

**T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU (GENEL KAMU HUKUKU)
ANABİLİM DALI**

KİŞİSEL VERİLERİN KORUNMASI

Doktora Tezi

Elif KÜZECİ

Ankara-2010

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU (GENEL KAMU HUKUKU)
ANABİLİM DALI

KİŞİSEL VERİLERİN KORUNMASI

Doktora Tezi

Elif KÜZECİ

Tez Danışmanı
Prof. Dr. Maksut MUMCUOĞLU

Ankara-2010

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU (GENEL KAMU HUKUKU)
ANABİLİM DALI

KİŞİSEL VERİLERİN KORUNMASI

Doktora Tezi

Tez Danışmanı: Prof. Dr. Maksut MUMCUOĞLU

Tez Jürisi Üyeleri

Adı ve Soyadı

İmzası

.....
.....
.....
.....
.....
.....

.....
.....
.....
.....
.....
.....

Tez Sınavı Tarihi

İÇİNDEKİLER

İÇİNDEKİLER	i
KISALTMALAR	viii
GİRİŞ	1
I. Konunun Önemi ve Çalışmanın Amacı	1
II. Çalışmanın Sınırları, Planı ve Kaynakları	5
A. Çalışmanın Sınırları.....	5
B. Çalışmanın Planı.....	7
C. Çalışmanın Kaynakları	9
III. Deyimsel Açıklamalar	10
A. “Kişisel veri”, “veri”, “enformasyon”, “bilgi”	10
B. “Kişisel Verilerin Koruması”, “Veri Güvenliği”	14
C. “Özel Yaşamın Gizliliği”, “Mahremiyet”	16
D. Diğer Bazı Önemli Deyimler.....	17

BİRİNCİ BÖLÜM

BİLGİ TOPLUMU

VE

KİŞİSEL VERİLERİN KORUNMASI GEREKSİNİMİ

I. BİLGİ TOPLUMUNDA KİŞİSEL VERİLERİN KORUNMASI GEREKSİNİMİ	20
A. GENEL OLARAK.....	20
B. KİŞİSEL VERİLERE DUYULAN GEREKSİNİM-MODERNİTE VE GÖZETİM.....	21
1. KİŞİSEL VERİLERİN İŞLENMESİ VE GÖZETİM.....	21
2. MODERN ÖRGÜTLENMEDE KİŞİSEL VERİLERE DUYULAN GEREKSİNİMİN TEMELLERİ.....	22
a. Modernleşme Sürecinde Gözetim	22
b. Bürokrasi ve Gözetim	26
c. Disiplin ve Gözetim.....	28
C. TEKNOLOJİDEKİ GELİŞMELER-ELEKTRONİK GÖZETİM.....	30
1. BİLGİSAYAR VE MERKEZİ VERİ BANKALARI.....	32
2. İNTERNET	36

3. GÖZETİM SAĞLAYAN YENİ TEKNOLOJİLER.....	41
D. GÖZETİM TEKNOLOJİLERİ KAYNAKLI KAYGILAR-ELEKTRONİK GÖZETİM KARŞISINDA ŞEFFAFLAŞMIŞ BİREY	44
1. BÜYÜK BİRADER	47
2. KÜÇÜK KARDEŞLER	52
3. PANOPTİK CESUR YENİ DÜNYA	57
4. DİJİTAL KİŞİLİK	60
II. KİŞİSEL VERİLERİN KORUNMASI HAKKI	66
A. GENEL OLARAK.....	66
B. BİR “HAK” ALANI OLARAK KİŞİSEL VERİLERİN KORUNMASI	67
1. EKONOMİK HAK YAKLAŞIMI	67
a. Mülkiyet Hakkı Teorisi	69
b. Fikrî Mülkiyet Hakkı Teorisi	71
c. Diğer Teoriler	72
2. İNSAN HAKKI YAKLAŞIMI	73
C. İNSAN HAKKI OLARAK KİŞİSEL VERİLERİN KORUNMASI	75
1. İNSAN ONURU, BİREYSEL ÖZERKLİK VE BİLGİLERİN GELECEĞİNİ BELİRLEME HAKKI	75
2. ÖZEL YAŞAMIN GİZLİLİĞİ HAKKI VE KİŞİSEL VERİLERİN KORUNMASI	78
a. Özel Yaşam	79
b. Özel Yaşamın Gizliliği Hakkı	80
c. Özel Yaşamın Gizliliği Hakkının Koruduğu Değer	85
d. Özel Yaşamın Gizliliği Hakkının Sonu mu?	88
3. DÜŞÜNCEYİ AÇIKLAMA ÖZGÜRLÜĞÜ VE KİŞİSEL VERİLERİN KORUNMASI	95
a. Düşünceyi Açıklama Özgürlüğü	95
b. Düşünceyi Açıklama Özgürlüğü ve Kişisel Verilerin Korunması Hakkı Arasındaki Gerilim Hattı	96
c. Düşünceyi Açıklama Özgürlüğü ve Kişisel Verilerin Korunması Hakkının Birbirini Destekleyici Nitelikleri	99
d. Anonimlik Hakkı	100
4. BİLGİ EDİNME HAKKI VE KİŞİSEL VERİLERİN KORUNMASI ...	102
a. Bilgi Edinme Hakkı	102
b. Bilgi Edinme Hakkı ve Kişisel Verilerin Korunması: Bilgi Toplumunun İki Sütunu	103
5. ÖZEL HABERLEŞMENİN GİZLİLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI	107
6. BİLİM ÖZGÜRLÜĞÜ VE KİŞİSEL VERİLERİN KORUNMASI	110
7. DİĞER BAZI HAK VE ÖZGÜRLÜKLER İLE KİŞİSEL VERİLERİN KORUNMASININ İLİŞKİSİ	113

İKİNCİ BÖLÜM
KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN GELİŞİMİ
VE
ULUSLARARASI KAYNAKLARI

I. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUKUKSAL DÜZENLEMELERİN TARİHSEL GELİŞİMİ	115
A. GENEL OLARAK.....	115
B. İLK DÜZENLEMELER	116
C. İNSAN HAKLARI KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI	121
D. BİLGİLERİN GELECEĞİNİ BELİRLEME HAKKI	123
E. YENİ GELİŞMELER KARŞISINDA KİŞİSEL VERİLERİN KORUNMASINI ETKİN BİR ŞEKİLDE SAĞLAMA ÇALIŞMALARI	125
II. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN ULUSLARARASI KAYNAKLARI	128
A. GENEL OLARAK.....	128
B. OECD.....	130
C. BİRLEŞMİŞ MİLLETLER	133
D. AVRUPA KONSEYİ	137
1. Genel Olarak	137
2. Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme.....	142
a. Sözleşmenin konusu ve uygulama alanı.....	142
b. Sözleşmenin Kapsamı	144
3. Avrupa İnsan Hakları Sözleşmesi	147
a. Genel Olarak.....	147
b. AİHS m.8/1 Hükmü Kapsamında Kişisel Verilerin Korunması.....	149
c. AİHS m. 8/2 Kapsamında Müdahalenin Meşruluğu	155
E. APEC.....	159
III. AVRUPA BİRLİĞİ'NDE KİŞİSEL VERİLERİN KORUNMASI	167
A. GENEL OLARAK.....	167
B. AB KURUMLARI.....	168
1. AB Komisyonu	169
2. AB Konseyi.....	169
3. Avrupa Parlamentosu	169
4. Avrupa Adalet Divanı (AAD).....	170
5. Avrupa Veri Koruma Denetçisi	170
6. 29. Madde Veri Koruma Grubu	171

7. 31. Madde Komitesi	171
C. AB TEMEL HAKLAR ŞARTI.....	172
D. 95/46/AT SAYILI KİŞİSEL VERİLERİN KORUNMASI YÖNERGESİ .	176
1. YÖNERGENİN AMACI	176
2. KAPSAMI VE UYGULAMA ALANI.....	179
3. KİŞİSEL VERİLERİN ÜÇÜNCÜ ÜLKELERE AKTARILMASI.....	185
a. Genel Olarak.....	185
b. 95/46/AT sayılı Yönerge Uyarınca “Veri Aktarımı”	186
c. “Yeterli Düzeyde Koruma” Koşulu	187
d. İstisnalar	189
e. Bağışıklık Sözleşmeleri (Safe Harbor).....	192
f. Havayolu Yolcu Kayıtlarının ABD’ye Aktarımı.....	196
C. TELEKOMÜNİKASYON ALANINDA DÜZENLEMELER.....	201
1. 2002/58/AT sayılı Özel Yaşamın ve Elektronik İletişimin Korunması Yönergesi	201
2. İletişim Trafik Verilerinin Saklanması Yönergesi	207

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL İLKELERİ

I. GENEL OLARAK	211
II. KİŞİSEL VERİLERİN NİTELİĞİNE İLİŞKİN İLKELER.....	211
A. HUKUKA VE DÜRÜSTLÜK KURALLARINA UYGUN İŞLEME	212
B. BELİRLİ, AÇIK VE MEŞRU AMAÇLAR İÇİN TOPLANMA.....	214
1. Verilerin Toplanma Amacının Belirli ve Açık Olması	215
3. Verilerin Daha Sonra İşlenme Amaçlarının Toplanma Amacı İle Uyumlu Olması	218
C. TOPLANMA VE SONRASINDA İŞLENME AMAÇLARINA UYGUN, İLGİLİ BULUNMA, AŞIRI OLMAMA	219
D. DOĞRU VE EĞER GEREKLİ İSE GÜNCEL OLARAK TUTULMA.....	225
E. AMACIN GEREKTİRDİĞİNDEN DAHA UZUN SÜRE TUTULMAMA.....	227
III. İLGİLİ KİŞİNİN KATILIMI VE DENETİMİNE YÖNELİK İLKELER.....	229
A. İLGİLİNİN BİLGİLENDİRİLMESİ.....	230
B. İLGİLİNİN BİLGİLERİNE ERİŞİM HAKKI.....	232
C. İLGİLİNİN VERİLERİNİ DÜZELTME HAKKI.....	235
D. İLGİLİNİN DİĞER HAKLARI.....	235
1. İlgilinin İtiraz Hakkı.....	236
2. İlgilinin Otomatik Kararların Konusu Olmama Hakkı	236
IV. İLGİLİNİN RIZASI.....	238

A. RIZA BEYANININ NİTELİĞİ.....	238
B. RIZA BEYANINDA BULUNMA EHLİYETİ	244
V. ÖZEL KATEGORİDEKİ (HASSAS) KİŞİSEL VERİLERİN NİTELİKLİ KORUNMASI.....	249
A. KAPSAMI.....	249
B. HASSAS OLAN VE HASSAS OLMAYAN VERİLERİN AYRIMI.....	252
C. İSTİSNALAR	259
VI. VERİ GÜVENLİĞİ İLKESİ.....	261
VII. İSTİSNALAR VE SINIRLAMALAR.....	268
VIII. DENETİM VE YAPTIRIM SİSTEMLERİ	270
A. BAĞIMSIZ ORGANLARCA DENETİM (VERİ KORUMA OTORİTELERİ).....	271
B. BİLDİRİM VE LİSANS VERME UYGULAMALARI.....	276
C. YARGI YOLLARI VE YAPTIRIM.....	278

DÖRDÜNCÜ BÖLÜM

TÜRKİYE’DE KİŞİSEL VERİLERİN KORUNMASI

I. GENEL OLARAK.....	280
II. KİŞİSEL VERİLERİN KORUNMASININ ANAYASAL TEMELLERİ.....	282
A. GENEL OLARAK.....	282
B. ANAYASA TASLAK VE ÖNERİLERİNDE KİŞİSEL VERİLERİN KORUNMASI HAKKI.....	284
C. ANAYASANIN İLGİLİ HÜKÜMLERİ	287
1. İnsan Onuru ve Kişinin Maddi ve Manevi Varlığını Geliştirme Hakkı....	287
2. Özel Yaşamın Gizliliği Hakkı.....	288
3. Düşünce Özgürlüğü.....	290
4. Diğer Bazı Temel Hak ve Özgürlükler	292
5. Anayasa Mahkemesi Kararları.....	293
III. ÖZEL HUKUKTA KİŞİSEL VERİLERİN KORUNMASI.....	296
A. MEDENİ HUKUKTA KİŞİSEL VERİLERİN KORUNMASI.....	296
B. İŞ HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI	300
IV. CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI	307
A. GENEL OLARAK.....	307
B. KİŞİSEL VERİLERİN KAYDEDİLMESİ	309

C. VERİLERİ HUKUKA AYKIRI OLARAK VERME, YAYMA VEYA ELE GEÇİRME	312
D. VERİLERİ YOK ETMEME	313
E. TCK'DA KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK DİĞER HÜKÜMLER.....	315
V. KOLLUK FAALİYETLERİNDE KİŞİSEL VERİLERİN KORUNMASI....	318
A. GENEL OLARAK.....	318
B. ÖZEL İLETİŞİME MÜDAHALE	322
C. GÖRÜNTÜ KAYDI	330
D. PARMAK İZİ VE DNA ANALİZİ KAYDI.....	335
VI. İDARE HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI	342
A. GENEL OLARAK.....	342
B. ELEKTRONİK DEVLET (E-DEVLET).....	344
1. Türkiye’de Genel Olarak E-Devlet Uygulamaları	344
2. Merkezi Nüfus İdaresi Sistemi (MERNİS)	346
C. İSTATİSTİK	351
D. ADLİ SİCİL KAYDI VE GÜVENLİK SORUŞTIRMALARI	356
1. Adli Sicil Kaydı	356
2. Güvenlik Soruşturması.....	359
E. SAĞLIK HİZMETİ.....	363
F. VERGİ MAHREMİYETİ.....	368
G. BİLGİ EDİNME HAKKI	374
VII. KİŞİSEL VERİLERİN KORUNMASI KANUN TASARISI.....	376
A. KİŞİSEL VERİLERİN KORUNMASI YASASI GEREKLİ Mİ?.....	376
B. KVKKT'DE BENİMSENEN SİSTEM	384
C. KVKKT'NİN AMACI VE KAPSAMI.....	388
D. KVKKT'DE BENİMSENEN TEMEL İLKELER.....	395
1. Kişisel Verilerin Niteliğine İlişkin İlkeler	395
2. Özel Nitelikteki Kişisel Verilerin Nitelikli Korunması İlkesi	399
3. Kişisel Verilerin Üçüncü Ülkelere Aktarımı.....	403
4. Veri Güvenliği.....	404
5. İlgili Kişinin Katılımı ve Denetimi	405
6. İstisna ve Sınırlamalar.....	406
E. KVKKT'DE ÖNGÖRÜLEN DENETİM VE YAPTIRIM SİSTEMİ	408

SONUÇ.....	412
KAYNAKÇA	417
I. KİTAP VE MAKALELER.....	417
II. BELGE, GÖRÜŞ, ARAŞTIRMA VE RAPORLAR.....	453
III. GAZETE VE DERGİ HABERLERİ.....	461
IV. YARARLANILAN BAŞLICA İNTERNET SİTELERİ	463

KISALTMALAR

a.g.e.	: Adı geçen karar
a.g.k.	: Adı geçen karar
a.g.m.	: Adı geçen makale
AAD	: Avrupa Adalet Divanı
AB	: Avrupa Birliği
ABTHŞ	: Avrupa Birliği Temel Haklar Şartı
AİD	: Amme İdaresi Dergisi
AİHK	: Avrupa İnsan Hakları Komisyonu
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AK	: Avrupa Konseyi
APEC	: Asia-Pasific Economic Co-Operation (Asya-Pasifik Ekonomik İşbirliği)
aşa.	: Aşağıda
AÜEHFD	: Atatürk 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
b.n.	: Başvuru no
Baş.	: Başlangıç
BDSG	: Bundesdatenschutzgesetz (Federal Veri Koruma Yasası-Almanya)
BEHK	: Bilgi Edinme Hakkı Kanunu
BK	: Borçlar Kanunu
Bkz.	: Bakınız
BVerfGE	: Bundesverfassungsgericht (Federal Anayasa Mahkemesi-Almanya)
C.	: Cilt
CCTV	: Close Circuit Television (Kapalı Devre Televizyon)

CMK	: Ceza Muhakemesi Kanunu
çev.	: Çeviren
d.n.	: Dipnot
der.	: Derleyen
diğ.	: Diğerleri
E.	: Esas sayısı
ECJ	: European Court of Justice (Avrupa Adalet Divanı)
EİHB	: Evrensel İnsan Hakları Beyannamesi
GPS	: Global Positioning System (Küresel Yer Belirleme Sistemi)
haz.	: Hazırlayan
HD	: Hukuk Dairesi
ILO	: International Labour Organisation (Uluslararası Çalışma Örgütü)
İÜHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
İÜY	: İstanbul Üniversitesi Yayınları
JICLT	: Journal of International Commercial Law and Technology (Uluslararası Ticaret Hukuku ve Teknoloji Dergisi)
K.	: Karar sayısı
k.t.	: Karar tarihi
KVKKT	: Kişisel Verilerin Korunması Kanun Tasarısı
m.	: Madde
MERNİS	: Merkezi Nüfus İdaresi Sistemi
MK	: Medeni Kanun
MMR	: Multimedia und Recht (Multi Medya ve Hukuk Dergisi)
NJW	: Neue Juristische Wochenschrift (Yeni Hukuk Dergisi)
no.	: Numara
OECD	: Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)
OJ	: Official Journal of the European Communities (Avrupa Toplulukları Resmi Gazetesi)
par.	: Paragraf
PVSK	: Polis Vazife ve Selahiyet Kanunu
RFID	: Radio Frequency Identification (Radyo Frekanslı Tanımlama)

RG.	: Resmi Gazete
s.	: Sayfa
S.	: Sayı
s.y.	: Son yararlanma
SÜHFD	: Selçuk Üniversitesi Hukuk Fakültesi Dergisi
t.	: Tarih
TCK	: Türk Ceza Kanunu
TDK	: Türk Dil Kurumu
vb.	: ve bunun gibi
vd.	: ve devamı
VUK	: Vergi Usul Kanunu
Y.	: Yıl
Yarg.	: Yargıtay
yuk.	: Yukarıda

** Yararlanılan Bazı Hukuksal Metinlere İlişkin Şu Kısaltmalar Kullanılmıştır:*

AB Elektronik İletişim Yönergesi	:Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, 12 Temmuz 2002.
AB Veri Koruma Yönergesi	:Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 Ekim 1995.
AB Veri Saklama Yönergesi	:Directive 2006/24/EC on the retention of data generated or processed in connection with the

	provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 15 Mart 2006.
AK (Verilerin Korunması) Sözleşmesi	: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 Ocak 1981.
APEC (Verilerin Korunması) Çerçeve Belgesi	: APEC Privacy Framework, 29 Ekim 2004.
BM (Verilerin Korunması) Rehber İlkeleri	:United Nations guidelines concerning computerized personal data files, 14 Aralık 1990.
OECD (Verilerin Korunması) Rehber İlkeleri	:OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 Eylül 1980.

GİRİŞ

I. Konunun Önemi ve Çalışmanın Amacı

Kişisel verilerin korunması, Türkiye’de önemi yeni yeni anlaşılmaya başlanan bir konudur. Hukuksal, siyasal, sosyal ve teknik boyutları olan kişisel verilerin korunmasına ilişkin akademik tartışmaların özellikle son dönemde geliştiği görülmektedir. Oysa Türkiye’de yeni sayılan bu alan, yarım asrı geçen bir süredir özellikle Avrupa devletlerinde hararetli tartışmaların konusu olmaktadır. Bu süreç içerisinde kişisel verilerin korunmasını güvence altına alan bir mevzuat gelişmiştir. Türkiye’de ise çeşitli düzenlemelerde konuya ilişkin bazı hükümler yer alsa da verilerin korunmasını sağlayıcı normlar Avrupa standartları ile uyumlu değildir. Buna karşın kişisel verilerin korunması, aşağıda değerlendirileceği üzere, temel hak ve özgürlüklerin kapsamında yer alır ve günümüz toplumlarında bireylerin karşılaşabileceği önemli ihlallere karşı bir güvence sistemi oluşturur. Dolayısıyla bu eksikliğin giderilmesi Anayasasında “*insan haklarına saygılı, demokratik bir devlet*” olma idealini ortaya koymuş Türkiye Cumhuriyeti açısından son derece önemlidir.

Bu bağlamda çalışmamız içerisinde temelde üç sorunun yanıtı aranacaktır: (i) kişisel verilerin korunması neden gereklidir; (ii) kişisel verilerin korunması yönünde dünyada ne gibi çalışmalar yapılmaktadır ve bunlar hangi ilkeleri kapsamaktadır; (iii) Türkiye’de kişisel verilerin korunmasının normatif temelleri nedir ve etkin hukuksal korumanın sağlanabilmesi için neler yapılmalıdır. Bu konulara ilişkin açıklamalar ilgili bölümlerde yapılacaktır. Ancak daha önce burada akademik bir incelemenin konusu olan kişisel verilerin korunmasının neden önemli olduğu üzerinde kısaca durmak gerekir.

İsmimiz, adresimiz, telefon numaramızdan kişiliğimiz, beğenilerimiz ve yaşamın çeşitli alanlarındaki tercihlerimize kadar geniş bir yelpaze kişisel verilerimizi oluşturur. Aşağıda çeşitli açılardan değerlendirilecek olan bu deyim burada kısaca “*biz*”e ilişkin olan pek çok bilgiyi nitelediği belirtilebilir. İşte tam da bu nedenle kişisel veriler önemlidir, çünkü “*biz*”e ilişkin olanın üzerindeki denetimimizi kaybettiğimiz noktada kendimiz olmamız ve bireysel özerkliğimizi

korumamız da olanak dışına çıkacaktır. Sürekli izlenen, gözlenen, davranışları yönlendirilen bireyin özgürlüğünden de söz edilemez.

Çeşitli kişi, grup ya da organizasyonların başkalarının yaşamlarına duydukları merak ve bu konuda bilgi toplama girişimleri oldukça eski olsa da “*kişisel verilerin korunması*” kavramı çerçevesinde değerlendirebileceğimiz, kişilerin özel yaşamlarının bu gibi tehditlerden korunmasına ilişkin hukuksal gelişmeler oldukça yenidir. 1970’li yıllardan günümüze konunun her geçen gün biraz daha önemli bir sorun olarak görülmeye başlamasında ise kuşkusuz, aynı dönemde hız kazanan teknolojik gelişmeler etkilidir. Bilgisayarların ortaya çıkıp daha çok bilginin, daha hızlı, daha kolay ve daha ucuz depolanması; bilgisayarları birbirine bağlayan ağlarla bunların kolaylıkla paylaşılabilmesi ve ilişkilendirilebilir hale gelmesi kişilerin özel yaşamlarına yönelik çeşitli risklerin ortaya çıkmasına neden olmuştur. Böylesi bir ortamda son dönemin en önemli buluşu olarak nitelenen dijital teknoloji¹, yaşamlarımızı adeta bir dönüşüme uğratmıştır. Teknolojinin ve bu kapsamda özellikle e-posta ve İnternet’in işleri yapma şeklimizi dönüşüme uğrattığı, yaşamlarımızı kolaylaştırdığı açıktır, ancak bunun her zaman olumlu yönde bir gelişme olduğunu söylemek olanaklı değildir².

