında kalırken,[388] veri işleyenler hassas verileri hukukçularına açıklarken bu istisnadan yararlanırlar.[389] Bu istisna ile veri işleyenler korunduğu gibi, veri işleyenlere yardım eden veya onlardan bilgi alan hukuk görevlileri de korunmuş olur.[390]

2.1.8.2.7. Cezalara Yönelik İşlenme

95/46/AT sayılı Yönerge m. 8/5'te "*suçlar*", "*adli hükümler*" veya "*güvenlik tedbirleri"*ne ait verilerin işlenmesinin, sadece resmi makamların kontrolünde veya ulusal yasal düzenlemeler kapsamında uygun özel korunma yöntemlerinin sağlanması halinde yapılacağı belirtilmektedir. Fakat, aynı maddede adli hükümlerin tam kaydının yalnızca resmi makamların kontrolünde tutulabileceği de düzenlenmiştir. Aynı husus, GDPR 10. m.'sinde ve KVKK'nın m. 28/2-d bendinde düzenlenmiştir.[391]

Öte yandan 5352 sayılı Adli Sicil Kanunu'nun *"Arşiv Bilgilerinin İstenmesi"* başlıklı 10. maddesinde şu şekilde bir düzenleme getirilmiştir:

"(1) Arşiv bilgileri;

a) Kullanılış amacı belirtilmek suretiyle, kişinin kendisi veya vekâletnamede açıkça belirtilmiş olmak koşuluyla vekili,

b) Bir soruşturma veya kovuşturma kapsamında Cumhuriyet başsavcılıkları, hâkim veya mahkemeler,

c) Yetkili seçim kurulları,

387 Ayözger, a.g.e., s.36.

388 Carey, a.g.e., s. 87.

389 Kaya, "Hassas Veriler", s. 330.

390 Room, a.g.e., s. 131.

391 Ayözger, a.g.e., s. 37.

d) Özel kanunlarda gösterilen hallerde ilgili kamu kurum ve kuruluşları, Tarafından istenebilir.

(2) Kanunda açıkça belirtilmediği takdirde, kişi hakkında alınacak bir karar veya yapılacak bir işlemle ilgili olarak, bir yakınının adlî sicil ve arşiv kayıtları istenemez ve bu bilgiler, kişiyi herhangi bir haktan yoksun bırakmak için dayanak olarak kullanılamaz.

(3) On sekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir."

Yine aynı kanunun 11. maddesinde *"Adlî sicil ve arşiv bilgileri gizlidir. Bu bilgiler, görevlilerce açıklanamaz ve bu Kanun hükümlerine göre verilen kişi, kurum ve kuruluşlarca veriliş amacı dışında kullanılamaz."* hükmü mevcuttur. Bu hükümlerden açıkça anlaşılacağı üzere KVKK'nın kabulünden önce dahi kişilerin mahkumiyetine ilişkin bilgiler hassas kişisel veri niteliğinde görülerek özel korumaya tabi tutulmuştur.[392]

İşlenen suçlar hakkında yürütülen soruşturmalar, suç işlenmesinin önlenmesi için uygulanan güvenlik tedbirleri ve bunların çeşitli aşamalarında gerçekleştirilen her türlü işlemin içerdiği hassas kişisel verilerin işlenmesi yetkili makamların denetimi altında yapılabilecektir.[393] Burada yetkili merciden kast edilen suçu soruşturan polis veya savcı olabileceği gibi, bazen hâkim de olabilir. Mahkûmiyet kararlarına ilişkin olan sicil resmi makam kontrolünde tutulmalıdır ki ülkemizde Adalet Bakanlığı bu sicili tutan makamdır.[394]

2.1.8.2.8. Sağlık Gerekleri

95/46/AT m. 8/2'ye göre *"sağlık hizmetlerinin yönetimi"* veya *"bakım veya tedavinin sağlanması", "tıbbi teşhis", "önleyici tıp"* gibi konularda veri işleme

---

392 Boz, Ahmet, "Kişisel Verilerin Korunması, Türkiye, ABD ve AB Örnekleri", (Yayınlanmamış Yüksek Lisans Tezi) Polis Akademisi, Güvenlik Bilimleri Enstitüsü, Güvenlik Stratejileri ve Yöntemi Anabilimdalı, Ankara. 2014, s. 103.

393 Özdemir, H, a.g.m., s. 132-133.

394 Ayözger, a.g.e., s. 37.

faaliyetinin gerekli olması halinde, mesleki anlamda gizlilik yükümlülüğünün yerine getirilmesi amacıyla, ulusal kanun kapsamında, yetkilendirilmiş ulusal kuruluş veya buna aynı statüde başka bir sağlık uzmanı tarafından verilerin işlenmesi halinde hassas verilerin işlenmesi yasağı uygulanmayacaktır.

Benzer düzenleme, GDPR m. 9/2-h-i'de yer almaktadır. Yani, koruyucu ve önleyici sağlık ihtiyaçları, çalışanların iş gücü kapasitelerinin değerlendirilmesi, sağlık ve sosyal güvenliğin sağlanması ve yönetilmesi konusunda hassas kişisel verilerin işlenmesi mümkün olup, hatta bu kapsamda kamu yararı için toplum sağlığının korunmasına dair kişisel verilerin işlenmesi zorunludur.[395]

Düzenlemede yer verilen "tıbbi" terimi geniş yorumlanmalı, her türden tıbbi faaliyet ile bunların sonuçları "tıbbi" kavramı kapsamında değerlendirilmelidir. Mesela, kan tahlili sonuçlarında bir kişinin HIV virüsü taşıyıcısı olduğunun tespit edilmesi halinde kişiye uygulanan tedaviler hakkındaki bilgiler kesin işlem yasağının istisnası olarak kabul edilir. Ancak sadece yetkili sağlık personeli veya gizlilik yükümlülüğü bulunan başka bir kişi tarafından bu veriler işlenebilecektir.[396]

KVKK m. 6/3'te sağlık ve cinsel hayata dair kişisel verilerin sadece *"kamu sağlığının korunması*", *"koruyucu hekimlik", "tıbbî teşhis", "tedavi ve bakım"* hizmetlerinin yerine getirilmesi, *"sağlık hizmetleri ve finansmanının"* planlanıp yönetilebilmesi amacı ile mesleki gizlilik yükümlülüğü bulunan kişi veya yetkili kurum ve kuruluşlar tarafından veri sahibinin açık rızasına gerek duyulmadan işlenebileceğine yer verilmiştir.

2.1.8.2.9. Ek İstisnalar

95/46/AT sayılı Yönergede üye ülkelere esneklik sağlayabilmek için hassas veri işleme konusunda üye devletlerin ek istisnalar getirebileceği düzenlenmiş, bu kapsamda, üye ülkelerin, uygun güvenceler sağlamak kaydıyla, üstün kamu yararı nedeniyle, ulusal yasal düzenlemeler yoluyla veya ulusal veri koruma yetkilisinin kararıyla, burada yer alan istisnalara ek olarak bir takım istisnalar getirebileceği

395 Ayözger, a.g.e., s. 38.

396 Özdemir, H, a.g.m., s. 131 vd.

benimsenmiş, üye ülkeler tarafından kabul edilecek olan bu ek istisnaların 95/46/AT sayılı Yönergede m. 8/6'da Komisyona bildirim yapılması gerektiği düzenlenmişti. GDPR ile birliğe üye devletlerin ulusal hukuk sistemlerindeki kişisel verilerin korunmasına dair olan düzenlemeler ilga edilse dahi, yine de bu devletler tarafından özellikle sağlık, genetik ve biyometrik verilerle alakalı ek istisnalar belirlenebilecektir. Ancak getirilen istisnaların Avrupa Komisyonu'na gecikmeksizin bildirilmesi gerekir. Bunun yanında Avrupa Komisyonu'na kişisel verilerin işlenmesi istisnalarına ek istisnalar getirme hususunda yetki de verilmiştir.[397]

95/46/AT sayılı Yönergeye ek olarak, GDPR madde 9/2-g'de, yeterli korumanın sağlanması şartıyla kamu yararına yerine getirilen bir görevin ifa edilmesi amacıyla gereken işlemelerle GDPR madde 9/2-j uyarınca tarihsel, istatistiksel ya da bilimsel nitelikli araştırma için gereken işlemelerde istisna olarak sayılmıştır.[398]

KVKK'nın 28/1. m.'sindeki düzenlemede hassas nitelikli veriler özel olarak ifade edilmese dahi, söz konusu verilerin işlenmesinde açık rızanın aranmayacağının belirtildiği ek istisnalar şu şekilde düzenlenmiştir;

- resmi istatistik ile anonim hale getirilen kişisel verilerin "araştırma", "planlama" ve "istatistik" gibi amaçlarla işlenmesi,
- millî savunma, millî güvenlik, kamu güvenliği, kamu düzeni, ekonomik güvenlik, özel hayatın gizliliği veya kişilik hakları ihlal edilmemek veya suç teşkil etmemek kaydıyla, kişisel verilerin "sanat", "tarih", "edebiyat" veya "bilimsel" amaçlarla veya "ifade özgürlüğü" kapsamında işlenmesi,
- millî savunma, millî güvenlik, kamu güvenliği, kamu düzeni veya ekonomik güvenlik sağlanmaya çalışılırken, kanunla görevlendirilip yetki verilmiş kamu kurum ve kuruluşları tarafından yerine getirilen

397 Ayözger, a.g.e., s. 38.

398 Ayözger, a.g.e., s. 39.

"önleyici", "koruyucu" ve "istihbari" faaliyetler kapsamında kişisel verilerin işlenmesi.

Bu madde kapsamındaki istisnalar kamu yararı göz önüne alınarak getirilmiş ise de düzenlemenin kapsamının genişliği nedeniyle bu istisnaların uygulamada pek çok insan hakları ihlallerine yol açması muhtemel olacağına ilişkin görüşler doktrinde kendisine yer bulmuştur.[399]

2.2. VERİLERİN KORUNMASINDA TEMEL İLKELER

Kişisel verilerin işlenmesi sırasında dikkate alınması gereken temel ilkeler uluslararası belgeler[400] ve iç hukukumuzdaki düzenlemeler[401] göz önüne alınarak aşağıdaki gibi gruplandırılabilir:

2.2.1. ESASA İLİŞKİN TEMEL İLKELER

2.2.1.1. Kişisel Verilerin Hukuka ve Dürüstlük Kuralına Uygun İşlenmesi

Kişisel verilerin *"hukuka ve dürüstlük kurallarına uygun bir şekilde işlenmesi"* ilkesi, aşağıda açıklanacak olan diğer ilkeleri de içinde barındırması ve bu ilkelere kaynak pozisyonunda olması sebebiyle kişisel verilerin korunması hukukun açısından "*asli ilke"* olarak değerlendirilmektedir.[402] Dürüstlük kuralına ve hukuka uygunluğun, kişisel verilerin işlenme sürecinin başlamasından sona ermesine kadar devam etmesi gereklidir.[403] *"Hukuka uygun olma"* ile kastedilen, kişisel verilerin işlenmesi sürecinde yasalar ve konu ile alakalı diğer hukuki düzenlemelerde yer alan kurallara uygun olarak davranma gerekliliğidir.[404]

95/46/AT sayılı Yönerge m. 5/1'de ve aynı doğrultuda KVKK m. 4/2-a'da *"kişisel verilerin hukuka ve dürüstlük kurallarına uygun işlenmesi"* gerektiği ilkesine yer verilmiştir. Hukuka uygun olması ilkesi ile kast edilen, veri işleyenin yasalardan

399 Ayözger, a.g.e., s. 39.

400 Kişisel verilerin işlenmesine ilişkin ilkeler için bkz. 95/46/AT sayılı Yönerge 6. madde.

401 Kişisel verilerin işlenmesine ilişkin ilkeler için bkz. KVKK madde 4/2.

402 Küzeci, a.g.e., s. 196.

403 Özdemir, H., a.g.m., s. 137.

404 Küzeci, a.g.e., s. 196.

ve diğer hukuki düzenlemelerden kaynaklanan ilke ve yükümlülüklere uygun olarak kişisel verileri işleme faaliyetlerinin yürütülmesidir.[405] Veri işleme faaliyetleri esnasında hukuka uygun hareket edilmemesi, işleme konusu ile alakalı bir kanun hükmünün ihlali sonucunu doğuracaktır.[406]

Kişisel verilerin dürüstlük kuralına uygun olarak işlenmesi ilkesi ise; veri denetçileri (sorumluları) tarafından, kişisel verilerin işlenmesi esnasında tarafların çıkarlarının ve makul beklentilerinin dikkate alınmasıdır.[407] Bu dürüstlük kuralına uygun olma ilkesi, verilerin işlenmesinin şeffaflığı açısından da önem arz etmektedir.[408] Mesela, yasal bir dayanağı bulunmadan veya kanunda öngörülen amaca aykırı olacak biçimde kayıt ve işleme araçlarıyla gizli olarak kişisel verilerin toplanması[409] ve gizli makineler kullanılmak suretiyle ilgilinin haberi olmadan kişisel verilerin işlenmesi "*hukuka ve dürüstlük kuralına uygun işlenme ilkesi"*ne aykırılık oluşturacaktır.[410] Ayrıca, kişisel verilerin işlenmesi esnasında bilgilendirme ve uyarı yükümlülüğüne uyulması, şeffaf olunması da *"dürüstlük kurallarına uygun olma ilkesi"*nin kapsamındaki hususlardır.[411]

GDPR m. 5/1-a'da *"hukuka ve dürüstlük kuralına uyma ilkesi"*nin yanı sıra şeffaflık ve adalet de dile getirilmiştir. Kişisel verilerin işlenmesinde uyulması için getirilmiş düzenlemelere uygun şekilde kişisel verilerin toplanarak işlenmesi ilkesi, kişisel verilerin işlenmesi sürecinin genelinde, veri toplama ve işleme hususlarında ilgili kişilerin aldatılmaması veya veri işleme amacıyla uyuşmayan ya da kişilerin anlamayacağı bir amaç için işlenmemesini kapsamına alır.[412] Bu hususlar aynı zamanda dürüstlük kuralının temelini de teşkil eden *"*amaca uygun davranma ve yanıltmama" prensipleri ile uyuşmaktadır.[413]

---

405 Küzeci, a.g.e., s. 196.

406 Jay, a.g.e., s. 244.

407 Küzeci, a.g.e., s. 197.

408 Özdemir, H., a.g.m., s. 137.

409 Şimşek, a.g.e., s. 85.

410 Başalp, a.g.e., s. 37.

411 Küzeci, a.g.e., s. 197.

412 Başalp, a.g.e., s. 37.

413 Ayözger, a.g.e., s. 120.

2.2.1.2. İlgilinin Rızasının Alınması İlkesi

Kişisel veriler işlenmeden önce kişisel veri ile ilgili olan kişinin rızasının alınması zorunludur.[414] Veri ilgilisinin -ilgili kişinin- kişisel verilerinin işlenmesi için gösterdiği rızanın geçerli bir rıza olması gerektiğinden, veri sahibi işlem konusunda yeterli derecede bilgilendirilmeli ve rızanın verilmesi konusunda dışarıdan bir etkiye maruz kalmamalıdır.[415] Bunun yanında, yasal metinlerde açıkça düzenlendiği hallerde veya kişisel verilerin işlenmesinde üstün tutulabilecek özel veya kamusal yararın söz konusu olması halinde, ayrıca kişinin rızasına gerek duyulmadan kişisel veriler işlenebilecektir.[416]

Veri ilgilisinin -ilgili kişinin- verdiği rızanın hukuken geçerli olarak kabul edilen bir rıza olması için, veri işleyicisinin, kişisel verilerde yapılacak işlemin amacı, işlemenin içeriği, bu işlemin süresi ve verilerin kullanılacağı yerler konusunda, veri ile ilgili kişinin ayrıntılı bir şekilde aydınlatılması gereklidir.[417] Taraflar veri işleme ile ilgili bu açıklamaları yapmamışsa, ilgili kişi bu bilgileri talep etmelidir. İlgili kişinin aydınlatılması için şablon bir metnin kullanılması halinde, bu metnin kişilere yön vermeye yönelik ve anlaşılır olması gerekir. Herkes tarafından anlaşılamayacak hukuki bir metin ilgili kişilerin bilgilendirilmesi için elverişli olmayıp bu amaca hizmet edemeyeceğinden, bu metin doğrultusunda verilen rızanın hukuken geçerli bir rıza olamayacağı açıktır. Bu bağlamda, GDPR m. 7/2'de başka hususlara ilişkin rızaları da içeren yazılı metin ile kişisel veriler için de ilgilinin rızası alınmış ise, ilgilinin vermiş olduğu rızanın hukuken geçerli bir rıza olabilmesi için bu rıza talebinin bu diğer hususlardan ayırt edilebilecek tarzda ilgiliye sunulmasının gerektiğine yer verilmiştir.

---

414 Lloyd, a.g.e., s. 97-98.

415 Atak, Songül, "Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri", Bahçeşehir Üniversitesi Hukuk Fakültesi, Kazancı Hakemli Hukuk Dergisi, Yıl: 2009, Sayı: 59–60, s. 211.

416 Özdemir, H., a.g.m., s. 139.

417 Article 29 Data Protection Working Party, Opinion 15/2011 on the Definition of Consent, 2011, s.17,ec.europa.eu/justice/dataprotection/article29/document/opinionrecommendation/files/2011/wp187 en.pdf, Erişim tarihi, 19.06.2019.

Rızanın hukuken geçerli olabilmesi için kişisel veri ile ilgili kişinin, başka kişilerin etkisi altında kalmadan kendi özgür iradesi ile rızasını bildirmesi gerekir.[418]

Kişisel verilerin işlenmesi hakkında verilecek rızanın geçerli olması için; rızanın serbestçe ve konuya özel olarak verilmiş, ilgili kişinin açıkça bilgilendirilmiş ve kesin olması gerekmektedir.[419] Rızanın ilgili kişi tarafından genel bir şekilde verilmemiş olması ve somut olarak belirli bir durum veya amaca yönelik olarak verilmesi gerekir. İlgili kişinin kendisi hakkında işleniyor olan veya daha sonraki zamanlarda işlenecek olan veriler için önden toplu bir rıza beyanında bulunması halinde, bu şekilde verilmiş olan rıza beyanı hukuka aykırı olacaktır.[420]

Avrupa hukukunda, rızanın hukuken geçerli olması için gereken şekil hakkında getirilmiş kurallar yoktur.[421] Fakat rızanın yazılı olarak verilmesi ispat açısından daha uygun olacaktır. GDPR m. 6/1-a, KVKK m. 5/1'de ve EHSKVİY'de de verilecek rızanın şekil şartına ilişkin bir düzenleme bulunmamaktadır. Yalnızca ETDK m. 6/1'de elektronik ticari mesajlara yönelik oluşturulan düzenlemede önceden alınan yazılı rızadan bahsedilmektedir.[422]

Kişisel verilerin işlenmesi için verilen rızanın zamanlaması da rızanın geçerli olup olmamasında önem arz etmektedir. Genel kural, belli bir veri işleme faaliyeti konusunda gerekli olduğu her zaman ve işleme faaliyeti başlamadan önce veri ilgilisinin rızasının alınmasıdır.[423] Bu durum, özellikle, kullanıcıların cihazlarına *"çerez"* yerleştirilmesi veya konumlarının katma değerli hizmetler veya pazarlama için kullanılması gibi "*çevrim içi davranışsal reklamcılık"* için geçerlidir. Her halde, kullanıcıların kolayca ve basit bir şekilde erişebilecekleri yollardan rıza verebilmeleri ve rıza verdikten sonra ise istedikleri zaman onaylarını geri alabilmeleri gereklidir.[424] Kişinin kişisel verileri işlendikten sonra onayının alınması, rızadan önceki işlemleri

418 Article 29 Data Protection Working Party, 15/2011, s. 12-13, 31.

419 Article 29 Data Protection Working Party, 15/2011, s. 34-35.

420 Özdemir, H., a.g.m., s. 140.

421 Article 29 Data Protection Working Party, 15/2011, s. 11-12.

422 Ayözger, s. 122.

423 Article 29 Data Protection Working Party, 15/2011, s. 30.

424 Şimşek, a.g.e., s. 107.

hukuka uygun duruma getirmez.[425] Ancak GDPR m. 7/3'te düzenlendiği gibi, daha önceden verilen onayın daha sonra geri alınması halinde, geri alma eyleminden önceki döneme ait olan ve ilgilinin rızasına dayanan işlemelerin hukuka uygun nitelikleri devam eder.[426] Ayrıca rızanın geri çekilmesinin rıza vermek kadar kolay olması gerekmektedir.

2.2.1.3. Belirli Bir Amacın Bulunması

Bu ilkeye göre kişisel veriler, sadece yasal düzenlemelerde açıkça belirlenmiş, hukuka uygun ve sınırlı olarak belirlenmiş amaçlar için işlenebilecektir.[427] Bu ilke, somut bir olayda, verilerinin işlenmesinden önce hangi amaç için verilerin toplandığı konusunda kişisel veri ilgilisinin bilgi sahibi olmasını sağlayacaktır.[428]

Kişisel veri ilgilisinin, kişisel verilerinin işlenme amacını önceden bilmesi ise, kişisel veri ilgilisine kendi verilerini kontrol etme ve kişisel verileri hakkında önleyici koruma imkânı sağlayacaktır.[429] Ayrıca bu sayede, ileriki zamanlarda, kişisel verilerin hangi sınırlar içerisinde ve hangi nedene dayanarak toplanmış ve işlenmiş olduğu hakkında "amaca uygunluk" yönünden denetleme yapılabilecektir.[430]

Bu nedenle, kişisel veriler toplanırken veri sorumlusunun belli bir amacının olup olmadığıyla da hangi amaçlar için kişisel verileri toplayıp işlediği hakkında herhangi bir şüphe de bulunmamalıdır.[431]

Kişisel veriler hakkında yapılan hukuki düzenlemelerde muğlak ifadelere yer verilmemesi gerekliliği kişisel verilerin işlenme amaçlarının belirli ve açık olması ilkesinin bir sonucudur. Kişisel verilerin, herhangi bir amaç güdülmeden *"belki bir gün gerekli olabilir"* düşüncesiyle kullanılması ihtimaline binaen toplanarak tutulması bu ilkeye aykırılık sonucunu doğuracaktır.[432] Bu kapsamda, belirli ve somut yasal bir

425 Lloyd, a.g.e., s. 100.
426 Ayözger, a.g.e., s. 122.
427 Şimşek, a.g.e., s. 83.
428 Başalp, a.g.e., s. 37.
429 Şimşek, a.g.e., s. 83.
430 Başalp, a.g.e., s. 38.
431 Şimşek, a.g.e., s. 84.
432 Küzeci, a.g.e., s. 198.

amaç bulunmadan kişisel verileri toplamak için oluşturulan veri depoları belirli bir amacın bulunması ilkesine aykırılık oluşturmaktadır.[433]

"Kişisel veri işlemede belli bir amacın bulunması" ilkesi, kişisel veri hukukuna ilişkin uluslararası metinlerde de benimsenmiştir. Örneğin, 108 sayılı sözleşmesinin 5. maddesinin 5. fıkrasında, bireylere ait kişisel verilerin, *"belirli ve meşru amaçlar"* doğrultusunda kaydedilebileceği ve söz konusu amaçlara uygun olmayacak tarzda kullanılmamaları gerektiği düzenlenmiştir. 95/46/AT sayılı Yönergenin 6. m.'sinde bireylerin kişisel verilerinin *"belli, açık ve yasal amaçlar"* doğrultusunda toplanması gerektiği belirtilmiş; verilerin söz konusu amaçlara aykırı bir şekilde işlenmesi ise yasaklanmıştır. Kişisel verileri işleme aşamalarının ilkinden sonuncusuna kadar bütün evrelerde bu ilke göz önünde bulundurulması gerekir. Hangi verilerin işleneceği ve elde edilen verilerin farklı bir amaç için kullanılıp kullanılamayacağı bu ilke sayesinde belirlenebileceği için, bu ilke özellikle iş çevreleri için daha önemlidir.[434]

Kişisel verilerin işlenme amacının açık olması ile ifade edilmek istenen ise, kişisel verilerin sadece açık bir şekilde ortaya konulmuş bir amaç için toplanıp işlenebileceğidir. Kişisel verilerin işlenmesi için açıklanan amaçla uyuştuğu ölçüde, belirlenen amacın sonradan değiştirilebilmesi mümkün olacaktır.[435]

Kişisel veri işleme amacının meşru olması demek, kişisel verilerin toplanması ve tutulmasının hukuki düzenlemelerde öngörülen gerekliliklere uygun ve yasal bir temelinin bulunması, verilerin işlenmesinden hedeflenen amaçla dengeli olması demektir.[436]

2.2.1.4. Amaca Bağlılık İlkesi

Kişisel verilerin işlenmesi amacını meşru hale getiren nedenler KVKK'nın 5. ve 6. m.'lerinde *"kişisel verilerin işlenme şartları"* başlığında sayılmışken, *"amaca bağlılık ilkesi"*, GDPR m. 5/1-b'de ve bununla uyumlu olarak da KVKK m. 4/2-c' de yer almıştır. *"Amaca bağlılık ilkesi"*, bireylere ait kişisel verilerin belirlenmiş ya da

433 Şimşek, a.g.e., s. 84.
434 Küzeci, a.g.e., s. 198.
435 Başalp, a.g.e., s. 38.
436 Küzeci, a.g.e., s. 199.

önceden belirlenmesi mümkün ve hukuka uygun amaçlar doğrultusunda toplanmasını ve söz konusu amaçlarla orantılı bir şekilde işlenmesini ifade eder.[437] Belli amaçlar doğrultusunda toplanan kişisel veriler, bu belirlenmiş amaçtan farklı bir amaç için kaydedilemeyecektir. Kişisel verilerin, toplanma amacından başka legal bir amaç için kaydedilebilmesi, ancak toplama amacına izin veren yasal düzenlemede bu tür bir kaydetmenin açıkça yer alması halinde söz konusu olabilir. Bu çerçevede, kişisel verilerin toplama amacına aykırı olarak toplanması ve bunun neticesinde işlenmesi hukuka aykırı olacaktır.[438]

"Amaca bağlılık ilkesi", kişisel verileri işlenen veri ilgilisine, verileri işleyenlerden hangi amaç doğrultusunda verilerinin toplandığını ve bu verilerinin bu amaç için işlenip işlenmediğini öğrenme imkânını sağlayacaktır.[439]

Eğer kişisel verilerin ilk işlenmesi esnasında taşıdığı amaç sonradan değişirse, kişisel veri ile ilgili olan kişinin rızasının yeniden alınması gerekecektir.[440] Bu durum kişisel verilerin hukuki niteliğinden birisi olarak ifade edilen "*bilginin geleceğini belirleme hakkı"*nın bir ortaya çıkardığı bir durumdur. Zira, kişisel veriler bir kere kaydedildikten sonra bu verinin her türlü işleme tabi tutulmasının makul karşılanması mümkün değildir.[441] Nitekim, veri ilgilisine, toplanılan kişisel verilerinin, belirlenmiş olandan başka amaçlarla kullanılmaması noktasında teminat sağlanmıştır.[442] Bir suçun soruşturulması esnasında alınan kişiye ait DNA örneklerinin bundan farklı bir amaçla kullanılamaması bu duruma örnek gösterilebilir.[443]

Bunun yanında, sonradan çıkan yeni amaç, eğer kişisel verilerin toplanması için veri ilgilisinin rıza gösterdiği başlangıçtaki amaca uygun veya onu tamamlayan bir amaç ise ve veri işleyen kişinin sonradan çıkan bir amaç kapsamında kişisel verileri

437 Özdemir, H., a.g.m., s. 141.

438 Şimşek, a.g.e., s. 98.

439 Özdemir, H., a.g.m., s. 141.

440 Özdemir, H., a.g.m., s. 141.

441 Küzeci, a.g.e., s. 207.

442 Şimşek, a.g.e., s. 85.

443 Küzeci, a.g.e., s. 208; ayrıntılı bilgi için bkz. Çalışmanın CMK Kapsamında Koruma Bölümü.

işlemesi dürüstlük kuralına aykırı düşmüyorsa, *"amaca bağlılık ilkesi"*nin ihlal edilmediği kabul edilecektir.[444]

Kişisel verilerin işlenmesinde söz konusu olan amaç "*belirli"*, "*açık"* ve "*meşru"* olmalıdır.[445] Amaca bağlılık ilkesi gereğince kişisel veriler bir gün gerekli olabileceği ihtimali üzerine toplanamayacağından,[446] kişisel verilerin toplanması esnasında bilinmeyen ya da ilerleyen zamanda ortaya çıkma ihtimali bulunan amaçlar, "*belirli amaç"* kapsamında değerlendirilemeyeceklerdir.[447]

"*Amacın açıklığı"* ise, kişisel verilerin işlenmesine dair olan hukuki düzenlemelerin muğlak ibarelerden uzak olması ve sadece açıkça ortaya konulmuş amaçlar doğrultusunda toplanıp işlenmesi anlamına gelmektedir.[448]

Bireylere ait kişisel verilerin sadece *"meşru amaç"*lar doğrultusunda işlenebiliyor olması, söz konusu işlemlerin hukuki bir dayanağının olmasını, aynı zamanda yasak düzenlemelerle kişisel verilerin işlenmesinde güdülen amaç arasında bir dengenin kurulması anlamına gelir.[449] Bu kurallar ile kişisel verilerin işlenme amaçları sınırlandırılmış olmaktadır.[450] Yani, amacın sınırlandırılması ile veri işleyenlerin kişisel verileri neden ve nasıl kullanacaklarına dair sınırlama getirilmek suretiyle veri sahiplerinin korunması hedeflenmiştir.[451]

Anayasa Mahkemesi bir kararında[452] bu konulara vurgu yaparak keyfi uygulamalara engel olacak şekilde sadece kanunla sayılı olarak tespit edilmiş amaçlar için kişisel verilerin işlenebileceği ifade edilmiştir.

---

444 Jay, a.g.e., s.273.

445 Article 29 Data Protection Working Party, s. 15.

446 Küzeci, a.g.e., s. 198.

447 Özdemir, H., a.g.m., s. 142.

448 Başalp, a.g.e., s. 38.

449 Küzeci, a.g.e., "Kişisel Veriler", s. 199.

450 Özdemir, H., a.g.m., s. 142.

451 Article 29 Data Protection Working Party, 03/2013, s. 22.

452 "*.. İptalini istediğimiz iş bu Kural'ın metninde, Telekomünikasyon İletişim Başkanlığı tarafından temin edilecek olan trafik bilgilerinin mâhiyetinin belirsiz olmasının yanı sıra, mezkûr bilgileri temin etme yöntemi de net ve sarih değildir. Bilindiği üzere, bilgi mefhûmunun, hassas bilgi, şahsî bilgi, gizli bilgi, ticârî sır gibi çeşitli türleri bulunmaktadır. Bu tür bilgilerden hangisinin, hangi yöntemlerle talep ve temin edileceği; kişisel hakların, mahremiyetin ve özel hayatın*

2.2.1.5. Orantılılık ve Gereklilik İlkesi

"Orantılılık ilkesi", kişisel veri işlemesinin, açıklanan işleme amacı yönünden gerekli ve faydalı olmasını ifade eder.[453] Kişisel veri işlemede, kişisel verileri işleyen ilgili makamların *"orantılılık ilkesine"* uygun hareket etmeleri gereklidir.[454]

Kişisel verilerin işleme amaçlarından başka amaçlar için kullanılması, işleme amacı için gerekli olmayana da bu amaçla alakası olmayan verilerin toplanması ve kullanılması yasak olduğu için, veri koruma görevlisinin amaca erişmekte yararı olmayacak kişisel verileri kullanmaktan imtina etmesi gerekmektedir.[455] Mesela, suç takibi için telefon dinlemesi yapılırken bu amaçla ilişkili olmayan telefon kayıtlarının kullanılması doğru değildir. Ayrıca, internette kullanıcıların bilgi taleplerinin giderilmesi için üyelik gerektiren sitelerde gereği olmayan kişisel verilerin toplanması durumundaki gibi, veri işleyen kişinin amaca ulaşmak için gerekli olmayan kişisel verileri kesinlikle toplamaması gerekir.[456]

"Gereklilik ilkesi", ulaşılmak istenen amaç ile işlenen kişisel veri ile arasında uygun illiyet bağının bulunması zorunluluğunu ifade eder.[457] Toplanan ve kaydedilen kişisel verilerin kapsamı ve türü veri toplanmasına gerekçe olan yasal amacın yerine getirilebilmesine uygun ve yeterli derecede olmalı, amacı sağlayacak ölçü aşılıp gerektiğinden fazla kişisel veri işlenmemelidir.[458]

---

gizliliğinin korunması için elzemdir. Anayasa'nın 2. maddesinde ifadesini bulan "hukuk devleti" ilkesinin, belirsizliğe, muğlak ya da müphem düzenleme ve uygulamalara tahammülü yoktur. Bu itibarla, 6552 sayılı Kanunun 126. maddesi ile 5651 sayılı Kanunun 3. maddesinin dava konusu dördüncü fıkrasında yapılan değişiklik, Anayasa'nın "hukuk devleti" ilkesini benimseyen 2. maddesine ve bu meyânda, "Temel hak ve hürriyetlere getirilen sınırlamaların, özlerine dokunulmaksızın, yalnızca kanûnîlik ve ölçülülük kriterlerine uygun olması" ilkesini öngören 13. maddesine de açıkça aykırılık teşkil etmektedir…" AYM'nin 02.10.2014. tarihli ve 2014/149 Esas ve 2014/ 151 Karar numaralı kararı.

453 Kılınç, a.g.m., s. 1125.

454 Özdemir, H., a.g.m. s. 143.

455 Küzeci, a.g.e.,"Kişisel Veriler", s. 203.

456 Şahin, Osman, "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğinin Korunması", (Yayımlanmamış Bilişim Uzmanlığı Tezi), Bilgi Teknolojileri ve İletişim Kurumu, 2011, http://btk.gov.tr/kutuphane_ve_veribankasi/tezler/ index.php, Erişim tarihi, 04.07.2019.

457 Başalp, a.g.e., s. 38.

458 Şimşek, a.g.e., s. 84 vd.

Bu ilkelere göre, her veri işlemesi somut olayında, işlem yapılmak istenen verinin işleme amacı için uygun olup olmadığı ve söz konusu verinin işlenmesinin bu amaca ulaşmak için gerekli olup olmadığı yönünde değerlendirme yapılmalıdır.[459] Bu yönde inceleme yapılırken, kişisel verilerin toplanması anındaki amaç ile daha sonraki safhalardaki amaçlar arasındaki bağlantı, kişisel verilerin işlendiği kapsam ve veri ilgilisinin sonraki aşamalardaki kullanım hakkındaki beklentileri, kişisel verilerin yapısı ve sonraki aşamalardaki veri işlemelerinin veri sahipleri üzerindeki etkisi göz önünde bulundurulmalıdır.[460]

Toplanan kişisel veriler amacı aşacak kadar olmamalı, yani veri ilgilisinin çıkarlarını tehlikeye düşürecek orantısızlık tehlikesi söz konusu olmamalıdır.[461] Bir diğer deyişle, kullanılan araç ile varılmak istenen amaç arasında bir denge olmalıdır.[462]

95/46/AT sayılı Yönerge m. 6/1(c)'de *"toplandığı ve/veya ayrıca işlendiği amaçlara ilişkin olarak yeterlidir, ilgilidir ve bu amacı aşmaz"* hükmü ile orantılılık ilkesi düzenlenmiştir. GDPR m. 5/1-c'de ise; amaca varmak için yetecek kadar, sadece amaç ile ilgisi olan ve hedeflenen amaç ile sınırlı olacak kadar verinin işlenmesi diğer bir ifade ile "veri minimizasyonu ilkesi" getirilmiştir. Uluslararası düzenlemelerle uyumlu olarak KVKK'nın 4/1-ç, EHK'nın 50/1 ve EHSKVİY 4/1-c hükümlerinde bireylere ait kişisel verilerin hangi amaç doğrultusunda toplanıyorsa, o amaçla *"bağlantılı", "yeterli"* ve *"orantılı"* şekilde işlenmesi gerektiği düzenlenmiştir.

"Orantılılık ilkesi", kişisel verilerin işlenmesi sürelerinin hedeflenen amaçla sınırlandırılmasını gerektirir. Kişisel veri işlemesi ile varılmak istenen amaca ulaşılmış ise, söz konusu veriler daha fazla saklanamaz.[463] Kişisel veriler, özellikle, teşhis etmeye imkân tanıyacak şekilde toplanmış ve işlenmiş ise, söz konusu amaçların

459 Özdemir, H., a.g.m., s. 143.

460 Article 29 Data Protection Working Party, 03/2013, s. 23-26.

461 Başalp, a.g.e., s. 38.

462 Kılınç, a.g.m., s. 1125.

463 Özdemir, a.g.m., s. 143-144.

gerçekleşmesi için gerekli olan süre dolduktan sonra kişisel veriler ya anonimleştirilmeli ya da silinmelidirler. [464]

GDPR m. 5/-e'de bu konu aynı şekilde düzenlenmiş, KVKK m. 4/2-d'de saklama süresi *"amaç için gerekli olan süre"* şeklinde sınırlandırılmıştır.

Kişisel verilerin işlenmesinin kullanım amacı açısından zorunlu olması kadar bu kişisel verilerin toplanmasının yanı sıra, toplanma ile hedeflenen amaca ulaşılmasından sonra kişisel verilerin daha fazla muhafaza edilmemesi de gereklidir.[465]

Kişisel verilerin saklanması, kişisel verilerin işlenmesi ile ulaşılmak istenen amaca ulaşılmasına kadar hukuka uygun olarak kabul edilecektir.[466] Kişisel verilerin, işlendiği amaçlar için gerekenden daha fazla süre tutulmaması[467], belirlenen sürenin geçmesine rağmen hâlâ daha saklanmaya devam edilebilmesi için ise bu kişisel verilerin anonim hale getirilmesi gereklidir.[468]

Kişisel verilerin korunabilmesi için bu kişisel verilerin zaman yönünden sınırlandırılmış olarak kaydedilmesi zorunludur.[469] Çünkü, kişisel verilerin korunması düşüncesinin temelinde de bu vardır. Kişisel verilerin, bir kez kaydedilmesinden sonra veri sahibinin hayatı boyunca gerektiğinde kullanılmak üzere bir yerde tutulması, kişilerin maddi ve manevi bütünlüğünü zedeleyecektir.[470]

2.2.1.6. Verilerin Doğruluğu ve Güncelliği İlkesi

GDPR madde 5/1-d'de doğruluk ilkesi aynı zamanda verilerin kaliteli olmasına yönelik düzenlenmiş, iç hukukumuzda ise KVKK madde 4/2-b'de "*doğru ve gerektiğinde güncel*" ifadesine yer verilerek bu ilke kabul edilmiştir.

---

464 Kılınç, a.g.m., s. 1126.
465 Şimşek, a.g.e., s. 84-85.
466 Başalp, a.g.e., s. 39.
467 Şimşek, a.g.e., s. 85.
468 Başalp, a.g.e., s. 39.
469 Şimşek, a.g.e., s. 85.
470 Küzeci, a.g.e., s. 210.

Kişisel verileri işlenecek olan veri sahiplerinin, kendilerine ait veya kendileriyle ilgili olan verilerin doğru ve güncel olmalarını isteme hakları vardır.[471] İşlenecek olan kişisel verilerin doğruluğu, kişisel veri işleme sürecinin başından sonuna kadar devam etmesi gerektiği için, veri sahibinin işleme sırasında kişisel verilerde meydana gelen değişikliklerin güncellenmesini talep etme ve bu kapsamda kendilerine ait verilerin doğru olup olmadıklarını düzenli olarak kontrol etme hakları vardır.[472] Kişisel veriler hatalı olduklarında ya da güncel olmadıklarında, bunların silinmesi veya düzeltilmesi için yapılması gerekli olan işlemlerin veri koruma görevlisi tarafından yerine getirilmesi ve bunun için lazım olan sistemlerin oluşturulması gereklidir.[473] Bu işlemler, aynı zamanda *"verilerin kaliteli olması"*nı da sağlayacaktır.[474]

Kişisel verilerin toplanma amacının *"açık ve belirli olması"*, verilerin içerik olarak tam, yeni durumda ve doğru olmalarını, yani bu verilerin güncel olmalarını da gerektirmektedir.[475]

"Güncellik ilkesi", kişisel verilerin maddi doğruluğunun sağlanması, bir başka ifadeyle tutulan kişisel verilerin güncel ve doğru olmasının sağlanmasını ifade eder.[476] Nitekim, kişisel verilerin işlenmesi ile elde edilmek istenen amaca varılması, kişisel verilerin doğru ve güncel olmalarını da gerekli kılmaktadır.[477] Ayrıca, kişisel verilerin doğru bir şekilde tutulması, kişilerin ekonomik çıkarlarını, temel hak ve özgürlüklerini ve manevi bütünlüğünü koruyabilmeleri yönünden de zorunludur. Aksi durumda, kişilerin bu hak ve menfaatlerinin zarar görmesi söz konusu olabilir.[478]

---

471 Özdemir, H., a.g.m., s. 145.
472 Özdemir, H., a.g.m., s. 145.
473 Özdemir, H., a.g.m., s. 145.
474 Kılınç, a.g.m., s. 1126.
475 Şimşek, a.g.e., s. 84.
476 Başalp, a.g.e., s. 38.
477 Özdemir, H., a.g.m., s. 138.
478 Küzeci, a.g.e., s. 208.

2.2.2. USULE İLİŞKİN İLKELER

2.2.2.1. Veri Güvenliği İlkesi

Verilerin güvenliği ilkesi, doğması muhtemel tehlikeler karşısında kişisel verilerin güvenliğini sağlamak suretiyle temel haklardan birisi olan kişisel verilerin korunmasını isteme hakkı da teminat altına almakta, bu ilke günümüzde modern veri koruma hukukunun temel yapı taşı olarak değerlendirilmektedir.[479]

"Veri güvenliği ilkesi" ile kişisel verilerin korunması için gereken bütün teknik, idari önlemlerin alınmasının sağlanması amaçlanmaktadır.[480] Bu ilke ile bireylerin kişisel verilerinin saklandığı yerlere haksız olarak erişimin önüne geçilmesi için veri işleyicilerine verilerin güvenliğinin sağlanması ödevi yüklenmiştir.[481] Bu ilkeye göre veri işleyicisi, kişisel verilerin, başka kimselerce tedarik edilmemesi, veri sahibinin izni olmaksızın dağıtılmaması, kaybolmaması ve imha edilmemesi gibi durumlara karşı korumaya yönelik tedbirleri almak zorundadır.[482]

"Verilerin güvenliği ilkesi" ile kişisel verilerin korunması hakkında gereken tüm teknik ve idari önlemlerin alınması amaçlanmakta ise de söz konusu ilke, *"kişisel verilerin korunması"* teriminden farklı bir anlam taşımaktadır. *"Kişisel verilerin korunması"* kavramı ile kişisel verilerin işlenmesi esnasında kişilerin haklarının ve hürriyetlerinin korunması ile verilerin işlenmesi amacıyla gerçekleştirilen faaliyetlerin hukuki çerçevesini ifade etmekteyken, *"veri güvenliği ilkesi"* ise, bizzat kişisel verilerin kendisinin korunması için başvurulması gereken idari ve teknik önlemleri ifade etmektedir. Bu ilke, yetkili olmayan kişilerin verilere erişim sağlaması, verilerin kaybolması, yetkili olmayan kişilerin verileri değiştirmesi veya alenileştirmesi, verilerin tesadüfen değiştirilmesi veya alenileştirilmesi gibi risklere karşı, "*haber verme yükümlülüğü*", "*veri sırrının korunması*", "*veri koruma görevlisine başvuru*"

479 Şimşek, a.g.e., s. 95.

480 Şimşek, a.g.e., s. 95.

481 Akgül, "Kişisel veri", s. 146.

482 Ayözger, a.g.e., s. 130.

gibi gerekli koruma tedbirlerinin alınması suretiyle kişisel verilerin korunmasını sağlamaya çalışmaktadır.[483]

OECD tarafından hazırlanan Rehber İlkelerin 11. m.'sinde "*elverişli (makul) koruma önlemleri*"ne yer verilmişken, 108 sayılı Sözleşme'nin 7. maddesinde "*uygun koruma önlemleri*" ifadesini kullanmış ise de tüm bu ifadeler ile kastedilen, kişisel verilerin en iyi şekilde korunmasının sağlanmasıdır.[484]

2.2.1.2. İlgili Kişilerin Bilgilendirilmesi İlkesi

Bilgi alma hakkının veya bilgi verme yükümlülüğüne yer verilen en önemli alan, bireylere ilişkin, bireylerin isimlerine bağlı ve otomatik şekilde işleme tabi tutulan kişisel bilgilerdir. Son zamanlarda hem kamuda hem de özel kesimde bilgisayarlar aracılığı ile kişisel veriler tutulup işlenmektedir. Bunun yanında, otomatik işleme yapılan veri ya da bilgiler kullanılmak suretiyle yeni bilgiler elde edilmekte ve değerlendirmeler yapılabilmektedir. Kişilerden habersizce yapılan bu işlemler yüzünden kişilerin özgürlükleri tehdit altında kalmaktadır.[485]

Kişisel verilerin hukuka uygun ve belirli bir amaçla işlenmesi, kişisel verileri işleyicilerinin, kişisel verilerin işlenmesi ve toplanması amacının bu verilerin öznesine bildirilmesini gerekli kılmaktadır.[486] Nitekim, kişisel verilerin işlenmesi sırasında kişisel veri ilgilisinin düzenli bir şekilde ve kapsamlı olarak bilgilendirilmesi, bir yandan da verilerin işlenmesinde uyulması gereken *"dürüstlük kuralı"*nın da bir gerekliliğidir. Bu ilkenin gerekleri yerine getirildiğinde, hakkında veri toplandığını bilen kişi, davranışlarını akılcı bir şekilde biçimlendirebilecektir.[487]

---

483 Şimşek, a.g.e., s. 95.

484 Akgül, "Kişisel veri", s. 147.

485 Akıllıoğlu, Tekin,"Yönetimde Açıklık- Gizlilik ve Bilgi Alma Hakkı", AÜSBF Dergisi, Ankara 1991, S. 3-4, C.46, s. 2.

486 Room, a.g.e., s. 23

487 Şimşek, a.g.e., s. 88.

Kişisel verilerinin işlenmesine ilişkin olarak veri ilgilisine bilgi verilmesi, kişinin kendisine tanınmış olan haklarını gerçekten kullanabilmesine olanak sağlayacaktır.[488]

"Veri sahibinin bilgilendirilmesi ilkesi" diğer yandan hukuk devletinde, kamu kurumlarının kişisel veri işlemeleriyle ilgili işlem ve faaliyetlerinde açık ve şeffaf olmasını sağlayacaktır.[489] Bu ilke gereğince, somut durumun tüm özellikleri göz önünde bulundurularak, kişisel verilerin işlenmesi esnasında verinin toplanması, işlenmesi, kullanılmasında güdülen amaç ve rıza verilmemesi halinde bunun sonuçları hakkında veri ile ilgili kişiye gerekli bilgiler verilmelidir.[490]

Kişisel verileri işleyecek kurum veya özel kişiler, kişisel verileri işlenecek ilgili kişiye, kişisel verilerin işlenmesi süreci hakkında, yani kişisel verilerin hangi amaç uğrunda toplandığı, depolandığı veya aktarıldığı ile ilgili olan gerekli bilgileri vermek yükümlülüğü altındadır.[491] İlgili kişinin, bu şekilde bilgilendirilmesi ile veri sahibi hem kendini baskı altında hissetmeden hür iradesi ile kişisel verileri hakkında karar verebilecek hem de kendisine ait olan bir veri ile ilgili işlem yapılıp yapılmadığını öğrenip, var olan kişisel verilerinin doğru ve güncel olmasını sağlama fırsatı bulacaktır. Veri sahibi kişiler, kişisel verilerinin işlenme şekli, verileri işleyen kişinin kimliği, verilerin işlenme amacı ve işlemenin ne kadar devam edeceği hakkında veri işleyenler tarafından bilgilendirilirler. Kişisel veriler işlenmeden önce veri sahiplerine verilecek bilgilerin eksiksiz olması gerekir. *"Veri sahiplerinin bilgilendirilmesi ilkesi"* ile ilgili kişilere getirilen bilgilendirme yükümlülüğü aracılığıyla veri sahipleri, kişisel verilerin işlenme aşamalarından haberdar olarak, kişisel verilerinin ihlal edilmesi durumunda kullanabilecekleri hukuki güvenceleri devreye sokabildikleri için, bu ilke kişisel verilerin korunması konusunda veri sahiplerine önemli bir yasal güvence

488 Küzeci, a.g.e., s. 212.

489 Şimşek, a.g.e., s. 88.

490 Şimşek, a.g.e., s. 89.

491 Akgül, "Kişisel Veri", s. 141.

sağlamaktadır. Bu yüzdendir ki, *"veri sahiplerinin bilgilendirilmesi hakkı"*, kişisel veri hukukunun "*Magna Carta*"sı olarak kabul edilebilir.[492]

Veri sahibinin bilgilendirilmesi ilkesi, 95/46/AT sayılı Yönerge m. 12'de "*veri öznelerinin verilere erişim hakkı"* başlığı altında yer almışken, GDPR m. 14'te *"veri sahibinin bilgilendirilmesi"* madde kenar başlığı altında yer almıştır. GDPR m. 14'te veri sahibinin bilgilendirilmesi gereken asgari konular belirlenmiş; *"denetleyicinin(sorumlunun) veya varsa temsilcisinin kimliği ve iletişim bilgileri"*, *"soruların yanıtlarının zorunlu veya gönüllü olup olmaması", "üçüncü kişilere ya da yurt dışına aktarım yapılması"*, *"veri otoritesine şikâyette bulunma hakkı ve veri otoritesinin iletişim bilgilerine yer verilmesi"*, *"veri işlenmesinde amaç, verilerin saklanma süreleri, veri sahibinin sahip olduğu haklar"*, *"kişisel verilerin alıcıları"*, *"veri sahibinden sağlanan verilerde yanıt vermemenin muhtemel sonuçları"*, *"veri sahibinden elde edilmesi mümkün olmayan verilerde verinin kaynağı"* ve *"toplama amacına uygun adil veri işleme konusunda verilmesi gereken diğer bilgiler"* bu konular arasında sayılmıştır. GDPR 15. m.' de bu konularda verilerin ait olduğu kişinin veriye erişim hakkı olduğuna yer verilmiştir. Bu düzenlemeler doğrultusunda KVKK m. 10'da da veri sorumlusuna, veri sahibini aydınlatma ödevi yüklenmiş, veri sorumlusunun veya temsilcisinin kimliği, verilerin kimlere ve neden aktarılacağı, veri işleme amacı, kişisel veri toplama yöntem ve hukuki sebebi bu kapsamda kabul edilmiştir.

2.2.1.3. Bilgi Edinme, Kişisel Verinin Düzeltilmesi ve Kaldırılması, Kişisel Veriyi Sildirme, Engelleme ve İtiraz Haklarının Garanti Edilmesi İlkesi

2.2.1.3. 1. Bilgi edinme hakkı:

"Bilgi edinme hakkı", kamu idaresinin eylem ve işlemleri, tutum ve davranışları konusunda bireylerin bilgi edinme istek ve ihtiyacından doğan, idarenin hukuk alanında tek taraflı irade beyanı ile gerçekleştireceği değişikliklere ilişkin ilgili

492 Marie, Tinnefeld, /Eugen Ehmann/ Rainer W. Gerling, "Einführung in das Datenschutzrecht", München, 2005, s. 413. (aktaran Ayözger, a.g.e., s. 133 vd.)

kişilerin, söz konusu işlemin niteliği ve doğuracak sonuçlar konusunda bilgilenmesine yarayan hak ve özgürlüktür.[493]

Veri sahibine veri işleme faaliyetleri hakkında bilgi verilmesi kamu kurumlarının bir sorumluluğu olduğu gibi, kişisel verilerinin işlenmesi ile ilgili veri sahibinin bilgi alması veri sahibine tanınmış bir hak olmakla beraber, bu iki husus birbirini tamamlayıcı olup birlikte ele alınmalıdırlar. Nitekim, veri işleme sorumlusu tarafından veri sahibi bilgilendirilmezse, veri sahibinin, hiç bilgi sahibi olmadığı bir kişisel veri işleme faaliyetine dair bilgi alma, engel olma, silinmesini sağlama, düzeltilmesini isteme gibi haklarını kullanması söz konusu olamayacaktır.[494] İlgili kişinin kişisel verilerine erişim hakkı, kendisine ait verilerin doğru olup olmadığını denetleme, bu verilerde eksiklik ve yanlışlıklarsa onları düzeltmesi *"sildirme ve engelleme hakkı"*nın doğal bir sonucudur.[495]

Kişinin kendisine ait olup işlenen verileri ile ilgili bilgi alma hakkının kapsamında asgari olarak; veri sorumlusu kişiden herhangi bir ücret ödemeden, engellemeye maruz kalmadan ve mümkün olan en kısa sürede, kendisiyle ilgili herhangi bir kişisel verinin toplanıp toplanmadığını öğrenme, kendisine ait verilerin hangi amaçla işlendiğini bilme, işleme faaliyetinin konusu olan kişisel verilerin hangi kategoride yer aldığını bilme, veri transferinin yapılacağı kişileri veya alıcı kategorileriyle kişisel verilerin kökeni hakkında bilgi edinme gibi haklar girmektedir.[496]

Veri sahibinin kendi ile ilgili olup işlenen kişisel verilere erişim hakkı vardır. Pek çok uluslararası metinlerrde de veri sahibine bu hak tanınmıştır. 108 sayılı sözleşmesinin 8. m.'sinde, 95/46/AT sayılı Yönerge m. 12'de, OECD tarafından hazırlanan Rehber İlkeleri m. 13-14'te *"bilgiye erişim hakkı"*na dair kurallar yer almaktadır. 95/46/AT sayılı Yönerge m. 12'de veri sahibinin, kişisel verilerine engellenmeden, serbest bir şekilde erişebileceği, verileri hakkında uygun periyotlarda

493 Yıldırım, Ramazan, "İdare Hukuku Açısından Bilgi Edinme Hak ve Özgürlüğü", İdari Usul Kanunu Hazırlığı Uluslararası Sempozyumu, Bildiriler, Ankara, 17-18 Ocak 1998, s. 227.

494 Şimşek, a.g.e., s. 90.

495 Küzeci, a.g.e., s. 216.

496 Şimşek, a.g.e., s. 91.

bilgi alabileceği, verilerini bir kere öğrendiğinde bilgi edinme hakkını tüketmeyeceği hüküm altına alınmıştır. Hatta, bu kişisel verilerde herhangi bir değişiklik söz konusu olmasa bile bilgi alabileceği benimsenerek tüm yönleriyle bir koruma sağlanması hedeflenmiştir. Bu kapsamda bekleme süresi sübjektif veya objektif şartlara bağlı olarak farklılık gösterebilecekse de *"bilgi edinme hakkı"*nın elverişli aralıklarla yerine getirilmesi yeterli olacaktır.[497]

Bilgi edinme hizmetinin ücretsiz yapılması zorunluluğu bulunmamakla beraber, üye ülkeler bilgi edinme hakkı için istenecek ücrette üst sınır belirleyebilir veya işlem ücreti adı altında ya da bunu aşan ek bir ücret talep edebilirler. Bunun yanında, talep eden hakkında veri toplanmıyor olsa bile, kendisi hakkında veri toplanmadığına dair bir belgeyi veri işleme sorumlularından talep edebilir.[498]

OECD Rehber İlkeleri'nin 13. m.'sinde, veri ilgilisinin, verilerden sorumlu olan kişi veya kurumdan kendisi ile ilgili veri toplanıp toplanmadığına dair bilgi alma hakkının bulunduğu ifade edilmiştir. Bireyin, kendisi ile ilgili verileri, uygun bir süre içinde, ücret alınmadan ya da uygun bir ücretle, kendisinin kavrayabileceği tarzda öğrenmesi bireye tanınmış bir haktır.[499]

İç hukukta BEHK (Bilgi Edinme Hakkı Kanunu)[500] çerçevesinde, kişilerin kendi haklarındaki kişisel verileri öğrenme hakkı tanınmış ise de bu kanunun verilerin korunması anlamındaki işlevi sınırlıdır. Zira, bu kanun verilerin korunmasına yönelik temel ilkeler ve ilgilinin haklarına dair düzenlemeler içermemektedir, nitekim bu düzenleme kişisel verilerin korunması hukuku kapsamında özel bir kanun olarak da nitelendirilemez.[501]

---

497 Başalp, a.g.e., s. 48.

498 Başalp, a.g.e., s. 49.

499 Şimşek, a.g.e., s. 91.

500 24/10/2003 tarih ve 4982 sayılı Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4982.pdf, Erişim tarihi, 05.01.2019.

501 Şimşek, a.g.e., s. 91.

2.2.1.3. 2. Düzeltme, Sildirme, Engelleme ve İtiraz Etme Hakkı

95/46/AT sayılı Yönergenin madde 12'deki düzenlemelere göre, kişisel verilerin hatalı olmaları ya da tam olmamaları halinde veri sahibinin bunları "*düzeltme", "sildirme", "engelleme"* ve bunlara *"itiraz hakkı"* vardır.

Veri işleme faaliyetleri sonucunda bir yanlışlık söz konusu olmuş ise, veri işleyenler bunu ilgili kişilere bildirme yükümlüğü altındadırlar.[502] Bununla birlikte, eğer veri öznesi, veri işleyicisince bilgilendirilmemesine rağmen bir şekilde bu yanlışlığı öğrense dahi, söz konusu bu hakkı kullanabilecektir.[503]

Kişilerin, devlet tarafından kendileri hakkında toplanan kişisel verileri öğrenme ve varsa bunlardaki yanlışları düzeltme imkânının olması, bireylerin güvenlik ve özgürlükleriyle doğrudan bağlantılıdır.[504]

"Düzeltme hakkı", hatalı veya eksik olan kişisel verilerin söz konusu olması karşısında veri ilgilisi tarafından kullanılabilecek bir haktır. Bununla birlikte, kişisel verilerin doğruluğunu yitirmiş veya eskimiş olmaları halinde, düzeltmeyi ilgili kişiler bizzat yapabilirler. Veri transferinin üçüncü kişilere yapıldığı hallerde, üçüncü kişiler söz konusu bu düzeltmelerden haberdar edilmelidirler.[505]

Yanlış bilgilerin düzeltilmesi gibi eksik bilgilerin tamamlanması da verilerin düzeltilmesi hakkı kapsamındadır.[506]

"Sildirme hakkı", veri sahibinin hukuk kurallarına aykırı bir şekilde toplanmış veya belli ve meşru bir amaç için toplandıktan sonra gereksiz hale gelen kişisel verilerinin ortadan kaldırılmasını ilgili kişilerin talep edebilmesi hakkıdır. Sildirme hakkı, veri işleyen kişilerin kişisel veriler üzerinde tasarrufta bulunabilmesine engel olarak, kişisel verilerin veri işleyenlerin hâkimiyet sahasından çıkmasını sağlamaktadır.[507]

---

502 Akgül, "Kişisel Veri", s. 143.

503 Akgül, "Kişisel Veri", s. 143.

504 Döner, "Şeffaf Devlet", s. 101.

505 Şimşek, a.g.e., s. 93.

506 Başalp, a.g.e., s. 50.

507 Şimşek, a.g.e., s. 93.

Sildirme hakkı, GDPR m. 17'de, veri öznesinin gösterdiği rıza ile işlenen verinin toplama amacının gerçekleşmiş olması nedeni ile daha fazla tutulmasına gerek olmaması veya veri sahibinin işlemden önce göstermiş olduğu rızasını geri alması ya da kişisel veri işlemlerine itiraz etmesi durumunda faydalanılabilecek bir temel hak olarak yer almıştır.

Silme işlemi ise, kişisel verilerin ortadan kaldırılmasıdır. Silme, kayıtlı bilgilerin bilgisayar ortamından silinmesi şeklinde yapılabileceği gibi, verinin karalanması, altının çizilmesi ve kişisel verilerin okunmasını olanaksızlaştıracak cisimlerle örtülmesi suretiyle gerçekleştirilebilir.[508] Silme işlemi ile kişisel veriler, veri sorumlusunun hâkimiyet alanından çıkarlar.[509]

"Engelleme hakkı", doğruluğu tartışmalı olan, doğru veya yanlış olduğu hususu tam olarak tespit edilemeyen durumlarda, kişisel verilerin kullanılmasına engel olunabilen bir haktır.[510] Söz konusu bu belirsizlik giderilene dek kişisel verilerin kullanılmasını önlemek amacını taşıyan, kişisel verilerin korunmasını sağlamaya yönelik önemli bir tedbirdir.[511]

"İtiraz hakkı", kamu görevi ifa edilirken veya üstün menfaatlerin korunması için kişisel verileri işlenen bireylerin, hukuk kurallarına uymayan faaliyet ve işlemlerden dolayı veri işleme işlemlerine itiraz etmelerini sağlayan haktır.[512] Veri sahibine bazı hallerde veri işlemlerine itiraz etme hakkı sadece 95/46/AT sayılı Yönergede düzenlenmiş bir hak olup, bu hak veri korumaya dair olan diğer uluslararası temel metinlerinde düzenlenmemiştir.[513]

2.2.1.4. İşlem Aleniyeti

Tarihsel süreç incelendiğinde, gizlilik ve kapalılığın hemen hemen bütün devletlerde devletin idari ve siyasi yönlerine hâkim olan bir yönetim politikası olduğu

508 Özdemir, H., a.g.m., s. 137.
509 Başalp, a.g.e., s. 50.
510 Akgül, "Kişisel veri", s. 144.
511 Şimşek, a.g.e., s. 94.
512 Akgül, "Kişisel veri", s. 145.
513 Küzeci, a.g.e., s. 216.

görülmektedir. Devletin elinde bulunan belge, bilgi ve diğer verilerin açıklanmaması "*gizlilik"* olarak tanımlanırken, "*kapalılık"* ise, devletin işlem ve eylemlerinin büyük kısmının dışarıdan görülememesi ve verdiği kararların gerekçelerini açıklamamasıdır.[514]

Ancak, günümüzde açıklığın ve şeffaflığın öneminin arttığı görülmektedir. Yönetimde şeffaflığın gerçekleşmesi sürecine, maliyet ve zamandan tasarruf edilmesine yarayan teknolojik gelişmeler, olumlu katkı sağlamışlardır.[515] "*Açıklık"*, devletin elindeki bütün bilgi ve belgeleri ilgilinin niteliğinden bağımsız olarak herkesin talep edebilmesi,[516] bütün belge ve bilgilerin isteyen tüm kişilere verilmesi, hatta sınırları aşan bilgi alışverişinin hukuki engellere takılmadan yapılması, idari yönetimin herkes tarafından görülebilmesi anlamına gelmekte olup, yönetilen yerlerin gezilebilmesi[517] dosyaların açık tutulup, isteyenlerin incelenmesine ve görmesine olanak tanınması,[518] açıklık kapsamına girmektedir.

İdari kararlar alma sürecinde, görünenden başka sebeplerle ve yasalarla düzenlenen yöntem kurallarını hiçe sayarak karar almasını, hukuk kuralları ile belirlenmiş sınırlar içinde serbest hareket etme imkânı olan mercilerin keyfi biçimde uygulamada bulunması yönetimin açık olması ile önlenir.[519] Açıklığın belge ve bilgilerde genel kural olarak benimsenmesinin pek çok faydası vardır. Bireyin korunması bu faydaların en başında gelmektedir. Kendisi ile ilgili yapılan bir işlemden veya işlenen bir veriden bireyin bilgi edinebilmesi, haklarını kullanabilmesi bakımından önemli bir şart olduğu gibi, kamu idaresinin şeffaf olması aynı zamanda, idarenin kişilerle iletişime geçmesini gerektirmesi nedeni ile de önemlidir. Almış olduğu kararların gerekçelerini açıklaması bireylerle iletişim kurmayı kabul eden yönetimden beklenebilir.[520]

---

514 Döner, "Şeffaf Devlet", s. 1.

515 Şengül, Ramazan, "Bilişim Çağında Şeffaf Yönetim", Ankara, 2008, s. 24.

516 Döner, "Şeffaf Devlet", s. 20.

517 Akıllıoğlu, "Bilgi Alma Hakkı", s. 9.

518 Döner, "Şeffaf Devlet", s. 20.

519 Çolak, N. İlker, "Kitle İletişim Hukuku", 2. Baskı, İstanbul, 2010, s. 12

520 Şengül, a.g.e., s. 34.