Burada dikkatten kaçmaması gereken bir nokta da şudur: kişisel verilerin korunması yalnızca teknoloji ile ilişkili değildir. Elle işlenen, yani geleneksel olarak alıştığımız şekliyle tutulan verilerimizin de korunmaya gereksinimi vardır. Ancak teknolojiadaki gelişmeler, bu işin yapılabilirliğine ilişkin bir dönüşüm yaratmıştır. Bu ise kişisel verilerin korunmasının öneminin anlaşılmasında ve bireylere yönelen tehdidin güçlenmesinde etkilidir. Kişisel verilerin korunmasına ilişkin tartışmaların, genellikle bilişim hukuku başlığı altında yapılmasının nedeni de budur. Oysa “*kişisel verilerin korunması*” yalnızca dijital ortamda bulunanları değil, elle tutulan bilgileri de kapsar.

Günümüzde trafik ihlallerini, suçluluğu önlemeye, ya da başka bir meşru amaca, hizmet eden kameralara, bize daha iyi hizmet sunmak için telefon görüşmelerimizi kayıt eden sistemlere, mağazalardan ya da marketlerden çeşitli

¹ Louise CADAUX, “Privacy: Our Future Under Close Surveillance”, **Freedom of Expression (And New Communication Technologies)**, Haz. Mich     PAR  , Peter DESBARATAS, IQ Collectif, Kanada 1998, s.113.

² Robert BOND, **New Economy Equity (Navigating Security and Legal Issues in Digital Business)**, John Wiley & Sons, LTD, İngiltere 2002, s. 156.

indirimler almamızı sağlayan kartlar aracılığıyla alışveriş profillerimizin veri bankalarına aktarılmasına, bilgisayarlarımızda çerezlere ve bize ilişkin olanın, özel olanın, yani alışkanlıklarımızın, zevklerimizin, tercihlerimizin kısacası yaşamlarımızın kayıt altına alınmasına alışmış durumdayız³. Artık modern yapılanmalara bilgi teknolojilerinin uygulanmasıyla kişisel bilgilerin toplanması, depolanması, yönetilmesi ve işlenmesi daha kolay hale gelmiştir⁴. Bütün bu etkinlikler kişisel veri yığınları sayesinde gerçekleştirilebilmektedir⁵. Devlet gibi gelişkin yapılanmalardan, en küçük şirketlere kadar pek çok örgütlenme için çok önemli kolaylıklar sağlayan dijital bilgileri oluşturma, işleme, saklama iletmeye ve birbirine bağlayabilme olanağının 20.yüzyılın en etkili buluşu olduğu söylenebilir⁶. Öte yandan, bu önemli buluş gelişmelere kayıtsız kalmayan, bu teknolojilerin neler sunduklarını bilen ve bunları doğru bir şekilde değerlendirebilen ve tabi hala özel yaşamların önemli olduğunu düşünen kişilerin sürekli izlenildiklerine ilişkin bir kuşku ve bunun sonuçlarına ilişkin haklı bir telaş duymasına neden olmaktadır.

Bir yanda bilgiye ulaşılması, toplanması, değerlendirilmesi ve bilginin özgürce akışından kaynaklanan çıkarlar, diğer yanda bireysel özerkliğin gerektirdiği bilgi üzerinde kişinin denetimi hakkı sürekli bir çatışma halindedir. Bu noktada önemli olan dengenin sağlanmasıdır. Devletler, yönetim, planlama, güvenliğin sağlanması gibi işlevlerini yerine getirebilmek; şirketler müşterilerine daha iyi hizmet sunmak, kârlılıklarını arttırmak gibi gerekçelerden hareketle kişisel verilere gereksinim duyarlar. Kişisel verilerin korunması hakkı ise bu aktarımı tamamen ortadan kaldırmayı değil, bu sürece herhangi bir aşamada etki olanağını kaybetmiş bireye, yeniden denetim hakkı vermeyi hedefler. Kişisel verilerin korunması, bu bağlamda, bir denge unsurudur. Hızla gelişen teknolojinin sunduğu olanaklarla, bireysel hak ve özgürlükler açısından neden olabileceği zararların değerlendirilip kendi kapsamı içerisinde terazinin tekrar makul bir dengeye kavuşmasına hizmet etmektedir.

³ David BRIN, **The Transparent Society (Will Technology Force Us to Choose Between Privacy and Freedom)**, Addison-Wesley, ABD 1998, s.57-58.

⁴ Colin J. Bennett, **Regulating Privacy , Data Protection and Public policy in Europe and United States**, Cornell university Press, Ithaca, Londra 1992, s.vii.

⁵ Louise CADAUX, s. 115.

⁶ Fred H. CATE, **Privacy in the Information Age**, Brookings Institution Press, ABD 1997, s. 5.

Çalışmamızın en başında altını çizerek vurgulamamız gereken ilk şey belki de bütün bu tehditlere karşın artık yaşamlarımızın bir parçası haline gelen teknolojinin düşmanımız olarak görülmemesi gerektiğidir. Teknoloji yaşamlarımızı pek çok açıdan kolaylaştırdığı gibi, artık onun vazgeçilmez bir parçası haline de gelmiştir. Bu durumda yapılması gereken kredi kartı kullanmayıp, İnternet bankacılığı yerine banka kuyruklarında beklemek, kimliğimizi belirtmemiz gereken her türlü ortamdan kaçınarak kendimizi toplumdan ve yeni gelişen sosyal ortamlardan soyutlamak değildir. Kaldı ki böylesine bir yaklaşım yanlış olmasının yanında çeşitli açılardan da olanaksızdır. Günümüzde teknolojiden soyutlanmış bir yaşam olanaklı değildir. Bu durumda, sorunlara ve tehlikelere karşı farkındalığımızı arttırmak, çözüm yolları üretmek, mevcut düzenleme ve uygulamaları çeşitli açılardan değerlendirmek önemlidir.

Öte yandan, gelişen teknolojinin sağladığı kolaylıklar dolayısıyla, kişisel verilerimizden ve dolayısıyla bireysel özerkliğimizden vazgeçmenin bir zorunluluk olarak da görülmemesi gerekir. Bilginin her geçen gün daha büyük bir önem kazandığı çağımızda, eğer bundan yararlanmak istiyorsak alışveriş alışkanlıklarımızın, tercihlerimizin, ya da daha geniş bir ifadeyle gündelik yaşam alışkanlıklarımızın veri bankalarında tutulmasına ses çıkarmamamız gerektiğini düşünebiliriz. Nitekim bilgi toplumuna ve bu yeni yapının ekonomik ve sosyal gerekliliklerine işaret eden çeşitli çevreler bu yaklaşıma vurgu yapmaktadır. Ancak böylesine bir takas gerekli olmadığı gibi yanlıştır da.

Sorun belki modern dünyanın özellikle 1960'lı ve 1970'li yıllarda karşı karşıya kaldığı başka bir kriz olan çevre kirliliği ile karşılaştırılarak açıklanabilir. Sanayinin yarattığı çevre kirliliğinin vahim sonuçlarının görülmeye ve tartışılmaya başlandığı bu yıllarda, iş çevreleri zehirlenen suyun ve havanın ekonomik gelişmenin, iş olanaklarının ve yaşam standardının iyileştirilmesinin bedeli olduğunu savunmuşlardır. Çevre korumaya ilişkin mücadele halen sürmekte olsa da en azından artık bu yaklaşımın yerinde olmadığı kanıtlanmıştır. Sürdürülebilir bir ekonomik kalkınma için çevrenin korunması bir gerekliliktir. Soluyacağımız temiz hava ya da içeceğimiz temiz su olmazsa insan yaşamının devamını sağlamak da olanaklı

olmayacaktır. Aynı şekilde teknoloji den tam anlamıyla faydalanabilmemiz için bireysel özgürlüklerimizi korumak da önemli bir gerekliliktir⁷.

Çalışmamızda yalnızca teknolojiye dair bir konu olmasa da çok yakından ilişki içinde bulunan ve bir anlamda onunla daha da önemli hale gelen kişisel verilerin toplanması, işlenmesi ve korunması konularında bu hassasiyetlere dikkat etmeye çalışılacaktır. Aşağıdaki açıklamalar ile hedefimiz, çağdaş, batılı ülkelerde neredeyse yarım asırdır tartışılan, dünya üzerinde pek çok devlette güvence altına alınan kişisel verilerin korunmasına ilişkin tanıtıcı açıklamalarda bulunmak, bu kapsamda Türkiye’deki duruma ilişkin de genel bir değerlendirme sunmaktır. Ancak konunun teknik boyutları ve genişliği nedeniyle kaçınılmaz bir şekilde çalışma belirli sınırlar içerisinde yürütülecektir.

II. Çalışmanın Sınırları, Planı ve Kaynakları

A. Çalışmanın Sınırları

Konunun genişliği ve bazı özellikleri dolayısıyla, çalışmanın sınırlarını burada belirlemenin gereklidir. Bu zorunlu sınırlandırma, konunun disiplinler arası niteliğinden kaynaklanır. Nitekim kişisel verilerin korunmasını, bilişim teknolojileri ile birlikte değerlendirmek bir zorunluluktur. Bu noktada, teknolojinin, uzmanlarının işi olması dolayısıyla yalnızca konumuz gerektirdiği ölçüde bazı teknik açıklamalar yapılmakla yetinilecek, konunun teknik boyutu doğal olarak çalışmanın dışında bırakılacaktır.

Ayrıca teknoloji hızla gelişen yapısı nedeniyle, her geçen gün yeni araçlar sunmakta, yeni araçlar ise yeni sorunları getirmektedir. Biz çalışmamızda güncel tartışmalara yeri geldikçe değinmeye çalıştık. Ancak kişisel verilerin korunmasına ilişkin açıklamalarımızı sürdürürken asıl hedefimiz, yeni teknolojileri değerlendirirken dikkate alınacak bir harita sunabilmektir. Bu kapsamda, konuya ilişkin her yeni araca ayrı ve ayrıntılı olarak değinilmediğini belirtmemiz gerekir.

Kişisel verilerin korunması, teknoloji yanında, siyaset ve sosyoloji başta olmak üzere başka araştırma alanları ile de yakından ilişkilidir. Bu çalışmada hukuksal bakış temel alındığı için, konunun diğer boyutlarına yine sınırlı bir şekilde

⁷ Simson GARFINKEL, “Privacy and the New Technology”, **The Nation**, S.270, s.12.

değerinilecektir. Bununla birlikte, kişisel verilerin korunmasının hukuksal açıdan da boyutlu niteliğine dikkat çekmek gerekir. Bu anlamda, kişisel verilerin korunmasının yarattığı hukuksal sorunlar ve tartışma noktaları açısından da bir sınırlamaya gitmek zorunludur. Nitekim kişisel verilere yönelik saldırılar hemen hemen hukukun her alanı ile ilgilidir ve bu nedenle değerlendirmeler çok çeşitli disiplinler açısından yapılabilir. Bu noktada kişisel verilere yönelik müdahalelerin kimlerden kaynaklandığı üzerinde kısaca durmak yararlı olabilir.

Kişisel verilere yönelik saldırılar temelde üç gruptan gelebilir: bireyler ve kişi toplulukları, çeşitli gruplar ve özel teşebbüsler ile devletler. Bireylerin başka bireylerin kişisel verilerine ulaşması ve bunları kullanmaları temelde Medeni Hukuk kapsamında kişilik haklarıyla ilişkilidir. Bu anlamda konunun, Medeni Hukuk ve Borçlar Hukuku boyutları olduğu açıktır. Bu saldırıların suç niteliğinde olması durumunda ise Ceza Hukuku devreye girecektir. Çeşitli gruplar ve özel teşebbüsler arasında da ilk akla gelenler kuşkusuz şirketlerdir. Pek çok şirket, piyasada güçlerini arttırmak, işlem hacimleri arttırmak, müşterilerine daha iyi hizmet vermek ve hepsinin temelinde kârlılıklarını yükseltmek amacıyla geniş oranda kişisel veriler toplamakta ve bunları işlemektedir. Benzer bir durum bankalar için de söz konusudur. Bu niteliğiyle kişisel veriler, Ticaret Hukuku, Bankacılık Hukuku, Sigortacılık Hukuku gibi disiplinler tarafından yakın bir şekilde incelenmektedir. Son olarak devletlerin, suçluluğu önleme, terörle mücadele, vatandaşlarına daha iyi hizmet sunma gibi nedenlerle, tuttuğu verilerin yarattığı hukuksal sorunlar bulunmaktadır. Çalışmamızda temel olarak devlet doktrinleri ve insan hakları bakışını benimsediğimizden, bizim için merkezi olarak incelenecek veriler de bunlar olacaktır. Ancak buna karşın başta uluslararası şirketler olmak üzere başka aktörlerden kaynaklı ihlaller de dikkate alınmıştır.

Ayrıca çalışmamızın başlığından da anlaşılacağı gibi inceleme alanımız “*kişisel*” verilerle, bir başka ifade ile veri öznesinin “*kişi*” olduğu durumlarla sınırlıdır. Bu noktada bireylerin yanında devletlerin, şirketlerin ve başka grupların da veri öznesi olabileceği unutulmamalıdır. Pek çok hukuk sisteminde olduğu gibi, ülkemizde de devlete ait veriler “*devlet sırrı*”, ticari şirketlere ait veriler “*ticari sır*” kapsamında korunmaktadır ve bu alan bizim çalışmamızın dışında kalmaktadır.

Biz, konuyu çeşitli açılardan değerlendirmenin ve bu doğrultuda farklı bakış açıları edinmenin son derece önemli olduğu düşüncesindeyiz. Bu çalışmanın odak noktası insan hakları açısından kişisel verilerin korunması olmakla birlikte, sorunun tek olduğunu, bu anlamda temelde bireyin özerk alanına yönelen saldırıların niteliğinin anlaşılmasının, çözüm yolları üretilmesinin ve mevcut yolların değerlendirmesinin gerekli olduğunu düşünüyoruz. Bu nedenle çalışmamızda devlet ve neredeyse devlet kadar güçlü bir hale gelmiş, şirketlerin saldırılarına karşı bireyin korunması odak nokta olarak alınmış olmasına karşın, diğer konular da tamamen göz ardı edilmeyecek, yeri geldikçe konuyu daha geniş bir şekilde araştırmak isteyen okuyucuya kısa açıklamalar ve atıflarla yardımcı olunmaya çalışılacaktır.

B. Çalışmanın Planı

Öncelikle çalışmamız içeriğinde önemli yer tutan bazı kavramlar konusunda bizim tercihler giriş içerisinde, izleyen bölümünde açıklanmıştır. Konumuz açısından merkezi öneme sahip bu kavramların konunun özüne ilişkin tartışmalara girmeden açıklanmasının yararlı olacağı düşüncesindeyiz.

“Bilgi Toplumu ve Kişisel Verilerin Korunması Gereksinimi” başlıklı birinci bölümde cevap aranan temel soru: kişisel verilerin korunmasının neden gerekli olduğudur. Bu doğrultuda birinci bölüm içerisinde kişisel verilere çeşitli örgütlerce duyulan gereksinimin siyasal, sosyal ve ekonomik temelleri; bilişim teknolojilerinin kişisel verilerin işlenmesi ile olan yakın ilişkisi, kişisel verilerin korunmasının bir hak alanı olarak kabul edilmesinin gerekliliği ve diğer temel hak ve özgürlükler ile olan ilişkisi üzerinde durulacaktır.

Çalışmamızın ikinci bölümü *“Kişisel Verilerin Korunması Hukukunun Gelişimi ve Uluslararası Kaynakları”* başlığını taşımaktadır. Burada öncelikle, kişisel verilerin korunmasına ilişkin hukuksal düzenlemelerin ortaya çıkışı, gelişimi ve evrimi değerlendirilecektir. Konunun tarihsel gelişimini incelemek, bugün yaşanan sorunları anlayabilmek açısından önemlidir. Ayrıca böylesine bir değerlendirmenin, Türkiye gibi kişisel verilerin etkin korunmasını sağlayan düzenlemeleri henüz kabul etmemiş ülkeler açısından yararlı olacağı düşünülmektedir. Yasa koyucuyu mevcut düzenlemelere getiren süreci, önceki

düzenlemelerin artı ve eksilerini öğrenmek yeni düzenlemelerin daha sağlıklı yapılmasını sağlayacaktır.

Bu bölümde daha sonra kişisel verilerin korunmasının uluslar arası kaynakları üzerinde durulacaktır. OECD, BM, AK, APEC gibi bölgesel ve evrensel kuruluşların kişisel verilerin korunmasına nasıl yaklaştıklarına ilişkin bir çerçeve sunulmaya çalışılacaktır. Kişisel verilerin korunmasına ilişkin ayrıntılı düzenlemeler içeren Avrupa Birliği mevzuatı da ikinci bölümde incelenecek konular arasındadır.

Ardından üçüncü bölümde bu açıklamaların ışığı altında “*kişisel verilerin korunmasında hâkim olan temel ilkeler*” belirlenecektir. Her ne kadar veri koruma sistemleri heterojen bir nitelik gösterse de bazı temel ilkelerin hemen hemen bütün sistemlerde benimsendiği söylenebilir. Bu ilkelerin incelenmesi uygulayıcıya yol gösterici olabilir ama daha da önemlisi bu ilkeler, kişisel verilerin korunmasının içeriğinin saptanmasını sağlayacaktır.

Çalışmamızın son bölümünde ise Türkiye’de kişisel verilere ilişkin hukuksal düzenlemeler incelenmiştir. Bu doğrultuda ilk olarak konunun Anayasal temelleri incelenmiştir. Bu değerlendirme bir yandan Türkiye Cumhuriyeti’nin anaysal düzeninde kişisel verilerin korunmasının yerini belirlemek, diğer yandan ise ülkemizde konuya yaklaşımı sergilemek açısından önemlidir. Bu bölüm içerisinde ikinci olarak Medeni Kanundan, Türk Ceza Kanununa, Vergi Usul Kanunundan Ticaret Kanuna kadar geniş bir yelpaze içinde serpiştirilmiş hükümlere ve başka bazı hukuksal düzenlemelerle uygulamalara değinilecektir. Ardından Kişisel Verilerin Korunması Kanun Tasarısı üzerinde durulacaktır. Kişisel Verilerin Korunması Kanun Tasarısının hazırlanma gerekçeleri arasında, Avrupa Birliği’ne giriş sürecinde birlik mevzuatına ve özellikle 95/46/AT sayılı Verilerin Korunması Yönergesine uyum sağlamak da yer almaktadır. Bu nedenle tasarının hükümleri, bu bölümde özellikle Yönergeyle uyumluluğu açısından karşılaştırmalı olarak incelenecektir. Ayrıca yeri geldikçe başka bazı ülkelerin yaklaşımları ve konuya ilişkin uluslararası sözleşmelerin getirdiği ilkeler de karşılaştırmalı bir değerlendirme kapsamına alınmıştır. Federal Almanya Cumhuriyeti’ndeki düzenlemelere, mahkeme kararlarına ve öğretiyeye, diğer ülkelerle karşılaştırıldığında, daha yoğun bir şekilde atıf yapıldığı söylenebilir. Bunun nedeni, kişisel verilerin korunması hukukunun anavatanı olarak nitelendirilebilecek Almanya’da konuya ilişkin çalışmaların zenginliğidir.

C. Çalışmanın Kaynakları

Yukarıda belirtildiği üzere kişisel verilerin korunması, özellikle batı Avrupa’da yaklaşık elli yıldır hem öğretide, hem uygulamada önemli tartışmaların ve ayrıntılı çalışmaların konusu olmuştur⁸. Bu kapsamda konuya ilişkin kapsamlı araştırmaların, yayınların yapıldığı, pek çok mahkeme kararı ile uygulamada yaşanan sorunlara somut çözümler arandığı görülmektedir.

Çalışmamız içerisinde elbette birincil kaynaklarımız hukuka ilişkindir. Ancak bunun yanında sosyoloji, siyaset bilimi, teknoloji gibi alanlardaki çalışmalardan da sıklıkla yararlanılmıştır. OECD, Birleşmiş Milletler, Avrupa Konseyi, Avrupa Birliği gibi örgütlerin konuya ilişkin çalışmaları incelememizde başvurduğumuz önemli kaynaklardır. Bunların içerisinde OECD Rehber İlkeleri’nin, Avrupa Konseyi’nin 108 sayılı Sözleşmesinin, başta 95/46/AT sayılı Yönerge olmak üzere AB bünyesinde kabul edilen metinlerin üzerinde özellikle durulacaktır. Aşağıda da açıklanacağı üzere, bunlar konuya ilişkin ilk uluslararası düzenlemeleri oluşturmaları yanında, pek çok ulusal hukuk sistemini de etkilemişlerdir. Bu bağlamda çeşitli ülkelerin konuya ilişkin benzer ya da farklı yaklaşımlarına da yeri geldikçe değinilecektir.

Ayrıca çeşitli ulusal ve uluslararası kuruluşların, hükümetlerin ve sivil toplum örgütlerinin sorunun çeşitli boyutlarını inceleyen raporları, önerileri, değerlendirmelerinin de temel kaynaklarımız arasında yer aldığını belirtmek gerekir. Bu metinler, kişisel verilerin korunmasının dinamik niteliği açısından oldukça önemlidir. Nitekim konuya ilişkin güncel sorun ve tartışmaların izlenmesi açısından da bu metinler yararlı olabilmektedir. Derinleşmek isteyen okuyucuya yararlı olacağı düşüncesiyle bu raporların listesi ve konuya ilişkin belli başlı İnternet sitelerinin adresleri kaynakçada ayrı bir başlık altında gösterilecektir.

⁸ Bygrave, verilerin korunmasına ilişkin öğretideki muazzam kaynağa işaret etmek için David Flaherty’nin 1984 yılında yayınlanan özel yaşamın gizliliği ve veri korunması ile ilgili uluslararası bibliyografyayı örnek olarak göstermektedir. Özellikle Birleşik Krallık, ABD, Almanya, Fransa, Kanada ve İsveç’te yapılan yayımlara odaklanan bu çalışmada 1900’e yakın kaynak yer almaktadır. Bkz. David H. FLAHERTY, **Privacy and Data Protection, An International Bibliography**, Mansell, Birleşik Krallık 1984; Lee A. BYGRAVE, **Data Protection Law, Approaching Its Rationale, Logic and Limits**, Kluwer Law International, Hollanda 2002, s. 14.

III. Deyimsel Açıklamalar

Kişisel verilerin korunmasına ilişkin bazı temel kavramların, burada, “*Giriş*” bölümünde açıklanması gerekir. Nitekim burada kullanılan pek çok deyim, bazı okuyucular için yeni ve ilk aşamada anlaşılabilir. Bu bağlamda, bazı temel deyimlerin konuya ilişkin değerlendirmelere girmeden açıklanması kanımızca hem çalışmamızı daha anlaşılır kılacak, hem de bazı deyimsel tercihlerimiz konusunda açıklık getirecektir.

Türkiye açısından yeni olan bu araştırma alanında, pek çok deyiminin yerleşmiş Türkçe karşılıkları bulunmamaktadır. Bunun hem hukuksal, hem teknik nedenleri vardır. İlk olarak özellikle Avrupalı devletlerde kişisel verilerin korunması 1970’li yıllardan beri hukuksal düzenlemelerin konusu olduğundan, geçen zaman içerisinde bu konuya ilişkin bir terminoloji gelişmiştir. Bu gelişimin ne yazık ki gerisinde kalmış Türkiye’de ilgili kavramların doğru karşılığını bulmak gerekir. Teknik açıdan ise, kişisel verilerin korunmasına ilişkin sorunlar, teknolojiyle yakından ilişkili olduğundan ve doğal olarak teknolojiyi üreten dilini de belirlediğinden pek çok yabancı kökenli teknik terim ile çalışmamız içerisinde karşılaşılması olasıdır.