Öteki taraftan, aslında, idareyi her zaman tüm işlemlerinin gerekçeli olmasına zorlamak ne olanaklı ne de yararlı olabilir. Zira, işaretle veya sözlü olarak açıklanan kararlarda ve üstü kapalı bir şekilde ortaya konan kabul veya ret iradelerinde, idare zaten gerekçe sunmamaktadır. Bunun gibi, çoğu zaman, olağan dışı veya acil durumlarda yetkili ve görevlilerin aldıkları kararların gerekçeli olması beklenmez ve istenmez. Bununla birlikte, tüm bu durumlarda dahi ilgililerin kararların uygulanmasından sonra, bu işlemlerin nedenlerini öğrenme hakkı vardır. Gizli ve saklı kalmasının gerekli görüldüğü veya açıklanmasının zararlı olacağı kabul edilen bir "*devlet sırrı*", "*meslek sırrı*" veya "*kişilerin özel hayatı"* veya "*ticari ve mali itibarı"* ile alakalı gizli kalması gereken durumların varlığı halinde, bu kapsamdaki nedenler kararda ve bazı durumlarda yargı önünde dahi gösterilmeyebilirler.[521]

BEHK ile iç hukukumuzda, idareye başvuruda bulunarak kendileri hakkında tesis edilen işlemlerin sebebini öğrenme hakkı ilgililere tanınmışken, idareye ise, başvuruda bulunan ile ilgili işlemin sebebini bu kişiye bildirme ödevi yüklenmiştir.[522]

Yönetimde şeffaflığı destekleyen teknolojik gelişmelerden bir diğeri elektronik iletişimin gündelik yaşamda ulaştığı noktadır. Yani, internet kullanımının gelişip yaygınlaşması sayesinde, idareden bilgi ve belge istenmesi kolaylaşırken, iletişim sürecinin ise kısaldığını söylemek mümkündür. Bireyler, elektronik posta aracılığıyla kamu kurum ve kuruluşlarına oldukça hızlı ve kolay bir şekilde bilgi istemlerini iletebilip aynı şekilde cevap da alabilmektedirler.[523]

AB'de şeffaflık en güçlü anlayışlardan birisi olduğundan, kişisel veriler hakkında yapılan işlemlerde, işlemlerinin kamuoyuna açıklığını gerçekleştirebilecek önlemleri üye devletlerin almaları zorunludur.[524] Veri işlemleri ile ilgili bir *sicil* tutulması suretiyle veri işlem açıklığı sağlanmaktadır. Zira 95/46/AT sayılı Yönergenin 21. m.'sinde, üye devletlere veri işlemlerinin açıklığı ilkesini sağlaması

---

521 Duran, Lütfi, "İdari Usulün İlkeleri ve Kapsadığı Konular", İdari Usul Kanunu Hazırlığı Uluslararası Sempozyumu, Bildiriler, Ankara, 1998, s. 8.

522 Çokmutlu, a.g.e., s. 162.

523 Şengül, a.g.e., s. 25

524 Başalp, a.g.e., s. 63

için bir sicil tutulması zorunluluğu getirilmiştir.[525] Ancak, herkese açık olan bu sicile kaydedilen bilgiler veri işlemlerinin konusunu teşkil eden kişisel verileri birebir göstermemektedir. Çünkü bu 21. m. gereğince oluşturulacak söz konusu bu sicil ile kişisel verilerin hangi amaçla işlendiği, işleme faaliyetinden sorumlu olanların kimler olduğu ve hangi kategorideki kişisel verilerin işleme konu olduğuna dair ilgililerin bilgilendirilmesi istenmiştir. Bilgilendirmenin konusuna girmeyen işlemler yönünden ise açıklık söz konusu olmayacağı için, sorumlular tarafından gereken önlemin alınması üye devletler tarafından sağlanmalıdır.[526]

Kişisel veriler ile ilgili olan uygulama, düzenleme ve politikaların bilinebilir olması açıklık ilkesi olarak adlandırılır. Açıklık ilkesi, kişisel veriler ile ilgili işlemlerin şeffaf bir şekilde yapılmasına yardım etmektedir. Bireyin kişisel veriler ile ilgili tutulan sicile ulaşabilmesi, kendi kişisel verilerinin tutulup tutulmadığı, işlenip işlenmediği konusunda bilgi sahibi olması ve bu hususstaki haklarını kullanabilmesi açısından önemlidir. Veri işlem sorumlusu, isteği üzerine kendisine ait verilerin tutulduğu sicile bireyin erişimini sağlama yükümlülüğü altındadır.[527]

2.2.1.5. İşlemin Gizliliği ve Güvenliği

Kişisel veriler hakkındaki bütün işlemler, bu işlemlerin gizli olması zorunluluğu nedeni ile koruma altındadır. Kişisel veri işlem sorumlusu ve onun sorumluluğunda çalışan kişilerden, kişisel verilere erişebilecek konumda olanlar, kişisel verileri bundan sorumlu olanın yönetimi altında ve onun talimatlarına uygun bir şekilde işlemelidirler. İç hukuk kurallarına göre bilgi verme zorunluluğu olan sorumlu ve onunla çalışanların işlem gizliliğine tabi olmaması bu kuralın istisnasıdır. Örnek vermek gerekirse, bir ceza kovuşturmasında çalışanların bilgi verme yükümlülüğü var ise bu kapsamda bilgi verilmesi halinde işlem gizliliği ilkesinin ihlali söz konusu olmayacaktır.[528]

525 Şimşek, a.g.e., s. 100.

526 Başalp, a.g.e., s. 63.

527 Şimşek, a.g.e., s. 100-101.

528 Başalp, a.g.e., s. 55.

95/46/AT sayılı Yönergenin 17. m.'sinin 1. fıkrasında işlem güvenliği gereği her türlü hukuka aykırı müdahaleye karşı alınması gereken yönetimsel ve teknik tedbirler düzenlenmiştir. Bu kapsamda alınacak önlemler, kişisel verilerin işlendiği sistem ve araçların bulunduğu yerler hakkında koruyucu özelliği olan ve uygun tedbirlerdir. Bu önlemlere verilerin şifreli bir şekilde aktarılması örnek olarak gösterilebilir.[529]

Bu hususa ilişkin Kamu Denetçiliği Kurumu'nun 03/12/2014 tarihli ve 2014/2832 sayılı tavsiye kararında, hakkında beraat kararına hükmolunan bir kişinin Ulusal Yargı Ağı Bilişim Sisteminde (UYAP), yargılamaya ilişkin tüm verilerin sistemden silinmesi gerektiğini, ayrıca 3. kişilerin bu verilere ulaşamaması gerektiğini, buna ilişkin idari ve teknik önlemlerin alınması hususlarında tavsiyede bulunduğu görülmektedir.[530]

2.2.1.6. Ön Denetim

95/46/AT sayılı Yönergenin 20. m.'sinde "*spesifik risk taşıyan işlemler"* yönünden üye devletlere "*ön denetimde bulunma"* görevi yüklenmiş, böylece, özel risk taşıyan işlem türlerinin mümkün olduğunca sınırlı tutulması sağlanmaya çalışılmıştır. Bununla birlikte, 20. m.'de spesifik risk taşıyan işlemlerin hangisi olduğu belirtilmemiş, özellik arz eden işlemlerin hangileri olduğunun belirlenmesi üye devletlerin görevi olarak kabul edilmiştir. Bu yolla, üye devletlere spesifik risk taşıyan işlemleri belirlemede geniş bir hareket alanı bırakılmıştır.[531]

95/46/AT sayılı Yönergeye göre ön denetim, kontrol birimi ya da onunla iş birliği içinde veri koruma görevlisi tarafından yerine getirilmelidir. Ön denetim yapılırken, veri koruma ilkeleri dikkate alınmak suretiyle kişilik hakkının ihlal edilmesi tehlikesinin bulunup bulunmadığı kontrol edilmelidir. Ön denetim sonucunda kontrol birimi tarafından görüş bildirilebilir veya işleme izin verilebilir.[532]

529 Başalp, a.g.e., s. 56.

530 https://www.ombudsman.gov.tr/contents/files/pdf/2014-2832.pdf, Erişim Tarihi: 01.12.2019

531 Başalp, a.g.e., s. 61-62.

532 Başalp, a.g.e., s. 63.

GDPR m. 36'da bu *husus "...bir veri koruma etki değerlendirmesi sonucunda kontrolör tarafından riskin azaltılması hususunda alınan tedbirlerin olmaması durumunda işleme faaliyetinin yüksek bir riske sebebiyet vereceğinin görüldüğü hallerde, kontrolör işleme faaliyetinden önce denetim makamına danışır."* şeklinde belirtilmiştir.

KVKK'da ise bu hususta özel bir düzenleme bulunmamaktadır.

2.2.1.7. Zararın Giderilmesi İlkesi

Kişisel veri sahipleri, verilerinin hukuka aykırı şekilde izin alınmadan, doğru olmadan veya geçersiz şekilde işlenmiş olması halinde, kişisel verileri işlemekle görevlendirilmiş gerçek veya tüzel kişilerden zararlarının tazmin edilmesini isteyebilirler.[533]

95/46/AT sayılı Yönergenin 55 no'lu gerekçesinde, denetleyicinin ilgili kişinin haklarını gözetmemesi halinde ulusal yargı yolunun sağlanması gerektiği ve hukuka aykırı veri işlemesi nedeni ile veri sahibinin bir zarara uğraması halinde bu zararın denetleyici -sorumlu- tarafından giderilmesi gerektiği, ancak denetleyicinin mücbir sebep veya hatanın veri sahibinden kaynaklanması, zararda denetleyicinin kusurunun bulunmamasının kanıtlanması halinde denetleyicinin zarardan sorumlu tutulamayacağı düzenlenmiştir. Ayrıca 95/46/AT sayılı Yönerge m. 23'te ve GDPR m. 78'de benzer şekilde veri işleyicilerinin ve denetleyicilerinin neden oldukları zararlara karşı etkili bir hukuksal güvence sağlanması hakkı, m. 82'de ise zararın giderilmesini talep hakkı yer almıştır.

Üye devletlere 95/46/AT sayılı Yönergenin 22. m.'si ile, kişisel veri işlemlerine karşı etkin bir hak arama yolu düzenleyerek kişilik haklarının korunması ödevi yüklenmiştir. Yönergeye göre kişisel verileri işlenen kişilerin, kontrol birimine başvurabilmelerinin sağlanmasının yanında ayrıca mahkemeye de başvurabilmelerinin sağlanması üye devletler tarafından teminat altına alınmalıdır. Üye devletler, öncelikli olarak kontrol birimine başvurulmasının zorunlu olup olmadığı konusunda yani usul

533 Şimşek, a.g.e., s. 109.

konusunda serbest bırakılmıştır.[534] Bunun yanında, veri ilgilisi tarafından dava yoluna başvurulabilmesi için, ihlale uğradığı iddia edilen hak, üye devletlerin ulusal düzenlemelerinde tanınmış haklar arasında yer almalıdır. Yönergenin 23. m.'sinde zararın giderilmesi düzenlenmektedir ancak, madde metninde maddi zarar ile birlikte manevi zararın yer alıp almadığına dair bir açıklık bulunmadığından, bu hususta üye devletlerin serbest bırakıldığı ifade edilmektedir.[535]

Bu maddeler kapsamında sorumluluğun doğması için; hukuka aykırı olarak kişisel verilerin işlenmesi, bu hukuka aykırı işleme yüzünden bir zararın meydana gelmiş olması, söz konusu zararın doğmasına hukuka aykırı işlemin sebep olmuş olması gerekmektedir.[536]

KVKK m. 11/ğ'de bireylere ait verilerin hukuka aykırı şekilde işlenmesi gerekçesiyle ortaya bir zararın çıkması durumunda, verilen zararın tazminini talep yetkisine ilişkin özel bir düzenleme getirilmiştir. Bu maddeyle veri sahibinin -ilgili kişinin- hukuka aykırı olarak verilerinin işlenmesinden kaynaklanan zararlarının tazminini talep edebilmesi hakkı açıkça düzenlenmiştir. Kanaatimizce buradaki düzenleme özel bir düzenleme niteliğinde olup ilgili kişiye kanuni bir hak tanımasından dolayı olumlu mütalaa edilmelidir. Yine belirtmek gerekir ki bu hak özel nitelikte olan bu kanunda tanınmamış olsaydı bile, normlar hiyerarşisinde en üst norm olan 1982 Anayasasının 20. m.'si ve genel bir düzenleme niteliğinde olan TBK'nın 49. m.'si ile TMK'nın 24. ve 25. m.'leri gereği maddi ve manevi tazminat davası açabilecektir.

534 Başalp, a.g.e., s. 64.

535 Başalp, a.g.e., s. 64.

536 Başalp, a.g.e., s. 65.

ÜÇÜNCÜ BÖLÜM

ANAYASA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASININ TEMELLERİ

Başta devlet olmak üzere, kamu hizmetlerinin yerine getirilebilmesi, bu hizmetlerin verimliliğinin artırılması, sosyal devlet ilkesinin gerektirdiği faaliyetlerde bulunulabilmesi ve yasalarda belirtilen diğer bazı iş ve işlemleri yapmak için kişisel verilerin işlenmesi bir zorunluluktur.[537] Böyle bir zorunluluğun söz konusu olduğu bir durumda, devletin anayasal alan başta olmak üzere gerekli yasal düzenlemeleri yapması hukuk devleti açısından kaçınılmazdır. Genellikle özel hayatın gizliliğinin korunması çerçevesinde ele alınan kişisel verilerin korunması hakkı, "özel hayatın gizliliği" başlığı altında 1961 ve 1982 Anayasalarında doğrudan olmasa da dolaylı olarak kendisine yer bulmuştur. Ama bu yer bulma tamamıyla gerek AİHM gerekse AYM'nin bu konuda genişletici yorumları vesilesiyle olmuştur. Yani, esasen, 1961 ve 1982 Anayasalarında, 12 Eylül 2010 tarihinde yapılan referanduma kadar, kişisel verilerin korunması hakkına anayasal bir hak statüsü doğrudan verilmemiştir.[538]

Uluslararası platformda da kişisel verilerin korunmasına yönelik ilk gelişmeler, özel hayatın gizliliği hakkı kapsamında değerlendirilmiş ve özel hayatın gizliliğine dair yapılan düzenlemelerin kişisel verileri de kapsayacağı düşüncesi benimsenmiştir. Kişisel verilerin korunması hakkının doğrudan doğruya ele alınarak bağımsız bir hak olarak tanınması, bilgi-işlem teknolojisinde yaşanan gelişmelere paralel olarak 1970'lerden sonra olmuştur.[539] Uluslararası belgelerde düzenlenmeye başlayan kişisel verilerin korunması hakkı, daha sonra ilerleyen zamanlarda anayasalarda kendine yer bulmaya başlamıştır.

Anayasal hükümler, demokratik hukuk devletlerinde, normlar hiyerarşisi bakımından, her türlü düzenlemenin üstünde yer aldıkları için, her türlü yasal veya

---

537 Şimsek, a.g.e., s. 3.

538 Uygun, Murat, "Avrupa Birliğinin 95/46 sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması", Yayınlanmamış Yüksek Lisans Tezi, Ankara 2010, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, s. 89.

539 Ersoy, "Bir İnsan Hakları Kavramı Olarak... ", s. 49.

idari düzenleme anayasaya uygun olmalı ve hiçbir şekilde anayasaya aykırı bir hüküm içermemelidir. Anayasalarda koruma altına alınan haklara anayasal haklar denilmekte olup, bu haklar yüksek korumaya alınarak, normlar hiyerarşisinde en üst norm olan anayasadan gücünü alan haklardır.[540]

Her bireyin, devlet eliyle yapılan kişisel verilerin, toplanma, depolanma, işlenme faaliyetleri sırasında temel hak ve hürriyetlerinin ihlal edilmemesini isteme hakkı bulunmaktadır. Kişisel verilerin korunması hakkının temel anayasal dayanağını *"özel hayatın gizliliği"* ve *"maddi ve manevi varlığı geliştirme"* hakları oluşturmaktadır. Bununla birlikte diğer temel haklar ise ilişkin oldukları özel hayat ilişkisi kapsamında kişisel veriler için dolaylı şekilde anayasal dayanak oluşturmaktadırlar.[541]

Biz de çalışmamızın bu bölümünde anayasal bir hak olan bireyin kişisel verilerinin korunması hakkının 1982 Anayasasındaki düzenleniş şekli ile kapsam ve sınırlarını incelemeye çalışacağız.

3.1. BİREYİN KİŞİSEL VERİLERİNİN KORUNMASI HAKKI

3.1.1. GENEL OLARAK

Hak kavramı özgürlükleri koruyup kurumsallaştıran, yani bireylere bir şeyleri yapma ya da yapmama konusunda bir baskının bulunmaması şeklinde somut hale gelen bir özgürlüğün hukuki bir kimliğe bürünmesi şeklinde tanımlanabilir.[542] İnsan hakları kavramı ise, kişilerin doğumla birlikte sahip oldukları "*dokunulmaz, devredilmez*" haklar olarak kabul edilmekte, uluslararası belge ve bildirilerde, ulusal anayasalarda temel bir konu olarak nitelendirilmektedir. İnsan hakları kavramı Karel Vasak tarafından 3 sınıfa ayrılarak incelenmiştir. *Birinci kuşak hakları*, siyasal haklar ve kişi özgürlükleri; *ikinci kuşak hakları*, ekonomik, sosyal hak ve özgürlükleri; *üçüncü kuşak hakları* ise, dayanışma hakları oluşturmaktadır. George Jellinek tarafından yapılan diğer bir sınıflandırma da kişi hak ve hürriyetleri "*negatif statü*

---

540 Boz, a.g.e., s. 17.

541 Şimşek, "Kayıt ve Verilerin İncelenmesi", s. 2001.

542 Gemalmaz , M. Semih, "Devlet, Birey ve Özgürlük", İstanbul 2012, 2. Baskı, s. 512.

hakları" olarak nitelendirilmekte olup, kişileri devlete ve toplumdaki diğer kişilere karşı koruyan haklardır. Bu yüzden bu haklara *"koruyucu haklar"* da denilmektedirler. Sosyal ve ekonomik haklar, bireylerin devletten bir şeyler istemesini sağlayan, devlete de vatandaşlarının istekleri doğrultusunda hizmet ve imkân sunma, sağlama gibi olumlu birtakım yükümlülükler yükleyen haklar olduğu için bu haklara "*pozitif statü hakları*" da denmektedir. Sosyal ve ekonomik haklar sayesinde devlet, bireylere sadece özgürlük tanımakla yetinemeyecek, bireylere insan onuruna yakışır bir hayat da sağlamak için gerekli tedbirleri de alacaktır.[543] Kişisel verilerin korunması hakkı ise bu hakların genel çerçevesine ve esasına baktığımızda negatif statü haklarındandır.[544] Keza 1982 Anayasasında kişi hakları ve hürriyetleri başlığı altında düzenlendiği için, kişisel verileri koruma hakkının bir "negatif statü hakkı" olduğunu söylemek de mümkündür.

Demokratik bir hukuk devletinde, kişisel verilerin korunması hakkı, bireyin, kendi hür iradesiyle kendi yaşamını kendisinin organize edebilmesinin bir zorunluluğu olarak kendisini gösterir. Zira, kamusal ve özel organlar tarafından kişisel veriler işlendiğinden, bireyin kişiliğini özgürce geliştirebilmesi, bireyin kişiliğinin korunarak özgür bireylerden teşekkül eden bir toplumsal düzen kurulması, yalnızca bireylerin kişisel verilerine dair haklarının korunmasıyla mümkün olabilecektir.[545] Bunun yanında, kişisel verilerin korunması hakkı sayesinde, bireylerin kişilik haklarının korunmasıyla kamu kurum ve kuruluşlarının veya özel ticari işletmelerin bilgilendirilmesi arasındaki denge de sağlanmış olmaktadır.[546]

Kişisel verilerin korunması hakkı, kişisel verilerin elde edilmesi, kullanılması ve devir işlemlerinde kişinin asıl söz sahibi olmasını gerektirdiğinden, veri sahibinin iradesine aykırı olarak ve yasal bir dayanağı olmadan yürütülen veri işleme çalışmaları, kişisel verilerin korunması hakkının ihlal edilmesi anlamına gelecektir.[547]

---

543 Kaboğlu, İbrahim Ö., "Özgürlükler Hukuku", 6. Baskı, Ankara 2002, s. 28.

544 Kılınç, a.g.m., s. 1198.

545 Şimşek, a.g.e., s. 4.

546 Küzeci, a.g.e., s. 70.

547 Şimşek, a.g.e., s. 112.

Günümüzde kişilik hakları ve insan hakları kavramları zamanla daha fazla önem kazandıkça, bu hakların gelişmesiyle orantılı olarak kişisel verilerin korunması hakkı da daha önemli hale gelmektedir.[548] Kişisel verilerin korunmasını isteme hakkı bir temel hak olarak, hukuka uygunluk nedeni veya kişinin kendisinin rızası bulunmadan kişisel verilere yapılacak müdahalelere karşı kişinin güvence altına alınmasını ve bireyin kişisel verileri üzerinde karar verme hürriyetinin korunmasını hedeflemektedir.[549]

Günümüzde gelinen süreçte, tarihçe kısmında da açıkça belirttiğimiz üzere, devletler veri koruma hukukuna ve kişisel verilerin korunması hakkına ilişkin anayasal düzeyde kendilerini bağlayıcı, bu hakka nasıl ve hangi durumlarda müdahale edilebileceğini ilişkin hükümler koydukları görülmektedir. Dolayısıyla anayasa hukuku anlamında, kişisel verileri koruma hukukunun kaynağını, dayanağını temel hak olarak anayasalarda yer almasından aldığını söylemek yanlış olmayacaktır. Böylelikle başta devlet otoritesi olmak üzere, onu oluşturan yasama, yargı ve yürütme kuvvetlerinin, bu hakka ilişkin yapacakları tasarruflarda anayasal çerçeve çizilmiş olacaktır.

3.1.2. T.C. ANAYASASI'NDAKİ DÜZENLEME

3.1.2.1. Anayasa'nın 20. Maddesindeki Düzenleme

Türkiye Cumhuriyeti Anayasasının[550] ikinci Kısmında *"Temel Haklar ve Ödevler*" başlığı altında[551] kişilere tanınan anayasal haklar düzenlenmiştir. Anayasalarda tanımlanan bu haklara yapılması söz konusu olan müdahalenin sınırları anayasalarda genel anlamda düzenlenmiştir. Kişisel verilerin korunması hakkı da 12

548 Şen, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa...", s. 1199.

549 Şimşek, a.g.e., s. 114.

550 Kanun No: 2709, Kabul Tarihi: 7.11.1982. 1982 Anayasasının en son güncel haline ulaşmak için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf, Erişim tarihi, 03.05.2019.

551 Zira kişisel verilerin korunması alanında kapsayıcı hukuki düzenleme yapması gerekliliğini benimsemiş ülkelerin büyük bir kısmında da aynı durum söz konusudur. Yani, birçok ulusal hukuk düzeninde bu önemli alan, anayasal dayanağını özel hayatın gizliliği hakkından alır. Aksoy, "Personal Data", s. 238); Bu yüzden kişisel verilerin korunması hakkının anayasal temelini, başta "özel yaşamın gizliliği hakkı", "bilgilerin geleceğini belirleme hakkı" olmak üzere, çağdaş ve demokratik anayasalarda koruma altına alınan çeşitli temel hak ve özgürlüklerde bulduğu söylenebilir. Küzeci, a.g.e., s. 261.

Eylül 2010 tarihinde gerçekleştirilen referandumla 1982 Anayasası'nda *"Özel Hayatın Gizliliği ve Korunması"* başlığı altında düzenlenen 20. maddesine eklenen 3. fıkra ile bir anayasal hak haline gelmiştir.

3.1.2.1.1. Anayasanın 20/3. Fıkrasının Eklenmesinden Önce Kişisel Verilerin Korunması

Aslında, kişisel verilerin korunması hakkının temeli olarak kabul edilebilecek anayasal hükümler 2010 yılında yapılan Anayasa değişikliğinden önce de ülkemizde vardı. Zira, 2. maddede düzenlenen *"hukuk devleti ilkesi",* 17. maddede düzenlenen "*bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı"*, 20. maddede yer alan "*özel hayatın gizliliği hakkı"*, 21. maddedeki "*konut dokunulmazlığı"*, 22. maddede ifade edilen "*haberleşmenin gizliliği ilkesi"*, 24. maddede getirilen "*dini ve vicdani kanaat hürriyeti"*, 25. maddede düzenlenen "*düşünce ve kanaat hürriyeti"* gibi hak ve hürriyetleri düzenleyen bu maddeler bunlara örnek olarak verilebilir.[552] Yani, esasen, anayasa değişikliği ile kişisel verilerin korunması hakkına yönelik bir ekleme yapılmasaydı bile bu haklara dayanarak bireylerin anayasadan kaynaklı kişisel verilerinin korunmasını isteyebileceği görülmektedir.

AİHM kararları ile benzer şekilde, AYM de Anayasa'nın 20. m.'sine 3. fıkra eklenmeden önce 2008 yılında verdiği bir kararında kişisel verilerin korunmasını 1982 Anayasası'nın "*özel hayatın gizliliği"* ve "*düşünce ve kanaat hürriyeti"* başlıkları altında düzenlenen 20. ve 25. maddeleri kapsamında yorumlamıştır. 5429 sayılı Türkiye İstatistik Kurumu Kanunu'nun, istatistik birimi tarafından kendisinden istenilen bilgi ve verileri vermekle yükümlü tutularak, bu yükümlülüğe aykırı davrananların para cezası ile cezalandırılmalarına dair 8. m. ve 54/2-b. bendinin iptaline ilişkin verdiği karar bu kapsamdadır.[553] Mahkeme bu kararında; iptali istenen

---

552 Kılınç, a.g.m., s. 1131.

553 AYM'nin, 25 Haziran 2008 T. ve 26917 sayılı R.G. 2006/167 Esas; 2008/86 Karar ve 20.3.2008 tarihli kararı: "*…Başvuru kararında, 5429 sayılı Yasa'da yer alan, istatistiki birimlerin kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz, doğru ve ücretsiz olarak vermekle yükümlü olduklarına ilişkin 8. maddesiyle bu yükümlülüğe uymayanların para cezasıyla cezalandırılacaklarına ilişkin 54. maddesinin ikinci fıkrasının (b) bendi hükümlerinin eşitlik ilkesi, temel hak ve hürriyetlerin niteliği, kişi hürriyeti ve güvenliği, özel hayatın gizliliği, düşünce ve kanaat hürriyetine ilişkin düzenlemelere aykırı olduğu, temel hak ve hürriyetlerin kanunla sınırlanabileceği ve bu sınırlamanın demokratik toplum düzeninin gereklerine aykırı olamayacağı, kişilerin her ne sebeple ve amaçla olursa olsun düşünce ve kanaatlerini açıklamaya zorlanarak yerine getirmeyenlerin cezai ya da idari*

8. m.'de net bir düzenleme olmadığı için kişisel veri olarak nitelendirilebilecek verilerin de bu madde kapsamında talep edilebileceği, bir ülkede en güçlü veri tekelinin idare olduğu, bu maddenin kişileri idare ve diğer kişiler karşısında korumasız bıraktığı, bu haliyle iptali istenen bu hükümlerin Anayasa'nın 20. ve 25. maddelerine aykırı olacağı gerekçesi ile iptaline karar verilmiştir.

Anayasa Mahkemesi bu konu hakkında verdiği önemli bir diğer kararında[554] ise 1774 sayılı Kimlik Bildirme Kanunu'na eklenen bir hükümle, bu yetki

bir yaptırımla karşı karşıya bırakılmasının hukuk devleti ilkesine aykırılık teşkil edeceği düşüncesiyle itiraz konusu kuralların, Anayasa'nın Başlangıç'ı ile 2., 5., 6., 10., 11., 12., 13., 17., 19., 20. ve 25. maddelerine aykırı olduğu ileri sürülmüştür. İstatistik, verilerin toplanması, düzenlenmesi ve uygun yöntemlerle analiz edilerek sonuçların yorumlanmasıdır. İstatistikten söz edebilmek için önce "veri"ye ihtiyaç vardır. Veriler, araştırma yapılacak konu ile ilgili bilinen veya herhangi bir kaynaktan doğrudan ya da dolaylı olarak elde edilen bilgilerdir. Verilerin doğrudan toplanmasında anket, gözlem, deney gibi yöntemlerin kullanıldığı bilinmektedir. Anket en çok kullanılan yöntem olup, bu yöntem de önceden hazırlanan anket formu/formları çeşitli şekillerde veri kaynağına (istatistik birimlerine) ulaştırılmaktadır. 5429 sayılı Yasa'nın 2. maddesinin (h) bendine göre istatistiki birim, yapılan sayım veya örnekleme çalışmalarına konu olan, hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşları ifade etmektedir. İtiraza konu 8. madde hükmüyle sayım ve örnekleme çalışmalarına konu olan, hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşların yetkililerine cevap verme yükümlülüğü getirilmiş, bu yükümlülüğe uymayanların da 54. maddede gösterilen biçimde idari para cezasıyla cezalandırılması öngörülmüştür.

Maddede açıklayıcı bir düzenleme bulunmadığı için, "kişisel veri" veya "isteme bağlı veri" olarak adlandırılan, belirli veya belirlenebilir kişilerle ilgili her türlü bilgilerin istenebileceği kuşkusuzdur. İstatistiki birimlerin kendilerinden istenen bilgileri belirlenen şekil ve sürede eksiksiz ve hatasız olarak vermek zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmış olmasına karşın, istenilecek veri ve bilginin kapsamı ya da sınırlarının ne/neler olacağına, başka bir anlatımla temel hak ve özgürlüklere müdahale niteliğinde olan veri ve bilgilerin bu zorunluluk kapsamında bulunup bulunmadığına ilişkin herhangi bir düzenlemeye rastlanmamaktadır. Dolayısıyla, istatistikî birimler kendilerinden istenildiği takdirde her türlü bilgiyi temel hak ve özgürlüklerine müdahale niteliğinde olsa bile vermek zorundadırlar. Anayasa'nın 20. maddesinde herkesin özel hayatına ve aile yaşayışına saygı gösterilmesini isteme hakkına sahip olduğu; 25. maddesinde de herkesin düşünce ve kanaatlerini açıklama hürriyetine sahip olduğu, her ne sebep ve amaçla olursa olsun kimsenin düşünce ve kanaatlerini açıklamaya zorlanamayacağı hüküm altına alınmıştır. 20. madde gerekçesinde, özel hayatın korunmasının her şeyden önce bu hayatın gizliliğinin korunması, resmi makamların özel hayata müdahale edememesi anlamına geldiği belirtilmiştir. AİHM kararlarında belirtildiği gibi, özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililerin rızası olmaksızın bilgi toplamasının her zaman söz konusu özel hayatını ilgilendireceği kuşkusuzdur. Anket formlarında yer alan bazı sorular özel yaşamın gizliliği ile düşünce ve kanaatin açıklanması sonucunu doğurabilir. Bir ülkede en güçlü veri tekeli idaredir. Bu gücün sınırlandırılması özel yaşamın ve düşünce ve kanaat özgürlüğünün korunması bakımından önemlidir. Anayasa 'nın 20. ve 25. maddelerinde yer alan güvencelere rağmen itiraza konu 8. madde hükmüyle kişiler, bilgi toplama, saklama, işleme ve değiştirme tekeli olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamanın sınırlarına yasal düzenlemede yer verilmemiştir. Açıklanan nedenlerle itiraz konusu kuralların Anayasanın 20. ve 25. maddelerine aykırı olduğundan iptali gerekir...".

554 AYM'nin T. 31.3.1987 ve E: 1986/24, K: 1987/8 sayılı kararı. (RG. 28.5.1987).

kullanılırken uyulacak kurallar belirlenmeden, genel kolluk kuvvetlerinin bilgisayarlarında kişisel bilgilerin depolanması yetkisinin verilmesine ilişkindir. AYM'nin kararda kullandığı ifadeden ve özel hayatın gizliliği hakkına dair yaptığı açıklamalardan kişisel verilerin korunmasının Anayasanın 20. m.'si kapsamında yorumladığı anlaşılmaktadır.[555]

Ayrıca, "*kişisel verilerin korunması hakkı"* sadece "*özel hayatın gizliliği hakkı"* ile ilişkili olmayıp, Anayasada kişisel verileri dolaylı olarak da olsa koruyan başka hükümler de vardır. Anayasanın 17. m.'sinde düzenlenen *"kişinin maddi ve manevi varlığını geliştirme hakkı"* ve *"düşünce ve kanaat hürriyeti"* bu kapsamda değerlendirilebilecek hak ve özgürlüklerdendir. Zira, bazı yazarlar, kişisel verilerin korunması hakkının Anayasa değişikliği ile Anayasal koruma altına alınmadan önce kişisel verilerin korunmasının anayasal dayanağının Anayasanın 17. m.'sindeki *"kişinin maddi ve manevi varlığını geliştirme hakkı"* olduğunu ifade etmişlerdir. [556]

Yine Anayasanın *"temel hak ve hürriyetlerin korunması" başlıklı* 40. m.'sinden bireylerin temel hak ve hürriyetlerinin, daha özelde ise kişisel verilerinin, meşru bir temele dayanmadan işlenmesi gibi hallerde kişilerin birtakım güvencelere sahip olduğu görülmektedir. Anayasa 40/1 m.'sinde, tanınan hak ve hürriyetlerine müdahale edilen kişilerin, geciktirilmeye maruz kalmadan yetkili mercilere müracaat etme imkânının verilmesini talep etme hakkının olduğu, 40/2'de ise devletin işlemleri ile ilgili olan kişilerin hangi kanun yollarına ve makamlara başvurabileceğini ve başvuru sürelerini göstermek mecburiyetinde olduğu düzenlenmiştir.[557] Bu madde kapsamında da, kişisel verilerin korunması hakkının ihlal edildiğini iddia eden kişilerin, bu ihlallerin giderilmesini ilgili kurumlardan talep etme hakkının olduğu gibi yargı yolunu kullanma haklarının olduğu da görülmektedir.

Dolayısıyla anayasal düzeyde kişisel verilerin korunması hakkının, bu hakka ilişkin olarak Anayasa m. 20'ye ekleme yapılmadan önce dahi korunduğunu

555 Küzeci, a.g.e., s. 294.

556 Şimşek, a.g.e., s. 111.

557 Şen, Ersan, "Devlet ve Kitle İletişim Araçları Karşısında Özel Hayatın Gizliliği ve Korunması", İstanbul,1996, Kazancı Yayınevi, s. 70.

görüyoruz. Fakat anayasa değişikliği ile vazıh şekilde bu hakkın temel haklar arasında anayasa koyucu tarafından sayılması hiç şüphesiz dünya hukuk sistemlerine paralel olarak olumlu bir gelişme olarak mütalaa edilmelidir.

3.1.2.1.2. Anayasanın 20/3. Fıkrasının Eklenmesinden Sonra Kişisel Verilerin Korunması

T.C. Anayasası'nın 20. maddesine 2010 yılında yapılan referandumla Kişisel Verilerin Korunmasına ilişkin, "*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 eklenerek kişisel verilerin korunması hakkına anayasal teminat getirilmiştir.

Bu düzenleme ile, kişisel verilerin korunması hakkının sınırlandırılmasında, yapılacak yasal düzenlemelerin çerçevesi oluşturulurken anayasanın yüksek korumasının dikkate alınmasının önemi ortaya çıkmaktadır. 1982 Anayasa'nın 20. m.'sine yapılan bu ekleme ile temel bir hak ihdas edilmiş ve kişisel verilerin korunması hakkı Anayasadaki yerini alarak anayasal bir hak niteliğine sahip olmuştur.[558] 1982 Anayasasına yapılan bu ekleme ile kişisel verilerin korunması hakkı bağımsız bir hak statüsüne kavuşarak, bu hakkın *temel, vazgeçilmez* ve *devredilemez* bir hak olduğu kabul edilmiş ve böylece, bu hakka yapılacak müdahalenin sınırları da oldukça daraltılmıştır.[559]

Anayasaya yapılan bu ekleme ile kişisel verilerin korunması konusunda sadece bu hakkın varlığı belirtilmekle kalınmamış, veri sahibinin bilgilendirilmesi, verilere erişiminin sağlanması, bu verilerin düzeltilebilmesini ve sildirebilmesini isteme hakkı

---

558 Civelek, Dilek Yüksel, "Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi", (Yayınlanmamış Uzmanlık Tezi), Ankara, 2011, Devlet Planlama Teşkilatı, s. 142.

559 Dağ, Güray, "Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması", (Yayınlanmamış Doktora Tezi), İstanbul, 2011, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, s. 59.

ve verilerin ne için kullanıldığını öğrenebilmesini de kapsayacak şekilde genişletilmiştir.[560]

3.1.2.2. Anayasa'nın 20. Maddesindeki Düzenlemenin Genel Bir Değerlendirmesi

1982 Anayasası'nın 20. m.'sine getirilen ek düzenleme, kişisel verilerin korunmasını isteme hakkının anayasal dayanağını açıkça oluşturması nedeniyle önemli olarak kabul edilse de bu düzenlemenin bazı eksik yönlerinin bulunduğu hususları da doktrinde ifade edilmiştir.

Buna göre, ABTHŞ'de yer almasına rağmen Anayasasının 20. m.'sindeki düzenlemede kişisel verilerin işlenmesini denetleyecek bağımsız bir kuruma yer verilmediği yönündeki eleştiri bunlardan biridir. Kişisel verilerin ancak kanunda öngörülen durumlarda veya kişinin açık rızasının bulunması halinde işlenebilmesi kuralının Anayasanın 13. m.'si ile çeliştiği, çünkü, 13. m.'de yalnızca Anayasa'da belirtilen sebeplerle temel hakların sınırlanabileceği düzenlenmişken, 20. m.'deki bu düzenlemenin ise sınırlama sebeplerini belirleme yetkisini kanuna verdiği, bu yüzden bu düzenlemenin kişisel verilerin etkin şekilde korunmasına engel olabileceği yönündeki eleştiri bu yönde getirilen bir diğer eleştiridir.[561] Zira, Anayasa'nın 13. maddesinde 2001'de yapılan değişiklikle, temel hak ve özgürlüklerin genel sınırlandırılması rejiminden vazgeçilerek, her hakkın kendi niteliğine özgü sınırlama sebeplerini içeren düzenlenme kabul edilmiştir. Temel hak ve özgürlükleri sınırlamanın sınırlarını belirleyen Anayasanın 13. m.'sinde, temel hak ve özgürlüklerin nasıl sınırlanacağı, söz konusu sınırlamayı yapan kanunun hangi standartta olacağı düzenlenmiştir.[562]

Anayasanın 13. m.'sinin bu hüküm nedeniyle Anayasanın temel hak ve özgürlükleri düzenleyen maddelerinde, her hak ve özgürlük için ayrı bir sınırlama sebebi öngörülmüştür. Örnek vermek gerekirse, Anayasasının 20. m.'sinde "*özel hayatın gizliliği hakkı"* ile ilgili düzenleme yapılarak bu hak güvence altına alınmış,

---

560 Boz, a.g.e., s. 92.

561 Küzeci, a.g.e., s. 266.

562 Yokuş, Sevtap, "Avrupa Birliğine Uyumda Siyasi Kriterler Doğrultusunda Türkiye'de Anayasal ve Yasal Dönüşüm Çabaları", İÜHFM, 2003, C. LXI, S. 1-2, s. 212.

özel yaşamın ve aile yaşamının gizliliğine dokunulamayacağı hüküm altına alınmıştır.[563] Bu hükmün 2. fıkrasında ise bu hakkın hangi hallerde sınırlanabileceği hüküm altına alınmış, kişilerin üstlerinin, özel evraklarının ve eşyalarının aranması ve bunlara el konulmasının hangi şartlar altında söz konusu olabileceği belirlenmiştir. Yani, "*özel hayatın ve aile hayatının gizliliği"* hakkının sınırları çizilmiştir. Benzer şekildeki düzenleme konut dokunulmazlığı ve haberleşme hürriyeti açısından da geçerlidir. Bu maddelerde de (m. 21-22) herkesin bu hakka sahip olduğu vurgulandıktan sonra bu hakların hangi sebeplere dayanılarak, nasıl sınırlandırılabileceği açıkça düzenlenmiştir. Kişisel verilerin korunması hakkının düzenlendiği 20. m.'sinin üçüncü fıkrasında ise bu yönde bir düzenleme yapılmamış sadece hakkın sınırlama yönteminden bahsedilmiştir.[564] Dolayısıyla böyle bir durumda, kanun ile kişisel verilerin korunması hakkına sınırlama getirirken sınırlama sebepleri konusunda elini daraltan herhangi bir hükme anayasa m.20'de yer verilmediğinden ötürü kanun çalışmasında hangi metodlar ve sebepler ile sınırlama yapılacağı hususunda parlamentonun tam yetki sahibi olduğu ileri sürülebilir. Mamafih, kişisel verilerin korunması hakkının hukuki niteliğinde belirttiğimiz üzere AİHM, AYM kararlarında vurgulandığı üzere, bu hak, sadece kişisel veriler ile değil özel hayatın gizliliği, haberleşme hürriyeti gibi haklar ile yakın ilişkidedir. Dolayısıyla kanun ile getirilen sınırlamalarda, kanaatimizce, bu haklarda sayılan özel sınırlama sebeplerine uyulmaması anayasaya aykırılık teşkil edecektir.

Öte yandan, anayasadaki "*özel hayatın gizliliği ve haberleşme özgürlüğü"* ne ilişkin düzenlemeler ile *temel hak ve özgürlüklerin* sınırlandırılmasının çerçevesini çizen 13. m.'deki düzenlemenin birlikte değerlendirilmesi gerektiğini doktrinde ileri süren görüşler vardır. Yani, Anayasa m. 13'te açıkça temel hak ve hürriyetlerin

---

563 Anayasa m. 20/1: "*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz."(Değişik fıkra 3/10/2001-4709/5 m.)Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.*"

564 Çokmutlu, a.g.e., s. 121.

yalnızca özel sınırlama sebepleri ile sınırlandırılabileceği, temel haklar *"yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak"* sınırlandırılabilir şeklinde ifade edilmiştir. Bu kapsamda 20. m.'nin ikinci fıkrasındaki sınırlamanın sadece kişilerin üzerlerinin, özel evraklarının ve eşyalarının aranması ve bunlara el konulmasına ilişkin olduğu görülmektedir. Öte yandan, belirli yönlerden kişisel verilerin korunması hakkı kapsamında değerlendirilebilecek olan konut dokunulmazlığı ve haberleşme özgürlüğüne getirilebilecek sınırlamaların ise 21. ve 22. m.'lerde düzenlenmiştir. Bu nedenle özel yaşamın gizliliği hakkının, belirtilen özel haller dışında anayasada mutlak olarak korunduğu göz önüne alındığında, kişisel verilerin korunması hakkının da bu kapsamda değerlendirerek anayasadaki bu korunmadan yararlanmasının gerektiğine dair görüşler ileri sürülmüştür.[565] Kanaatimizce, kişisel verilerin korunması hakkı bu bahsedilen korumadan yararlanmakla beraber, 1982 Anayasasının sistematiğine ve 13. m.'sine uygun olacak şekilde, bu hakka yapılabilecek sınırlamaların, anayasanın 20. m.'sinde spesifik olarak belirtilmesi gerekmektedir. Temel bir hakka yapılacak olan müdahalenin sadece kanunla düzenlenmesi isabetli görünmemektedir.

3.2. KİŞİSEL VERİLERİN KORUNMASI HAKKI İLE GETİRİLEN KORUMA ALANI ve BU ALANIN SINIRLARI

Kişisel verilerin korunması hakkı, normatif temelini insan onuru ve insan kişiliğinin serbest geliştirilmesi hakkı ile özel hayatın gizliliğinden almaktır. Bununla birlikte kişisel verilerin korunması hakkı, sınırsız olarak tanınmış, garanti edilmiş değildir. Yani bireyin kişisel verileri üzerindeki hakimiyeti mutlak ve sınırsız değildir. Bireyler bir toplum düzeni içerisinde yaşadıkları için, genellikle ortak kamu yararı söz konusu olduğunda, bireyler kişisel verilere yönelik olarak anayasaya uygun ve hukuki temele dayanan sınırlamalara uymak mecburiyetindedirler.[566]

565 Küzeci, a.g.e., s. 269.

566 Şimşek, a.g.e., s. 149.

3.2.1. KİŞİSEL VERİLERİN KORUNMASI HAKKI İLE GETİRİLEN KORUMA ALANI

Kişisel verilerin korunması hakkı ile temelde amaçlanan şey; kendi özgür iradesiyle yaşamını belirleme yeteneğine sahip olarak, özgür ve demokratik bir toplumda yaşamını sürdüren bireyi ve bireyin verileri üstündeki haklarının korunmasının sağlanmasıdır. Bu nedenle, temel insan haklarından olan kişisel verileri koruma hakkı, modern toplumda gelişen teknoloji ile kişisel verilerin işlenmesinin riskleri nedeniyle, kişinin korunabilmesi için öncelikli olarak kişinin sahip olduğu veriler üstündeki belirleme hakkını, yani kişilerin kişisel verileri üzerindeki karar verme serbestliğini garanti etmektedir.[567] Yalnızca verinin kendisinin korunması veri güvenliğini ilgilendirdiğinden, kişisel verilerin korunması hakkı, kişi hak ve hürriyetlerinden ayrı bir şekilde, yalnızca veriyi korumayı değil tam tersi kişilerin hürriyetlerinin korunmasını sağlamayı hedeflemektedir. Bu nedenle, kişisel verilerin korunması hakkı, kamu kurumları ve özel kişiler tarafından, kişilerin kişisel verilerinin hiçbir sınır olmadan toplanılması, kullanılması, kaydedilmesi ve aktarılması ihtimaline karşı, kişinin temel hak ve özgürlüklerinin korunmasına yardım etmektedir.[568] Kişisel verilerin korunması hakkı ile kişinin kendine ait kişisel verileri üzerindeki belirleme hakkının koruması amaçlandığından hak sahibinin hayatta ve gerçek bir kişi olması gereklidir. Kişisel verilerin korunması hakkının, insan kişiliğini ve insanın özel alanını temel haklar kapsamında koruduğu göz önüne alındığında, tüzel kişilerin verilerin korunması hakkına sahip olmadığı kabul edilebilir.[569]

Ayrıca, kamusal organlara karşı kişisel verilerin korunması hakkının muhatabı özünde devlet olsa da bu konudaki düzenlemelerin özel sektör ile kamu sektörü hakkında uygulanması gerektiğine dair ulusal düzenlemeler vardır. Mesela, İsviçre

---

567 Şimşek, a.g.e., s. 111.

568 Şimşek, a.g.e., s. 119.

569 Şimşek, a.g.e., s. 123; Bunun yanında kişisel verilerin, gerek gerçek kişilere gerekse tüzel kişilere ait olabileceğini ileri süren görüşler de vardır. Ayrıca bkz. Tezcan, Durmuş, "Bilgisayar Karşısında Özel Hayatın Korunması", Anayasa Dergisi, Cilt:8, Yıl: 1991, s. 385-392 ; Bazı Avrupa Birliği'ne üye ülkelerde (İtalya ve Avusturya gibi) kişisel verilere dair kanunlarda veri sahibinin "*natura lor legal person*" (*gerçek veya tüzel kişi*) olabileceği kabul edilmiştir. Cammilleri and Levallois, 2007, s. 14.

kendi kişisel veri kanununda kişisel verilerin gerçek veya tüzel kişiler tarafından işlenmesi halinde kanunun uygulama alanı bulacağı belirtilmiştir.[570]

3.2.2. KİŞİSEL VERİLERİN KORUNMASI HAKKINA GETİRİLEN SINIRLAR

Kişisel verilerin korunması hukukunda bu hakkının sınırlarının tespit edilmesinin özel bir önemi vardır. Sınırları belirlenmiş olmayan bir hak için tam olarak bir güvence sağlanmayacağı gibi, söz konusu hakkın ihlaline yönelik yaptırım uygulanmasında da çeşitli sorunların yaşanması riski ortaya çıkabileceğinden, kişisel verilerin korunması hakkının sınırlarının belirlenmesi özel bir öneme sahiptir.[571]

3.2.2.1. Genel Olarak Özgürlük

Her insanın hak ve özgürlüklerinin bulunduğu anayasal devletlerde kabul edilir.[572] Bununla birlikte, anayasal devlette önemli olan teorik veya felsefi olarak kişilerin hak ve hürriyetlere sahip olmalarından ziyade bireylerin toplum içinde gerçek anlamda kendilerine tanınan hak ve hürriyetlere sahip olabilmeleridir.[573] Ayrıca, her özgürlük bir hak olarak kabul edilse bile her hakkın bir özgürlük olarak değerlendirilmesi söz konusu değildir. Özgür olmak ile kastedilen, kişinin başkalarına karşı öne sürebileceği haklara sahip olması demektir. Tüm hakların ortak kökeninde özgürlük varken, özgürlükleri sağlamak için bireye hukuk düzeninde tanınan yetkiler, yani legal araçlar ise hak olarak ifade edilebilir.[574] Ayrıca, herkes için özgürlükten bahsedilebilmesi için bu özgürlüğün tüm bireyler arasında paylaşılması gerekir. Eğer "*paylaşılmış özgürlük*" sınırları var ise, orada *"sınırlı"* bir özgürlükten basedilir. Anayasaların kapsamlı olarak bireylere tanıdığı hak ve hürriyetlerin birbirleri ile uyumlarını sağlarken, bu hürriyetlerin kötüye kullanılmalarını engellemek amacıyla, kendi içlerinde *"uzlaştırılmaları"* gerektiği gibi *"sınırlandırılmaları"* da bir

---

570 Şimşek, a.g.e., s. 124.

571 Akgül, Aydın, "Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi", (Yayınlanmamış Doktora Tezi), Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli, 2013, s. 95.

572 Turhan, Mehmet, "Anayasal Devlet", Ankara, 2005, Naturel Yayınları, 4. Baskı, s. 159.

573 Mill, John Stuart, "Hürriyet Üzerine", Liberal Düşünce Topluluğu Komisyonu, Çev.Dostel, Mehmet Osman, Ankara, 2003, s. 35.

574 Kaboğlu,"Özgürlükler Hukuku", s. 88.

zorunluluktur.[575] Bir başkasına zarar vermediği müddetçe o özgürlüğün mutlak olduğu öne sürülmekteyse de[576] mutlak hiçbir özgürlüğün bulunmadığı ve her özgürlüğün bir sınırının olduğu da ileri sürülmektedir. Aslında, temel hak ve özgürlüklere bir sınır getirilmesi, bir açıdan onların niteliklerinin gereği olduğu gibi, hak ve özgürlüklerin her kötüye kullanımı da bir sınırlama doğurmaktadır.[577] Zira, bir temel hak sahibinin, o temel hak ve özgürlüklerini kontrolsüz veya orantısız olarak kullanması ile kamu yararı veya başka temel hak sahiplerinin haklarının çatışması söz konusu olabilir.[578] Kötüye kullanılmalarının önlenmesi ve herkesin yararlanmasının sağlanması amacıyla özgürlüklerden yararlanma belli sınırlamalara tabi tutulmuştur.[579]

3.2.2.2. Hak ve Özgürlüklere İlişkin Başlıca Güvence Ölçütleri

Kişilerin temel hak ve hürriyetlerinin korunması düşüncesi kişisel verilerin korunması hakkının temelinde yattığı için, kişisel verilerinin korunması ile aynı zamanda kişilerin özgürlüğü de korunmuş olmaktadır.[580] Kişi hak ve özgürlüklerinin teminat altına alınması yoluyla devletten bu hak ve özgürlüklere karşı saygılı davranmasını beklemek ve bunu sağlamak anayasal devletin temel amacıdır.[581] Nitekim, kişi hak ve özgürlükleri bireylere devlet tarafından bahşedilen haklar olmayıp, bu kişi hak ve özgürlükleri hukuksal anlamda devletten daha önce mevcut olan haklardır. Bu nedenledirki, temel hak ve hürriyetler, aslında devletin müdahale etme riskine karşı bireylerin özgürlük alanlarına teminat sağlayan, koruyucu haklardır. Söz konusu temel haklar, anayasal formda nesnel temel hukuk kuralları biçiminde düzenlendiğinde hukuken her alanı ve her açıdan etkileyen bir nitelik kazanmaktadır.[582] Bir hakkın sınırlanması anayasa hukukunda hakkın *"norm alanı"*nın küçültülmesini ifade ederken, hakkın sınırlandırılması ayrıca, hakkın

---

575 Kaboğlu,"Özgürlükler Hukuku", s. 88.

576 Mill, a.g.e., s. 47.

577 Akgüner, Tayfun, "Laiklik Üzerine…", İdare Hukuku ve İlimleri Dergisi, Prof. Dr. İsmet Giritli'ye Armağan, Yıl:12, Sayı: 1-3, s. 78.

578 Gören, Zafer, "Temel Hak Genel Teorisi", Ankara, 1995, Dokuz Eylül Üniversitesi Döner Sermaye İşletmesi Yayınları, Yayın No:57, s. 78.

579 Kaboğlu, "Özgürlükler Hukuku", s. 88.

580 Şimşek, a.g.e., s. 2.

581 Turhan, a.g.e., s. 173.

582 Ünal, Şeref, "Temel Hak ve Özgürlükler ve İnsan Hakları Hukuku", Ankara 1997, Yetkin Yayınları, s. 40 vd.

kapsama alanı içinde olması icap eden bazı etkinliklerin hakkın kapsamı dışında bırakılarak, koruma alanının dışına çıkarılması anlamına gelmektedir.[583] Bununla birlikte, genel anlamda hak ve hürriyetlerin, özel anlamda ise kişisel verilerin korunması hakkının sınırlanması konusunda, bazı kriterlerin göz önüne alınması anayasal devletin gereği olarak karşımıza çıkmaktadır. Anayasanın 13. ve 15. m.'lerinde gösterilen çerçeve, kişisel verilerin dokunulmazlığı ve korunması hakkının sınırlandırılmasında ve bu hakkın kısmen veya tamamen kullanımının durdurulmasında göz önünde bulundurulmalıdır. Bir hak ve özgürlük sınırlandırılacağı zaman öncelikle o hak ve özgürlüğün düzenlendiği anayasa maddesinde özel sınırlandırma nedenlerinin gösterilmiş olması gerekmektedir. İlgili anayasa maddesinde özel bir sınırlama nedenine yer verilmemesi halinde, o temel hak ve özgürlüğe sınırlama getirilmesi mümkün değildir.[584] AİHS, özgürlük ilkesini ortaya koyduktan sonra, özgürlüğün sınırlandırılmasına ilişkin; sınırlandırmanın "*kanun ile yapılması" ve* "*meşru bir amaç için yapılması"*, diğer bir ifade ile sözleşmede yer verilen sebeplerden birisinin yer alması ve sınırlandırmanın "*demokratik toplumda zorunlu olması"* olarak üç kriter belirlemiştir.[585]

Aynı şekilde, Anayasanın 13 m.'sine göre ise; temel hak ve özgürlükler sadece kanun ile sınırlandırılabilirken bu hak ve özgürlüklerin özlerine dokunulmayacak ve sadece anayasada belirtilen sebepler göz önüne alınarak sınırlandırma yapılabilecektir. Yine aynı madde gereğince temel hak ve hürriyetlere getirilecek sınırlandırmalar *"Anayasanın sözüne ve ruhuna"*, *"demokratik toplum düzeni ve laik Cumhuriyetin gereklerine"* ve son olarak da *"ölçülülük ilkesine"* aykırı olamayacaktır.

Bu açıklamalar ışığında temel hak ve özgürlüklerin sınırlandırılması kriterlerinden yola çıkılarak kişisel verilerin korunmasının sınırlandırılmasında aşağıdaki ölçütlerin göz önüne alınacağı kabul edilebilir.

---

583 Erdoğan, Mustafa, "Türkiye'de Anayasalar ve Siyaset", Ankara, 2008, s. 178.

584 Şen, Ersan/Yasemin Yurttaş, "Bilgisayar Programları Karşısında Özel Hayatın Korunması", Terazi Hukuk Dergisi, 2010, Yıl:.5, S. 42, s. 31.

585 Kaboğlu, "Özgürlükler Hukuk", s. 89.

3.2.2.2.1. Kamu Düzeni İlkesi

Bir hak ve özgürlük sınırlandırılırken ve kötüye kullanılması halinde yaptırım uygulanırken söz konusu hak ve özgürlüğün amacına uygun bir şekilde kullanımının sağlanması esas alınmalıdır. Özgürlüklerin kullanımı esnasında öne çıkan amaç baz alınmaksızın kişisel menfaat ile toplumsal menfaat arasındaki dengenin korunması gereklidir. Burada, özgürlüğün kötüye kullanılması durumunda bireysel çıkar ile toplum çıkarı arasındaki denge göz önünde bulundurularak uygulanacak olan yaptırımda *"kamu düzeni"* temel ölçüt olarak değerlendirilebilir.[586] Özgürlüklerin düzenlenerek belli sınırlar içine alınmasının öncelikli olarak kamu düzeninin sağlanması için gerekli olduğu kabul edilmektedir.[587] Zira, özgürlükler ve kamu düzeni demokratik toplum hayatının iki temel unsuru olduğu için, bu iki temel unsur dengelenirken, unsurlardan kamu düzenine gereğinden fazla ağırlık tanınması ile özgürlüklerin zarar görmesi söz konusu olabilecekken, kamu düzeninin gereklerinin ihmal edilmesi halinde ise toplumda kargaşanın çıkması söz konusu olabilecektir.[588]

"*Dirlik-düzenlik(dinginlik)*", "*güvenlik*" ve "*sağlık*" olmak üzere kamu düzeninin üç ögeden oluştuğu kabul edilir. Bu nedenle bir özgürlüğün kullanımı, güvenlik açısından tehlike arz etmemeli, halkın sağlığına tehdit oluşturmamalı ve kamu dinginliğine zarar vermemelidir. Bu nedenle, kamu düzeninin bu üç ögesinin toplumun ortak alanlarıyla ilgili olup, soyut olmayıp maddi olması nedeniyle, kamu düzeninin sınırları çizilebilen bir kavram olduğu değerlendirilmektedir.[589]

"Kişi özgürlüğü, *kişi güvenliği* ve *kişi dokunulmazlığı"* gibi kavramlar bireyin endişe duymadan yaşamını sürdürmesini sağlama amacı taşıyan ögelerdir. Geçmişten günümüze, insanlar tarafından uzun yıllar boyunca verilen tarihi mücadeleler sonunda, bu güvenceler çeşitli uluslararası belgelerde ve anayasalarda hak ettikleri yeri almayı başarmışlardır. Bununla birlikte, kişinin toplumda güvenli bir şekilde yaşayabilmesi için devletin kamu düzeninin sağlanması arasında kurulması istenen hassas denge her

---

586 Yokuş, Sevtap, "Avrupa İnsan Hakları Sözleşmesi'nde ve 1982 Anayasası'nda Hak ve Özgürlüklerin Kötüye Kullanımı", Ankara, 2002, Yetkin Yayınları, s. 71.

587 Kapani, Münci, "Kamu Hürriyetleri", Ankara, 1993, 7. Baskı, s. 223.

588 Yokuş, "Hak ve Özgürlükler", s.70.

589 Kaboğlu, İbrahim Ö., "Anayasa Hukuku Dersleri (Genel Esaslar)", İstanbul, 2011, 7. Baskı, s. 251.

zaman sağlanamadığından kişinin özgürlüğüne, güvenliğine ve dokunulmazlığına ilişkin problemler günümüzde de halen varlığını korumaktadır.[590]

AİHS'de, *"düşünce, din ve vicdan özgürlüğü", "özel hayatın ve haberleşmenin gizliliği"*, *"ifade özgürlüğü"* gibi hak ve hürriyetlerin *"kamu düzeni"*, *"kamu yararı"*, *"genel ahlak"*ın korunması gibi sebeplerle sınırlandırılmasını, bu sınırlamanın demokratik bir toplumda *"zorunlu" ve "gerekli"* olması şartlarına bağlamıştır. AİHM de "*demokratik toplum düzeni"* ifadesinin kullanılması ile, sözleşmeye taraf devletlerdeki demokrasi anlayışında müşterek bir standart oluşturma gayretindedir. AİHS'de hak ve hürriyetlerin sınırlandırılabilmesi için, bu sınırlamanın "*demokratik toplum düzeni"* için zorunlu ve gerekli olması şartı getirilmiş, AİHM de *"gereklilik"* ile zorlayıcı bir toplumsal ihtiyacın varlığının kastedildiği belirtmiştir.[591] Kişilerin mahremiyetinin korunması demokratik ülkelerde kişi temel hak ve özgürlükleri çerçevesinde kesin bir zorunluluk olarak karşımıza çıksa bile, tüm devletler, vatandaşlarının hak ve hürriyetlerini teminat altına alabilmek için, ülkelerindeki kamu güvenliğini sağlayarak toplumsal anlamda sosyal düzeni korumak zorundadırlar. Bundan dolayı, kamu kurumları, suçlularla etkin mücadele etmek, vergi toplayabilmek, kamu hizmetini daha sağlıklı sunabilmek gibi amaçlarla, kişiler hakkındaki bazı bilgileri toplayabilmektedir.[592] Ayrıca, devlet tarafından kamu yararı nedeni ile temel haklardan olan kişisel verilerin korunması hakkına müdahale edilebilir. Bunun yanı sıra sosyal, hukuk devleti olarak devletin yüklendiği ödevleri yerine getirirken lazım olan bilgiler için kişisel verilerin korunması hakkına sınırlamalar getirmesi meşru kabul edilecektir.[593]

3.2.2.2.2. Demokratik Toplum Düzeni İlkesi

Anayasanın sözüne ve ruhuna aykırı olmayacak şekilde, temel hak ve özgürlüklerde kanunla yapılacak sınırlamanın çerçevesinin *"demokratik toplum düzeni"* ilkesi oluşturmaktadır.[594] Zamanla "demokratik toplum" anlayışının

590 Kuzu, Burhan, "Ülkemizde Kişi Özgürlüğü ve Güvenliği", İstanbul, 1997, s. 17.

591 Yokuş,"Hak ve Özgürlükler", s. 75.

592 Aksoy, "Kişisel Verilerin Korunması", s. 76.

593 Şimşek, a.g.e., s. 119.

594 Gören, Zafer,"Anayasa Hukuku", Ankara, 2011, Yetkin Yayınları, s. 403.

ilerlemesi ile demokratik toplum düzeni ilkesinin yorum yoluyla güçlendirilebilecek nitelikte olduğu ifade edilmektedir. Bununla birlikte, bu ilke, bütün haklar ve özgürlükler için teker teker somutlaştırılmasının güç olması, daha çok siyasal rejimin ve demokrasinin alanına girip hak ve özgürlüğün dışında kalması nedeniyle *"öz"* güvencenin yerini alabilecek bir kriter olmadığı noktalarından eleştirilmektedir.[595]

AİHM tarafından demokrasinin veya demokratik toplumun genel, kapsayıcı bir tanımı yapılmamakta ise de başvurunun konusuna göre yeri geldikçe demokrasinin önemi vurgulanmaktadır. AİHM tarafından verilen çeşitli kararlarda; AİHS ile teminat altına alınmış olan hak ve hürriyetlerin sadece demokratik bir devlette söz konusu olabileceği, sözleşmede öngörülen tek siyasi modelin demokrasi olduğu belirtilmektedir. Hak ve özgürlüklere müdahale yapıldığı yönündeki iddialarda AİHM tarafından yapılan incelemelerde bu müdahalelerin demokratik toplum düzeninin temel ilkelerine uygun ve gerekli olup olmadığı yönünde değerlendirme yapılmaktadır.[596] [597]

3.2.2.2.3.Ölçülülük İlkesi

"Ölçülülük ilkesi", hak ve özgürlükleri sınırlarken kullanılan aracın sınırlama amacını gerçekleştirmek için uygun olmasını; kullanılan aracın, sınırlandırma amacının gerçekleşmesi için gerekli olmasını ve araç ile amacın *"ölçülü bir oran"* içinde bulunması anlamına gelir.[598] Anayasa Mahkemesi ise bir kararında[599] ölçülülük

---

595 Bu eleştiriler kapsamında "*demokratik toplum düzeninin gerekleri*"nden bahsedilenin "*hangi demokrasi*" anlayışı olduğu sorgulanmaktadır. Bu sorunun cevabını ararken şu soru yöneltilmektedir: "*Anayasanın Başlangıç metninde belirtilen "bu Anayasada gösterilen hürriyetçi demokrasi" mi, yoksa evrensel standartlarıyla çoğulcu-özgürlükçü demokrasi mi?*" Bülent Tanör/ Necmi Yüzbaşıoğlu, "1982 Anayasasına Göre Türk Anayasa Hukuku", İstanbul, 2012, 11. Baskı, s. 151; "*Demokratik toplum düzeninin*", sadece 1982 Anayasasında ifade edilen düzenin değil, bütün özgürlükçü ve çağdaş demokrasilerde genel geçer "*demokratik düzen*" anlayışı şeklinde kabul edilmesi gerekir. Bu sayede Türkiye'nin de taraf olduğu insan haklarına ilişkin uluslararası sözleşmelerin ve söz konusu sözleşmelerin tarafı olan diğer devletlerin iç hukuklarındaki müşterek standartların Anayasa Mahkemesi kararlarında en azından destek ölçü norm şeklinde kullanılması mümkün olacaktır. Özbudun, Ergun, "Anayasa Hukuku", Ankara, 2009, Yetkin Yayınları, 10. Baskı. s. 115.

596 Erhan, Tanju, "AİHM Kararları Işığında İfade ve Basın Özgürlüğü", Ankara, 2012, s. 143.

597 Demokratik toplum düzeni ölçütleri için ayrıca bkz. https://www.anayasa.gov.tr/media/4802/mturhan.pdf, Erişim tarihi, 15.09.2019.

598 Özbudun, a.g.e., s. 113.

599 AYM, 18.6.2009 tarihli E:2006/121, K:2009/90, 26.11.2009 tarihli ve 27418 sayılı Resmi Gazete.

ilkesini *"Anayasa'nın 13. maddesinde yer alan ölçülülük ilkesi, amaç ve araç arasında hakkaniyete uygun bir dengenin bulunması gereğini ifade eder. Ölçülülük, aynı zamanda yasal önlemin sınırlama amacına ulaşmaya elverişli olmasını, amaç ve aracın ölçülü bir oranı kapsamasını ve sınırlayıcı önlemin demokratik toplum düzeni bakımından zorunluluk taşımasını da içeren bir ilkedir."* şeklinde tanımlamıştır.

Ölçülülük ilkesi; hukukun genel ilkeleri içinde özgürlüklerin güvencesi olarak kabul edilen bir ilke olmakla birlikte bu ilke hukuk devletinin bir sonucudur.[600] Esasında ölçülülük ilkesi, temel hak ve özgürlüklerin kendilerine özgü yapılarından doğmaktadır.[601]

Alman Anayasa Mahkemesinin kararlarında, temel hak ve özgürlük ihlalleri ile ilgili denetimlerde başvurulan temel ölçüt olarak ölçülülük ilkesi geniş yer tutmakta,[602] AİHM'nin de ölçülülük ilkesini sık sık kullandığı görülmektedir. AİHS'deki hiçbir düzenlemede "ölçülülük ilkesi" tanımlanmamış olsa da AİHM'nin, vermiş olduğu kararlarında ortak ifadelerle; *"sınırlamada kullanılan aracın uygun, sonuca yeterli, elverişli, gerekli, orantılı olması"* olarak ölçülülük ilkesini tanımlamış ve bu tanımı sık sık kullanmıştır.[603]

AİHM hem uygulamada hem de mevzuatta, temel hak ve özgürlüğe müdahale ederken ulaşılmak istenen fayda ile söz konusu bu müdahale arasında bir oran olup olmadığını inceleyerek, aleyhine başvuruda bulunulan devletten yaptığı müdahale ile ölçülülük ilkesini ihlal etmediğini ispatlamasını istemektedir.[604]

AİHM *"ölçülülük ilkesi"* bakımından yaptığı değerlendirmelerde, bir hak veya özgürlüğe getirilen sınırlandırmanın ulaşılmak istenen meşru amaç ile dengeli olması zorunluluğunu ifade etmektedir. Türk Anayasa Mahkemesine kıyasla AİHM başvurularda ölçülülük ilkesi yönünden daha detaylı değerlendirme yaparken, yine ölçülülük ilkesi kapsamında, *"zorunluluk"* ifadesini, sınırlamayı *"ulaşılmak istenen*

600 Yokuş, "Hak ve Özgürlükler", s. 78.

601 Kaboğlu, "Anayasa Hukuku", s. 382.

602 Özbudun, a.g.e., s. 113.

603 Yokuş, "Hak ve Özgürlükler", s. 78 vd.

604 Tanju, a.g.e., s. 143.

meşru amaçla orantılılık", "zorlayıcı toplumsal ihtiyaç" ve "*demokratik toplumda zorunlu olma"* şeklindeki alt terimlerle incelemekte, yani "*ölçülülük ilkesi*" hakkında detaylı bir kontrol gerçekleştirmektedir.[605]

AYM de yaptığı incelemelerde bazı alt ilkeler ile ölçülülük ilkesini birlikte değerlendirmektedir.[606] AYM bu kapsamdaki bazı kararlarında: *"Fiil ile müeyyide arasında adil bir denge kurulabilmesi için bu durumun ölçülülük ilkesine uygun olması gerekmektedir. Bu ilkenin alt ilkelerinden olan, "elverişlilik ilkesi", öngörülen müeyyidenin hedeflenen amaçla uygun olmasını, "gereklilik ilkesi" öngörülen müeyyidenin hedeflenen amaç açısından gerekli olmasını ve "orantılılık ilkesi" ise öngörülen müeyyide ile hedeflenen amaç arasında olması gereken orantıyı ifade etmektedir*."[607] diyerek eylem ile yaptırım arasında ölçülülük ilkesinin bulunması gerektiğini vurgulamış ve ölçülülük ilkesinin alt kavramlarını açıklamıştır.

AYM'ye göre, *"ölçülülük ilkesi"*nin alt ilkeleri; "*elverişlilik"*, "*zorunluluk"* ve "*orantılılık"*tır. *"Elverişlilik ilkesi"*; alınmış olan bir tedbir aracılığı ile elde edilmek istenen sonuca yaklaşılması halinde aracın elverişli olduğu kabul edilir. Bununla beraber kullanılması tercih edilen araç erişilmek istenen amaca varılmasını zorlaştırmış veya amaca ulaşma açısından hiçbir etki göstermemiş ise aracın *elverişsiz* olduğu değerlendirilir. *"Gereklilik"* ulaşılmak istenen amaca aynı oranda elverişli olan birden fazla araç içinden, tercih edilmesi halinde hak ve özgürlüklere en az müdahale edilecek olan araçla ulaşmayı ifade eder.[608]

Bu kapsamda, kişisel verilerin korunması hakkına, idare tarafından sınırlandırma getirilirken; alınan önlem ile hedeflenen amaca ulaşılabilmesi mümkün ise, bu durumda alınan tedbirin *elverişlilik ilkesine*, amaca ulaşmaya yarayabilecek birden fazla sınırlama içinde bu hakka en az müdahaleye neden olacak sınırlamanın seçilmiş olması durumunda *gereklilik ilkesine*, tercih edilen bu sınırlandırma ile elde

605 Yokuş, "Hak ve Özgürlükler", s. 79.

606 Akgül, "Yargısal Denetim", s. 102.

607 AYM, 15.6.2012 T., E:2012/24, K:2012/95, 13.10.2012 T. ve 28440 sayılı R.G.

608 Yüksel, Metin,"Temel Hakların Sınırlandırılması ve Ölçülülük, Ölçülülük İlkesi Evrensel Bir Anayasal İlke midir?", SDÜHFD, C. 7, No: 1, Y: 2017, s. 7 vd.

edilmek istenen amaç arasında *ölçülü* bir oranın söz konusu olması halinde de *orantılılık ilkesine*, neticede de hukuka uygun müdahale edildiği söylenebilir.[609]

Anayasa ve ilgili kanun hükümleri göz önünde tutularak kişilerin kişisel verilerinin korunması hakkına sınırlama getirilmesi veya müdahale edilmesi hukuka uygun olarak kabul edilmekte, Anayasa'nın 13. m.'sine göre kişisel verilerin korunması hakkına yapılan söz konusu müdahale veyahut sınırlamanın "*ölçülülük ilkesi*"ne uygun olması gerekmekte ise de, yapılacak sınırlama veya müdahalede Anayasa Mahkemesi ve AİHM kararları çerçevesinde izah etmeye çalıştığımız alt ilkelerin de göz önünde bulundurulması gerekmektedir. [610]

3.2.2.2.4. Sınırlamanın "Kanun" ile Düzenlenmesi İlkesi

Kişinin özel hayatı ve aile mahremiyeti hakkında, başka kişilerin değer yargıları üretmelerine neden olacak bilgilerinin kendisinden habersiz veya yanlış olarak toplanması ve bilgi sahibi kişiye bunları düzeltilmesi için imkân tanınmaması, kuvvetlinin zayıfı ezmesi sonucunu doğurabilir. Bundan dolayı, çoğulcu demokratik rejimlerde kişilerin kendi özel koşulları dışında, kişiliklerinin bir parçası olan temel haklarının açıkça ihlali niteliğindeki bu tür hareketlerin önene geçebilmek için gerekli olan hukuksal düzenlemeler yapılmaktadır.[611]

Kişinin özel hayatı hakkındaki bilgi yetkili kamu idareleri tarafından sadece yasal nedenler ve toplumun menfaati söz konusu olduğunda istenebilecektir. Bu yasal nedenlere örnek olarak doğum, evlilik ve ölüm kayıtlarına dair bilgiler verilebilir.[612]

Halkın temsilci olarak seçtiklerine güven duymaları, yürütme organının ise yetkilerini keyfi kullanma eğiliminde olması nedeni ile, anayasalar, hak ve özgürlüklerin, yasama organınca ve ancak yasayla sınırlanabileceğini kabul etmektedir.[613] Hak ve özgürlüklerin ancak kanun ile sınırlaması şartı, kanun yapıcının yasalar ile temel haklara direkt müdahale etmesine, bunlara sınırlar belirlemesine ya

609 Akgül, "Yargısal Denetim", s. 102.

610 Akgül, "Yargısal Denetim", s. 102.

611 Tezcan, a.g.m., s. 386.

612 Jayawickrama, Nihal, "The Judicial Application of Human Rights Law", Cambridge University Press, s. 606.

613 Kaboğlu, "Özgürlükler Hukuku", s. 89.

da temel hak ve özgürlüklere müdahale etme hakkında idari organları yetkili kılmasına olanak sağlamaktadır.[614] Temel hak ve özgürlükler modern demokrasilerde, idari işlemler ile sınırlandırılamazlar. Anayasanın 13. m.'si de bunu gerektirmektedir.

Anayasanın 20. m.'sinin 3. fıkrasında; kişisel verilerin kişinin açık rızası ile ya da sadece kanunda öngörülen hallerde işlenebileceği düzenlenmiştir. Bu nedenle, anayasal güvence altına alınmış temel bir hak ve hürriyet olan kişisel verilerin korunması konusunda idari makamlar tarafından getirilen sınırlamalar hukuka aykırı olacaktır. İdari makamlar tarafından, kanuni dayanak olmadan kişisel verilerin korunması hakkına sınırlandırma getirmek amacıyla düzenleyici bir işlem yapılamayacak, aynı şekilde bireysel herhangi bir işlem dahi tesis edilemeyecektir. AİHS ile Ek Protokollerinde, devlet tarafından hak ve hürriyetlere yapılması öngörülen müdahalelerin sadece kanunlarla yapılması gerektiğine yer verilmiştir. Sözleşmede yer alan bir hakkın sınırlandırılmasının sadece yasal düzenlemeler ile olabilmesinin, söz konusu hakka keyfi gerekçelerle müdahale edilmesinin önüne geçen bir teminat olduğu değerlendirilmektedir.[615]

Bu hususa ilişkin Anayasa Mahkemesi, son olarak, 24/07/2019 tarih ve 2018/73 esas ve 2019/65 karar sayılı kararı ile memuriyette girişte güvenlik soruşturması yapılması şartını "*Kişisel verilerin korunmasını isteme hakkı, insan onurunun korunması ve bireyin kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Anayasa'nın 20. maddesi uyarınca kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Dolayısıyla kişisel verilerin korunmasını isteme hakkına sağlanan anayasal güvencenin yaşama geçirilebilmesi için bu hakkı ilgilendiren yasal düzenlemelerin açık, anlaşılabilir ve söz konusu hakkın kullanılabilmesine elverişli olması gerekir. Ancak böyle bir düzenleme ile kişilerin özel hayatlarını ilgilendiren veri, bilgi ve belgelerin resmi makamların keyfi müdahalelerine karşı korunması mümkün hale gelebilir. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. maddesine göre*

614 Gören, "Anayasa Hukuku", s. 397.

615 Tanju, a.g.e., s. 142.

kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Anayasa Mahkemesinin yerleşik kararlarında da belirtildiği üzere "...adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler..." kişisel veri olarak kabul edilmektedir. "Bu bağlamda güvenlik soruşturması ve arşiv araştırmasıyla elde edilen veriler kişisel veri niteliğindedir. Kuralla güvenlik soruşturması ve arşiv araştırması kapsamında kamu mercileri tarafından özel yaşamı ile ilgili sorular sorulması da dahil olmak üzere bir bireyin özel hayatı, iş ve sosyal yaşamıyla ilgili bilgilerinin alınması, kaydedilmesi ve kullanılması özel hayata saygı hakkına sınırlama niteliğindedir. Güvenlik soruşturması ve arşiv araştırması sonucunda devlet memurluğuna atanmada esas alınacak kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına ve işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesi Anayasa'nın 13., 20. ve 128. maddeleriyle bağdaşmamaktadır." gerekçesiyle iptal etmiştir.[616] Dolayısıyla sınırlama kanun ile yapılacak ancak sınırlamayı yapan kanunun anayasaya uygun olmasının yanında, açık, anlaşılır ve temel hakkın uygulamasına elverişli olması gerekmektedir.

Bununla birlikte, "*normların açıklığı ilkesi"* gereğince, kişisel verilerin korunması hakkına sınırlandırma öngören düzenlemelerin açık ve vatandaşlar tarafından anlaşılabilir olması gerekmektedir. Nitekim, bu kural, bir yandan da "*veri işlemenin şeffaflığı"* ilkesinin mantıksal bir sonucudur. Ayrıca, *"normların açıklığı ilkesi", "hukuk devleti ilkesi"*nin zorunlu unsuru olan *"hukuk güvenliği ilkesi"*nin de işlevini yerine getirmesine yardım etmektedir.[617]

616 https://www.resmigazete.gov.tr/eskiler/2019/11/20191129-7.pdf, Erişim tarihi: 30.11.2019.

617 Şimşek, a.g.e., s. 125.

3.2.2.2.5. Hakkın Özü Kavramı

Modern devletlerde, devletin, temel hak ve özgürlükleri sınırlayabileceği ancak, sınırlarken bu hak veya özgürlüğün *"öz"*üne dokunamayacağı, yani esas çekirdeğini ortadan kaldıramayacağı hususu hak ve özgürlüklerin sınırlandırılmasında temel ölçüt olarak kabul edilmiştir.

"Hakkın özüne dokunmama"; bir hakka getirilen sınırlamanın hakkı anlamsız hale getirecek seviyeye varmamasını ifade etmektedir. Temel hak ve hürriyetlerin sınırlanmasında, aşılması halinde neredeyse söz konusu hak ve hürriyetin ortadan kalkması sonucunu doğuracak bir çizginin varlığı kabul edilir. Yani, hakkın varlığının ortadan kalkmasına neden olacak derecede ağır nitelikte ve hakkın özüne dokunan bir sınırlama bu ilkeye aykırılık teşkil edecektir.[618]

Tüm hak ve özgürlükler için geçerli bir *"hakkın özü"* tanımı yapılması pek mümkün olmasa da yine de genel bir tanım yapmak gerekirse, temel hak ve hürriyetin özü kavramından, *"söz konusu hakkın vazgeçilmez nitelikte bir unsuru; dokunulması durumunda söz konusu hürriyeti anlamsız hale getirecek olan hakkın asli çekirdeği"* şeklinde tanımlanabilir. Bu haliyle öz kavramı, *"hakkın çekirdeği, temel cevheri"* gibi anlamlara da gelmektedir.[619] Öz teminatı, temel her hakta bir cevher, öz var olduğu ön kabulüne dayanmakta, bir hakkın özüne dokunulmaması ise, hakkı belirli bir içeriğe sahip kabul etme anlamına gelmektedir.[620]

AYM de farklı kararlarında "hakkın özü" tanımını yaparak, "*Anayasal bakımdan dokunulması mümkün olmayan öz, her temel hak ve hürriyet bakımından farklılık arz etmekte; kanun ile getirilen sınırlamanın söz konusu hakkın özüne dokunmadığının kabul edilmesi için temel hakkın kullanımını ciddi ölçüde zorlaştırıp, amacına ulaşmasına engel teşkil etmememesin ve etkisini ortadan kaldırıcı bir nitelik taşımaması gerekir.[621]"* şeklinde açıklamada bulunmuştur.

---

618 Sağlam, Fazıl, "Temel Hakların Sınırlandırılması ve Özü", AÜSBF Yayını, Ankara, 1982, s. 155 vd.

619 Gören," Anayasa Hukuku", s. 400.

620 Sağlam, a.g.e., s. 155.

621 AYM, T.18.6.2009, E.2006/121, K.2009/90, 26.11.2009 tarih ve 27418 sayılı Resmi Gazete.

AYM başka bir kararında ise "hakkın özü" tanımı ile ilgili olarak *"Anayasa'nın 13. maddesinde, özüne dokunmaksızın sadece özel sınırlama sebeplerine uygun olarak ve sadece kanunla temel hak ve özgürlüklerin sınırlanabileceği ifade edilmiştir. Ayrıcasız konusu sınırlamaların, Anayasa'nın özüne ve ruhuna, demokratik toplum düzeni ile laik Cumhuriyetin gereklerine ve hatta ölçülülük ilkesine aykırı olamayacağı açık şekilde belirtilmiştir. Çağdaş demokrasi anlayışının gereği, temel hak ve hürriyetlerin en geniş kapsamda sağlanıp güvence altına alınmasıdır. Temel hak ve hürriyetleri geniş ölçüde kısıtlayarak kullanılmasını imkânsız kılan sınırlamalar o hakkın özüne dokunacaktır. Temel hak ve hürriyetlere getirilen sınırlamaların sadece ölçüsü değil, bu sınırlamanın şartları, sebepleri, uygulanma yöntemleri, sınırlamaya yönelik getirilen kanun yolları gibi teminatların hepsi demokratik toplum düzeninin içinde değerlendirilmelidir. Bu yüzden, temel hak ve hürriyetler, istisnaî şekilde ve sadece özüne dokunmaması şartıyla demokratik toplum düzeninin gerekleri açısından gerekli olduğu miktarda ve yalnızca kanunla sınırlandırılabilirler."* diyerek hakkın özü kavramı ile ilgili ayrıntılı açıklama yapmıştır.[622]

1961 Anayasası dönemindeki, AYM kararlarında "hakkın öz"ü ifadesini sıkça kullanmaktayken, 1982 Anayasası döneminde ise, daha ziyade *"demokratik toplum düzeninin gerekleri"* kavramını kullanmış, *"öze dokunma yasağı"*nı[623] ise bu kavramın kapsamında ya da yanında destek bir norm olarak kullanmayı tercih etmiştir.[624]

---

622 AYM, Tarih: 18.5.2011, E.2009/1, K.2011/82, 26.11.2009 tarihli ve 28208 sayılı Resmi Gazete.

623 Anayasa Mahkemesi'nin 1982 Anayasası döneminde bu yöndeki yaklaşımının nedeni olarak, 1982 Anayasasının ilk halinde, "hakkın özü" kavramına yer verilmemesi gösterilebilir. Hak ve özgürlükleri "sınırlamanın sınırı" olarak 1961 Anayasası'nda "öze dokunamama" ilkesi yer almakta iken, 1982 Anayasasının ilk halinde bu ilke kaldırılıp, sınırlamalara "demokratik toplum düzeninin gereklerine aykırı olmaması ve bunların amaçları dışında kullanılamaması" şeklinde iki sınır getirilmiştir. Bkz. Eroğul, Cem, "Anatüzeye Giriş, (Anayasa Hukukuna Giriş)", Ankara 2005, s. 323; Ancak, 1982 Anayasasında 2001 de yapılan değişikliklerle "hakkın özüne dokunmama" güvencesi yeniden getirilerek, Anayasa Mahkemesi kararlarında eksik olduğu belirtilen bir teminat yeniden sağlanmıştır. Tanör /Yüzbaşıoğlu, a.g.e., s. 153.

624 Tanör/Yüzbsaşıoğlu, a.g.e., s. 153.

"Öz" ifadesi tüm hak ve özgürlükler hakkında kişiye dokunulmaz *"asgari bir alan"* teminatı sağlamaktadır.[625] Öz teminatı, temel her hakta bir *"öz, cevher"* olduğu varsayımından kaynaklandığını belirtmiştik. Zira bir hakkın dokunulmaz bir özünün olduğunu kabul etmek, onun belli bir içeriğe sahip olduğunu kabul etmek demektir. Nesnel nitelikli temel hak normunu, bu normun oluşturduğu öznel nitelikli kamu hakkından ayırmanın, temel hakka getirilen güvencenin bütünlüğünü bozacağı, bundan dolayı hakkın özü güvencesinin, nesnel nitelikteki temel hak normunu ve öznel nitelikli hakkın özünü koruma altına alan bir kural olduğu belirtilmektedir.[626]

Bu açıklamalar ışığında, hakkın özünün, kişisel verilerin korunması hakkı ile ilgili yapılacak sınırlamaların güvencesini oluşturduğu ifade edilmektedir. Çünkü, kişisel verilerin korunması hakkına bir sınırlama getirilirken "hakkın öz"ü göz önüne alınarak düzenleme yapılması halinde, getirilen sınırlama ile bu hakkın kullanılabilmesi mümkün olacakken, bu hakka getirilen sınırlama ile bu hakkın "öz"üne dokunulması halinde, artık kişisel verilerin korunması hakkının kullanılabilmesi söz konusu olmayacaktır. 1982 Anayasasının 20. m.'sine göre, kişisel verilerin korunması hakkı ile ilgili düzenlemelerin yasayla yapılması gerekli olmakla birlikte, Anayasanın 13. m.'sine göre de bu hakkın sınırlandırılmasına dair yapılacak düzenlemelerde *"hakkın özü"*ne dokunulmaması gerekmektedir.[627]

AYM, kişisel verilerin korunmasına dair bazı hükümler içeren ve 703 sayılı KHK ile ilga edilen 5952 sayılı Kamu Düzeni ve Güvenliği Müsteşarlığı Teşkilat Kanununun ilgili maddesinin iptali talebiyle açılan davada, *"hakkın özü"* kavramı ile ilgili değerlendirme yaparak ilgili yasa hükümleri hakkında karar vermiştir. Anayasa Mahkemesi söz konusu kararında *"Terörle mücadele alanında politikalar geliştirme konusunda yetkili olan Kamu Düzeni ve Güvenliği Müsteşarlığının verilen görevleri ifa edebilmesi için bireylerin kişisel verileri de dahil olmak üzere bazı bilgi ve belgelere gereksinim duyması kaçınılmazdır. İptali istenen düzenlemede, veri ve bilgilerin terörle mücadele konusuyla sınırlı olacağı net bir şekilde ifade edilmiştir. Söz konusu düzenleme kişisel verilerin korunması konusunda Anayasa'nın 20.*

625 Tanör/Yüzbaşıoğlu, a.g.e., s. 153.

626 Sağlam, a.g.e., s. 155.

627 Akgül, "Yargısal Denetim", s. 107.

maddesi ile getirilen korumaya aykırı herhangi bir düzenleme de bulunmamaktadır. TCK'nın kişisel verilerin korunması konusunda getirdiği düzenlemelerin, Müsteşarlık personeli bakımından da geçerli olduğu açıktır. Bu yüzden, davaya konu teşkil eden düzenleme ile Kamu Düzeni ve Güvenliği Müsteşarlığına terörle mücadele konusu ile sınırlı olmak kaydıyla sağlanan veri ve bilgi toplama yetkisinin, özel hayatın gizliliği ilkesi kapsamında kişisel verilerin korunması hakkına ölçüsüz bir sınırlama olduğunu söylemek mümkün değildir. Ayrıca, bu kuralın kişisel verilerin korunması hakkını radikal şekilde güçleştiren ya da ortadan kalkmasına neden olan, dolayısıyla hakkın özüne dokunan bir sınırlama olmadığı da nettir."[628] demek suretiyle, kişisel verilerin korunmasını isteme hakkını ortadan kaldıran ya da kullanılmasını aşırı şekilde zorlaştıran sınırlandırmaların hakkın özüne dokunan sınırlamalar olacağı ifade edilmiştir.

Anayasa Mahkemesi söz konusu kararında, "…*terörle mücadele konusu ile sınırlı olmak kaydıyla sağlanan veri ve bilgi toplama yetkisinin, özel hayatın gizliliği ilkesi kapsamında kişisel verilerin korunması hakkına ölçüsüz bir sınırlama olduğunu söylemek mümkün değildir. Ayrıca, bu kuralın kişisel verilerin korunması hakkını radikal şekilde güçleştiren ya da ortadan kalkmasına neden olan, dolayısıyla hakkın özüne dokunan bir sınırlama olmadığı da nettir."* şeklinde açıklama yapmış ise de, terörle mücadele için toplanması istenen kişisel verilere dair bir sınır çizmeden, kişisel veri toplanmasına dair koşullar belirlenmeden, kapsam tespit edilmeden her türlü kişisel verinin toplanabilmesine imkân verilmesinin, kişisel verilerin korunması hakkının özüne dokunulmasına yol açacağı ileri sürülmüştür.[629]

---

628 AYM, T.19.1.2012 E. 2010/40, K. 2012/8, 6.3.2013 T. ve 28579 sayılı R.G.

629 Akgül, "Yargısal Denetim", s. 108. Zira, bu Anayasa Mahkemesi kararına yazılan karşı oyların birinde; "*İptali istenen kural, kişisel verilerin, bilgi ve belgelerin toplanmasına ve tasnif edilmesine olanak vermekte, veri, bilgi ve belgelerin kişisel veri ve bilgileri kapsamadığı yönünde bir güvence de içermemektedir. Anayasa'nın 20. maddesinde özel hayatın gizliliğine milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması sebeplerine bağlı olarak hâkim kararıyla sınırlanabileceği öngörülmüş ise de iptali istenen kural bu kapsama girmemektedir. Kişinin bu kural uyarınca fişlendiğinden haberdar olması, bunların silinmesini talep etmesi ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmesi de mümkün değildir. Bu nedenle kural, Anayasa'nın 20. maddesiyle güvence altına alınmak istenen temel hakka karşı yapılmış pervasız bir müdahaledir*." denilerek iptali istenen yasa maddesi ile kişisel verilerin korunması hakkına pervasız bir müdahale imkânı tanındığı ifade edilmiştir. Bir diğer karşı oy gerekçesi ise: "*Dava konusu kural ile Kamu Düzeni ve Güvenliği Müsteşarlığının Araştırma-Geliştirme Daire Başkanlığı'na kapsamı ve koşulları belirlenmeksizin her türlü veri,*

3.3. KİŞİSEL VERİ HUKUKUNDA İNSAN ONURU

3.3.1. GENEL OLARAK İNSAN ONURU

İnsan, insana kişilik değeri katarak onu özgün kılan bir takım ahlaki ve akli yetileri ile diğer canlılardan farklılık gösterir. Bu anlamda *"insan onuru"*, birey olarak insanın en yüksek ahlaki ve akli değerlere sahip olması ve dolayısıyla da dokunulamayan ve kaybedilemeyen bir öz değerin sahibi olduğu ön kabulüne dayanmaktadır.[630] Bu açıklamadan yola çıkarak, *"insan onuru"*nun, insanı insan yapan ve insanı diğer canlılardan ayıran bir öz değer ve insan haklarının da temeli olduğu söylenebilir.[631] Başka bir deyişle, bütün temel insan hakları, insan onuru için gerekli görülmekte ve hepsi temelde ortak düşünce olan insan onurundan doğmakta ve insan onurunun bağımsız parçalarını oluşturmaktadır.[632]

Modern pozitif hukuktaki ahlaksal ve doğal hukuk doktrinlerinde, insan onuru, en üstün ve vazgeçilmez bir değer olarak kabul edilmektedir.[633] İnsan onuruna, pek çok uluslararası düzenlemelerde ve ülke anayasalarında yer verilmekle birlikte, insan onurunun tanımı bu metinlerin birçoğunda yer verilmemiştir. Alman Anayasa Mahkemesi insan onurunu *"İnsan onuru, insanın bizzat kendisinden sorumlu olması, tinsel-ahlâkî bir varlık olup kendini gerçekleştirme özgürlüğüne sahip olması demektir."* şeklinde tanımlamıştır.[634]

---

bilgi ve belgeleri toplama görevi verilerek kişilerin özel hayatlarının gizliliğinin korunması kapsamında bulunan, kişisel verilerin korunmasını isteme hakları ihlâl edilmiştir." şeklindedir.

630 Bulut, Nihat, "Eski Yunan'dan Aydınlanma Çağı'na İnsan Onuru Kavramının Gelişimine Bir Bakış" EÜHFDi, C. XII, S. 3-4, 2008, s. 2.

631 Kafadar, Muhammet Fatih, "Hukuk, Sivil Toplum ve Demokrasi: 'İnsan Onuru'", Umut Vakfı Araştırma Merkezi, 3. Hukukun Gençleri Sempozyumu, 11-12 Ekim 2013, Antalya, s. 2; "*Tabi ki, kavramın ortaya ilk çıktığı andan itibaren hiç değişmeden günümüze kadar geldiği söylenemez. İnsan onuru, Eski Yunan ve Roma'da olduğu gibi Ortaçağ'da da insanların toplumsal statülerine bağlı bir kavram olarak kendini göstermektedir. Ancak Rönesans ile birlikte ise insan onuru küçük bir seçkinler grubuna ait olan bir nitelik olarak değil, herkesin sahip olduğu bir nitelik olarak kabul edilmiş ve insan onuru herkesi kapsayan bir ideal haline gelmiştir. Yani, Rönesansı müteakiben aydınlanma ile birlikte artık insan başlı başına bir değer olarak görülmüş ve bir özne olarak kabul edilmiştir.",* Bulut, s. 11.

632 Gören, "Temel Hak", s. 499.

633 Aldanmaz, Orhan, "İnsan Onuru Işığında Kişisel Özerklik ve Yerellik Kavramı", Erzincan Üniversitesi Hukuk Fakültesi Dergisi, Cilt: XIV, Sayı: 1-2, Yıl: 2010, s. 82.

634 Topakkaya, Arslan, "H. Jonas'ta İnsan ve Doğanın Değeri", Felsefe ve Sosyal Bilimler Dergisi, S. 15, Yıl: 2013, s. 45.

İnsan onuru, en yalın hali ile insanın insan olmasından dolayı değerli ve saygıyı hak eden bir varlık olması şeklinde tanımlanabilse[635] de insan onuru esasen çok yönleri bulunan ve oldukça kapsamlı bir kavramdır.[636]

İnsan onuru birinci olarak, sosyal bir kavram olup, kişinin kendi kendine duyduğu saygıyı ifade ettiği gibi kendisine karşı diğer insanlar tarafından duyulan saygıyı da ifade etmektedir.[637] İkinci olarak insan onuru felsefi bir kavram olup, insanın en üstün değer olarak görüldüğü *"hümanizm (insancıllık) ilkesinden"* doğmuştur. İnsanı temel alan bir felsefe olan hümanist felsefede, insan onuru bu felsefenin bir gereği olarak kabul edilmiştir.[638] Üçüncü olarak ise, teolojik bir kavram olarak insan onuru hakkında birçok dinde değerlendirmeler ve tespitler yapılmıştır.[639]

Son olarak ise, hukuki bir kavram olan insan onuru hem hukuki olan hem de hukukun bütün alanlarında kendisinden yararlanılması mümkün olan bir kavramdır. Bir sosyal düzen kural çeşidi olan hukuk kuralları insanın bulunduğu her alanda; insanları diğer insanlara, toplumun geneline ve devlete karşı korumaktadır. Bu nedenle hukuk düzeninde insan onuru ifadesi genel kabul görmesi zorunlu ve temel bir kavramdır.[640]

Bu açıdan, insan hakları gibi aynen insan onuru da hiçbir ayrım ya da kısıtlama olmadan insan olmaya bağlı olması gereken ve sadece bu surette evrensel geçerliliği teminat altında olabilecek bir kavram olarak karşımıza çıkmaktadır. Nitekim insan onuru kavramı BM Antlaşması, Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi, AİHS ve ABTHŞ gibi oldukça ehemmiyetli uluslararası belgelerde yer verilen önemli bir kavramdır.[641]

---

635 Çakar, Ayşen Seymen, "Hukuki Bir Kavram Olarak İnsan Onuru", Umut Vakfı Araştırma Merkezi, 3. Hukukun Gençleri Sempozyumu, Antalya 2013, s. 3.

636 Arslan, Kahan Onur,"İnsan Onuru Kavramı ve Koruma Tedbirleri Bağlamında Temel Bir İlke Olarak İnsan Onurunun Korunması", Türkiye Barolar Birliği Dergisi, Yıl: 2015, Sayı: 120, s. 157.

637 Seymen, Çakar, a.g.m., s. 2.

638 Seymen, Çakar, a.g.m., s. 2

639 Arslan, K.O., a.g.m., s. 158.

640 Seymen Çakar, a.g.m., s. 3.

641 Arslan, K.O., a.g.m., s. 159.

İHEB'in 1. m.'sinde*, "bütün insanların özgür ve onur ile haklar bakımından eşit olduğu"* ifade edilmiştir. Aynı belgenin 5. m.'sinde *"hiçbir insana işkence yapılamayacağı, insanlık dışı muamele ve onur kırıcı davranışta bulunulmayacağı ve bu yönde ceza verilemeyeceği"* belirtilmiştir. Yine benzer şekilde 22. m.'sinde ise "*herkesin onur ve kişiliğini serbestçe geliştirmek amacıyla gereken sosyal, ekonomik ve kültürel hakların gerçekleştirilmesi hakkına sahip olduğu"* vurgulanmıştır. 23. m.'sinde ise *"herkesin kendisi ve ailesi için insan onuruna yaraşır sosyal koruma tedbirleri ile desteklenen adil bir hayat ve ücret hakkına sahip olduğu"* düzenlenmiştir. Bununla birlikte AİHS'in 2. m.'sinde *"yaşam hakkı"*, 3. m.'sinde *"işkence yasağı"*, 4. m.'sinde "*kölelik ve zorla çalıştırılma yasağı"*, 5. m.'sinde *"özgürlük ve güvenlik hakkı"*, 7. m.'sinde *"suç ve cezanın şahsiliği"*, 8. m.'sinde *"özel ve aile hayatına saygı hakkı"*na dair yer verilerin düzenlemeler ile insan onuruna yakışır bir korumanın sağlanması amaçlanmıştır. Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesinin 17. m.'sinde de "*kimsenin insan onurunun hukuka aykırı şekilde gerçekleştirilen saldırılara maruz bırakılamayacağı*" ifade edilmiştir.[642]

3.3.2. T.C. ANAYASASI'NDA İNSAN ONURU

Uluslararası bu belgelerde insan onuru ile ilgili yukarıda yer verdiğimiz düzenlemeler ulusal anayasalara da yansımıştır.

1982 Anayasası'nın 2. m.'sinde *"Türkiye Cumhuriyeti insan haklarına saygılı bir hukuk devletidir."* ifadesi yer almaktadır. Yine 5. m.'sinde *"Devletin temel amaç ve görevleri"* madde kenar başlığı altında *"insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışma"* ifadesi ile devletin önemli bir görevinden bahsedilmiştir. Bu konuda, Anayasanın Başlangıç Bölümünün 6. paragrafında ise "*her Türk vatandaşının bu Anayasadaki temel hak ve hürriyetlerden eşitlik ve sosyal adalet gereklerince yararlanarak milli kültür, medeniyet ve hukuk düzeni içinde onurlu bir hayat sürdürme ve maddi ve manevi varlığını bu yönde geliştirme hak ve yetkisine sahip olduğu…tevdi olunur"* ifadelerine yer verilmiştir. Temel hak ve hürriyetler bölümünde yer alan 17. m.'nin 1.fıkrasında ise; *"herkesin*

642 Ayözger, a.g.e., s. 42.

hayata, maddi ve manevi varlığını koruma ve geliştirme hakkına sahip olduğu" ve aynı maddenin 3. fıkrasında *"kimseye işkence ve eziyet yapılamayacağı; kimsenin insan haysiyetiyle bağdaşmayan bir cezaya veya muameleye tabi tutulamayacağı"* düzenlenerek insan onuru ile ilgili anayasal güvence sağlanması hedeflenmiştir.

İnsan onurunu, AYM aldığı bir kararda; *"Kişinin maddi ve manevi varlığını geliştirme hakkı, insan onurunun korunmasını sağlayan bir güvencedir. İnsan onuru kavramı, insanın hangi durumda ve hangi şartlar altında olursa olsun sadece insan olmasının bir gereği olarak taşıdığı değerin tanınmasını ifade eder."*[643] şeklinde açıklamıştır. AYM yine bir başka kararında ise *"insanın hangi durum ve koşullar altında olursa olsun sırf insan oluşunun sağladığı değerin tanınmasını ve sayılmasını ifade eder. Bu öyle bir davranış çizgisidir ki bu çizgiden aşağı düşülmesi durumunda, söz konusu muameleye muhatap olan insan, insan olmaktan çıkar."*[644] şeklinde ifade etmiştir.

Modern veri işleme teknolojisi ve araçlarının gelişmesiyle kişilerin kişisel verilerinin hiçbir sınırlama olmadan toplanıp kullanılması, işlenebilmesi ve aktarılması işlemlerine karşı bireyi korumayı amaçlayan ve bireyin kendi kişisel verileri üzerinde karar verme hakkını teminat altına alan *kişisel verilerin korunması hakkı*, Anayasa Hukuku açısından esasen *"insan onuru"* bağlantısı ile maddi ve manevi kişiliği geliştirme hakkı ile temellendirilmektedir.[645] Daha önce defalarca değindiğimiz üzere, günümüzde gelişen bilgi teknolojileri aracılığı ile kişisel verilerin kolayca işlenebilmesi yüzünden, insan onurunun korunabilmesi için Gören'e göre anayasa hukuku açısından şu hususların göz önünde tutulması gerekmektedir:

- Kamu kurumları kanunla verilen görevi yerine getirmek için kişisel veri topluyorsa, ilgili kamu kurumu bu görevi ifa ederken sadece amacın gerçekleşmesine yarayacak ölçüde ve mümkün olduğunca az miktarda kişisel veri toplamalıdır.

643 AYM, E. 2012/7, K. 2012/102, T. 05.07.2012, R.G. 28433, Y.T. 06.10.2012.

644 AYM, E. 1963/132, K. 1966/29, T. 28 Haziran 1966; Ömer İZGİ/ Zafer GÖREN, "Türkiye Cumhuriyeti Anayasası Yorumu", Ankara, 2002, s. 216.

645 Şimşek, a.g.e., s. 112.

-veri sahibine, kendisiyle ilgili hangi kategorideki verinin toplandığı ve bunların hangi kurumda bulunduğu, hangi amaç ile bunların tutulup kullanılacağı bilgisi verilmelidir.

-idarenin bütünlüğü ilkesi gereğince, resmi makamlar birbirleri ile idari ve hukuki konularda yardımlaşırken bireylerin kişisel verileri korunarak temel hak ve hürriyetlerine saygılı davranılmalıdır.

- veri sahibinin izni ile bir resmi kurumdan diğerine kişisel veri aktarılması yapılabilmelidir.

-düzenleyici işlemlerle, kamu kurumlarının yerine getireceği görevin ifa edilmesi için gereken bilginin türü ve bu bilgilere hangi resmî kurumların ulaşabileceği belirlenmelidir. Bu yolla, bireyler, kişisel verilerinin hangi amaca hizmet edeceğini bilecek ve davranışlarını ayarlama imkânına sahip olacaklardır.

-bir resmi kurum kişiye ait özel verilerin devredilmesi hususunda hukuken korunan bir çıkar olduğunu ispatlayamazsa, bu kuruma veri aktarımının yapılması yasaklanmalıdır.[646]

3.3.3. İNSAN ONURU, KİŞİNİN MADDİ VE MANEVİ VARLIĞINI GELİŞTİRME HAKKI VE KİŞİSEL VERİLERİN KORUNMASI HAKKI

İnsan onuru, kişilerin iç alemlerinde kendilerini değerli hissetmelerini sağladığı için, bu değerli hissetmenin, başka bir kişinin davranışlarıyla yok olması ya da azaltılması, insanın kendisini değersizmiş gibi hissedip, bunun sonucunda da yaşaması ve kendisini geliştirmesi için gerekli olan itici gücü kaybetmesine yol açacaktır.[647]

Ayrıca insan onuru kişi hürriyetlerinin temeli ve eşitliğinin de ölçütü olarak görülmektedir. Mutlak eşitlik ilkesinden faydalanmakta olan *insan onuru*, insan hak

646 Gören, "Anayasa Hukuku", s. 456.

647 Avşar, B. Zakir / Gürsel Öngören, "Radyo ve Televizyon Hukuku", Ankara, 2003, RTÜK Yayın No: 3, s. 89.

ve özgürlüklerinin ortak temeli olup[648], insan onuruna saygı duyulmasının sağlanması ile, düzenin merkezinde bulunan insanın bağımsızlığı ve yine insanın ilk ve en temel hakkı olarak görülen kişilik haklarının korunması hedeflenmektedir.[649]

Yukarıda da belirttiğimiz gibi, insan haklarının temelinde insan onuru bulunduğu gibi, kişisel verilerin korunması hakkının temelinde de insan onuru bulunmaktadır. Hukuka aykırı olarak kişisel verilerin işlenmesi, veri ilgilisinin kendi geleceğini belirleyebilmesi hakkının ve insan olarak sahip olduğu değerlerin ihlal edilmesi sonucunu doğuracağı için, kişisel verilerin hukuka aykırı olarak işlenmesinin önüne insan onurunun korunması ile geçilebilir.

Anayasal bir hak olan "*insanın maddi ve manevi varlığını geliştirme hakkı"* kaynağını hak ve özgürlüklerin ortak temeli olan insan onurundan alsa[650] da insan onurunun tanımlanması çok da kolay bir kavram değildir. Bu bağlamda, Federal Almanya Anayasa Mahkemesi insan onurunun ihlal edilip edilmediği yönündeki değerlendirmesinde "obje formülü"nü kullanmıştır. Yani, insanın kamu erkinin işlemleri karşısında basit bir araç veya obje haline indirgenmiş olduğu durumlarda insan onurunun ihlal edildiğinden söz edilebilecektir.[651]

Federal Almanya Anayasa Mahkemesi tarafından kullanılan *"obje formülü"* kişisel verilerin korunmasının anayasal dayanağı ve önemi konusunda ayrıca fikir de vermektedir. Zira, teknolojinin gelişmesi ile kişilerin farklı kaynaklardan devamlı olarak gözetimi kişilerin bireysel özerkliğinin kaybına neden olabileceği gibi, ayrıca otomatik karar alma süreci ile yaşamına yön verilmek istenen kişinin bir özneden bir nesneye doğru evrilmesi ihtimali de söz konusudur. Oysa öncelikle kişinin kendisi, kendisine ilişkin bilgileri, ne zaman, nasıl, ne kadar ve kimlere açıklayacağına karar verebilmelidir. Zira, bu konularda karar verme yetkisini kaybeden kişi özneden nesneye doğru dönüşeceği gibi, maddi ve manevi varlığını geliştirebilme hakkını da kaybedecektir. Her ne kadar kişisel verilerin korunması hakkı dokunulmaz bir hak

---

648 Kaboğlu, "Anayasa Hukuku", s. 25.

649 Gören, Zafer, "Avrupa Birliği Temel Haklar Şartının Ana İlkesi: Dokunulmaz İnsan Onuru", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Yıl: 2007, Cilt: 6, Sayı: 12, s. 24.

650 Kaboğlu, a.g.e., s. 25.

651 Şimşek, a.g.e., s. 130.

olmayıp, belirli durumlarda sınırlandırılabilecekse de bu durumların *"belirli"* olması bu konuda kilit unsurdur. Bireyin hangi şartlarda hakkının sınırlandırılacağını bilmesi, bu sınırların ise meşru bir temele dayanması gereklidir. Bu yolla kişi, kendisine ait kişisel veriler konusunda karar verme güç ve yetkisini elinde tutmaya devam edebilecektir.[652]

Kişisel verilerin korunması hakkı ile günümüzde gelişen bilişim teknolojileri ile kişisel nitelikteki bilgileri sınırsızca toplanılan, kullanılan, aktarılan kişilerin korunmasının sağlanması hedeflenmektedir. Bu kapsamda "*kişisel verilerin korunması hakkı"*nın ilk önce *"insan onuru"* ve bu kapsamda da *"kişiliğin serbestçe geliştirilmesi hakkı"*na dayandırıldığı görülmektedir.[653]

Almanya Anayasa Mahkemesi 1983'te verdiği Nüfus Sayımı (Volkszahlung) kararında bu durumu vurgulamıştır. Bu karara göre, demokratik toplum yapısının özgür bir üyesi olan kişinin onuru, anayasal düzenin merkezinde yer alır. Günümüzdeki teknolojik gelişmelere paralel bir şekilde baş gösteren tehlikeler karşısında bireyin kişiliğinin korunması özel bir anlam kazanmaktadır. Bireyin hakkında toplanılan bilgilerin hangileri olduğu ve kimin bu bilgileri elinde tuttuğunu öğrenme imkânına sahip olmaması halinde, bireyin kararlarını kendisinin verebilmesi özgürlüğü ciddi bir biçimde zarar görmüş olacaktır. Bilhassa otomatik veri işleme cihazları ile verilerin sınırsızca kaydedilebilmesi, bu verilerin her zaman erişilebilecek türden olması ve bireyin detaylı kişilik profilinin oluşturulabilme ihtimali da göz önüne alındığında, kişinin üzerinde psikolojik baskı kurulması ve onun kamusal yaşama katılımını etkilemesi söz konusu olabilecektir. [654] Örneğin, resmi makamlar tarafından toplantı, sivil toplum örgütlerine veya gösteri yürüyüşlerine katılmasının kaydedildiğini ve bu tür faaliyetlerinden dolayı bazı mağduriyetler yaşayabileceğinden endişe eden bir kişi bu hakları kullanmak konusunda çekince yaşayabilir. Bu durum ise, kişinin kendi kişiliğini geliştirme hakkına zarar vereceği gibi kamu menfaatlerine de zarar verecektir. Çünkü, özgürlükçü bir demokrasinin işleyebilmesi için topluma katılabilme ve toplum içerisinde işlev görebilme becerisinin gelişmesi gereklidir.

652 Küzeci, a.g.e., s. 288.

653 Küzeci, a.g.e., s. 75.

654 Küzeci, a.g.e., s. 76.

Bundan dolayı, bireyin kişiliğin özgürce gelişmesi ve demokratik toplum düzeninin sürekliliğinin sağlanması için devletin kişisel verileri toplaması, kaydetmesi, kullanması ve aktarması işlemlerine karşı bireyin korunması zorunluluk arz etmektedir. Çeşitli yaşam ilişkilerinin ortaya çıkacağı zamana ve bunun sınırlarına bireyin kendisinin karar verebilmesi gereklidir. Zira, "*bilgilerin geleceğini belirleme hakkı"* ilke olarak bireyin kendine ait kişisel verileri hakkında tasarruf yetkisinin bulunmasını gerektirmektedir.[655]

Sürekli olarak izlenip, yaşamına dair bilgileri kayıt altına alınan, bunların sonucunda ise neredeyse şeffaflaşmış olan bireyin kendi kişiliğini özgürce geliştirebilmesi mümkün değildir. Böyle bir ortamdaki bir kişinin, kendinden beklenen davranış kalıplarına göre hareket ederek, toplum yaşamında kişiliğini serbestçe oluşturamaması ihtimali söz konusu olabilecektir. Bu açıdan kişisel verilerin korunması hakkı, kişisel verilerinin hukuka aykırı olarak ve hiçbir sınırlama olmadan kaydedilmesi, işlenmesi, paylaşılması karşısında kişiye temel bir hak sağlayarak kişiyi sıradan bir veri objesi olmaktan kurtarmaktadır.[656]

İnsanın, devlet için istenilen zamanda ve biçimde erişilebilecek sıradan bir veri nesnesi gibi görülerek alçaltılması, kişisel verilerinin korunması hakkını ihlal ettiği gibi, ayrıca özel hayatın gizliliğini de ortadan kaldırmaktadır. Bu ihlaller ile bireyin insan onuru aracılığıyla sahip olduğu öz değerin hiçe sayılması sonucu doğar ki; bu husus insan onuru ile bağdaşmaz. Bunun yanında yine devletin, insana bir eşya gibi davranma ve insan kişiliğini kayıt altına alma hak ve yetkisini kendisinde görmesi de insan onuru ile bağdaşamayacaktır.[657] Özetle, verilerin geleceğini belirleme hakkı, bireye verilerinin kullanılması hakkında karar verme yetkisi tanır. Görüldüğü üzere özel hayatın gizliliği hakkı ve dolayısı ile de kişisel verilerin korunması hakkı kaynağını öncelikli olarak bireysel özerklik, kişilik hakkı ve insan onurunda bulmaktadır.[658]

---

655 Schomerus, Rudolf, Bundesdatenschutzgesetz Kommentar, Beck, Almanya, 2007, s. 77, (aktaran, Küzeci, a.g.e., s. 77).

656 Şimşek, a.g.e., s. 112.

657 Şimşek, a.g.e., s. 130 vd.

658 Küzeci, a.g.e., s. 95.

3.4. KİŞİSEL VERİLERİN KORUNMASI HAKKINI KORUYAN DİĞER TEMEL HAK VE ÖZGÜRLÜKLERİN KISMİ GARANTİLERİ

Kişisel verilerin korunması hakkı, başka hak ve özgürlüklerle kimi zaman karşılıklı destekleme, kimi zaman da çatışma şeklinde olmak üzere yakın ilişki halindedir.[659] Bu başlık altında kişisel verilerin korunması hakkının yakın ilişki içinde olduğu haklardan bazılarını incelemeye çalışacağız.

3.4.1. DİN, VİCDAN VE İNANÇ ÖZGÜRLÜĞÜ VE KİŞİSEL VERİLERİN KORUNMASI

Din ve inanç kavramları, insanlığın başından beri tartışılan, her devirde farklı pozisyonlar alabilen, kişilerin siyasi ve toplumsal tavırlarında, ahlaki yaklaşımlarının biçimlenmesinde etkili görev alan bir kavramdır. Bundan dolayı, kişilerin özgürce inanma veya inanmama ve de inandığı gibi yaşama haklarının bulunması gayet tabiidir.[660]

"Din özgürlüğü" insanlara önerilen dinler arasından bir dini tercih etme veya etmeyip inançsız kalma hakkında tercih özgürlüğü ile, eğer katılmayı tercih ettiği bir din varsa bu dinin gereklerini yerine getirme konusunda özgür olma olarak tanımlanabilir.[661]

Din ve vicdan hürriyeti, herkes açısından tüm hürriyetlerin en kutsal olanı olarak nitelendirilmese bile insanların çoğu için temel mahrem özgürlüklerden biri olup[662] insanın sadece insan olması nedeni ile sahip olduğu evrensel nitelikteki insan haklarındandır.[663]

Uluslararası belgelerdeki düzenlemeler göz önünde bulundurulduğunda, din hürriyetinin temel unsurları; kişinin bir dine girmeyi istemesi, dinini değiştirmeyi

---

659 Küzeci, a.g.e., s. 60.

660 Aslan, Zühtü, "Avrupa İnsan Hakları Sözleşmesinde Din Özgürlüğü",Ankara, 2005, Liberal Düşünce Topluluğu, s. 1.

661 Kaboğlu, "Anayasa Hukuku", s. 293.

662 Nal, Sabahattin "Avrupa İnsan Hakları Sözleşmesi Çerçevesinde Düşünce, Vicdan ve Din Özgürlüğü" AÜSBFD, C. 57, S. 4, Y.2002, s. 66.

663 Arslan, Z., a.g.e., s. 1.

istemesi halinde değiştirebilmesi, inandığı dinini veya inancını ibadetleri aracılığıyla ortaya koyabilmesi, din eğitimi yapabilmesi ve dine ait görenekleri yerine getirebilmesini içerir.[664]

Din özgürlüğü, devletin olası müdahalesi ve dini konulardaki tahakkümü karşısında bireyi korumayı hedefleyen bir haktır. Zira devletin bu konuda tarafsız olma mecburiyeti söz konusudur. Bu nedenledir ki, bu hak *"olumsuz statü hak grubu"*ndadır.[665] Bunun yanında, akıl ve bilime dayalı olarak yönetilen ve laik olan çağdaş ve modern devletlerde dinlerden birinin diğer dinlere karşı üstün pozisyonda tutulması söz konusu olamayacağı için, farklı dini inançlara sahip bulunan kişiler hukuk önünde eşittirler. Ayrıca, laik bir devlette, kamu düzeni bozulmadığı müddetçe, farklı dinlerdeki kişilerin ibadet hürriyetine müdahale etmez; buna gereken saygıyı gösterir.[666]

AİHM din, vicdan ve inanç özgürlüğüne devlet tarafından yapılacak müdahale ve sınırlandırmada üç şartın gerçekleşmesi gerektiğini ifade etmektedir. Bu şartlardan birincisi, bu hakka yapılacak müdahalenin kanunla yapılmasıdır. İkincisi, müdahale ve sınırlandırma için meşru bir amacın bulunmasıdır. Söz konusu müdahalenin demokratik bir toplumda zorunlu olması ise bu şartların üçüncüsüdür.[667]

AİHM Kokkinakis/Yunanistan kararında[668]; Sözleşmenin 9. m.'si koruma altına alınan "*düşünce, din ve vicdan hürriyeti*"nin *"demokratik toplum"*un temel unsurlarından birisi olarak belirtip; söz konusu hürriyetin dini yönüyle, herhangi bir dine inanan insanların kimlik ve yaşam tarzlarını şekillendiren en önemli öğelerden biri olmasının yanı sıra, ateist, septik ve herhangi bir dini benimsemeyen kişiler açısından da anlam ifade ettiğini vurgulamıştır. Bu nedenle başvurucunun başka kişileri kendi inancına inandırmaya çalışması nedeniyle başvurana verilen cezanın,

664 Nal, a.g.m., s. 67.

665 Nal, a.g.m., s. 66.

666 Akgüner, a.g.m., s. 26.

667 David, Haris / Michael O'Boyle, Colin Warbrick, Carla Buckley, "Law of the European Convention on Human Rights", New York, 2013, Oxford University Pres, 2th Edition, s. 435 vd.

668 AİHM Kararı: Kokkinakis v Yunanistan, Başvuru No: 14307/88, Tarih: 25.05.1993. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-57827, Erişim tarihi, 08.05.2019.

ulaşılmak istenen legal amaçla orantılı ya da *"başkalarının hak ve hürriyetlerini korumak için… demokratik toplumda düzenlerinde gerekli"* bulunmadığına hükmetmiştir.[669]

Kişisel verilerin korunması hakkı yönünden din, vicdan ve inanç özgürlüğü değerlendirilecek olursa, din veya inanca dair olan verilerin belirli veya belirlenebilir bir kişiyle irtibatlandırılmaları durumunda bu veriler kişisel veri haline dönüşürler. Bireyin din veya inancına dair veriler özel olarak korunmaktadır. Çünkü, bu veriler, verilerin korunması hukukuna göre hassas nitelikli veriler olarak kabul edilmektedirler.[670] Bu nedenle din, vicdan ve inanç özgürlüğü ile kişisel verilerin korunması hakkının birbirini destekler nitelikte hak ve özgürlükler olduğu çıkarımı yapılabilir.[671]

3.4.2. ÖZEL HAYATIN GİZLİLİĞİ İLKESİ VE KİŞİSEL VERİLERİN KORUNMASI

3.4.2.1. Genel Olarak

Özel hayatın, kişinin mutlak bir şekilde diğer insanlardan gizli tuttuğu yaşam parçaları ile diğer insanların bilmesini uygun görmediği, sadece kendi seçtiği kişilerle ve belli ölçü ve şekilde paylaşacağı yaşam parçalarının toplamda oluşturdukları yaşam alanı olarak tanımlanması mümkündür.[672] Kişiliklerinin gelişmesine ve başka kişilerin kendileri için hangi anlamı taşıdığının anlaşılmasını sağladığı için kişiler özel hayatlarına değer vermektedirler.

İHEB, Medeni ve Siyasi Haklar Sözleşmesi ve pek çok bölgesel düzeyde veya uluslararası nitelikteki insan hakları antlaşmalarında özel hayatın gizliliği hakkı

669 Arslan, Z., a.g.e., s. 107 vd.

670 Şimşek, a.g.e., s. 139.

671 "Anayasa Mahkemesi nüfus kütüğünde kişilerin dininin bir veri olarak kaydedilmesine imkân veren 5.5.1972 tarihli ve 1587 sayılı Nüfus Kanunu'nun 43. maddesindeki "dinini" kelimesinin Anayasa'nın 2. ve 24. maddesine aykırılığı ileri sürülerek iptali talebiyle yapılan başvuru hakkında verdiği kararda "...dinini..." sözcüğünün Anayasa'ya aykırı olmadığına karar vermiştir.",http://kararlaryeni.anayasa.gov.tr/Karar/Content/0314984f-1d85-42a5-b3f3-3d5a0b874c83?excludeGerekce=False&wordsOnly=False, Erişim tarihi: 28.11.2019.

672 Araslı, Oya, "Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi", Ankara, 1979, s. 4

korumaya alınmıştır. Yine pek çok ülke anayasasında özel hayatın gizliliği hakkına dair düzenlemelere yer verilmiştir.[673]

Kişinin özel hayatının genellikle üçe ayrılarak incelendiğini, bu alanların *"kamuya açık alan"* (ortak alan), *"özel alan"* ve *"sır alanı"* (gizli alan) olduğunu çalışmamızın 2. bölümünde açıklamaya çalışmıştık. Bunlardan *"giz alanı"*, kişilik hakkının dokunulamayan alanı olarak, kamusal tüm müdahalelere kapalı olan bir alan iken, *"sır alanı"* ise, dokunulamayan iç alan olarak iletişime kapalı olan bir alandır.[674] Sır alanı kişinin sadece kendisine ayırmayı tercih ettiği alanı oluşturmaktayken *"kişinin özel hayat alanı"* ise kişinin paylaşmayı tercih ettiği belli kimselerle ve belli ölçüde paylaştığı hayat parçalarını kapsar.[675]

Günümüz modern devletleri, kişilerin özel hayatları ve kişilikleri ile ilgili pek çok bilgiyi ellerinde bulundurmaktadırlar. Ancak, bu bilgilerin başka kimselerin eline geçmesi, kişinin temel hak ve özgürlüklerinin ve özel hayatının tehdit veya ihlal edilmesine yol açabilir. İşte bu konuda "*gizlilik"* özel hayatın ve bununla bağlantılı olarak da kişiliğin korunmasında bir aracı olarak hizmet eder.[676]

Kişinin özel hayatının kişinin etrafına açılma derecesi, bunun istifade edeceği korumanın miktarı ve şekliyle alakalıdır. Zira, cinsel hayat, dinsel tercihler ve ırksal köken gibi kişinin sır alanı içinde olarak değerlendirilen hususlara ilişkin kişisel veriler hassas kişisel veri kategorisinde kabul edilerek daha nitelikli ve özel bir koruma altına alınırlar. Nitekim, yine belirli prensiplere uyulması şartıyla, kişinin özel yaşam alanına müdahale edilebilmesi için üstün kamu yararının varlığı zorunludur.[677]

Özel hayatın gizliliği hakkı temel bir insan hakkı olup, insan onuru, düşünce hürriyeti ve dernek kurma özgürlüğü gibi diğer hak ve değerleri de anlamlandıran bir kavram olduğu gibi, günümüzde en önem verilen insan haklarından birisidir.[678] Özel

673 Electronic Privacy Information Center, Privacy&Human Rights: An International Survey of Privacy Laws and Developments Washington, D.C., 2004, s. 1.

674 Şimşek, a.g.e., s. 141.

675 Küzeci, a.g.e., s. 71.

676 Döner, "Şeffaf Devlet", s. 76.

677 Küzeci, a.g.e., s. 72.

678 Privacy&Human Rights, a.g.e., s. 1.

hayatın gizliliği hakkının çok yönlü bir hak olması nedeni ile, teknolojik gelişmelere ayak uydurmasına ihtiyaç vardır.[679] Temelini bireyin gücünden alan bu hak, bireyin özel alanının muhafaza edilmesinden, özgür karar verebilmesine, bireysel özerklikten kişisel verilerin korunmasına kadar pek çok hususu kapsamına almaktadır. Mesela, kişinin mektupları ve fotoğrafları gibi özel şeyleri, cinsel eğilim ve tercihleri, kurduğu özel ilişkileri gibi bilgileri, konutu gibi özel alanı özel yaşamın gizliliği hakkının koruma alanı içindedir.[680]

Özel yaşamın gizliliği hakkına bir müdahale veya sınırlama yapılması söz konusu ise, ilk olarak bu sınırlamanın *"kanunla"* yapılması gerekir. Özel hayatın gizliliği hakkına dair yapılan bu düzenlemenin, bireyler tarafından erişilebilir olması, müdahalenin koşulları ve neticeleri yönünden anlaşılabilir ve açık olması gerekir. İkinci olarak, özel hayatın gizliliği hakkına yapılacak bu müdahale ile *"meşru bir amaç"* hedeflenmelidir. AİHS madde 8'de meşru amaç olarak şu kriterler belirlenmiştir: *"sağlığın ve ahlakın korunması",* "*kamu güvenliği", "suç işlenmesinin önlenmesi", "milli güvenlik", "dirlik ve düzenin korunması", "ülkenin ekonomik refahı"*. "*Müdahalenin demokratik bir toplumda gerekli olması"* şartı ise bu hakka yapılacak müdahale ve sınırlamanın üçüncü şartıdır.[681]

3.4.2.2. Avrupa İnsan Hakları Mahkemesi Uygulamasında Özel Hayatın Gizliliği Hakkı

Özel hayatın tanımı teknolojik gelişmeler ve oldukça rağbet gören liberalizmin karşısında zamanla yetersiz kalmaya başlamıştır. Bundan dolayı AİHM, her somut olayın özelliklerini ve koşullarını dikkate alarak konuya yaklaşmakta, bu yolla zamanın ve olayın şartlarına göre geliştiren ve ileriye taşıyan bir yorumla bu kavrama belli bir içerik kazandırmayı başarmaktadır.[682]

AİHM'nin AİHS uygulayıcısı olarak, özel hayatı tanımlamaktan özellikle kaçındığını, ancak bu yöndeki çeşitli kararlarında '*özel hayat*'ın '*giz alanı*'ndan daha

679 Jayawickrama, a.g.e., s. 602.

680 Room, a.g.e., s. 4.

681 Güntürk, M. Serdar, "Türk Yüksek Mahkemeleri ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Özel Hayatın Gizliliğinin Korunması", Ankara, 2012, s. 116.

682 Polater, Yusuf Ziya, "Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesinde Özel Hayatın Gizliliği ve Korunması", Ankara, 2010, s. 121.

kapsamlı olduğunu vurgulayarak, özel hayat kavramının tanımlanmasının mümkün ve gerekli olmadığını ifade ettiğini ve AİHM'nin bu konudaki değerlendirmelerini çalışmamızın ikinci bölümünde açıklamaya çalışmıştık. AİHM'nin özel hayatın gizliliği hakkında yaptığı açıklamaların yer aldığı Niemietz v. Almanya kararına yine kısaca değinmek gerekirse; AİHM bu kararında, kişinin özel hayatının, hayatın iç alanıyla sınırlandırılmaması gerektiği, dış dünyanın iç alandan tamamen ayrılamayacağı vurgulanmış, bireyin çeşitli ilişkiler kurabilmesi ile bu ilişkileri geliştirme hakkının da özel hayat kavramı içinde olduğu değerlendirilmesi yapılmıştır.

Özel hayatın gizliliğine yapılan müdahalenin hukuka uygun olması gerektiği yönündeki AİHS'nin 8. m.'sindeki düzenleme, AİHM tarafından, bu hakka getirilecek sınırlamanın veya yapılacak müdahalenin açık bir yasal düzenlemeye dayandırılmasının zorunlu olması şeklinde kabul edilmektedir.[683] Polisin yaptığı telefon dinlemelerinin hukuka aykırı olduğu iddiasına ilişkin Malone v. Birleşik Krallık davasında[684] AİHM; telefon dinlemeleri konusunda kamu idaresine takdir yetkisi tanındığına dair söz konusu kanunda uygun, hukuki bir belirlilik bulunmadığı gerekçesi ile başvurucunun sözleşmenin ihlal edildiği iddiasının makul olduğuna karar vermiştir.[685]

AİHM tarafından verilen çeşitli kararlarda, kişisel verilere yetkili olmadan erişim sağlamak, kişisel verilerin gerekli olduğundan uzun süre sistemde saklanması gibi "*kişisel verilerin korunması hakkı"* kapsamına giren alanlara "*özel hayatın gizliliği"* ilkesin dair ilkeler uygulanmıştır.[686]

3.4.2.3. Özel Hayatın Gizliliği ve Kişisel Verilerin Korunması Hakları Arasındaki Temel İlişki

1948 tarihli Evrensel İnsan Hakları Bildirgesi modern anlamda ve uluslararası düzeyde kişinin özel hayatının gizliliği hakkı konusunda dönüm noktasıdır. Kişinin

683 Richard, Stone, "Civil Liberties and Human Rights", Büyük Britanya, 2002, Oxford University Pres., s. 166.

684 AİHM Kararı, Malone v. Birleşik Krallık, Başvuru No: 8691/79, Tarih: 02.08.1984.

685 Stone, a.g.e., s. 166.

686 Küzeci, a.g.e., s. 74.

hayatının ve iletişiminin gizliliği bildirgede özel olarak koruma altına almıştır.[687] 1950'de kabul edilen AİHS'de sadece özel hayatın gizliliği hakkına ilişkin düzenlemeye yer verilmişken, AB Temel Haklar Şartı'nda kişisel verilerin korunması hakkı ile özel hayatın gizliliği hakkı değişik maddelerde birbirinden ayrı olarak ele alınmıştır. 1988'de BM İnsan Hakları Komitesi tarafından yayımlanan yorumda, kişisel verilerin korunmasına dair temel prensiplerin, Medeni ve Siyasi Haklar Sözleşmesi'nin özel hayatın korunmasına dair olan 17. m.'si göz önünde bulundurulmak suretiyle ele alınması gerektiği belirtilmiştir.[688]

Negatif statü haklarından olan kişisel verilerin korunması hakkı, özel hayatın gizliliği hakkının ayrılmaz bir parçası olarak özel hayatın korunmasında önemli bir yere sahiptir.[689]

Kişisel verilerin korunması hakkının, özel yaşamın gizliliği hakkının iyi bir şekilde uyarlanmış şekli olarak görüldüğündendir ki,[690] pek çok ülkede, özel hayatın gizliliği hakkının tanımlanması esnasında kişisel verilerin korunması ile ilişki kurularak,[691] *"kişisel verilerin korunması hakkı"*nın, *"özel hayatın gizliliği hakkı"*nın kendine has nitelikleri bulunan bir çeşidi olduğu ve bu haklar arasında yakın bir ilişki olduğu kabul edilmektedir. Zira, Kanada, ABD, Avustralya, Yeni Zelanda gibi bazı devletlerde özel hayatın gizliliği ilkesi kapsamında kişisel verilerin korunması hakkına ilişkin düzenlemelere yer verilmiş olması bunun en önemli kanıtıdır.[692]

Kişisel verilerin korunması hakkı ile özel hayatın gizliliği ilkesi arasında belirgin farklılıklar var ise de her iki hakkın temel çıkış noktalarının örtüştüğü açıktır. Bunun yanında kişisel verilerin korunması hakkıyla alakalı mahkeme kararları, zorunlu bir şekilde kişinin özel yaşamına ilişkin hususlarda daha kapsamlı soruların sorulmasına yol açmıştır. Mesela; Almanya Anayasa Mahkemesi tarafından verilen, nüfus sayımına ilişkin kararda, hükümete ülke genelinde yapılan nüfus sayımlarında

687 Privacy& Human Rights, a.g.e., s. 1.
688 Küzeci, a.g.e., s. 74-75.
689 Kılınç, a.g.m., s. 1099.
690 Room, a.g.e., s. 7.
691 Privacy& Human Rights, a.g.e., s. 1.
692 Küzeci, a.g.e., s. 70.