Bu deyimlerin doğru Türkçe karşılıklarını bulmak ve bu karşılıkların tercih edilme sebeplerini açıklamak gerekir. Burada, halen ilgili komisyonda görüşülmekte olan Kişisel Verilerin Korunması Kanun Tasarısını da dikkate aldığımızı belirtmeliyiz. Tasarının yasalaşma sürecinin tamamlanmasının ardından, gelişecek terminolojiyle paralel deyimlerin kullanılması, konunun anlaşılabilirliği açısından önemlidir. Ancak farklı deyimlerin konuyu daha iyi nitelediği düşünüldüğünde gerekçeleri ile birlikte bu tercihlerimizin nedenleri de açıklanacaktır. Bunun yanında, yerleşik kullanımları dolayısıyla pek çok deyim, İngilizce ve/veya Almanca karşılıklarına da çalışmamız içerisinde parantez içerisinde yer verilecektir.

A. “Kişisel veri”, “veri”, “enformasyon”, “bilgi”

Deyimsel açıklamalara ilk olarak kişisel verinin ne olduğu ile başlanmalıdır. Ulusal ve uluslararası pek çok hukuksal düzenlemede belirtildiği gibi, kişisel veri,

belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgidir. Bu durumda kişisel veriyi, kişisel olmayan verilerden ayırabilmek için temelde iki ölçütten yararlanıldığı söylenebilir. Buna göre, kişisel veriden söz edebilmek için, verinin (i) bir kişiye ilişkin ve (ii) bu kişinin de belirli ya da belirlenebilir nitelikte olması gerekir.

Bu ayrımı, kişinin adı gibi, basit bir örnekle açıklamaya çalışalım. Bir kişinin adı, onun belirli ya da belirlenebilir olması için ilk akla gelen bilgidir. Bu anlamda ad, pek çok durumda kişisel veri niteliğindedir. Ancak bazı durumlarda tek başına yeterli olmayabilir. Örneğin, yaygın bir ada ve soyada sahip olan bir kişiye ilişkin yalnızca bu bilgiye sahip olmak onu belirlenebilir kılmaz. Aynı şekilde bazen bir kişinin, tam adı bilinmese de belirlenebilir olduğu görülür. “*Türkiye Cumhuriyetinin şu anki başbakanı*” ya da “*Başkent Üniversitesi Hukuk Fakültesi Sekreteri*” bilgisini aldığımız zaman, bu kişiler adları belirtilmese de kolaylıkla belirlenebilecektir. Bu anlamda ölçütlere dikkat edilerek hangi verilerin kişisel olduğunu saptamakta herhangi bir güçlük bulunmamaktadır⁹.

Bu noktada “*veri*”nin ne olduğuna da kısaca değinmek gerekir. Nitekim, öğretide özellikle “*veri*” (data), “*enformasyon*”(information) ve “*bilgi*”(knowledge) deyimleri arasındaki ilişki tartışmalı bir alanı oluşturur. Çeşitli yazarlar bu üç terimin birbirlerinin yerine geçiyormuş gibi kullanımının önemli bir hata oluşturduğuna, deyimlerin arasında farklılık bulunduğuna işaret etmektedir¹⁰. Bu durumda öncelikle farklılığın ne olduğunu ortaya koymak gerekir.

Ayrıntılı açıklamalara girmeden verinin enformasyonun, enformasyonun da bilginin hammaddesini oluşturduğu söylenebilir¹¹. Çeşitli kaynaklarda verinin yalnızca sonuç çıkarılabilecek olgular, bilgiler ve sayılardan oluştuğu¹² ve bir bilgisayar sistemi tarafından işlenen ham materyali nitelemek için kullanıldığı

⁹ Bu konuya ilişkin ayrıntılı bir değerlendirme için bkz. Article 29 Data Protection working Party, Opinion 4/2007 on the Concept of Personal Data, 20 Haziran 2007, 01248/07/EN, WP 136, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm (s.y. 20 Mart 2009).

¹⁰ Örneğin bkz. Construction Project Data Exchange and Management Module, <http://cig.bre.co.uk/dataexchange/subjectIntro/dataOrInformation.jsp> (son yararlanma: 20.09.2007).

¹¹ A.Semih İŞEVİ, Burçin ÇELME, “Bilgi Çağında Yeni Hazine: Entelektüel Sermaye ile Rekabeti Yakalamak”, I. ÜNAK Genel Konferansı, ÜNAK 2002, 19 Mayıs Üniversitesi, Samsun, 10-12 Ekim 2002, Araştırma ve Teknoloji Genel Müdür Yardımcılığı, 2002 Ulusal ve Uluslar arası Bildiriler, Şişecam İstanbul 2002, (s.38-50), <http://eprints.rclis.org/archive/00005618/01/bilgidunyasiES.pdf>.

¹² Ünal TEKİNALP, *Fikri Mülkiyet Hukuku*, 2. Baskı, Beta, İstanbul 2002, s. 123.

belirtilmektedir¹³. Ancak “veri”nin yalnızca bilgisayar verisi olarak kabul edilmesi, koruma alanını olukça daraltır. Bu anlamda, “bilgisayar verisi”, hem bilgisayar dışında elektronik ortamda tutulan verilerin¹⁴, hem de elektronik ortam dışında tutulan verilerin kapsam dışında kalmasına neden olur¹⁵. Bunun ise çeşitli hukuksal sonuçları olacaktır. Elektronik ya da elektronik olmayan ortamlarda tutulmuş olsun, veriyi yalnızca bilgi, olgu ya da sayıların ham hali olarak düşünersek, onun insanlara anlamlı gelen bir enformasyona dönüştürülebilmesi için bazı işlemlerden geçmesi gerekir¹⁶. Nitekim çeşitli yazarlarca bilginin, alıcısına anlamlı gelecek bir biçime dönüşmesini sağlayacak şekilde işlenmiş veri olduğunun¹⁷ ya da daha açık bir ifadeyle bilginin veri ile anlamın birleşimine denk bulunduğunun¹⁸ belirtildiğini görüyoruz. Bu doğrultuda bilgi, “anlamlı bir biçime sokularak, kullanıcısına güncel ve olası kararların alınmasında yardımcı olan veri” olarak tanımlanmaktadır¹⁹.

¹³ Avrupa Konseyi Siber Suçlar Sözleşmesi’nde “bilgisayar verisi”, “bir bilgisayar sisteminin belirli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde işlemeye uygun nitelikteki her türlü bilgi ve konsept” olarak tanımlanmıştır. Bkz. Avrupa Konseyi Siber Suçlar Sözleşmesi, m.1/b. Metnin Türkçe çevirisi için bkz. **Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı**, İnternet ve Hukuk Platformu, Ankara Barosu, Ankara 2006. 5237 sayılı Türk Ceza Kanununun 243. maddesinin gerekçesinde ise “sistem içindeki bütün soyut unsurlar”ın burada geçen “veri” teriminin kapsamında yer aldığı belirtilmiştir.

¹⁴ Elektronik veri, “disket, CD gibi araçlarla kaydedilen ses ve görüntü şeklindeki bilgiler olarak tanımlanabilir”. Bkz. Veli Özer ÖZBEK, “Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi”, **İÜHFİM**, İstanbul, C.LIX, S.1-2,2001, s.197.

¹⁵ Murat Volkan DÜLGER, **Bilişim Suçları**, Seçkin, Ankara, 2004, s.49.

¹⁶ Tony GUNTON, **Dictionary of Information Technology and Computer Science**, Penguin, Büyük Britanya 1992, s. 47. Veri (data) sözcüğü ilk başta “tek bir gerçek” anlamına gelen “datum”un çoğulu olarak kullanılmıştır. Veri işleme ise, “veriyi hesaplamalar yapmak ve kararlar almak gibi işlerde kullanmayı kapsamaktadır”. Douglas A. DOWNING, Michael A. COVINGTON, Melody Mauldin COVINGTON, **Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü**, çev. haz.: Boğaç ERKAN, Murat SONGÜR, 5. Baskı, Hacettepe-Taş, Ankara 1999, s. 139.

¹⁷ Gordon B. DAVIS, Margrethe H. OLSON, **Management Information Systems: Conceptual Foundations, Structure and Development**, 2. Baskı, NY, Mc Graw-Hill, 1985, s.200.

¹⁸ Peter CHECKLAND, Jim SCHOLLES, **Soft Systems in Action**, New York, John Wiley & Sons, 1990, s.330.

¹⁹ Faruk ÇUBUKÇU, **Bilgisayar Terimleri Sözlüğü**, V Yayınları, Ankara 1987, s.24. KURT’a göre: “Her iki tanım birlikte irdelendiğinde anlaşılacağı üzere bilgi ve veri birbirinden farklı kavramlar olup, en basit anlatımla bilgi bizim algıladığımız temel ve her türlü malumat, bu malumatın bilgisayarın anlayıp işleyebileceği haline de veri denilmektedir. Suyun katı, sıvı ve gaz halinde olduğu gibi tabii ortamda sıvı halde bulunan suyun örneğin buhar makinesinde fonksiyon görebilmesi için gaz haline dönüştürülmesi gerekir. Veri ve bilginin özde her iki hali de aynı olup, aralarında şekil farklılığı bulunmaktadır”. Levent KURT, **Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Seçkin, Ankara 2005, s. 38.

Bu yaklaşımda bilgi, bir üst aşamayı ifade eder. Ancak sorunun bu şekilde çözüldüğünü söyleyebilmek olanaklı değildir. Her şeyden önce, enformasyon ve bilgi, tanımlanması oldukça zor kavramlardır. Gerçekten, enformasyon, çok yönlü ve farklı değer gruplarını barındıran bir kavram olduğundan “*enformasyon nedir?*” sorusu yanıltıcı bir basitliğe sahiptir. Bu yönüyle “*ahlak nedir?*” ya da “*gerçek nedir?*” gibi kolaylıkla sorulabilen ancak cevaplanmasının çok zor olan başka felsefi kavramlara benzer. Pek çok araştırmacı da enformasyonun tek ve ortak bir tanımı bulunmadığı konusunda hemfikirdir²⁰. Aynı durum, “*bilgi*” için de söz konusudur. Nitekim bu kavramlara ilişkin yapılan tanımlar ve ayrımlar çeşitli açılardan eleştirilmektedir²¹.

Türk Dil Kurumu, Güncel Türkçe Sözlük’e²² göre, enformasyon, “*danışma, tanıtma/haber alma, haber verme, haberleşme*”yi, bilgi, “*(bilişim açısından) kurallardan yararlanarak kişinin veriye yönelttiği anlamı*” ve veri de “*bilgi,data/(bilişim açısından) olgu, kavram ve komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi*”ni ifade etmektedir. Görüldüğü gibi dilimizde bilgi ile veri hemen hemen birbirine eş anlamlı şekilde kullanılmaktadır. Enformasyon ise Türk Dil Kurumu tarafından diğer ikisinden oldukça farklı bir şekilde anlamlandırılmıştır.

Enformasyon’dan söz edebilmek için sürece insanın katılımı zorunludur. Türk Dil Kurumu Güncel Türkçe Sözlük’ünde olduğu gibi, çoğu zaman kitle iletişim araçları ve haber alma ile ilişkili olarak düşünülür. Bu yaklaşımda enformasyon hakkı, “*kitle iletişim araçları yoluyla, haber, bilgi ve belgelere erişebilme ve bunları iletebilme anlamına gelir*”²³. Biz burada enformasyonun, bir ya da birden çok amaca

²⁰ Luciano FLORIDI, “Information” (s.40-62), **The Blackwell Guide to the Philosophy of Computing and Information**, haz. Luciano Floridi, 2003, s. 40. Bunun yanında “enformasyonun”nin farklı tanımları da bulunmaktadır. Örneğin WINKEL’e göre, enformasyon içinde bulunduğu ortamla çeşitli şekillerde iletişim kuran anlamlı sinyaller şeklinde sınıflandırılabilir. Olaf WINKEL, “The Democratic Potentials of Interactive Information Technologies under Discussion-Problems, Viewpoints, and Perspectives”, **Elektronische Demokratie (Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis)**, haz. Bernd Holznagel, Andreas Grünwald, Anika Hanssmann, s.28.

²¹ Örneğin bkz. Luciano FLORIDI, “Is Information Meaningful Data?” <http://citeseer.ist.psu.edu/cache/papers/cs/18292/http:zSzzSzwww.wolfson.ox.ac.ukzSz~floridizSzfi.pdf/is-information-meaningful-data.pdf>

²² Büyük Türkçe Sözlük, <http://www.tdk.gov.tr> (s.y. 12 Mart 2007).

²³ Cemil KAYA, **İdare Hukukunda Bilgi Edinme Hakkı**, Seçkin, Ankara 2005, s. 38. İbrahim KABOĞLU da “*enformasyon hakkı*” ile “*bilgilenme hakkı*”nı eş anlamlı olarak kullanmıştır.

ulařmak için bir dizi olguyu resmeden (bizi o konuda bilgilendiren) kavramsal, insani bir ürün²⁴ ifade ettięi řeklindeki tanımını kabul ediyoruz.

Bu ayrımlara ve tartışmalara kısaca değinmekle birlikte çalışmamızda veri, enformasyon ve bilgi kelimelerini birbirinin yerine geçer řekilde kullandığımızı belirtmek isteriz. Bu tercihimizin nedeni, bu deyimler arasındaki farklılıklara ilişkin duyarsızlığımız değildir. Aksine felsefi açıdan olduęu gibi, biliřim teknolojileri açısından bu deyimler arasında farklılık bulunduęu açıktır. Bizim tercihimiz, yalnızca verilerin korunması hukuku dolayısıyladır. Veri koruması hukukunda, enformasyon ve veri deyimleri arasında ufak bir ayrım bulunsa da yasal düzenlemelerde ya da hukuksal tartışmalarda bu iki deyim arasında bir ayrım yapmaya çalışmak kanımızca yapay ve gereksizdir. Ayrıca iki deyim arasında bir sınır çizmek uygulamaya geçildiğinde daha da zorlaşmaktadır.

Her iki deyim de son derece karışık ve belirsiz yapısı ve bundan dolayı da her ikisi için de, yukarıda kısaca değindiğimiz gibi, tanım bolluğunun bulunması nedeniyle, ayrım yapmakta ısrarcı olmak yasal düzenlemelerde de istenmeyen bazı sonuçların alınmasına neden olabilir²⁵. O halde deyimlerin arasında bir farklılık bulunduğunu kabul etmekle birlikte, kişisel verilerin korunmasına ilişkin olarak birbirlerinin yerine geçer řekilde kullanımlarının herhangi bir sakıncası bulunmadığının altını çizmek gerekir.

B. “Kişisel Verilerin Koruması”, “Veri Güvenlięi”

“*Verilerin korunması*” ve “*veri güvenlięi*” deyimlerinin etimolojik kökeni belirsiz olsa da ilk olarak Almanca’da kullanıldığı ve deyimlerin Almanca karşılığı olan “*datenschutz*” ve “*datensicherheit*”dan başka dillere çevrildięi düşünülmektedir. Bu deyimler, ilk olarak kıta Avrupa’sında kabul görmüş, daha

Bkz. İbrahim Ö. KABOĞLU, “Düşünce Özgürlüğü (Avrupa Ölçütleri ve Türkiye)”, **İnsan Hakları Yıllığı**, C. 15, Y. 1993, s. 46.

²⁴ Lee A. BYGRAVE, **Data Protection Law**, s. 20.

²⁵ Aynı yönde bkz. Lee A. BYGRAVE, **Data Protection Law**, s. 20.

sonra dünyanın çeşitli dillerinde kullanılmaya başlanmıştır²⁶. ABD, Kanada, Avusturalya gibi ülkelerde ise “*verilerin korunması*” yerine, “*özel yaşamın gizliliğinin korunması*” (privacy protection) deyiminin tercih edildiği görülür.

Verilerin korunması, temelde “*veri*”lerin değil, bu verilerin ilişkili olduğu kişi ve kurumların korunmasını hedef alır. Bizim çalışmamız kişisel verilerin korunması ile sınırlandırıldığından, bu noktada hedef, gerçek kişilerin korunmasıdır. Verilerin korunması kişileri onlar hakkındaki bilgilerin (bilgisayarla ya da elle) işlenmesinden doğacak zararlardan koruma amacına yönelmiş ve kişisel verilerin korunmasına ilişkin ilkelerde somutlaşmış bir dizi (yasal ya da yasal olmayan) önlemi ifade eder²⁷. Bu anlamda kişisel verilerin korunmasının, kişilere ilişkin bilgilerin toplanması, saklanması, kullanılması gibi veri işlem sürecinin bütün aşamalarını kapsar şekilde bireylerin denetim hakkını yeniden kazandırmaya yöneldiğini söyleyebiliriz. Bu niteliği dolayısıyla, kişisel verilerin korunması ile veri güvenliği arasında bir ayrım bulunduğunu belirtmek gerekir. Çeşitli yazarlar, bu alanda korunanın veriler değil, kişiler olması dolayısıyla “*veri koruması*” deyiminin yanlış bir seçim olduğunu belirtmektedir²⁸. Bu deyimsel tercih, kişisel verilerin korunmasının veri güvenliği ile karıştırılmasına neden olabilir.

Nitekim veri güvenliği, doğrudan verilerin güvenliğini hedef almıştır. Bu açıdan amaç, kişilerin değil, verilerin korunmasıdır. Ancak bu veriler, kişilerle ilgili olduğu ölçüde, veri güvenliği, kişisel verilerin korunmasına da hizmet edecektir²⁹. Kişisel verilerin korunmasına ilişkin pek çok hukuksal düzenlemede veri güvenliğinin temel ilkeler arasında yer alması da bu nedenledir.

Bizim çalışmamızda da esas olan kişisel verilerin korunmasına ilişkin açıklamalarda bulunmak olduğu için, bu alandan daha çok veri denetçilerinin, işleyicilerinin, kullanıcılarının çıkarlarını (ulusal güvenlik, ticari yarar ya da yönetimin verimliliği gibi nedenlerle) korumaya yönelmiş veri güvenliği deyimini³⁰

²⁶ “*Verilerin korunması*” deyiminin İngilizce karşılığı “*data protection*”, Fransızca karşılığı “*protection des données*” dir. Bu konuya ilişkin olarak bkz. Cemil KAYA, **İdare Hukukunda Bilgi Edinme Hakkı**, Seçkin, Ankara 2005, s. 92.

²⁷ Lee A. BYGRAVE, **Data Protection Law**, s. 22.

²⁸ Viktor MAYER-SCHÖNBERGER, “Generational Development of Data Protection in Europe”, **Technology and Privacy: The New Landscape**, haz. Philip E. AGRE, Marc ROTENBERG, MIT Press, ABD 1998, s. 219.

²⁹ Peter GOLA, Rudolf SCHOMERUS, **Bundesdatenschutzgesetz Kommentar**, Verlag C.H. Beck, 9. Baskı, Almanya 2007, s. 344.

³⁰ Lee A. BYGRAVE, **Data Protection Law**, s. 23.

tercih edilmemiştir. Her şeyden önce kişisel verilerin korunmasında amacın verilerin değil kişilerin korunması olduğu unutulmamalıdır.

C. “Özel Yaşamın Gizliliği”, “Mahremiyet”

Özellikle yabancı dilde yazılmış kaynaklardan edindiğimiz bilgileri aktarırken, kimi deyimlerin doğru Türkçe karşılıklarını bulmak ciddi bir sorun oluşturmaktadır. Bu noktada, “*özel yaşamın gizliliği*” önemli bir tartışma noktasını oluşturulabilir. Kanımızca, bu noktadaki tercihimizi ve bu tercihin nedenlerini çalışmanın başında belirtmek gereklidir.

Sorun, iki açıdan kendini göstermektedir. Birincisi, yukarıda da belirtildiği gibi, özellikle Anglo-Amerikan sistemine dâhil ülkelerde, “*kişisel verilerin korunması*” yerine, “*özel yaşamın gizliliği*” deyimini kullanılmaktadır. Bu noktada konuya ilişkin akademik çalışmaların, mevzuat ve mahkeme kararları değerlendirilerek, içeriğin kişisel verilerin korunması kapsamında bulunması durumunda kişisel verilerin korunması deyiminin kullanımı tercih edilecektir.

İkinci olarak, dilimizde İngilizce “*privacy*” deyiminin karşılığı olarak kimi metinlerde “*özel yaşamın(ya da hayatın) gizliliği*”nin kimilerinde ise “*mahremiyet*”in kullanıldığı görülmektedir. Çalışmamız içinde bu iki ifadeden hangisinin tercih edileceğine de karar verilmesi gerekir. Mahremiyet deyimini, tek kelimeden oluşması dolayısıyla ifade açısından bir kolaylık sağlamaktadır. Bununla birlikte, “*privacy*” deyiminin karşılığı olarak “*mahremiyet*”i kullanmak içerik açısından yanlış olacaktır.

Mahremiyet, “*kişinin herkesle paylaşmayacağı veya herhangi bir kimse ile paylaşmamak hakkının bulunduğu olay, inanç ve duygularının, isteği üzerine o kişiyle paylaşılması*” durumunu ifade eden “*intimacy*” deyiminin karşılığıdır³¹. Oysa özel yaşamın gizliliği hakkı, bireyin yalnızca mahrem alanını korumamakta, mahrem olmayan kamuya açık alanını da koruma kapsamına almaktadır. Burada makul özel

³¹ Oya ARASLI, *Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenleniş*, Ankara 1979, (yayınlanmamış doçentlik tezi), s.6, d.n.12.

alan beklentisinin ne olduğu sorusu önem taşır³². Bu nedenle, özellikle “*informational privacy*” gibi deyimlerin Türkçe karşılıklarını oluşturmada bazı sözsel sıkıntılar yaratsa da “*privacy*”nin karşılığı olarak “*özel yaşamın gizliliği*”nin kullanım tercih edilmiştir.

D. Diğer Bazı Önemli Deyimler

Kişisel verilerin korunması, bir ya da birden çok kişi veya örgütün dahil olduğu bir sürece ilişkin düzenlemeleri içerir. Bu süreç “*kişisel verilerin işlenmesi*” olarak adlandırılır. Kişisel verilerin işlenmesi, kişisel verilerin otomatik ya da otomatik olmayan yollarla elde edilmesi, toplanması, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi, sınıflandırılması veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen bir işlemi ya da işlemler bütünü nitelendirmek için kullanılmaktadır³³.

Verilerin işlenmesini etkileyen ya da bundan etkilenen çeşitli gerçek ve tüzel kişiler bulunmaktadır. Bu kişilere ilişkin deyimler kısaca açıklanmalıdır. Bu kapsamda ilk akla gelen, korumanın konusu olan kişidir. Verilerin nitelediği kişiyi belirtmek için genel olarak “*veri öznesi*” (data subject) ya da “*ilgili kişi*” deyimlerinin kullanıldığı görülür³⁴.

³² Sultan ÜZELTÜRK, **1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı**, Beta, İstanbul 2004, s. 2-3.