çeşitli yetkiler sağlayan yasanın anayasaya aykırı olduğu yönünde karar vermiş; mahkeme her bir veri sahibinin kişisel verilerinin kullanılması ve açıklanması konusunda karar verme hakkının bulunduğunu ifade etmiştir. Kişilere haklarındaki verilerin geleceğini tayin etme hakkı veren bu karar, Almanya'daki kişisel verilerin korunmasına dair çıkarılmış olan kanunda radikal değişiklik yapılmasına neden olmuştur.[693]

Kişisel verilerin korunması hakkının kapsadığı alanın, özel hayatın gizliliği hakkının kapsadığı alandan çok daha dar olduğu ifade edilerek,[694] özel hayatın gizliliğinin korunması hakkının, kişinin özel bilgilerinin ele geçirilmesi amacıyla potansiyel olarak müdahale edilmesi durumunun gerçekleşip gerçekleşmediğine bakılmadan, bireyin maddi ve manevi bütünlüğünü koruduğu hususu bu konuda örnek olarak gösterilmektedir.[695]

Doktrinde özel hayatın gizliliği ilkesini inceleyen şu 4 temel görüş vardır:[696]

- Bireyin kişisel verilerinin gizliliği,
- Fiziki ve bedensel bütünlüğünün gizliliği,
- İletişiminin gizliliği,
- Hayatının gizliliği.

"Bireyin kişisel verilerinin gizliliği" aynı zamanda *"kişisel verilerin korunması"* olarak da bilinmekte olup, kişilerin sağlık ve idare ile ilgili kayıtları, kredi bilgileri gibi kişisel verilerinin ele geçirilmesi, toplanması ve bu verilerin yönetimini kapsamaktadır.[697] *Kişinin fiziki ve bedensel bütünlüğünün gizliliği* ise, ilaç testleri, genetik testler vs. bireyin bedensel bütünlüğüne yapılabilecek müdahalelere karşı

693 Chris, Reed, John Angel, " Computer Law", Oxford University Press, New York, 2003, s. 420.

694 Küzeci, a.g.e., s. 74.

695 Deryck, Beyleveld/ David Towned, Segolene/ Rouille- Mirza and Jessica Wright, a.g.e., s. 25.

696 Privacy &Human Rights, a.g.e., s. 3.

697 Lawrence, Karen Oqvist, "Virtual Shadows: Your Privacy in the Information Society", Swindon 2009, s. 111.

bireyin güvence altına alınmasıyla alakalıdır.[698] Bireyin posta, telefon, elektronik posta ve diğer iletişim cihazlarıyla sağladığı iletişiminin gizli kalması ve güvenliğinin sağlanması *bireyin iletişiminin gizliliği* olarak ifade edilir.[699] *Bireyin hayatının gizliliği* ise, bireye karşı kamusal alanda ya da iş ortamında çevreden ve toplumdan gelmesi muhtemel müdahalelerin ve sınırlamaların düzenlenmesiyle alakalı olup, araştırmalar, kimlik sorgulamaları ve kamera kayıtları bu kapsamda değerlendirilmektedir.[700]

İlgili kişinin rızası alınmadan ve hukuka aykırı bir şekilde, kişinin özel alanı içinde yaptığı konuşmalarının kaydedilmesi, telefon konuşmalarının dinlenilmesi, özel yaşamın gizliliğinin ihlali olacağı gibi, dolayısıyla kişisel verilerin korunması hakkına müdahale edilmesi anlamına da gelecektir.[701]

Birçok menfaat özel hayatın gizliliği hakkında birbiriyle rekabet etmektedir. Hukukun görevi ise birbiri ile rekabet halindeki bu menfaatler arasında en uygun olan dengeyi yakalamaktır.[702] [703]

Kişisel verilerin korunması hakkına ilişkin bazı ilkeler AİHM tarafından AİHS'nin 8. maddesinin koruma alanı içinde değerlendirilmektedir. Buna göre;

---

698 Privacy &Human Rights, a.g.e., s. 3.

699 Lawrence, a.g.e., s. 111.

700 Privacy &Human Rights, a.g.e., s. 3.

701 Şimşek, a.g.e., s. 143.

702 Room, a.g.e., s. 5.

703 Danıştay 10. Dairesinin 20/02/2018 tarihli ve 2015/2696 esas ve 2018/776 karar sayılı kararında "... davacı sendika tarafından, davalı idarenin taşra birimlerinde görev yapan personelin izlenmesini teminen odalarına monitör yerleştirildiği ve kamera kayıt sisteminin kurulduğu, güvenlik amacıyla binaların girişlerine yerleştirilenler dışında çalışanların birimlerde (odalarda) izlenmesine imkân veren kamera sisteminin kişi mahremiyetini ihlal edeceği ileri sürülerek, personelin izlenmesine imkân veren kamera sisteminin kaldırılması talebiyle 5/12/2013 tarih ve 825 sayılı dilekçeyle yapılan başvurunun zımnen reddine yönelik davalı idare işleminin iptali istemiyle açılmıştır. Kameralı takip sistemi ile kurumca amaçlanan kamu yararı arasında orantılılık bulunmadığından uygulama ölçülülük ilkesine de aykırılık teşkil etmektedir. Anayasa'nın 13. maddesinde, temel hak ve hürriyetlerin ancak kanunla sınırlanabileceği, değişik 20/3. maddesinde de, kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğinin belirtildiği, ancak konuyla ilgili dava konusu işlemin gerçekleştirildiği aşamada yasal bir düzenlemenin yapılmadığı anlaşılmaktadır. Kamera takip sisteminin kurulmasının özel hayatın gizliliğini ihlal ettiği ve bu haliyle yukarıda belirtilen temel haklar ve Anayasal ilkelerle bağdaşmaması nedeniyle dava konusu işlemin iptaline karar verilmesi gerekirken davanın reddi yolunda verilen mahkeme kararının hukuka aykırı olduğu" nedeniyle bozmuştur. https://www.danistay.gov.tr/upload/yayinlar/12_03_2014_104214.pdf, Erişim tarihi: 17.12.2019.

bireyin kişisel verilerinin kamu kurumları tarafından toplanıp arşivlenmesi, elde edilen kişisel verilerin toplanılma amacından başka amaçlar için kullanılması, sağlık verilerinin gizli tutulması, emniyet güçleri tarafından kişinin parmak izinin alınması ve fotoğraflarının çekilmesi, kişisel verilere erişebilme hakkı, kişisel verilerin amacın gerçekleşmesi için gerekenden uzun süre tutulması gibi hususlar AİHM'nin çeşitli içtihatlarında sözleşmenin 8. m.'si kapsamında yorumlanmıştır.[704]

3.4.3. BİLGİ EDİNME HAKKI VE KİŞİSEL VERİLERİN KORUNMASI

3.4.3.1. Genel Olarak

Normatif temelini ifade özgürlüğünden alan "*bilgi edinme hakkı"*[705] düşünce ve ifade özgürlüğünün ön şartı olduğu gibi aynı zamanda demokratik bir toplumun temel niteliklerinden birini de oluşturmaktadır.[706] Düşünce özgürlüğü sağlanmadan ifade özgürlüğünden bahsedilemeyeceği gibi, bilgi edinme hakkının kesin olarak güvence altına alınması kişide bir düşüncenin oluşabilmesi için zorunludur.[707] Zira, çağdaş demokrasilerde, özgür haber ve bilgi dolaşımının sağlandığı bir ortamda bilgi edinme hakkı, demokratik sistemin aksamadan işlemesinin vazgeçilmez bir şartı olarak değerlendirilmektedir.[708]

İfade özgürlüğü kapsamında bir hak olarak, ifade özgürlüğünün tanınması ve anayasal düzenlemelerde yer almasının oldukça uzun tarihsel bir geçmişe sahiptir. Amerika'da ortaya çıkan 1786 Virginia Bildirgesi ve Avrupa'da ortaya çıkan 1789 Fransız İnsan ve Yurttaş Hakları Bildirgesi, ifade hürriyeti konusunda söz edilecek ilk anayasal nitelikli evrensel düzenlemelerdendir.[709]

---

704 Küzeci, a.g.e., s. 142.

705 Soykan, Cavidan, "Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Yıl: 2007, Sayı: 2, C. 56, s. 63.

706 Gemalmaz, M. Semih/ Gemalmaz, Haydar Burak,"Ulusalüstü İnsan Hakları Standartları Işığında Türkiye'de Bilgi Edinme Düşünce- İfade ve İletişim Mevzuatı", İstanbul 2004, s. 248

707 Yaşamış, Firuz Demir,"Anayasa Hukuku ve İnsan Hakları Açısından Bilgi Edinme Hakkı", Türk İdare Dergisi, Yıl: 2004, S. 444, s. 12.

708 Can, Azer, "Bilgi Edinme Hakkı", Ankara, 2010, Yetkin Yayınları, s. 193.

709 Yaşamış, a.g.m., s. 4.

Bilgi edinme hakkı genel anlamda; "*idarenin tuttuğu bilgilere ulaşabilme hakkı"*[710] olarak tanımlanabilir ve bireyleri idarenin eylem ve işlemleri ile, yetkileri hakkında bilgi sahibi yapmak suretiyle bireylerin toplumu ilgilendiren bilgileri edinmelerine, idare tarafından alınan kararları sorgulayabilmelerine olanak tanımakta ve böylece kamu hizmetlerinin daha etkili bir biçimde yürütülmesini teminat altına almaktadır.[711]

Bu yönü ile bilgi edinme hakkı; idarenin eylem ve işlemleri ile kararları hakkındaki bilgilere ulaşma olgusu iken, bu olgu, zamanla idarenin elinde bulunan bilgi ve belgelere ulaşmaktan kamusal bir hakka evrilmiştir. Bilgi edinme hak ve özgürlüğü, esasen bireylerin, kamusal organların işlem, davranış ve tutumları hakkında bilgi edinme gereksiniminden doğmuştur. Bu nedenle, kişinin bilgilenmesinin sağlanması yoluyla, idarenin alacağı kararları hukuk içinde etkileyebilmesinin sağlanması, bilgi edinme hak ve özgürlüğünün temel amacı olarak gösterilebilir.[712]

Bilgi edinme hakkı, kamuya açık olan kaynaklardan bilgi alırken herhangi bir müdahale ile karşılaşmamanın yanında, öncelikle devletin elinde bulunan belge, bilgi ve evraklar olmak üzere, genel olarak erişimin olmadığı bilgi kaynaklarından bilgi alınabilmesini teminat altına alan bir haktır.[713]

Bilgi edinme hakkının yalnızca kişilerin çıkarlarını koruma değil, aynı zamanda idareyi geliştirme ve denetleme fonksiyonları da vardır.[714] Bireye kamu kurumlarının elinde bulunan bilgi ve belgelere ulaşma ve bunlardan yararlanma hakkının tanınması; bu yolla idareye nüfuz edilerek idarenin etkilenmesi ve denetlenmesinin sağlanması yoluyla, kişinin hak arama hürriyetini kullanabilmesini ve hukuk devleti ilkesinin gereklerinin yerine getirilmesini sağlayan bir mekanizma

---

710 Akıllıoğlu, Tekin, "İnsan Hakları I, Kavram, Kaynaklar ve Koruma Sistemleri", Ankara, 1995, s.185.

711 Kaya, "Bilgi Edinm"e, s. 42.

712 Yıldırım, a.g.m., s. 227 vd.

713 Döner, "Şeffaf Devlet", s. 95.

714 Gürsel, Özkan, "Demokratik Yönetimin Birinci Adımı Bilgi Edinme Hakkı", Ankara, 2004, s. 21.

olacaktır.[715] Kişileri ve toplumu alakadar eden hususlarda daha fazla bilginin ortaya çıkması, bireysel hak ve özgürlüklerin olduğu gibi toplum hayatının gerektirdiği hakların da daha etkin olarak kullanılabilmesini sağlayacaktır.[716] Bu çerçevede, bilgi edinme hakkı ile, milli güvenlik ve diğer ülkelerle ilişkiler gibi sınırlandırılması zor olabilen alanlar dışında, kamu yönetiminin elinde bulundurduğu bilgi ve belgelere ulaşılmasını sağlamak suretiyle, vatandaşlara önemli bir denetleme imkânı verilmiştir. Bu nedenle bilgi edinme hakkı aynı zamanda, kamu yönetiminin yolsuzluk faaliyetlerinde bulunması, idarenin kusurlu eylem ve işlemlerini engellemeye yönelik de bir haktır.[717]

Kişilerin bilgiye ulaşma hakkının etkin olarak kullanılabilmesi için iletişim faaliyetleri oldukça önem arz etmektedir. Çünkü, bilgi edinme ihtiyacı, sadece idarenin elinde tuttuğu belge ve bilgilere erişebilmeyi değil, bireylerin toplumsal olarak kitlesel iletişim araçları aracılığı ile doğru bilgilenebilmesini de gerektirmektedir. Kitlesel iletişim araçları vasıtası ile bilgi edinme hakkı kapsamında bireyin ihtiyaç duyacağı bilgilerin pek çoğu herhangi bir resmi talepte bulunmasına gerek kalmadan topluma iletilmiş olur.[718]

İdarenin elindeki bilgileri gereksiz ve usulsüz bir şekilde gizlemesi demokrasinin işlerliği bakımından sorun yaratabileceği gibi, bilgiyi tekeli altında bulunduranların, bu bilgileri imtiyazlı şekilde kullanmaları tehlikesi de söz konusu olabilmektedir.[719] Kamu gücünü kullanarak çeşitli işlemleri yapan ve faaliyetlerde bulunabilen kamu otoritesi karşısında, bu kamu gücüne göre zayıf konumda bulunan vatandaşlara hukuk devletinin gereği olarak hukuki güvenceler sağlanmalıdır.[720]

Bilgi edinme hakkı, bu sakıncaların giderilmesini sağlamak için kabul edilmiş, kamu kurum ve kuruluşlarına ve bu nitelikteki meslek kuruluşlarına, görevleri nedeni

---

715 Akyılmaz, Bahtiyar, "İdari Usul İlkeleri Işığında Rekabet Kurulunun Çalışma Usulü", Ankara Barosu Uluslararası Hukuk Kurultayı, C. 2., Yıl: 2002, s. 116.

716 Yaşamış, a.g.m., s. 13.

717 Özkan, a.g.e., s. 21.

718 Çolak, "İletişim", s. 10.

719 Küzeci, a.g.e., s. 93.

720 Akgül, Aydın, "İdari Usul Açısından Ödeme Emrinde Kanun Yolunun ve Dava Açma Süresinin Gösterilmemesi", Terazi Dergisi, Yıl: 2008, C. 3, Sayı: 26, s. 101.

ile elinde bulundurdukları bilgi ve belgeleri bu konuda başvuruda bulunan bireylerle paylaşmaları zorunluluğu getirilmiştir. Bilgi edinme hakkı, yasal olarak tanınırken hakkın kullanılması konusundaki öncelikli düzenleme, idarenin, görevi gereği sahip olduğu bilgi ve belgeleri kendisinden talepte bulunan kişilerle paylaşmaya mecbur olmasıdır.[721]

AİHM, ifade özgürlüğünün unsurları içinde kabul edilen bilgi edinme hakkına ilişkin olarak; bu hakkın bilgiye ulaşma, bilgiyi arama ve toplayabilme haklarını da kapsadığı ve bilgi edinme hakkı ile bilgi ve fikirleri açıklama özgürlüğünün birbirini tamamladığını ifade etmektedir. Yine AİHM, bilgi edinme hakkının, bireylerin bilhassa kamu yararını ilgilendiren konularda yeteri kadar bilgilendirilmesi hakkını da içerdiğini belirtmiştir.[722]

AİHM, *bilgi edinme hakkı* ihlallerine ilişkin davalara AİHS'nin ifade özgürlüğünün düzenlendiği 10. maddesinin, bilgi edinme hakkı ile ilgili olarak devletlere pozitif bir sorumluluk yüklememesi gerekçesi ile bu madde kapsamında değil de AİHS'nin özel yaşamın gizliliği ve korunmasının düzenlendiği 8. maddesi kapsamında görmekte iken, *bilgi alma hakkı* ihlallerine dair başvuruları ise AİHS'nin 10. maddesi kapsamında görmektedir.[723]

AİHM, kendisine yapılan başvuruların bazılarında sağlık ve bunun gibi konulara ilişkin kişisel veri taleplerinin dava konusunu oluşturmasına rağmen, AİHS'nin 8. maddesi çerçevesinde *"adil denge ilkesi"* kriterini kullanarak, idare tarafından bilginin paylaşılmamasındaki kamu çıkarının, bireysel çıkardan ağır gelmesi sebebiyle başvurularda hak ihlalinin olmadığına hükmetmiştir. Bunun yanında AİHM, yine bireysel çıkardan daha ağır gelen toplumsal çıkarın varlığını belirttiği

721 Çolak, N. İlker, "Bilgi Edinme Hakkının Sınırları ve Sınırlama Ölçütleri", e-akademi Hukuk, Ekonomi ve Siyasal Bilimler Aylık İnternet Dergisi, Sayı: 39, Yıl: 2005, paragraf 1, http://www.e-akademi.org/makaleler/nicolak-2.htm, Erişim tarihi, 27.06.2019.

722 Tanju, a.g.e., s. 164.

723 Soykan, a.g.m., s. 68.

Roche/Birleşik Krallık[724] ve M.G/Birleşik Krallık[725] davalarında ise, iç hukukta kamusal yarar ve kişisel çıkar çatışmasını ölçebilecek bağımsız kuruluşun bulunması gerektiğini belirterek, böyle bir kuruluşun olmaması halinde ise AİHS'nin 8. m.'sinin ihlal edildiğine hükmetmiştir.[726]

Diğer taraftan AİHM, var olan ve erişilebilecek nitelikteki bir bilgiye ulaşmanın devlet eliyle engellenmiş olmasını, AİHS'nin 10. m.'si açısından "*ifade özgürlüğü"*nün ihlal edilmesi olarak kabul etmişken, devletin tuttuğu ve kişisel vasıftaki bir kayda ulaşmanın engellenmiş olmasını AİHS'nin 10. m.'sinin ihlali olarak kabul etmemiştir. Ancak bu durumun, aile hayatını ve özel hayatı korumayı hedefleyen ve bu konuda devletlere pozitif sorumluluk yükleyen AİHS'nin 8. m.'si kapsamında hak ihlallerine yol açabileceği ihtimali unutulmamalıdır.[727]

Kişisel verilere erişim taleplerinin AİHM tarafından ifade özgürlüğü çerçevesinde yorumlanması, açıklığı sağlama ve kişilerin devlet karşısında korunması şeklindeki bilgi edinme hakkının iki fonksiyonu göz önünde bulundurulduğunda daha yerinde olacağı ifade edilmektedir. Bu kapsamda, bilgi edinme hakkının kişisel verilere ve resmi verilere erişim hakkı ile kamu yararı bulunan konularda bilgilendirilme hakkı olmak üzere 3 temel hakkın toplamından oluştuğu ifade edilmektedir.[728]

3.4.3.2. Bilgi Edinme Hakkının Sınırları

Temel hak ve özgürlüklerin genelinde olduğu gibi bilgi edinme hakkı da herhangi bir sınırlamaya tabi tutulmadan yararlanabilecek bir hak değildir. Yani, bireylerin bilgi edinme hakkı çerçevesinde idareye başvuru hiçbir sınırlama olmadan bütün bilgi ve belgelere erişim fırsatı verilmeyeceği ortadadır. Bu nedenle bilgi edinme

724 AİHM Kararı: Roche v. Birleşik Krallık, Başvuru No: 32555/ 96, Tarih: 19.10.2005, Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-70662, Erişim tarihi, 08.02.2019.

725 AİHM Kararı: M. G. v. Birleşik Krallık, Başvuru No: 39393/98, Tarih: 24.09.2002, Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-5964, Erişim tarihi, 08.02.2019.

726 Soykan, a.g.m., s. 70.

727 Soykan, a.g.m., s. 70.

728 Soykan, a.g.m., s. 73.

hakkının kullandırılması esnasında kişilerin bireysel yararları ve kamunun ortak çıkarı bir arada değerlendirilerek adil bir denge kurulmalıdır.[729]

4982 sayılı Bilgi Edinme Hakkı Kanunu'nun dördüncü bölümünde, bilgi edinme hakkının sınırlarına yer verilmiştir. Buna göre şu durumlar 4982 sayılı Bilgi Edinme Hakkı Kanunu'nun ve bilgi edinme hakkının kapsamı dışındadır:

- Yargı denetimi dışında kalan işlemler (Madde 15. Ancak bu işlemlerden bireylerin çalışma hayatını ve mesleki onurunu etkileyecek nitelikte olanlar yine kanun kapsamındadır.),
- Devlet sırrına ilişkin bilgi veya belgeler (Madde 16),
- Ülkenin ekonomik çıkarlarına ilişkin bilgi veya belgeler (Madde 17),
- İstihbarata ilişkin bilgi veya belgeler (Madde 18.Ancak bu bilgi ve belgeler kişinin çalışma hayatını ve mesleki onurunu etkileyecek nitelikte ise kanun kapsamındadır.),
- İdari soruşturmaya ilişkin bilgi veya belgeler ve adli soruşturma ve kovuşturmaya ilişkin bilgi veya belgeler (Madde 19-20)[730]
- Özel hayatın gizliliği kapsamındaki bilgi veya belgeler (Madde 21 İlgilinin rızası bu kuralın istisnasını oluşturmaktadır.)
- Haberleşmenin gizliliği esasını ihlal edecek bilgi veya belgeler (Madde 22)
- Kanunlarda ticari sır olarak nitelenen bilgi veya belgeler (Madde 23)
- Fikir ve sanat eserlerine ilişkin bilgi veya belgeler (Madde 24)

729 Çolak, "Bilgi Edinme", s. 1.

730 Ancak ilgili maddelerde adli ve idari soruşturma ve kovuşturmaya dair tüm bilgi ve belgeler değil belli koşullar altında bazı bilgi ve belgeler kanun kapsamına çıkarılmıştır. bkz. 4982 sayılı Kanun 19-20. maddeler.

- Kurum içi düzenlemelere ilişkin bilgi veya belgeler (Madde 25, ancak bu düzenlemeden etkilenecek kurum çalışanlarının bilgi edinme hakları yine bu kanun kapsamında kabul edilmiştir.)

- Kurum içi görüş, bilgi notu teklif ve tavsiye niteliğindeki bilgi veya belgeler (Madde 26)

- Tavsiye ve mütalaa talepleri (Madde 27.).

Kesin ve haklı bir neden bulunmaması halinde kişilerin özel hayatına devletin müdahale etmesine izin verilmemelidir. Bu nedenle, özel hayatın gizliliği hakkı, demokratik anayasalarda ve bunların uygulamalarında bilgi edinme hakkının sınırlanmasını gerekli kılan belli sayıdaki sebeplerden birisi olarak kabul edilmiştir.[731]

Bunun yanında, kişinin özel hayatına dair bilgilerin kişinin açık veya örtülü rızası üzerine açıklanması, kişinin kendisinin talebi üzerine idare tarafından kişinin özel hayatına dair bilgi ve belgelerin ilgiliye verilmesi gibi hususlarda özel hayatın gizliliğinin ihlal edildiği iddia edilemeyecektir.[732]

3.4.3.3. Kişisel Verilerin Korunması ile Bilgi Edinme Hakları Arasındaki Temel İlişki

Bilgi edinme hakkı ile kişisel verilerin korunması hakkı arasındaki ilişki açısından konu değerlendirilecek olursa, bireylerin kamu idaresinin işlem ve faaliyetleri ile ilgili bilgiye ulaşmalarını sağlayan hak bilgi edinme hakkıdır. Bilgi edinme hakkı kişisel verilerin korunması hakkı ile yakın ve sıkı ilişkilidir.[733] Farklı kaynaklarda bu iki hak arasındaki ilişki "bilgi toplumu hukukunun iki sütunu" ve "bir madalyonun iki yüzü" şeklinde tarif edilmektedir.[734]

Kişilerin kendi haklarında tutulan veya kendileri ile ilgili işlenen bilgilere erişiminin sağlanması suretiyle, kişilere kişisel verilerini kontrol etme imkânı bilgi edinme hakkı ile sağlanmış ise de bu hakkın bu kapsamda kullanılabilmesi için daha

731 Zengin, Mehmet Ali, "Türk Hukukunda Bilgi Edinme Hakkının Sınırları", Ankara, 2012, s. 111.

732 Zengin, a.g.e., s. 113.

733 Şimşek, a.g.e., s. 143.

734 Küzeci, a.g.e., s. 94.

önce işlenmiş bir verinin bulunması gereklidir. Bilgi edinme hakkı ile kişisel verilerin korunması hakkı birbirleriyle yakın ilgili ise de bu ilişki iki konuda ters orantılı olarak kendisini göstermektedir. Bunlardan biri; bilgi edinme hakkı çerçevesinde erişilebilecek bilgi kategorisinde kişisel verilerin yer alıyor olması, diğeri ise, bilgi edinme hakkını sınırlayan haklardan olan özel hayatın gizliliği hakkının kapsamında kişisel verilerin korunması hakkının yer almasıdır.[735] Diğer bir deyişle, bazı durumlarda kişisel verilerin, bilgi edinme hakkı çerçevesinde erişimi talep edilebilecek bir bilgi kategorisini oluşturması mümkündür. Kişiler kural olarak, bilgi edinme hakkı kapsamda idareye başvurarak kendilerine veya başka kişilere ve olaylara ilişkin idarenin tuttuğu verileri öğrenmeyi isteyebilirler. Ne var ki, idareden öğrenilmesi talep edilen verilerin başka kişilerin özel hayatına ilişkin olması halinde, idare tarafından bu veriler, bilgi edinme hakkının kapsamına girmediği gerekçe gösterilerek verilmeyebilecektir.[736] Konuya bu çerçeveden bakıldığında, kişisel verilerin korunması hakkı ile bilgi edinme hakkının birbirini bütünlediği ve bir yandan kişilerin kendi haklarındaki bilgilere ulaşması sağlanırken, diğer yandan özel yaşamlarının korunmasına hizmet edildiği görülmektedir.[737]

Bir diğer açıdan bakıldığında ise, aslında bilgi edinme hakkı ile kişisel verilerin korunmasının farklı alanları düzenledikleri görülecektir. Kamu idaresinin topladığı verilerin büyük bir kısmı vatandaşların yönetime dahil olmalarını sağlamak için oldukça önemli olup bilgi edinme hakkı kapsamında koruma altındadır. Örneğin; şehir planlamasına, çevre kirliliği ve trafik sorunlarına ilişkin tutulan veriler bu kapsamda değerlendirilebilir. Ayrıca bu konulara ilişkin bilgilerin kişisel veri niteliği taşımadığı da ortadadır. Bu gibi konularda bilgi edinme hakkı ile kişisel verilerin korunması hakkının alanları ayrıştığı için aralarında bir çatışmadan söz edilemeyecektir.[738]

Kamu yönetiminin elinde tuttuğu verilere bireyin ulaşmasını bilgi edinme hakkı sağladığı için, bu hak yönetimin şeffaflaşması noktasında oldukça önemli bir haktır. Bilgi edinme hakkı, kişisel verilerin korunması hakkı yönünden

735 Kaya, "Bilgi Edinme", s. 89.

736 Çokmutlu, a.g.e., s. 63.

737 Çokmutlu, a.g.e., s. 63.

738 Küzeci, a.g.e., s. 94.

değerlendirildiğinde, bilgi edinme hakkının, bireyin kendisiyle ilgili olup da kamu kurumlarının tutmuş olduğu verilere, bireyin erişiminin sağlanmasına hizmet ettiği görülür. Ancak, kişisel verilerin korunması hakkı alanında bilgi edinme hakkının oldukça sınırlı bir yerinin olduğu görülür.[739]

Bilgi edinme hakkı, kişinin kendisi hakkındaki bilgileri öğrenmesini sağladığı gibi, bununla birlikte, bu verilerin hukuka uygun, doğru ve güncel olup olmadığı gibi konular hakkında kişinin bilgilenmesine fayda da sağlayacaktır. Bu nedenle, kişinin kendisine ait veriler hakkında işleme yapılıp yapılmadığına dair bilgi edinme hakkının olması, kişisel verilerinin işlenmiş olması ihtimalinde, kişinin bu nedenle sahip olduğu haklarını kullanabilmesinin bir ön koşulunu teşkil etmektedir.[740]

İdarenin keyfi davranmasını önlemek ve idareden demokratik yollardan hesap sorulmasını sağlamak gibi işlevleri açısından, bilgi edinme hakkı demokrasilerin vazgeçilmez öğesi haline gelmiştir.[741] Bu yönüyle, kişisel verilerin korunması hakkı ile bilgi edinme hakkı arasında amaçları bakımından benzerlik olduğu görülmektedir.

Kişisel verilerin korunması ve bilgi edinme hakkına dair yasal düzenlemeler genellikle bir arada kabul edilmiştir. Birçok ülkede her iki hak hakkındaki yasal düzenlemenin aynı anda yapılmasının yanında, bazı ülkelerde her iki hakkın sağlanmasını denetleyen bağımsız kurulların aynı çatı altında toplandığı da görülmektedir. Bu yöndeki uygulamada, her iki hak alanının birbirinin bütünleyicisi olduğu ve düzenlemelerin birbirleriyle uyumlu olmasının yararlı olacağı düşüncesi etkin olmuştur.[742]

Bilgi edinme hakkı ile kişisel verilerin korunması hakkı arasında bazı durumlarda birbirini sınırlayan, bazı durumlarda ise birbirinin içine geçmiş olan konuları düzenleme şeklinde farklı bir ilişki vardır. Nitekim, kişisel veriler bir yönüyle bilgi edinme hakkı çerçevesinde erişimi talep edilebilecek bir bilgi kategorisini

739 Küzeci, a.g.e., s. 95.

740 Şimşek, a.g.e., s. 145.

741 Yüksel, Hız/Zekeriya Yılmaz, "Bilgi Edinme ve Dilekçe Hakkı", Seçkin Yayınları, Ankara, 2004, s. 47.

742 Küzeci, a.g.e., s. 94.

oluşturmakta iken; bir başka yönüyle ise kişisel verilerin korunması, bilgi edinme hakkını sınırlandırmaktadır.[743]

Bunun yanında, kamu idaresi tarafından kendisine ilişkin tutulan verilere kişinin ulaşabilmesini sağlaması nedeni ile bilgi edinme hakkının kişisel verilerin korunmasını desteklediği söylenebilir.[744]

Bilgi edinme hakkının sınırlarını oluşturan haklardan biri olan özel hayatın gizliliği açısından konuya bakıldığında, bilgi edinme hakkının kişisel verilerin korunması açısından faydaları daha açık bir şekilde görülecektir. Çünkü devletin oldukça geniş ve kapsamlı bir kişisel veri arşivine sahip olduğu göz önüne alındığında, bu gücün sınırlandırılmamış olması özel hayatın gizliliği hakkının özüne müdahale sonucunu doğurur.[745] Zira devletin elinde vatandaşlara ve ülkeye giren yabancılara ait doğum, ölüm, evlatlık edinme, sabıka, sağlık kayıtları, seçmen kütükleri kayıtları, banka, sosyal güvenlik, vergi, iflas ve malvarlığına ilişkin kayıtlar gibi çok fazla alana ait kayıtlar bulunmaktadır. Bu kayıtların bir kısmının oldukça hassas nitelik taşıyan verilere ilişkin olması nedeni ile, kişinin isteği dışında ve herhangi bir kamusal zorunluluk olmadan, başka kişilerin ele geçirmesi halinde kişilerin temel hak ve özgürlükleri ile özel yaşamları zarar görebileceği gibi kişilerin bağımsızlıkları da zedelenebilecektir.[746]

3.4.4. DÜŞÜNCEYİ AÇIKLAMA ÖZGÜRLÜĞÜ VE KİŞİSEL VERİLERİN KORUNMASI

3.4.4.1. Genel Olarak

Bireyin iç aleminin en gizli alanından doğan *düşünce*;[747] *görüş, kanaat* ve *fikir* ögelerini ifade etmektedir.[748] Hukuk düzeni ise, amacı nedeni ile ilkesel olarak yalnızca dış aleme yansıtılan toplumsal davranışları konu edinir. Bunun yanında,

743 Kaya, "Bilgi Edinme", s. 89-91.
744 Küzeci, a.g.e., s. 94.
745 Kaya, "Bilgi Edinme", s. 89-91.
746 Küzeci, a.g.e., s. 95.
747 Kaboğlu, "Anayasa Hukuku", s. 287.
748 Gören, "Anayasa Hukuku", s. 461.

düşünce geçişli olup doğasında *iletişimsellik* vardır. Söz, yazı ve öğretim aracılığıyla düşünce ve kanaatlerin iletişimi, doğrudan doğruya hukuk alanına toplumsal bir olgu halinde girmiştir.[749] Düşüncenin serbest şekilde oluşumu, bir yandan düşünceyi özgürce açıklayıp yayabilme, yani ifade özgürlüğünü, diğer yandan ise açıklanmış olan fikirlerden haber alabilmeyi ve bilgi edinebilmeyi gerekli kılmaktadır.[750]

Düşünce özgürlüğü, bireylerin serbest bir şekilde fikir ve bilgilere erişebilmesini, edindiği fikir ve kanaatleri dolayısıyla diğer bireyler tarafından kınanmaması ve bu fikirleri tek başına ya da başkalarıyla birlikte çeşitli suretlerle serbest bir şekilde açıklayabilmesini, savunabilmesini, başkalarına aktarabilmesini ve yayabilmesini ifa eder.[751] Düşünceyi açıklama ya da ifade özgürlüğü insan haklarının en başında gelen haklardan olup, amacı düşüncenin korunmasıdır. Düşünce ise, insanın iç dünyası ile ilgili olup, açıklanmaması halinde başkaları tarafından bilinmesi mümkün değildir. Bu nedenle, insanın, özgür düşünmesinin bir anlamının olması için kişilerin özgür düşüncelerini açıklayabilme özgürlüğünün de tanınmış olması gerekmektedir. Düşünceleri açıklama ise değişik şekillerde meydana gelebilir.[752]

Kişi kendi dünyasındaki gerçekleri düşünce özgürlüğü ile bulma imkânını yakalarken, düşüncelerini başka kişilere iletme imkânını ise düşünceyi açıklama özgürlüğü sağladığından; bu iki hak birbirinden ayrılmayan iki özgürlük türüdür.[753]

Bu nedenle, düşünce hürriyeti kavramından, fikirlerin oluşmasına imkân tanıyan *"haber alma ve öğrenme hürriyeti"*, söz konusu hürriyetin tanınması ile meydana gelen düşünce ve kanaatlerden dolayı kişinin kınanmaması anlamına gelen *"kanaat* hürriyeti*"* ve ancak tüm bunlar ile birlikte sahip olunabilen *"düşüncenin açıklanması, yayılması hürriyeti"* bir arada değerlendirilmelidir.[754]

---

749 Kaboğlu, "Özgürlükler Hukuku", s. 334.

750 Gören, "Anayasa Hukuku", s. 458.

751 Bülent, Tanör, Türkiye'nin İnsan Hakları Sorunu, BDS Yayınları, 3. Baskı, İstanbul 1994, s. 59.

752 Özcan, Özbey, "Avrupa İnsan Hakları Sözleşmesi Işığında İfade Özgürlüğü Kısıtlamaları", TBBD, Yıl: 2013, s. 42.

753 Günaydın, Barış, "İnternet Yayıncılığı ve İfade Özgürlüğü", Ankara, 2010, s. 72.

754 Karaaslan, Erol," Avrupa İnsan Hakları Sözleşmesi Çerçevesinde Düşünce Özgürlüğü", İstanbul Barosu Dergisi, Yıl: 2004, Cilt:78, S.4, s. 1437.

Bu kapsamda, *düşünce hürriyeti*, "*bilgi edinme hakkı"* ve "*kanaat hürriyeti"* ile başlayarak, "*ifade hürriyeti"* ile devam eden,[755] insan kişiliğinin toplum içinde en doğrudan anlatımı olduğu için en kıymetli insan haklarından birisidir.[756] İnsana tanınan özgürlüklerden birçoğu, düşünce özgürlüğünün gerçekleşmesi için aracı bir görev görürken, düşünce özgürlüğü ise diğer hakların ve hürriyetlerin büyük bir bölümüne karşı *"besleyici"* bir görev[757] üstlenmektedir.

Kişinin kendisini entelektüel ve iletişimsel açıdan gerçekleştirmesini ve toplumun demokratik olarak biçimlenmesini sağlamak ifade özgürlüğünün iki temel amacıdır.[758] Düşünce özgürlüğünde esas olan bilgi edinme hakkından yararlanmak sureti ile kişide özgürce oluşan, fikirlerin, kanaatlerin ve görüşlerin özgürce açıklanabilmesi ve yayılabilmesidir.[759]

Düşünce ve kanaat serbestisi, bilgi ve düşünceleri açıklama ve bunlara erişebilme haklarını kendisine temel ifade özgürlüğü, çoğulcu demokrasilerde bulunması gereken en önemli özgürlüklerden birisidir.[760] İfadenin konusunu, din, fikir, vicdani inanç ve düşünce kavramları ile ifade edilen tüm değerler oluştururken; ifade biçimi ise, dil ile söylemenin yanında fikirleri savunmak, tanıtmak, oluşturmak, anlatmak, açıklamak ve yaymak şeklinde geniş tutulmalıdır.[761]

Anayasa Mahkemesi kamuoyunda "Twitter kararı"[762] olarak bilinen kararında, ifade özgürlüğünün, düşünce ve kanaate sahip olma özgürlüğünün yanında, kişide oluşan düşünce ve kanaatleri açıklayabilme ve yayabilme, bununla birlikte görüş öğrenebilme veya haber alabilme, verebilme hürriyetlerini de kapsadığı belirtilmiştir.[763] Yine aynı kararda ifade özgürlüğü *"bireylerin serbestçe haber ve*

---

755 Kaboğlu, "Özgürlükler Hukuku", s. 335.

756 Gören, "Anayasa Hukuku", s. 458.

757 Kaboğlu," Özgürlükler Hukuku", s. 335.

758 Beydoğan, T. Ayhan, "Türk Hukukunda Siyasi İfade Hürriyeti", Ankara 2003, s.22.

759 Kaboğlu,"Anayasa Hukuku", s. 291.

760 Günaydın, a.g.m., s. 72.

761 Kaboğlu, "Anayasa Hukuku," s. 291.

762 AYM'nin 02.04.2014 T. ve 2014/3986 bas no. 3.4.2014 tarihli ve 28961 sayılı R.G. de yayınlanan kararı.

763 Akgül, "Kişisel Veri", s. 90.

bilgilere, başkalarının fikirlerine ulaşabilmesi, edindiği düşünce ve kanaatlerden dolayı kınanmaması ve bunları tek başına veya başkaları ile birlikte çeşitli yollarla serbestçe ifade edebilmesi, anlatabilmesi, savunabilmesi, başkalarına aktarabilmesi ve yayabilmesi"[764] olarak tanımlanmıştır.

Anayasa Mahkemesinin bir başka kararında ise başvurucu video paylaşım sitesi "*www.youtube.com*" isimli internet sitesine erişimin engellenmesine dair Telekomünikasyon İletişim Başkanlığı (TİB) işlemi nedeniyle başvuruculaların Anayasa'nın 26. m.'sinde güvence altına alınan ifade özgürlüğünün ihlal edildiğine dair karar vermiştir. [765]

İnsan hakları hukukunda ifade özgürlüğünün kapsamı ve sınırları konusunda ortak bir standardın varlığından bahsedilebilse de bu konuda ülkeler arasında önemli farklılıklar da vardır. Bu ortak standardı belirleyen uluslararası belgelerin başlıcaları, Medeni ve Siyasi Haklar Sözleşmesi ve AİHS'tir.[766] Öte yandan, AİHS'ye göre demokratik bir toplumda *düşünceyi açıklama özgürlüğü*ne sınırlama getirilebilecekse de sınırlamaların çok sıkı bir şekilde denetiminin yapılması gerekli görülmüştür. İç hukuk düzenlemelerinde öngörülen sınırlamaların AİHS'nin 10. m.'sine göre hak ihlali teşkil etmemesi için üç koşulun gerçekleşmiş olması gerekir. Bu koşullardan birincisi, söz konusu müdahalenin yasada öngörülmesi; ikincisi; bu müdahalenin yasada belirlenen amaçlarla sınırlandırılması; üçüncüsü ise, demokratik bir toplum açısından bu müdahalenin yapılmasının gerekli olmasıdır. AİHM'nin yaptığı incelemelerde bu 3 şartın çok katı bir şekilde yorumlandığını söylemek mümkündür.[767]

Diğer taraftan AİHM, AİHS'nin 10/2. fıkrası ile ilgili bir sınırlandırmanın koşulları taşıyıp taşımadığını değerlendirmeden evvel 1. fıkrada düzenlenmiş hak ve özgürlüklere dair bir sınırlandırmanın söz konusu olup olmadığı konusunu incelemektedir. Bu konuya örnek olarak AİHM tarafından karara bağlanan, Open

764 AYM'nin 02.04.2014 T. ve 2014/3986 bas no. 3.4.2014 tarihli ve 28961 sayılı R.G. de yayınlanan kararı, benzer yönde AYM "youtube" kararı için ayrıca Bkz. https://www.resmigazete.gov.tr/eskiler/2014/06/20140606-10.pdf, Erişim tarihi: 29.05.2019

765 https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/4705?BasvuruNoYil=2014& BasvuruNoSayi=4705, Erişim tarihi 28.11.2019.

766 Günaydın, a.g.e., s. 73.

767 Karaaslan, a.g.m., s. 1450.

Door Dublin Well Woman/İrlanda davası[768] örnek verilebilir. Söz konusu davada İrlanda dışındaki kürtaj klinikleri ve kürtaj yaptırılmasıyla ilgili, hamile kadınlara bilgi dağıtılması, İrlanda Anayasası'nda "*fetüsün yaşam hakkı*" korunduğu gerekçesine dayanılarak Yüksek Mahkeme tarafından yasaklanmıştır. Bu durum AİHM'ye taşınmış; AİHM kararında, yasaklamanın sözleşmenin ifade hürriyeti hakkını güvence altına alan 10. m.'sine aykırı olduğuna ve hamile kadınların düşünce özgürlüğünün ihlal edildiği yönünde karar vermiştir.[769] Bu dava sonucunda İrlanda Anayasası'nda 1992 yılında önemli bir değişikliğe gidilmiş ve bilgi dağıtma ve alma hakkını içeren bir hüküm İrlanda Anayasasına eklenmiş, ardından 1995 yılında da bu konuya ilişkin bir kanun çıkartılarak hakkın kapsamı yasal anlamda genişletilmiştir.[770]

3.4.4.2. Kişisel Verilerin Korunması Hakkı ile Düşünceyi Açıklama Özgürlüğü Arasındaki İlişki

İfade hürriyeti ile kişisel verilerin korunması hakkı genellikle çatışma içinde olduğunu söylemek mümkündür. Bu çatışma daha ziyade düşünceyi açıklama özgürlüğü kapsamı içinde kabul edilen basın özgürlüğü açısından gündeme gelir.[771] Çünkü toplumun ilgisini çekmesi muhtemel olan konuları araştıran, değerlendirip yayınlayan basın kuruluşları bir yanda, kişisel bilgilerinin paylaşılmasını istemeyen kişiler ise diğer tarafta olmak üzere, bu iki tarafın menfaatleri arasındaki çekişme söz konusu olmaktadır. Özel yaşamın gizliliği ve kişisel verilerin korunması hakları ile basın özgürlüğü arasındaki ilişkide, hangi hakka üstünlük tanınacağının belirlenmesi suretiyle çözüm sağlanacaktır. Bu durumda, karşılaşılan olaylarda ölçme ve değerlendirme yapılarak, olayın kendine has koşulları göz önünde bulundurulup haklardan hangisine ağırlık verileceği tespit edilmelidir.[772]

Bunun yanında ifade özgürlüğü ile kişisel verilerin korunması hakkı her zaman çatışma içinde olmayıp, birbirlerini desteklediği alanlar da söz konusu olabilmektedir.

---

768 AİHM Kararı, Open Door Dublin Well Woman v. İrlanda, Tarih: 29.10.1992, Erişim Tarihi: 11.11.2019, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57789%22]}.

769 Karaaslan, a.g.m., s. 1450.

770 Çavuşoğlu, Naz, "Avrupa İnsan Hakları Mahkemesi Kararlarının Uygulanması: Türkiye Kararları", İstanbul, 2003, s. 60.

771 Küzeci, a.g.e., s. 86.

772 Küzeci, a.g.e., s. 87.

Düşünceyi açıklama özgürlüğü kapsamında kabul edilen kimsenin düşüncelerini açıklamak için zorlanmaması kuralı, aynı zamanda kişisel verilerin korunması açısından da kısmi de olsa bir takım güvence sağlamaktadır. Yani, bu kural, kişinin gizli kalmasını tercih ettiği verileri açıklaması için zorlanmaması ve hassas verilerinin kişinin kendisinde saklı tutması açısından destek olur. Böylece, kişisel verilerin kural olarak sadece kişinin kendi rızası ile toplanabilmesi ilkesi ve kişisel verilerinin açıklanması konusunda kişinin kendisinin karar vermesi hakkı ifade özgürlüğü ile de desteklenmiş olur.[773] Bir başka deyişle, devletin, bireyin düşüncesini açıklaması için bireyi zorlayamaması, düşünceyi açıklama özgürlüğünün negatif yönünü oluşturduğu için, buradan bireyin gizli kalmasını tercih ettiği verilerini açıklamaya zorlanamaması sonucuna varılır. Böylece, düşünceyi açıklama özgürlüğünden bireyin *sır alanına* konu olan kişisel verilerinin korunması sağlanmış olur.[774] Zira, düşünce özgürlüğü, aynı zamanda bir "*düşünceye katılmama"* ya da başka bir ifade ile "*düşünceyi açıklamama*" hürriyetini de içerir. AİHM, Young James ve Webster/Birleşik Krallık davasında[775], İngiliz Hukukunda var olan sendikaların tekelleşme uygulamalarını, *"benimsenmeyen fikir ve düşünceye katılmaya zorlama"* biçiminde yorumlayarak AİHS'nin 10'uncu maddesinin ihlal edildiği yönünde karar vermiştir.[776]

Düşünceyi açıklama hürriyeti ile kişisel verilerin korunması hakkının birbirlerine destek olduğu konulardan bir diğeri de; düşünceyi açıklama özgürlüğünün, kişinin yapacağı açıklamalarının içeriğini ve açıklama yapacağı muhatabı belirleme hakkını güvence altına almasıdır.[777] Yine düşünceyi açıklama özgürlüğü, kişinin kişisel veri niteliğindeki bilgilerinin bulunduğu düşüncelerini özgür bir şekilde aktarmasını garanti ettiğinden, bu açıdan bireyin kişisel verileri üzerindeki *"belirleme hakkı"*nın bir unsurunu teşkil eder.[778]

---

773 Şimşek, a.g.e., s. 146-147.

774 Şimşek, a.g.e., s. 147.

775 AİHM Kararı, Young James ve Webster v Birleşik Krallık, Tarih: 13.08.1981. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/rus?i=001-57608, Erişim tarihi, 08.02.2019.

776 Karaaslan, a.g.m., s. 1443.

777 Küzeci, a.g.e., s. 89.

778 Şimşek, a.g.e., s. 146.

Düşünceyi açıklama özgürlüğü ile kişisel verilerin korunması hakkının zaman zaman çatışma içinde olduğunu yukarıda belirtmiştik. Bilhassa magazin basınında, toplumda tanınmış kişilerle ilgili oldukça mahrem bilgilerin fotoğraf, yazı veya görüntülerle aktarıldığı belirtilerek, bu çatışmanın; *"düşünceyi açıklama özgürlüğü"* kapsamı içinde kabul edilen *"basın özgürlüğü"* ile *"kişisel verilerin korunması hakkı"* arasında gerçekleşebileceği ifade edilmektedir. Bu çatışmanın düşünceyi açıklama özgürlüğü kapsamında değerlendirilen basın özgürlüğü ile gerçekleşebileceği ifade edilmektedir.[779] Gazetecilerin ve yayıncıların önemli bir dostu olarak düşünceyi açıklama özgürlüğü görülmektedir. Nitekim, gazeteciler ve yayıncılar kişisel bilgiler ile ilgili yaptıkları yayınları haklı çıkarmak için düşünceyi açıklama özgürlüğüne başvurmaktadırlar.[780]

Kişisel verilerin korunması hakkında yapılan düzenlemelerde düşünceyi açıklama özgürlüğünü korumak için *"eğer gerekli ise"* istisna tanınabileceğine dair hükümlere yer verilmektedir. *"Gereklilik"* ön şartı, olayın kendine has şartları devletler tarafından göz önünde bulundurularak yapılacak bir değerlendirme ile belirlenebilecektir.[781]

AİHM, önüne gelen başvurularda AİHS'nin 10/2. fıkrasında düzenlenen sınırlama sebeplerine dayanarak ifade özgürlüğüne yapılan müdahalenin kanunda düzenlenip düzenlenmediği, öngörülen legal amaçlara ulaşmak için *"demokratik bir toplumda"*, *"zorunlu"* olup olmadığı açılarından inceleme yapmaktadır. AİHM'ye göre, kanun ile emredilmiş olma ya da şartların kanun ile belirlenmiş olması yasaya uygun olma ile ifade edilen hususlardır. AİHM müdahalenin demokratik toplumda gerekli olması ölçütünün uygulanmasında ise *"gereklilik"* unsurunu *"vazgeçilmezlik"* ya da *"uygunluk"* olarak değil de devletin *"zorlayıcı toplumsal ihtiyacı dikkate almasının zorunlu olması"* anlamına geldiğini vurgulamaktadır.[782]

779 Küzeci, a.g.e., a.g.e., s. 86.

780 Room, a.g.e., s. 6.

781 Küzeci, a.g.e., a.g.e., s. 87.

782 Yokuş,"Hak ve Özgürlükler", s. 120 vd.

Bu kapsamda ifade özgürlüğü, diğer özgürlüklerin temelini oluşturduğu, demokratik toplum düzeninin esaslı unsurunu meydana getirdiği için, bu hakkın toplum güvenliği gibi diğer değerlerle karşı karşıya gelmesi durumlarında, ancak başka çare kalmazsa ve tüm şartlar değerlendirilip uygulandıktan sonra sınırlandırılabilmelidir. Bu hakkın sınırlandırılması halinde ise devletin, meşru ve anayasal bir çıkarının söz konusu olduğunu kanıtlaması gerektiği gibi,[783] bu müdahalenin gerekliliği, aynı zamanda inandırıcılığı da olmalıdır.[784]

Anayasa Mahkemesi ise, özgürlüklere getirilen sınırlandırmaların haklı olarak kabul edilebilmesi için *"açık ve mevcut tehlike"* kriterini kullanmıştır. Bu uygulamanın esas nedeni olarak, 1982 Anayasası'nın ifade özgürlüğü hakkında çok fazla sınırlamalara yer vermiş olması gösterilmiştir. Bu kritere göre, bir düşüncenin açıklanmasının, toplum ya da kişiler yönünden *"açık ve mevcut bir tehlike"* oluşturması halinde, bu düşüncenin açıklanması sınırlandırılabilecektir.[785]

3.4.5. HABERLEŞME ÖZGÜRLÜĞÜ VE KİŞİSEL VERİLERİN KORUNMASI HAKKI

Haberleşme, insanların, grupların ve diğer canlı topluluklarının günlük hayatlarında sahip oldukları bilgi, fikir ve düşüncelerini ortak semboller kullanarak kendi aralarında gerçekleştirdikleri paylaşım sürecidir.[786]

Haberleşme özgürlüğü kişinin en temel haklarından olup, insan hakları ile ilgili düzenlemelerin yapıldığı uluslararası belgelerde kişilerin bu hakka sahip olduğu kabul edilerek, bu belgelerde bu hakkın tanınması ve korunması gerekliliği vurgulanmıştır.[787]

1982 Anayasasının 22. m.'sinde haberleşmenin özgürlüğü güvence altına alınmıştır. Bu maddede, herkesin haberleşme hürriyetine sahip olduğu ve bireyler

783 Yokuş, "Hak ve Özgürlükler", s. 119.

784 Yokuş, "Hak ve Özgürlükler", s. 120 vd.

785 Yokuş, "Hak ve Özgürlükler", s. 82 vd.

786 Gedik, Ömer, "Türk Yargı Kararları Çerçevesinde Kitle İletişim Özgürlüğü", Ankara, 2008, s. 39.

787 Yokuş, Handan Sevük "Haberleşmenin Gizliliğini İhlal Suçu", s. 1, http://dergipark.gov.tr/dovnload/article-file/213966, Erişim tarihi, 25/06/2019.

arasındaki haberleşmede gizliliğin esas olduğu açık bir şekilde ifade edilerek haberleşme hürriyeti anayasal bir hak olarak tanınmıştır. Kişilerin serbestçe haberleşebilmesi demokratik toplumlarda insan kişiliğinin bir sonucu olarak görülmüştür.[788]

Kişilerin mektup, telefon, elektronik posta gibi iletişim vasıtaları ile gerçekleştirdikleri özel iletişimlerinin gizliliğinin ve güvenilirliğinin korunması haberleşmenin gizliliği ile sağlanmaya çalışılmaktadır. Bu hakkın temelini özel yaşamın gizliliği hakkı oluşturmaktadır.[789]

Haberleşmenin gizliliği ilkesinin nesnel unsurunu belli ve sınırlı sayıda kişi tarafından bilinme oluştururken, haberleşmenin taraflarının bu haberleşmeden ve haberleşmenin içeriğinden başkalarının bilgi edinemeyeceğine dair bir kanaat ve iradeye sahip olmaları ise haberleşmenin gizliliğinin sübjektif unsurunu teşkil eder. Haberleşmenin gizliliğinden söz edebilmek için, kişilerin haberleşmenin ve içeriğinin gizli kalacağına dair iradelerinin olması yeterli olmayıp, kişilerin bu haberleşmenin gizliliğini sağlamak için elverişli araçları kullanmış olmaları da gereklidir.[790]

Haberleşmenin gizliliğinin ana ilkeleri, kişinin bir engellenme ile karşılaşmadan istediği kişiyle istediği şekilde haberleşebilmesi ve bu haberleşmenin ilgilinin onayı veya yasal gereklilik yoksa üçüncü kişilerin müdahalesinden korunmasıdır. Zira, özel hayatın korunmasına dair AİHS'nin 8. ve İHEB'nin 12. maddesi ile birçok ülke anayasalarında haberleşmenin gizliliği hakkından da bahsedilmektedir.[791]

Haberleşme içeriklerinin kişisel veri niteliğinde olması halinde haberleşmenin gizliliği ile kişisel verilerin korunması hakkı birlikte gündeme gelmektedir. Çünkü, hukuka aykırı bir şekilde iletişimin dinlenmesi veya kaydedilmesi ile kişisel verilerin

---

788 Özek, Çetin, "Türk Ceza Kanunu'na Göre Hürriyet Aleyhine Cürümlerin Genel Prensipleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: XXIX, S.4, Yıl: 1994, s. 965.

789 Gözübüyük Ahmet Şeref / Gölcüklü, Feyyaz "Avrupa İnsan Hakları Sözleşmesi ve Uygulaması", 5. Bası. Ankara, 2005, s.341.

790 Kaymaz, Seydi, "Ceza Muhakemesinde Telekominikasyon Yoluyla Yapılan İletişimin Denetlenmesi", Ankara 2009, s. 82.

791 Küzeci, a.g.e., s. 97.

elde edilmesi halinde haberleşmenin gizliliği ihlal edileceği gibi kişisel verilerin korunması hakkı da ihlal edilmiş olacaktır.[792] Bu açıdan bakıldığında haberleşmenin gizliliği hakkının kişisel verilerin korunması hakkına dolaylı yönden güvence sağladığı söylenebilecektir.

10/12/2015 tarih ve 2013/7666 başvuru numaralı Bülent POLAT başvurusu davasında başvurucu e-posta yazışmaları dikkate alınarak subay sözleşmesinin yenilenmemesi işlemi nedeniyle özel hayatın gizliliği ve haberleşme hürriyetinin, bu işleme karşı açtığı davanın reddi nedeniyle de adil yargılanma hakkının ihlal edildiğini savunmuştur. Anayasa Mahkemesi kararında özel hayatın gizliliği hakkı ile haberleşme hürriyetinin ihlal edildiğine ilişkin iddiaların kabul edilebilir olduğuna oybirliğiyle karar vermiştir. [793]

3.4.6. ÖZEL HABERLEŞMENİN GİZLİLİĞİ İLKESİ İLE KİŞİSEL VERİLERİN KORUNMASI HAKKI ARASINDAKİ İLİŞKİ

1982 Anayasasının 22. m.'sinde haberleşmenin gizliliği hakkı güvence altına alınmıştır. Bu maddede, *"...Haberleşmenin gizliliği esastır..."* denilerek haberleşmenin gizliliğinin esas olduğu net bir şekilde ifade edilmiştir.

Özel hayatın gizliliği kapsamında koruma altına alınan *"haberleşme hürriyeti"*nin de ötesinde, kamusal ve toplumsal bir anlam taşıyan iletişim hürriyeti, temel insan haklarına duyulması gereken saygının ve demokrasinin vazgeçilmez unsurlarındandır.[794]

Günümüzde, iletişimin artık kitleler üzerinden yapılmasından dolayı, bu kapsamda bireyin kişisel verilerinin korunması ayrı bir önem arz etmektedir. Çünkü, kitlesel iletişim faaliyetleri esnasında başvurulan araç ve yöntemlerle varılmak istenen gaye, bu iletişim sürecinin gizli kalmasının yanında ve ötesinde mümkün olduğu kadar çok daha geniş kitlelere mesajın ulaşmasının sağlanmasıdır.[795] Nitekim, *"kitle iletişim*

---

792 Şimşek, Anayasa Hukuku, s. 149.

793 https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/7666?BasvuruNoYil=2013&BasvuruNoSayi=7666, Erişim tarihi, 28.11.2019.

794 Kaboğlu, "Anayasa Hukuku", s. 310.

795 Çolak, "İletişim", s. 23.

özgürlüğü", bireylerin, bilgi, haber ve fikirlere serbestçe erişebilmesi ve edindikleriyle kendinde oluşan kanaatleri aynı yollarla açıklayabilip yayabilmesidir.[796]

Gelişen teknolojinin de getirdiği imkânlarla özellikle kişinin iletişim araçlarıyla gerçekleştirdiği haberleşme esnasında, bu haberleşmenin içeriğinin ve gizliliğinin sınırlanmasına neden olacak müdahale imkânları artmıştır. Temel bir hak olan *"haberleşme hürriyeti"*, haberleşme için kullanılan teknolojik gereçlerden ayrılarak, gerçekleştirilen haberleşmenin hem içeriğini hem de gizliliğini teminat altına almaktadır.[797] Kişilerin çeşitli iletişim vasıtalarıyla gerçekleştirdikleri özel iletişimlerinin gizliliklerinin ve güvenilirliklerinin korunması özel haberleşmenin gizliliği ile sağlanmaktadır.[798]

Temel bir hak olan özel haberleşmenin gizliliği hakkı, kamu kurumlarının müdahalesine karşı kişiye bir savunma hakkı verdiği gibi, bunun yanında da haberleşmenin gizliliğinin korunması ve bu alana müdahale edilmemesi yükümlülüğünü de devlete yüklemektedir.[799]

Yasal düzenlemelere aykırı şekilde haberleşmenin dinlenmesi veya kaydedilmesi suretiyle kişisel verilerin elde edilmesinde gerek kişisel verilerin korunması hakkı gerekse özel haberleşmenin gizliliği ihlal edilmiş olacaktır.[800] Haberleşme sürecinin özellikle kamu kurumlarınca hukuka aykırı bir şekilde dinlenilmesi, temel haklar açısından bir müdahale anlamına gelecektir. Bu nedenle, haberleşmenin gizliliği ihlal edilmek suretiyle kişisel verilerin kaydedilmesi, kaydedilen bu verilerin kullanılması veya aktartılması şeklindeki faaliyetlerin ayrıca kişisel verilerle korunması konusunda kabul edilen temel ilkelerden birisi olan, "kişisel veri toplama ve işlenme faaliyetlerinin hukuka uygun ve dürüstlük kuralına uygun olması" kuralına da aykırılık teşkil edecektir.[801]

---

796 Gedik, a.g.e., s. 40.

797 Şimşek, a.g.e., s. 148.

798 Küzeci, a.g.e., a.g.e., s. 97.

799 Şimşek, a.g.e., s. 148

800 Küzeci, a.g.e., a.g.e., s. 98.

801 Şimşek, a.g.e., s. 149.

Özel haberleşmenin gizliliği ile, haberleşmelerin içeriğini ve muhatabını serbest olarak belirleme özgürlüğü desteklenmekte, haberleşmenin içeriği üçüncü kişilerin müdahalesinden korumakta ve bu yolla kişisel verilerin korunması hakkı ile özel haberleşmenin gizliliği ilkesi sağlanmış olmaktadır.[802]

3.5. ANAYASA'NIN 90. MADDESİ YOLLAMASI İLE AİHS KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI VE AİHM'NİN ROLÜ

Kişisel verilerin korunması ile ilişkilendirilebilecek bir diğer önemli Anayasa maddesi ise *"Milletlerarası andlaşmaları uygun bulma"* başlıklı 90. m.'nin son fıkrasıdır. Buna göre *"Usulüne göre yürürlüğe konulmuş Milletlerarası andlaşmalar kanun hükmündedir. Bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz."* denilmek suretiyle usulüne uygun şekilde yürürlüğe konmuş olan milletlerarası sözleşmelerin normlar hiyerarşisi içerisinde kanun gücünde olduğu ve bir milletlerarası andlaşmanın usulüne göre yürürlüğe girmiş olması şartıyla AYM tarafından iptal edilmesinin mümkün olmadığı vurgulanmıştır. Her ne kadar milletlerarası andlaşmaların usulüne göre yürürlüğe girmesi halinde kanun hükmünde olduğu ifade edilse de, Anayasa Mahkemesine iptal istemi ile götürülemediğinden bahisle bu andlaşmaların doktrinde kanunun bile üzerinde kabul edilmesi gerektiğini ileri süren görüşler de mevcuttur.[803] Bununla birlikte Anayasanın aynı maddesinde "*Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası anlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası anlaşma hükümleri esas alınır."* denilmek suretiyle bir temel hak ve özgürlüğe ilişkin andlaşma ile kanun hükmünün çatışması halinde, milletlerarası andlaşmanın üstün tutularak milletlerarası andlaşma hükümlerinin uygulanacağı ifade edilmiştir. Bu şekilde Türkiye'nin de taraf olduğu temel hak ve

802 Küzeci, a.g.e., s. 98.

803 Bazı yazarlar, bu antlaşmaları anayasadan üstün, bazıları kanundan üstün bazıları ise kanun ile eş değer görmüştür. Bu hususlarda, doktrinde belirtilen ayırntılı görüşler için bkz.. Bilgin, Ahmet Burak, "AİHS ve Diğer Uluslararası Anlaşmaların İç Hukuktaki Yeri Bağlamında 2004 Değişikliğinin Beraberinde Getirdiği Sorunlar ve Bazı Çözüm Önerileri", MÜHFD, C.22, S.1, s. 132-133.

özgürlüklere ilişkin en önemli sözleşmelerden birisi AİHS'dir. Zira yukarıdaki bölümlerde AİHM'nin kişisel verileri koruma hukukunda sözleşmenin 8. m.'sini esas alarak hakkın incelemesini yaptığını da belirtmiştik.

Anayasa'nın 90. maddesindeki bu düzenleme ile AİHS bir iç hukuk normu haline gelmiştir. Sözleşmenin yorumlayıcısı olan AİHM'nin içtihatları ve AİHS'nin kapsamı iç hukukumuz açısından büyük önem arz etmektedir.[804]

AİHS'nin önemli özelliği, kapsamına aldığı temel haklar ve özgürlüklerin korunması amacıyla öngördüğü kontrol mekanizmasında kendisini gösterir. AİHM de bu kontrol mekanizmasının en ehemmiyetli ayaklarından birisidir.[805]

AİHM içtihatları ile, sistemin hukuki yapısını güçlendirerek, AİHS sistemi ile birlikte üzerinde konuşulan konuların insan hakları hukuku, insan haklarının korunması ve bu kapsama giren diğer konular olmasını sağlamıştır.[806]

AİHM, kişisel verilerin korunması kavramını, AİHS ile sağlanan teminatlar içinde kabul etmiştir. Zira, AİHM'nin, AİHS'nin 8'inci maddesiyle getirilen teminatların yorumlanmasında "*bireysel özerkliği* ve *bilgilerin geleceğini belirleme hakkı"*nı önemli temel bir ilke olarak değer verdiği gözlemlenmektedir. Bu kapsamda AİHM, kişisel verilerin kullanılması ve kayıt altına alınması hususunda kişilerin kontrol etme hakkının olduğunu da dile getirmektedir.[807]

Bunun yanında, AİHM, önüne gelen bazı davalarda, kişisel verilerin korunması hakkını AİHS'in 8. m.'si kapsamında değerlendirmişken, bir yandan da kişisel verilerin işlenmesinin tüm yönleriyle AİHS tarafından koruma altına alınmadığını ifade etmiştir. AİHM, somut uyuşmazlıklarda öncelikli olarak, ihlal edildiği iddia edilen hakkın sözleşmenin 8. m.'sinin 1. fıkrasında ifade edilen durumdan herhangi

---

804 Çalışmamızın genelinde, kişisel verilerin korunması hakkı ile ilgili yaptığımız açıklamalarda, AİHM'nin içtihatlarına yer verdiğimiz için çalışmamızın bu kısmında Anayasa'nın 90. maddesinin son fıkrası gereğince AİHM'nin iç hukuktaki rolüne değinmek adına AİHM'nin bu konudaki yaklaşımına genel hatları ile değinilmiştir.

805 Kapani, a.g.e., s. 71.

806 Yokuş, Sevtap, "Avrupa İnsan Hakları Sözleşmesi'nin Türkiye'de Olağanüstü Hal Rejimine Etkisi", Beta Yayınları, İstanbul, 1996, s. 9.

807 Küzeci, a.g.e., s. 136.

biri içerisinde olup olmadığına baktıktan sonra, ortada söz konusu hakkın ihlaline neden olan bir sınırlama bulunup bulunmadığına bakmakta, en sonunda ise bu sınırlamanın ya da müdahalenin AİHS'nin 8. m.'sinin 2. fıkrasında ifade edilen durumlar nedeniyle gerçekleştirilip gerçekleştirilmediğine bakarak uyuşmazlığı karara bağlamaktadır.[808]

Ayrıca; AİHM, AİHS'nin 8. . m.'si çerçevesinin geniş, evrimsel bir bakış açısı ile ele almıştır. Mahkeme, günümüz koşullarını göz önünde bulundurarak, AİHS'nin yorumlanmasında kendine özgü yaklaşımını sürdürmektedir.[809]

3.5.1. 8. MADDE: ÖZEL VE AİLE HAYATINA (YAŞAMINA) SAYGI HAKKI

AİHS'nin 8. maddesinde[810] belirtildiği üzere, özel yaşam hakkı ve özel yaşamın gizliliği mutlak değildir. Bu nedenle, AİHS bunun üzerinde bir sınırlama rejimi uygulamaktadır. Yine de bu tür bir kısıtlama, AİHM tarafından test olarak adlandırılan bazı belirli koşulların yansıtılmış olmasına bağlıdır. Strasburg Mahkemesinin, AİHS kapsamındaki "kişisel veriler" kavramının, özellikle de tanımlanmış veya tanımlanabilir kişilere ilişkin durumla ilgili olarak, 108 sayılı Sözleşme'deki tanımı esas aldığı söylenebilir.[811] Genel hatları ile sınırlama sebepleri:

3.5.1.1. Kanuna Uygun Olarak

Yasal zeminde etkin ve uygun bir korumaya duyulan önemli ihtiyaç, müdahalenin kanun tarafından öngörülmesi gerektiği anlamına gelir ki, bu bir hakkın ayrıntılı olarak kanun ile sınırlandırılmasını ifade eder. Genel düzenleme ile sınırlama rejimi oluşturmak yasal kabul edilemez, kişisel bilgilerin toplanması, saklanması ve

---

808 Akgül, Aydın, "Avrupa İnsan Hakları Mahkemesi Kararlarında Kişisel Verilerin Korunması Hakkı", Terazi Hukuk Dergisi, Cilt: 9, S. 92, Yıl: Nisan 2014, s. 75.

809 Data Protection Pursuanttothe Right to Privacy in Human Rights Treaties, International Journal of Law and Information Technology, 1998, Vol: 6, s.7.

810 AİHS'nin tam metni için bkz. https://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf, Erişim tarihi, 05.04.2019.

811 AİHM Kararı: Amann v. Switzerland, Başvuru No: 27798/95, Tarih: 16.02.2000. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-58497, Erişim tarihi, 05.04.2019.

ifşa edilmesi için yasal bir temel oluşturulmasını gerektirir. Bu yasal sistemde, kanuni olarak özellikle de hakka orantısız müdahalelere karşı alınması gereken tedbirler belirlenmelidir.

3.5.1.2. Meşru Amaç

Bu hakka müdahalede bulunulmasını gerektiren meşru amaç söz konusu olduğunda, AİHS, m. 8/2'de kabul edilebilir bir zeminin sınırlı bir listesini ortaya koymaktadır. Bunlar sırasıyla, ulusal güvenlik konuları, kamu güvenliği, ülkenin ekonomik refahı, düzensizlik veya suçun önlenmesi, sağlık veya ahlakın korunması ve başkalarının hak ve özgürlüklerinin korunmasıdır.

3.5.1.3. Demokratik Bir Toplumda Gerekli Olmak

Bu hakka müdahalenin gerekçesini oluştururken, en zorlu kısım olarak, müdahalenin demokratik bir toplumda gerekli olup olmadığı tartışmasını ileri sürebiliriz. Strasburg Mahkemesi herhangi bir müdahalenin ilgili ve yeterli nedenlerle desteklenmesi gerektiğini ve izlenen meşru amaç veya amaçlarla orantılı olması gerektiğini belirtmektedir. Buna paralel olarak, Mahkeme, ulusal makamların -yargı organlarının- takdir yetkisine sahip olduklarını ve bunun kapsamının sadece meşru amacın doğasına değil, aynı zamanda müdahalenin özel niteliğine de bağlı olacağı düşüncesindedir.

3.5.2. AİHM İÇTİHADI

Kişisel verilerin korunması hakkına yönelik olarak AİHS'de ayrı bir hak tanımlanmadığını, Strasburg Mahkemesinin kişisel verilerin korunması hakkına yönelik yapılan başvuruları AİHS m. 8 üzerinden incelemeye aldığını, bu incelemeyi yaparken hangi kriterlere baktığını ve ne gibi sınırlama sebeplerini uyguladığını yukarıdaki bölümlerde ifade etmiştik. Bu bölümümüzde AİHM kararlarının belli başlılarını özellikle uygulamaya yön veren kararlarını inceleyeceğiz.

İncelememizi kararları gruplandırmak suretiyle yapacağız. Bu minvalde; "*Kişisel Verilerin Toplanması ve Saklanması*", *"Telefon Dinleme-Kaydetme, Ses-Fotoğraf-Görüntü Kaydı", "Tıbbi Verilerin Saklanması ve İfşa Edilmesi*

(Açıklanması)" şeklinde mahkemenin önüne en çok gelen kişisel verilerin korunması hakkının ihlalini içeren kararları ele alacağız.

3.5.2.1. Kişisel Verilerin Toplanması ve Saklanması

Kişisel verilere ilişkin olarak Mahkeme tarafından yapılan ilk uygulama **Klass and Others v. Germany**[812] davasıdır. Bu davada başvurucular, beş Alman hukukçudur. Almanya'da çıkarılan bir yasa ile yetkili mercilere, telefon dinlemesi, kişisel yazışmaların ve haberleşmenin takibi yetkisi verilmiştir. Ancak bireylere, kendileri aleyhinde alınan tedbirlere ilişkin, tedbir uygulaması bittiğinde dahi bilgi verilmemesi hususunda ve haklarında tedbir hükmedilenlere herhangi bir bildirim yükümlülüğü yüklemeyen Almanya'daki mevzuat hakkında şikâyette bulunmuştur. Mahkeme, **AİHS madde 8'in ihlal edilmediğine** karar vermiş ve Alman yasama organının, tartışmalı mevzuattan kaynaklanan müdahaleyi, 8. maddede güvence altına alınan demokratik bir toplumda ulusal güvenlik çıkarları ve düzensizlik veya suçun önlenmesi için gerekli gördüğü haktan yararlanarak değerlendirmek için gerekçelendirdiğini tespit etmiştir. Mahkeme, özellikle, polis devleti olarak niteleyen vatandaşların gizli gözetimine ilişkin yetkilerin, yalnızca demokratik kurumları korumak için kesin bir şekilde gerekli olduğu kadarıyla AİHS uyarınca kabul edilebilir olduğunu belirtmiştir. Ancak, AİHM'ye göre, günümüzde demokratik toplumlar, son derece sofistike casusluk ve terörizm biçimleriyle kendilerini tehdit altında buldukları ve bu durum, devletin, bu tür tehditlere karşı etkili bir biçimde mücadele etmesi gerektiği için, kendi yetki alanında faaliyet gösteren yıkıcı unsurların gizli gözetimini üstlenebilmesi için gerekli olması sonucunu doğurmuştur. *Mahkeme, e-posta, posta ve telekomünikasyon üzerinde gizli gözetim yetkileri veren bazı mevzuatların varlığının, istisnai koşullar altında, demokratik bir toplumda ulusal güvenlik ve/veya düzensizlik veya suçun önlenmesi için gerekli olduğunu değerlendirmiştir.*

Öte yandan, 23 Mart 1987 tarihli **Leander v. Sweden**[813] davası, bir marangozun işe alınmasında gizli bir idari kolluk dosyasının kullanılmasıyla ilgilidir.

---

812 AİHM Kararı: Klass and Others v. Germany, Başvuru No: 5029/71, Tarih: 06.09.1978. Kararın İngilizce tam metni için bkz. https://hudoc.echr.coe.int/eng#{"itemid":["001-57510"]}, Erişim tarihi, 28.01.2019.

813 AİHM Kararı: Leander v Sweden, Başvuru No: 9248/81, Tarih: 26.03.1987. Kararın İngilizce tam metni için bkz.. https://hudoc.echr.coe.int/eng?i=001-57519, Erişim tarihi, 28.01.2019.

Başvurunun konusu; Askeri Güvenlik Bölgesinin yanında yer alan Deniz Müzesinde geçici olarak görev yapan başvuru sahibi, sendikal faaliyetleriyle ilgili verilerin depolanmasından şikayetçi olmuş ve bunun, söz konusu istihdamdan dışlanmasına yol açtığını iddia etmiştir. Kişisel veya siyasi geçmişinde hiçbir şeyin, onu Güvenlik Departmanı siciline kaydettirmeyi ve kendisinin "güvenlik riski" olarak sınıflandırılmasını gerekli kılacak bir şey olarak değerlendirilemeyeceğini savunmuştur. Mahkeme, Sözleşme'nin **8. maddesinin ihlal edilmediğine** karar vermiştir. *Mahkeme ayrıca, demokratik bir toplumda, istihbarat servislerinin varlığının ve verilerin depolanmasının, yasal amaçlara, yani kargaşa veya suçun önlenmesine ya da ulusal güvenliğin sağlanmasına yönelik olarak, vatandaşların çıkarları üzerinde yasal ve geçerli olabileceğini de hatırlatmıştır*. İsveç Hükümeti, ulusal güvenlik menfaatlerinin başvuru sahibinin kişisel çıkarları üzerinde olduğunu düşünmeye yetkili olduğu kararda belirtilmiştir. *Mahkeme, aynı zamanda, söz konusu yasanın, ombudsman ve Adalet Bakanı tarafından denetlenmesini içeren pek çok önlemi içerdiğini vurgulamıştır*. Yine de bu karar, Mahkeme'nin başvurucunun meslekte ne kalitede iş yapacağı ve bu tür işlerin gerekliliklerini göz ardı etmesi nedeniyle eleştirilebilir. Dahası, iç hukuk yolu ile yeterli izleme mekanizması uygulanmış olsa bile, başvuru sahibi, güvenlik soruşturmalarına ilişkin verileri almalıdır. Bu karardan hemen sonra, Bakanlar Komitesi, Polis Sektöründe Kişisel Verilerin Kullanımının Düzenlenmesine İlişkin No. R(87) 15 sayılı Tavsiye Kararını Yayımladı.[814] Bu tavsiye kararının 2/2 maddesinde *"Bir bireyle ilgili verilerin, onun bilgisi olmadan toplandığı, saklandığı ve verilerin silinmediği hallerde, polis faaliyetlerinin amacı ile ilgili olarak, mümkün olduğu ölçüde, bu bilginin kendisine bildirilmesi, polis faaliyetlerinin amacının artık önyargılı olma olasılığının olmaması nedeniyle, gereklidir."* denilmiştir.

7 Temmuz 1989 tarihli **Gaskin v. the United Kingdom**[815], kararına baktığımızda; sosyal hizmetler çatısı altında bir çocuk olarak büyüyen başvuru sahibi,

814 http://ec.europa.eu/justice/data-protection/law/files/coe-fra-rpt-2670-en-471.pdf, Erişim tarihi, 28.01.2019.

815 AİHM Kararı: Gaskin v. the United Kingdom, Başvuru No: 10454/83, Tarih: 07.07.1989. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-57491, Erişim tarihi, 28.01.2019.

reşit olduğunda, kişisel sorunlarını aşmak için geçmişini öğrenmek istemiştir. Gizli bilgiler içerdiği gerekçesiyle, dosyasına erişimi idare tarafından reddedilmiştir. Mahkeme, **Sözleşmenin 8. maddesinin ihlal edildiğine** karar vermiş ve başvuru sahibinin özel ve aile hayatına saygı gösterilmediğini tespit etmiştir. Böyle bir sistemde, bağımsız bir denetim otoritesinin idareden talep edilen kişisel verilerin verilmemesi nedeninin orantılılık ilkesine uygun olup olmadığının denetlenmesi halinde hukuka uygun sayılabileceği vurgulanmıştır. Mevcut davada başvuru sahibi için böyle bir prosedür mevcut değildir. AİHM, özellikle bu kararda, devletlerin orantılı olarak pozitif yükümlülüklerini vurgulamıştır. İdarenin, başvuranın kişisel verilerini istemesi ile ilgili talebini reddetmesi halinde, bu ret kararının bağımsız bir denetim organı tarafından denetlenmesi koşuluyla, ulusal güvenliğe vurgu yaparak veri öznesi olan kişinin başvurusunu reddedebilir. Bu nedenle, başvuru sahiplerinin her türlü kişisel veri dosyasına ulaşmakta özgür oldukları söylenemez.[816]

16 Şubat 2000 tarihli **Amann v. Switzerland**[817] kararında, başvuru sahibine eski Sovyet Büyükelçiliğinden gelen bir telefon çağrısı üzerine yetkili savcılık tarafından başvuru sahibi hakkında bir gizli servis dosyası oluşturulmasını talep eden koruma tedbiri ile ilgilidir. *Mahkeme, telefon görüşmesinin kaydedilmesi, dosyanın oluşturulması ve saklanması nedeniyle Sözleşmenin* **8. maddesinin ihlal edildiğine karar vermiş** ve gerekçesinde İsviçre yasalarının, yetkililere tanınan takdir marjını açıkça belirtmediğini, hukuki öngörülebilirlik hususunun mevcut olmadığını bundan mütevellit başvuru sahibinin özel hayatına saygı hakkının ihlal edildiğini tespit etmiştir. Mevcut mevzuat, AİHM tarafından, polisin verileri nasıl topladığı ve sakladığına ilişkin şartları tespit etmeye yeterli görülmemiştir.

04 Mayıs 2000 tarihli **Rotaru v. Romania**[818] davasında, başvuru sahibi komünist rejime yönelik eleştirisini dile getirdiği için 1948 yılında bir yıl hapis

---

816 http://folk.uio.no/lee/oldpa.g.e/articles/Human_rights.pdf, Erişim tarihi, 30.01.2019; Lee A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", International Journal of Law and Information Technology, Vol. 6, No. 3, s. 278.

817 AİHM Kararı: Amann v. Switzerland, Başvuru No: 27798/95, Tarih: 16.02.2000. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-58497, Erişim tarihi, 28.01.2019.

818 AİHM Kararı: Rotaru v Romania, Başvuru No: 28341/95, Tarih: 04.05.2000. Kararın İngilizce tam metni için bkz.. http://hudoc.echr.coe.int/eng?i=001-58586, Erişim tarihi, 01.02.2019.

cezasına çarptırılmıştır. Bununla beraber, başvuru sahibi, Romanya İstihbarat Servisi tarafından kendisi hakkında tutulan bir dosyada yanlış olduğunu iddia ettiği bilginin aksinin ispat edilmesinin imkânsız olduğundan şikâyetçi olmuştur. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vermiştir. Mahkeme, kamuya ait bilgilerin, yetkililer tarafından tutulan dosyalarda sistematik olarak toplandığı ve depolandığı durumların özel yaşam kapsamına girebileceğini özellikle belirtmiştir. Bu tür bilgilerin bir kişinin uzak geçmişiyle ilgili olduğunu vurgulayan mahkeme, *ayrıca iç hukuka ait hiçbir hükmün kaydedilecek bilgi türlerini, bilgi toplama ve tutma gibi gözetim tedbirlerinin kimlere karşı alınabileceğini, bu tedbirlerin alınabileceği koşullar veya bu prosedürün nasıl uygulanabileceğini tanımlamadığını not etmiştir*. *Benzer şekilde, yasa, tutulan bilginin güncelliğine veya tutulabileceği sürenin uzunluğuna yönelik bir sınırlama getirmemiştir. Son olarak, dosyalara başvurma yetkisine sahip kişiler, dosyaların niteliği, izlenecek prosedür veya bu şekilde elde edilen bilgilerin kullanılması ile ilgili açık ve ayrıntılı bir hüküm bulunmamaktadır.*

06 Haziran 2006 tarihli **Segerstedt/Wibergand Others v. Sweden**[819], kararına değinecek olursak, bu davada, başvuru sahiplerinin İsveç Güvenlik Polisi tarafından haklarında tutulan tüm dosyalara erişim talepleri, kendilerine erişim verilmesi halinde suçun önlenmesine ya da ulusal güvenliğin korunmasına zarar verebileceği gerekçesiyle reddedilmiştir. Mahkeme, başvuru sahiplerine Güvenlik Polisi tarafından saklanan bilgilere tam erişim izni verilmemesi nedeniyle **Sözleşme'nin 8. maddesinin ihlal edilmediğine** karar vermiştir. Ulusal gizli polis siciline tam erişimin reddedilmesinin, *Devletin bu tür bilgilerin sağlanmasının, ulusal güvenliği korumak ve terörizmle mücadele için tasarlanmış bir gizli gözetleme sisteminin etkinliğini tehlikeye atabileceğinden gerekli olduğunu mahkeme hatırlatmıştır.* Mahkeme, mevcut geniş kapsamlı takdir marjını dikkate alarak, İsveç'in, ulusal güvenlik çıkarlarının ve terörle mücadelenin, başvuranların güvenlik polis sicilinde kendilerine ait bilgilerin ne ölçüde tutulduğu konusunda, menfaat sahiplerinin çıkarları üzerinde etkili olduğunu dikkate almaya yetkili olduğuna karar vermiştir.

819 AİHM Kararı: Segerstedt/Wibergand Others v Sweden, Başvuru No: 62332/00, Tarih: 06.06.2006. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-75591, Erişim tarihi, 01.02.2019.

10 Şubat 2011 tarihli **Dimitrov-Kazakov v. Bulgaria**[820] kararında, başvuru sahibinin adı, bir tecavüzle ilgili olarak, bir tecavüz hakkında ifadesi alındıktan sonra, bahse konu suçtan dolayı hakkında bir suçlama olmamasına rağmen, polis siciline "fail" olarak kişisel verileri işlenmiştir. Bu nedenle başvurucu, daha sonra, farklı tarihlerde polis tarafından tecavüz şikayetleri veya genç kızların kaybolmalarıyla ilgili birtakım polisiye kontrollere tabi tutulmuştur. Başvuru sahibi, kendisinin suçlanmamasına rağmen fail olarak polis kayıtlarına yazılması nedeniyle şikâyetçi olmuştur. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vermiş ve polis dosyasına dahil edilmenin, bu madde anlamında "yasaya uygun" olmadığına hükmetmiştir.

3 Eylül 2015 tarihli **Sõro v. Estonia**[821] kararında; başvuru sahibinin, Sovyetler Birliği döneminde SSCB Devlet Güvenlik Komitesi'nde (KGB) bir şoför olarak istihdam edilmesine yönelik bilginin, 2004 yılında Estonya Devlet Gazetesinde yayınlanmasına ilişkin şikâyeti ile ilgilidir. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vermiş ve başvuru sahibinin davasında bu tedbirin, aranılan amaçlarla orantısız olduğunu tespit etmiştir. Mahkeme, özellikle, ilgili ulusal mevzuat kapsamında, eski güvenlik hizmetlerinin tüm çalışanları hakkındaki bilgilerin -başvuru sahibinin davasında olduğu gibi, sürücüler de dahil olmak üzere- gerçekleştirdikleri özel görevden bağımsız olarak yayınlandığını not etmiştir. Başvuru sahibinin davasında, söz konusu bilgiler 2004 yılında, Estonya bağımsızlığını ilan ettikten yaklaşık 13 yıl sonra yayınlanmıştır ve duyurunun yayınlandığı tarihte başvuru sahibinin maruz kaldığı olası tehdit hakkında bir değerlendirme yapılmamıştır. Son olarak, İfşa Yasası'nın kendisi, başvuru sahibinin istihdam edilmesi konusunda herhangi bir kısıtlama getirmemesine rağmen, görüşleri nedeniyle meslektaşları tarafından alay edilerek işini bırakmaya zorlanmıştır. Mahkeme, bu tür bir sonuç kanun tarafından aranmasa bile, vermiş olduğu kararda, başvuru sahibinin özel

820 AİHM Kararı: Dimitrov-Kazakov v. Bulgaria, Başvuru No: 11379/03, Tarih: 10.02.2011. Kararın İngilizce tam metni için bkz. https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/11379-03-dimitrov-kazakov-v-bulgaria-rezolucja-komitetu-521918425, Erişim tarihi, 01.02.2019.

821 AİHM Kararı: Sõro v. Estonia, Başvuru No: 50073/07, Tarih: 3.09.2015. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-156518, Erişim tarihi, 03.02.2019.

hayatına saygı gösterme hakkına yapılan müdahalenin ne kadar ciddi olduğuna yer vermiştir.

Eylül 2017 tarihli **Barbulescu v. Romania**[822] kararında; başvuru -Büyük Dairenin karar bağladığı bir başvurudur-, özel bir şirketin, bir çalışanını (başvuru sahibi) elektronik iletişimini izledikten ve içeriklerine eriştikten sonra işten çıkarma kararı alması olayı ile ilgilidir. Başvuru sahibi savunmasında, işverenin kararının kendi mahremiyetinin ihlal edilmesine dayandığını ve yerel mahkemelerin özel hayatına ve yazışmalarına saygı hakkını koruma konusunda yerel makamların ve mahkemelerin yeterince denetleme yapmadığı hususunu ileri sürerek şikâyetçi olmuştur. Büyük Daire, altıya karşı on bir oyla, **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vermiş ve Romanya makamlarının, başvuru sahibinin özel hayatına ve yazışmalarına saygı gösterme hakkını yeterince korumamış olduğuna hükmetmiştir. Sonuç olarak, mahkeme, devletin söz konusu çıkarlar arasında adil bir denge kurmayı başaramadığını belirtmiştir. *Özellikle, ulusal mahkemeler, başvuru sahibinin haberleşmesinin izlenebileceği olasılığı konusunda, işveren tarafından önceden bildirimde bulunup bulunmadığını tespit edememiş; ya da izlemenin niteliği ya da kapsamı ya da özel hayatına ve yazışmalarına izinsiz girme derecesi hakkında bilgilendirilmediği gerçeğini de dikkate almadıklarını belirterek* ayrıca, ulusal mahkemeler, öncelikle, izleme şeklideki tedbirlerin uygulamaya konulmasını haklı kılan özel nedenleri, ikinci olarak, işverenin başvuru sahibinin özel yaşamı ve yazışmalarına daha az müdahale gerektiren önlemleri kullanıp kullanamayacağını ve üçüncü olarak, iletişimin bilgisi olmadan erişilmiş olup olmadığını belirleyemediklerinden bahisle,AİHM ihlal kararı vermiştir.

3.5.2.2. Telefon Dinleme-Kaydetme, Ses-Fotoğraf-Görüntü Kaydı

26 Nisan 1985 tarihli **Malone v. the United Kingdom**[823] kararında, çalıntı malların haksız ticaretiyle ilgili bir dizi suç ile suçlanan başvuru sahibi, özellikle polis

822 AİHM Kararı: Bărbulescu v Romania, Başvuru No: 61496/08, Tarih: 05.09.2017. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-177082, Erişim tarihi, 04.02.2019.

823 AİHM Kararı: Malone v the United Kingdom, Başvuru No: 8691/79, Tarih: 26.04.1985. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-57533, Erişim tarihi, 05.02.2019.

tarafından veya polis adına ve belirli bir telefon üzerinde aranan numaraları ve her aramanın süresini ve zamanını kaydeden bir cihazın kullanımını içeren bir işlem uygulanarak telefonunun "kontrol edilmesi" gerekçesi ile posta ve telefon iletişiminin engellenmesinden şikayetçi olmuştur. Mahkeme, yasaya uygun olmadıkları için hem iletişimin ele geçirilmesi hem de polis tarafından kontrol (ölçüm) kayıtlarının serbest bırakılması ile ilgili olarak, **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vermiştir. *Mahkeme, özellikle, kanunda belirtilmiş olan bir şeyin, devlet tarafından hukuka göre düzenlenmiş olsa bile, bunun yasal olduğu anlamına gelmediğine vurgu yapmıştır. AİHM, yasanın, hukukun üstünlüğünün ruhunu taşıması gerektiğine ve bireyleri keyfi müdahaleye karşı korumak için bazı yasal önlemleri bünyesinde barındırması gerektiğine hükmetmiştir. Ayrıca, yasa ve bağımsız denetleyicilerin -bu kurum veya mahkeme olabilir- otoritelerin takdir payını nasıl uygulanmasına ilişkin olarak hükümler içermesi gerektiği mahkeme tarafından belirtilmiştir.*

24 Nisan 1990 tarihli **Kruslin v. France**[824] davasına değinecek olursak, bu başvuruda, cinayet davasında sorgu hakiminin hükmettiği bir telefon kaydının tespiti ile ilgilidir. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vermiş ve *Fransız hukukunun, yetkililerin bu alandaki takdir yetkisinin kapsamını ve şeklini makul bir açıklıkla belirtmediğine hükmetmiştir.* Bu bağlamda, AİHM, başvurucunun, *hukukun üstünlüğünün kabul edildiği demokratik bir toplumda her bir vatandaşın sahip olduğu asgari korumadan başvurucunun istifade etmediği gerekçesiyle ihlal kararı vermiştir.*

26 Haziran 1997 tarihli **Halford v. the United Kingdom** davasında[825], emniyet müdür yardımcısı olarak görev yapan başvurucuya iş ve özel kullanımı için olmak üzere iki adet telefon tahsis edilmiştir. Bu telefonlar, kamu ağının dışındaki bir telekomünikasyon sistemi olan polis dahili telefon şebekesine bağlı olarak

824 AİHM Kararı: Kruslin v. France, Başvuru No: 11801/85, Tarih: 24.04.1990. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-57626, Erişim tarihi, 04.02.2019.

825 AİHM Kararı: Halford v the United Kingdom, Başvuru No: 20605/92, Tarih: 26.06.1997. Kararın İngilizce tam metni için bkz.. http://hudoc.echr.coe.int/eng?i=001-58039, Erişim tarihi, 04.02.2019; AİHM Kararı: Huvig v France, Başvuru No: 11105/84, Tarih: 24.04.1990. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-57626 , Erişim tarihi, 04.02.2019.

çalışmaktadır. Ev telefonu ise, "ağ sonlandırma noktası" üzerinden kamu telekomünikasyon ağına bağlı bir telefon aygıtından oluşuyordu. Başvurucu, kendisine tahsis edilen ev ve iş telefonu usule aykırı bir şekilde telefon ağlarının polis merkezine bağlı olmasının sağladığı kolaylıkla dinlendiğini belirtmiştir. Başvuru sahibinin ofis telefonlarından yapılan aramalarla ilgili olarak AİHM, başvurucunun ofis telefonu dahi olsa özel hayatın gizliliğinin korunmasına hükmederek **8. maddenin ihlali** yönünde karar vermiştir. Yukarıdaki nedenlerin tümü için Mahkeme, Bayan Halford'un ofis telefonlarından yaptığı konuşmaların "özel yaşam" ve "yazışma" kavramları kapsamında yer aldığına karar vermiştir.

25 Mart 1998 tarihi **Kopp v. Switzerland**[826] kararına baktığımızda, bu başvuru, başvuru sahibinin avukatlık firmasına ait telefon hatlarının Federal Cumhuriyet Savcısının emirleri kapsamında izlenmesi ile ilgilidir. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vererek, *İsviçre yasalarının, konuyla ilgili makamların takdir yetkisinin kapsamını ve şeklini yeterince açık bir şekilde belirtmediğine hükmetmiştir. Mahkeme sonuç olarak, bir avukat olarak başvuru sahibinin, demokratik bir toplumda hukukun üstünlüğünün gerektirdiği asgari koruma derecesinden yararlanamadığı değerlendirmesinde bulunmuştur*.

25 Eylül 2001 tarihli **P. G. and J.H. v. the United Kingdom**[827] kararında, başvuru sahipleri bir polis karakolunda seslerinin kayıt altına alınması neticesinde bir soygun gerçekleştirmek üzere oldukları iddiası ile tutuklanmalarına yönelik bir karardır. Burada polisin elinde başvurucuların yakın bir tarihte hırsızlık yapacağına ilişkin bir ihbar almasının akabinde, polis, dinlemek ve telefon kayıtlarını incelemek için başvurucuların evlerine bir cihaz yerleştirdi. Polis tarafından yakalandıktan sonra bir hapishaneye götürüldüklerinde, içinde bulundukları hapishaneye bir dinleme cihazı daha konuldu. Mahkeme, polis karakolunda gizli dinleme cihazlarının kullanımına ilişkin olarak **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vermiştir. *Mahkeme,*

826 AİHM Kararı: Kopp v. Switzerland , Başvuru No: 23224/94, Tarih: 25.03.1998. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-58144, Erişim tarihi, 04.02.2019.

827 AİHM Kararı: P. G. and J.H. v. the United Kingdom, Başvuru No: 44787/98, Tarih: 25.09.2001. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-59665, Erişim tarihi, 04.02.2019.

bahse konu zamanda, polis tarafından gizli dinleme cihazlarının kullanımının düzenlenmesi için yasal bir alt yapısının bulunmadığına özellikle dikkat çekerek, başvuru sahiplerinin özel yaşam hakkına müdahalenin kanuna uygun olmadığını tespit etmiştir. Bu davada Mahkeme ayrıca, gizli dinleme cihazının bir apartman dairesinde kullanılması nedeniyle **Sözleşme'nin 8. maddesinin ihlal edildiğin** eve bir telefon kullanımı hakkındaki bilgilerin elde edilmesine ilişkin olarak ise **8. maddenin ihlal edilmediğine** karar vermiştir. AİHM, ayrıca, müdahalenin mahkeme içtihatlarında belirtilen yasa ile sınırlama hususlarının sağlanmadan gerçekleştirildiğini de tespit etmiştir.[828]

22 Ekim 2002 tarihli **Taylor-Sabori v. the United Kingdom**[829] kararında; özellikle, gizli bir izleme ve gözetleme operasyonunun bir parçası olarak, başvuru sahibinin çağrı cihazına gönderilen mesajların polis tarafından ele geçirilmesi ile ilgilidir. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vermiştir. Söz konusu olayların gerçekleştiği zamanda, özel bir telekomünikasyon sistemi aracılığıyla iletilen çağrı mesajlarının dinlenmesini (müdahale edilmesini) düzenleyen herhangi bir yasal düzenleme bulunmadığından bahisle mahkeme, müdahalenin yasaya uygun olmadığını tespit etmiştir.

17 Ekim 2003 tarihli **Perry v. the United Kingdom**[830] kararında, başvuru sahibi, kaçak taksi (mini-cab) şoförlerine yönelik bir dizi silahlı soygun ile bağlantılı olarak tutuklanmış ve bir kimlik tespiti yapılmasını beklemeden serbest bırakılmıştır. Polis başvurucunun kimliğini tespit edebilmek için onu gizli bir şekilde kameraya almıştır. Başvuru sahibi, polisin kendisini teşhis amacıyla gizli bir şekilde videoya

---

828 AİHM Kararı: Lewis v. the United Kingdom, Başvuru No: 1303/02, Tarih: 25.11.2003. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/fre?i=001-67226, Erişim tarihi, 05.02.2019; AİHM Kararı: Chalkley v. the United Kingdom, Başvuru No: 63831/00, Tarih: 12.09.2003. Kararın İngilizce tam metni için bkz.. http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-61135&filename=001-61135.pdf, Erişim tarihi, 05.02.2019.

829 AİHM Kararı: Taylor-Sabori v. the United Kingdom, Başvuru No: 47114/99, Tarih: 22 October 2002. Kararın İngilizce tam metni için bkz. https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-637291-642797&filename=003-637291-642797.pdf, Erişim tarihi, 06.02.2019.

830 AİHM Kararı: Perry v. the United Kingdom, Başvuru No: 63737/00, Tarih: 17.10.2003. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/fre?i=001-61228, Erişim tarihi, 06.02.2019.

aldığını ve video kasetinin kendisine yönelik kovuşturmada kullanıldığını belirterek şikayetçi olmuştur. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vermiştir. Mahkeme, başvuranın, bir video tanımlama prosedüründe kullanılmak üzere polis karakolunda görüntü çekilmesinin kameraların normal kullanımının ötesine geçtiğini ve başvuru sahibinin özel hayatına saygı gösterme hakkına müdahale anlamına geldiğini belirterek ihlal kararı vermiştir. AİHM'e göre, söz konusu müdahale yasaya uygun değildir. *Çünkü polis, yürürlükteki yasalarda belirtilen prosedürlere uymamıştır. Başvuru sahibinin rızasını almadıkları ve teybe kayıt yapıldığını da bildirmedikleri gibi, bu konudaki hakları konusunda kendisini bilgilendirmemişlerdir.*

28 Ocak 2003 tarihli **Peck v. the United Kingdom**[831] davasına baktığımızda, bu dava, yerel meclis tarafından kurulan kapalı devre televizyon (CCTV) kamera ile bir sokakta çekilen ve başvuru sahibinin bileklerini kestiğini gösteren görüntülerin medyaya sunulmasıyla ilgilidir. Mahkeme, **Sözleşmenin 8. maddesinin ihlal edildiğine** karar vermiş ve Belediye Meclisi'nce yapılan çekimlerin ifşasına yeterli güvenlik önlemlerinin sağlanmadığını ve başvuru sahibinin özel yaşamına, orantısız ve haksız müdahalede bulunulduğunu tespit etmiştir. AİHM, özellikle, meclis tarafından *başvuru sahibinin rızası alınmadan veya kimliğini gizlemeksizin alınan görüntülerin kamuoyuna doğrudan doğruya ifşa edilmesini haklı gösterecek, ya da meclisin, medya tarafından bu tür maskelemenin gerçekleştirilebileceği yönünde gerekli adımları atmadan medyaya ifşa etmesini haklı gösterecek uygun veya yeterli nedenlerin bulunmadığını tespit etmiştir*. Suçun önlenmesi amacı ve ifşa edilmesinin içeriği, bahse konu davada, bu bağlamda özel inceleme ve özen gösterilmesini taraf devlete yüklemektedir.

02 Eylül 2010 tarihli **Uzun / Almanya**[832] kararında, aşrı sol bir hareket tarafından gerçekleştirilen bomba saldırılarına karıştığından şüphelenilen başvuru sahibi, özellikle GPS üzerinden gözetlenmesinin ve ona karşı yürütülen ceza

831 Peck v. the United Kingdom, bas.no.44647/98, T.28.01.2003. Kararın İngilizce tam metni için bkz.. http://hudoc.echr.coe.int/eng?i=001-177082, Erişim tarihi, 04.02.2019.

832 Uzun v. Almanya, bas. no.35623/05, Kararın İngilizce tam metni için bkz.. http://hudoc.echr.coe.int/eng?i=001-177082, Erişim tarihi, 04.02.2019.

yargılamalarında elde edilen verilerin kullanımının özel hayata saygı hakkını ihlal ettiğini belirterek şikâyetçi olmuştur. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edilmediğine** karar vermiştir. *GPS gözetimi ve bu şekilde elde edilen verilerin işlenmesi ve kullanılması, kabul edilmelidir ki, başvuru sahibinin özel hayatına saygı gösterme hakkı ile çelişmektedir. Ancak, Mahkeme, ulusal güvenliğin, kamu güvenliğini, mağdurların haklarının korunmasını ve suçun önlenmesinin meşru amaçlarını gözettiğini not etmiştir.* Aynı zamanda AİHM bu müdahalenin ölçülü bir müdahale olduğuna karar vermiştir. GPS gözetimi, ancak daha az müdahaleci inceleme yöntemlerinin yetersiz olduğu kanıtlandıktan sonra, nispeten kısa bir süre (yaklaşık üç ay) gerçekleştirilmiş ve başvuru sahibini, yalnızca suç ortağının arabasıyla seyahat ederken bu tedbire başvurulmuştu. Bu nedenle, başvuru sahibinin tam ve kapsamlı bir gözetime tabi tutulduğu söylenemez. Soruşturmanın çok ciddi suçlarla ilgili olduğu göz önünde bulundurulduğunda, başvuru sahibinin GPS tarafından izlenmesi demokratik bir toplumda gerekli olmasından bahisle AİHM başvurucunun hakkının ihlal edilmediğine karar vermiştir.

18 Mayıs 2010 tarihli ve 26839/05 sayılı **Kennedy v. the United Kingdom**[833] kararında, öldürme suçundan mahkûm edilen -eksik ve çatışan deliller nedeniyle tartışmalı bir davada- 1996 yılında hapishaneden salıverilen başvuru sahibi, daha sonra adaletin işlemediğine dair yürütülen kampanyada aktif rol üstlenmiştir. Küçük bir iş kurduktan sonra polis tarafından dinlenildiğinden şüphelenerek, yetkili mahkemeye şikâyette bulunmuştur. Sonuç olarak, 2005 yılında kendisine, şikayetlerine ilişkin olarak lehine hiçbir tespit yapılamadığı bildirilmiştir. Başvuru sahibi, iletişimlerinin dinlendiği iddiasıyla AİHM'ye bu kez başvurmuştur. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edilmediğine** karar vermiş ve Birleşik Krallık Hukukunun, bir *Uygulama Tüzüğü'nün yayınlanmasıyla getirilen açıklıklarla birlikte iç iletişimin engellenmesi hakkındaki kanunun, dinleme izinlerinin izlenmesi ve işlenmesi ile toplanan verilerin işlenmesi, iletilmesi ve imha edilmesi prosedürlerini yeterli bir*

833 AİHM Kararı: Kennedy v. the United Kingdom, Başvuru No: 26839/05, Tarih: 18 Mayıs 2010. Kararın İngilizce tam metni için bkz. https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-98473&filename=001-98473.pdf, Erişim tarihi, 08.02.2019.

açıklıkla ortaya koyduğunu tespit etmiştir. Ayrıca, bu prosedürlerin hukuki denetiminde ve işleyişinde önemli eksiklikler olduğuna dair bir kanıt bulunamamıştır.

Aralık 2015 tarihli **Roman Zakharov v. Russia**[834] Büyük Daire kararına baktığımızda, bu karara konu olayın Rusya'daki cep telefonu iletişiminin gizli olarak dinlenmesi sistemi ile ilgili olduğu görülmektedir. Bir yayıncılık şirketinin genel yayın yönetmeni olan başvuru sahibi, özellikle, Rusya'daki mobil şebeke operatörlerinden, yasalar uyarınca, yasa uygulayıcı kuruluşların operasyonel arama faaliyetlerini yürütmesine olanak tanıyan teçhizat tesis etmelerinin talep edildiğini ve Rusya yasalarında yeterli güvenceler olmadan örtülü dinlemeye izin verildiğinden bahisle şikayetçi olmuştur. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vermiş ve iletişimin dinlenmesini düzenleyen Rusya yasalarının, keyfiliğe karşı yeterli ve etkili önlemler sağlamadığını ve özellikle Rusya'da olduğu gibi gizli servislerin ve polisin teknik yollarla tüm cep telefonu iletişimine doğrudan erişime sahip olduğu bir sistemde kötüye kullanım riskine sahip olduğunu tespit etmiştir. Rusya'daki kamu yetkililerinin gizli gözetim tedbirlerine başvurma yetkileri, bu tedbirlerin süresi, özellikle de devam edilmediği (durdurulduğu) durumlar; dinlemenin yanı sıra, elde edilen verilerin saklanması ve imha edilmesi için izin verme prosedürleri ve dinlemenin denetlenmesi alanlarında Mahkeme, özellikle yasal çerçevede eksiklikler tespit etmiştir. Üstelik, haberleşmenin denetlenebilmesi için yalnızca bir ihbar notunun yeterli ve makul bir gerekçe olmadığını Mahkeme not etmiştir.

12 Ocak 2016 tarihli **Szabóand Vissy v. Hungary**[835] kararında, 2011 yılında başlatılan gizli terörle mücadele gözetimine ilişkin Macar mevzuatı ile ilgiliydi. Başvuru sahipleri, özellikle, ulusal güvenlik amaçlarına yönelik gizli gözetleme konusunda Macaristan yasal mevzuatı çerçevesinde haksız ve orantısız olarak müdahaleci tedbirlere maruz kalabilecekleri yönünde şikâyetçi olmuşlardır. Başvuru sahipleri, bu yasal çerçevenin, özellikle adli kontrol talebinde bulunmak için kötüye

834 AİHM Kararı: Roman Zakharov v. Russia, Başvuru No: 82201/54 Tarih: 04.12.2015. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-159324, Erişim tarihi, 08.02.2019.

835 AİHM Kararı: Szabóand Vissy v. Hungary, Başvuru No: 0142016, Tarih: 12.01.2016. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-160020, Erişim tarihi, 08.02.2019.

kullanıldığını iddia etmişlerdir. Macaristan Hükümeti, bunun, günümüz terörizminin almış olduğu şeklin doğal bir sonucu olduğunu, iletişimin büyük çapta gözetimi de dahil olmak üzere, terör olaylarını önlemek için hükümetlerin en son teknolojilere başvurduklarını savundu. Ancak, Mahkeme söz konusu mevzuatın kötüye kullanımdan kaçınmak için yeterli koruma sağladığına ikna olmayarak özellikle yeni teknolojiler sayesinde, operasyon kapsamı dışındaki kişilerle ilgili verilere kolayca müdahale edebileceğini belirtmiştir. Üstelik, bu tür önlemlerin emri, tamamen yürütme alanında gerçekleşmekteydi ve iletişimin dinlenmesinin sıkı bir şekilde gerekip gerekmediği herhangi bir etkin düzeltici önlem olmaksızın yargı denetimine imkân vermeksizin bu tedbirin gerçekleştiğinden bahisle ihlal olduğuna hükmetmiştir.

28 Kasım 2017 tarihli ve 365201 sayılı **Antovićand Mirković v. Montenegro**[836] kararına değinecek olursak, bu karar, Karadağ Üniversitesi Matematik Okulu'nda öğretim görevlisi olan iki profesörün, video gözetim sistemi kurulduktan sonra mahremiyetin ihlaline ilişkin şikayetleri ile ilgilidir. Profesörler, toplanan bilgiler üzerinde etkili bir denetimin bulunmadığını ve gözetimin yasaya aykırı olduğunu belirttiler. Yerel mahkeme, başvuru sahiplerinin eğitim verdikleri yerlerin kamusal alan olması nedeniyle tazminat talebini reddetti. AİHM ise önüne gelen bu olay ile ilgili olarak, kamera gözetlemesinin yasaya uygun olmadığına ve **Sözleşme'nin 8. maddesinin (özel hayata saygı hakkı) ihlal edildiğine** hükmetmiştir. *Mahkeme öncelikle, Hükümet'in, gözetlenen alanın bir kamu, çalışma alanı olması nedeniyle hiçbir gizlilik meselesinin söz konusu olmadığı gerekçesiyle davanın kabul edilemez olduğu yönündeki iddiasını reddetmiştir*. Bu bağlamda, Mahkeme özellikle, özel hayatın mesleki faaliyetler içerebileceği tespitinde bulunmuş ve bu hususun başvuru sahipleri için de geçerli olduğunun düşünüldüğünü belirtmiştir. Davanın esasına müteallik olarak Mahkeme, daha sonra, kamera gözetiminin başvuranların gizlilik hakkına müdahale teşkil ettiğini ve kanıtların, denetiminin iç hukuk hükümlerini ihlal ettiğini gösterdiğini tespit etmiştir.

836 AİHM Kararı: Antovićand Mirković v. Montenegro, Başvuru No: 365201, Tarih: 28.11.2017. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-178904, Erişim tarihi, 08.02.2019.

3.5.2.3. Tıbbi Verilerin Saklanması ve İfşa Edilmesi (Açıklanması)

Daha önce de belirtildiği üzere, tıbbi veriler hem 108 sayılı sözleşmeye göre hem de Bakanlar Komitesi'nin tavsiye niteliğindeki kararına göre ek önlemler alınmasını gerektiren hassas verilerdir. Tavsiye kararına[837] göre, *"... "Tıbbi veriler" ibaresi, bir bireyin sağlığıyla ilgili tüm kişisel verileri ifade eder. Aynı zamanda, genetik verilere olduğu kadar sağlıkla açık ve yakın bir bağlantıya sahip olan verilere de atıfta bulunur."... "genetik veri" ibaresi, bir bireyin kalıtsal özellikleri ile ilgili olarak, ne türden olursa olsun, ilgili bir birey grubu içindeki bu tür özelliklerin kalıtım paterniyle ilgili her türlü veriyi ifade eder."*.

Aynı zamanda, herhangi bir genetik bilginin (genlerin) tanımlanabilir nitelikte olup olmadığına bakılmaksızın, sağlık veya hastalığın herhangi bir yönü ile ilgili olarak, bir bireyde veya genetik bir satırda herhangi bir genetik bilginin (genler) taşınmasına ilişkin tüm verilere atıfta bulunur.

Genetik satır (hat), yaratılıştan kaynaklanan ve iki veya daha fazla kişi tarafından paylaşılan genetik benzerliklerin oluşturduğu satırdır.".

Öte yandan, tıbbi verilerle ilgili bir başka belgede, 10. maddeye[838] göre, *"Herkes, kendi sağlığıyla ilgili bilgilerle ilgili olarak özel hayata saygı gösterme hakkına sahiptir. Herkes kendi sağlığı hakkında toplanan bilgileri öğrenme hakkına sahiptir. Ancak, bireylerin bu şekilde bilgilendirilmemesi istekleri incelenir*." denilmektedir.

25 Şubat 1997 tarihli ve 22009/93 sayılı **Z v. Finland**[839] davasında, başvuru sahibinin durumunun, kocasına yönelik uygulanan cezai işlemler neticesinde HIV-pozitif olarak ifşa edilmesiyle ilgilidir. Mahkeme, **Sözleşmenin 8. maddesinin ihlal edildiğine** karar vermiş ve başvuru sahibinin kimliğinin ve HIV enfeksiyonunun,

---

837 Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997), http://hrlibrary.umn.edu/instree/coerecr97-5.html, Erişim tarihi, 31.012019.

838 Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, https://rm.coe.int/168007cf98, Erişim tarihi, 31.01.2019.

839 AİHM Kararı: Z v. Finland, Başvuru No: 22009/93, Tarih: 25.02.1997. Kararın İngilizce tam metni için bkz.. http://hudoc.echr.coe.int/eng?i=001-58033, Erişim tarihi, 08.02.2019.

Temyiz Mahkemesi kararının basına verilmiş olan metninde ifşa edilmesinin herhangi bir gerekçeli sebeple desteklenmediğini ve buna göre, ilgili bilgilerin yayınlanmasının başvuru sahibinin özel yaşam ve aile hayatı hakkının ihlal edilmesi olduğunu tespit etmiştir. *Mahkeme, özellikle sağlık verilerinin gizliliğine saygı duymanın AİHS'e taraf olan tüm devletlerin hukuk sistemlerinde olukça önemli bir ilke olduğunu ve tıp mesleğinde ve genel olarak sağlık hizmetlerinde, sadece bir hastanın mahremiyetine saygı duyulmakla kalmayıp, aynı zamanda onun güvenini korumanın da önemli olduğunu belirtmiştir. Bu nedenle iç hukuk, Sözleşme'nin 8. maddesindeki güvencelerle uyuşmayabileceği için, kişisel sağlık verilerinin ifşa edilmesini önlemek için uygun önlemleri devletler almalıdır*.

27 Ağustos 1997 tarihli **M. S. v. Sweden**[840] kararında, başvuru sahibine yapılan bir kürtajla ilgili bilgilerin bir klinik tarafından tıbbi kayıtları tutan bir sosyal güvenlik kurumuna iletilmesi ile ilgilidir. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edilmediğine** karar vermiştir ve başvuru sahibine ait tıbbi kayıtların klinik tarafından sosyal güvenlik kurumuna iletilmesi için uygun ve yeterli nedenlerin bulunduğunu ve yapılan işlemin, izlenen meşru amaç ile orantısız olmadığını olduğunu tespit etmiştir. Üstelik, bu tür verilere önemli sınırlamalara tabi tutulmuş ve kötüye kullanıma karşı etkili ve yeterli güvenceler sağlanmıştır.

04 Aralık 2008 tarihli **S. and Marper v. the United Kingdom**[841] davası, başvuru sahiplerinin parmak izleri, hücre örnekleri ve DNA profillerinin bir veri tabanında süresiz bir şekilde tutulması (el konulması) ile ilgilidir. Mahkeme, **Sözleşme'nin (AİHS) 8. maddesinin ihlal edildiğine** karar vermiş ve söz konusu el koymanın, başvuru sahiplerinin özel hayatına saygı hakkına orantısız bir müdahale teşkil ettiğini ve demokratik bir toplumda gerekli görülemeyeceğini tespit etmiştir. Mahkeme, özellikle, ceza adalet sistemindeki modern bilimsel tekniklerin kullanılmasının, herhangi bir maliyete ve bu tekniklerin önemli özel hayat çıkarlarına

840 AİHM Kararı: M. S. v. Sweden, Başvuru No: 20837/92, Tarih: 27.08.1997. Kararın İngilizce tam metni için bkz. http://www.hrcr.org/safrica/privacy/ms_sweden.html, Erişim tarihi, 08.02.2019.

841 AİHM Kararı: S. And Marper v. the United Kingdom, Başvuru No: 30562/04 - 30566/04, Tarih: 04.12.2008. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-90051, Erişim tarihi, 08.02.2019.

karşı yaygın olarak kullanılmasının potansiyel faydaları dikkatlice dengelenmeden izin verilemeyeceğine hükmetmiştir. Yeni teknolojilerin geliştirilmesinde öncü bir rolü olduğunu iddia eden herhangi bir devlet "doğru dengeyi kurmak" için özel sorumluluk taşımaktadır. *Mahkeme, bu davada uygulandığı şekliyle, suç işlediğinden şüphelenilen ancak mahkûm edilmeyen kişilerin parmak izlerinin, hücre örneklerinin ve DNA profillerinin tutulma yetkisinin gizli ve ayrım gözetmeyen niteliğinin, rekabet halindeki kamu ve özel çıkarları arasında adil bir denge kuramadığı sonucuna varmıştır.*

29 Nisan 2014 tarihli **L. H. v. Latvia**[842] davası. Başvuru sahibi özellikle, kendi rızası olmaksızın bir devlet kurumu -bu davada, Tıbbi Bakım ve İşe Uygunluk için Kalite Kontrol Müfettişliği (MADEKKI)- tarafından kişisel tıbbi verilerinin toplanması suretiyle, özel hayatına saygı duyma hakkının ihlal edildiğini iddia etmiştir. Bu davada Mahkeme, tıbbi verilerin korunmasının[843], bir kişinin özel hayata saygı hakkından yararlanması konusundaki önemini hatırlatmıştır. Başvuru sahibinin davasında Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edildiğine** karar vermiş ve yürürlükteki yasaların, yetkili makamlara verilen takdir yetkisinin kapsamını ve çalışma şeklini yeterince açık bir şekilde belirtmediğini tespit etmiştir. Mahkeme, özellikle, Letonya hukukunun, başvuru sahibi hakkında yedi yıllık bir dönemle ilgili tıbbi verilerin ayrım gözetilmeksizin toplanması ile sonuçlanan ve MADEKKI tarafından toplanabilecek özel verilerin kapsamını hiçbir şekilde sınırlamadığını belirtmiş ve söz konusu verinin potansiyel olarak belirleyici olup olmadığına dair önceden herhangi bir değerlendirme olmaksızın, söz konusu soruşturma ile hangi amaca ulaşıldığının önemli veya ilgili olabileceğini belirtmiştir.

842 AİHM Kararı: L.H. v. Latvia, Başvuru No: 52019/07, Tarih: 29.04.2014. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-142673&filename=001-142673.pdf, Erişim tarihi, 08.02.2019.

843 Danıştay 15. Dairesinin. 08/02/2016 tarih, 2015/10101 esas, 2016/664 karar sayılı kararıyla *"özetle sağlık verilerinin hassas veri kategorisnde özel hayata müdahale kapsamnda kalmasına ilişkin kararı",* http://danistay.gov.tr/arsiv-sayfa-4.html, Erişim Tarihi: 17.12.2079.

22 Haziran 2017 tarihli **Aycaguer v. France**[844] kararına değinmemiz gerekirse, başvuru sahibi, ulusal bilgisayarlı DNA veri tabanına (FNAEG) dahil edilmek üzere biyolojik bir örnek vermesinin istenmesi üzerine bu talebi geri çevirmiş ve özel yaşamına saygı hakkının ihlal edildiğini ve bunun da cezai hüküm ile sonuçlandığını iddia etmiştir. Mahkeme, **Sözleşme'nin 8. maddesinin ihlal edildiğine** (özel hayata saygı hakkı) karar vermiştir. Mahkeme özellikle, saklanan dosyanın ve söz konusu suçların niteliği ve/veya suçların ciddiyetine dayanarak, 16 Eylül 2010 tarihinde Anayasa Konseyi'nin, FNAEG ile ilgili hükümlerin Anayasaya uygun olduğunu ve bunun yanı sıra, söz konusu amaca yönelik olarak bu tür kişisel verilerin depolanma süresinin belirlenmesine ilişkin bir karar vermiş olduğunu gözlemlenmiştir. Mahkeme, bugüne kadar, bahse konu rezervasyon için uygun bir işlem *yapılmadığını ve işlenen suçların niteliğine ve ağırlığına bağlı olarak depolama süresinin farklılaştırılmasına yönelik bir hüküm bulunmadığını kaydetmiştir. Mahkeme ayrıca, FNAEG'deki DNA profillerinin depolanması hakkındaki yönetmeliklerin, verilerin süresi ve silinememeleri nedeniyle, veri konularının yeterli korumaya sahip olmadığına hükmetmiştir. Bu nedenle düzenlemeler, rekabet halindeki kamusal ve özel çıkarlar arasında adil bir denge kurmayı başaramamıştır.*[845]

3.5.3. AİHM İÇTİHADININ DEĞERLENDİRİLMESİ

AİHM, verilerin korunması konusuna ilişkin pek çok durumu insan hakları boyutuyla denetlemiştir. Özellikle iletişime müdahalede bulunulması ile ilgili olanlar, çeşitli koruma tedbirlerinin uygulanması sırasında kişisel verilere ulaşılan durumlar ve kişisel verilerin kamu makamları tarafından saklanmasına karşı korunma, sağlık verilerinin ifşasına ilişkin birçok konuyu incelemiştir. AİHM'nin yapmış olduğu denetimlerde esasa girerek özellikle aşağıdaki hususlara değindiği ve bu nedenle

844 AİHM Kararı: Aycaguer v. France, Başvuru No: 8806/12, Tarih: 22.06.2017. Kararın İngilizce tam metni için bkz.. https://swarb.co.uk/aycaguer-v-france-echr-22-jun-2017/, Erişim tarihi, 08.02.2019.

845 http://danistay.gov.tr/arsiv-sayfa-4.html, Erişim Tarihi: 17.12.2079, Danıştay 15. Dairesinin 06/07/2017 tarihli ve 2016/10500 esas sayılı kararında "Kişisel verileri koruma kurulunun genel denetim mekanizması olması yanında mevzuat uyarınca kişisel verilere yönelik düzenlenecek olan mevzuatlarda görüşünün alınması gerektiği, hassas veriler kapsamındaki sağlık verilerine yönelik yönetmelik çalışmasında görüşünün alınmamasını iptal sebebi saymıştır."

kişisel verilerin korunması hakkında AİHS'nin 8.m.'si çatısı altında ihlal kararları verdiği gözlemlenmiştir.

Mahkeme, AİHS'nin 8. maddesinin, devletleri bu sözleşmeden doğan hakkı ihlal edebilecek herhangi bir eylemden kaçınmaya mecbur etmediğini, ancak belirli durumlarda, özel hayata etkin bir şekilde saygı gösterilmesini sağlamak için belirli yükümlülükler altında olduklarını açıklığa kavuşturmuştur.[846]

AİHM kararlarını incelediğimizde, başlangıçta, sınırlama veya müdahalenin, 8/2 maddesinde sayılan, -sırasıyla kanuna uygun olmak, meşru amaç ve demokratik bir toplumda gerekli olmak- bileşenleri ile uyumlu olması gerektiğini açıkça vurgulamaktadır. Mahkeme, bu hakka, özellikle kişisel verilerle ilgili müdahalenin, AİHS ve 108 sayılı sözleşmeye uygun olarak iç hukukun getirdiği katı güvenceleri gerektirdiğini kararlarında vurgulamaktadır.

Mahkeme içtihatlarında vazıh bir şekilde göstermiştir ki, taraf devletler, kişisel bilgilerin saklanmasına, kişinin bilgisayarı ve telefonuna el konulmasına, gözetime, video-görüntü kaydına ve kişilerle ilgili tıbbi bilgi temin edilmesine, bazı yasal şartlar altında, çatışan hak dengesine dikkat ederek ve tabii ki yasal olarak, olanak tanımaktadır. Bununla birlikte, AİHM'ye göre, bir hakka müdahale için, tabi bu kişisel verilerin korunması hakkını da kapsamaktadır, bir yasanın çıkarılması yeterli değildir. Yani hukukun üstünlüğünü esas alan, bireyleri keyfi müdahaleye karşı korumak için belirli yasal önlemleri ihtiva eden ve hakkın ihlaline karşı AİHM dahil belli başlı kanun yollarını öngören bir yasal düzenleme olması gerekmektedir. Dahası, söz konusu yasa, adli kolluk ve idarenin kişisel verileri toplama ve saklama şeklini açıkça belirlemeli ve bunun yanı sıra, bağımsız bir üst denetleme organı ile bu tip eylemlerin mahkemeler tarafından denetlemeye açık olması hususlarını içermesi gerekmektedir. Diğer bir deyişle, iç hukukta, taraf devletler, kişisel verilerin korunması ile ilgili olarak bir yasa çıkaracakları zaman bu yasada, kişilere ilişkin kaydedilebilecek bilgi türlerini, bilgi toplama, saklama ve denetleme mekanizmalarını, eğer bir koruma tedbiri kişisel

846 Örneğin bkz. AİHM Kararı: Malone v the United Kingdom, Başvuru No: 8691/79, Tarih: 02.08.1984; AİHM Kararı: Copland v. the United Kingdom, Başvuru No: 62617/00, Tarih: 03.04.2007; AİHM Kararı: Klassand Others v Germany, Başvuru No: 5029/71, Tarih: 6.11.1978.

verilerin ele geçirilmesini içeriyorsa bu koruma tedbirlerinin haklarında hükmedilebileceği kişiler, bu tedbirlerin alınabileceği koşulları veya bu prosedürün nasıl uygulanabileceğini düzenlemeli ve verinin ne kadar saklanması gerektiğini veya ayrıntılı olarak saklanabileceği zamanın uzunluğunu belirlemelidir.

Bu bölümde içtihatlar olarak belirttiğimiz AİHM kararlarından da açıkça anlaşılacağı üzere, kamu otoritelerinin özellikle bir suçun soruşturması ve kovuşturması aşamasında bir koruma tedbiri ve delil elde etme yolu olarak başvurduğu gizli gözetim tedbirlerine ilişkin -telefon dinlemesi, bilgisayara el koyulması, gizli soruşturmacı atanması vb. gibi- söz konusu tedbirlerin süresi, müdahaleye izin vermenin yanı sıra, yakalanan verilerin saklanması, depolanması ve imha edilmesi prosedürleri ve müdahalenin denetimi konusunda bağımsız idari otoritelerin ve mahkemelerin yetkili ve görevli olması zaruridir.

Öte yandan, her halükârda, devletlerin bir takdir marjı olduğunu AİHM kabul etmektedir. Bununla birlikte; sınırlamayı öngören yasa, denetleyici otoritelerin takdir marjının nasıl belirlenmesi gerektiğini açıklamalıdır. Yani, yasa bu alanda yetkililerin takdir yetkisinin kapsamını ve şeklini makul bir açıklıkla belirtmelidir.

DÖRDÜNCÜ BÖLÜM

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

4.1. KİŞİSEL VERİLERİN KORUNMASI KANUNU

Kişisel verilerin korunması konusunda ülkemizde özel bir kanun hazırlamak için 1989 yılında ilk komisyon kurulmasına rağmen çalışmalarını tamamlayamamış[847]; bu konuda 2000 yılında ikinci bir komisyon kurularak Kişisel Verilerin Korunması Kanun Tasarısı'nı 2003 yılında tamamlamıştır.[848] Tasarının 2003 yılında kanunlaşamaması üzerine Adalet Bakanlığı tarafından bu tasarıda ilave çalışmalar yapılarak Kişisel Verilerin Korunması Kanunu Tasarısı 2008 ve 2014 yıllarında Türkiye Büyük Millet Meclisi Başkanlığına gönderilmesine rağmen tasarı yine kanunlaşamamıştır. Adalet Bakanlığı'nca tasarı, 18.01.2016 tarihinde tekrar Türkiye Büyük Millet Meclisi Başkanlığı'na gönderilmiş 6698 sayılı Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde nihayet TBMM'de kabul edilerek kanunlaşmıştır.[849]

4.1.1. KANUNUN AMACI VE KAPSAMI

KKVK'nın "Amaç" başlığı altında düzenlenen 1. maddesinde Kanunun amacı, "*kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek"* olarak tarif edilmiştir.

1. maddenin gerekçesinde; bu kanun'un amacının, kişisel verilerin işlenmesi konusunun bir kurala bağlanması ve en başta özel hayatın gizliliği olmak üzere Anayasa'da öngörülen temel hak ve özgürlüklerin korunması olduğu belirtilmiştir.[850]

---

847 Aydın, Sedat Erdem "AİHM İçtihatları Kapsamında Kişisel Verilerin Kaydedilmesi Suçu", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul, 2014, s. 98.

848 Başalp, a.g.e., s. 107.

849 Korkmaz, a.g.m., s.87.

850 Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, s. 6, https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf, Erişim tarihi, 18.07.2019.

KKVK'nın 2. maddesinde ise Kanun'un kapsamı konusunda; "*kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında*" uygulanacağı açık bir şekilde belirlenmiştir. Yine kanunun gerekçe kısmında da, kanunun, kişisel verileri işlenen gerçek kişiler ile bu verileri işleyen tüzel ve gerçek kişiler hakkında uygulanacağı; kanunun uygulaması yönünden kamu sektörü ve özel sektör ayrımı yapılmayıp, Kanunda yer alan usul ve esasların her iki sektör bakımından da uygulama alanı bulacağı belirtilmiştir.[851] Çalışmamızın 2. bölümünde kişisel verilerin korunması kapsamına sadece gerçek kişilerin dahil edildiği ülkelerin olduğu gibi, hem gerçek hem de tüzel kişilerin bu koruma kapsamına alındığı ülkelerin olduğunu belirtmiştik. KVKK'nın 2. maddesi kapsamına da sadece gerçek kişiler alınmış, tüzel kişiler bu kanunun koruma kapsamı dışında bırakılmıştır. Ayrıca kişisel verilerin tanımının yapıldığı 3/1-ç maddesindeki "*İlgili kişi: Kişisel verisi işlenen gerçek kişiyi…"* şeklindeki tanımdan da bu kanunun kapsamına sadece gerçek kişilerin alındığı anlaşılmaktadır.