³³ Bkz. Kişisel Verilerin Korunması Kanun Tasarısı, 3(e) hükmü, <http://www.kgm.adalet.gov.tr/tbmmkom/kisiselveriler.pdf> (s.y. 20 Mart 2009); 95/46/AT sayılı AB Yönergesi, 2 (b) hükmü. Daha ayrıntılı bir tanımlama örneği için bkz. Bundesdatenschutzgesetz (Federal Almanya Veri Koruma Yasası, bundan sonra BDSG olarak anılacaktır), 1 Ocak 2002, par. 3/2, 3, 4, 5. 108 numaralı AK Sözleşmesi ise yalnızca otomatik yolla işlenen verilere hasredilmiş bir metindir. Bu nedenle yalnızca otomatik işlemenin tanımı yapılmıştır. Sözleşmenin 2(c) hükmü uyarınca otomatik işleme, tamamı veya bir kısmı otomatik yöntemlerle gerçekleştirilen şu işlemleri içerir: verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanışı, verilerin değiştirilmesi, silinmesi veya çıkarılması.

³⁴ 95/46/AT sayılı AB Yönergesi, 2(a) maddesine göre kişisel veri “*belirli ya da belirlenebilir gerçek kişi (veri öznesi)*” ile ilgili herhangi bir bilgi anlamına gelir. Yönerge’yi iç hukuklarıyla uyumlaştıran AB üyesi ülkelerin konuya ilişkin yasalarında da benzer ifadeler yer almaktadır. Örneğin bkz. BDSG m. 3/1. 108 sayılı Avrupa Konseyi Sözleşmesi’nin 2(a) maddesi de hemen hemen aynı hükmü içermektedir. Ancak bu Sözleşme’nin resmi Türkçe çevirisinde “*veri öznesi*” yerine “*ilgili kişi*” deyiminin kullanıldığı görülmektedir. Bkz. http://www.avrupakonseyi.org.tr/antlasma/aas_108.htm (s.y. 20 Mart 2009). Aynı şekilde

İlgili kişi dışında sürece dahil olan başka kişi ve örgütler de bulunur. Buna göre, “*veri denetçisi*” (data controller) verilerin işlenmesinin amaç ve araçlarına karar veren kişi ya da örgütü ifade eder³⁵. Türkçe metinlerde “*veri denetçisi*” yerine “*veri kütüğü sahibi*” deyiminin tercih edildiği görülmektedir³⁶. Ancak buradaki temel ölçütün verilere sahiplik değil, işlemler üzerindeki denetim olduğunu³⁷ belirtmek gerekir.

Bunun yanında “*kişisel verileri işleyen*”, “*veri kütüğü sahibi adına, bu verileri işleyen gerçek ve tüzel kişileri*”³⁸; “*veri kullanıcısı*” (data user) ya da “*alıcı*” (recipient) ise, verileri alan ve bunları çeşitli amaçlar için kullanan kişi ya da örgütü niteler³⁹.

Böylece, “*ilgili kişi*”, “*veri denetçisi*”, “*verileri işleyen*” ve “*veri kullanıcısı*” olmak üzere sürece dahil olan dört aktörü kısaca tanımlamış bulunuyoruz. Ancak bu noktada şunu da belirtmek gerekir: uygulamada, bu kişi ya da organlar arasındaki ayrımı belirleyebilmek her zaman kolay olmamaktadır. Özellikle belirli bir veri işleme sürecinde, kimin ya da neyin veri denetçisi olduğunu saptayabilmekte çeşitli sıkıntılar ile karşılaşılabilir. Bu sıkıntı kendini özellikle geniş ve karmaşık yapılanmalarda ve elektronik iletişim ağlarında gösterir⁴⁰.

Son olarak kişisel verilerin korunması teknolojiyle etkileşim halinde bir alan olduğundan çeşitli teknik deyimlere de çalışmamız içerisinde yer verileceğini

Kişisel Verilerin Korunması Kanun Tasarısı’nın 3 (c) hükmünde de hakkında kişisel veriler işlenen gerçek ve tüzel kişileri nitelemek için “*ilgili kişi*” deyimini tercih edilmiştir. Çalışmamız içinde hakkında kişisel veriler işleneni nitelemek üzere, her iki deyim de kullanılacaktır.

³⁵ Lee A. BYGRAVE, **Data Protection Law**, s. 21.

³⁶ Kişisel Verilerin Korunması Kanun Tasarısı’nın 3(h) hükmü “*veri kütüğü*”nü, “*gerçek ve tüzel kişilere ilişkin belirli bir kritere göre kişisel verilere ulaşımı kolaylaştıracak şekilde yapılandırılmış herhangi bir veri grubu*” olarak tanımlar. “*Veri kütüğü sahibi*” ise, madde 3(ı) hükmü uyarınca “*kişisel verilerin işlenmesinin amaç ve metodlarını tek başına veya başkaları ile belirleyen gerçek ve tüzel kişiler*”dir. Bu tanım, AB Yönergesi’nin 2(d) hükmü ile de uyumludur. BDSG’de ise “*denetçi*”, “*kendi adına ya da başkalarını görevlendirerek, kişisel verileri toplayan, işleyen veya kullanan kişi ya da organ*” anlamına gelir.

³⁷ Lee A. BYGRAVE, **Data Protection Law**, s. 21, dn. 51.

³⁸ Kişisel Verilerin Korunması Kanun Tasarısı, m. 3(d); AB Yönergesi, m. 2(e).

³⁹ Tanımlarında bazı farklılıklar bulunsu da pek çok metinde, “*alıcı*” (recipient) deyiminin tercih edildiği görülmektedir. Örneğin bkz. AB Yönergesi, m. 2(g); BDSG m. 3/8. Nitekim Kişisel Verilerin Korunması Kanun Tasarısı’nda m. 3/a hükmü uyarınca “*alıcı*”, “*kişisel verileri belirli bir soruşturma çerçevesinde alan makamlar hariç olmak üzere, üçüncü kişi olsun veya olmasın verinin açıklandığı herhangi bir gerçek veya tüzel kişi ile kişi topluluğunu, kamu kurum ve kuruluşunu*” ifade eder şekilde kullanılmıştır. Ancak kanımızca kişisel verilerin korunmasının teknolojiyle yakın ilişkisi düşünüldüğünde “*alıcı*” deyiminin kullanılmasının yanıltıcı olabileceği ortadadır.

⁴⁰ Lee A. BYGRAVE, **Data Protection Law**, s. 21.

belirtmemiz gerekir. Okuyucu açısından konunun anlaşılır kılınması kaygısı ile bu teknik ve özel deyimlere ilişkin kısa açıklamalar ilgili yerlerde, genellikle bilgi dip notları aracılığıyla yapılmaya çalışılacaktır.

BİRİNCİ BÖLÜM

BİLGİ TOPLUMU

VE

KİŞİSEL VERİLERİN KORUNMASI GEREKSİNİMİ

I. BİLGİ TOPLUMUNDA KİŞİSEL VERİLERİN KORUNMASI GEREKSİNİMİ

A. GENEL OLARAK

Kişisel veriler, tarih boyunca “*diğerleri*” için önemli olmuştur. Farklı nedenlerle, farklı bilgilere yönelik olsa da diğer kişiler(eşler, akrabalar, arkadaşlar, komşular...), çeşitli topluluklar (işverenler, cemaatler, dernekler...), yöneticiler (modern öncesi ya da modern) hep bizi daha kapsayıcı bir şekilde bilmeyi istemiştir. Bu istek, elbette çok çeşitli nedenlerden kaynaklanır. En basit nedeni insanî bir duygu olan meraktır. Merakın kökenleri psikolojinin inceleme alanına girmektedir ve bu duygudan hareketle kişilerin birbirine yönelttiği bilme isteği, temelde, bizim konumuzun dışında kalmaktadır. Ancak bunun yanında sosyolojik, siyasal ve hukuksal açılardan değerlendirilebilecek çok farklı gereksinimlerle de karşılaşılır.

İşverenler açısından verimliliği arttırmak, ticarî açıdan kârlılığını yükseltmek, idarî açıdan akılcı yönetimi ve güvenliği sağlamak, bu geniş yelpaze içinde ilk akla gelenlerdir. Ancak hangi gerekçeden hareket edilirse edilsin, aşağıda inceleneceği üzere, pek çok cepheden yönelen bu bakışlar, temel hak ve özgürlüklere ilişkin çeşitli sorunlar yaratmaktadır. Bu sorunlara çözüm bulma ve çatışan gereksinimler arasında dengenin kurulması gerekliliği ise tarihsel açıdan daha yakın bir dönemde aciliyet kazanmıştır.

Gerçekten, verilerimize yönelen bilme isteği yeni olmasa da, kişisel verilerin korunması 1960’larda tartışılmaya, 1970’lerde ise hukuksal düzenlemelerin konusu olmaya başlar. Bunda teknolojiadaki, özellikle de bilişim teknolojilerindeki gelişmenin etkisi yadsınamaz. Bu dönemde bir yanda kökeni çok daha eskilere dayanan devletin gözetim isteği, diğer yanda yeni gelişmeler ile bu isteğin eski dönemlerde görülme-ye-n ol-çü-de kapsayıcı bir şekilde gerçekleşme olasılığı, bireysel

özerkliğe ilişkin kaygıların gelişmesine neden olmuştur. O halde, kişisel verilerin korunması hukukunun ortaya çıkışında temelde üç etkenin bulunduğu söylenebilir: (i) çeşitli örgütlerce kişisel verilere duyulan gereksinim, (ii) teknolojideki gelişmeler ve (iii) gözetim teknolojilerindeki gelişmeler nedeniyle duyulan kaygı.

Bu noktada şunu da belirtmek gerekir: kişisel verilerin korunması hukuku ilk aşamada devlete karşı bireyin korunmasına yönelmiştir. Ancak ticarî şirketlerin de konumuz açısından önemli bir yeri bulunmaktadır. Bu nedenle aşağıda başta devlet ve onun yönetsel araçları olmak üzere, bize çevrilen daha büyük “göz”lerin üzerinde durulacaktır. Dünya’da ve Türkiye’de konuya ilişkin yasal düzenlemelerin ortaya çıkışı, gelişimi ve dönüşümü üzerine açıklamalara geçmeden önce bu bölümde kamu sektöründe ve özel sektörde kişisel verilerimizi bilme isteğinin kaynaklarını ve onları korumamızın neden gerekli olduğunu açıklamaya çalışacağız.

B. KİŞİSEL VERİLERE DUYULAN GEREKSİNİM-MODERNİTE VE GÖZETİM

1. KİŞİSEL VERİLERİN İŞLENMESİ VE GÖZETİM

Gözetim (surveillance), en genel şekliyle, bir ya da daha fazla kişinin hareketlerinin veya iletişiminin sistemli olarak araştırılması ya da izlenmesi olarak tanımlanabilir

¹. Gözetim toplumu ise, gözetime elverişli teknikler kullanılarak örgütlenmiş ve yapılanmış bir toplumdur². Kişilere ilişkin bilgilerin toplanması ve saklanması da bu kapsamda temel bir gerekliliği oluşturur³. Hatta sosyolojik açıdan incelendiği şekliyle gözetim, doğrudan kişisel verilerle ilişkilidir. David Lyon’a göre gözetim, *“hakkında veri toplananları etkileme veya idare etme amacıyla tanımlanmış ya da tanımlanmamış herhangi bir kişisel veri toplanması ve işlenmesidir”*, genellikle

¹ Roger CLARKE, “Dataveillance: Delivering ‘1984’”, 9 Şubat 1993 <http://www.anu.edu.au/people/Roger.Clarke/DV/PaperPopular.html>, (s.y. 1 Şubat 2009).

² **A Report on the Surveillance Society**, For the Informational Commisioner by the Surveillance Society Network, Eylül 2006, haz. David Murakami WOOD, s. 3.

³ Gözetime ilişkin önemli teorisyenlerden Christopher DANDEKER’e göre gözetim şu etkinliklerden en az birini içerir: (i) insanlar ya da nesnelere ilişkin (önemli sayılan) bilgilerin toplanması ve saklanması; (ii) fiziksel konumları yada talimatlara uyumları açısından insanların ya da nesnelerin hareketlerinin izlenmesi; (iii) denetim altındakilerin davranışlarının ve talimatlara uyumluluklarının izlenmesine bilgi toplama etkinliklerinin uygulanması. Bkz. Christopher DANDEKER, **Surveillance, Power and Modernity, Bureaucracy and Discipline from 1700 to the Present Day**, St. Martin’s Press, ABD 1990, s. 37.

somut kişilerin birbirini izlemesini içermez ve bireylerden özellikle soyutlanmış gerçeklik parçalarını araştırmaya yönelmiştir⁴.

Çeşitli örgütlerce kişilere ilişkin bilgilere duyulan gereksinim tarihin çok eski dönemlerinden beri kendini gösterir⁵. Hatta kişilere ilişkin kayıt tutmanın medeniyetin kendisi kadar eski olduğu söylenebilir⁶. Bu nedenle, kişiler hakkında bilgi toplama, onları izleme ya da daha genel ifadesiyle gözetleme ve bunun için geliştirilen pek çok araç yeni değildir. Ancak günümüzde önceki dönemlere göre önemli bir farklılık dikkat çekmektedir. Burada bir dönüm noktası olarak modernliğin ve onunla birlikte de modern devletin ortaya çıkışını alabiliriz. Nitekim bugün bildiğimiz şekliyle gözetim modern çağlara özgü bir kavramdır⁷.

2. MODERN ÖRGÜTLENMEDE KİŞİSEL VERİLERE DUYULAN GEREKSİNİMİN TEMELLERİ

a. Modernleşme Sürecinde Gözetim

Tarih boyunca pek çok topluluk, komüne yaşamlara odaklı örgütlenmiştir. Dünyanın çeşitli yerlerindeki pek çok kabilede, Ortaçağ Avrupa'sında, hatta Amerika'da ilk kolonilerde insanlar genellikle bir arada, aynı çatı altında hatta tek odada yaşadıklarından birbirleri hakkında bilmedikleri çok az şey bulunuyordu. Eski zamanlarda kişisel bilgiler, ilişki içinde bulunan kişilerin hatıralarında saklıydı ve bilgi anlatılan hikâyeler ile yayılıyordu⁸.

18. yüzyılda başlayan Sanayi Devrimi ile öncelikle İngiltere ve Batı Avrupa'da insanların yaşam koşullarında ciddi değişiklikler olmaya başladı. Bu gelişim ise, binlerce insanı, fabrikalarda ya da başka oluşumlarda çalışmak üzere kalabalık ve gittikçe büyüyen şehirlere yönlendirdi. Bu hareketli ama bir o kadar da soyutlanmış yaşamlar beraberinde yeni sosyal gereklilikler getirdi. Bu bağlamda,

⁴ David LYON, **Günlük Hayatı Kontrol Etmek, Gözetlenen Toplum**, çev. Gözde SOYKAN, Kalkedon, İstanbul 2006, s.13.

⁵ Örneğin günümüzden 2500 yıl önce yazılmış Sun Tzu'nun ünlü eseri Savaş Sanatı'nda casusluğun bir kişinin düşmanlarına karşı nasıl etkili bir yol olacağı tartışılmaktadır. Bkz. SUN-TZU, **The Art of War**, Oxford University Press, Büyük Britanya 1971.

⁶ Colin J. BENNETT, **Regulating Privacy, Data Protection and Public Policy in Europe and the United States**, Cornell University Press, ABD 1992, s. 18.

⁷ David LYON, **Elektronik Göz, Gözetim Toplumunun Yükselişi**, çev. Dilek HATTATOĞLU, Sarmal, İstanbul 1997, s. 42.

⁸ Daniel J. SOLOVE, **The Digital Person, Technology and Privacy in the Information Age**, New York University Press, ABD 2004, s. 2.

bireylerin ve ailelerin kişisel alanının sınırlarını belirleme gereksinimi özel yaşamın gizliliği hakkında anlam bulmuştur. Ayrıca bu durum kültürel ve hatta psikolojik değişimleri de tetiklemiştir⁹.

İnsanlar, özel yaşamın gizliliği hakkını koruyan yeni sosyal davranışlar tanımlamaya ve John Locke gibi çeşitli filozof ve düşünürler de haklara ve devlet ile ilişki içinde bulunan bireyin özerkliğine vurgu yapmaya başlamıştır¹⁰. İşte tam da bu nedenle özel yaşamın gizliliği hakkı ve onun kapsamı içinde yer alan, ancak ondan son dönemde gittikçe ayrılmaya başlayan kişisel verilerin korunması, düşünceyi açıklama özgürlüğü gibi, ilk aşamada, devlete karşı ileri sürülen haklardandır. Bu nedenle de kişisel verilerin korunmasını devletin taleplerini, gereksinimlerini ve uygulamalarını dışlayarak açıklayabilmemiz olanaklı değildir. Onun için de öncelikle modern devleti kavramamız gerekir.

16. yüzyılda ayak sesleri duyulan ve 20. yüzyılda bütün dünyaya yayılan modernlik¹¹, *“aralarında eşgüdüm sağlanmış çok sayıda görevin hizmetindeki tek bir merkezden gelen bilgiyle harekete geçen ve o merkezce yönetilen bir makine olarak”*¹² tasarlanan modern devleti ortaya çıkarmıştır. Merkezi yönetimi sağlayabilmek için hüküm sürdüğü alanın en ücra köşelerine kadar uzanmış bürokratik kollarıyla bu karmaşık mekanizma, ilk ortaya çıktığı günden beri yurttaşlara ilişkin bilgilere gereksinim duyar. Bu, modern toplumda değişimin ve akılcılığın bir gerekliliği¹³ olduğu gibi, modern devletin şiddet tekeli, ulusal egemenlik gibi başka bazı özellikleri dolayısıyla da kaçınılmazdır. Ayrıca sosyal devlet ilkesinin benimsendiği durumlarda, halkın refahının sağlanmasına yönelik planların yaşama geçirilmesi için de bu bilgilere gereksinim duyulur. Bu anlamda modern örgütlenme için kişisel veriler, temelde yönetim, planlama gibi işlevlerin yerine getirilmesi ve güvenliğin sağlanması için gereklidir.

Merkezi bir yönetsel birim olarak modern devlet, ülke topraklarını düzenleme, kurallar koyma ve bunlara uymaya zorlama, düzeni sağlama, vergi

⁹ Bkz. Ferdinand SCHOEMAN, “Privacy: Philosophical Dimensions of the Literature”, **Philosophical Dimensions of Privacy**, haz. Ferdinand David SCHOEMAN, Cambridge University Press, ABD 1984, s. 1-34.

¹⁰ Harry HENDERSON, **Privacy in the Information Age**, Facts of File, ABD 2006, s. 6-7.

¹¹ Marshall BERMAN, **Katı Olan Herşey Buharlaşıyor**, İletişim, 4. Baskı, İstanbul 2001, s. 29.

¹² Gianfranco POGGI, **Modern Devletin Gelişimi, (Sosyolojik Bir Yaklaşım)**, çev. Şule KURT, Binnaz TOPRAK, İstanbul Bilgi Üniversitesi Yayınları, 2. Baskı, İstanbul 2002, s. 119.

¹³ Lee A. BYGRAVE, **Data Protection Law**, s. 98.

toplama, harcamalarda bulunma, kapitalist işletmeler için sosyal ve ekonomik yapıyı oluşturma ve daha genel ifadesiyle modern dünyada ticari, diplomatik ve askeri gücünü geliştirme gibi amaçlarını gerçekleştirirken hep bilgiye gereksinim duymuştur¹⁴. Bu nedenle çeşitli kaynaklardan yurttaşlara ilişkin bilgiler toplanır. Toplanan bu bilgiler olanaklar dahilinde kayıt edilir ve bunlardan rasyonel sonuçlar çıkarılmaya çalışılır.

Modern devletin kişisel bilgilere olan bağımlılığının kaynağı da budur. Çünkü artık yönetici ile yönetilen arasındaki ilişki Ortaçağ'da görülen kişisellikten sıyrılmıştır. Modern devlet yurttaşları ile olan ilişkisini objektif bir temele oturtmak zorundadır. Mali ilişkiler, vergilerin belirlenmesi, devlet bütçesinin hazırlanması gibi konularda bu zorunluluk açıkça görülür. Bütün verilerin belgeleştirilmesi gereği ise yönetimin her işini yazılı olarak görmesi temeline dayanır. Devletin uğraştığı kişilerin hepsi dosyaların içine konulup arşivlenirse modern bürokrasi gelişebilir. Bu belgeleştirilmiş önlemler büyük ölçüde tek taraflı bir istekle/zorla toplansa da mutlaka objektif bir ölçüt gerektirmektedir¹⁵.

Bu noktada devletin oluşturduğu kayıtları temelde üçe ayırarak inceleyebiliriz¹⁶:

- (i) Yönetmelik kayıtlar [bireyin bir yönetim birimiyle (lisans, pasaport başvurusu, vergi beyanı, medeni durum değişikliği bildirimi gibi) bir işlem yapması nedeniyle oluşturulan kayıtlar];
- (ii) Haber alma(istihbarat) kayıtları (polislin topladığı bilgiler gibi herhangi bir soruşturma amacıyla oluşturulan kayıtlar);
- (iii) İstatistik kayıtlar (nüfus sayımları ya da çeşitli alan araştırmaları ile politika oluşturmak amacıyla toplanan bilgiler).

¹⁴ Reg WHITAKER, **The End of Privacy, How Total Surveillance Is Becoming a Reality**, The New Press, ABD 1999, s. 40-41. Kişilerin kendilerini tanımayanlara kimliklerini tanıtmalarını veya onlar tarafından tanınmalarını sağlayan belgelerin kullanımı ise Ortaçağ'ın sonlarından beri görülmektedir. Kişilerin kimliklerine ilişkin belgelerin Ortaçağ'ın sonları ve erken modern dönemden günümüze uğradığı değişime ilişkin olarak bkz. Valentin GROEBNER, **Who Are You?, Identification, Deception, and Surveillance in Early Modern Europe**, Almanca'dan İngilizce'ye çev. Mark KYBURZ, John PECK, Zone Books, ABD 2007.

¹⁵ Peter SCHAAR, **Das Ende der Privatsphäre, Der Weg in die Überwachungsgesellschaft**, Goldmann, Almanya 2009, s. 98.

¹⁶ **Records, Computers and the Rights of Citizen**, U.S. Department of Health, Education and Welfare(HEW), Report of Secretary's Advisory Committee on Automated Personal Data Systems, Haziran 1973, <http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm> , (s.y. 2 Şubat 2009).

Bu kayıtların oluşturulmasında önemli, belki de en önemli araç ise gözetimdir.

Modernlik ile bir yandan bilgiye daha önce hiç olmadığı oranda gereksinim duyulurken, diğer yandan da bilgi toplamak ve bunları değerlendirmek konusunda daha önce varolmayan çeşitli araçları geliştirilmiştir. Karşılıklı olarak birbirini besleyen bu iki durum, gözetimdeki farklılaşmayı da beraberinde getirir. Artık modern öncesi dönemin parçalanmış yapısında yerel, ailevî ya da dinsel temelde olan gözetim gerilemiş, merkezi gözetim ise gittikçe daha da güçlenmiş ve yaygınlaşmıştır.