95/46/AT sayılı Yönergenin örnek alınarak KVKK'nın 2. maddesinin düzenlendiği görülmektedir. 95/46/AT sayılı Yönerge madde 3'te, yönergenin uygulama bulacağı alanları belirtilmiştir.[852] Buna göre yönerge, kişisel verilerin tamamen veya kısmen otomatik araçlarla işlenmesi ve bir dosyalama sistemine kaydedilen ya da kaydedilecek kişisel verilerin otomatik olmayan yollarla işlenmesi halinde uygulama alanı bulacaktır. Dolayısıyla, kişisel verilerin bir dosyada organize edilmesi ve verilere ulaşımın belli kriter veya kriterlere göre kolaylaştırılması durumlarında, bu kişisel veriler otomatik olarak işlem görmeseler dahi, bu işlemler Yönergenin koruması kapsamında kabul edilecektir.[853]

851 Gerekçe, s. 18.

852 Başalp, a.g.e, s. 13.

853 Başalp, a.g.e, s. 36.

4.1.2. KİŞİSEL VERİLERİN İŞLENMESİNDE BENİMSENEN GENEL İLKELER

Kişisel verilerin korunması hakkında yapılan düzenlemelerde, verilerle yapılan işlemlerin insan onuru ve değerlerine uygun olarak yapılmasının sağlanması amacıyla bazı ortak ilkeler[854] belirlenmiştir. Kişisel verilerin işlenmesinde benimsenen bu ilkelerin kesin hatlarla birbirinden ayrılması çok kolay değildir. Bu ilkelerden bazıları diğer ilkelere kaynaklık ederken bazıları ise tamamlayıcı rol oynamaktadır.[855] Bu ilkelere uygun hareket edilmemesi halinde kişisel verilerin, hukuka uygun bir şekilde iyi niyetli olarak işlenmediği, kötüye kullanımın söz konusu olduğu kabul edilmektedir.[856]

KVKK'da kişisel verilerin işlenmesi hakkında benimsenen genel ilkeler 4. maddede düzenlenmiştir. Buna göre, maddenin birinci fıkrasında kişisel verilerin ancak bu Kanunda ve diğer Kanunlarda düzenlenen usul ve esaslar çerçevesinde işlenebileceği ifade edildikten sonra, ikinci fıkrada şu ilkelere yer verilmiştir:

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

4.1.3. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

2010 Anayasa değişikliği ile Anayasası'nın 20. maddesine eklenen kişisel verilerin korunması ile ilgili paragrafta da " *kişisel veriler, ancak kanunda öngörülen*

854 Kişisel verilerin işlenmesi hakkında uluslararası düzenlemelerde benimsenen ilkeler hakkında detaylı bilgi için bkz. Çalışmamızın birinci bölümü.

855 Küzeci, a.g.e., s. 196 vd.

856 Kuşkonmaz, a.g.e., s. 87.

hallerde veya kişinin açık rızasıyla işlenebilir." düzenlemesi yer almaktadır. Bu hükme uygun olarak KVKK'nın 5. maddesinin 1. fıkrasında da *" kişisel verilerin ilgili kişilerin açık rızası olmaksızın işlenemeyeceği"* ifade edildikten sonra, 2. fıkrada kişisel verilerin şu şartlardan birisinin varlığı halinde işlenebileceği ifade edilmiştir. Bu şartlar:

- Kanunlarda açık şekilde öngörülmesi durumunda,
- Fiili imkânsızlığın varlığı nedeniyle rızasını açıklayamayacak durumdaki veya rızasına hukuki geçerlilik tanınması mümkün olmayan kişilerin kendisi veya bir başkasının hayatı ya da beden bütünlüğünün korunması bakımından gereklilik olması durumunda,
- Bir sözleşmenin kurulması ya da yerine getirilmesi doğrudan doğruya ilgili olması şartıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması durumunda,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması durumunda,
- İlgili kişi tarafından alenileştirilmiş olması durumunda,
- Bir hakkın tesisi, kullanımı veya korunması amacıyla veri işlemenin zorunlu olması durumunda,
- İlgili kişinin temel hak ve hürriyetlerine zarar vermemek koşuluyla, veri sorumlusunun meşru çıkarları için veri işlenmesinin zorunlu olması durumunda.

olarak düzenlenmiştir. Bu maddeye göre kişisel veriler, ilgilinin rızasının bulunduğu haller ve maddede sayılan istisnalar dışında işlenemeyecektir.[857]

[857] Kişinin göstereceği rızanın geçerli olabilmesi için ne zaman ve nasıl açıklanması gerektiği konusunu, kişisel verilerin işlenme yasağının istisnaları hakkında çalışmamızın 2. Bölümünde ayrıntılı açıklama yapmaya çalıştığımızdan tekrara düşmemek adına çalışmanın bu bölümünde sadece KVKK'daki düzenlemeyi vermekle yetiniyoruz. Bkz. çalışma, s. 33 vd.

KVKK'nın 5/2-a bendindeki, ilgilinin açık rızası alınmadan da yasal düzenlemelerde açık şekilde öngörülen durumlarda kişisel verilerin işlenebileceği durumlara, kolluk güçlerince suç soruşturması kapsamında, 2559 sayılı Polis Vazife ve Salahiyet Kanununun 5.m.'si gereğince şüpheli kişilerin parmak izlerinin alınması; 5352 sayılı Adli Sicil Kanunu gereğince Adalet Bakanlığı'nın bireylerin ceza mahkûmiyetlerine dair verileri işlemesi gibi düzenlemeler örnek olarak verilebilir.[858]

KVKK madde 5/2-b'ye göre; ilgilinin rızasını açıklamadığı ya da söz konusu rızanın geçersizliği durumlarında, bireylerin yaşam veya vücut bütünlüklerini korumak amacıyla kişisel verilerin işlenmesi durumuna, kişinin bilincinin yerinde olmaması ya da akıl hastalığı nedeniyle rızasının alınamadığı veya geçerli olmadığı bir durumun varlığı halinde, yaşam ya da vücut bütünlüğünün korunması için, yapılan tıbbi müdahale esnasında, kişisel verilerinin işlenebilmesi örnek olarak verilebilir. Bu kapsamda geçirilen hastalık ve ameliyatlar, kan grubu, kişinin kullandığı ilaçlar, vb. veriler, resmi nitelikli sağlık sistemi aracılığıyla işlenebilir. Yine özgürlüğü kısıtlanan kişiyi kurtarma amacıyla, ilgili şahsın ya da şüpheli kişinin taşıdığı telefon, kredi kartı, bilgisayar, banka kartı ya da diğer teknik bir gereç sayesinde yer tespitinin yapılması amacıyla bu verilerin işlenmesi de bu bent kapsamında değerlendirilir.[859]

İlgili düzenlemenin (c) bendi gereğince, sözleşmelerin kurulması ya da ifası konusunda da kişisel verilerin işlenmesi mümkündür. Örneğin, taraflar arasındaki sözleşmenin bir gereği olarak paranın ödenmesi amacıyla borçlu kişiler alacaklının hesap numarası gibi kişisel verilerini alabilecektir. Benzer şekilde bankayla yapılan kredi sözleşmesi esnasında banka tarafından, ilgili kişiye ait maaş bordrosu, tapu kaydı, icra borcu olup olmadığı gibi durumlara ilişkin belgelerin edinilmesi bu kapsamda değerlendirilecektir.[860]

Yine ilgili düzenlemenin (ç) bendinde; veri sorumlusunun, hukuki yükümlülüğünü ifa etmesi için gerekli olan verileri, ilgilinin rızası olmadan da işleyebileceği düzenlenmiştir. Bu duruma ise bir şirketin çalışanlarının maaşını

858 Gerekçe, s. 7.

859 Gerekçe, s. 8.

860 Gerekçe, s. 9.

ödeyebilmesi için, çalışanlarının banka hesap numaraları, evli olup olmadıkları, bakmakla yükümlü oldukları kişiler, eşlerinin çalışıp çalışmadığı, sosyal sigorta numaraları gibi verileri işlemesi bu bendin verdiği yetkiye örnek olarak verilebilir.[861]

Fıkranın (d) bendinde veri sahibinin kendisi tarafından alenileştirilen yani herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verilerin işlenebileceği düzenlenmiştir. Çünkü veri sahibi tarafından alenileştirildiği için herkes tarafından bilinebilecek hale gelen bu tür verilerin işlenmesinde, korunması gerektiği düşünülen hukuki yararın ortadan kalktığı kabul edilmektedir.[862]

Fıkranın (e) bendine göre, kişisel verilerin işlenebileceği bir diğer durum ise bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması durumudur. Bu kapsamda, örneğin, bir şirket çalışanı tarafından şirkete karşı açılan bir davada şirketin ispat için bazı verileri kullanması veya kısıtlı bir kişinin haklarının korunması için vasinin veya kayyımın, kısıtlının mali bilgilerini kaydetmesi bu fıkra kapsamında hukuka uygun işleme olarak kabul edilecektir.[863]

Fıkranın (f) bendine göre, açık rıza şartı aranmadan veri işlemesi yapılabilecek bir diğer durum ise, ilgilinin temel hak ve hürriyetlerine zarar vermemek şartıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumudur. Bu duruma, şirket sahiplerinin, çalışanların temel hak ve hürriyetlerine zarar vermemesi koşuluyla, bu kişilerin terfi işlemleri, maaşlarına zam yapılması veya sosyal hak ve güvencelerin düzenlenmesi ya da şirketin tekrardan yapılandırılması süreçlerinde görev ve rol dağılımında kullanmak üzere çalışanların kişisel verilerini işleyebilmesi örnek olarak verilebilir. Burada, şirketin yeniden yapılandırılması konusunda ya da ehliyet ve liyakat sahibi personelin terfi alması konusunda, veri sorumlusu niteliğinde olan şirket sahibinin meşru menfaati olduğu için hukuka aykırılık söz konusu değildir. Ancak bu durumda da kişisel verilerin korunmasına ilişkin temel ilkelere uyulması ve veri sorumlusu ile veri ilgilisinin menfaat dengesinin gözetilmesi gereklidir.[864]

---

861 Gerekçe, s. 9.

862 Gerekçe, s. 9.

863 Gerekçe, s. 9.

864 Gerekçe, s. 9

4.1.4. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

4.1.4.1. Kapsam

KVKK madde 6/1'de; *"kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri..."* gibi bilgileri "*özel nitelikli kişisel veriler*" olarak nitelendirilmiştir.[865] Aynı maddenin 2. fıkrasında ilgili kişinin açık rızasının bulunmaması halinde özel nitelikli kişisel verilerin işlenmelerinin yasak olduğu belirtilmiştir.

İç hukukumuzdaki düzenlemelerde *"hassas veri"*, *"özel koruma gerektiren veri"*, *"özel tür veri"* şeklindeki farklı terimler ile ele alınan bu tür kişisel verilerin[866], niteliklerinin doğal bir sonucu olarak bireylerin temel hak ve özgürlükleri ve mahremiyetleriyle alakalı olduğundan dolayı diğer kişisel verilere göre daha sıkı bir koruma altına alındığını söylemek mümkündür.[867]

4.1.4.2. Özel Nitelikli Verileri İşleme Yasağının İstisnaları

KVKK'nın 6. maddesinin 3. fıkrasında hangi hallerde ilgili kişinin açık rızası aranmaksızın özel nitelikli kişisel verilerin işlenebileceği düzenlenmiştir. Buna göre: *"... sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir."* Bununla birlikte aynı maddenin 4. fıkrasında özel nitelikli kişisel verilerin işlenmesinde Kişisel Verileri Koruma Kurulu tarafından belirlenecek olan gerekli tedbirlerin alınmasının gerektiği de ifade edilmiştir.

---

865 Kişilerin mezhebi ve kılık kıyafeti KVKK'da özel nitelikli kişisel veri olarak kabul edilmiştir. TBMM Komisyon Raporu, s. 73.

866 Hassas kişisel veriler hakkında detaylı bilgi için bkz. Çalışmamızın Hassas Veriler Başlığı.

867 Aydın, Sedat, a.g.e., s. 7.

4.1.5. KİŞİSEL VERİLERLE İLGİLİ İŞLEMLER

4.1.5.1 Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi

KVKK'nın 7. maddesinin 1. fıkrasında ifade edilen *"Yasal düzenlemelere 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."* şeklindeki düzenleme ile kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi düzenlenmiştir.

Buna göre, hukuka uygun olarak işlenmiş olan bir verinin işlenmesini gerektiren sebeplerin ortadan kalkması halinde, söz konusu verilerin resen veya ilgili kişinin talep etmesi üzerine silineceği, yok edileceği veya anonim hale getirileceği şeklindeki düzenleme ile, kişisel verilerin silinmesi suretiyle, bu verilerin daha sonra tekrardan hiçbir şekilde kullanılamayacak ve geri getirilemeyecek şekilde imhasının amaçlandığı belirtilmiştir.[868]

Bu maddede *verilerin silinmesi* ile; kişisel verilerin kayıtlı oldukları evrak, dosya, CD, disket, hard disk gibi araçlardan bir daha geri dönüştürülemeyecek biçimde silinmesi kast edilmiş iken, *kişisel verilerin yok edilmesi*nden ise; kişisel bilgilerin tekrar geri getirilemeyecek ve kullanılamayacak biçimde, verilerin kaydedildiği evrak, dosya, CD, disket, hard disk gibi veri saklamak için elverişli olan materyallerin imha edilmesini kast edilmektedir. *Verilerin anonim hale getirilmesi*yle kast edilen ise, kişisel verilerin başka verilerle eşleştirilmesi halinde bile kimliği belirli olan veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.[869]

KVKK'nın 7. maddesinin 2. fıkrasında ise, "*Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır*." denilmektedir. Bu kapsamda, mesela, Adli Sicil Kanunundaki verilerin

868 Gerekçe, s. 10.

869 Gerekçe. s. 10.

silinmesi veya yok edilmesi hakkındaki hükümler, özel hüküm olmasından mütevellit, bu maddeye göre öncelikli olarak uygulanacak hükümlerdir.[870]

KVKK'nın 7. maddesindeki, hukuka uygun olarak işlenmiş olan bir verinin işlenmesini gerektiren sebeplerin ortadan kalkması halinde, söz konusu verilerin resen veya ilgili kişinin talep etmesi üzerine silineceği, yok edileceği veya anonim hale getirileceği şeklindeki düzenleme, GDPR'de m. 5/1-e'de benimsenen *"orantılılık ve gereklilik ilkesi"* ve bu ilkenin KVKK madde 4/2-d'de *"amaç için gerekli olan süre"* olarak ifade edilmiş şekli ile uyumludur.

Yine bu maddedeki "…*ilgilinin talebi üzerine…"* şeklindeki düzenleme GDPR madde 17'de veri sahibinin rızasıyla işlenen verinin toplanma amacının gerçekleşmiş olması nedeni ile daha fazla tutulmasına gerek olmaması veya veri sahibinin daha önce vermiş olduğu rızasını geri almış olması ya da verinin işlenmesine itiraz etmiş olması halinde kullanılabilecek bir hak olarak düzenlenmiş olan "*sildirme hakkı"* ile de uyumludur.

Son olarak, bu hususlara ilişkin olarak, AYM bir kararında, KVKK'nın 7/2, 8/3 ve 9/6 maddelerinde yer alan kişisel verilerin silinme, yok edilme ya da anonim hâle getirilme, bunların aktarılma ile yurt dışına aktarılması hakkında diğer kanunlardaki hükümlerin saklı olduğu şeklindeki hükümlerin iptali talebiyle açılan dava hakkında talebin reddine karar vermiştir.[871]

4.1.5.2. Kişisel Verilerin Aktarılması

KVKK'nın 8. maddesinde yurt içinde kişisel verilerin aktarılması düzenlenmiştir. Buna göre KVKK'nın 8. maddesinde kural olarak kişisel verilerin aktarılamayacağı düzenlendikten sonra bu kuralın istisnaları sayılmıştır. Buna göre, işlenen kişisel verilerin kanunun 5. maddesinin 2. fıkrasındaki durumlarda[872], işlenen özel nitelikli (hassas) kişisel verilerin ise kanunun 6. maddesinin 3. fıkrasında

870 Gerekçe, s. 10.

871 https://www.anayasa.gov.tr/media/6115/kd_55_1.pdf, Erişim tarihi: 28.11.2019.

872 KVKK m. 5.

belirtilen şartlarda[873] ancak yeterli önlemlerin alınması kaydıyla ilgili kişinin açık rızası aranmadan aktarılabileceği hüküm altına alınmıştır.[874]

Başka bir deyişle, bu düzenleme yapılırken *kişisel verilerin ilgilinin açık rızası aranmadan aktarılabilmesi* için KVKK'nın 5. Maddesinin 2. fıkrası uyarınca *ilgilinin açık rızası olmaksızın kişisel verilerin işlenmesi*ne izin veren şartlar aranmakta olup, bu şartlardan birinin varlığı halinde, kişisel verilerin üçüncü kişilere aktarılmasına olanak sağlanmaktadır.[875] Bu kapsamda, *hassas kişisel verilerin ilgilinin açık rızası aranmadan aktarılabilmesi* için ise KVKK'nın 6. maddesinin 3. fıkrası uyarınca *ilgili kişinin açık rızası olmadan hassas nitelikli kişisel verilerin işlenmesi*ne izin veren şartların aranmasına ek olarak ayrıca yeterli önlemlerin alınması şartı da aranmaktadır.

Maddenin 3. fıkrasında da diğer kanunlarda kişisel verilerin 3. kişilere aktarılmasına dair hükümlerin saklı olduğu belirtilmiştir.

4.1.5.3. Kişisel Verilerin Yurt Dışına Aktarılması

KVKK'nın 9. maddesinde kanunun 5. maddesinde düzenlenen kişisel veriler ve 6. maddesinde düzenlenen özel nitelikli kişisel verilerin yurt dışına aktarılması düzenlenmiştir. Bu bağlamda, bu düzenleme yapılırken *kişisel verilerin ilgili kişinin açık rızası aranmadan yurt dışına aktarılabilmesi* için KVKK'nın 5. maddesinin 2. fıkrası uyarınca *ilgilinin açık rızası olmaksızın kişisel verilerin işlenmesi*ne izin veren şartlar, *hassas kişisel verilerin ilgilinin açık rızası aranmadan yurt dışına aktarılabilmesi* için ise KVKK'nın 6. maddesinin 3. fıkrası uyarınca *ilgilinin açık rızası olmadan hassas nitelikli kişisel verilerin işlenmesi*ne izin veren şartlar aranmakta olup, bu şartların gerçekleşmesinin yanında, kişisel verilerin ve hassas kişisel verilerin aktarılacağı yabancı ülkede bu kişisel veriler için yeterli korumanın bulunması, yeterli korumanın bulunmaması halinde ise Türkiye'deki ve söz konusu

873 KVKK m. 6.

874 KVKK'nın 3/1-d bendinde verilerin aktarılması veya devralınması işlemleri kişisel verilerin işlenmesi olarak nitelendirildiğinden; verileri alanların, kişisel verilerin işlenebilmesi için kanun'un 5. ve 6. maddelerinde öngörülen şartları yerine getirmeleri gerektiği gibi, bu kapsamda hassas veriler yönünden ayrıca kurul tarafından belirlenen yeterli önlemleri almaları da gereklidir. Gerekçe, s. 11.

875 Gerekçe, s. 11.

yabancı ülkedeki veri sorumlularının yeterli düzeyde korumayı yazılı olarak taahhüt etmeleri ve kurulun izninin bulunması gerekli görülmüştür.

Kişisel verilerin aktarılması için yeterli korumaya sahip ülkelerin belirlenip ilan edilmesi yetki ve sorumluluğu kanunun 9. maddesinin 3. fıkrası ile Kişisel Verileri Koruma Kurulu'na verilmiştir. Maddenin 4. fıkrasında ise Kişisel Verileri Koruma Kurulu'nun yabancı ülkede yeterli koruma olup olmadığı ve bu veriler yurt dışına aktarılırken izlenecek yol ve buna izin verirken dikkate alınacak kriterler düzenlenmiştir. Buna göre kurul bu kapsamda karar alırken *"Türkiye'nin taraf olduğu uluslararası sözleşmeleri, kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu, her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini, kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını, kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle"* karar verecektir.[876]

4.1.5.3.1 Kurumsal Yapılandırmada Ülke Örnekleri:

Avusturya: Avusturya'da 2000 yılında yürürlüğe girerek 1978 yılında kabul edilmiş olan eski kanunu değiştiren *"Veri Koruma Kanunu (Datenschutzgesetz)"* ve söz konusu kanunun denetimini yerine getirecek olan bağımsız nitelikte bir *"Veri Koruma Komisyonu ve Veri Koruma Konseyi"* bulunmaktadır.[877] Bu Komisyon tarafından verilen kararlara karşı "*Yüksek İdare Mahkemesi*"ne temyiz başvurusu yapma hakkı getirilmiştir. Avusturya Veri Koruma Komisyonu'nun yapısına bakıldığında, Federal Hükümet tarafından 5 yıl süre için teklif edilen ve Federal hükümetin Başbakanı'nın atadığı 6 üyeden meydana gelmektedir. Bütün üyelerin şu iki temel şartı taşıması gerekmektedir. Bu şartlar; hukuk alanında veri koruma konusunda uzmanlığa sahip olma ve en az bir üyenin hâkim olması.[878]

---

876 KVKK m. 9/4.

877 Ayrıntılı bilgi için Bkz., https://www.data-protection-authority.gv.at/home, Erişim Tarihi, 29.05.2019.

878 Civelek, a.g.e., s. 167.

Finlandiya: Finlandiya'da *"Veri Koruma Ombudsmanı"* olarak adlandırılan kişinin Kişisel Veri Koruma Kanununa uyarınca Finlandiya Danıştay'ı tarafından 5 yıllık bir süre için seçilmektedir.[879] Bunun yanı sıra ombudsmanlık makamı haricinde de Danıştay'ın 3 yıllık bir süre için 5 üyeden oluşan bir kurul yer almaktadır. Bu kurul, ombudsman tarafından verilen kararlar bakımından temyiz merci niteliği taşımaktadır.[880]

Polonya: Veri koruma hukuku konusunda Polonya'da çıkarılan ilk düzenlemenin 29 Ağustos 1997 tarihinde kabul edilerek 1998 yılında yürürlüğe konulan Polonya Kişisel Verileri Koruma Kanunu olarak ifade edilmektedir. Belirtmek gerekir ki bu kanunla kurulmuş bulunan Kişisel Verilerin Korunması Müfettişliği[881] bir üst kurum olarak görev yapmaktadır.[882]

Fransa: Enformatik ve Özgürlükler Milli Komisyonu (CNIL), hem Fransa'nın veri koruma konusunda sorumlu otoritesidir, hem de 1978 yılında Veri Koruma Kanunu ile kurulmuş bulunan bağımsız nitelikte bir komisyondur.[883]

Veri Koruma Kanununun gerek kamu kurum ve kuruluşları gerekse özel kurum ve kuruluşlar tarafından tutulan verileri kapsamaktadır. Ayrıca belirtmek gerekir ki, kişisel veri işleme faaliyeti yürüten her kişinin bu faaliyetlerden önce komisyona başvuru yapmak suretiyle kayıt yapmalı ve izin almalıdır. Ayrıca veri toplayan kişilerin, verileri toplanan bireylere veri toplama faaliyetlerinin sebeplerini bildirme yükümlülükleri vardır. Komisyon, parlamentonun içinden seçilen 2 milletvekili ve 2 senatör olmak üzere 4; Ekonomik ve Sosyal Konsey'den seçilen 2; 2 tanesi Danıştay, 2 kişi Yargıtay ve 2 kişi Hesap Mahkemesi olmak üzere yüksek yargı organlarından seçilen 6 kişi; Bakanlar Kurulu tarafından atanan 3 kişi; Meclis Başkanı tarafından atanan 1 kişi; Senato Başkanı tarafından atanan 1 kişi olmak üzere toplamda 17 kişiden teşekkül etmektedir. Komisyonun çalışmasına ilişkin usul ve esaslar ise bir iç tüzük

879 Ayrıntılı bilgi için Bkz., https://tietosuoja.fi/en/home, Erişim Tarihi, 29.05.2019.
880 Civelek, a.g.e., s. 116.
881 Ayrıntılı bilgi için Bkz., https://www.uodo.gov.pl/en, Erişim Tarihi, 29.05.2019.
882 Civelek, a.g.e., s. 118.
883 Ayrıntılı bilgi için Bkz., https://www.cnil.fr/en/home, Erişim Tarihi, 29.05.2019.

aracılığıyla düzenlenmektedir. Kanuna göre, komisyonun mali denetimi ise Sayıştay tarafından yapılmaktadır.[884]

Almanya: Almanya da ise federal devlet yapısının bir gereği olarak veri koruma hukuku bakımından farklı mevzuatlar uygulanmaktadır. Almanya'da Federal Veri Koruma Komiseri[885] haricinde, Alman Sağlık Birliği, Ulusal Etik Konseyi, Berlin Veri Koruma Komiseri ve Bavyera Bioetik Komisyonu olmak üzere veri koruma konusunda dört merciinin var olduğu görülmektedir.[886]

İngiltere: İngiltere'de ilk veri koruma kanunu1984 yılında yürürlüğe girmiştir. İlgili kanunun 1998 yılına kadar yürürlükte kalmıştır.[887] İngiltere'de üç farklı yerde bulunan ofisiyle Bilgi Komiseri Ofisi (ICO), Veri Koruma Yasası, Bilgi Edinme Hakkı Kanunu, Çevre Verisi düzenlemeleri ile Mahremiyet ve Elektronik Haberleşme Düzenlemelerinin uygulanması ve izlenmesi konularında sorumlu olarak görev yapmaktadır. Veri koruma kurumlarında genel olarak görev süresi bağımsızlığın sağlanabilmesi için uzun bir süre olarak belirlenmektedir. Bu süre, birçok ülkede 5 ila 7 yıl arasında değişmektedir. [888]

TABLO 1: Kişisel Verilerin Ülkelere Göre Mevzuat Adları, Yürürlük Tarihleri ve Kurum Adları[889]

Ülke Adı	Mevzuat Adı	Yürürlük Tarihi	Sorumlu Kurum Adı
Bosna Hersek	Kişisel Verilerin Korunması Kanunu	20/12/2001	Veri Koruma Komisyonu
Bulgaristan	Kişisel Verilerin Korunması Kanunu	21/12/2001	Kişisel Verilerin Korunması Komisyonu

884 Civelek, a.g.e., s. 108.

885 Ayrıntılı bilgi için Bkz., https://www.bfdi.bund.de/EN/Home/home_node.html;jsessionid=DDDCFFB149216D5F0B7079EFED95E1B1.2_cid344, Erişim Tarihi, 29.05.2019.

886 Civelek, a.g.e., s. 85.

887 Ayrıntılı bilgi için Bkz., https://ico.org.uk/ Erişim Tarihi, 29.05.2019.

888 Civelek, a.g.e., s. 88.

889 Civelek, a.g.e., s. 189-196.

Hırvatistan	Kişisel Verilerin Korunması Kanunu	01/10/2005	Kişisel Verileri Koruma Ajansı
Almanya	Federal Veri Koruma Kanunu	01/01/2002	Federal Veri Koruma Komiseri
Macaristan	Kişisel Verilerin Korunması ve Kamuyu İlgilendiren Bilgilerin Açıklanması Hakkında Kanun	17/11/1992	Veri Koruma Ombudsmanı
İzlanda	Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunmasına İlişkin Kanun	01/01/2000	Kişisel Veri Koruma Kurumu
İrlanda	1988 Tarihli Veri Koruma Kanunu (2003'te değişti)	13/07/1988	Veri Koruma Komiseri
İtalya	196/2003 sayılı Kişisel Veri Koruma Kanunu	01/01/2004	Kişisel Verileri Koruma Kurumu
Lüksemburg	Kişisel Verilerin İşlenmesi Halinde Bireyin Korunması Hakkında Kanun Telekomünikasyon Kanunu	02/08/2002	Veri Koruma Ulusal Komisyonu
Malta	Veri Koruma Kanunu, 2001	14/12/2001	Veri Koruma Komiseri
Hollanda	Kişisel Veri Koruma Kanunu	06/07/2000	Veri Koruma Komisyonu
Norveç	Kişisel Veri Koruma Kanunu	14/04/2000	Veri Müfettişliği
Polonya	Kişisel Veri Koruma Kanunu	29/08/1997	Kişisel Veri Koruma Genel Müfettişi

İspanya	Kişisel Verilerin Korunması Hakkında 15/99 sayılı Kanun	13/12/1999	Veri Koruma Ajansı
İsveç	Federal Veri Koruma Kanunu	29/04/1998	Federal Veri Koruma ve Bilgi Komiseri
Makedonya	Kişisel Veri Koruma Kanunu	25/01/2005	Kişisel Veri Koruma Müdürlüğü (İdari organ)
ABD	1-Mahremiyet Kanunu 2-Kişisel Verilerin Korunmasında Farklı Sektörlere Ait Kanunlar 3- Güvenli Liman Kuralları	1974	
Kanada	1- Mahremiyet Kanunu 2- Kişisel Verilerin Korunması ve Elektronik Belgelere İlişkin Kanun	01/07/1983	Mahremiyet Komiseri Federal Kurumlar
Meksika	Federal Şeffaflık ve Kamu Kurumlarındaki Bilgilere Erişim Kanunu	05/2002	Kamu Bilgilerine Erişim Enstitüsü
Yeni Zelanda	Mahremiyet Kanunu	17/05/1993	Mahremiyet Komiseri
Lihtenştayn	Veri Koruma Kanunu, 2002	14/03/2002	Veri Koruma Komiseri
Yunanistan	1997 tarihli ve 2472 sayılı Kişisel Verilerin İşlenmesi ile İlgili Bireyin Korunması Hakkında Kanun	26/03/1997	Kişisel Veri Koruma Kurumu

Arnavutluk	9887 sayılı Kişisel Verilerin Korunması Hakkında Kanun, 2008	10/03/2008	Veri Koruma Komiseri
Türkiye	Kişisel Verilerin Korunması Kanunu	26/03/2016	Kişisel Verileri Koruma Kurulu

4.1.6. VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ VE İLGİLİKİŞİNİN HAKLARI

4.1.6.1. Veri Sorumlusunun Aydınlatma Yükümlülüğü

KVKK'nın 10. maddesinde veri sorumlusu veya onun yetkilendirdiği kişinin ilgili kişileri aydınlatma yükümlülüğü düzenlenmiştir. Buna göre veri sorumlusu veya görevlendirdiği ilgili kişilerin, *"veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi ve KVKK'nın 11. maddesinde sayılan diğer hakları"* gibi konularda bilgilendirme yükümlülüğü vardır.[890]

KVKK'nın 10. maddesinde, veri ilgilisi kişinin aydınlatılması yükümlülüğü[891] 95/46/AT sayılı Yönergeye paralel şekilde düzenlenmiştir.[892]

4.1.6.2. İlgili Kişinin Hakları

KVKK'nın 11. maddesi ile kişisel verileri işlenen kişinin hakları düzenlenerek, kişinin kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenme, eğer işlenmiş ise buna ilişkin bilgileri talep etme, kişisel verilerin işlenme amacı ile bu verilerin işlenme amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içinde veya yurt dışında verilerin aktarıldığı üçüncü kişileri bilme, kanunun 7. maddesinde belirlenen koşullar çerçevesinde, kişisel verilerin silinmesini, yok edilmesini veya verilerin içeriğinin eksik ya da gerçeğe aykırı olması hallerinde ise bunların düzeltilmesini isteme hakları

890 KVKK m. 10/1.

891 Veri ilgilisinin aydınlatılması yükümlülüğünün yerine getirilmesinin kişisel verilerin korunması açısından önemi için bkz. Çalışmanın ilgili bölümü.

892 Gerekçe, s. 11.

tanınmıştır.[893] Ayrıca, yine ilgili kişinin, kendi talebi üzerine yapılan düzeltme, silme ve yok etme işlemlerinin, verilerin aktarılmış olduğu üçüncü kişilere bildirilmesini isteme, verilerin kanuna aykırı olarak işlenmesi nedeniyle veri sahibinin zarara uğramış olması halinde, zararın giderilmesini talep etme hakkı da düzenlenmiştir.

OECD Rehber İlkeleri madde 13'te, ilgili kişinin, bir veri ya da veri topluluğundan sorumlu olan kişi veya kurumdan kendisine ilişkin veri toplanıp toplanmadığına dair bilgi alma hakkının bulunduğu ifade edilmiştir. Bireylerin, kendisi ile ilgili verileri, uygun bir süre içinde gerek ücretsiz şekilde gerekse uygun bir ücret karşılığında, kendisinin anlayabileceği şekilde öğrenme hakkı vardır.[894] 95/46/AT sayılı Yönerge madde 12'deki düzenlemelere göre de kişisel verilerin tam olmaması veya hatalı olması halinde veri sahibinin bunları *düzeltme, sildirme, engelleme* ve *bunlara itiraz hakları* bulunmaktadır. KVKK'nın 11. maddesinde veri ilgilisine tanınan bu haklar uluslararası düzenlemelere paralellik arz etmektedir. Veri ilgilisine tanınan bu haklarla ilgili kişinin verilerin korunması sürecine aktif olarak katılması sağlanmaya çalışılmıştır.

Veri ilgilisinin verilere erişim hakkı, veri sorumlusunun bilgilendirme yükümlülüğü ile yakından ilgilidir. Veri sorumlusunun, kişisel verilerinin işlendiği konusunda veriler ile ilgili kişiyi bilgilendirmemesi halinde, ilgili kişinin verilerin işlendiğinden haberi olamayacağından, verilere erişim, düzeltme, sildirme, yok etme, üçüncü kişilere aktarılmasını engelleme gibi haklarını kullanabilmesi de söz konusu olamayacaktır.[895]

4.1.6.3. Veri Güvenliğine İlişkin Yükümlülükler

Veri sorumlusunun kişisel verilerin güvenliklerine ilişkin yükümlülükleri düzenleyen KVKK'nın 12. maddesine göre, veri sorumlusu, hukuka aykırı bir şekilde kişisel verilerin işlenmesini ve kişisel verilere erişilmesini önlemekle yükümlü tutulduğu gibi, veri sorumlusu ayrıca verilerin muhafazasının sağlanması için uygun

893 Gerekçe, s. 12.

894 Şimşek, a.g.e., s. 91.

895 Şimşek, a.g.e., s. 90.

güvenlik düzeyini temin etmeye dair gerekli tüm teknik ve idari tedbirleri almakla da yükümlü tutulmaktadır.[896]

Maddenin 2. fıkrasında *"veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde"* yukarıda ifade edilen önlemlerin alınması konusunda, verileri işleyen kişilerle birlikte ortak bir sorumluluğa sahip olacağı düzenlenmiştir. Bu düzenleme ile veri sorumlusunun, örneğin; şirketine ilişkin kayıtları bir muhasebe şirketine tutturması halinde, verilerin işlenmesine ilişkin gerekli tedbirlerin alınması konusunda muhasebe şirketiyle beraber müşterek bir şekilde sorumlu olacağı düzenlenmiştir.[897]

Maddenin 3. fıkrasında, veri sorumlusunun, "*kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorunda"* olduğu belirtilerek, veri sorumlusuna kanun hükümlerinin uygulanması konusunda ayrıca denetim yapma veya yaptırma yükümlülüğü getirilmiştir.

Maddenin 4. fıkrasında, veri sorumluları ile veri işleyenlerin sır saklama yükümlülüğü kapsamında veri sorumlularının ve veri işleyen kişilerin, öğrendikleri kişisel verileri hukuka aykırı olarak başkasına açıklayamayacağı ve işleme amacı haricinde kullanamayacağı ve söz konusu yükümlülüğün bu kişilerin görevden ayrılmalarından sonra dahi devam edeceği düzenlenmiştir. Yani, veri sorumluları ile veri işleyenler, bu kapsamda öğrendikleri kişisel verileri, kanuna aykırı biçimde başkalarına açıklayamayacak veya bu verileri şahsi çıkarları için kullanamayacaklardır. Veri sorumluları ile veri işleyenlerin bu yükümlülüklerinin görevden ayrılmalarından sonra da devam edeceği belirtilmiştir.[898]

Kişisel verilerin güvenliğine ilişkin olarak uluslararası düzenlemelerden OECD Rehber İlkeleri madde 11'de makul koruma önlemlerine yer verilmişken, 108 sayılı Sözleşme madde 7'de uygun koruma önlemleri ifadesini kullanmış ise de tüm bu ifadeler ile ifade edilmek istenen, kişisel verilerin en iyi şekilde korunmasının

---

896 Gerekçe, s. 12.

897 Gerekçe, s. 12.

898 Gerekçe, s. 12.

sağlanmasıdır.[899] İç hukukumuzda ise veri güvenliği KVKK'nın 12. maddesindeki düzenlemeler aracılığı ile sağlanmaya çalışılmıştır.

4.1.6.4. Veri Sorumlusuna Başvuru

KVKK'nın 13. maddesinin 1. fıkrasında ilgili kişinin KVKK'nın uygulanmasıyla ilgili taleplerini yazılı bir şekilde veya kurulun belirleyeceği başka yöntemlerle öncelikle veri sorumlusuna ileteceği düzenlenmiştir. KVKK'nın 13/2. fıkrasına göre; *"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 maliyeti gerektirmesi hâlinde, Kurulca belirlenen tarifedeki ücretin" alınması* mümkündür. Maddenin 3. fıkrasına göre veri sorumlusu kendisine yapılan talep hakkında kabul veya ret kararı verebilecektir. Yine aynı fıkraya göre veri sorumlusu talep hakkında verdiği kararı yazılı veya elektronik ortamda ilgili kişiye bildirecektir. Yapılan başvurunun kabul edilmesi halinde talebin gereği veri sorumlusu tarafından yerine getirilecektir. İşlemin maliyet gerektirmesi nedeni ile başvurucudan ücret alınmış ise, başvurunun konusu veri sorumlusunun hatasından kaynaklanıyorsa bu ücret başvurucuya iade edilecektir.

Kişisel Verileri Koruma Kurulu tarafından verilen 18.09.2019 tarih ve 2019/271 sayılı Kararda[900] veri sorumlusunun ilgiliye yaptığı veri ihlaline ilişkin bildirimde bulunması zorunlu olan asgari unsurlar belirtilmiştir. Buna göre, veri sorumlusunun ilgiliye yaptığı ihlal bildiriminin sade ve açık bir dil kullanılarak yapılması gerekmektedir. Ayrıca bu bildirimin asgari düzeyde şu şartları taşıması gerekmektedir:

- İhlalinin gerçekleştirildiği zamanı,
- İhlal edilen verilerin kişisel/özel nitelikli kişisel veri ayrımında hangi veri içinde yer aldığının ve hangi verilerin ihlal edildiğinin tespiti,
- Söz konusu veri ihlalinin muhtemel sonuçları,
- İhlalinin negatif etkilerinin en aza indirilmesi açısından alınmış veya alınması gerekli olan tedbirler,

899 Akgül, "Kişisel veri", s. 147.

900 https://www.kvkk.gov.tr/Icerik/5547/2019-271, Erişim tarihi, 30/11/2019.

- Veri ihlali hakkında ilgili kişilerin bilgi almalarını kolaylaştıracak irtibat kurulacak kişilerin isim ve diğer iletişim bilgileri ya da veri sorumlusuna ait olan internet sitesinin tam adresi, çağrı merkezi gibi iletişim yolları.

Kişisel Verileri Koruma Kurulu, 05/07/2018 tarih ve 2018/75 sayılı Kararı[901] ile arabulucuların veri sorumluları siciline kayıt zorunluluğundan istisna tutulması konusunda önemli bir karara imza atmıştır. Buna göre, *"6698 sayılı Kişisel Verilerin Korunması Kanununun 16. maddesinin (2) numaralı fıkrasında yer alan "Kişisel verileri işleyen gerçek ve tüzel kişiler, veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorundadır. Ancak, işlenen kişisel verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması veya üçüncü kişilere aktarılma durumu gibi Kurulca belirlenecek objektif kriterler göz önüne alınmak suretiyle, Kurul tarafından, Veri Sorumluları Siciline kayıt zorunluluğuna istisna getirilebilir." hükmü ile 30 Aralık 2017 tarih ve 30286 sayılı Resmî Gazetede yayımlanarak yürürlüğe giren Veri Sorumluları Sicili Hakkında Yönetmeliğin "İstisna Kriterleri" başlıklı 16. maddesi göz önünde bulundurularak; Arabulucular bakımından Veri Sorumluları Siciline kayıt yükümlülüğüne istisna getirilmesine ve Kararın Resmi Gazete ile Kurumun internet sayfasında yayımlanmasına oy birliği ile karar verilmiştir."* denilmektedir.

4.1.6.5. Kurula Şikâyet

KVKK'nın 14. maddesinde ilgili kişinin Kişisel Verileri Koruma Kuruluna şikâyet hakkı ve yolu düzenlenmiştir. Buna göre, 13. madde uyarınca yapmış olduğu başvurusu reddedilen, kendisine verilen cevabı yetersiz bulan veya yaptığı başvuruya süresinde cevap verilmeyen ilgili kişi, eğer kendisine bir cevap verilmiş ise veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve herhalde başvuru tarihinden itibaren altmış gün içinde Kurul'a şikâyette bulunabilecektir. Maddenin 2. fıkrasında, 13. maddede öngörülen veri sorumlusuna başvuru müessesesinin zorunlu bir başvuru yolu olduğu ve bu yol tüketilmeden kurul'a şikâyet yoluna gidilemeyeceği düzenlenmiştir. Bu yolla bu konuda çıkan uyuşmazlıkların belirli bir kısmının veri

901 https://www.kvkk.gov.tr/Icerik/5270/2018-75, Erişim tarihi, 30/11/2019.

sorumluları tarafından giderilmesi ve böylece kurulun yoğun bir iş yükü altında kalmasının önlenmesi istenmiştir.[902]

Veri sorumlusuna başvuru yapmanın zorunlu, kurula şikâyet yoluna gitmenin ise ihtiyari olarak belirlenmesi nedeni ile, veri sorumlusuna yaptığı başvurusu zımnen veya açıkça reddedilen ilgili kişi bir yandan kurula şikâyette bulunabileceği gibi, diğer yandan da doğrudan adli veya idari yargı yoluna başvurabilecektir. Ancak, masrafsız ve daha hızlı sonuç alınması mümkün olan şikâyet yolunun ilgililerce tercih edileceği değerlendirilmektedir.[903]

Maddenin 3. fıkrasında ise, kişilik hakları ihlal edilen kişilerin, genel hükümlere göre yapacağı başvurulardaki tazminat haklarının saklı tutulduğu belirtilmiştir. Bu durumda ilgili kişiler veri sorumlusunun hukuki statüsüne göre adli ya da idari yargıda dava açabileceklerdir.[904]

4.1.6.6. Şikâyet Üzerine veya Resen Yapılacak İncelemenin Usul ve Esasları

KVKK'nın 15. maddesinde, kurul tarafından gerçekleştirilecek incelemenin usul ve esaslarına ilişkin bir düzenleme getirilmiştir. Buna göre kurul şikâyet üzerine ya da ihlal iddiasını öğrendiğinde resen görev alanına giren konularda gerekli incelemeyi yapacaktır. Bunun yanında kurulun resen genel inceleme yetki ve görevi bulunmamaktadır.[905]

Ancak kanunun 15/2. fıkrasına göre *"... 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanunun 6. maddesinde belirtilen şartları taşımayan ihbar veya şikâyetler"*in incelemeye alınması mümkün değildir.

Maddenin 3. fıkrasına göre veri sorumlusu kişi, devlet sırrı niteliğini haiz bilgi ve belgeler haricinde, *"Kurulun, inceleme konusuyla ilgili istemiş olduğu bilgi ve belgeleri 15 gün içinde göndermek ve gerektiğinde yerinde inceleme yapılmasına imkân sağlamak"* yükümlülüğü altına sokulmuştur. Buradan anlaşılacağı üzere, devlet

902 Gerekçe, s. 12.
903 Gerekçe, s. 12
904 Gerekçe, s. 12.
905 Gerekçe, s. 13.

sırlarını içeren bilgi ve veriler hariç tutularak kurulun bu verileri isteyemeyeceği ve inceleme yapamayacağı belirtilmiştir. Ancak benzer bir sınırlama CMK kapsamında "hâkim" veya "savcı" kararı gerektiren durumlar için açıkça sayılmamıştır. Örneğin, Kurul bir şirketin bilgisayar üzerinde tutulan veri kayıt sisteminin tamamını isterse ne olacaktır? Burada, esasen hukuki manada bir el koyma, bilgisayar üzerinde aramadan bahsedileceğinden ancak hâkim veya mahkeme kararı ile bu hususun olabileceği yani Kurulun böyle bir yetkisi olmasının düşünülemeyeceği kanaatindeyiz.

Maddenin 4. fıkrasında, şikâyet üzerine yapacağı inceleme sonunda kurulun cevap vermesi öngörülmekte olup, kurulun şikâyet tarihinden itibaren altmış günlük süre içinde cevap vermemesi halinde talebin reddedilmiş sayılacağı hükme bağlanmaktadır. Bu durumda, şikâyet tarihinden itibaren altmış günlük sürenin geçmesiyle idari yargıda dava açma süresi başlayacaktır.[906]

KVKK'nın 15/4. fıkrasında, şikâyet üzerine Kurul'un yapacağı inceleme için 60 günlük süre içinde karar verilmesi aksi durumda talebin reddedilmiş sayılacağı öngörülmüş ise de kurulun resen yapacağı incelemeler yönünden herhangi bir süre öngörülmemiştir.[907]

Maddenin 5. fıkrasına göre, kurul *"şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ"* etmek zorundadır. Bu durumda söz konusu kararın, tebliğden itibaren derhal, her hal ve şartta en geç 30 gün içinde yerine getirilmesi gerekmektedir.

Yine maddenin 6. fıkrasına göre, şikâyet üzerine veya resen yapılan inceleme sonucunda, kurul kanuna aykırı uygulamanın yaygın olduğunu tespit ederse, ilgili kurum ve kuruluşların görüşü de alınmak suretiyle, bu konuda ilke kararı alıp bu kararı yayımlar.

Maddenin 7. fıkrasına göre ise kurul, *"telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması durumlarında, veri işlenmesinin veya*

906 Gerekçe, s. 13.

907 Gerekçe, s. 13.

verinin yurt dışına aktarılmasının durdurulmasına" karar verebilecektir. Ayrıca, kurul tarafından verilen kararlara karşı ilgililerin idare mahkemelerinde dava açabilmeleri mümkündür.[908]

4.2. TÜRK MEDENİ KANUNU KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI

4.2.1. GENEL OLARAK

Kişisel verilerin korunması hakkı kişilik hakkının özel bir görünümü olarak kabul edildiğinden[909] 1982 Anayasasında da bu yönde bir tercih yapılarak *özel hayatın gizliliği*, *kişisel verilerin korunması*, *haberleşme hürriyeti* gibi haklar kişinin hak ve ödevleri bölümünde düzenlenmiştir.

Kişilik hakkı, kişisel değerlerin bütünü üzerinde geçerli olduğundan kişisel verileri korumaya yönelik bazı hükümleri, medeni hukuk kapsamında bulabilmek mümkündür.[910] Kişinin, genel bir kişilik hakkına mı sahip olduğu, yoksa kişisel değerlerinin her biri üzerinde ayrı ayrı olarak kişilik haklarının mı bulunduğu konusunda öğretide farklı görüşler var ise de, kişilik hakkının genel nitelikli olup sınırlı sayıyla belirlenmediği görüşünün kabul edilmesi halinde, teknolojik gelişmeler ve günlük yaşam ihtiyaçlarından doğacak değerlerin de bu kapsamda kabulü gerekir.[911] Başka bir ifade ile kişisel verilerin, kişilik hakkının bir parçası olduğu[912] ve kişilik hakkı kapsamında korunacağı söylenebilir. Önemine binaen çalışmamızın çeşitli yerlerinde yer verdiğimiz Alman Anayasa Mahkemesi'nin Nüfus Sayımı Kararında da kişisel verilerin korunmasının, genel kişilik hakkı kapsamında anayasal korumadan yararlanacağı ifade edilmiştir.[913] Alman Anayasa Mahkemesi'nin bu kararı

---

908 Gerekçe, s. 13.

909 Aksoy, "Kişisel Verilerin Korunması", s. 80.

910 Kişilik kavramından kişisel değerlerden oluşan bir bütün anlaşılmaktadır. Kişinin bedensel bütünlüğü ve sağlığı gibi, maddi bedensel değerleri, onuru, saygınlığı, sır alanı, inancı, adı ve resmi üzerindeki hakkı gibi, manevi değerleri ve mesleki ve ticari sırları, mesleki itibarı gibi, bazı mesleki-ticari değerleri bu bütünün parçalarıdır. Jale AKİPEK, Turgut AKINTÜRK, "Türk Medeni Hukuku (Yeni Medeni Kanun'a Uyarlanmış Başlangıç Hükümleri, Kişiler Hukuku)", Cilt: I, 4. Baskı, İstanbul, 2002, s. 358.

911 Küzeci, a.g.e., s. 296.

912 Kişisel verilerin hukuki niteliğine ilişkin görüşler için bkz. Çalışma, s. 9 vd.

913 Bkz. çalışma, s.10.

ile kişiliğin korunmasının insan hakları çerçevesinde yeniden ele alındığı görülmekte ve insan hakları ve kişiliğin korunması arasındaki yakın ilişki nedeni ile kişisel verilerin korunması yasalarının, özel hukuk anlamında kişiliğin korunmasının bir bölümünü somutlaştırdığı düşünülebilir.[914]

4.2.2. MEDENİ KANUN'DAKİ KORUMA

Kişinin *onur ve saygınlığı*, *adı ve resmi üzerindeki hakkı*, *sır alanı* gibi kavramlar her biri kişisel veriler ile doğrudan ilgili olan ve kişilik hakkının konusu içinde değerlendirilen kavramlardır. Bu kapsamda özel hayatın çeşitli görünümleri hukuksal sonuçları da belirlemek amacıyla genel olarak 3'e ayrılarak incelenir. Bunlar:[915]

- Kişinin diğer kişilerin bilgisinden uzak tuttuğu *gizli yaşam alanı*,
- Kişinin sadece kendisine yakın hissettiği kişilerle paylaştığı fakat bu kişilerden başkasından gizli kalmasını istediği *özel yaşam alanı,*
- Toplumsal ilişkilere karışıp başka kişilerle paylaştığı *ortak yaşama alanı*dır.

Türk Medeni Kanunu[916] kapsamında, kişinin gizli ve özel yaşam alanlarına yönelen saldırılar karşı belirli oranda koruma sağlandığı görülmektedir. Kişinin *gizli alanına* sızmak suretiyle çeşitli sırlarını öğrenme, teknik cihaz ve araçlarla kayıt altına alma, fotoğraf çekme ve video kaydı yapma, bunun yanında bunları yayma ve aktarma bu kapsamda kişiye yönelebilecek saldırı türlerindendir. Bu saldırılara karşı TMK'nın "*Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır."* şeklindeki kişiliğe yönelik saldırılara karşı temel ilkenin yer aldığı 24. maddesi ve *"Davacı, hakimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının*

914 Küzeci, a.g.e., s. 297.

915 Öztan, Bilge,"Medeni Hukuk'un Temel Kavramları", 8. Baskı, Turhan Kitabevi, Ankara, 2002, s. 255.

916 4721 sayılı.Kanun, R.G. Tarihi: 8/12/2001 Sayı: 24607.

hukuka aykırılığının tespitini isteyebilir. Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir." şeklindeki saldırılara karşı başvurulacak olan hukuki yolların düzenlendiği 25/1-2 fıkraları ile koruma sağlanması hedeflenmiştir.[917]

TMK'nın 23. maddesinin 1. fıkrasındaki *"Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez. Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlâka aykırı olarak sınırlayamaz..."* şeklindeki ifade ile kişiliğin korunmasından vazgeçme ve aşırı sınırlamaya karşı genel ilke düzenlenmiştir.

TMK'nın 24. maddesinde kişilik haklarına yönelen saldırıların meşru kabul edildiği durumların, konuya ilişkin ulusal ve uluslararası düzenlemeler ile büyük oranda uyumlu olduğu görülmektedir. Sır ve özel yaşam alanı ihlal edilen kişinin buna rıza göstermesi[918], kişilik haklarına yönelen müdahalenin kamu yararının gerekliliklerinden kaynaklanması, tarihsel araştırmalar için kullanılması ya da başkalarının haklı çıkarları bu kapsamda sayılabilir.[919]

Görüldüğü gibi bir kişi kişisel verilerinin hukuka aykırı olarak kaydedildiğini veya kullanıldığını düşünüyorsa TMK hükümlerinden faydalanarak bu saldırının önlenmesini, durdurulmasını veya tespitini talep edebileceği gibi, bu saldırı nedeniyle uğramış olduğu bir zarar var ise bu zararların da tazminini isteyebilecektir.[920]

---

917 Küzeci, a.g.e., s. 297.

918 Bu maddede düzenlenen istisnalardan olan kişinin rızasının geçerli kabul edilebilmesi için, rızayı veren kişinin ayırt etme gücüne sahip olması ve rızanın hukuka, ahlaka, kamu düzenine aykırı olmaması gereklidir. Kişinin vereceği rıza beyanı kural olarak açık veya örtülü olarak verilebilir. Bunun yanında ilgili yasada rızanın mesela yazılı olarak verilmesi şart koşulmuş ise buna uyulması gerekir. Bkz. Gençcan, Ömer Uğur, "Türk Medeni Kanunu", Bilimsel Açıklama-İçtihatlar-İlgili Mevzuat, Madde 1-184, 2. Baskı, Yetkin, Ankara, 2007, s. 246-249.

919 Zevkliler, Aydın, "Medeni Hukuk (Giriş, Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku)", haz. Aydın Zevkliler, Beşir Acabay, Emre Gökyayla, 6. Baskı, Ankara 1999, s. 470 vd.

920 Yargıtay 4. Hukuk Dairesinin 18/12/2013 tarihli ve 2013/2039 esas ve 2013/20094 karar sayılı kararında "Davacılar, dava konusu....başlığı ile yapılan haberde kişilik haklarının ihlal edildiğini, davacılardan ...'e ait pasaportun fotoğraf ve kimlik bilgilerinin bulunduğu sayfalarına burada yer alan her türlü bilgi okunacak şekilde yer verilip kişisel verilerin kullanılarak suç işlendiğini belirterek manevi tazminata hükmedilmesini istemişlerdir. Ceza davasında da, davacı ...'e yönelik kişisel verileri hukuka aykırı yaymak ve kişisel verilerin kaydedilmesi suçlarından davalılardan ...hakkında beraat kararı verilmiştir Davaya konu olayda; haberin veriliş biçimi, kullanılan ifadeler ve yukarıdaki ilkeler gözetildiğinde, davacılardan ...yararına hükmedilen manevi tazminat miktarı fazladır. Davacı yararına daha alt düzeyde manevi tazminata

Kanaatimizce, TMK madde 24 ve 25 ile TBK madde 49 kişisel verilerin korunması bakımından, bu hak ihlalinin gerçekleşmeden önlenmesi veya gerçekleştikten sonra def edilmesi bakımından genel hükümler içermektedir. Ancak anayasal bir hak olan kişisel verilerin korunması alanına yapılabilecek tecavüzler ile mücadelede genel hükümler yetersiz kaldığı doktrinde ileri sürülmekle beraber kanaatimizce son yıllarda gerek anayasal olarak gerekse KVKK'nın yürürlüğe girmesi ile yasal olarak epey ilerleme kaydedilmiştir.[921]

Kişisel Verileri Koruma Kanunun "Kurula şikâyet" başlıklı 14. maddesinin üçüncü fıkrasına göre de "kişilik hakları ihlâl edilenlerin, genel hükümlere göre tazminat hakkı saklıdır". 14. maddede sözü edilen genel hükümler, 6098 sayılı Türk Borçlar Kanunu'nun 53, 54, 56 ve 58. maddeleri ile ilgilidir.[922]

4.3. TÜRK CEZA KANUNU KAPSAMINDA KORUMA

4.3.1. GENEL OLARAK

765 sayılı ve daha önceki Ceza Kanunlarında kişisel verilere karşı işlenen suçlar özel olarak yer almadığından 5237 sayılı Türk Ceza Kanunu[923] kişisel verilerin korunması alanındaki suçları düzenleyen ilk ceza kanunu olmuştur.[924] 5237 sayılı TCK'nın *"Kişilere Karşı Suçlar"* kısmının *"Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar"* başlıklı 9. bölümünde yer alan 135, 136 ve 138. maddelerinde kişisel verilere karşı işlenen suçlar düzenlenmiştir. Bu suçların düzenlendiği maddelerin kanundaki yeri göz önüne alındığında, kanun koyucunun kişisel verileri *"özel hayat"* kavramı kapsamında değerlendirdiği anlaşılmaktadır.[925]

---

hükmedilmek üzere karar bozulmalıdır." gerekcesiyle kararı bozmuştur. https://kararara rama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/, Erişim tarihi: 17.12.2019.

921 Ayözger, a.g.e., s. 98.

922 Gürpınar, a.g.m., s. 688.

923 5237 sayılı Kanun, Resmi Gazete: 12/10/2004 Tarih, Sayı:25611.

924 Her ne kadar kişisel verilere yönelik suçlar 765 sayılı TCK'da düzenlenmemiştiyse de kişisel verilerle ilgili olabilecek, "*haberleşmenin gizliliğini ihlal*", "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" ve "*özel hayatın gizliliğini ihlal*" suçları ceza hukuku sisteminde 765 sayılı TCK'da da hüküm altına alınmıştı. Bkz. 756 sayılı TCK m. 525-a.

925 Çokmutlu, a.g.e., s. 144.

TCK'nın 135. maddesinde *"kişisel verilerin hukuka aykırı olarak kaydedilmesi"*, 136. maddesinde *"kişisel verilerin hukuka aykırı olarak başkasına verilmesi yayılması veya ele geçirilmesi"*, 138. maddesinde ise, *"sistemdeki verilerin yasal süresinde yok edilmemesi"* suç olarak düzenlenmiştir. Öte yandan, bu suçlardan ayrı olarak kişisel verilerin korunması açısından dolaylı olarak koruma sağlayan çeşitli suçlar da TCK'da düzenlenmiştir. Bu suç tipleri genellikle, *maddi konusu* ve *koruduğu hukuki değer* yönüyle kişisel verilere karşı işlenen suçlara benzerlik göstermektedir. TCK'nın 132. maddesinde düzenlenen *"haberleşmenin gizliliğini ihlal", 133.* maddesinde düzenlenen *"kişiler arası konuşmaların dinlenmesi ve kayda alınması"* ve 134. maddesinde düzenlenen *"özel hayatın gizliliğini ihlal"* suçları bu suçlara örnek olarak verilebilir.

Tüm bu suçların yanında *sırrın açıklanması* ile ilgili suçlar da TCK'da düzenlenmiştir. Meslek sırrı olarak değerlendirilebilecek çeşitli konulara ilişkin düzenlemeler kapsamında, banka ve sağlık personelinin, muhasebecilerin, vergi memurlarının ya da benzeri görev yapan diğer kişilerin meslekleri nedeni ile edindikleri bilgileri açıklamama yükümlülüğünü içeren düzenlemeler TCK'nın 239. ve 258. maddelerinde yer almaktadır. Ayrıca, TCK'nın *"Bilişim Suçları"* başlıklı Üçüncü Kısmının Onuncu Bölümünde yer alan suçların da bazı durumlarda dolaylı yönden kişisel verilerin korunmasına yardımcı olacağı değerlendirilebilir. Özellikle *"bilişim sistemine girme" (*madde243) ve *"sistemi engelleme, bozma, verileri yok etme veya değiştirme"* (madde 244), suçları, kişisel verilerin güvenliğinin sağlanması açısından oldukça önemli düzenlemelerdir.

KVKK'nın "Suçlar" başlıklı 17. maddesinin;

"1-Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140. madde hükümleri uygulanır.

2- Bu Kanunun 7. maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138. maddesine göre cezalandırılır."

şeklindeki düzenlemesi ile de kişisel veriler ile ilgili suçlarda TCK'nın 135-140. maddelerinin uygulanacağı hüküm altına alınmıştır.

4.3.2. KİŞİSEL VERİLERE DOĞRUDAN KORUMA SAĞLAYAN SUÇ TİPLERİ

4.3.2.1. Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu

TCK'nın 135. maddesinde *"...kişisel verilerin hukuka aykırı olarak kaydedilmesi"* fiili suç olarak düzenlenmiştir. Maddenin 2. fıkrasında, "*kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine*; *hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına…"* ilişkin kişisel verilerin kaydedilmesi halinde öngörülen cezanın yarı oranında artırılacağı düzenlenmiştir.

Bu suçla korunan hukuki değer kişinin özel hayatının gizliliği ve kişisel verilerinin korunması hakkıdır.[926] Kişisel verilerin korunması bütüncül bir sistem olup, kişisel verilerin toplanıp kaydedilmesi, depolanıp üçüncü kişilere aktarılması ve silinmesi dahil tüm aşamaları kapsamına almaktadır. Tüm bu aşamaların hepsinde, veri işleyenlerin hukuka uygun davranma mecburiyetlerinin bulunmasının yanında, kişinin de kendisine ait veriler hakkında bilgi alma, bu verilerin silinmesini veya güncellenmesini talep etme gibi hakları vardır. Bu aşamalardan herhangi birinde hukuka aykırı davranılması veya kişinin kendisine tanınan haklarını kullanmasının engellenmesi bu hakkın ihlali edilmesi sonucunu doğuracaktır. Anayasa'da 2010 yılında yapılan değişiklikten sonra TCK'da düzenlenen *"kişisel verilerin hukuka aykırı olarak kaydedilmesi"* suçu ile korunmak istenen hukuki değerin, *özel hayatın gizliliği ve kişisel verilerin korunması hakkı* olduğundan kuşku bulunmamaktadır.[927]

Kişisel verilerin korunması hakkı 2010 yılından itibaren anayasal güvenceye kavuşmuş ve herkesin kendisi ile ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu kabul edilmiştir. Çalışmamızın önceki bölümlerinde de bahsettiğimiz üzere bu hak, veri sahibinin kendisi ile ilgili olan kişisel verileri hakkında

926 Özbek, Veli Özer/ Kanbur, Mehmet Nihat/Doğan, Koray / Bacaksız, Pınar/ Tepe, İlker,"Türk Ceza Kanunu Özel Hükümler", Ankara, 2013, Seçkin Yayınevi, s. 527.

927 Çokmutlu, a.g.e., s. 175.

bilgilendirilme, tutulan bu verilere erişebilme, bu verilerin silinmesi veya düzeltilmesini isteme haklarını da kapsamaktadır. Bu kapsamda TCK'nın 135. maddesindeki bu suçun, anayasal koruma altına alınan *"kişisel verilerin korunması hakkı*"nın ihlaline yaptırım öngören bir düzenleme olarak karşımıza çıktığından, bu suçla, özel hayatın gizliliğinin ihlalinden daha ziyade kişisel verilerin korunması hakkının muhafaza edilmek istendiği kanaatindeyiz.

Bu suçun maddi konusu kişisel veridir.[928] KVKK'nın yürürlüğe girmesinden önce *kişisel veri*nin ne olduğu veya bu terimden ne anlaşılması gerektiği konusunda madde metninde bir açıklık bulunmaması nedeniyle, bu düzenlemenin kanunilik ilkesinin bir gereği olan *açıklık ve belirlilik* ilkelerine uymadığı yönünden eleştiriler yöneltilmiş ise de KVKK'nın yürürlüğe girmesiyle bu konudaki eleştiriler geçerliliğini yitirmiştir.

TCK'nın 135. maddesinin 1. fıkrasında düzenlenen bu suç bakımından *gerçek kişi*yle ilgili olan her türlü bilgi kişisel veri olarak kabul edilecektir. TCK'nın 135. maddesinin 2. fıkrasında düzenlenen suçun konusu ise; kişilerin "*siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, ahlaki eğilimlerine, cinsel yaşamlarına sağlık durumlarına* veya *sendikal bağlantılarına"* ilişkin bilgilerdir.[929] Çalışmamızın önceki bölümünde belirttiğimiz gibi bu maddenin 2. fıkrasında sayılan ve daha fazla ceza öngörülen veriler hassas nitelikli kişisel verilerdendir.

TCK'nın 135. maddesinin 2. fıkrasında yer verilen hassas kişisel veriler arasında bir ayrım yapılarak, kişilerin *"siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin bilgiler" mutlak dokunulmaz* veriler olarak kabul edilirken; kişilerin *"ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgiler*" nisbi dokunulmaz veriler olarak kabul edilmiştir. Başka bir ifade ile, ilk grupta yer verilen veriler hiçbir şekilde kaydedilemeyecekken, fıkrada yer alan *"hukuka aykırı olarak"* ibaresi nedeniyle, ikinci grupta yer verilen verilerin

928 Özbek, Veli Özer/ Kanbur, Mehmet Nihat/Doğan, Koray / Bacaksız, Pınar Tepe, a.g.e., s. 527.

929 Parlar, Ali/ Hatipoğlu, Muzaffer, "Türk Ceza Kanunu Yorumu", 2. Baskı, Cilt: 2. Ankara, 2008, s. 2043.

kaydedilmesi, bunun için mevzuatta bu tür verilerin işlenmesine izin veren hükümlerin bulunması kaydıyla, mümkün olabilecektir.[930]

Madde metninde *"kimse"* ifadesine yer verildiği için herkes bu suçun faili olabilir. Bundan dolayı bu suç, fail açısından özellik arz eden bir suç değildir.[931] Ancak TCK'nın "Nitelikli Haller" başlıklı 137. maddesinde bu suçun da içinde olduğu suçların nitelikli hali düzenlenmiştir. Söz konusu düzenlemeye göre bu suçun kamu görevlisi tarafından ve görevinin verdiği yetkinin kötüye kullanılması suretiyle ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanılması suretiyle işlenmesi halinde verilecek cezanın yarı oranında artırılacağı hüküm altına alınmıştır.

Bu suçun mağduru herkes olabilir.[932] Her ne kadar bazı ülkelerde tüzel kişilerin de kişisel verilerin korunması kapsamında kabul edildiği düzenlemeler var ise de iç hukukumuzda kişisel verilerin korunması hakkının sadece gerçek kişiler yönünden kabul edildiği göz önüne alındığında bu suçun mağdurunun sadece gerçek kişiler olabileceği ortadadır.

Kişisel verilerin kaydedilmesi suçunun hareket unsuru ise *"kişisel verileri kaydetmek"*tir.[933] Kaydetme eylemi ise *icrai hareket* olduğundan, bu suç ihmal hareketi ile işlenemeyecektir. Bu suç, sırf hareket suçu yani neticesiz suç olarak düzenlenmiştir. Bu kapsamda bu suçun neticesi harekete bitişik olduğu için kişisel verilerin hukuka aykırı olarak kaydedilmesi ile bu suç tamamlanacaktır.[934] Başka bir deyişle, bu suçun oluşması için, verileri kaydedilen kişinin, herhangi bir zarara uğramış olması şart değildir.[935]

Maddenin 2. fıkrasındaki düzenlemede, "*kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması"* durumu

930 Özbek ve diğerleri, a.g.e., s. 529.

931 Özbek ve diğerleri., a.g.e., s. 529.

932 Özbek ve diğerleri., a.g.e., s. 529.

933 Özen, Mustafa, "Kişisel Verilerin Kaydedilmesi, Verilmesi veya Ele Geçirilmesi ve Yok Edilmemesi Suçları", Kamu Hukuku Arşivi, 2009, S. 1, Y. 12, Ankara, s. 15.

934 Özbek ve diğerleri.,a.g.e., s. 530.

935 Parlar/Hatipoğlu, s. 2044.

cezalandırıldığından, maddenin bu fıkrasındaki suç, bağlı hareketli bir suçtur. Suç, sadece maddede sayılan verilerle sınırlıdır. Bu fıkrada sayılan verilerin dışında kalan şeylere ilişkin bilgilerin kaydedilmesi durumunda ikinci fıkradaki suç oluşmayacaktır. Bu yönüyle TCK'nın 135. maddesinin 2. fıkrasında düzenlenen bu suç aynı konuyu düzenleyen 135. maddenin 1. fıkrası, 136. madde ve 138. maddesinden ayrılır.[936]

TCK'nın 135. maddesinde düzenlenen bu suç genel kastla işlenebilen bir suçtur. Başka bir ifadeyle, suçun kanuni tanımında yer alan bütün unsurlar fail tarafından bilinmiyorsa kasten işlenen bir suçtan bahsedilemeyeceğinden, suç açısından failin, mağdurun kişisel verilerini kaydetme niteliğindeki davranışları *bilerek ve isteyerek* yapması suçun oluşması için gerekli ve yeterli olup bu konuda saik önemli değildir. Suçun taksirle işlenebilen hali TCK'da düzenlenmediği için bu suç, taksirle işlenebilen bir suç değildir.[937] Zira TCK'nın 22/1. maddesine göre taksirle işlenen fiiller ancak kanunda açıkça belirtilmiş ise cezalandırılabilecektir. Bu nedenle fail, taksirli hareketiyle kişisel verileri kaydederse bundan dolayı sorumlu olmayacaktır.

TCK'nın 135. maddesinde bu suç için olabilecek hukuka uygunluk nedenlerine yer verilmemiştir. Bu konuda TCK'nın "Genel Hükümler" kısmında yer verilen; "*kanun hükmü ve amirin emri, hakkın kullanılması ve ilgilinin rızası, meşru savunma ve zaruret hali, cebir, şiddet, korkutma ve tehdit"* gibi nedenler bu suç açısından da kısmen uygulanma olanağı bulabilir. Kanaatimizce burada amirin emrinin hukuka uygunluk sebebi olarak sayılabilmesi için amirin meşru bir amaç için kanundan meşruiyetini alan bir emir vermesi gerekmektedir. Aksi takdirde anayasal bir hüküm olan kanunsuz emrin yerine getirilmesi tekrar yazılı bir şekilde o emrin tekrarı ile mümkündür.[938] Fakat emrin konusu hiçbir şekilde suç teşkil edemeyeceğinden kanunda düzenlenmeyen bir hususta amirin kişisel veri toplanması veya kaydedilmesi

936 Özbek ve diğerleri.,a.g.e., s. 530.

937 Parlar/Hatipoğlu, a.g.e., s. 2045.

938 1982 Anayasası Madde 137/1.

emri vermesi durumunda Anayasanın amir hükmü gereğince emir yerine getirilmeyecektir.[939]

Çalışmamızın 2. bölümünde "*İşlem Yasağının İstisnaları*" başlığı altında kişisel verilerin işlenmesini hukuka uygun kılan nedenler açıklanmıştır. Ayrıca KVKK'nın 28. maddesinde de "İstisnalar" başlığı altında KVKK'nın ilgili hükümlerinin uygulanmayacağı durumlar düzenlenmiştir. Buna göre, KVKK hükümleri şu durumlarda uygulanmakta ve bu durumlardan birisinin varlığı halinde hallerinde herhangi bir suç vücut bulmamaktadır:

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

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

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

- *"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."*

- *"Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi."*

Ayrıca KVKK'nın kişisel verilerin işlenme şartlarının düzenlendiği 5. maddesinde;

---

939 1982 Anayasası Madde 137/2.

“ ... Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

d) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

e) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

g) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.”

şeklinde ifade edildiği üzere, kişisel verilerin işlenmesinin hukuka uygunluk nedenleri sayılmıştır.

Kişisel verileri kaydetme suçuna teşebbüsün mümkün olup olmadığı konusunda doktrinde tam bir görüş birliği yoktur. Bu konuda bazı yazarlara göre; bu suç neticesi harekete bitişik suçlardan olduğundan, kişisel verilerin hukuka aykırı olarak kaydedilmesiyle suç tamamlanır ve bu yönüyle bu suç kural olarak teşebbüse elverişli bir suç değildir.[940] Zira, kişisel verilerin ele geçirilmiş olmasına rağmen henüz kaydedilmemiş olması durumunda da teşebbüs söz konusu olmayacaktır, çünkü kişisel verilerin hukuka aykırı olarak ele geçirilmiş olması da ayrıca suç olarak

940 Özbek ve diğerleri., a.g.e., s. 537.

düzenlenmiştir.[941] Bu konuda başka bir görüşe göre ise, bu suç teşebbüse elverişli bir suçtur. TCK'nın 135. maddesinde düzenlenen bu suçun tamamlanması için, mağdurun herhangi bir zarara uğramış olmasına gerek yoktur. Bundan dolayı, bu suç, sırf hareket suçu olduğu için, hareketlerin bölünebildiği oranda bu suça teşebbüs mümkün olacaktır. Bu konuya, bir failin, mağdur hakkındaki kişisel verileri depolamaya başladığı anda yakalanması halinde eylemin teşebbüs aşamasında kalmış olacağı örnek olarak gösterilmektedir.[942] Her ne kadar teknik olarak hareketin bölünme imkânı olduğu sürece suça teşebbüsün mümkün olduğu düşünülse bile, uygulamada bu suçun teşebbüs haline rastlanmasının pek mümkün olmayacağı kanaatindeyiz.

TCK'nın 135. maddesinde düzenlenen bu suça iştirakin her çeşidi mümkündür. Madde metninde iştirake ilişkin özel bir düzenleme bulunmadığı için, iştirak konusunda genel hükümler uygulanacaktır.[943]

Aynı suç işleme kararının icrası kapsamında olmak üzere kişisel verilerin kaydedilmesi suçu aynı kişiye karşı farklı zamanlarda birden fazla işlenmiş ise, zincirleme suç[944] hükümleri uygulanacaktır. Bunun yanında, failin tek bir hareketiyle birden fazla kimsenin kişisel verilerini kaydedilmesi halinde de yine zincirleme suç (aynı neviden fikri içtima) hükümleri uygulanacaktır.

Kişisel verilerin hukuka aykırı olarak kaydedilmesinden sonra, bir başkasına verilmesi veya yayılması durumunda TCK'nın 136. maddesindeki suç da ayrıca oluşacağı için, gerçek içtima kuralları uygulanarak her iki suçtan ayrı ayrı ceza verilecektir. Kaydedilen kişisel verilerin ifşa edilmesi halinde ayrıca hakaret suçu da oluşuyorsa, bu durumda da gerçek içtima kuralları uygulanacaktır.[945] [946]

---

941 Özbek ve diğerleri., a.g.e.,s. 537; TCK madde 136.

942 Parlar/Hatipoğlu, a.g.e., s. 2045.

943 Parlar/Hatipoğlu, a.g.e., s. 2045.

944 TCK m. 43/1-2.

945 Parlar/Hatipoğlu, a.g.e., s. 2046.

946 Bunun yanında, failin hukuka aykırı olarak kişisel veriyi kaydetme ve başkasına verme ya da yayma fiillerini aynı anda gerçeklemesi mümkündür. Mesela, kişisel verinin ulaşılabilir bir internet sitesine kaydedilmesi durumunda kaydetmenin yanında aynı zamanda yaymak fiili de gerçekleşmiş olur. Kişisel verileri hukuka aykırı olarak yaymak fiili, TCK'nın 136. maddesinde ayrı bir suç olarak düzenlendiği için, bu durumda fikri içtima hükmü gereği daha ağır cezayı gerektiren 136. madde uygulanmalıdır. Özbek ve diğerleri, s. 537.

4.3.2.2. Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu

TCK' nın 136. maddesinde kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak ve ele geçirmek suçu *"kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."* şeklinde düzenlenmiştir.

Bu maddede, herhangi bir şekilde elde edilmiş veya kaydedilmiş kişisel verilerin başkalarına verilmesi, yayılması veya bu verilerin ele geçirilmesi fiilleri suç olarak kabul edilmiştir. Bu suçun oluşması için *verme, yayma ve ele geçirmek* eylemleri açısından, suça konu kişisel verilerin, hukuka uygun olarak elde edilmiş veya kaydedilmiş olması ile hukuka aykırı bir şekilde elde edilmiş veya kaydedilmiş olması arasında bir fark yoktur.[947]

Kişisel verileri hukuka aykırı olarak verme ve yayma fiillerinin yaptırıma bağlanması ile kişisel verilerin yetkisiz üçüncü kişilere aktarılmasının ve verilerin yetkisiz üçüncü kişilerce ele geçirilmesinin önüne geçilmek istenmiştir. Bu durumda, daha önceden kaydedilmiş olsun veya olmasın kişisel verileri hukuka aykırı olarak ele geçiren kişi TCK'nın 136. maddesi gereğince cezalandırılacaktır.[948] Ayrıca, TCK'nın 136. maddesinin başlığında "yayma" fiili sayılmamışken, madde metninde "yayma" fiilinin de düzenlenmiş olması kanun yapma tekniği açısından uyumlu olmamıştır. Yine suçun konusunun kişisel veri olması ve "veri" ile "kişisel veri"nin aynı kavramlar olmaması nedeni ile madde başlığında "veri" ifadesinin kullanılmasının da yerinde olmadığı kanaatindeyiz.

TCK'nın 136. m.'sinde yer verilen düzenleme kişisel verilerin korunmasını sağlayıcı niteliği nedeni ile oldukça önemli bir düzenlemedir. Çünkü, veri ilgilisinin, *"kişisel verilerin hukuka aykırı olarak ele geçirilmesi, başkalarına verilmesi veya yayılmasında"*, kişisel verilerin kaydedilmesi suçuna oranla daha büyük zararlara uğraması söz konusu olabilecektir. Nitekim, bu suç ile kişinin özel hayatının gizliğinin ihlal edilmesinin yanında, kişinin; şantaja maruz kalabilme, verilerinin başkaları

947 Hakeri, Hakan, "Hasta Hakları Bakımından Yeni Türk Ceza Kanunu", http://portal.hakanhakeri.com/index.php?option=com_content&task=view&id=27&Itemid=35, Erişim tarihi, 05.07.2019.

948 Küzeci, a.g.e., s. 291.

tarafından öğrenilecek olması nedeniyle toplumda küçük düşme, onurunun ve itibarının zedelenmesi veya ayrımcılığa maruz kalması gibi ağır nitelikli zararlarla karşılaşabilmesi söz konusu olabilecektir.[949]

TCK'nın 136. m.'sinde düzenlenen bu suç ile korunan hukuki yarar, kişisel verilerin korunması ve özel hayatın gizliğine ilişkin bireysel ve toplumsal yarardır. Bu suç ile korunmak istenen hukuki değer, kişisel verilerin kaydedilmesi suçu ile korunmak istenen hukuki değer aynıdır. Bu nedenle kişisel verilerin kaydedilmesi suçu yönünden yaptığımız açıklamalar bu suç için de geçerlidir.

TCK'nın 136. m.'sinde *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi"*nin cezalandırılacağı düzenlendiğine göre, failin kişisel verileri, hukuka aykırı olarak bir "*başkasına vermesi, yayması veya ele geçirmesi"* eylemleri cezalandırılacaktır. Maddede kişisel veriler için bir ayrım veya sınırlandırma yapılmadığına göre her türlü kişisel veriye karşı bu suçun işlenmesi mümkündür.

Suçun konusu "*kişisel veri*"lerdir.[950] Madde metninde herhangi bir ayrım yapılmadığına göre tüm kişisel veriler bu suçun konusunu oluşturabilecektir. TCK'nın 135. m.'sinde kişisel veriler ile hassas kişisel veriler arasında ayırım yapılarak, hassas kişisel verilerin kaydedilmesi daha ağır cezayı gerektirecek şekilde düzenlenmiş ise de bu maddede böyle bir ayrıma gidilmemiştir.

TCK'nın 136. m.'sinde; *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi…"* ifadesine yer verilmesi nedeni ile bu suçun faili herkes olabilecektir.

Bu suçun mağduru her gerçek kişi olabilir. Çalışmamızın önceki bölümlerinde açıkladığımız üzere ülkemizde kişisel verilerin korunması kapsamında sadece gerçek kişilerin kabul edilmesi nedeni ile bu suçun da mağduru sadece gerçek kişiler olabilecektir.

---

949 Özen, a.g.m., s. 20.

950 Özbek ve diğerleri,a.g.e., s. 538.

TCK'nın 136. m.'sinde, kişisel verilerin bir başkasına verilmesi, yayılması ve ele geçirilmesi eylemleri, suç olarak düzenlendiğinden, bu suç, seçimlik hareketli bir suçtur. Bu kapsamda, kanunda yer alan hareketlerden birinin veya birkaçının birlikte gerçekleştirilmesi suçun oluşumunu etkilemeyecek, tek bir suç oluşacaktır.[951]

Maddede suç olarak sayılan hareketler, kişisel verileri hukuka aykırı olarak; *"bir başkasına vermek"*, *"yaymak"* veya *"ele geçirmek"* eylemleridir.

*Vermek***,** eylemini gerçekleştirebilmek için kişisel verilerin failin elinde veya uhdesinde bulunması gerekir. Zira ancak kişi elde bulundurduğu şeyi bir başkasına verebilecektir. Vermek eylemi iki kişi arasında gerçekleşen bir eylemdir.[952]

*Yaymak***,** kişisel verilerin korunması açısından, kişisel verilerin içeriğinin birçok kişinin öğrenmesine imkân tanıyacak şekilde başkalarının bilgisine sunulması, duyurulması anlamındadır. Yaymak eyleminde birden fazla kişi hedeflemektedir.[953]

Kişisel verileri *verme ve yayma* eylemleri, kitle iletişim araçları kullanılmak sureti ile gerçekleştirilebileceği gibi bir araç kullanmadan doğrudan da gerçekleştirilebilir.[954]

*Kişisel verileri ele geçirmek*se, failin başkalarına ait olan veya başkalarının tasarrufu altında olan kişisel verileri kendi tasarruf alanına sokmasıdır. Başka bir ifade ile, bir şekilde kişisel verileri elde etmek, uhdeye almaktır. Bu kapsamda, ele geçirme eylemi fiziki bir dosyada bulunan verileri elde etmek şeklinde olabileceği gibi, bilgisayar ortamında, hususiyle de internet üzerinde bulunan kişisel verileri, yine internet üzerinden ele geçirme şeklinde de gerçekleşebilir. Bu noktada ele geçirmek fiili, kaydetmek şeklinde de gerçekleşebilir. Ancak TCK'nın 135. maddesi kişisel verilerin kaydedilmesini ayrıca cezalandırdığı için, bu maddede geçen ele geçirmek fiili "kaydetme" dışında kalan eylemleri kapsayacak şekilde anlaşılmalıdır.[955]

---

951 Hafızoğulları, Zeki/Özen, Muharrem, "Türk Ceza Hukuku, Özel Hükümler, Kişilere Karşı Suçlar", Ankara, 2011, s. 279.

952 Hafızoğulları/Özen, a.g.e., s. 279.

953 Özbek ve diğerleri, a.g.e., s. 539

954 Özen, a.g.m., s. 21.

955 Özbek ve diğerleri, a.g.e., s. 539.

"Kişisel verileri, hukuka aykırı olarak bir başkasına verme, yayma veya ele geçirme suçu" da sırf hareket suçu olarak düzenlenmiş olup, söz konusu kişisel verilerin "*verilmesi*", "*yayılması*" veya "*ele geçirilmesi*" hareketlerinin gerçekleşmesiyle suç tamamlanmış olur. Yani, bu suçun tamamlanmış kabul edilmesi için kişisel verilerin hukuka aykırı olarak "*verilmesi, yayılması ya da ele geçirilmesi"* yeterli olup, ayrıca bundan bir zarar doğmuş olması da şart değildir. Yine bu suçun oluşması için bu verilerin kaydedilmesi de gerekli değildir. Bu yönüyle bu suç aynı zamanda "*tehlike suçu*"dur.[956]

Fail fiilini gerçekleştirdikten sonra, bu suçun oluşması için belli bir sürenin geçmesi veya kişisel verinin bir süre saklanmış olması da şart değildir. Bu suçun verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesiyle tamamlanmış olacağından, bu yönüyle bu suç neticesi bakımından "*ani bir suç"*tur.[957]

Kişisel verileri verme, yayma ve ele geçirme suçu, suçun oluşumu için gerçekleştirilmesi gereken eylemlerin niteliği gereği ancak icrai hareketle işlenebilecek olan bir suçtur. Yani ihmali hareketle bu suç işlenemez.[958]

Bu suç genel kastla işlenebilir bir suçtur. Bu suç açısından, bir kimsenin kişisel verilerini bir başkasına verdiğini, yaydığını veya ele geçirdiğini bilmesi ve istemesi failin kastı için yeterlidir. Bu konuda saik önemli değildir. Bu suçun taksirle işlenen hali kanunda düzenlenmediği için bu suç taksirle işlenemez.[959]

TCK'nın 136. maddesinde *"kişisel verilerin hukuka aykırı olarak"* bir başkasına verme, yayma veya ele geçirme fiillerinden söz edilmiş ve "*hukuka aykırılık*" ibaresine ayrıca vurgu yapılmıştır.[960] Bu suçun oluşabilmesi için, başka bir hukuk kuralı tarafından kişisel verilerin verilmesi, yayılması veya ele geçirilmesi için izin verilmemiş olması gerekir. Başka bir hukuk kuralının bu eylemlere izin vermesi halinde eylem bu suçu oluşturmayacaktır.

---

956 Özbek ve diğerleri, a.g.e., s. 539.

957 Özbek ve diğerleri, a.g.e., s. 539.

958 Özen, a.g.m., s. 21.

959 Parlar/Hatipoğlu, a.g.e., s. 2049.

960 Özbek ve diğerleri, a.g.e., s. 540.

Suçun oluşumu için TCK'nın 136. maddesinde sayılan fiillere başka kanun tarafından izin verilmemiş olması gerektiğine göre hukuka uygunluk nedenlerinin bu suç için de belirlenmesi gerekmektedir. Suçun düzenlendiği bu maddede bu suç için olabilecek hukuka uygunluk nedenlerine yer verilmemiştir.

Kişisel verileri kaydetme suçunda bahsetmiş olduğumuz üzere, Türk Ceza Kanunu'nun genel hükümler kısmında yer alan, *"kanun hükmü ve amirin emri, hakkın kullanılması ve ilgilinin rızası, meşru savunma ve zaruret hali, cebir şiddet, korkutma ve tehdit"* gibi nedenler somut olayın özelliklerine göre bu suç açısından da uygulama alanı bulabilecektir. Ayrıca KVKK hükümlerinin uygulanmayacağı "istisnalar"ın düzenlendiği KVKK'nın 28. maddesinde sayılan hususlar ile "*kişisel verilerin işlenmesi şartları*"nın düzenlendiği aynı kanunun 5. maddesindeki hususlar bu suç yönünden de hukuka uygunluk nedeni teşkil edecektir.

Kişisel verilerin kaydedilmesi suçunda teşebbüsün mümkün olup olmadığı yönünde yaptığımız açıklamada da belirtmeye çalıştığımız üzere, bu suç her ne kadar sırf hareket suçu olsa da ve suç hareketin yapılması ile tamamlansa bile hareketin bölünebildiği sürece, teorik olarak, bu suça teşebbüsün mümkün olduğu kanaatindeyiz.

Bu suç iştirak açısından bir özellik göstermediğinden, bu suça iştirakin her şekli mümkün görünmektedir.[961]

TCK'nın 136. maddesinde içtima açısından özel bir düzenleme söz konusu olmadığından, içtima konusunda genel hükümler çerçevesinde değerlendirme yapılmalıdır. Bu suçun zincirleme suç olarak işlenmesi mümkündür. Örneğin, failin internet üzerinden aynı anda birden fazla kişinin kişisel verilerini hukuka aykırı olarak yayınlaması durumunda, TCK'nın 43/2 hükmüne göre zincirleme suç hükümleri uygulanabilecektir. Bunun yanında, failin hukuka aykırı olarak kişisel verileri kaydetme ile başkasına verme ya da yayma eylemlerini aynı anda gerçekleştirmesi durumunda, fikri içtima hükmü gereğince en ağır cezayı gerektiren madde

961 Parlar/Hatipoğlu, a.g.e., s. 2050.

uygulanmalıdır. Çünkü bu durumda kişisel verileri kaydetme fiili verileri yayma fiilinin içinde eriyecektir.[962]

TCK'nın 137. maddesinde yer verilen ağırlaştırıcı sebep bu suç için de geçerlidir. Yani, verileri hukuka aykırı olarak verme veya ele geçirme suçunun, "*kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle"* işlenmesi halinde faile verilecek ceza yarısı oranında artırılacaktır.

Yargıtay 12. Ceza Dairesinin 15/05/2019 tarih, 2018/8198 Esas ve 2019/6187 Karar sayılı kararında *"Şikayetçinin babasına ait facebook adresinde daha önce yayınladığı sadece baş ve yüz kısmını gösteren resmi, şikayetçinin başkalarının görmesini ve bilmesini istemeyeceği özel yaşam alanına ilişkin bir görüntü olarak kabul edilemeyeceğinden, şikayetçinin kişisel veri niteliğindeki resmini, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle internet sitesinde şikayetçi adına oluşturduğu sahte hesapta profil resmi olarak kullanan sanığın eyleminin, TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden, suç vasfında yanılgıya düşülerek, yasal ve yeterli olmayan gerekçelerle sanık hakkında TCK'nın 134/2. madde ve fıkrasında düzenlenen özel hayatın gizliliğini ihlal suçundan mahkumiyet kararı verilmesi"* sebebiyle bozmuştur.

4.3.2.3. Verileri Yok Etmeme Suçu

Çalışmamızın önceki bölümlerinde de belirttiğimiz üzere, kişisel verilerin işlenmesi, kişisel verilerin elde edilmesinden başlayarak, bu verilerin kaydedilmesine, üçüncü kişilere aktarılmasından yok edilmesi de dahil olmak üzere geçen süreçte kişisel veriler üzerinde yapılan her türlü işlemi kapsamaktadır. Bunun gibi kişisel verilerin korunması da bütüncül bir sistem olarak, bu kapsamda sadece kişisel verilerin kaydedilmesini değil, tüm veri işleme aşama ve hallerini de korumaktadır.

Kişisel verilerin korunması hakkı kişinin kendisi ile ilgili olan kişisel veriler hakkında bilgi edinme, bilgilendirilme, bu verilere erişme, bu verilerin düzeltilmesini

962 Özbek ve diğerleri, a.g.e., s. 541.

veya silinmesini talep etme ve kişisel verilerin işlenme amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsamaktadır.

Diğer taraftan kişisel veriler, nerede ve hangi amaçla bulunurlarsa bulunsunlar, kişinin özel hayatına dahil olup, cezai himayenin konusunu oluştururlar. Bunun yanında bazı kişisel veriler, süresiz olarak başka kişilerin bilgisine açıkken, bazı kişisel verilerin saklanılması ise, kullanım amaçları açısından, bir süre ile sınırlandırılabilmektedir. Kişisel verilerin korunmasının zorunlu bir sonucu olarak, saklanılması belirli süre ile sınırlandırılmış olan kişisel veriler, bu sürenin sonunda, bu verilerin bulundukları yerde yok edilmelidirler. Bu durumda bu kişisel verileri yok etmeme kişisel verilerin korunması hakkının ihlali anlamına gelecektir. Bu nedenle *"Verileri yok etmeme"* başlıklı TCK'nın 138. maddesinde, kanunlarla belirlenen sürelerin geçmiş olmasına rağmen, kişisel verileri bulundukları sistem içinde yok etmekle yükümlü olan kişilerin bu görevlerini ihmal ederek, yerine getirmemeleri suç olarak düzenlenmiştir.[963]

TCK'nın 138. maddesinde verileri yok etmeme suçu, *"kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası"* verileceği şeklinde düzenlenmiştir. Verileri silmeme suçunun oluşması için, hukuka uygun bir şekilde kaydedilmiş olan kişisel verilerin bulunması, bu verilerin silinmesi için kanunlarda sürelerin belirlemiş olması ve bu verilerin silinmesi için yetkili ve görevli olan failin, bu sürelerin geçmiş olmasına rağmen, failin bu görevlerini yerine getirmemiş olması gerekir.

Verileri yok etmeme eyleminin suç olarak düzenlenmesi ile, kişisel verilerin korunmasının temel ilkelerinden olan ve KVKK m. 4/2-d'de düzenlenen, kişisel verilerin *"amaç için gerekli olan süre"* için işlenmeleri prensibinin gereği karşılanmıştır. Bu ilke gereğince kişisel veriler, toplanma amaçları için gerekli olan süreden daha uzun süre tutulamayacaklardır. Kişisel verilerin süresiz olarak tutulamaması, "*amaçla bağlantılılık ilkesi*" açısından da oldukça önemli olup, artık

963 Hafızoğulları/Özen, a.g.e., s. 280.

ihtiyaç kalmayan verilerin silinmesi veya anonimleştirilmesi ile kişisel niteliğinin ortadan kaldırılması bu konudaki keyfi uygulamaların önüne geçilmesi için gereklidir.[964] Ancak, kanun metninde bu suçun oluşabilmesi için *"kanunların belirlediği sürelerin geçmiş olması"* ölçütü esas alınmış, bu konuda "*verinin toplanma amacı"* ile bir irtibat kurulmamıştır.[965] Başka bir deyişle, verilerin toplanma amacı gerçekleşmiş veya ortadan kalkmış olsa bile bu kişisel verilerin yasada belirtilen süreler boyunca saklanabilmesi amaca bağlılık ilkesi ile bağdaşmamaktadır.[966]

Verileri silmeme suçu ile korunan hukuki yarar, kişisel verilerin korunması hakkıdır. Şöyle ki; bu suçta kişisel veriler hukuka uygun olarak kaydedilmiş ve hâlâ sistem içinde muhafaza edilmektedir. Söz konusu bu verilerin kanunda belirlenen süre geçmesine rağmen silinmemiş olmasında her zaman kişilerin özel hayatını ihlal edebilecek bir durum söz konusu olmayabilir. Nitekim, kişisel veriler öğrenmesi gereken kişiler tarafından zaten öğrenilmiş olup, verilerin sistem içinde kaldıkları sürece de başkaları tarafından öğrenilmeleri söz konusu olmayacaktır. Diğer taftan, kişisel verilerin korunmasının bütüncül bir sistem olduğu ve kişisel verilerin toplanmasından, kaydedilmesine, depolanmasından, üçüncü kişilere aktarılmasına veya silinmesine kadarki geçen tüm aşamaları kapsadığı da göz önüne alındığında, bu suç ile korunan hukuki değerin özel hayatın gizliliği değil kişisel verilerin korunması hakkı olduğu kanaatindeyiz.

TCK'nın 138. maddesinde *"Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde…"* cezalandırılacakları ifade edildiğine göre, kanunlarda belirlenen sürelerin geçmesine rağmen, söz konusu verileri sistem içinde yok etmekle yükümlü olan failin görevini yerine getirmemek sureti ile kişisel verileri yok etmemesi eylemi cezalandırılmaktadır. Kanaatimizce, burada fail kamu görevlisi ise, görevi ihmal suçunu düzenleyen TCK hükmü ile bu hüküm yarışma halinde olacaktır. Ancak bu hüküm TCK'ya göre özel nitelikte olduğu için görevi ihmal suçu değil bu suç

964 Küzeci, a.g.e., s. 291.

965 Ketizmen, a.g.m., s. 241.

966 Küzeci, a.g.e., s. 291.

oluşacaktır. Bununla beraber, bu suçu kamu görevlisi olmayanların da işleyebileceği aşikârdır.[967]

Hukuka uygun olarak kaydedilmiş olan kişisel veriler, verileri silmeme suçunun konusunu oluşturur.[968] Başka bir ifade ile bu suçun konusu, hukuka uygun olarak kaydedilmiş ve belli süre geçmesi halinde silinmesi gerektiği kanunla belirlenmiş olan kişisel verilerdir.

TCK'nın 138/1. maddesinde suçun faili *"verileri sistem içinde yok etmekle yükümlü olanlar"* şeklinde belirlendiği için suç bu konudaki diğer suçlardan farklı olarak fail bakımından özellik arz etmektedir. Yani bu suçu ancak *"verileri sistem içinde yok etmekle yükümlü olan"* kişiler işleyebilir. Bu yönüyle verileri silmeme suçu, *özgü suç*lardır.[969] Verileri "*sistem içinde yok etmekle yükümlü olan" kişiler* kamu görevlisi olabileceği gibi, kamu görevlisi olmayan kişiler de olabilir. Bu konuda önemli olan nokta, bir kişinin kanunlarda belirlenen sürelerde sistemde kayıtlı olan kişisel verileri yok etmekle yükümlü olup olmadığı hususudur.[970] Bu kapsamda failin bir kamu görevlisi olması mümkün olduğu gibi bir meslek ve sanat sahibi olması da mümkün olduğundan, TCK'nın 137. maddesinde benzer diğer suçlar bakımından kabul edilen cezayı ağırlaştıran nedenler, bu suç bakımından öngörülmemiştir.[971]

Maddedeki düzenleme göz önüne alındığında bu suçun mağdurunun sadece kişisel verileri sistemde kayıtlı bulunan gerçek kişiler olduğu anlaşılmaktadır. Zira, bu suç, kişisel verileri sistem içinde yok etme yükümlülüğü yerine getirilmeyerek işlendiğine göre, suçun konusu sistem içinde bulunan kişisel veri olduğu gibi, suçun mağduru da bu verinin sahibi olan kişi olacaktır.[972]

---

967 Akdağ, Hale, "TCK Kapsamında Kişisel Verilerin Korunması", Yüksek Lisans Tez, Ankara Sosyal Bilimler Enstitüsü, 2010, s. 134.

968 Parlar/Hatipoğlu, a.g.e., s. 2053.

969 Özgü suç, ilgili suçun tanımında failin özel bir niteliğe sahip olmasının arandığı suçlardır. Erdem, M.Ruhan, "Yeni TCK'da Faillik Ve Suç Ortaklığı", Hukuki Perspektifler Dergisi, Sayı: 5,Yıl: Aralık 2005, s. 206.

970 Ersan, Şen, Türk Ceza Kanunu Yorumu, Cilt: I, İstanbul, 2006, s. 611.

971 Özbek ve diğerleri, a.g.e., s. 5 42.

972 Özbek ve diğerleri, a.g.e., s. 542.

TCK'nın bu maddesinde tanımlanan suçu oluşturan hareket, kişisel verilerin konulduğu sistemde yok edilmesi yükümlülüğünün ihlal edilmesi, yerine getirilmemesidir.[973]

Kişisel verilerin korunması sisteminde kişisel verinin yok edilmesi ile kast edilen şey, verinin, bir yerde kullanılabilir olmaktan çıkartılıp, silinmesi, ortadan kaldırılmasıdır. Yani burada asıl olan, söz konusu verinin kimsenin eline geçmemesinin, bir daha kullanılamamasının sağlanmasıdır.[974] "*Yok etmeme*" eyleminin maddedeki anlamını; bir verinin tamamen ortadan kaldırılmaması, dış dünyada beş duyu organı ile algılanmayacak hale getirilmemesi şeklinde kabul etmek gerekir.[975]

Bu suçun oluşması için failin verileri yok etmekle yükümlü olması ve bu yükümlüğün failin görev alanına giriyor olması, bu suç yönünden dikkat edilmesi gereken bir diğer husustur. Bu durum ise failin tabi olduğu mevzuat hükümlerine bakılarak belirlenecektir.[976]

Verileri yok etmeme suçu sadece ihmal yoluyla işlenebilecek bir suç olup, yasal yükümlülük altında bulunanlar, bu yükümlülüklerini ihmalen yerine getirmediklerinde bu suç gerçekleşmiş olacaktır. Bu kapsamda, kanun ile belirlenen süre aşıldıktan sonra verilerin yok edilmesi, failin eylemini suç olmaktan

---

973 Parlar/Hatipoğlu, a.g.e., s. 2055.

974 Hafızoğulları/Özen, a.g.e., s. 281.

975 Özen, a.g.m., s. 25.

976 Örneğin, Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmeliğin 16. maddesi, "*Kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde bu Yönetmeliğin 15'inci maddesi hükümleri uyarınca elde edilen veriler, Cumhuriyet savcısının huzurunda ve uygun göreceği usullerle derhâl yok edilir ve bu husus tutanağa geçirilir.*" şeklindedir. Yönetmeliğin 17. maddesinde ise "*Mahkûmiyet kararı verilmesi hâlinde bu Yönetmeliğin 15'inci maddesinin birinci ve ikinci fıkrası uyarınca elde edilen veriler kolluk tarafından, üçüncü fıkrasında belirtilen diş izleri ise bu işlemi yapan sağlık kuruluşu tarafından arşivlenir*" hükmü yer almaktadır. Bu iki hüküm birlikte değerlendirildiğinde Cumhuriyet savcısının verileri silmekle asıl yükümlü olan görevli olduğu görülmektedir. Aynı zamanda bu Cumhuriyet Savcısının o dosyaya bakmakla görevli savcı olması gerekir. Nitekim aynı Yönetmeliğin 22. maddesi "*Cumhuriyet başsavcılıklarınca yapılan iş bölümlerinde, bu Yönetmelik kapsamında elde edilen verilerin imha edilmesi ve diğer işlemlerin yürütülmesi amacıyla yeterli sayıda Cumhuriyet savcısı görevlendirilir*" hükmünü içermektedir. Özbek ve diğerleri, a.g.e., s. 543.

çıkarmayacağı gibi, mağdurun bu noktadaki rızası da fiili hukuka uygun hale getirmeyecektir.[977]

Bu suçun tamamlanması için failin yükümlüğüne aykırı olarak kişisel verileri yok etmemiş olması yeterli olup, bundan bir zarar doğması bu suçun tamamlanması açısından şart değildir. Bu nedenle suç bir *tehlike suçu*dur. Kanun metninde tanımlanan suç tipinde hareket ile tehlike neticesi arasında bir nedensellik ilişkinin varlığının araştırılması yönünde zorunluluk olduğuna dair bir ifade yer almadığından bu suçun *soyut tehlike suçu*[978] olduğu söylenebilir. Yine bu suç, failin hareketini yapmasıyla yani failin yükümlülüğünü yerine getirmemesiyle tamamlandığı için ayrıca *ani hareketli bir suç* olarak kabul edilebilir.[979]

Verileri yok etmeme suçu, genel kastla işlenen bir suç olduğu için, failin "*kişisel verileri sistem içinde yok etme yükümlülüğünü"* kasten yerine getirmemesi yeterlidir. Bu suçta fail "*yok etme*" için kanunun belirlediği sürelerin geçmiş olduğunu bilmesine rağmen verileri silmemelidir. Failin saikinin bir önemi yoktur. Bu suçun taksirle işlenebilen hali kanunda düzenlenmediğine göre bu suç taksirle işlenemeyecektir.[980] Bu suçun taksirle işlenememesi nedeni ile, failin verilerin yok edilmesi için kanunla belirlenen sürelerde verileri taksirle (örneğin unutularak) yok etmemesi halinde bu suç oluşmayacaktır.[981]

Hukuka aykırılık, *"kanundaki tarife uygun bulunan fiile hukuk düzenince cevaz verilmemesi, fiilin yalnız ceza hukuku ile değil, bütün hukuk düzeni ile çelişki ve*

977 Hafızoğulları/Özen, s. 141 vd.

978 Suçun oluşması için bir zararın meydana gelmesinin gerekli olduğu suçlara "zarar suçu" denir. Zarar suçlarında korunan hukuki yarara zarar verilmesi gereklidir. Suçun oluşması için zarar tehlikesinin doğmasının gerekli olduğu suçlara ise "tehlike suçları" denir ki; tehlike suçlarında korunan hukuki yarar tehlikeye sokulur. Tehlike suçları da kendi arasında soyut tehlike suçu ve somut tehlike suçu olmak üzere iki gruba ayrılır. Somut tehlike suçu; suçun oluşması için suç ile korunan hukuki yararın gerçek anlamda tehlikeye sokulduğu suçlardır. Yani zarar tehlikesi olmalı olup, tehlikenin oluşup olmadığı varsayıma dayanmamalıdır. Soyut tehlike suçu ise; suçun oluşması için suç ile korunan hukuki yararın bir tehlikeye sokulmasının gerekmediği suçlardır. Bu suçlarda tehlikenin oluşup oluşmadığı konusu bir varsayıma dayanır. Bu nedenle soyut tehlike suçları neticesi harekete bağlı yani şekli suç türlerindendir. Detaylı bilgi için Bkz. Nur, Centel/Hamide, Zafer/Özlem, Yenerer Çakmut, Türk Ceza Hukuku'na Giriş, İstanbul, 2005, s. 260 vd.

979 Özbek, Veli Özer/ Kanbur, Mehmet Nihat/ Doğan,Koray / Bacaksız, Pınar/ Tepe, İlker., s. 544.

980 Parlar/Hatipoğlu, a.g.e., s. 2056.

981 Özen, a.g.m., s. 26.

çatışma halinde bulunması" demektir.[982] Bu suç açısından da fiilin, hukuka aykırı olması gerekli olmakla birlikte kanun metninde "*hukuka aykırı*" ibaresine diğer suçlarda olduğu gibi yer verilmemiştir. Böylece suçun kanundaki düzenlenişi itibariyle kanun koyucu bu suç yönünden "*hukuka aykırılık*" müessesesini daraltmıştır. Kanunda belirlenen süre sonunda failin kişisel verileri yok etmemesi halinde eylem hukuka aykırı olmakta ve diğer unsurların da gerçekleşmesi ile bu suç oluşmaktadır. Bir başka deyişle, zorunlu bazı nedenler yüzünden kişisel verilerin yok edilmemesini öngören başka bir kanun hükmü olmadıkça, bu eylem hukuka aykırı kabul edilecektir. Bu suçta kanuna aykırılık arandığından mağdurun rızası sanığın eylemini hukuka uygun hale getiremeyecektir.[983] Çünkü ilgilinin rızasına bakılmadan verilerin yok edilmesi kanunda emredici hüküm olarak kabul edilmiştir.[984]

Verileri silmeme suçunun tamamlanması için, mağdurun herhangi bir zarara uğramasına gerek olmayıp, kanununda belirlenen sürenin geçmiş olmasına rağmen, kişisel verilerin sistem içinde yok edilmemesiyle suç tamamlanmış olacağından, bu suça teşebbüsün mümkün olmadığı konusunda doktrinde görüş birliği vardır.[985]

Verileri silmeme suçunun, kişisel verileri sistem içinde silmekle yükümlü olan kişilerin işleyebileceği özgü suç olması nedeni ile, böyle bir görev ve yetkisi olmayan kişilerin TCK'nın 40/2. maddesi gereğince sadece azmettiren ya da yardım eden olarak suça iştirak edebileceklerdir. [986]

Verileri yok etmeme suçunun, *aynı suç işleme kararının icrası kapsamında olmak üzere aynı kişiye karşı birden fazla kez işlenmesi halinde*, zincirleme suç hükümleri uygulanacak, bunun yanında, aynı kişisel verinin uzun zaman silinmemesi

---

982 Artuk, M. Emin/ Ahmet, Gökcen/ Ahmet, Caner Yenidünya, "Türk Ceza Hukuku Genel Hükümler", 7. Baskı, Ankara 2013, s. 369.

983 Hafızoğlu/Özen, a.g.e., s. 281.

984 Özen, a.g.m., s. 26.

985 Özbek, Veli Özer/ Kanbur, Mehmet Nihat/ Doğan, Koray / Bacaksız, Pınar/ Tepe, İlker, s. 544; Şen, a.g.e., s. 611; Parlar/Hatipoğlu, a.g.e., s. 2056.

986 Parlar/Hatipoğlu, a.g.e., s. 2056.

veya yok edilmemesi halinde failin eylemi tek suç oluşturacak, zincirleme suç hükümleri uygulanamayacaktır.[987]

Failin verileri yok etmeme eylemi, birden fazla kişinin kişisel verilerine yönelik olursa, bu durumda da zincirleme suç hükümleri uygulama alanı bulacaktır. Çünkü bu durumda fail tek bir yok etmeme eylemi ile birden fazla kişiye karşı aynı suçu işlemektedir. Kişisel verileri yok etmekle görevli ve yetkili olan failin, bu verileri yok etmeyerek, aynı zamanda bu verileri bir başkasına vermesi veya yayması halinde, TCK'nın 136. ve 138. maddelerindeki suçlar ayrı ayrı oluşacak ve gerçek içtima kuralları uygulanacaktır.[988]

TCK'nın 138. maddesine 6526 sayılı Kanunla eklenen "*Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır."* şeklindeki 2. fıkra ile yok edilmesi gereken verilerin Ceza Muhakemesi Kanunu[989] hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veriler olması hâli ağırlaştırıcı neden olarak düzenlenmiştir. CMK'ya göre ortadan kaldırılması veya yok edilmesi gereken veriler ise; moleküler inceleme sonucu elde edilen veriler (CMK madde 75, 76, 78, 80), kimlik teşhisi için ele geçen veriler (CMK madde 81), telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sonucu elde edilen kişisel veriler (CMK madde 135, 137), gizli soruşturmacı atanması sonucu elde edilen kişisel veriler (CMK madde 139), teknik araçlarla izleme sonucu elde edilen kişisel verilerdir (CMK madde 140). Görüldüğü üzere CMK tarafından imha edilmesi öngörülen verilerin esas itibarıyla büyük çoğunluğunu hassas kişisel verilerin oluşturduğu görülmektedir.

4.4. CEZA MUHAHAKEMESİ KANUNU KAPSAMINDA KORUMA

CMK'daki hükümler genel olarak değerlendirildiğinde; şüpheli, sanık, mağdur gibi bireylerin kişisel, özel bilgilerini ihtiva eden birtakım hassas verilerin CMK'ya konu edildiğini görmekteyiz. CMK 75 vd. maddelerde kişisel verilerin korunması

987 Parlar/Hatipoğlu, a.g.e., s. 2056.

988 Parlar/Hatipoğlu, a.g.e., s. 2056.

989 5271 sayılı Kanun, R.G.: T. 17/12/2004, S., 25673.

hususları düzenlenmiştir. 75. madde[990], 76. madde[991] ve aynı kanunun 78. maddesi[992] uyarınca elde edilen bulgular 80. madde uyarınca kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz ve mahkûmiyet dışında bir hüküm tesis edilirse derhal imha edilir.[993]

Diğer taraftan, CMK 134 ve 135. maddeleri uyarınca teknik takip, telekomünikasyonun ve iletişimin denetlenmesi vb. hususlar bireylerin genel veya hassas kişisel verilerinin elde edilmesine matuf birtakım düzenlemelerdir. Bu hususta, CMK amaca bağlılık, derhal imha ve yetkili kişi ve kurumların erişimine bu bilgilerin açılması gibi ilkeleri gözettiğini kanunun lafzından anlayabiliriz.

990 "*Bir suça ilişkin delil elde etmek için şüpheli veya sanık üzerinde iç beden muayenesi yapılabilmesine ya da vücuttan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınabilmesine; Cumhuriyet savcısı veya mağdurun istemiyle ya da re'sen hâkim veya mahkeme, gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilebilir. Cumhuriyet savcısının kararı, yirmidört saat içinde hâkim veya mahkemenin onayına sunulur. Hâkim veya mahkeme, yirmidört saat içinde kararını verir. Onaylanmayan kararlar hükümsüz kalır ve elde edilen deliller kullanılamaz*."

991 "*(1) Bir suça ilişkin delil elde etmek amacıyla, mağdurun vücudu üzerinde dış veya iç beden muayenesi yapılabilmesine veya vücudundan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınabilmesine; sağlığını tehlikeye düşürmemek ve cerrahî bir müdahalede bulunmamak koşuluyla; Cumhuriyet savcısının istemiyle ya da re'sen hâkim veya mahkeme, gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilebilir. Cumhuriyet savcısının kararı, yirmidört saat içinde hâkim veya mahkemenin onayına sunulur. Hâkim veya mahkeme, yirmidört saat içinde kararını verir. Onaylanmayan kararlar hükümsüz kalır ve elde edilen deliller kullanılamaz.*

(2) Mağdurun rızasının varlığı halinde, bu işlemlerin yapılabilmesi için birinci fıkra hükmüne göre karar alınmasına gerek yoktur.

(3) Çocuğun soy bağının araştırılmasına gerek duyulması halinde; bu araştırmanın yapılabilmesi için birinci fıkra hükmüne göre karar alınması gerekir."

992 "*(1) 75 ve 76 ncı maddelerde öngörülen işlemlerle elde edilen örnekler üzerinde, soybağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için zorunlu olması hâlinde moleküler genetik incelemeler yapılabilir. Alınan örnekler üzerinde bu amaçlar dışında tespitler yapılmasına yönelik incelemeler yasaktır.*

(2) Birinci fıkra uyarınca yapılabilen incelemeler, bulunan ve kime ait olduğu belli olmayan beden parçaları üzerinde de yapılabilir. Birinci fıkranın ikinci cümlesi, bu hâlde de uygulanır."

993 Boz, a.g.e., s.101-105; Ayözger, a.g.e., s. 101.

4.5. DİĞER KANUNLAR KAPSAMINDA KORUMA

5070 sayılı Elektronik İmza Kanunu[994] 12. m. uyarınca:

"Elektronik sertifika hizmet sağlayıcısı;

a) Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,

b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,

c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz."

hükmünü amirdir.

4982 sayılı Bilgi Edinme Kanunu[995] uyarınca kişisel verilerin koruma altına alındığı görülmektedir. İlgili kanun uyarınca "*bilgi*" kamu kurum ve kuruluşlarının kayıtlarında yer alan her türlü veri olarak tanımlandığından, bu kanunun konusu kapsamında kişisel verilerin olduğuna dair bir şüphe bulunmamaktadır.[996] Adı geçen kanunun 21. maddesinde kişisel bilgilerin aleni bir şekilde paylaşılması yasaklanarak sadece ilgili bireye yazılı bir bildirim yapılarak "*kamu yararı*" bulunması halinde kişisel veri niteliğindeki bilgilerin açıklanabileceği belirtilmiştir. Kanaatimizce bu düzenleme çok genel olmakla beraber insan hakları ihlallerine neden olabilecek ölçüde geniştir.

---

994 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf, Erişim tarihi: 26.11.2019.

995 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4982.pdf, Erişim tarihi, 26.11.2019.

996 Boz, a.g.e., s. 101-105; Ayözger, a.g.e., s. 103.

Yine 4857 sayılı İş Kanunu[997] 75. madde uyarınca işverenin işçisine ilişkin kişisel verileri saklama ve açıklamama mecburiyeti vardır.

213 sayılı Vergi Usul Kanunu[998] madde 5 ve 148, kişisel verilerin toplanmasına ilişkin olarak Vergi Usul Kanunu'nda, vergi yükümlüleri hakkında bilgi toplama ve saklamaya ilişkin özel hükümler bulunmaktadır. 148. maddeye göre; kamu idare ve müesseseleri, mükellefler veya mükelleflerle muamelede bulunan diğer gerçek ve tüzel kişiler, Maliye Bakanlığının veya vergi incelemesi yapmaya yetkili olanların isteyecekleri bilgileri vermeye mecbur olduğuna ilişkin hükme ilgili maddelerde yer verilmiştir.

5490 sayılı Nüfus Hizmetleri Kanunu madde 1, kanunun amacının *"Kişinin doğumundan ölümüne kadar kişisel ve medeni durumuna, uyrukluğuna ve bunlarda meydana gelebilecek değişikliklere ait doğal ve hukuki olayların belirlenip saptanması, bu amaçla düzenlenmiş kütüklere yazılması, elektronik ortamda ulusal adres veri tabanının oluşturulması, nüfus kayıtları ile adres bilgilerinin ilişkilendirilmesini sağlamak"* şeklindeki ifadeye yer verilmiştir.[999]

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 9. Maddesi kişisel verilere ilişkin yapılan hak ihlalleri konusunda tecavüzlerin önlenmesi noktasında olumlu bir katkı sunmaktadır. Adı geçen Kanunun 9. maddesinin 1. fıkrasına göre "*İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine*

997 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4857.pdf, Erişim tarihi:26.11.2019.

998 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.4.213.pdf, Erişim tarihi: 26.11.2019.

999 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5490.pdf, Erişim tarihi, 26.11.2019.

başvurarak içeriğe erişimin engellenmesini de isteyebilir."[1000] Yine aynı kanunun 9/A maddesinde ise "*İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir*" hükümlerine yer verilmiştir.

9.6.2004 tarihli ve 5187 sayılı Basın Kanunu'nun[1001] 14. maddesinde düzeltme ve cevap düzenlenmiştir. Söz konusu madde "*Süreli yayınlarda kişilerin şeref ve haysiyetini ihlâl edici veya kişilerle ilgili gerçeğe aykırı yayım yapılması halinde, bundan zarar gören kişinin yayım tarihinden itibaren iki ay içinde göndereceği suç unsuru içermeyen, üçüncü kişilerin hukuken korunan menfaatlerine aykırı olmayan düzeltme ve cevap yazısını; sorumlu müdür hiçbir düzeltme ve ekleme yapmaksızın, günlük süreli yayınlarda yazıyı aldığı tarihten itibaren en geç üç gün içinde, diğer süreli yayınlarda yazıyı aldığı tarihten itibaren üç günden sonraki ilk nüshada, ilgili yayının yer aldığı sayfa ve sütunlarda, aynı puntolarla ve aynı şekilde yayımlamak zorundadır.*" şeklinde hüküm altına alınmıştır.

5352 sayılı Adli Sicil Kanunu[1002], kesinleşmiş ceza ve güvenlik tedbirlerine mahkûmiyete ilişkin bilgilerin otomatik işleme tâbi bir sistem kullanılarak toplanmasına, sınıflandırılmasına, değerlendirilmesine, muhafaza edilmesine ve gerektiğinde en seri ve sağlıklı biçimde ilgililere bildirilmesine dair usul ve esasları belirlemek amacıyla 25/05/2005 tarihinde kabul edilerek yasalaşmıştır. Kanunun 4. maddesinde kişiler hakkında verilen hükümlerin adlî sicile kaydedileceği hükme bağlanmıştır. Yine 9. maddesinde getirilen düzenleme ile ise adlî sicildeki bilgilerin şu durumların varlığı halinde silineceği düzenlenmiştir:

1. Cezanın veya güvenlik tedbirinin infazının tamamlanması,

1000 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf, Erişim tarihi, 26.11.2019.

1001 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5187.pdf, Erişim tarihi, 26.11.2019.

1002 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5352.pdf, Erişim tarihi, 26.11.2019.

2. Ceza mahkûmiyetini tüm sonuçlarıyla ortadan kaldıran şikâyetten vazgeçme veya etkin pişmanlık hallerinin varlığı,
3. Ceza zamanaşımının dolması,
4. Genel af,
5. İlgilinin ölümü.

4.4.2013 tarihli ve 6458 sayılı Yabancılar ve Uluslararası Koruma Kanunu'nun[1003] 99. maddesinde "*Yabancılara, başvuru ve uluslararası koruma statüsü sahiplerine ait kişisel veriler, Genel Müdürlükçe veya valiliklerce ilgili mevzuata ve taraf olunan uluslararası anlaşmalara uygun olarak alınır, korunur, saklanır ve kullanılır.*" hükmüne yer verilerek yabancılara ve uluslararası koruma altındaki kişilere ilişkin kişisel verilerin bilgilerinin işlenmesinde göz önünde bulundurulacak esaslar düzenlenmiştir.

13.10.1983 tarihli ve 2918 sayılı Karayolları Trafik Kanunu'nun[1004] 5. maddesinde İçişleri Bakanlığının görevleri arasında "*Ülke çapında taşıtların ve sürücülerin sicillerini tutmak, bunlara ilişkin teknik ve hukuki değişiklikleri işlemek, işlettirmek, istatistiksel bilgileri toplamak ve değerlendirmek" ve " trafik kazalarının oluş nedenleri ile ilgili tüm unsurları kapsayan istatistik verileri ve bilgilerini toplamak, değerlendirmek, sonuçlarına göre gereken önlemlerin alınmasını sağlamak ve ilgili kuruluşlara teklifte bulunmak*" gibi faaliyetlere yer verilerek, İçişleri Bakanlığına bu görevleri yerine getirirken veri işleme faaliyetleri yürütmesine izin verilmiştir.

Spor alanları ile bunların çevresinde gerek müsabaka öncesinde gerek müsabaka esnasında veya gerekse müsabaka sonrasında taraftarların sürekli veya geçici olarak gruplar halinde bulundukları yerlerde yahut müsabakanın yapılacağı yere gidiş ve geliş güzergâhlarında gerçekleşecek şiddet ve düzensizliğin önlenmesini amaçlayan 31.3.2011 tarihli ve 6222 sayılı Sporda Şiddet ve Düzensizliğin

---

1003 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6458.pdf, Erişim tarihi, 26.11.2019.

1004 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2918.pdf, Erişim tarihi, 26.11.2019.

Önlenmesine Dair Kanun'da[1005] kişisel verilerin işlenmesi ile ilgili bazı düzenlemelere yer verilmiştir. İlgili Kanunun 5. maddesinin 4. fıkrasına göre, "*..bilet satın almak isteyen kişilerle ilgili olarak, üzerinde adı, soyadı, Türkiye Cumhuriyeti kimlik numarası ve fotoğrafı olan bir elektronik kart oluşturulur. Kişinin yabancı olması halinde kart üzerinde Türkiye Cumhuriyeti kimlik numarası yerine uyruğu olduğu devletin adı ile Türkiye'ye giriş yaptığı pasaportun seri numarası kaydedilir. Bilet satışları kişilere özgü elektronik kart üzerinden yapılabilir…*" hükmüne yer verilerek kişisel verilerden bahsedilmiştir.

Resmî istatistiklerin üretimine ve organizasyonuna ilişkin temel ilkeleri ve standartları belirleyen; ülkenin ihtiyaç duyduğu alanlarda veri ve bilgilerin derlenmesini, değerlendirilmesini, gerekli istatistiklerin üretilmesini, yayımlanmasını, dağıtımını sağlayan Türkiye İstatistik Kurumu'nun kurulmasına ilişkin 10/11/2005 tarihli ve 5429 sayılı Türkiye İstatistik Kanunu'nda[1006] kişisel verilere dair önemli düzenlemelere yer verilmiştir.

Buna göre kanunun 14. maddesinde "*Kişisel veriler, istatistikî birimlerin doğrudan veya dolaylı olarak tanınmasına yol açacak bölümleri gizlendikten sonra, münferit birimlere atıfta bulunmayan bilimsel amaçlı araştırmalarda kullanılması kaydı ve Başkanlığın yazılı izniyle verilebilir. Kişisel verileri kullanma hakkı elde edenler, bu verileri üçüncü şahıslara veremezler.*" hükmü ile kişisel verilerin yalnızca bilimsel amaçlarla kullanılabileceği ve kesinlikle 3. kişilere verilemeyeceği düzenlenmiştir. Aynı kanunun 53. maddesinde ise kanunda belirtilen kişisel verilere ilişkin yasaklara aykırı hareket eden kamu görevlilerinin 5237 sayılı Türk Ceza Kanunu'nun 258. maddesine göre cezalandırılacağı ifade edilmiştir.

1005 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6222.pdf, Erişim tarihi, 26.11.2019.

1006 Kanunun tam metni için bkz. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5429.pdf, Erişim tarihi, 26.11.2019.

5.12.1951 tarihinde kabul edilen ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun[1007] 4. maddesinde "*güzel sanat eserleri, estetik değere sahip olan; yağlı ve suluboya tablolar, her türlü resimler, desenler, pasteller, gravürler, güzel yazılar ve tezhipler, kazıma, oyma, kakma veya benzeri usullerle maden, taş, ağaç veya diğer maddelerle çizilen veya tespit edilen eserler, kaligrafi, serigrafi*" gibi eserlerden bahsedilerek kişisel veriler korunmuştur.

19.10.2005 tarihli ve 5411 sayılı Bankacılık Kanunu'nun[1008] 73. maddesinde sırların saklanması konusunda getirilen düzenleme ile kurum personelinin görevleri sırasında öğrenmiş oldukları bankalara ve bunların bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıkları ve müşterilerine ait sırların, yetkili olan kişiler haricinde başka birisine açıklanamayacağı ve başkalarının yararına kullanılamayacağı ve bu yükümlülüğün görev bittikten sonra da devam ettiği ifade edilmiştir.

1512 sayılı Noterlik Kanunu'nun[1009] 54. maddesinde ise gerek noterin gerekse noterlik katiplerinin, görevleri esnasında öğrenmiş oldukları sırları, yasalarda belirtilen durumlar haricinde açıklayamayacağı düzenlenmiştir.

Bir diğer önemli kanuni koruma mekanizması ise Elektronik Haberleşme Kanunu[1010] olarak karşımıza çıkmaktadır. Adı geçen kanunun 12. maddesinin d bendi uyarınca *"Kişisel veri ve gizliliğin korunması*" yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketlilerin görevleri arasında saymıştır. Burada dikkat çeken önemli husus AYM'nin de önüne denetim için gelen 51. madde olmuştur. Bu maddede *"Bilgi Teknolojileri ve İletişim Kurumu elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye*

1007 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.3.5846.pdf, Erişim tarihi, 26.11.2019.

1008 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5411.pdf, Erişim tarihi, 26.11.2019.

1009 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.1512.pdf, Erişim tarihi, 26.11.2019.

1010 Kanunun tam metni için bkz. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf, Erişim tarihi, 26.11.2019.

yetkilidir." hükmü AYM'nin kararı[1011] ile 1982 Anayasasının 20. maddesi uyarınca böyle bir düzenlemenin ancak kanun ile yapılabileceğinden bahisle bu hüküm iptal edilmiştir.

Yine 6563 sayılı ETDK'nın 5. ve 6.m.'si gereği kişisel bilgilerin aktarılması ve işlenmesi faaliyetlerinin zımni rıza ile yapılabileceği görülmektedir.[1012]

Kişisel verilerin korunmasına ilişkin mevzuat çok geniş olmakla beraber dağınık ve parçalı bir görünüm sergilemektedir. Ancak 2010 yılında kişisel verilerin korunması hakkının anayasal bir hüküm haline gelmesi bunun yanında 2016 yılında KVKK'nın kabul edilmesi ile bu hakka ilişkin sağlanan korumada mevzuat dağınıklığının bir nebze olsun giderildiği ve derli toplu bir koruma alanı bireylere sağlanarak hukuki öngörülebilirliğin artırıldığı müşahede edilmektedir.

TABLO 2: Kişisel Veriler ile ilgili maddeler bulunan kanunlar.

S.NO	MEVZUAT ADI	MADDESİ
1	Türk Ceza Kanunu (TCK)	132-140
2	Ceza Muhakemesi Kanunu (CMK)	75, 80, 134-138, 140
3	Elektronik Haberleşme Kanunu	51,52
4	Elektronik İmza Kanunu	12
5	Elektronik Ticaretin Düzenlenmesi Hakkında Kanun	5, 6
6	Bankacılık Kanunu	73
7	Banka Kartları ve Kredi Kartları Kanunu	23
8	Türk Medeni Kanunu	23, 24 ve 25.

1011 AYM Esas 2013/122, Karar 2014/74, T. 09.04.2014, R.G. 29072.

1012 https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6563.pdf, Erişim Tarihi, 29.05.2019

9	Bilgi Edinme Kanunu	19-22
10	Fikir ve Sanat Eserleri Kanunu	19,70, 83-86
11	İş Kanunu	75
12	İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun	9
13	Adli Sicil Kanunu	11
14	Türk Medeni Kanunu	23, 24, 25
15	Türk Ticaret Kanunu	56, 58
16	Türk Borçlar Kanunu	49, 53, 54 ve 56
17	Noterlik Kanunu	54
18	Karayolları Trafik Kanunu	5
19	Sporda Şiddet ve Düzensizliğin Önlenmesine Dair Kanun	5
20	İstatistik Kanunu	14, 53
21	Yabancılar ve Uluslararası Koruma Kanunu	99
22	Vergi Usul Kanunu	5, 148

SONUÇ

Modern dünyada teknoloji ve bilişim alanındaki gelişmelerle birlikte en güncel konulardan birisi haline gelen bilginin-verinin korunması *-özellikle de kişisel verilerin korunması-* konusu olmuştur. Teknolojinin günümüzdeki boyuta evrilmesi ve gelişmesi, kişisel verilerin güvenliğine ilişkin kaygıların artmasına neden olmakla beraber bu verileri koruma usul ve esaslarının hukuk gündemine taşınmasında ana etkenlerden biri olmuştur. Diğer taraftan temel bir hak olan kişisel verilerin korunması hakkı sadece teknolojik gelişmelere paralel olarak uluslararası hukuka, hukukumuza, anayasalarımıza eklemlenmiş bir hak, konu değildir. İlk anayasacılık hareketlerinin başlaması ile birlikte kişisel verilerin koruması hususu terim olarak karşımıza çıkmasa da kişilere ait olan bilgilerin işlenmesi faaliyetini yürüten *–bu bilgileri işleyen kamu gücü olsun veya olmasın-* otoritelerin ne şekilde sınırlanabileceği ve kişisel verilerin korunması hakkı dahil bu hakla ilişkili diğer temel haklara ne ölçüde otoriterler tarafından müdahale edilebileceği her zaman anayasa hukukunun gündeminde olmuştur. Bu bağlamda, esasen, kişisel verilerin korunması yeni gelişmekte olan herhangi bir hak olarak algılansa dahi kişisel verilerin ilişkili olduğu diğer haklar ile çalışmamızda gösterdiğimiz üzere hukukun pek çok disiplini ile iç içe geçmiş olan yapısı göz önüne alındığında, kişisel verilerin korunması hakkı ve hukuku dendiğinde bir hakkın ötesinde, devletleri, kamu gücünü etkileyen bir hukuki disiplinden söz edildiği görülmektedir.