Devletin görevleri geniş bir bilgi varlığı ile yerine getirilmektedir. Artık devletin geleneksel görevi olan kamu güvenliği ve esenliğini sağlama aşılmıştır. Bugün bütün toplumsal alanlar devlet ile bağlantılıdır. Eğitimden sağlığa kadar pek çok alanda bunun örnekleri görülebilir. Devletten adaleti yerine getirmesi ve yurttışı dış tehditlerden koruması beklenir. Devlet, kültürü geliştirmekte ve kitle iletişim araçlarına ilişkin ilkeleri belirlemektedir. Trafik güvenliğini sağlamak, suçluları yakalamak devletin görevleri arasındadır. Vergi ve sosyal sigorta yükümlüsü olarak toplumun pek çok gerkesinimini de devlet karşılamaktadır. Bütün bu görevleri yerine getirirken bilgiye gereksinim duyulduğu açıktır. Hele ki günümüzde teknolojik araçlarla donatılmış devlet yapılanmasında bu daha da açık bir şekilde hissedilmektedir. Son yıllarda uygulamaya geçirilen e-devlet projeleri ile bazı hizmetler sanal ortamda sunulmaktadır. Bu projelerin temelinde yurttaşların talep ve gereksinimlerinin daha kolay sağlanması yatar. Ancak öte yandan yurttaşlar yalnızca müşteri olarak değerlendirildiği izlenimini yaratmaktadır¹⁷. Sonuçta hedef “*müşteri memnuniyeti*”nin sağlanmasıdır. Bu arada aşağıda değerlendireceğimiz üzere, şeffalık, katılım ve kişisel verilerin korunması gibi son derece önemli konular ihmal edilebilmektedir. Bu, günümüzde özel sektörün veri işleme pratiklerinde sıklıkla karşılatığımız türdeki bir algının devlet yönetiminde de söz konusu olabileceğini göstermektedir.

Bu noktada, modernitenin gelişmesiyle bilgiye gereksinim duyanın yalnızca devlet yönetimi olmadığı da dikkatten kaçmamalıdır. Kapitalist işletmeler de verimliliklerini arttırmak amacıyla çalışanlarını ve bir sonraki aşamada da

¹⁷ Peter SCHAAR, *Das Ende der Privatsphäre*, 99-100.

müşterilerini gözetlemiş, haklarında bilgiler toplamış, onları dosyalamış ve bu dosyalarda yer alan bilgileri değerlendirmiştir. O halde kişisel verilerin korunmasının sosyal, siyasal ve ekonomik gerekliliklerle yakından ilişkili olduğu söylenebilir.

Hem kamu sektöründe, hem de özel sektörde bilgilere duyulan gereksinimin temelinde verimliliğin arttırılması isteği yatar. Aradaki farklılık daha çok verimliliğe yüklenen anlamdadır. Modern devlet verimliliği; savunma, ulusal egemenlik ve kimi zaman refah düzeyini arttırmak olarak algılarken; kapitalist işletmede amaç her zaman daha çok kazanç sağlamaktır¹⁸. Bu bağlamda para ve pazarlama özel sektörde kişileri bilme isteğinin temelinde yatan iki önemli çıkarı oluşturur¹⁹.

b. Bürokrasi ve Gözetim

Modernlikle birlikte ortaya çıkan gözetimin kapitalist üretim sistemi ile ilişkisinin ilk dönem analizlerini Karl Marx'ın ve Max Weber'in eserlerinde bulmak olanaklıdır. Her iki düşünür de gözetimin bürokrasi ile ilişkisi üzerinde durmuşlardır. Karl Marx gözetimi, emek ve sermaye arasındaki mücadelenin bir ögesi olarak görür. İşçilerin izlenmesi, burada, sermaye adına yönetsel denetimin sürdürülmesinin bir aracı olarak ele alınır. Öte yandan Max Weber'e göre, modern toplum kitlesel, karmaşık ve değişken bir yapıdadır. Bu yapı, modern devlet örgütlenmesini toplumsal yaşamın her alanına yönelik rasyonel planlama, örgütleme, siyaset yapma ve denetlemeye zorlamaktadır²⁰. Bu ise ancak, rasyonel yönetsel bir araçla, Weber'in deyimiyle “*modern bürokrasi*” ile sağlanabilir²¹.

Bürokrasi devlet yönetimi ile de sınırlı değildir, ticaretin işleyişi için de kullanılır²². Weber, bürokrasiyi modern kapitalist işletmeleri ve modern orduyu da kapsayacak şekilde, modern toplumun bütün büyük ölçekli örgütlenmelerinin yönetiminin soysal bir biçimi olarak görür. Bu ise Weber'in modernleşme ile özdeşleştirdiği akılcılığın bir bileşenidir²³. Bu anlamda o, bütün modern örgütlerin bürokrasi içinde verimli uygulama arayışının bir gerekliliği olarak dosyalarda veri

¹⁸ Ayrıca bkz. Lee A. BYGRAVE, **Data Protection Law**, s. 98.

¹⁹ Daniel J. SOLOVE, **The Digital Person**, s. 16.

²⁰ Hans Van Der LOO, Williem Van REIJEN, **Modernleşmenin Paradoksları**, İnsan Yayınları, İstanbul 2003, s. 143- 144.

²¹ Reg WHITAKER, s. 42.

²² Daniel J. SOLOVE, **The Digital Person**, s. 38.

²³ Christopher PIERSON, **Modern Devlet**, çev. Dilek HATTATOĞLU, Çiviyazıları, İstanbul 2000, s. 42.

saklama ve çağırma araçları geliştirmesi üzerinde yoğunlaşmıştır. Bu tip dosyalar, tüm örgütlerin ama özellikle devlet yöneticilerinin bireyleri “*fışkılayabileceği*” kişisel bilgiler içerir²⁴.

Bu bilgilerin toplanmasının ve sürecin tamamının hem bu işlemleri gerçekleştirenler, hem de bu işlemler haklarında gerçekleştirilenler açısından çeşitli sonuçları bulunur. Gerçekten bürokratik süreçler dünyasında memurlar da bir makinenin işlemlerini sağlayan dişliler gibi mekanikleşmekte, bu ise bireysel yaratıcılığın dışlandığı “*demir kafes*”e yol açmaktadır. Korkulan sonuç ise insanın kendi yarattığı bir aygıtın mahkûmu olmasıdır²⁵.

Benzer bir yaklaşıma Habermas’ın “*iletişimsel eylem teorisi*”nde²⁶ de rastlamak olanaklıdır. Habermas, kültür, kişilik ve sosyal iletişim ağlarını kapsayan yaşam dünyası ile devlet ve ekonomiye hâkim bürokratik aygıtların alanı olan sistemi birbirinden ayırmıştır. Burada bürokratik örgütlerin her türlü sosyal ilişkilere müdahalesi ile toplumsal yaşamın tehdit edildiğini göstermeye çalışmıştır. Bu şekilde bireyler, kendi yaşam dünyalarından uzaklaşarak bürokrasinin soyut kuralları içinde sıkışmışlardır²⁷. Oysa yaşamın sürmesi için özgür iletişimsel eylem şarttır. Bu anlamda, kişisel verilerin korunmasının yaşam alanının korunmasına da hizmet edeceği açıktır.

Bu noktada şuna da dikkat çekmek gerekir: modern örgütlenme içinde gözetim, yalnızca yurttaşlara, topluluklara ya da sınıflara yönelmemiştir. Modern devlet işlevini yerine getirebilmek için gözlerini kendine ve kendi etkinliklerine de çevirir²⁸. Nitekim Anthony Giddens bu durumu modern örgütlenme açısından değerlendirmiştir. Giddens’a göre gözetim bir örgütteki etkinliklerin denetimidir ve

²⁴ David LYON, **Elektronik Göz**, s. 20,43.

²⁵ Hans Van Der LOO, Williem Van REIJEN, s.144.

²⁶ Bu kurama ilişkin ayrıntılı açıklama için bkz. Jürgen HABERMAS, **Theorie des kommunikativen Handelns**, 2 Cilt, Schurkamp, 6. Baskı, Almanya 2006. Kitap Türkçe’ye de çevrilmiştir: Jürgen HABERMAS, **İletişimsel Eylem Kuramı**, çev. Mustafa TÜZEL, Kabalcı, İstanbul 2001.

²⁷ Hans Van Der LOO, Williem Van REIJEN, s.145. Habermas’ın tezinden belli açılarda ayrılma da bir başka düşünür Luhmann da benzer bir soruna işaret etmiştir. Niklas Luhmann’ın sosyal kuramına ilişkin bir değerlendirme için bkz. Hans-Ulrich DALLMANN, “Niklas Luhmann’s System Theory as a Challenge for Ethics”, **Ethical Theory and Moral Practice**, C.1, S.1, Y.1998, s.85- 102. Ona göre her insan ancak belirli bir veri profilini kendi etkinliği olarak işlediği bir role sahipse sistem içerisinde iletişim kurabilir. Bu nedenle kişi ve rol ayrılmalıdır ve roller kişilere göre belirlenmelidir. Alessandra Di MARTINO, **Datenschutz im europäischen Recht**, Nomos, Baden-Baden 2005, s. 21-22.

²⁸ Reg WHITAKER, s. 40-41.

iki şekilde gerçekleşir. İlki altların çalışmalarının üstleri tarafından doğrudan denetlenmesidir. İkincisi ise daha zor fark edilen bir nitelik taşır, ancak aynı oranda önemlidir: çalışanlar hakkında dosyalar tutulması, kayıtların incelenmesi, geçmişlerinin değerlendirmesi gibi etkinlikler bu kapsamda yer alır. Çalışanlara ilişkin kayıtlar çoğu zaman geçmiş çalışmalarını, kişisel bilgilerini ve karakterlerine ilişkin değerlendirmeleri içerir. Giddens, bu tür kayıtların modern örgütlenmeler açısından önemini Weber'in de fark ettiğini, ancak bunların davranışları düzenleme konusunda ne kadar etkili olduklarını ortaya koyamadığını söyler²⁹.

Giddens, maddi zenginliği oluşturan asıl aracın nüfusu düzenlemek için kullanılan bilginin toplanması ve depolanması olduğu görüşündedir: *“Bilgi depolama, ‘otorite kaynaklarının’ kabile kültürlerinden çok daha geniş mekan ve zaman alanlarını kapsayan sosyal sistemlerin yapılanmasındaki rolü açısından temel önem taşımaktadır. Gözetleme-bilgi denetimi ve bazı grupların faaliyetlerinin diğerleri tarafından denetlenmesi-sonradan bu tür kaynakların genişlemesi için anahtar rolünü oynamaktadır”*³⁰. Ona göre, gözetim, ulus devlet yapılanmasının içerdiği otorite kaynaklarına odaklanmasının yanında kaynağını endüstriyel kapitalizmde bulan ve *“içsel uzlaş”* (internal pacification) olarak tanımlanabilecek geniş çaplı bir dönüşümün de işaretidir. *“İçsel uzlaş”*, bizi *“şiddet”* konusunda düşünmeye zorlayan sorular ortaya koyar³¹. Öte yandan, güç ve denetim, kapitalist toplum yapısının uyumluluğu ve üretkenliği için kilit öneme sahip bir başka gereklilikle, planlama ve yönetimle de yakından ilişkilidir³².

c. Disiplin ve Gözetim

Gözetimin ayrı bir olgu olarak dikkate alınmasında asıl büyük etkiyi Michel Foucault'nun görüşlerinin yarattığı söylenebilir. Foucault gözetimi, yalnızca örgütlerdeki değil, tüm toplumdaki daha geniş bir disiplin bağlamında değerlendirir

²⁹ Anthony GIDDENS, **Sociology**, Polity Press, 2. Baskı, Birleşik Krallık 1994, s. 300.

³⁰ Anthony GIDDENS, **The Nation-State and Violence (Volume Two of a Contemporary Critique of Historical Materialism)**, Polity Press, Birleşik Krallık 1996, s.2.

³¹ Anthony GIDDENS, **The Nation-State and Violence**, s.181.

³² Kevin ROBINS, Frank WEBSTER, **Times of the Technoculture, From the Information Society to the Virtual Life**, Routledge, İngiltere 1999, s. 92.

ve gözetimin bürokratik örgütlenmenin sınırlarını aşan yapısına işaret eder. Bu nedenle Foucault'nun analizlerine gözetimin sosyal yapısına ilişkin çalışmalarda sıklıkla başvurulması şaşırtıcı değildir³³.

Foucault görüşlerini özellikle Jeremy Bentham'ın hazırladığı bir hapishane mimarisi planından, "*panoptikon*"dan hareketle açıklamıştır³⁴. Daha sonra bu mimarinin temelinde yatan mantığın fabrika ve okul için de geçerli olabileceğini savunacaktır³⁵. Bu yapının dış çevresinde halka halinde bir bina, merkezde ise bir kule yer alır. Bentham'ın ayrıntılı olarak açıkladığı bu yapılanmada, düzen öyle sağlanmıştır ki mahkumların, kendilerini gardiyanların ne zaman izlediğini bilmeleri olanaklı değildir. Panoptik hapishanenin gücü işte tam da bundan kaynaklanır, çünkü bu yapılanmada gözetlenenlerin sürekli görünürlüğü ve gözetleyenlerin sürekli görünmezliğinin bir bileşimi söz konusudur³⁶. Foucault'nun deyimiyle; "*görünürlük bir tuzaktır. (...) Görülmekte, ama görememektedir; bir bilginin nesnesidir ama asla bir iletişim öznesi olamamaktadır*"³⁷. Foucault, panopticon'u modern devletin toplumu disipline etme amacının temel mantığı olarak açıklamıştır³⁸.

Foucault'ya göre, modern toplum, "*disipliner bir toplum*"dur. Bu toplumda iktidar teknikleri ve stratejileri her zaman varolmuştur. Bunlar, ilk başta ordular,

³³ Toplum ve gözetim açısından Foucault'nun görüşlerini farklı açılardan değerlendiren bir derleme için bkz. "Foucault and Panopticism Revisited", **Surveillance & Society**, C.1, S.3, <http://www.surveillance-and-society.org/journalv1i3.htm> (s.y. 23 Kasım 2008).

³⁴ Foucault'nun Panoptikon değerlendirmeleri için ayrıca bkz. Abdurrahman SAYGILI, "Mikro-İktidarın Bir Fiziği: Hapishane", **AÜHFD**, C.53, S.2, Y.2004, s.186-196.

³⁵ Ancak örneğin Giddens'a göre Foucault, hapishane ve fabrika arasındaki ilişkiyi fazla abartmıştır: "*Kapitalizmin ilk yıllarında bazı işverenlerin iş disiplinini pekiştirmek için bilinçli bir biçimde model olarak hapishanelere baktıklarına şüphe yoktur. Bazen fiilen köle emeği kullanılmıştır. Ama hapishane ile fabrika arasında iki temel fark vardır. "Çalışma" hapishane dışındaki bireylerin günlük hayatlarını işgal eden (normalde en fazla zamanını götürse de) sektörlerden yalnızca birini oluşturur. Çünkü kapitalist işyeri, Goffman'ın terimiyle bir total kurum değildir; oysa hapishane böyledir, klinik ve hastane ise böyle olabilir. Daha da önemlisi, işçi fabrikaya ya da büroya zorla hapsedilmiş değildir., işyerinin kapısından içeriye "özgür ücretli emek" olarak girer. Bu da formel olarak "özgür" bir iş gücünün "yönetilmesi" ile ilgili tarihsel olarak özgül sorunlara yol açar; Pollard'ın başta olmak üzere bu konuyu analiz eden ilginç çalışmalar vardır. Aynı zamanda, hapishane disiplininin normal işleyişinin bir parçası olmayan işçi direnişi biçimlerine (özellikle sendikalaşma ve kolektif olarak işten el çekme tehdidi) de kapı açar. Foucault'nun disiplinin ürettiğini söylediği "uysal bedenler" sık sık o kadar da uysal olmadıklarını ortaya koyarlar". Anthony GIDDENS, **Siyaset, Sosyoloji ve Toplumsal Teori**, Metis, İstanbul 2000, s.274.*

³⁶ Zygmunt BAUMAN, **Küreselleşme, (Toplumsal Sonuçları)**, Ayrıntı, 2. Baskı, İstanbul 2006, s. 42- 43.

³⁷ Michel FOUCAULT, **Hapishanenin Doğuşu, Gözetim Altında Tutmak ve Cezalandırmak**, çev. Mehmet Ali KILIÇBAY, 3. Baskı, İmge, Ankara 2006, s.295-296.

³⁸ Foucault'nun görüşlerinin teknolojik gelişmeler neticesinde günümüz koşulları içerisinde değerlendirilmesi aşağıda yapılacaktır. Bkz. Bölüm I, D-3.

hapishaneler, fabrikalar gibi belirli kurumlar içinde gelişmeler bile etkileri sosyal yaşamın dokusuna işler. Modern toplumlarda, toplumsal normlara boyun eğmelerini sağlamak için insanlar, giderek daha fazla gözetlenir. İnsanların hareketleri belgelenir ve sınıflandırılır. Tüm bu bilgiler özünde iktidarla ilişkilidir³⁹.

O halde şöyle söylenebilir: modern devlet (ve diğer modern örgütlenmeler) verimliliği arttırmak ve hedeflerini gerçekleştirmek için kişisel verilere gereksinim duyar. Bunun için geliştirilen çeşitli sistemler ve araçlar, gözetim, denetim, disiplin ve yönlendirme gibi toplumun tamamı üzerinde bir değişim yaratabilecek etkileri de beraberinde getirebilir.

Modern örgütlenmenin bu özellikleri, ilk aşamada kamusal yönetimin, toplumsal sistem içinde gücü tartışılmaz bir bilgi hazinesine, bir anlamda “*en güçlü bilgi tekeline*”⁴⁰, kavuşmasına neden olmuştur. Kapitalist işletmeler de bilgi kaynaklarını ve değerlendirme yeteneklerini her geçen gün biraz daha geliştirmiştir. İster devletten, ister kapitalist işletmelerden kaynaklansın iktidar oluşturmak amacıyla bilginin gücüne duyulan bu gereksinim ve bağımlılık, bilişim teknolojilerinin gelişmesi dolayısıyla, özellikle 1980’lerde sonra kullanılan, bir deyim, “*bilgi toplumu*”nun aslında modern dönemin bir bileşeni olduğunu ortaya koymaktadır⁴¹.

C. TEKNOLOJİDEKİ GELİŞMELER-ELEKTRONİK GÖZETİM

Kişisel verilerin korunması, ileri sanayi toplumlarının sosyal ve ekonomik yapısının ciddi bir dönüşüme uğradığı dönemde gelişmeye başlamıştır. Özellikle son yirmi yıldan beri pek çok alanda ileri teknoloji kullanılmaktadır. Bu gelişmeler dolayısıyla oldukça güçlü ama sessiz bir devrimin yaşandığı söylenebilir⁴². Pek çok

³⁹ David LYON, **Elektronik Göz**, s. 44.

⁴⁰ Tekin AKILLIOĞLU, “Yönetimde Açıklık-Gizlilik ve Bilgi Alma Hakkı”, **AÜSBFD**, C.46, S.3-4, Haziran-Aralık 1991, s. 1.

⁴¹ David LYON, **Elektronik Göz**, s. 45; Kevin ROBINS, Frank WEBSTER, **Times of the Technoculture, From the Information Society to the Virtual Life**, Routledge, Büyük Britanya 1999, s. 91.

⁴² James D. DANZIGER, William H. DUTTON, Rob KLING, Kenneth L. KRAEMER, **Computers and Politics, High Technology in American Local Governments**, Columbia University Press, ABD 1982, (William H. DUTTON, James N. DANZIGER) s. 1.

özelliğinin yanında bu yeni dönemde “bilgi”ye sahip olmak da merkezi bir öneme kavuşmuştur⁴³. “Bilgi toplumu”⁴⁴, “üçüncü dalga”⁴⁵ ya da “endüstri sonrası toplum”⁴⁶ gibi hangi ifade ile adlandırılırsa adlandırılırsın içine girdiğimiz yeni dönemde temel vurgunun “bilgi”ye yapıldığı açıktır. Bilgi toplumuna ilişkin değerlendirmelerde ise verilerin korunması kilit öneme sahiptir⁴⁷. Hatta kişisel verilere ilişkin sorunlar “bilgi toplumunun yumuşak karnı” olarak nitelendirilebilir⁴⁸.

Modernliğin ilk çağlarından itibaren “bilgi”ye duyulan gereksinim ve bu doğrultuda bireylerin yaşamlarına ilişkin çok çeşitli verilerin toplanması ve değerlendirilmesi isteği özellikle 20. yüzyılda yaşanan gelişmeler sonucunda dönüşüme uğramıştır. Dönüşümün nedeni ise, teknolojiye, özellikle de bilişim teknolojilerindeki gelişmeler sonucunda o zamana kadar tatmin edilmesinde pek çok güçlüklerle karşılaşılın bu isteğin, giderek daha da kolayca elde edebilen bir gerçeklik haline gelmesidir. Artık kişilere ilişkin çok daha fazla sayıda veri toplanabilmekte ve birbirleri ile ilişkilendirilebilmektedir. Bu değişim, teknolojik gelişmeler ile sosyal, yönetsel ve siyasal kararların, karşılıklı olarak birbirini etkileyen, dinamik yapısının

⁴³ Colin J. BENNETT, **a.g.e.**, s. 14.

⁴⁴ Örneğin Naisbitt yaşamlarımızı değiştiren on yeni yönelimden birini sanayi toplumundan bilgi toplumuna yönelim olarak belirlemiştir. Bkz. John NAISBITT, **Megatrends, Ten New Directions Transforming Our Lives**, Warner Books, ABD 1988. Naisbitt bu eserinde kullandığı “bilgi içinde yaşıyoruz ve bilime büyük açlık duyuyoruz” saptamasının sonraki dönemde de devam ettiğini, bilgideki büyümenin yalnızca hız kazandığına ve yeni bin yıla ilişkin büyük eğilimlerin de bilgi birikimindeki hızlı artışla ilişkili olduğuna 2000’lerdeki büyük eğilimlere ilişkin kitabında da işaret etmiştir. John NAISBITT, Patricia ABURDENE, **Megatrends 2000, Ten New Directions for the 1990’s**, William Morrow and Company, Inc, ABD 1990. Ayrıca bkz. Manuel CASTELLS, **Enformasyon Çağı: Enformasyon Çağı, Ekonomi, Toplum ve Kültür**, I. ve II. Cilt, çev. Ebru KILIÇ, 2. Baskı, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2004; Frank WEBSTER, **Theories of the Information Society**, Routledge, 1995; James R. BENIGER, **The Control Revolution, Technological and Economic Origins of the Information Society**, Harvard University Press, ABD 1989; Marie-Theres TINNEFELD, Eugen EHMANN, Rainer W. GERLING, **Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht**, 4. Baskı, Oldenbourg Verlag, Almanya 2005, s.6-18.

⁴⁵ Alvin TOFLER, **Üçüncü Dalga**, çev. Ali SEDEN, Altın Kitaplar Yayınevi, İstanbul 1981.

⁴⁶ Daniel BELL, **The Coming of Post-Industrial Society**, Basic Books, ABD 1973; Alain TOURAINE, **Return of the Actor, Social Theory in Postindustrial Society**, University of Minnesota Press, ABD 1988; Yoneji MASUDA, **The Information Society as Post-Industrial Society**, 2. Baskı, World Future Society, ABD 1983; Krishan KUMAR, **From Post-Industrial to Post-Modern Society, New Theories of the Contemporary World**, Blackwell, Büyük Britanya 1997.

⁴⁷ Pelopidas K. DONOS, **Datenschutz, Prinzipien und Ziele, Unter Besonderer Berücksichtigung der Entwicklung der Kommunikations- und Systemtheorie**, Nomos, Almanya 1998, s.19.

⁴⁸ Ceylin, BEYLİ, “Bilgi Toplumunda Kişisel Veriler- Kişisel Verilerin Korunması Kanun Tasarısı Üzerine Eleştiriler”, **Bilişim Hukuku**, Der. Mete Tevetoglu, Kadir Has Üniversitesi Yayınları, İstanbul 2006, s.70.

bir sonucu olarak ortaya çıkmıştır. Güçlü devletin karmaşık yapısı ve bilişim teknolojilerindeki ilerleme birbirine bağımlı ve paralel ilerleyen süreçleri ifade eder⁴⁹.

Konumuz açısından, birbiriyle yakından ilişkili, önemli teknolojik gelişmeler üç döneme ayrılarak incelenebilir: (i)bilgisayarın ortaya çıkışı ve veri bankalarının kurulması, (ii)İnternet'in yaygın kullanımına başlanması, (iii) gözetime yönelik yeni araçların gelişmesi.

1. BİLGİSAYAR VE MERKEZİ VERİ BANKALARI

Veri koruma yasalarının ortaya çıkışı, bilişim teknolojilerinde, özellikle de 1950'li yıllarda bilgisayarların⁵⁰ ortaya çıkışı ile başlayan gelişim dikkate alınmadan açıklanamaz. Her ne kadar veri koruma yasalarının özünü oluşturan değerlerin kökleri çok daha eskilere dayansa da bu düzenlemelerin ortaya çıkışında bir anlamda bilişim teknolojilerindeki gelişmeye yönelik bir tepkinin etkili olduğu açıktır⁵¹. Bu noktada ise ilk adımı bilgisayarların ve veri bankalarının ortaya çıkışı oluşturur. Öyleyse şu soru yanıtlanmalıdır: hızla gelişen ve gelişmeye devam eden bilişim teknolojileri ne getirmiştir ki, bu yıllarda verilerin korunması yönünde yasal düzenlemeler yapılması aciliyet kazanmıştır?

Başta bilgisayarlar olmak üzere, yeni teknolojilerin değiştirdiği şey temelde, işin yapılabilirliğine ilişkindir. Teknolojinin sunduğu olanaklar ile verilerin toplanması, işlenmesi, saklanması ve birbirleri ile ilişkilendirilmesinin daha hızlı,

⁴⁹ Colin J. BENNETT, s. 21.

⁵⁰ Bilgisayar, Türk Dil Kurumu tarafından, “çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç” olarak tanımlanmaktadır. Bkz. **Türk Dil Kurumu, Milliyet Türkçe Sözlük**, C.1, İstanbul 1992, s. 187. Bilgisayar ilk ortaya çıktığı günlerin aksine artık yalnızca hesap yapma makinesi olmanın çok daha ötesinde bir yapı sergilemektedir. “Bilgisayar teknolojisi insanların(örneğin, kullanıcılar, bilgisayar uzmanları, yöneticiler) oluşturduğu karmaşık, bağımsız bir sistemi, ekipmanı (donanım olarak örneğin, ana kasa ve yanbirimler; yazılım olarak örneğin, işletim sistemleri, uygulama programları ve veriler) ve teknikleri (örneğin, işlem, uygulama ve ayarları) içermektedir”. Bkz. James D. DANZIGER ve diğ., (William H. DUTTON, James D. DANZIGER)s. 4-5.

⁵¹ Lee A. BYGRAVE, s. 93. XIX. yüzyıl öncesinde çok az sayıda kayıdın kamusal organlarca tutulduğu görülmektedir. Bunların büyük bir bölümü ise sınırlı bir alana ilişkin olarak tutulmaktadır. Özellikle hristiyan inancının yaygın olduğu toplumlarda bu kayıtlar kiliseye bağlı kuruluşlarca tutulmuştur. Bkz. Daniel J. SOLOVE, **The Digital Person**, s. 13.

daha kapsamlı ve daha kolay bir hâle gelmiştir⁵². Bunun yanında dönemsel bir gerçeklikten de söz etmek gerekir.

1950’li ve 1960’lı yıllarda bilgisayarlar günümüzde alıştığımızdan çok daha farklı bir nitelikteydi. Büyük, karmaşık, kullanımı zor bu makineler, maliyetleri nedeniyle de yalnızca büyük şirketlerin ve devletlerin kullanımındaydı⁵³. Bir başka anlatımla henüz kullanımı yaygınlaşmamış bu teknolojiler, merkezî güçlerin elindeydi. Bu ise teknolojiyi kullanabilen kuruluşlarda bir güç yoğunlaşmasından çekinilmesine neden oldu.

Bu kaygıda verilerin merkezileştirilmiş veri bankalarında⁵⁴ toplanmalarının olanaklı duruma gelmesi de etkilidir. Toplanan verilerdeki büyük artış, “*veri ambarları*”nın (data warehouse) oluşmasına neden olmuştur ve bunlar, çok büyük miktarda bilgilerin bir yerde toplanması ve saklanması temeline dayanır⁵⁵. Toplanan verilerin niceliksel artışı, bunların içerisinde kullanışlı olanların bulunmasını zorlaştırmaktadır. Bu zorluğun “*veri madenciliği*” (data mining) ile aşıldığı görülür. “*Veri madenciliği*”, çeşitli bilgi parçaları arasında şimdiye kadar tahmin edilemeyen ilişkilerin kurulmasını olanaklı hâle getirmektedir⁵⁶.

⁵² Arthur R. MILLER, *The Assault on Privacy, Computers, Data Banks, and Dossiers*, The University of Michigan Press, ABD 1971, s. 216 vd.

⁵³ Harry HENDERSON, s. 13.

⁵⁴ Veri bankası, genellikle belirli bir konuda, bilgisayar dosyalarında büyük miktarda verinin depolanmasına ilişkin olarak kullanılan genel bir ifadedir. Bkz. Tony GUNTON, *Dictionary of Information Technology and Computer Science*, Penguin, Büyük Britanya 1992. Bunun yanında AK’nin bir kararında elektronik veri bankası “kişisel bilgileri tutmak ve bunları yaymak için kullanılan herhangi bir veri işleme sistemi” olarak tanımlanmıştır. **Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector**, s. 1. Veri bankası ile veri tabanı deyimleri genellikle birbirlerinin yerine kullanılmaktadır. Ancak aralarında, ufak da olsa, bir ayrım bulunduğu söz edilebilir. Buna göre veri ya da bilgi bankası, “[b]elli bir konuda (spesifik) bilgi içeren ve özel yazılımıyla bu bilgilere ulaşma olanağı sağlayan bilgi yığını yada bilgi sistemidir. Bilgi bankalarını, veri tabanlarından ayıran özellik, daha küçük çaplı ve spesifik olmalarıdır”. Bkz. Faruk ÇUBUKÇU, *Bilgisayar Terimleri Sözlüğü*, V Yayınları, Ankara 1987, s.24. Bunun yanında konumuz açısından, insanlara ve onların çevresine (nüfus veya ekonomi gibi) ilişkin olgular havuzu olarak da tanımlanabilir. James D. DANZIGER ve diğ., (Kenneth L. KRAEMER, William H. DUTTON) s. 174. Veri bankası ve tabanı arasındaki farklılık ve çeşitli tanımlardan seçmeler için bkz. Frits W. HONDUS, *Emerging Data Protection in Europe*, North-Holland Publishing Company, Hollanda 1975, s. 91-96.

⁵⁵ Veri ambarı en genel şekliyle, “*karar destek uygulamaları için tasarlanan bir ortam*” olarak tanımlanabilir. Bu anlamda karar destek sistemlerinin teknik altyapısını oluşturmakta, yeni veriler yanında, artık kullanılmayan eski verileri de kullanılabilir ve çözümlenebilir duruma getirmektedir. Bkz. *Türkiye Bilişim Ansiklopedisi*, haz. Tuncer ÖREN, Tuncer ÜNEY, Rıfat ÇÖLKESEN ve diğ., Papatya, İstanbul 2006, s. 879-883.

⁵⁶ Louise CADAUX, s.120. Veri madenciliği, geniş veri tabanlarından kullanışlı bilgilerin çıkarılma süreci olarak tanımlanabilir. *Dictionary of Computer and Internet Words*, Houghton Miffling Company, ABD 2001, s.68. Bir sistem içinde yararlı örüntülerin bulunması işleminin

1960'lı ve 1970'li yıllarda, bürokratların, çeşitli yerlerde bulunan dağınık bilgilerin tek merkezde toplanmasının sağlayacağı yararları görmeleri ve elbette bilişim teknolojilerinin bunu olanaklı kılması ile pek çok devlet, merkezi veri bankaları kurulması yönünde girişimlerde bulunmuştur⁵⁷. Aynı dönemde tartışılmaya ve uygulamaya başlanan her yurttaş için bir kimlik numarasının belirlenmesi de veri korumaya ilişkin tartışmaların alevlenmesine neden olur. Bu dönemde pek çok soruyu beraberinde getiren bir diğer uygulama ise, nüfus sayımlarında otomatik sistemlerin kullanılmasıdır⁵⁸.

Kamunun gösterdiği duyarlılık, bu gelişmelerin özel yaşamın gizliliği ve bireysel özerklik gibi temel değerlere saldırı oluşturma potansiyeli ile çoğulcu demokratik toplum yapısının sarsılması korkusundan kaynaklanır⁵⁹. Artık kişisel bilgiler, yakınların hatıralarından ya da çeşitli kurumların tozlu arşivlerinde yer bulan dosyalardan hızla bilgisayar ortamına aktarılmaya başlanmıştır. 1960'lı yılların başından itibaren kamunun, düşünürlerin, hukukçuların ve çeşitli yazarların hızla yaygınlaşan bilgisayar kullanımının özel yaşam üzerinde yaratabileceği tehlikelere dikkatle yaklaşması bu nedenledir⁶⁰.

Ancak zaman içerisinde bilgisayarlar yalnızca gelişmiş örgütlerin elindeki bir araç olmaktan çıkmış ve yaygınlaşmıştır. Ancak kişisel verilerin korunmasına ilişkin bilgisayar sistemlerinin taşıdığı önem azalmamış, hatta bilgisayarlar yaygınlaştıkça kişisel verilerin korunması gerekliliği daha da artmıştır. Bu ilk olarak, kayıt altında tutulan kişisel verilerin sayısal artışından kaynaklanır. Yeni teknolojilerin getirdiği dört temel özelliğin verilerin sayısal artışına etki ettiği söylenebilir⁶¹:

- (i) Bilgileri oluşturmak, işlemek, yaymak ve saklamak daha önce hiç olmadığı kadar kolay hale gelmiştir;
- (ii) Üstelik bu işlemler elektronik ortamda eskisinden çok daha düşük maliyetlere yapılabilir;

veri madenciliği yanında, veri harmanlama (data harvesting), VTBK gibi farklı adlarla anıldığı da görülmektedir. Bkz. **Türkiye Bilişim Ansiklopedisi**, s. 883-887.

⁵⁷ Çeşitli örnekler için bkz. Colin J. BENNETT, s.46-49.

⁵⁸ Colin J. BENNETT, s. 49-53.

⁵⁹ Lee A. BYGRAVE, **Data Protection Law**, s. 95.

⁶⁰ Daniel J. SOLOVE, **The Digital Person**, s. 15.

⁶¹ Fred H. CATE, **Privacy in the Information Age**, Brookings Institution Press, ABD 1997, s. 14-16.

- (iii) Günümüz bilgi toplumunda elektronik ortamda tutulan bilgiler, elle yazılı olanlara göre daha değerli bir hale gelmiştir, çünkü bu şekilde tutulan verilerin toplanması, saklanması, işlenmesi ve kullanılması çok daha kolaydır;
- (iv) Bilgisayar sistemleri ve ağlar, kendine özgü nitelikleri dolayısıyla daha fazla bilginin varlığına katkıda bulunmaktadır⁶².

Günümüzde hâlen en önemli gözetim aracının, toplanan verilerin saklanması, eşlenmesi, geri getirilmesi, işlenmesi, pazarlanmasına olanak tanıyan bilgisayarlar olduğu söylenebilir. Veriler, yalnız sayıların ve isimlerin ötesinde DNA kodları, fotoğraflar ve ses kayıtlarına kadar uzansa da, gözetlemenin gerçekleşebilmesini sağlayan teknolojiler bilgisayar gücü içerir. Bu nedenle bilişim teknolojilerini gözetlemenin merkezine koyan şeyin bilgisayar teknolojisindeki büyüme ve uygulama alanlarının genişlemesi olduğu rahatlıkla söylenebilir. Pek çok sıradan işlemi gerçekleştirmek ya da bunların verimliliğini arttırmak için gereksinim duyulan bu tarz gözetleme, modern yaşamın da kilit özelliğidir⁶³.

Devletin elinde bulunan veri tabanları dışında, kredi kartı yada telefon veritabanları gibi ticari nitelik taşıyanlar da kullanılarak, artık yurttaşların bir araya getirilen (tümleşik) profillerinin oluşturulması olanaklı duruma gelmiştir ve bu yönetime giderek daha sık başvurulmaktadır. Artık farkında olalım ya da olmayalım bilgisayar ağları içinde çeşitli sayılarla formüle edilmiş benlikler, bilgisayar koridorlarında her geçen gün biraz daha ayrıntılı resimler oluşturmaktadır.

Bizi en ayrıntılı şekilde tasvir eden resmin oluşturulmasında kamu sektörü ile özel sektör arasındaki bilgi akışı da dikkate değerdir. Daniel J. Solove'a göre bu "*dijital siciller*" üç çeşit bilgi akışı üzerine kurulmakta ve kullanılmaktadır. Buna göre edinilen bilgiler:

- (i) Özel sektör kuruluşları arasında;
- (ii) Kamu sektöründen özel sektöre;
- (iii) Özel sektörden kamu sektörüne sürekli bir akış halindedir⁶⁴.

⁶² 1990'lı yılların ortalarında bir MIT araştırma takımı yeni teknolojilerin ürettikleri veri miktarının her yirmi ayda iki katına çıktığını hesaplamıştır. Louise CADAUX, "Privacy: Our Future Under Close Surveillance", **Freedom of Expression (And New Communication Technologies)**, Haz. Mich  l   PAR  , Peter DESBARATAS, IQ Collectif, Kanada 1998, s.114.

⁶³ David LYON, **G  nl  k Hayatı Kontrol Etmek**, s. 13.

⁶⁴ Daniel J. SOLOVE, **The Digital Person**, , s. 3.

Kişilerin mâlî durumlarından, sağlık kayıtlarına, tüketim tercihlerinden yaşam alanı içindeki pek çok davranış biçimine; eğitim, etnik köken, ikamet yeri gibi bilgilere, sosyal yardım almaya uygunluk durumu ya da suç oluşturan faaliyetlere, bilgisayarsız gözetim sistemleri ile olanaklı olmayacak ölçüde kolaylıkla ulaşılabilmektedir. Bu da gözetim kapasitesinin yeni teknolojilerin kullanılması ile arttığını ortaya koymaktadır. Üstelik özellikle İnternet sayesinde, hem görevleri hem de yerleri açısından birbirine uzak olan örgütlerin ellerinde bulunan verilere kolaylıkla ulaşılabilmesi ve bunların karşılaştırılması da olanaklıdır⁶⁵. Artan oranda veri saklama ve işleme kapasitesi yanında bir başka gerçek, teknolojinin niteliği dolayısıyla, kişisel bilgileri denetim altında tutmanın sanal dünyada gerçek dünyadakinden çok daha zor olmasıdır⁶⁶.

2. İNTERNET

Kişisel verilerin toplanması ve işlenmesi açısından teknolojik gelişmelerin etkisini değerlendirirken ilk önemli dönüm noktasının bilgisayarların ve veri bankalarının ortaya çıkması olduğundan söz ettik. İkinci büyük dönüşümü ise İnternet'in gelişmesi ve yaygınlaşması yaratmıştır⁶⁷. Gerçekten İnternet'in ve İnternet'le ilişkili diğer teknolojilerin (world wide web, e-posta, haber grupları gibi...) kullanımının yaygınlaşması ile bilişim teknolojileri de yeni bir döneme girmiştir. “Ağların ağı” İnternet, 20. yüzyılda hızla yaşamımızın içine girmiş, 21. yüzyılda ise kaçınılmaz olarak bir parçası haline gelmiştir. Bilgisayarların

⁶⁵ David LYON, **Elektronik Göz**, s. 120; Bruce Schneier, **a.g.e.**, s.33.

⁶⁶ Patricia L. BELLIA, Paul Schiff BERMAN, David G. POST, **Cyberlaw, Problems of Policy and Jurisprudence in the Information Age**, Thomson-West, 2. Baskı, ABD 2003, s. 605.

⁶⁷ İnternet deyimi, “*international*” (uluslararası) ve “*network*” (ağ yapısı) kelimelerinin birleştirilmesiyle oluşturulmuştur. Bu nedenle en genel şekliyle uluslar arası ağların ağı olarak tanımlanabilir. Karmaşık yapısı ve birbirinden farklı pek çok alanda kullanılması nedeniyle öğretide ve yargı kararlarında değişik tanımlarının yapıldığı görülmektedir. Birkaç örnek için bkz. Doe v. Roe, 955 P.2d 951, 956 (Arizona 1998)’dan aktaran James MAGEE, **Freedom of Expression**, Greenwood Press, ABD 2002, s. 277; US Court of Appeals, Whirlpool Financial Corporation v. GN Holdings, 28 Eylül 1995’den aktaran Yavuz KAPLAN, **İnternet Ortamında Fikri Hakların Korunmasında Uygulanacak Hukuk**, Seçkin, Ankara 2004, s. 23; Robert E. KAHN, Vinton G. CERF, “What is the Internet (and What Makes it Work)”, Aralık 1999, <http://www.policyscience.net/cerf.pdf> ; “FNC Resolution of ‘Internet’”, 24 Ekim 1995, http://www.itrd.gov/fnc/Internet_res.html . İnternet’in gelişimine ilişkin olarak bkz. Katie HAFNER, Matthew LYON, **İnternet Tarihi: Sihirbazların Gecelediği Yer**, çev. Sinem YAZICIOĞLU, Güncel, İstanbul 2000. Günümüzde İnternet’in yaklaşık bir buçuk milyar kullanıcısı olduğu tahmin edilmektedir. Bkz. Internet Usage Statistics, The Internet Big Picture, <http://www.internetworldstats.com/stats.htm> . Çin’de İnternet kullanımına ilişkin ilgi çekici bir değerlendirme için bkz. “Dauerlauf gegen in die Sucht”, **Der Spiegel**, S. 35, Y. 2009, s. 136-138.

birbirlerine bağlanması ile tamamen farklı veri tabanları arasında paylaşım, ilişkilendirme ve birleştirme olanaklı duruma gelmiştir. Ancak İnternet'in etkileri yalnızca bunlarla da sınırlı kalmamaktadır.

Dünyanın gittikçe daha da küçülen bir bölümü dışında başta İnternet olmak üzere elektronik iletişim günlük yaşantılarımızda gittikçe daha geniş yer almaktadır. Artık metinler, kelime işlemcilerle oluşturulmakta, bilgisayar hafızalarında saklanmakta, yerel ağlar, telefon hatları, uydular üzerinden iletilmekte, faks, yazıcı ve bilgisayar ekranları aracılığıyla görülmektedir. Metinler, görüntüler ve sesler; kameralar, tarayıcılar, mikrofonlar tarafından kayda alınmakta, hafıza kartlarında, disklerde, teyplerde saklanmakta, havadan ya da fiber optik kablolardan yayınlanmakta, cep telefonunda, televizyonda, bilgisayarda gösterilmektedir. Bir başka anlatımla sanayileşmiş dünyamızda bilgi büyük oranda elektrondur⁶⁸.

İnternet ortamındaki her hareketimiz veri üretir⁶⁹. Bu ise biz farkında bile olmada iletişimin izlenmesine kişisel verilerin toplanmasına neden olabilir. Nitekim son yıllarda İnternet kullanıcıları, bilgisayar ekranının bir tabela ya da aynadan çok bir pencere olduğunu giderek daha çok fark etmeye başlamıştır. Kullanıcılar çeşitli bilgileri aradıkça ve tercihlerde bulundukça, onlar hakkındaki bilgiler de dışarıya akıp veri tabanlarında toplanmaktadır⁷⁰. Özellikle ticari hedeflere hizmet eden bu bilgiler temel olarak iki şekilde elde edilmektedir.

Birincisi web siteleri doğrudan ve açıkça kullanıcılarından bu bilgileri toplamaktadır. Pek çok siteyi kullanabilmek için kayıt olmak gerekmekte ve bu kayıt işlemi sırasında da çoğunlukla kullanıcı adı ve şifre bilgisi yanında çeşitli soruları içeren formların doldurulması gerekmektedir⁷¹. Bu durumda kişisel bilgilerin

⁶⁸ Fred H. CATE, **Privacy in the Information Age**, Brookings Institution Press, ABD 1997, s.6. Ayrıca bkz. Jeffrey ROSEN, **The Unwanted Gaze, The Destruction of Privacy in America**, Vintage Books, ABD 2001, s.159-195.

⁶⁹ Lawrence LESSIG, **Code Version 0.2.**, s. 216.

⁷⁰ Harry HENDERSON, s. 4. Kullanıcıların İnternet üzerindeki hareketlerine ilişkin kayıtların tutulması ve bunların kişisel verilerin korunması açısından yaratacağı sorunlara ilişkin olarak bkz. Daniel B. GARRIE, Rebecca WONG, "The Future of Consumer Web Data: A European/US Perspective", **International Journal of Law and Information Technology**, Y. 2006, C.15, S.2, s. 129-152. İnternet ortamında tüketicilerin özel yaşamlarının gizliliği hakkını korumada, kişisel verilerin korunması hukukunun yetersiz kalmasına ilişkin bir tartışma için bkz. Lilian EDWARDS, "Reconstructing Consumer Privacy Protection On-line: A Modest Proposal", **International Review of Law, Computers and Technology**, Y.2004, C. 18, S. 3, s. 313-344. Ayrıca bkz. Peter SCHAAR, **Datenschutz im Internet, Die Grundlagen**, Verlag C.H. Beck, Almanya 2002.

⁷¹ Daniel J. SOLOVE, **The Digital Person**, s.23.

ilgilinin rızası ile dolaşıma girdiği görülür. Ancak acaba bir kullanıcı örneğin İnternet üzerinden kitap sipariş verirken ilgilendiği konulara ilişkin doldurduğu bir formun, başka sitelerde karşısına çıkan reklamların içeriği ile doğrudan ilişkili olabileceğinin farkında mıdır?

Bu çalışma içerisinde açıklanmaya çalışılacak kişisel verilerin korunması düzenlemeleri verilerin üçüncü kişilerle paylaşımına ilişkin bazı sınırlamalar öngörmektedir. Ancak uygulamada bunlar çoğu zaman yeterli olmamaktadır. Nitekim verilerin ilk elden iletildiği İnternet sitesi bu bilgileri başka şirketlere aktarmasa bile hami şirketi içerisinde yer alan başka kuruluşlara iletebilmektedir.

İkinci olarak İnternet üzerinde gezinirken kişisel bilgilerin bazıları kullanıcının bilgisi ve onayı olmaksızın gizlice toplanabilmektedir. Bunun bir yolu IP adresinin izlenmesi iken, bir diğer yolu “çerez”lerin (cookies) kullanımıdır⁷². Çerezler, ticarî sitelere hedef tüketicilerini saptayabilmek için büyük bir kolaylık sağlar, ancak bunun yanında İnternet’teki davranış biçimlerini gözlemleyebilmek için akademisyenlerce kullanıldığı da bilinmektedir⁷³. Çerezler, kullanıcının İnternet üzerinde gezdiği siteler hakkında bilgi sahibi olmaya yardım eder. Bu ise kullanıcın kişisel eğilimlerini ortaya koyan profilinin çıkarılmasını sağlayabilir⁷⁴.