Günümüz dünyasında, bireye ait sağlık alanından tutun kamusal alandaki CCTV görüntüsüne kadar pek çok resim, görüntü, tahlil sonucu, yargılama neticesi verilen hüküm, alışveriş alışkanlıkları gibi kişisel veriler rahatlıkla depo edilebilmekte ve gerektiğinde değişik parametreler kullanılmak suretiyle analiz edilip anlamlı çıktılar elde edilebilmektedir. Bu analizi yaparken yapay zekâ kullanılmak suretiyle insan müdahalesine dahi gerek duyulmamaktadır. Yine bireylerin, sanal dünyada *-sosyal medya, internet arama motorları üzerinde yapılan aramalar dikkate alındığında-* sanal kimlikleri üzerinden kişilik çalışmaları yapılarak kamusal ve özel alanda bireye ilişkin *"profilleme"* yani o kişinin yakından tanınması, alışkanlıkları ve bakış açısına ilişkin kanaat edinilmesi çalışmaları yapılabildiği bilinmektedir. Böylelikle bir kişinin günlük rutini, alışveriş alışkanlıkları hatta cinsel hayatı bile

başkalarınca *-kamu ve özel otoriteler-* yapılacak bir tespite konu olabilmektedir. Dolayısıyla teknolojinin bu denli gelişmesi ile birey faaliyetleri ve bireye ilişkin veriler kolaylıkla elde edilip işlenmeye başlamıştır. Geniş bir anlatımla, teknolojinin hızlı bir şekilde gelişmesi ile insanın manevi şahsiyetine yönelik tehditler artmış bu artışın bir soncu olarak kişileri bu tehditlere karşı en üst düzeyde hukuki olarak korumanın yolları aranmıştır.[1013]

Teknolojik gelişmelere paralel şekilde artış gösteren, gerçek kişilere ilişkin veri işleme faaliyetleri karşısında, kişisel verilerinin kolayca elde edilebilmesi, bu kişisel verilerin yine hiçbir sınırlama olmadan toplanması, kullanılması ve başka kişilere aktarılması ihtimallerine binaen bireyin korunması devlet, kamu sektörü ve özel sektör tarafından amaçlanmıştır.[1014] Zira teknolojik gelişmelerin getirdiği imkânlar aynı zamanda belli riskleri de beraberinde getirmektedir. Bu baş döndürücü teknolojik gelişmenin ve bu gelişmeden kaynaklı kargaşa ortamının bireye ciddi tehlike oluşturduğu su götürmez bir gerçek olarak karşımıza çıkmaktadır. Devletler ve kurumsal özel teşebbüsler bu teknolojik imkânlardan yararlanarak bireylere yönelik her türlü veriyi kolaylıkla elde edebilir hale gelmiş, tabiri caizse terazinin dengesi kamu ve özel sektör lehine bozulmuştur. Bireyler lehine bu dengenin tekrar kurulması ve bireyin ön plana çıkarılarak tekrar hak temelli gücü eline alabilmesi gerekmektedir. Zaten kişisel verilerin korunması hukukunun, bu gelişme ve düşüncelerin ürünü olduğunu söylemek yanlış olmayacaktır.

Öte yandan teknolojik gelişmenin durdurulması imkânsız olması hasebiyle kişinin kendisini maddi manevi geliştirebileceği ve kendisine ait olan şeyler üzerindeki hak ve yetkilerini açıkça belirlendiği bir sisteme duyulan ihtiyaç gün geçtikçe kendisini hissettirecektir. Teknoloji üretimi ve bilgi kullanımı ile kişisel verilerin korunması hukuku arasında hassas ve bireyin özerkliği lehine denge kurulmalıdır. Bu denge kurulurken kişisel veriler meselesinin çok boyutlu olduğu göz önünde bulundurularak bu hassas konu; siyasi, ekonomik, sosyal ve hukuki yönden ele alınmalıdır. Hukuk içerisinde ise başta anayasa ve idare hukuku olmak üzere ticaret

1013 Şimşek, a.g.e., s. 115.

1014 Şimşek, a.g.e, s. 112.

hukuku, ceza hukuku, medeni hukuk ve tabi ki insan hakları hukuku ile yakından ilişkili bir alan olduğu gözden kaçırılmaması gereken bir durumdur. Bu bakımdan kişilerin özel hayatının gizliliğinin korunması; sosyolojik olarak mahremiyetin korunmasını, hukuken ise kişisel verilerin korunmasını zorunlu hale getirmiştir. İnsanların rahat ve özgür bir hareket alanına sahip olması yanında, kendi bireysel tercihleri doğrultusunda demokratik toplum hayatının gereklerini yerine getirebilmeleri büyük önem taşımaktadır. Bu nedenlerle artık kişisel verilerin korunması kanun bağlamında olduğu kadar hatta ziyadesiyle anayasa düzeyinde koruma altına alınacak hususlardan birisi olmuştur.

İşte tam bu noktada, anayasa ve insan hakları bağlamında, "insan onuru", "bireyin özerkliği", "kişisel verileri üzerinde tasarruf ve verilerinin geleceğini belirleme" gibi birtakım haklar ve hukuki müesseseler temelinde kişisel verilerin ele alınarak hukuki zemine oturtulması gerektiği kanaati günden güne artan bir şekilde kendisini hukuk aleminde göstermiştir. Bu minvalde tarihsel süreçte 1970'li yıllardan itibaren kişisel verilerin korunması ile ilgili tartışmalar uluslararası platformda kendini göstermeye başlamıştır. Bu konuyu uzun yıllar tartışan devletler gerek anayasal gerekse yasal düzenlemelerle kişisel verileri koruma hukuku alanında önemli mesafe kaydetmişlerdir. Bu tartışmalarda öncelikli olarak devletlerin anayasal düzeyde sınırlanması hedef alınmış iken, zaman içerisinde kişisel verilere yönelik yapılan düzenlemelerin özel hukuk kişilerini kapsayacak şekilde genişlediği görülmüştür.

Tüm bu gelişmelere bir bütün olarak değerlendirildiğinde görüyoruz ki; kişisel verilerin korunması hakkı ile ilgili ilk somut adım, 1980 yılında İktisadi İşbirliği ve Kalkınma Teşkilatı tarafından atılmıştır. Kişisel verilerin korunması ile ilgili temel ilkelerin belirlendiği "*OECD Rehber İlkeler*" yayınlanmıştır. Bu düzenlemeyi, üye devletler arasında hukuki uyum sağlanması amacı ile kurulmuş olan Avrupa Konseyi'nin "*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması*"na dair 108 sayılı Avrupa Konseyi Sözleşmesi takip etmiştir. 108 sayılı sözleşmede üye devletler arasında kişisel verilerin korunması konusunda uygulama birliği sağlanmaya çalışılmış ve uluslararası veri akışının standartları belirlenmiştir.

Daha sonra ise Avrupa Birliği kişisel verilerin korunmasına ilişkin yürüttüğü çalışmaların sonucunda, üye ülkelerdeki mevzuat farklılıklarının giderilmesi, çelişkilerin önlenmesi ve kişisel verilerin korunmasında ortak bir standartın sağlanması ve ayrıca birlik içinde kişisel verilerin serbestçe dolaşımının sağlanması amacıyla 95/46/AT sayılı Kişisel Verilerin Korunması Yönergesini kabul ederek yürürlüğe koymuştur. Onun akabinde, onu yürürlükten kaldırarak GDPR'yi yürürlüğe koyarak kişisel verilerin korunması hakkını daha kurumsal bir aşamaya taşımıştır. Ancak bu alanda en yenilikçi ve derli toplu düzenlemeleri ihtiva eden ilk belge olarak yönergeyi görmek yanlış olmayacaktır.

Yukarıda sayılan bütün düzenlemelerin ortak yönüne baktığımızda, kişisel verilerin toplanması ve kayıt altına alınması işlemlerini zorlaştırıcı birtakım tedbirler öngördüğünü, bu tedbirler ile herhangi maddi ve manevi bir zararı oluşmadan önce bireyin kişisel verilerinin korunmasını amaçladığını söylemek yanlış olmayacaktır. Adeta bireyin verisinin zaruri değilse depolanmamasına yönelik adımların atıldığını görüyoruz. Bu bağlamda, son evrede, veri işlemesine hâkim olan temel ilkelerin belirlenmesinden, veri sahibinin rızasına ve veri türlerinden hassas verilerin kaydedilememesine yönelik pek çok birey lehine düzenleme içerdikleri görülmektedir. Görüldüğü üzere, kişisel verilerin korunmasının amacı, en yalın hali ile *"bireyin verisini kaydetme ve onu kullanma aksini yapacaksan rızasını ara ve haber ver"* anlayışı üzerine bina edilmiştir.

Avrupa Birliği'nin 95/46/AT sayılı Yönergesinde kişisel verinin *"Bireylerin Kişisel Verilerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Yönergen*in 2/a maddesinde kişisel veri: *"Bir gerçek kişinin belirli veya belirlenebilir olması, şifre numarasına göre ya da psişik, psikolojik, fiziksel, ekonomik, kültürel veya sosyal benliği ifade eden bir veya birden fazla unsura, aidiyeti aracılığıyla doğrudan veya dolaylı olarak teşhis edilebilmesi anlamına"* geldiği ifade edilmişken, OECD Rehber İlkelerin 1/b maddesinde ise kişisel veri *"belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler"* şeklinde tanımlanmaktadır.

Ulusal mevzuatta ise Kişisel Verilerin Korunması Kanunu'nun 3. Maddesinde *-özellikle GDPR ve Yönergeye paralel olarak-* uluslararası belgelerdeki kişisel veri

tanımının tekrar edildiği görülmekte ve kişisel veri, "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmaktadır. Tüm bu tanımlamalardan kişisel verilerin bilgi, kimliği belirli veya belirlenebilir bir kişi ve bilginin kimliği belirli veya belirlenebilir bir kişiye ait olması şeklinde üç unsurunun olduğu görülmektedir.

Zaman içerisinde bazı kişisel verilerin diğerlerine oranla daha fazla korunması ihtiyacı hissedilmiş ve özleri itibarı ile kişisel veri niteliğinde olmalarına rağmen, daha fazla koruma ihtiyacı duyulan küçük bir kişisel verileri grubu "hassas kişisel veri" olarak adlandırılmış[1015] ve bu veriler daha farklı koruma rejimine tabi tutulmuşlardır.

Uluslararası düzenlemelerde ve iç hukukumuzda kural olarak hassas kişisel verilerin işlenmesi yasaklanmış ancak istisnai hallerde buna izin verilmiştir. Bu istisnalar, ilgilinin rızası, hayati çıkarların korunması, kamuya yararlı özel hukuk kişisi tarafından işlenme, iş hukukundan kaynaklanan yükümlülüklere uyulması, verinin ilgili kişi tarafından kamuya açıklanması, yargılama sebebi ile işleme, cezalara yönelik işleme ve sağlık gerekleridir.

Kişisel verilerin hukuki niteliği de tartışılan konular arasında yer almış ve bu konuda farklı görüşler ileri sürülmüştür. Bu görüşler; insan onuru, bireysel özerklik ve bilgilerin geleceğini belirleme hakkı görüşü, mülkiyet hakkı görüşü, özel hayatın gizliliği görüşü ve fikri mülkiyet hakkı görüşü başlıkları altında toplanabilir.

Kişisel verilerin işlenmesi sırasında dikkate alınması gereken temel ilkeler uluslararası belgeler ve iç hukukumuzdaki düzenlemeler göz önüne alınarak; kişisel verilerin işlenmesinde esasa ilişkin ilkeler, kişisel verilerin hukuka ve dürüstlük kuralına uygun işlenmesi, ilgilinin rızasının alınması ilkesi, belli bir amacın bulunması ilkesi, amaca bağlılık ilkesi, orantılılık ve gereklilik ilkesi, verilerin doğruluğu ve güncelliği ilkesi olarak gruplandırılabilir.

Kişisel verilerin işlenmesinde usule ilişkin ilkeler ise, veri güvenliği ilkesi, ilgili kişilerin bilgilendirilmesi ilkesi, bilgi edinme, düzeltme, kaldırma, sildirme,

---

[1015] Kaya, "Hassas veriler", s. 318.

engelleme ve itiraz hakkının garanti edilmesi ilkesi, işlem aleniyeti ilkesi, işlemin güvenliği ve gizliliği ilkesi, ön denetim ve zararın tazmin edilmesi ilkesidir.

Kişisel verilerin korunması hakkının sınırlarının belirlenmesi bu haktan tam olarak yararlanılması ve bu hakkın güvence altına alınabilmesi açısından önemlidir. Anayasalarda kapsamlı olarak tanınan hak ve özgürlüklerin en iyi biçimde uyumları sağlanırken, kötüye kullanılmalarını engellemek amacıyla, kendi içlerinde *"uzlaştırılmaları"* gerektiği gibi *"sınırlandırılmaları"* da bir zorunluluktur. Başka bir deyişle, temel hak ve özgürlüklere bir sınır getirilmesi, bir açıdan onların niteliklerinin gereği olduğu gibi, hak ve özgürlüklerin kötüye kullanılmaları da bir sınırlama doğurmaktadır. Zira bir temel hak sahibinin, o temel hak ve özgürlüklerini kontrolsüz veya orantısız olarak kullanması ile kamu yararı veya başka temel hak sahiplerinin haklarının çatışması söz konusu olabilir. Kötüye kullanılmalarının önüne geçilmesi ve herkesin bu hak ve özgürlüklerden yararlanabilmesi amacıyla özgürlükleri kullanma belli sınırlamalara tabi tutulmuştur.

Kişisel verilerin korunması hakkına sınırlamalar getirilirken göz önünde bulundurulması gereken ilkeler vardır, aksi durumda bu hakka yapılan müdahaleler hakkın kullanılmasını imkânsızlaştırabileceği gibi bu hakkı anlamsızlaştırabilir. Bu ilkeler, kamu düzeni ilkesi, demokratik toplum düzeni ilkesi, ölçülülük ilkesi, sınırlamanın yasa ile yapılması ilkesi ve hakkın özüne dokunulmaması ilkesidir.

Bazı hak ve özgürlükler ile kişisel verilerin korunması hakkı arasında hem birbirlerini sınırlandıran hem de korunmalarına yardımcı olmak gibi girintili bir ilişki vardır. Bu kapsamda en dikkat çeken kavramlardan birisi insan onurudur. İnsan haklarının temelinde insan onuru bulunduğu gibi, kişisel verilerin korunması hakkının temelinde de insan onuru bulunmaktadır. Hukuka aykırı olarak kişisel verilerin işlenmesi, veri ilgilisinin kendi geleceğini belirleyebilmesi hakkının ve insan olarak sahip olduğu değerlerin ihlal edilmesi sonucunu doğuracağı için, kişisel verilerin hukuka aykırı olarak işlenmesinin önüne insan onurunun korunması ile geçilebilir.

Kişisel verilerin korunması hakkı yönünden din, vicdan ve inanç özgürlüğü değerlendirilecek olursa, din veya inanca dair olan verilerin belli veya belirlenebilir bir kişiyle irtibatlandırılmaları durumunda bu veriler kişisel veri haline dönüşürler.

Bireyin din veya inancına dair veriler özel olarak korunmaktadır. Çünkü bu veriler verilerin korunması hukukuna göre hassas nitelikli veriler olarak kabul edilmektedir. Bu nedenle din, vicdan ve inanç özgürlüğü ile kişisel verilerin korunması hakkının birbirini destekler nitelikte hak ve özgürlükler olduğu çıkarımı yapılabilir.

Kişisel verilerin korunması hakkı ile özel hayatın gizliliği hakkı arasındaki ilişki oldukça yakındır. Özel hayatın gizliliği hakkı ile kişisel verilerin korunması hakkı arasında belirgin farklılıklar var ise de her iki hakkın temel çıkış noktalarının örtüştüğü açıktır. Kişisel verilerin korunması hakkının, özel yaşamın gizliliği hakkının iyi bir şekilde uyarlanmış şekli olarak görüldüğündendir ki, pek çok ülkede, özel hayatın gizliliği hakkının tanımlanması esnasında kişisel verilerin korunması ile ilişki kurularak, *"kişisel verilerin korunması hakkı"*nın, *"özel hayatın gizliliği hakkı"*nın kendine has nitelikleri bulunan bir çeşidi olduğu ve bu haklar arasında yakın bir ilişki olduğu kabul edilmektedir.

Bir diğer vurgulanması gereken nokta ise, bilgi edinme hakkı ile kişisel verilerin korunması hakkı arasında bazı durumlarda birbirini sınırlayan, bazı durumlarda ise birbirinin içine geçmiş olan konuları düzenleme şeklinde farklı bir ilişki olduğudur. Nitekim, kişisel veriler bir yönüyle bilgi edinme hakkı çerçevesinde erişimi talep edilebilecek bir bilgi kategorisini oluşturmakta iken; bir başka yönüyle ise kişisel verilerin korunması, bilgi edinme hakkını sınırlandırmaktadır.

Kişisel verilerin ilişki içinde olduğu bir diğer alan ise, haberleşme hürriyeti ve özel haberleşmenin gizliliği hakkıdır. Özel haberleşmenin gizliliği ile, haberleşmelerin içeriğini ve muhatabını serbest olarak belirleme özgürlüğü desteklenmekte, haberleşmenin içeriği üçüncü kişilerin müdahalesinden korumakta ve bu yolla özel haberleşmenin gizliliği hakkı ile kişisel verilerin korunması hakkına hizmet edilmektedir.

Düşünce özgürlüğü ile kişisel verilerin korunması hakkı da zaman zaman çatışma zaman zaman birbirine yardımcı olma şeklinde bir ilişki içindedirler. Ancak gerek AİHS'te kişisel verilerin korunması bakımından özel bu hakka münhasır bir düzenleme olmaması bu hakka yönelik sağlanan korumayı zayıflattığı kanaatindeyiz. Dolayısıyla AİHS'e ek bir protokol ile bu hakkın işlenmesi yerinde olacaktır.

Uluslararası platformda kişisel verilerin korunmasına yönelik ilk gelişmeler, özel hayatın gizliliği hakkı kapsamında değerlendirilmiş ve özel hayatın gizliliğine dair yapılan düzenlemelerin kişisel verileri de kapsayacağı düşüncesi benimsenmiştir.

Türk hukukuna geldiğimizde; kişisel verilerin korunması hakkının temeli olarak kabul edilebilecek anayasal hükümler 2010 yılında yapılan Anayasa değişikliğinden önce de ülkemizde vardı. Zira "*Hukuk devleti ilkesi"* (m.2), "*bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı"* (m.17), "*özel hayatın gizliliği hakkı"* (m.20), "*konut dokunulmazlığı"* (m.21), "*haberleşmenin gizliliği"* (m.22), "*dini ve vicdani kanaatleri açıklamaya zorlanamama"* (m.24), "*düşünce ve kanaatleri açıklamaya zorlanamama"* (m.25) gibi hak ve hürriyetleri düzenleyen bu maddeler bunlara örnek olarak verilebilir.[1016]

Genellikle özel hayatın gizliliğinin korunması çerçevesinde ele alınan kişisel verilerin korunması hakkına 1961 ve 1982 Anayasalarında, 12 Eylül 2010 tarihinde yapılan 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun ile ilgili referanduma kadar yer verilmemiştir. Ancak 2010 yılında yapılan referandum sonrasında Anayasa'nın 20. maddesine eklenen 3. fıkra ile kişisel verilerin korunması hakkına anayasal güvence sağlanmıştır.

KVKK'nın kabulünden önceki sürece baktığımızda, Türk hukuk sisteminde kişisel verilerin kullanımı sonrasında ortaya çıkan zararı gidermeye yönelik düzenlemelerin olduğunu görüyoruz. Bu düzenlemelere örnek olarak idareye başvurma hakkı, TCK'da tanımlanan bazı suç tipleri gösterilebilir. Esasen Türkiye AK 108 sayılı sözleşmesine taraf olmasına rağmen ondan 30 yıl sonra kişisel verilerin korunması hakkını anayasasına eklemiş 36 yıl sonra ise kanun çıkarmıştır. KVKK'nın kabulü ile AK ve AB hukukuna daha yakın bir korumanın sağlandığını söylememiz gerekir. Özellikle, KVKK'nın kabulü ile Türkiye'de kişisel verileri işleyenlerin uyması gereken usul ve esasların net bir şekilde belirlenmesinin yanı sıra işlemede gözetilecek ilkelere kanunda yer verilmiştir. Başta temel kanunlar olmak üzere pek

[1016] Kılınç, a.g.m., s.1131.

çok yasal düzenlemeye dağılmış vaziyette olan kişisel verilere ilişkin mevzuatın toparlanması da sağlanmıştır.

Yine 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu ile yapılmıştır. KVKK'daki kişisel verilerin korunması hakkındaki düzenlemeler çalışmamızda yer verdiğimiz uluslararası düzenlemeler ile büyük ölçüde paralellik arz etmektedir. Bu kanunun yürürlüğe girmesi ile tarafı olduğumuz uluslararası anlaşmaların gereği yerine getirildiği gibi, temel insan haklarından olan kişisel verilerin korunması hakkının kapsamı belirlenmiş, sınırları çizilmiş, bu hakkın korunması ile ilgili düzenleme yapılmış ve uygulamada çıkabilecek karışıklıkların önüne geçilmiştir.

Öte yandan kişisel verileri koruma hakkını tetkik eden çalışmamızın neticesinde bazı problemli alanların olduğu göze çarpmaktadır. İlk olarak, AİHS'te kişisel verilerin korunması bakımından bu hakka münhasır bir düzenleme olmaması nedeniyle bu hakka yönelik sağlanan korumanın zayıf kaldığı kanaatindeyiz. Dolayısıyla AİHS'e ek bir protokol ile bu hakkın açık bir şekilde metne dercedilmesi yerinde olacaktır.

İç hukukumuzda kişisel verilerin korunması dair, anayasa hukuku bağlamında, 1982 Anayasasının 20. maddesinde sınırlama ve bu hakka müdahale çeşitlerinin sarih ve tahdidi bir şekilde belirlenmeyerek *-ki bu anayasal hakların sınırlanması rejimine ve 1982 anayasasının sistematiğine aykırı görünmektedir-* kanun ile bu hususların düzenlenmesi gerektiğinin belirtilmesi hakka yönelik anayasal korumayı zayıflatmaktadır. Burada bir anayasa değişikliği ile diğer temel haklarda sağlanan korumayı bu hakta da sağlamayı teminen bir anayasa değişikliği ile bu hususun çözüleceği kanısındayız.

Her ne kadar anayasal bir hak olarak anayasada yer almasına karşın, kişisel verilerin korunmasına ilişkin esas düzenlemelerin yasal düzeyde ele alınmış olduğu görülmektedir. Bu minvalde TCK, CMK, TMK ve İş Kanunu gibi başlıca kanunlarımızın yanı sıra diğer mevzuatımızda dağınık ve yeknesaklıktan uzak bir vaziyette, bu anayasal hakkın korunmasına ilişkin kanuni düzenlemeler mevcuttur. Bu gibi düzenlemelerin tekrar ele alınarak uluslararası anlaşmalar, 1982 Anayasası ve

KVKK'nın lafzına ve özüne uygun olarak sistematik bir şekilde gözden geçirilmesinin faydalı olacağı mütalaa edilebilir.

Bu bağlamda, TCK'nın suç saydığı birtakım eylemlerin aynı zamanda KVKK ile idari para cezası gerektiren kabahatler olarak düzenlendiği görülmektedir. KVKK 17. m.'si ile kişisel verilere ilişkin suçlar bakımından TCK'nin 135 ila 140 hükümlerine atıfta bulunularak kişisel verilerin ceza hukuku bağlamında korunması konusunda doğrudan TCK hükümlerinin uygulanacağı öngörülmüştür. Bununla birlikte, KVKK'nin 22/1-ğ bendi uyarınca Kişisel Verileri Koruma Kurulu'nun KVKK'nın 18. m.'si uyarıca kabahatler karşılığı idari yaptırımlara karar verme yetkisi bulunmaktadır. Nitekim Kurul bu yönde çokça idari yaptırım kararını verdiği bilinmektedir. Ancak Kabahatler Kanunu'nun 15/3. m.'sinde düzenlenen içtima hükmü karşısında tek bir fiil ile aynı anda hem suça, hem de kabahate vücut verilmesi, yani suç ve kabahatlerin içtimaının incelenmesi ihtiyacı ortaya çıkmaktadır. Kanatimizce bu konuda bir yasal düzenlemeye gidilerek bir fiille hem idari yaptırım hem suç oluşuyor ise hem suç soruştuması hem de idari takibat yapılabilecek bir düzenlemenin yürürlüğe sokulması gerekmektedir. Başka bir deyişle, bu durumda herhangi bir uyuşmazlık olması halinde aynı fiil nedeniyle hem idari para cezası hem adli bir yaptırım uygulaması olabilecektir. Bunun ise "non bis in dem" ilkesine aykırı olduğu ileri sürülebilir. Bu alandaki farklı hukuki uygulamaların önüne geçmek maksatlı olarak bir yasal düzenleme yoluna gidilmesinin yararlı olacağını düşünmekteyiz.

Yine 6563 sayılı Elektronik Ticaretin Düzenlenmesi Kanunu ile KVKK'nın bazı hükümleri çelişmektedir. Örneğin, 6563 sayılı kanunun zımni rızayı kabul ettiği görülmektedir. Oysaki gerek anayasa gerekse KVKK'da açıkça belirtildiği üzere kişisel verilerin işlenmesinde veri sahibinin açık rızasının bulunması genel presnsip olarak kabul görmüştür ki uluslararası düzenlemelerde de açık rıza şartı bulunmaktadır. Bu konuda 6563 sayılı kanun KVKK'ya göre özel kanun niteliğinde olsa dahi bu alanda bir yasal düzenleme ile çelişkinin giderilmesinin uygulamadaki karışıklığı önlemesi bakımından fayda sağlayacağı mütaala edilebilir.

Diğer taraftan dünya genelinde oluşan eğilime baktığımızda kişisel verilerin korunması hakkının kapsamı konusunda ülkeler arasında uygulama birliği yok ise de, genel eğilim ve iç hukukumuzdaki uygulama, kişisel verilerin korunmasının kapsamına sadece gerçek kişilerin girdiği yönündedir. Kişisel verilerin korunması hakkının, insan kişiliğini ve insanın özel alanını temel haklar kapsamında koruduğu göz önüne alındığında, tüzel kişilerin verilerin korunması hakkına sahip olmadığı kabul edilebilir. Başka bir anlatımla, kişisel verilerin korunması hukukunda gerçek kişilerin mağdur olabileceğinden bahisle hukuk sistemleri gerçek kişileri koruma eğilimindedir. Tüzel kişilerin ise ticaret ve ceza kanunları çerçevesinde çerçevesinde "ticari itibar" ekseninde koruma sağlandığı görülmektedir. Fakat, modern dünyada, bazı dev tüzel kişiliklerin oluştuğu gözden kaçırılmaması gereken bir gerçekliktir. Bu tüzel kişilikler öyle bir konuma gelmiştir ki, sadece ticari sır kapsamında verileri ve bilgilerinin korunması mümkün görülmemektedir. Zira bu tüzel kişilikler toplum nezdinde takip edilen, açıklamalarına itibar edilen kurumsal yapılar haline gelmişlerdir. Bunlara örnek olarak Apple, Huawei ve bazı büyük savunma sanayi şirketleri verilebilir. Bu gibi, tüzel kişiliklerin kurumsal itibarının olduğu ve bu itibarın korunmasının tüzel kişilerin faaliyetlerinin devamı açısından hayati olduğu malumdur. Tüm bunlar değerlendirildiğinde, bilgi ve teknoloji çağında, tüzel kişilere, özellikle uluslararası firmaların kendisine ait birtakım verilerin, hukuken koruma altına alınması gerekliliğinden bahsedilmesi kaçınılmazdır. Bu hususa ilişkin uluslararası alanda ve ulusal bazda düzenlemelere yer verilmesi ve tüzel kişilere ait verilere ilişkin düzenleme yapılması elzem görünmektedir.

Son olarak, uluslararası alanda, pek çok uluslararası organizasyonun kişisel verilerin korunmasında uygulancak olan usul ve esasları içeren metinleri değişik adlar ile kabul ettiklerini çalışmamızda belirttik. Ancak bu denli güncel ve teknolojik gelişmlere bağlı olarak değişkenlik gösteren dinamik bir alana sahip olan kişisel verilerin korunması hukukunda AB'nin son uygulamaya koyduğu GDPR hariç kapsamlı bir uluslararası metnin ve çalışmanın son yıllarda yapılmadığı müşahede edilmektedir. Dolayısıyla başta BM ve AK olmak üzere insan hakları ile ilgilenen diğer uluslar arası kuruluşlar ile devletlerin kişisel veriler hukukunu düzenlemek ve denetlemek ile görevli kurumlarının çoğulcu bir yapı oluşturacak şekilde bir araya

gelerek kapsamlı bir uluslararası ve hukuki bağlayıcılığı olan metin üzerinde çalışmaları gerekliliği göze çarpmaktadır.

KAYNAKÇA

ALAN, Ercan "Kadıasker Ruznamce Defterlerine Göre XVII. Yüzyılda Rumelide Kaza Teşkilatı ve Kadılar" Güneydoğu Avruupa Araştırmaları Dergisi 2013-1, sayı 23.

ALDANMAZ, Orhan, İnsan Onuru Işığında Kişisel Özerklik ve Yerellik Kavramı, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, Cilt: XIV, Sayı: 1-2, Yıl: 2010.

AKDAĞ, Hale, TCK Kapsamında Kişisel Verilerin Korunması, Yüksek Lisans Tez, Ankara Sosyal Biilimler Enstitüsü, Ankara 2010.

AKGÜL, Aydın, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, İstanbul 2014.

AKGÜL, Aydın, İdari Usul Açısından Ödeme Emrinde Kanun Yolununve Dava Açma Süresinin Gösterilmemesi, Terazi Dergisi, 2008, Yıl: 3, Sayı: 26.

AKGÜL, Aydın, Avrupa İnsan Hakları Mahkemesi Kararlarında Kişisel Verilerin Korunması Hakkı, Terazi Hukuk Dergisi, Cilt: 9, Sayı: 92, Yıl: Nisan 2014.

AKGÜL, Aydın, Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi, Yayınlanmamış Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli 2013.

AKGÜL, Aydın, Kişisel Verilerin Korunmasında Yeni Bir Hak: Unutulma Hakkı ve AB Adalet Divanı'nın Google Kararı, Türkiye Barolar Birliği Dergisi, Yıl: 2015, Cilt: 27. Sayı: 116.

AKİPEK, Jale/AKINTURK, Turgut, Türk Medeni Hukuku (Yeni Medeni Kanun'a Uyarlanmış Başlangıç Hükümleri, Kişiler Hukuku), Cilt: I, 4. Baskı, İstanbul, 2002.

AKILLIOĞLU, Tekin, İnsan Hakları I, Kavram, Kaynaklar ve Koruma Sistemleri, Ankara, 1995.

AKILLIOĞLU, Tekin, Yönetimde Açıklık- Gizlilik ve Bilgi Alma Hakkı, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, Sayı: 3-4, Cilt :46, Yıl: 1991.

AKSOY, Hüseyin Can, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara, Çakmak Yayınları, 2010. (Kişisel Verilerin Korunması olarak anılmıştır.)

AKSOY, Hüseyin Can, "The Right to Personality and Its Different Manifestations As the Core of Personal Data", Ankara Law Rewiev, Yıl: 2008, Cilt: 5, Sayı: 2.

AKYILMAZ, Bahtiyar, İdari Usul İlkeleri Işığında Rekabet Kurulunun Çalışma Usulü, Ankara Barosu Uluslararası Hukuk Kurultayı, Cilt: 2, Ankara, 2002.

ANI, Nevzat Ali, Kişisel Verilerin İşlenmesi ve Açık Rıza, Yüksek Lisans Tezi, İstanbul Üniveristesi Sosyal Bilimler Enstitüsü, İstanbul 2018.

ARSLAN, Çetin, Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması, Kazancı Hakemli Hukuk Dergisi, Yıl: Mart-Nisan 2011.

ARSLAN, Kahan Onur, İnsan Onuru Kavramı ve Koruma Tedbirleri Bağlamında Temel Bir İlke Olarak İnsan Onurunun Korunması, Türkiye Barolar Birliği Dergisi, Yıl: 2015.

ARSLAN, Zühtü, Avrupa İnsan Hakları Sözleşmesinde Din Özgürlüğü, Liberal Düşünce Topluluğu, Ankara 2005.

ARTUK, M. Emin/Ahmet Gökcen/ YENİDÜNYA, Ahmet Caner, Türk Ceza Hukuku Genel Hükümler, 7. Baskı, Ankara 2013.

ATAK, Songül, Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri, Bahçeşehir Üniversitesi Hukuk Fakültesi, Kazancı Hakemli Hukuk Dergisi, Yıl: 2009, Sayı: 59–60.

ATAY, Ender Ethem, "Hukuk Başlangıcı", 1. Baskı, Ankara 2013.

ATAK Songül, Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, Türkiye Barolar Birliği Dergisi, Sayı: 87, Yıl: 2010.

ATEŞ, Mustafa, Fikir ve Sanat Eserleri Üzerindeki Hakların Kapsamı ve Sınırlandırılması, Ankara, 2003.

AYÖZGER, Ayşe Çiğdem, Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması, Yayımlanmamış Doktora Tezi, İstanbul 2016.

AVŞAR, B. Zakir, Gürsel Öngören, Radyo ve Televizyon Hukuku, RTÜK Yayın No: 3, Ankara, 2003.

AYDIN, Sedat Erdem, AİHM İçtihatları Kapsamında Kişisel Verilerin Kaydedilmesi Suçu, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2014.

BAŞALP, Nilgün, Kişisel Verilerin Korunması ve Saklanması, Ankara, 2004.

BAŞALP, Nilgün, Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri, Marmara Üniversitesi Hukuk Fakültesi, Cilt: 21, Sayı: 1.

BAŞBUĞ, Aydın, Hekimin Yükümlülükleri ve Hukuki Sorumluluğu, Kuzey Kıbrıs Türk Cumhuriyeti, Lefke Avrupa Üniversitesi, 17-18 Mayıs 2010, II Sağlık Hukuku Sempozyumu.

BAYKAL, Sanem GÖÇMEN, İlke Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi, Prof. Dr. Erdal Onar'a Armağan, Cilt: II Ankara 2013.

BELLE, Gerald Van / RUITER, Leslie, Data and Law: Beyond the Sweat of the Brow: Who Owns Published Data? And What Is Data?, Journal of Significance, April, 2014.

BENNETT Colin J. / RAAB Charles D., The Governance of Privacy Policy Instruments in Global Perspective, Ashgate Publishing Company, England, 2004.

BERGKAMP Lucas, EU Data Protection Policy, The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Dirven Economy, Computer Law and Security Report, Sayı: 18, Yıl: 2002.

BEYDOĞAN, T. Ayhan, Türk Hukukunda Siyasi İfade Hürriyeti, Liberal Düşünce Topluluğu Yayınları, Ankara 2003.

BEYLEVELD Deryck/ David TOWNED/ Segolene ROUİLLE- Mirza and Jessica Wright, The Data Protection Directive and Medical Research Across Europe. Burlington: Ashgate Publishing Limited, Yıl: 2004.

BİLGİN, Ahmet Burak, AİHS ve Diğer Uluslararası Anlaşmaların İç Hukuktaki Yeri Bağlamında 2004 Değişikliğinin Beraberinde Getirdiği Sorunlar ve Bazı Çözüm Önerileri, MÜHF - HAD, Cilt: 22, Sayı: 1.

BLOUSTEIN, Edward J., Privacy as an Aspect of Human Dignity: An Answerto Dean Prosser, 39 N.Y.U. L. Rev. 962, Yıl: 1964.

BUCHER, Andreas, Natürliche Personen und Persönlichtkeitschutz, Basel 1986.

BULUT, Nihat, Eski Yunan'dan Aydınlanma Çağı'na İnsan Onuru Kavramının Gelişimine Bir Bakış, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, Cilt: XII, Sayı: 3-4, Yıl: 2008.

BOZ, Ahmet, Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri, Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi, Güvenlik Bilimleri Enstitüsü, Ankara 2014.

CAMMİLLERİ Anne, Clarie LEVALLOİS, Data Protection in the European Union. Bruxelles: Bruylant, 2007.

CAN, Azer, Bilgi Edinme Hakkı, Ankara 2010.

CAREY, Peter, Data Protection, A Practical Guide to UK and EU Law, Oxford University Press, 2004.

CAREY Peter, Data Protection: A Practical Guide to UK and EU Law, Third Edition, Oxford University Pres, Oxford 2009.

CENTEL, Centel/ZAFER, Hamide/YENERER ÇAKMUT Özlem, Türk Ceza Hukukuna Giriş, İstanbul, 2005.

CLARKE, Roger, Internet Privacy Concerns Confirm the Case for Intervention, (Internet), Comminication of the ACM, Cilt: 42, Sayı: 2, Yıl: 1999.

ÇAKAR, Ayşen Seymen, Hukuki Bir Kavram Olarak İnsan Onuru, Umut Vakfı Araştırma Merkezi, 3. Hukukun Gençleri Sempozyumu, Antalya, 11-12 Ekim 2013.

CİVELEK, Dilek Yüksel, Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, Yayınlanmamış Uzmanlık Tezi, Ankara 2011, Devlet Planlama Teşkilatı.

CoE, Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personaldata, regarding supervisory authorities and transborder data flows, CETS No. 181, 2001.

ÇAVUŞOĞLU, Naz, Avrupa İnsan Hakları Mahkemesi Kararlarının Uygulanması: Türkiye Kararları, İstanbul 2003.

ÇAYIR, Murat, "Kültepe'den Yerli Bir Tüccara Ait Beş Belge" Archıvum Anatolıcum 7/1, 2004

ÇOKMUTLU, Metin, Türk Ceza Hukukunda Kişisel Verilerin Korunması (Doktora Tezi), Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü, Kocaeli, 2014.

ÇOLAK, N. İlker, Kitle İletişim Hukuku, 2. Baskı, İstanbul, 2012.

CUNNINGHAM, McKay, Complying with International Data Protection Law", 84 University of Cincinnati Law Review, Sayı:421, Yıl:2016.

DAĞ, Güray, Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması, Yayınlanmamış Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2011.

DETERMANN, Lothar/SPRAGUE Robert, Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States, Berkeley Technology Law Journal, Sayı: 26, Yıl: 2011.

DİNKÇİ, Fatih, Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye Örneği, Yayımlanmamış Yüksek Lisans Tezi, Çanakkale 2014.

DÖNER, Ayhan, Şeffaf Devlette Bilgi Edinme Hakkı ve Sınırları, İstanbul 2010.

DÖNER, Ayhan, Kişisel Verilerin Korunması Hakkında Federal Kanun, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, Yıl: 2006, Cilt: X, Sayı: 1 – 2.

Duran, Lütfi, İdari Usulün İlkeleri ve Kapsadığı Konular, İdari Usul Kanunu Hazırlığı Uluslararası Sempozyumu, Bildiriler, Ankara 17-18 Ocak 1998.

Electronic Privacy Information Center, Privacy&Human Rights: An International Survey of Privacy Laws and Developments Washington, D.C. 2004.

ERDEM, M. Ruhan, Yeni TCK'da Faillik ve Suç Ortaklığı, Hukuki Perspektifler Dergisi, Sayı: 5,Yıl: Aralık 2005.

EROĞLU, Cem, Anatüzeye Giriş, (Anayasa Hukukuna Giriş), Ankara 2005.

ERSOY, Uğur, Bir İnsan Hakları Kavramı Olarak "Kişisel Verilerin Korunması", Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2009.

EVANS, A.C., European Data Protection Law, American Journal of Comparetive Law, Cilt: 29, Yıl:1981.

GEDİK, Ömer, Türk Yargı Kararları Çerçevesinde Kitle İletişim Özgürlüğü, Ankara 2008.

GEMALMAZ, Mehmet Semih, Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş, Ankara 2003.

GEMALMAZ, M. Semih, Devlet, Birey ve Özgürlük, 2. Baskı, İstanbul 2012.

GENÇCAN, Omer Uğur, Türk Medeni Kanunu (Bilimsel Açıklama-İçtihatlar-İlgili Mevzuat, Madde 1-184), 2. Baskı, Ankara 2007.

GÜNTÜRK, M. Serdar, Türk Yüksek Mahkemeleri ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Özel Hayatın Gizliliğinin Korunması, Ankara 2012.

GÜRSEL, İlke, Protection of Personal Data in International Law and The General Aspects of The Turkish Data Protection Law, D.E.Ü. Hukuk Fakültesi Dergisi, Cilt: 18, Sayı: 1, Yıl: 2016.

GORDON, Keith, Principles of Data Management, Facilitating Information Sharing, BCS Learning Development, Second Edition, November 2013.

GÖREN, Zafer, Avrupa Birliği Temel Haklar Şartının Ana İlkesi: Dokunulmaz İnsan Onuru, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Cilt: 6, Sayı: 12, Yıl: 2007.

GÖREN, Zafer, Anayasa Hukuku, Ankara, 2011.

GÖREN, Zafer Temel Hak Genel Teorisi, Ankara, 1995, Dokuz Eylül Üniversitesi Döner Sermaye İşletmesi Yayınları, Yayın No:57.

GÖZÜBÜYÜK, Şeref, Hukuka Giriş ve Hukukun Temel Kaynakları, 35. Baskı, Ankara 2013.

GÖZÜBÜYÜK, Ahmet Şeref/ GÖLCÜKLÜ Feyyaz, Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, 5. Bası, Ankara 2004.

GRUPA Fritz H. / KUECHLER William/ SWEENEY Scott, Dealing with Data Privacy Protection: An Issue for the 21st Century, LawInvestigations and Ethics, January/February 2002.

HANDBOOK on European Data Protection Law, European Union Agency for Fundamental Rights, 2014, Council of Europe.

HAFIZOĞULLARI Zeki/ÖZEN, Muharrem, Türk Ceza Hukuku, Özel Hükümler, Kişilere Karşı Suçlar, Ankara 2011.

HARİS, David/ O'BOYLE, Michael/ WARBRİCK Colin/ BUCKLEY, Carla, Law ofthe European Convention on Human Rights. New York: Oxford University Pres, 2th. Edition, 2013.

HENDERSON, Sandra C./ASYNDER Charles, Personal Information Privacy: Implicationsfor MIS Managers, Information & Management, Sayı: 36, Yıl: 1999.

HERT, Paul De/PAPAKONSTANTINOU Vagelis, The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection of Individuals, Yıl: 2012, Sayı: 28, Computer Law & Security Review.

HIZ, Yüksel/Yılmaz, ZEKERİYA, Bilgi Edinme ve Dilekçe Hakkı, Ankara 2004.

HORNUNG, Gerrit, A general data protection regulation for Europe? Light and Shade in the Commission's Draft of 25th January, 2012, Script-ed 9, No: 1.

İZGİ, Ömer/ GÖREN Zafer, Türkiye Cumhuriyeti Anayasası Yorumu, Ankara 2002.

KABOĞLU, İbrahim Ö., Anayasa Hukuku Dersleri (Genel Esaslar), 7. Baskı, İstanbul 2001.

KABOĞLU, İbrahim Ö., Özgürlükler Hukuku, 6. Bası, Ankara 2002.

KACROROWSKA, Alina, European Union Law, Routledge, Cavendish, Taylor and Francis Group, London and New York, 2009.

KAFADAR, Muhammet Fatih, Hukuk, Sivil Toplum ve Demokrasi: 'İnsan Onuru', Umut Vakfı Araştırma Merkezi, 3. Hukukun Gençleri Sempozyumu, Antalya, 11-12 Ekim 2013.

KARAASLAN Erol, Avrupa İnsan Hakları Sözleşmesi Çerçevesinde Düşünce Özgürlüğü, İstanbul Barosu Dergisi, Yıl: 2004, Cilt: 78, Sayı: 4.

KARAHİSAR, Tuba, Özel Hayatın Gizliliği ve İnternette İşlenen Suçlar, II. Medya ve Etik Sempozyumu, Medya Kültür İlişkisinde Etik.

KAYA, Cemil, Avrupa Birliği 1995/46/EC Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LXIX, Sayı: l -2, Yıl:2011.

KAYA, Cemil, İdare Hukukunda Bilgi Edinme Hakkı, Ankara 2005.

KAYA, Semih Batur, "Hukuk Devleti, Demokrasi ve Anayasacılık Ekseninde Anayasa Yargısı ve Yargısal Aktivitizm, Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XIX, Y. 2015, S.. 3,

KAYMAZ, Seydi, Ceza Muhakemesinde Telekominikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Ankara 2009.

KAZANCI, Behiye Eker, Kişilerin İzinsiz Görüntülerinin Alınmasının TCK m. 134 Çerçevesinde Değerlendirilmesi, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 9, Sayı: 1, Yıl: 2007.

KRAUSE Rüdiger, New Developmentsin Data Privacy for Employees in German Law, TheLaw in the Information and Risk Society, (Ed. GunnarDuttge/SangWon Lee), Universitäts verlag Göttingen.

KEKLİK, Ramazan, Özel Hayatın Gizliliğini İhlal Suçları, Ankara 2012.

KILIÇOĞLU, Ahmet, Fikri Hakların İhlalinde Koruma Yolları (Sınai Haklarla Karşılaştırmalı Olarak), Türkiye Barolar Birliği Dergisi,, Sayı:54, Yıl:2004.

KILINÇ, Doğan, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", Ankara Üniversitesi Hukuk Fakültesi Dergisi,Cilt: 61,Cilt: 3, Yıl:2012.

Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu.

KOKOTT, Juliane/ SOBOTTA Christoph, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Yıl:2013, Sayı:3.

KORKMAZ, Ali, İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması, KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi, 16, (Özel Sayı), Yıl:2014.

KORKMAZ, İbrahim, Kişisel Verilerin Korunması Kanunu Hakkında Bir Derlendirme, Türkiye Barolar Birliği Dergisi, Yıl:2016, Sayı:124.

KORFF, Douwe, Study On The Protection Of The Rights And İnterests Of Legal Persons With Regard To The Processing Of Personal Data Relating To Such Persons, Commission Of The European Communities (Studycontract ETD/97/B5-9500/78) Final Report.

KUNER, Christopher, European Data Privacy Law and Online Business, Oxford University Press, 2003.

KUNER Christopher, European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford UniversityPress, United Kingdom 2007.

KUŞKONMAZ, Elif Mendos, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Yüksek Lisans Tezi, İstanbul 2013.

KUZU, Burhan, Ülkemizde Kişi Özgürlüğü ve Güvenliği. İstanbul1993.

KÜZECİ, Elif,"Kişisel Verilerin Korunması", Doktora Tezi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilimdalı, Ankara 2010

KÜZECİ, Elif, Kişisel Verilerin Korunması, 3. Baskı, Ankara 2019.

KROFF, Douwe: EC Study on Implementation of Data Protection Directive – Comparative Summary of National Laws, Cambridge, 2002.

LILIAN Edwards, The Problem with Privacy: A ModestProposal", International Review of Law Computers&Technology,Cilt: 18, Yıl:2004.

LLOYD, Ian J., İnformation Tecnology Law, Fifth Edition, Oxford University Pres, Oxford, 2008.

McCULLAGH, Karen, Data Sensitivity: resolvingtheconundrum,Journal of International Commercial LawandTechnology, Cilt: 2, Sayı:4, Yıl:2007.

McCARTY-Snead Steven S/ HILBY, Anne Titus Research Guide to European Data Protection Law, 42 Int'lJ.Legal Info. 2014.

MULLOCK James, Piers Leigh- Pollit, The 1998 Data Protection Act. 2 th ed., United Kingdom: The Stationery Office Limited, 2000.

NAL, Sabahattin, Avrupa İnsan Hakları Sözleşmesi Çerçevesinde Düşünce, Vicdan ve Din Özgürlüğü, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, Cilt: 57, Sayı: 4, Ankara 2002.

OĞUZ, Habip, "Elektornik Ortamda Kişisel Veriilerin Korunması Bazı Ülke Uygulamaları ve Ülkemizdeki Durum" Uyuşmazlık Mahkemesi Dergisi. 2013

OLTEANU, Florina/OLTEANU Mariana Olteanu, Mihalena Olteanu, Protection of Personal Data–Actual and Proposed Issues, 2012, The 7th Edition of the International Conference European Integration Realities and Perspectives.

OQVİST, Karen, Lawrence Virtual Shadows: Your Privacy in the Information Society, Swindon, Büyük Britanya: The British Computer Society Publishing and Information Products., 2009.

ÖZBEK, Veli Özer, Yeni Türk Ceza Kanunun Anlamı (Açıklamalı, Gerekçeli, İçtihatlı), Cilt: 2 (Özel Hükümler), Ankara 2008.

ÖZBEK, Veli Özer/KANBUR, Mehmet Nihat/DOĞAN, Koray/BACAKSIZ, Pınar, TEPE, İlker Tepe, Türk Ceza Kanunu Özel Hükümler, Ankara 2013.

ÖZBEY, Özcan, Avrupa İnsan Hakları Sözleşmesi Işığında İfade Özgürlüğü Kısıtlamaları, Türkiye Barolar Birliği Dergisi, Yıl:2013 Sayı:106.

ÖZBUDUN, Ergun, Anayasa Hukuku, 10.Baskı, Ankara 2009.

ÖZDEMİR, Kenan, Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesi İle Avrupa İnsan Hakları Mahkemesi Kararlarında Özel Hayatın Gizliliği, Adalet Dergisi, Sayı: 23,Yıl:2005.

ÖZDEMİR, Hayrunnisa, Haberleşmenin Gizliliği ve Kişisel Veriler, Erzincan Üniversitesi Hukuk Fakültesi Dergisi,Cilt: XIII, Sayı:1-2, Yıl:2009.

ÖZEK Çetin, Türk Ceza Kanunu'na Göre Hürriyet Aleyhine Cürümlerin Genel Prensipleri, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: XXIX.

ÖZKAN, Gürsel, Demokratik Yönetimin Birinci Adımı Bilgi Edinme Hakkı, Ankara 2004.

ÖZTAN, Bilge, Medeni Hukuk'un Temel Kavramları, 8.Baskı, Ankara 2002.

PARLAR, Ali/HATİPOĞLU Muzaffer, Türk Ceza Kanunu Yorumu, 2. Baskı, Cilt: 2.Ankara 2008.

PEARCE, Graham/ PLATTEN Nicholas, AchievingPersonal Data Protection in the European Union, Journal of Common Market Studies, Sayı:36, December 1998.

PRİNS, Corien, When Personal Data, Behavior And Virtual Identities Become A Commodity: Would A Property Rights Approach Matter?, Cilt: 3, Sayı:4, Yıl:2006.

POLATER, Yusuf Ziya,Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesinde Özel Hayatın Gizliliği ve Korunması, Ankara 2010.

POULLET Y./GUTWIRTH S., The Contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of reflexive governance?, Brussels 2008

REED, ChrisReed/ANGEL John, ComputerLaw, TheLawandRegulation of Information Technology, Sixth Edition, Oxford UniversityPress 2007.

REED, Chris/ ANGEL, John,Computer Law. New York: Oxford University Press, 2003.

RİNGELHEİM Julie, Processing Data On Racial or Ethnic Origin For Antidiscrimination Policies: How to Reconcile the Promotion of Equality with the Right to Privacy, New York: NYU School of Law, 2006.

ROGERS, Kevin M., The Internet and The Law,1st., edn., Palgrave Macmillan,2011.

SALİHPAŞAOĞLU, Yaşar, Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları ışığında bir değerlendirme, Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt: XVII, Yıl:2013, Sayı:3.

SIEMEN, Birte; Datenschutz als europäisches Grundrecht, Berlin 2006.

STONE, Richard, Civil Liberties and Human Rights. Büyük Britanya, Oxford University Pres.2002

SOYKAN, Cavidan, Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı, Ankara Üniversitesi Hukuk Fakültesi Dergisi, Sayı:2, Cilt:56, Yıl:2007.

ŞEN, Ersan, Devlet ve Kitle İletişim Araçları Karşısında Özel Hayatın Gizliliği ve Korunması. İstanbul: Kazancı Yay., 1996.

ŞEN, Ersan, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", İstanbul Barosu Dergisi, Cilt: 83, Cilt: 3, Yıl:2009.

ŞEN, Ersan, Türk Ceza Kanunu Yorumu, Cilt: I, İstanbul 2006.

ŞENGÜL, Ramazan, Bilişim Çağında Şeffaf Yönetim, Ankara 2008.

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

ŞİMŞEK, Oğuz, 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu ve Kanunun 4. Maddesine Göre "Kayıt ve Verilerin İncelenmesi" ve Kişisel Nitelikli Verilerin Korunması, İzmir Barosu Dergisi, Yıl:2001, Sayı:1.

SOLOVE Daniel J./ROTENBERG Marc/SCHWARTZ Paul M., Information Privacy Law, Apsen Publishers, New York, 2006.

TANÖR, Bülent, Türkiye'nin İnsan Hakları Sorunu, BDS Yayınları, 3. Baskı, İstanbul 1994.

TANÖR, Bülent/ YÜZBAŞIOĞLU Necmi, 1982 Anayasasına Göre Türk Anayasa Hukuku, 11. Bası, İstanbul 2012.

TANJU, Erhan, AİHM Kararları Işığında İfade ve Basın Özgürlüğü,Ankara2012.

TAPPER Colin, New European Directions in Data Protection, 3 J.L. &Inf. Sci. 9 (1992)

TAŞTAN, Furkan Güven, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 1. Baskı, İstanbul 2017.

TEZCAN, Durmus, Bilgisayar Karsısında Özel Hayatın Korunması, Anayasa Yargısı, Sayı:8, Yıl:1991.

TICHER, Paul Ticher, Data Protection vs Freedom of Information, Access and Personal Data, IT Governance Publishing Ely, 2008.

TİNNEFELD, Marie/Eugen Ehmann/Rainer W. Gerling: Einführung in das Datenschutzrecht, München, 2005.

TÖRENLİ, Çakıroğlu, Maral. "Hekimin Borçlarından Özel Olarak Sır Saklama Borcu", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 12, Sayı: 2, 2010, (Basım Yılı: 2012)

RODOTA, S, Data Protection as a Fundamental Right. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?, Springer, Dordrecht, 2009.

ROOM, Stewart, Data Protection and Compliance in Context, BCS, Swindon 2007.

TOPAKKAYA, Arslan, H. Jonas'ta İnsan ve Doğanın Değeri, Felsefe ve Sosyal Bilimler Dergisi, Sayı:15, Yıl:2013.

UNCULAR, Selen, İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Ankara2014.

UYGUN, Murat, Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi ışığında kişisel verilerin korunması, Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2010.

UYARER, Göçmen, Sinem, 6698 Kişisel Verilerin Korunması Kanunu ve 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Galatasaray Üniversitesi, Sosoyal Bilimler Enstitüsü, Yüksek Lisans Tezi ,İstanbul,2019

ÜÇÜNCÜ, Sümeyye Hilal, Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması, Yayınlanmamış Doktora Tezi, Ankara 2018.

ÜZELTÜRK, Sultan, 1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı, İstanbul 2004.

YAŞAMIŞ, Firuz Demir, "Anayasa Hukuku ve İnsan Hakları Açısından Bilgi Edinme Hakkı". Türk İdare Dergisi, Sayı:444, Yıl:2004.

YÜKSEL, Metin, Temel Hakların Sınırlandırılması ve Ölçülülük, Ölçülülük İlkesi Evrensel Bir Anayasal İlke midir?, Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 7, Sayı:1, Yıl: 2017.

YILDIRIM, Ramazan, "İdare Hukuku Açısından Bilgi Edinme Hak ve Özgürlüğü". İdari Usul Kanunu Hazırlığı Uluslararası Sempozyumu, Bildiriler, Ankara 17-18 Ocak 1998.

YOKUŞ, Sevtap, "Avrupa Birliğine Uyumda Siyasi Kriterler Doğrultusunda Türkiye"de Anayasal ve Yasal Dönüşüm Çabaları", İstanbul Üniversitesi Hukuk Fakültesi Dergisi,Cilt: LXI,Sayı:1-2, Yıl: 2003.

YOKUŞ, Sevtap, Avrupa İnsan Hakları Sözleşmesi'nde ve 1982 Anayasası'nda Hak ve Özgürlüklerin Kötüye Kullanımı, Ankara 2002.

YOKUŞ, Sevtap., Avrupa İnsan Hakları Sözleşmesi'nin Türkiye'de Olağanüstü Hal Rejimine Etkisi, Beta Yayınları, İstanbul 1996.

WİTT, Bernhard, C; Datenschutz kompakt und verständnis: Eine praxisorientierte Einführung, 2. Baskı, Wiesbaden 2010.

ZENGİN, Mehmet Ali, Türk Hukukunda Bilgi Edinme Hakkının Sınırları, Ankara 2012.

ZEVKLİLER, Aydın,Medeni Hukuk (Giriş,Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku), haz. Aydın ZEVKLİLER, BeşirACABEY, Emre GOKYAYLA, 6. Baskı, Ankara 1999.

İNTERNET KAYNAKLARI

ACQUISTI, Alessandro, Privacy and Security of Personal Information-Economic Incentives and Technological Solutions, Economics of Information Security Advances in Information Security

AKILLIOĞLU, Tekin, İdari Usul ve Kişisel Verilerin Korunması, www.idare.gen.tr/akillioglu-idariusul.htm

ARTICLE 29 DATA PROTECTION WORKING PARTY; Opinion 4/ 2007 on the concept of personal data, http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Article 29 Data Protection Working Party, Opinion 15/2011 on the Definition of Consent, 2011, ec.europa.eu/justice/data-protection/article-29/document/opinion-recommendation/files/2011/wp187 en.pdf

ÇOLAK, N. İlker, "Bilgi Edinme Hakkının Sınırları ve Sınırlama Ölçütleri", e-akademi Hukuk, Ekonomi ve Siyasal Bilimler Aylık İnternet Dergisi, S. 39. Mayıs 2005, http://www.e-akademi.org/makaleler/nicolak-2.htm. (Bilgi edinme diye anılacak)

HAKERİ, Hakan, "Hasta Hakları Bakımından Yeni Türk Ceza Kanunu", Http://portal.hakanhakeri.com/index.php?option=com_content&task=view&id=27&Itemid.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

http://sozluk.gov.tr/

http://www.sivas.gov.tr/divrigi-ulu-camii-ve-darussifasi

http://www.avrupakonseyi.org.tr/antlasma/aas_108.htm

http://www.government.se/content/1/c6/01/55/42/b451922d.pdf

http://www.lawandtech.eu/nea-eidiseis/data-protection-law-ingreece.html

http://www.legislation.gov.uk/ukpga/1998/29/section/2

http://www.oecd.org/

http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

http://www.refworld.org/docid/3ddcafaac.html

https://curia.europa.eu/jcms/jcms/j_6/en/

https://poseidon01.ssrn.com/delivery.php?ID, pdf

https://verikorumahukuku.org/veri-sahibi-nedir/

https://www.ab.gov.tr/avrupa-birliginin-tarihcesi_105.html

https://www.guvenlikonline.com/makale/197/-cctv-nedir.html

https://www.heinz.cmu.edu/~acquisti/papers/acquisti_eis_refs.pdf

https://www.icisleri.gov.tr/merkez-nufus-idare-sistemi-mernis

https://www.kisiselverilerinkorunmasi.org/mevzuat/kisisel-verilerin-otomatik-isleme-tabi-tutulmasi-karsisinda-bireylerin-korunmasi-sozlesmesine-ek-denetleyici-makamlar-ve-sinirasan-veri-akisina-iliskin-protokol-181-sayili-ek-protokol/

https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf

https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-SorulanSorular

https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf

https://www.un.org/en/about-un/

https://www.data-protection-authority.gv.at/home

https://tietosuoja.fi/en/home

https://www.uodo.gov.pl/en

https://www.cnil.fr/en/home

https://www.bfdi.bund.de/EN/Home/home_node.html;jsessionid=DDDCFFB149216D5F0B7079EFED95E1B1.2_cid344

https://ico.org.uk/

KETİZMEN, Muammer, "Kişisel Verilerin Korunması" Tebliğ, http//www.tbd.org.trusr_imgcdkamubib14raporlarPDFRP2-2008.pdf.

SEVÜK YOKUŞ, Handan, Haberleşmenin Gizliliğini İhlal Suçu, http://dergipark.gov.tr/dovnload/article-file/213966.

ŞAHİN, Osman: Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğinin Korunması, (Yayımlanmamış Bilişim Uzmanlığı Tezi), Bilgi Teknolojileri ve İletişim Kurumu, 2011, http://btk.gov.tr/kutuphane_ve_veribankasi/tezler/ index.php, (Çevrimiçi, 04.10.2014).www.dutchdpa.nl/Pages /en_wetten_wbp.aspx

AİHM KARARLARI

Antovićand Mirković v. Montenegro, Başvuru No: 365201, Tarih: 28.11.2017. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-178904, Erişim tarihi, 08.02.2019.

Szabóand Vissy v. Hungary, Başvuru No: 0142016, Tarih: 12.01.2016. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-160020, Erişim tarihi, 08.02.2019.

Roman Zakharov v. Russia, Başvuru No: 82201/54 Tarih: 04.12.2015. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-159324, Erişim tarihi, 08.02.2019.

Kennedy v. the United Kingdom, Başvuru No: 26839/05, Tarih: 18 May 2010. Kararın İngilizce tam metni için bkz. https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-98473&filename=001-98473.pdf, Erişim tarihi, 08.02.2019.

Perry v. the United Kingdom, Başvuru No: 63737/00, Tarih: 17.10.2003. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/fre?i=001-61228, Erişim tarihi, 06.02.2019.

Taylor-Sabori v. the United Kingdom, Başvuru No: 47114/99, Tarih: 22 October 2002. Kararın İngilizce tam metni için bkz. https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-637291-642797&filename=003-637291-642797.pdf, Erişim tarihi, 06.02.2019.

Chalkley v. the United Kingdom, Başvuru No: 63831/00, Tarih: 12.09.2003. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-61135&filename=001-61135.pdf, Erişim tarihi, 05.02.2019.

Lewis v. the United Kingdom, Başvuru No: 1303/02, Tarih: 25.11.2003. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/fre?i=001-67226, Erişim tarihi, 05.02.2019

P. G. and J.H. v. the United Kingdom, Başvuru No: 44787/98, Tarih: 25.09.2001. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-59665, Erişim tarihi, 04.02.2019.

Kopp v. Switzerland, Başvuru No: 23224/94, Tarih: 25.03.1998. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-58144, Erişim tarihi, 04.02.2019.

Huvig v France, Başvuru No: 11105/84, Tarih: 24.04.1990. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-57626 , Erişim tarihi, 04.02.2019.

Halford v the United Kingdom, Başvuru No: 20605/92, Tarih: 26.06.1997. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-58039, Erişim tarihi, 04.02.2019.

Kruslin v France, Başvuru No: 11801/85, Tarih: 24.04.1990. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-57626, Erişim tarihi, 04.02.2019.

Malone v the United Kingdom, Başvuru No: 8691/79, Tarih: 26.04.1985. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-57533, Erişim tarihi, 05.02.2019.

Bărbulescu v Romania, Başvuru No: 61496/08, Tarih: 05.09.2017. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-177082, Erişim tarihi, 04.02.2019.

Sõro v Estonia, Başvuru No: 50073/07, Tarih: 3.09.2015. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-156518, Erişim tarihi, 03.02.2019.

Dimitrov-Kazakov v Bulgaria, Başvuru No: 11379/03, Tarih: 10.02.2011. Kararın İngilizce tam metni için bkz. https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/11379-03-dimitrov-kazakov-v-bulgaria-rezolucja-komitetu-521918425, Erişim tarihi, 01.02.2019.

Segerstedt/Wibergand Others v Sweden, Başvuru No: 62332/00, Tarih: 06.06.2006. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-75591, Erişim tarihi, 01.02.2019.

Rotaru v Romania, Başvuru No: 28341/95, Tarih: 04.05.2000. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-58586, Erişim tarihi, 01.02.2019.

Amann v. Switzerland, Başvuru No: 27798/95, Tarih: 16.02.2000. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-58497, Erişim tarihi, 28.01.2019.

Gaskin v. the United Kingdom, Başvuru No: 10454/83, Tarih: 07.07.1989. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-57491, Erişim tarihi, 28.01.2019.

Leander v Sweden, Başvuru No: 9248/81, Tarih: 26.03.1987. Kararın İngilizce tam metni için bkz. https://hudoc.echr.coe.int/eng?i=001-57519, Erişim tarihi, 28.01.2019.

Klass and Others v Germany, Başvuru No: 5029/71, Tarih: 06.09.1978. Kararın İngilizce tam metni için bkz. https://hudoc.echr.coe.int/eng#{"itemid":["001-57510"]}, Erişim tarihi, 28.01.2019.

Aycaguer v. France, Başvuru No: 8806/12, Tarih: 22.06.2017. Kararın İngilizce tam metni için bkz. https://swarb.co.uk/aycaguer-v-france-echr-22-jun-2017/, Erişim tarihi, 08.02.2019.

L.H. v. Latvia, Başvuru No: 52019/07, Tarih: 29.04.2014. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-142673&filename=001-142673.pdf, Erişim tarihi, 08.02.2019.

S. And Marper v. the United Kingdom, Başvuru No: 30562/04 - 30566/04, Tarih: 04.12.2008. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-90051, Erişim tarihi, 08.02.2019.

M. S. v. Sweden, Başvuru No: 20837/92, Tarih: 27.08.1997. Kararın İngilizce tam metni için bkz. http://www.hrcr.org/safrica/privacy/ms_sweden.html, Erişim tarihi, 08.02.2019.

Z v. Finland, Başvuru No: 22009/93, Tarih: 25.02.1997. Kararın İngilizce tam metni için bkz. http://hudoc.echr.coe.int/eng?i=001-58033, Erişim tarihi, 08.02.2019.