⁷² Alessandra Di MARTINO, **Datenschutz im europäischen Recht**, Nomos, Almanya 2005, s. 20. Çerez, web tabanlı bir bağlantıda bağlantının sunucu tarafının, kullanıcı tarafındaki bilgileri almasını ve saklamasını sağlayan bir tekniktir. Bir başka ifadeyle çerez, kullanıcı bir web sitesini ziyaret edildiğinde kullanıcının bilgisayarına yerleştirilen ve kullanıcı bir daha o siteyi ziyaret ettiğinde sitenin sunucusu tarafından erişilebilen ve okunabilen bir metin dosyasıdır. Bkz. **Practices to Implement the OECD Privacy Guidelines on Global Networks**, OECD Working Papers, C. 6, S.97, Y.1998, s.6, d.n. 1. Ayrıca bkz. Ali Osman ÖZDİLEK, **İnternet ve Hukuk**, Papatya, İstanbul 2002, s. 194-203.

⁷³ Jeremy Haris LIPSCHULTZ, **Free Expression in the Age of the Internet, Social and Legal Boundaries**, Westview Press 2000, s.225.

⁷⁴ Prof. Jerry KANG, gerçek ve sanal dünyadaki alışveriş pratiklerini karşılaştırarak teknolojiyle birlikte yaşanan değişimi ortaya koymaktadır. Maddi dünyadaki bir alışveriş merkezinde kimi dükkanları gezip kimilerinden bir şeyler satın alarak, kiminden almadan çıktığımızda iletişim içine geçtiğimiz bütün kişiler bizim hakkımızda bazı bilgiler toplamış olacaktır. Ancak bu bilgiler, istisnalar hariç, bilgisayarlarda işlenerek birbirleri ile bağlantılarının kurulabileceği bilgiler olmadıkları gibi, çoğu da insan hafızasında saklandıklarından geçici bir nitelik taşıyacaktır. Oysa sanal ortamda bir alışveriş sitesini ziyaret ettiğimizde istisna kural haline gelir: sanki üzerimize yapıştırılmış bir barkod varmış gibi her hareketimiz bu barkodu okuyan bilgisayarlar tarafından kayda geçirilir. Yalnızca satın aldığımız ürünler değil, ziyaret ettiklerimiz, incelediklerimiz de profilimizin oluşturulmasına yardımcı olacak şekilde kayıt altına alınmıştır bile. Bu kayıtlar ise gerçek yaşamdakinden farklı olarak, bilgisayarlarca işlenir, kataloglanır ve kalıcı bir nitelik taşır. Bu anlamda “siber uzayı mümkün kılan muazzam teknoloji, kendimiz hakkında ayrıntılı, toptan, görünmez değerlendirmeleri de olanaklı kılmaktadır”. Bkz. Jerry KANG, “Information Privacy in Cyberspace”, **Stanford Law Review**, C.50, Nisan 1998, s. 1198-1199.

Ancak çerezler dışında siber uzayda gezinen kullanıcıların izlenmesini sağlayan başka yöntemler de bulunur. “Tıklama akışlı veriler”den (clickstream data), “casus yazılımlar” (spyware) kadar geniş bir yelpaze içerisindeki çeşitli araçlarla pek çok kuruluş İnternet gezginlerine ilişkin kişisel bilgilere ulaşmaktadır⁷⁵. Mevcut yöntemler zaman içinde geliştiği gibi, başka bazı yeni teknolojiler de kişisel verilerin korunmasına ilişkin yeni sorunlar meydana getirmektedir. Yazılım, müzik, metin, film gibi fikir ve sanat ürünleri sahiplerinin haklarını korumak için geliştirilen “sayısal haklar yönetimi” (Digital Rights Management-DRM) sistemleri örnek olarak gösterilebilir⁷⁶.

Dünyanın en kapsamlı kütüphanesi olarak nitelenebilecek İnternet ortamında çeşitli amaçlarla yapılan aramalar da benzer sorunları gündeme getirir. Pek çok kullanıcı, bu uçsuz bucaksız bilgi kaynağı içinde aradıklarını bulabilmek için arama motorlarını⁷⁷ kullanmaktadır. Google, Yahoo!, AltaVista gibi her gün milyonlarca kişinin ziyaret ettiği sitelerin kimin neyi araştırdığına ilişkin tuttukları kayıtlar, kişisel verilerin korunması açısından çeşitli sorunların ortaya çıkmasına neden olmaktadır. Arama motorlarının kullanımının her geçen gün artmasıyla bu sorun da daha önemli bir hale gelmektedir⁷⁸. Özellikle bu kayıtların tutulma süresi ciddi tartışmalara neden olmuştur.

⁷⁵ Bu yöntemlere ilişkin kısa bir açıklama için bkz. Daniel J. SOLOVE, *The Digital Person*, s. 23-26.

⁷⁶ Bkz. Chris Jay HOOFNAGLE, Privacy Self-Regulation: A Decade of Disappointment, 4 Mart 2005, <http://www.epic.org>, s. 7. Sayısal Haklar Yönetimi’ne ilişkin olarak ayrıca bkz. **Sayısal Haklar Yönetimi(DRM)**, İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi, İstanbul 2006, http://bthukuku.bilgi.edu.tr/documents/DRM%20rapor%20son_temiz%20versiyon.pdf.

⁷⁷ Arama motorları, kullanıcıların web ortamında aradıkları bilgilere ulaşmalarına yardımcı olan hizmetlerdir. Bu bağlamda yazılı bilgiler yanında, resimlere, videolara, ses kayıtlarına ya da başka biçimdeki bilgilere de ulaşmak olanaklıdır. Bunun yanında, yeni gelişen bir alan ise İnternet ortamında bulunan kişisel bilgilere dayanarak kişilerin profillerinin oluşturulmasını hedefleyen arama motorlarıdır. Bkz. Article 29, Data Protection Working Party, **Opinion 1/2008 on Data protection Issues Related to Search Engines**, 4 Nisan 2008, 00737/EN, WP 148, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm (s.y. 20 Mart 2009). Arama motorlarının işleyişine ilişkin genel bilgi için bkz. Hayri SEVER, Yaşar TONTA, “Arama Motorları”, **Türkiye Bilişim Ansiklopedisi**, haz. Tuncer ÖREN, Tuncer ÜNEY, Rifat ÇÖLKESEN, Papatya, İstanbul 2006, s. 95-99.

⁷⁸ PEWİnternet’in yaptığı araştırmaya göre Amerika’da 2002 yılında İnternet kullanıcılarının üçte biri olağan bir günde arama motorlarına başvururken, 2008 yılında bu oran %49’a ulaşmıştır. Bkz. **Almost half of all Internet users now use search engines on a typical day**, haz. Deborah Fallows, 6 Ağustos 2008, http://www.pewinternet.org/~media/Files/Reports/2008/PIP_Search_Aug08.pdf.

Google açısından dikkat çekici bir diğer konu ise bu kuruluşun sunduğu gmail e-posta hizmetine ilişkindir. Bu hizmetten yararlananların otomatik olarak postalarının içeriğini değerlendirilmekte ve postanın yanına içeriğine uygun reklamlar ekleyen bir sisteme sahiptir. Her ne kadar bu işlem insan eliyle gerçekleştirilmese de yalnızca bilgisayarlar tarafından bu bilgilerin okunması bile makul gizlilik beklentisine sekte vuracak niteliktedir⁷⁹.

Son olarak şunu da belirtmek gerekir: İnternet ortaya çıktığı ilk dönemde bu yeni aracın teknik yapısı, kullanıcılarının coğrafi açıdan dağınıklığı, içeriğinin niteliği gibi nedenlerle devlet denetiminden bağımsık olduğu düşüncesi hâkimdi. Bu düşünce ulus devletin İnternet'i düzenlemek istememesinden kaynaklanmıyordu. Devlet bu küresel ağı düzenlemek için fazla yavaş ve hem coğrafi, hem de teknik açıdan fazla sınırlı görülüyordu⁸⁰. Geçen zaman içerisinde bu varsayımın çok da yerinde olmadığı anlaşıldı. Devletler de gelişen teknolojilerin kullanıcıları olarak çeşitli amaçlarla İnternet iletişimine müdahalelerini geliştirmektedir⁸¹. Bu anlamda İnternet'in insan hakları açısından güçlü yanlarının, onun zayıflıklarıyla aynı olduğunu söyleyebiliriz⁸².

Özellikle devletlerin İnternet iletişimine çeşitli amaçlarla müdahalesi ve bu ortamı düzenleme isteği sonucunda gelişen uygulamalar, çeşitli hak alanlarının ihlaline neden olmaktadır⁸³. Kişisel verilerin korunması hakkı da bu kapsamda değerlendirilebilir.

⁷⁹ Bkz. "Thirty-One Privacy and Civil Liberties Organizations Urge Google to Suspend Gmail", 6 Nisan 2004, <http://www.privacyrights.org/ar/GmailLetter.htm> . Google uygulamaları ve özellikle de son dönemde hararetli tartışmaların konusu olan "ağ-işlemcilik"e (cloud computing) ilişkin değerlendirmeler için bkz. Randall STROSS, **Planet Google: One Company's Audacious Plan to Organize Everything We Know**, Simon and Schuster, 2009. Ayrıca bkz. David G. HILL, **Data Protection, Governance, Risk Management and Compliance**, CRC Press, ABD 2009, s. 229-234.

⁸⁰ James BOYLE, "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwire Censors", **University of Cincinnati Law Review**, C.66, Y.1997, s. 178.

⁸¹ Bir örnek olarak yeni geliştirilen teknolojiler ile İnternet üzerinden yapılan sesli görüşmelerde de kelime temelli arama yapılabilmesi olanaklı hale gelmesi gösterilebilir. "Lauschangriff im Internet", **Der Spiegel**, Y. 2008, S.26, s.128.

⁸² Valerie STEEVES, "Privacy, Free Speech and Community: Applying Human Rights Law to Cyberspace", **Human Rights and the Internet**, Macmillan Press, Birleşik Krallık 2000, s. 187.

⁸³ Devletlerin İnternet üzerindeki içeriği sınırlama girişimlerine ilişkin olarak kapsamlı bir çalışma için bkz. **Access Denied: The Practice and Policy of Global Internet Filtering (Information Revolution and Global Politics)**, haz. Ronald J. DEIBERT, John G. PALFREY, Rafal ROHOZINSKI, Jonathan ZITTRAIN, The MIT Press, ABD 2008. İnternet'in düzenlenmesine ilişkin bir değerlendirme için bkz. "freiheit@unendlich.welt", **Der Spiegel**, Y. 2009, S. 33, s. 68-79.

3. GÖZETİM SAĞLAYAN YENİ TEKNOLOJİLER

İzleme, gözetleme, veri toplama etkinlikleri teknolojinin sunduğu çok çeşitli araçlarla gerçekleştirilebilmektedir. Bu ise bilgi çağında kişisel verilerin korunması hakkını ihlal eden eylemleri tanımlamayı daha da zorlaştırır⁸⁴. Bu konuda uzmanlaşmış kurumların kişisel verilerimizi toplayan gelişmiş araçları düzenli olarak kullanması, kişileri de bu izlemenin hedefi ve olası şüphe nesneleri haline sokması, önceki dönemlerde istisna olarak görülen izlemenin, kural haline geldiğinin işaretidir⁸⁵. “ECHELON”⁸⁶ gibi geniş çaplı etki alanına sahip ve temelde devlet gibi güçlü örgütlerin elinde bulunduğu düşünülen araçlar yanında, “RFID”⁸⁷, “CCTV”⁸⁸, biyometrik yöntemler⁸⁹ gibi günlük yaşamlarımızın içine sızmış ve bir anlamda artık herkesin elinde bulunan teknolojiler yalnızca birkaç örnek olarak sayılabilir.

⁸⁴ Avniye TANSUĞ, “AB’nin Yeni Ekonomi Silahı: “Veri Saklama Hukuku””, **Bilişim Hukuku**, Der. Mete Tevetoğlu, Kadir Has Üniversitesi Yayınları, İstanbul 2006, s.536.

⁸⁵ David LYON, **Elektronik Göz**, s.16.

⁸⁶ ECHELON’un, Amerikan Ulusal Güvenlik Kurumu tarafından kullanılan ve bütün uydu, mikrodalga, hücresel ve fiberoptik iletişim trafiğini tutan ve analiz eden bir sistem olduğu düşünülmektedir. Bkz. Valerie STEEVES, s.192. Geniş çaplı elektronik izleme(massive electronic surveillance) olarak nitelendirilebilecek ECHELON’un, telefon görüşmeleri, e-posta mesajları, uydu yayınları dâhil, günde üç milyar kadar iletişim aracının yolunu kestiği tahmin edilmektedir. Hatta kimi kaynaklar bu sistemin İnternet trafiğinin %90’ını elediğini dahi ileri sürmektedir. ECHELON’un yanında İnternet’i hedef alan başka sistemler de bulunmaktadır. Çin ve Singapur kendi ülkelerindeki İnternet trafiğini izledikleri gibi, Rusya’da servis sağlayıcılar, SORM-2 adlı dahili bir casusluk programının bir parçası olarak, haber alma örgütüne özel e-posta yazışmalarını ve diğer İnternet trafiğini izlemekte yardımcı olmaktadır. Ancak özellikle Echelon gibi geniş çaplı bir sistemin beraberinde pek çok sorunu getirdiği de unutulmamalıdır. Her şeyden önce bir veri, ancak insanların onu anlayabileceği bir forma sokulduğu zaman işe yarar. Bunu değerlendirmenin zorluğu kadar büyük başka bir zorluk ise neyin kaydedileceğine karar vermektir. Bruce SCHNEIER, s.35,56.

⁸⁷ Hızla yaygınlaşan RFID (Radio Frequency Identification-Radyo Frekanslı Tanımlama) “*nesnelerin İnternet’i*” olarak adlandırılan bir teknolojinin kapsamında yer alır. En genel şekliyle, kabloyla bağlanmamış aletlerin radyo dalgası ile tanınması olarak tanımlanabilir. Bonnekoh HOLZNAGEL, “Radio Frequency Identification-Innovation vs. Datenschutz?”, **MMR**, 2006, Heft 1, s.17. Günlük yaşamımızda karşılaştığımız pek çok örnek ile renklenmiş aydınlatıcı bir çalışma için bkz. Katherine ALBRECHT, Liz McINTYRE, *Spychips, How Major Corporations and Government Plan to Track your Every Purchase and Watch Your Every Move*, A Plume Book, ABD 2006. Nesnelerin İnterneti’ne ilişkin olarak bkz. **The Internet of Things, First International Conference**, IOT 2008 Zurich, Switzerland, March 2008 Proceedings, haz. Christian FLOERKEMEIER, Marc LANGHEINRICH, Elgar FLEISCH, Friedemann MATTERN, Sanjay E. SARMA, Springer, Almanya 2008.

⁸⁸ CCTV (Close Circuit Television-Kapalı Devre Televizyon)sistemi, belirli bir yerdeki sinyalleri ileten kameraların kullanımı olarak tanımlanabilir. Ayrıntılı bilgi için bkz. Clive NORRIS, Gary ARMSTRONG, **The Maximum Surveillance Society: The Rise of CCTV**, Berg Publishers, ABD 1999.

⁸⁹ Biyometrik yöntemler, “*yaşayan bir kişinin fiziksel ve davranışsal özellikleri çerçevesinde kimliğinin doğrulanması veya tanınmasına ilişkin otomatik yöntemler*” olarak tanımlanabilir. Bkz. Leyla KESER BERBER, Murat LOSTAR, **Bilişimde Biyometrik Yöntemler**, Yetkin, Ankara 2006, s.103.

Teknoloji kişisel verilerin toplanmasını sağlayan yeni araçlar sunduğu gibi, eskiden bilinmeyen bazı yeni ve önemli verilerin ortaya çıkmasını da sağlamıştır. Bunun en açık örneği “DNA”⁹⁰ verileridir. Gerçekten gen, bir kişinin taşıyabileceği en büyük veri hazinesidir⁹¹. “DNA”, gen parçalarından oluşur. Genetik veri, bir yandan bizi benzersiz kılan bilgileri içerdiği için, diğer yandan yalnızca bize ilişkin değil, akrabalarımıza ilişkin bilgileri de taşıdığından kişisel verilerin korunması hukuku açısından son derece önemlidir.

Bunun gibi yeni nesil arabaların sunduğu olanaklar da birkaç açıdan tartışmaya açıktır. Pek çok yeni araba, hız, sürüş ve direksiyon tutuşa ilişkin bilgileri kaydetmekte ve pek çoğu da küresel yer belirleme sistemi (GPS) hizmeti sunmaktadır. Bu tür araçlar daha rahat ve güvenli sürüş sağlamaktadır. Ancak öte yandan alışkanlıklar ve daha pek çok kişisel bilgi de kayıt altına alınabilir. Bu durumda araç sahiplerinin hangi bilgilerin toplanıp saklandığını bilmeye ve bunlara kimlerin ulaşabileceğine karar vermeye hakkı olmalıdır⁹². Benzer şekilde hızla yaygınlaşan cep telefonları da hem kullanıcılarını, her gün ve her saat, pek çok yerden ulaşılabilir kılarken, servis sağlayıcılarına da telefonun ne zaman, nerede bulunduğuyla ilişkin yer ve zaman bilgileri vermektedir⁹³. Cep telefonu kullanıcılarının, bu bilgilerin kimlerin elinde, ne amaçlarla kullanıldığını bilmeye hakları bulunmalıdır.

Hızla yaygınlaşan ve her gün yeni araçlar sunan teknoloji ile birlikte artık yeni bir gözetim türüyle karşılaştığımız ortadadır. Gözetimin farklılaşan yapısı,

⁹⁰ DNA (Deoksiribonükleik asit), en genel şekliyle kalıtımın moleküler temelidir. Roger C. KING, William D. STANSFIELD, **A Dictionary of Genetics**, Oxford University Press, 5. Baskı, Büyük Britanya 1997, s. 95. DNA, bu anlamda, bilinen tüm yaşayan organizmalar ve bazı virüslerin canlılık işlevleri ve biyolojik gelişmeleri için gerekli olan genetik talimatları taşıyan bir nükleik asittir. DNA moleküllerinin başlıca rolü bilgiyi uzun süre saklamalarıdır. Bkz. <http://en.wikipedia.org/wiki/DNA> (s.y. 7 Şubat 2009).

⁹¹ Alessandra Di MARTINO, s. 20.

⁹² MacRonin, *Electronic Data Recorders in Vehicles*, 17 Aralık 2008, <http://www.privacydigest.com/2008/12/17/electronic+data+recorders+vehicles>.

⁹³ **Constitutional Rights and New Technologies**, A Comparative Study Covering Belgium, France, Germany, Sweden, and the United States, haz. Bert-Jaap KOOPS, Ronald LEENES, Paul de HERT, Tilburg, Şubat 2007, <http://www.voxinternet.fr/IMG/crant-report-2007def-1.pdf> (s.y. 20 Şubat 2009), s.9.

eskiden bu kadar açıkça görülmeyen bazı özellikleri bünyesinden barındırmasından kaynaklanır. Gary T. Marx'a göre yeni gözetimin ayırt edici özellikleri şunlardır⁹⁴:

- (i) görünmezdir ya da görünürlüğü düşüktür,
- (ii) irade dışıdır,
- (iii) emek yoğunluğuna değil, sermaye yoğunluğuna bağlıdır,
- (iv) merkezileştirilmiş kendini denetlemeyi içerir,
- (v) belirli bireyleri hedeflemekten çok herkes şüpheli durumundadır,
- (vi) daha yoğun ve daha yaygındır.

Marx ayrıca bu yeni gözetimin devletin şiddet araçları üzerindeki geleneksel tekelinde kaynağını bulduğunu savunur. Artık zorlama yerine yönlendirme, hapisane parmaklıkları yerine çipler, kelepçe yerine uzaktan izleme kullanılmaktadır ve bunlar bir bütün olarak topluma nüfuz edebilme yetisine de sahiptir⁹⁵. Üstelik gittikçe hızlanan bir akışla teknoloji her geçen gün yeni olanaklar sunmaya devam etmektedir. Geleceğimize sürücülerin kalp atışlarını, yorgunluk ya da uykululuk hallerini belirleyebilen sensörlerin, küresel yer belirleme sistemlerinin (GPS), gelişmiş mikro kameraların ve telefonların hâkim olacağını söyleyebiliriz⁹⁶.

Teknoloji henüz uyuşturucu pazarlıklarını rasgele telefon konuşmalarından, şüpheli davranışları uydu görüntülerinden, ya da aranan listelerinde yer alan yüzleri kalabalığın içinden otomatik olarak arayıp bulacak seviyeye erişmedi. Ancak zaman içerisinde bunların da gerçekleşeceği şüphesizdir⁹⁷. Bunun yanında ulaşılan verilerin daha az yer kaplayacak şekilde ve daha ucuza depolanması eğilimini de dikkate alacak olursak, birkaç nesil sonra bütün hayatımızın, hem sesli hem de görüntülü olarak, kayıt edilebileceği öngörüsünde bulunmak sanırız abartılı olmayacaktır.

Yukarıda her geçen gün biraz daha genişleyen, yaygınlaşan, ucuzlayan bilişim teknolojileri içerisinde görece önemli bazıları kısaca açıklanmıştır. Görüldüğü gibi, elektronik ortamda verilerimizin toplanması kayıtların yalnızca elle

⁹⁴ Her ne kadar yazar, bu sınıflandırmayı polis gözetimini dikkate alarak yapmış olsa da bu altı özellik kanımızca daha geniş bir alan için genel bir değerlendirme sunmaktadır.

⁹⁵ Gary T. MARX, **Undercover, Police Surveillance in America**, University of California Press, ABD 1988, s.217-219.

⁹⁶ Louise CADAUX, "Privacy: Our Future Under Close Surveillance", **Freedom of Expression (And New Communication Technologies)**, Haz. Mich     PAR  , Peter DESBARATAS, IQ Collectif, Kanada 1998, s.115.

⁹⁷ Bruce SCHNEIER, s.31.

tutulduğu zamana göre çok daha kolaylaşmış ve bilgilere ulaşma yolları çeşitlenmiştir. Kişisel veriler bir kez toplandıktan sonra ise bunları çok çeşitli şekillerde işlemek düşük maliyetle ve kolaylıkla gerçekleştirilebilmektedir⁹⁸.

D. GÖZETİM TEKNOLOJİLERİ KAYNAKLI KAYGILAR-ELEKTRONİK GÖZETİM KARŞISINDA ŞEFFAFLAŞMIŞ BİREY

Yeni bir teknoloji uygulamaya geçtiğinde, ilk aşamada fark edilemeyen bazı uzantıları ve karmaşayı; denetimi ve sosyal etkileriyle ilgili kendine özgü pek çok sorunu beraberinde getirir⁹⁹. Ancak bazı teknolojilerde (otomobil, uçak ya da nükleer güç gibi), neden olabileceği sonuçlar, somut ve açık olarak belirlenebilirken, bilişim teknolojileri için durum biraz daha farklıdır¹⁰⁰. Yukarıda da açıklandığı üzere, bilgisayar ve merkezi veri bankalarının bulunuşu ile başlayan süreç içerisinde ilk aşamada fark edilmeyen pek çok sorun daha sonradan ortaya çıkmıştır. Bunlar teknolojinin görünmez yan etkileri olarak nitelenebilir. Kişisel verilerin korunmasına ilişkin tartışmalar da bu kapsamdadır. Bilişim teknolojileri ile birlikte gelişen uygulamalar karşısında gösterilen tepki, kişisel verilerin korunması hukukunun ortaya çıkışında ve temel ilkelerin belirlenmesinde etkili olmuştur. Bu nedenle yeni teknolojilerin taşıdığı potansiyel ile ilintili korkular, kişisel verilerin korunmasının gerekliliğini anlayabilmemiz açısından son derece önemlidir.

Bilişim teknolojilerinin kullanımının yaygınlaşması, hükümetlerin ve şirketlerin etkisini ve gücünü arttırmaktadır. Teknolojinin sunduğu yeni olanaklar, bir yandan bireylerin yaşamlarını, özel teşebbüslerin iş yapma tekniklerini, devletlerin yönetim becerilerini güçlendiren sayısız olanak sunarken, diğer yandan yeni saldırı tekniklerini, yeni tehditleri de beraberinde getiriyor. Bu durum özellikle elektronik gözetimin suçlulukla mücadelede artan oranda kullanımında kendini göstermektedir.

Bu yeni yöntemler suçlulukla mücadelede çeşitli açılardan etkin araçlar olarak karşımıza çıkıyor, ancak beraberinde çeşitli sorunları da getirerek¹⁰¹. Herkesin

⁹⁸ Pamela SAMUELSON, “Privacy as Intellectual Property?”, *Stanford Law Review*, C.52, Mayıs 2000, s.1126.

⁹⁹ Colin J. BENNETT, s.22; James D. DANZIGER, ve diğ. (William H. DUTTON, James N. DANZIGER), s. 8.

¹⁰⁰ Colin J. BENNETT, s.22.

¹⁰¹ Daniel J. SOLOVE, “Reconstructing Electronic Surveillance Law”, *The George Washington Law Review*, C. 72, Y. 2004, s. 1267-1270.

bir kimlik numarası ve yongalı, benzersiz bir kimlik kartı sahibi olması, suçlulukla mücadelede bir yarar sağlayabilir. Ancak tarih göstermektedir ki bu çeşit uygulamalar eninde sonunda sıradan insanlara karşı kullanılan otorite araçları olmaktadır. Aynı şey başımızı kaldırıp baktığımız hemen hemen her köşede görmeye başladığımız kapalı devre televizyonlar (CCTV) için de söz konusudur. Bunlar kapkaç, hırsızlık, taciz gibi suçların önlenmesinde etkili araçlardır. Ancak kamu ahlakının ve kamu düzeninin sağlanması hedefinden hareketle gerçekleştirilen bu uygulamalar, bireylere belirli ve oldukça sınırlı bir hareket tarzının dayatılmasına da neden olabilir. Bütün bunlara karşın, şurası açıktır: teknolojiye olan bağlılığımız tarihin her hangi bir aşamasından çok daha fazladır¹⁰². Teknolojiye olan bağlılığımız arttıkça, oluşabilecek zararların boyutları da artmaktadır. Böylece teknoloji bir yüzü ile bize gülümser ve her geçen gün ona biraz daha bağlanmamızı sağlarken, diğer yüzü ile korktuğumuz, bizleri huzursuz eden bir figür haline gelmektedir.

Kabul etmek gerekir ki adımızın, adresimizin, beğenilerimizin, kişiliğimizin kısacası bize dair olan her şeyin daha değerli olduğu ve daha kolay ulaşılabilir, birleştirilebilir, değerlendirilebilir bir hâle geldiği bir dünyada yaşıyoruz. İngiliz Veri Koruma Denetçiliği (ICO) için 2006 yılında hazırlanan bir raporda da belirtildiği gibi, artık gözetim toplumundan gelecek zaman mastarıyla söz etmek anlamsızdır, çünkü bizler artık o toplumun birer üyesiyiz¹⁰³.

Artık bireylere daha da yakın gelen tehditler gözetim teknolojilerine karşı bir savunma mekanizmasının geliştirilmesini zorunlu kılmıştır. Kişisel verilerin korunması hukukunun gerekliliği de böylesine bir ortamda anlaşılmıştır. Kişisel veriler üzerinde ilgili kişinin tekrar denetimini sağlamayı amaçlayan bu düzenlemelerin ilk kez 1970’li yıllarda Avrupa’da ortaya çıkması ne zaman, ne de mekân açısından elbette bir tesadüfün ürünü değildir. Bilgisayarların hızla gelişmesi ve merkezî veri bankalarının oluşturulma girişimleri veri koruması hukukunun ortaya çıkış zamanını, Avrupa’nın yakın tarihinde yaşadığı acılı olaylar ise anavatanını belirlemiştir. Bu anlamda veri koruma hukukunun gelişmesinde çeşitli açılardan değerlendirilebilecek “*korku*”ların etkili olduğu söylenebilir.

¹⁰² Simon DAVIES, **Big Brother, Britain’s Web of Surveillance and the New Technological Order**, Pan Books, İngiltere 1996, s. 17.

¹⁰³ **A Report on the Surveillance Society**, For the Informational Commisioner by the Surveillance Society Network, Eylül 2006, haz. David Murakami WOOD, s. 1.

Bu korkuların neden kaynaklandığını saptamak ve objektif bir değerlendirme yapmak kişisel verilerin korunmasının gerekliliğinin anlaşılması açısından önemlidir. Bu noktada kişisel verilerin korunmasının neden gerekli olduğu sorusuna yanıt ararken edebi eserlerin çeşitli ipuçları sunduğunu belirtmek gerekir. Kişisel verilerin korunmasının “*birey*” ile ilişkisinin doğrudanlığı, hukuk, ekonomi ve siyaset yanında sosyoloji ve psikolojiyi de kapsama alır. Özellikle son iki etmen dolayısıyla edebiyat eserleri de değerlendirme kapsamına alınabilir.

İlk bakışta bu yaklaşım sorunlu bulunabilir. Edebi eserlerde kaçınılmaz olarak estetik kaygılar önemlidir, bu nedenle belirtilen türdeki çalışmaların gerçekçi olması asla bir zorunluluk olmadığı gibi, ahlak ya da siyaset felsefesinin göz önünde tutulması da beklenemez¹⁰⁴. Buna karşın edebi eserlerin sunduğu metaforlar çeşitli sorunları kavrayışımız açısından görmezden gelinemeyecek bir öneme sahiptir. Bu nedenle kişisel verilerin korunmasına ilişkin sorunların somut ve açık bir şekilde algılanabilmesi ve bu sorunlara karşı kamusal ilginin oluşması için edebi eserler oldukça yararlıdır¹⁰⁵. Nitekim konunun sosyal, siyasal, ekonomik ve hukuksal boyutlarını inceleyen pek çok yazarın sıklıkla edebi eserlere atıf yaptığı görülmektedir. Özellikle George Orwell’ın “*1984*”ü, Aldous Huxley’nin “*Cesur Yeni Dünya*”sı, Jevgeni Zamyatin’in “*Biz*”i ve Franz Kafka’nın “*Dava*”sı burada ilk akla gelenlerdir. Aşağıda bu eserlere yeri geldikçe tekrar değinilecektir. Ancak burada belirtilen yapıtlarda konumuz açısından dikkat çeken özellikler belki şöyle sıralanabilir:

- *1984*, “*büyük birader*” ile kişilerin sürekli gözetlenmesi ve bunun yıkıcı sonuçlarını,
- *Cesur Yeni Dünya*, bu gözetiminin total kabullenilişinin nasıl yaratılabileceğini,
- *Biz*, herşeyin matematiksel bir kesinlik içinde işleyişinin “*ben*”i, yok edişini,

¹⁰⁴ Richard A. POSNER, “Orwell versus Huxley: Economics, Technology, Privacy and Satire”, **John M. OLIN Law and Economics Working Paper No.89**, <http://www.law.uchicago.edu/Publications/Working/index.html> , s. 31.

¹⁰⁵ Bkz. aynı yönde, Daniel J. SOLOVE, *The Digital Person*, s. 28.

- *Dava* ise bürokrasinin hantal kollarının yarattığı çaresizlik ve yitişi tasvir etmektedir. Bu eserlerin tamamında ortak olan ise madden ve manen olarak özgür olan bireyin yok oluşuna ve bunun sonuçlarına ilişkin çarpıcı bir tablo sunmalarıdır.

1. BÜYÜK BİRADER

Avrupa'nın yakın tarihinde yaşadığı trajik olaylar bireylerin özel yaşamlarına ilişkin bilgileri toplayan devlet yönetiminin bunları ne şekilde kullanabileceğini gözler önüne sermiştir. 1930'lu yıllardan itibaren yeni ve güçlü totaliter sistemler¹⁰⁶ olan komünizm ve faşizm, dönemin iletişim araçlarını etkin bir şekilde kullanmışlardır. Bu anlamda, telefon kişilerin özel yaşamına sızmak için, radyo yayınları ise geniş kitlelerin görüşlerini biçimlendirmek için kullanılmıştır. II. Dünya Savaşı ve hemen öncesi, benzersiz bir fiziksel yıkım yaratan araçların geliştirilmesine tanıklık eden bir dönem olmasının yanında, sosyal denetim tekniklerinin etkisini de gözler önüne sermiştir. Bu ise o döneme kadar çok az sayıda kişinin (suçluların, ajanların ve belki de paranoyakların) endişe duyduğu telefon dinleme gibi yöntemlerin yaygınlığının ve olası sonuçlarının kavranmasını sağlar¹⁰⁷.

Bu deneyim, siyasal açıdan bilişim teknolojilerinin totaliter bir devlet yapılanmasının önemli bir aracı olabileceği korkusunun gelişmesinde etkilidir. Bu korku, yeni iletişim teknolojileri geliştikçe artarak hissedilmeye devam etmiştir. Nitekim telefon dinleme neredeyse telefonun kendisi kadar eskidir, veri toplama ise kimin kim olduğunu araştırmanın daha yeni bir yoludur¹⁰⁸. Eski Doğu Almanya Devleti gizli servisi Stasi'nin yurttaşları izleme, gözleme, dinlemeye yönelik akıl

¹⁰⁶ Totalitarizm, I. Dünya Savaşı'ndan bu yana kullanılan siyasal bir deyimdir. Totalitarizm 20. yüzyıla ait bir kavramdır ve çeşitli nitelikleri ile Antik Yunan'dan bu yana tanımlanan klasik diktatörlüklerle arasında farklılıklar bulunmaktadır: *"Totalitarizmin çoğu tanımında modern diktatörlük; siyasal, toplumsal ve entelektüel yaşamın tüm boyutlarının komple merkezleştirilmesi ve tektip tasnif (regimentation) ile şekillenen ve bu açılardan daha önceki mutlak ve otokratik yönetimleri ve bu yönetimlerin tebaalarını kitlesel olarak kontrol altına alma kapasitesini aşan bir model olarak betimlenir"*. **Blackwell'in Siyaset Bilimi Ansiklopedisi**, C.II, haz. Vernon BOGDANOR, Türkçe yayıma haz. Erhan YÜKSELÇİ, çev. Erhan YÜKSELÇİ, Sema YÜKSELÇİ, Bülent PEKER, Ümit Yayıncılık, Ankara 2003, s. 426.

¹⁰⁷ Harry HENDERSON, s. 11.

¹⁰⁸ Bart CUSTER, "Tapping and Data Retention in Ultrafast Communication Networks", **Cyberlaw Security & Privacy**, haz. Sylvia Mercado KIERKEGAARD, The Second International Conference on Legal, Security and Privacy Issues in Information Technology (LSPI) 2007, Beijing, Çin, Ankara Barosu Yayınları, 2. Baskı, Ankara 2007, s. 290. (289-300)

almaz uygulamaları, günümüzde gelişen teknoloji ile çok daha etkili, kolay ve ucuz bir şekilde gerçekleştirilir hale gelmiştir¹⁰⁹.

Kişisel verilerin toplanmasının olası sonuçlarına işaret etmek için, konuya ilişkin çalışmalarda, sıklıkla hatırlatılan George Orwell'in "*1984*" adlı romanında da¹¹⁰ II. Dünya Savaşı ve öncesinde Avrupa'da yaşanan travmanın etkisi hissedilir. Liberal bir yazar olan Orwell, bu romanı 1948 yılında tamamlar ve dünyanın 1984 yılında nasıl olabileceğine ilişkin çizdiği kara tasvir gözetim tekniklerine ilişkin edebi bir sembol olarak etkisini halen sürdürmektedir¹¹¹.

Yazarın kendi deneyimi ve gözlemleri İspanya iç savaşına, Sovyetler Birliği'ndeki Stalin, Almanya'daki Hitler ve İtalya'daki Mussolini yönetimlerine dayanmaktadır¹¹². Olasılıkla Orwell bu örneklerden hareketle kapitalist yönetimlerdeki otoriter eğilimlerden de etkilenmiştir¹¹³. Orwell'in hikâyesinde "*büyük birader*"ın İngiltere'de hüküm süren bir diktatör olması, yalnızca buranın yazarın anavatanı olmasından kaynaklanmaz. Orwell, okuyucusuna böylesine bir sistemin anadili İngilizce olan bir ülkede de kurulabileceğini göstermek istemiştir.

"*1984*"ün dünyasında devletin bireyleri izlemesi istisna değil, kuraldır. Orwell'in, yurttaşlarını evlerinde televizyon ekranından ve dışarıda başka araçlarla gözetleyen, onları yöneten ve düşüncelerini yönlendiren hayali diktatörü "*büyük birader*"e ve "*büyük birader seni izliyor!*" sloganına gözetim araçlarına ilişkin tartışmalarda sıklıkla atıfta bulunmaktadır¹¹⁴. Bunun gözetimin özellikle bireysel haklar açısından neden olabileceği sonuçlara ilişkin ciddi bir algı yarattığı açıktır,

¹⁰⁹ Steve WRIGHT, "Political Control and the Internet", **Human Rights and the Internet**, haz. Steven HICK, Edward F. HALPIN, Eric HOSKINS, Macmillan Press, Büyük Britanya 2000, s. 201.

¹¹⁰ George ORWELL, **Nineteen eighty-four**, Penguin, Büyük Britanya 2000. Türkçe çevirisi için bkz. George ORWELL, **Bin dokuz yüz seksen dört**, çev. N. AKGÖREN, Can, İstanbul 1989.

¹¹¹ Peter SCHAAR, **Das Ende der Privatsphäre**, 96.

¹¹² George Orwell 1946 yılında kaleme aldığı ve yazar olma serüvenini anlattığı bir makalesinde, özellikle 1936 yılından itibaren bütün yazılarında, doğrudan ya da dolaylı olarak, totalitarizme karşı çıktığını belirtmiş ve görüşlerinin gelişmesinde özellikle İspanya iç savaşının ve Hitler Almanya'sının etkili olduğunu söylemiştir. Bkz. George ORWELL, "Why I Write", 1946, <http://www.netcharles.com/orwell/essays/whyiwrote.htm> (s.y.: 6 Mart 2009).

¹¹³ David LYON, **Elektronik Göz**, s.91.

¹¹⁴ "*Büyük birader*" vurgusunu yalnızca akademik çalışmalarda ya da gazete haberlerinde değil, bazı sivil toplum girişimlerinde de görmek olanaklıdır. Bunların en bilineni, "*büyük birader ödülleri*" (big brother awards)dır. Her yıl, "*Privacy International*" ve başka pek çok sivil toplum örgütünün katılımıyla, özel yaşamın gizliliğini ve kişisel verilerin korunmasını en ağır şekilde ihlal eden devletlerin, özel teşebbüslerin ve kişilerin belirlenerek, bu ihlallere karşı kamuoyu oluşturmak amacıyla, çeşitli ülkelerde "*büyük birader ödülleri*" verilmektedir. Bkz. <http://www.bigbrotherawards.org/> (s.y. 10 Mart 2009).

hatta teknoloji kullanılarak özgürlüğün ve bireyselliğin yıkımı konusunda öğrenebilecek pek çok şey ortaya koymaktadır¹¹⁵.

Çok sayıda kişi, bu kara ütopyanın bir bilim kurgu romanı olmanın ötesine geçip kapkara bir potansiyel tehlike olarak bireyin karşısına dikildiği düşüncesindedir. Özellikle devletin her alanda bütüncül bir gözetleme yapma olasılığının şiddetle tartışıldığı 1970’li yıllarda Orwell’in “*Büyük Birader*”i ile Hobbes’un “*Leviathan*”ının¹¹⁶ bir gerçeklik olarak bireylerin karşısına gelebileceği korkusu belirmiştir¹¹⁷. Peki her geçen gün gelişen teknoloji ile bizi biraz daha fazla kuşatan gözetim araçları totaliter bir yönetimin en bilinen simgesi olan büyük biraderi kaçınılmaz olarak yaratacak mıdır? Bu soruya bir çırpıda cevap vermek elbette kolay değildir, ama çeşitli açılardan tartışılması gerekir.

Totaliter yönetim içerisinde gözetimin önemli bir yeri olduğu açıktır. Ancak bu önemin derecesi başka etkenler dikkate alınmadan belirlenemez. Örneğin, Giddens’a göre, “*totalitarizm her şeyden önce gözetimin aşırı derecede odaklaşmasıdır*”¹¹⁸. Bu yaklaşım totaliter yönetim biçimi ile gözetim arasında oldukça yakın bir ilişki kurar. Bu görüş kabul edildiğinde devlet yönetiminde ya da güvenliği sağlamada yeni teknolojilerin artan oranda kullanılmasının yaratacağı paniğe şaşırmamak gerekir. Oysa Lyon’a göre “*İleri toplumların kendilerini bilgisayar kapasitelerini uyarlar ve yükseltirken bulmaları olgusu, tek başına, bu toplumların yokuş aşağı tiranlığa doğru sürüklendiği anlamına gelmez. Bununla birlikte, eğer gözetimin yoğunlaşması totalitarizmin asli bir bileşeni ise, demokratik yaklaşımlı yurttaşlar hiç değilse, devlette yeni teknolojilerin rolü hakkında sorular sormakta haklıdırlar*”¹¹⁹.

Klasik liberal görüş, sınırlı hükümet anlayışı ile güç uygulamalarına güvenmeme üzerine kurulmuştur. Bilişim teknolojileri, devletlerin bireyler hakkında geniş oranda bilgi toplamasına ve bunları kullanmasına olanak vererek yönetimin elindeki gücü genişletmektedir. Devletin kişisel verilerin toplanması, kullanılması ve

¹¹⁵ Harry HENDERSON, s. 11.

¹¹⁶ Leviathan, “*dev ejderha*” anlamına gelir ve güçlü, merkezî devleri simgelemek için kullanılmıştır. Bkz. Thomas HOBBS, *Leviathan, veya Bir Din ve Dünya Devletinin İçeriği, Biçimi ve Kudreti*, çev. Semih LİM, 4. Baskı, YKY, İstanbul 2004.

¹¹⁷ Alessandra Di MARTINO, *Datenschutz im europäischen Recht*, Nomos, Baden-Baden 2005, s. 17-18.

¹¹⁸ Anthony GIDDENS, *The Nation-State and Violence*, s. 303.

¹¹⁹ David LYON, *Elektronik Göz*, s. 26.

iletimi üzerindeki denetimi siyasal bazı etkiler yaratabilir¹²⁰. Bu anlamda “1984”te çizilen tüyler ürpertici tablonun, bireylerin devletin gözetim araçlarına karşı uyanık olmasını sağladığı söylenebilir. Gelişen teknolojinin yardımıyla, günümüz devletlerinin büyük birader benzeri bir şekilde her hareketimizi izlemesi, en azından teorik olarak, olanaklıdır. Ancak yine günümüz koşulları dikkate alındığında karşılaşılan tablonun “1984”de çizilenden oldukça farklı olduğu da dikkatten kaçmamalıdır.

Gerçekten “1984”de tasvir edilen ortam, günümüzdeki izleme, gözetleme ve kişisel verileri toplama uygulamalarından birkaç açıdan farklılık gösterir. Romanın kahramanı *Winston*, hangi aletlerle hangi açılardan izlendiğini bildiği gibi, izlemeyi yapanlar bilgisayarlar olmadığı için Winston’ın tüm yaşamını kapsayan bir resminin oluşturulabilmeleri de olanaklı değildir. Günümüzde ise bu uygulamalar haberimiz bile olmadan makineler tarafından gerçekleştirilebilmektedir. Hatta potansiyel olarak bu bilgilerle bütün yaşamımızı kapsayan ayrıntılı bir resim oluşturabilmesi olanaklıdır. Bunun yanında işlenen bilgilerin veya ham verilerin istek sahiplerine çeşitli amaçlarla aktarılması, bir başka anlatımla çeşitli merkezler arasında değiş-tokuş edilmesi de söz konusu olabilir. Bütün bu işlemler, bilgileri elinde bulunduran otoritelere büyük bir güç vermektedir. Bunlar bireyleri onlara bağımlı hatta tutsak hale getirebilir¹²¹. Artık her şey görüntülenemediği gibi, içinde arama da yapılabilir. İşte bu, gerçekten “*Orwell’in bile hayal edemediği bir şeydir*”¹²².

Bunun yanında Orwell, demokratik yönetim sürerken bilişim teknolojilerinin totalitarizme yönelme eğilimindeki gözetime izin verebileceğini, bir başka anlatımla kadife eldivenin demir yumruğu gizleyebileceğini öngörmemiştir¹²³. 2000’lerin dünyasında Çin ve Ortadoğu ülkeleri gibi çeşitli coğrafyalarda büyük biraderi aratmayacak yöntemlerle bireysel özerkliğe pek çok cepheden saldırılmaktadır. Ancak bunun yanında demokratik pek çok ülkede de yönetimlerin kadife eldivenlerini giydikleri yönünde hiç de iç açıcı olmayan çeşitli uygulamalar dikkat çekmektedir. Bunun olası sonuçları demokratik toplum sürerken demokrasinin

¹²⁰ Colin J. BENNETT, s. 29.

¹²¹ Tekin AKILLIOĞLU, “Yönetimde Açıklık-Gizlilik ve Bilgi Alma Hakkı”, s. 11.

¹²² Lawrence LESSIG, **Code Version 0.2.**, Basic Books, ABD 2006, s.208-209.

¹²³ Gary T. MARX, “The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures”, **The Social Fabric: Dimensions and Issues**, der. E., SHORT, Jr., ABD 1986, ayrıca bkz. şu kaynakta: <http://web.mit.edu/gtmarx/www/iron.html> .

önemli gerekliliklerinin yara almasıdır. Her hareketinin bir yerde kayıt altında tutulduğunu bilen, ya da en azından bu olasılığı hisseden kişi, düşüncelerini açıklarken, derneklere üye olurken, toplantı ve gösteri yürüyüşlerine katılırken bunların ileride aleyhine kullanılabileceğini düşünür. Bu o kişinin özgür iradesi ile hareket etmesini engelleyebilir¹²⁴.

Gelişmiş veri bankalarında kendisine ilişkin bilgileri kayıt edilen birey, yalnızca bunların mevcut kullanımları dolayısıyla değil, henüz verileri tutanlarca bile bilinmeyen gelecekteki olası kullanımları dolayısıyla da tehdit altındadır. Bu noktada Franz Kafka'nın "*Dava*" adlı eseri hatıra gelebilir¹²⁵. *Dava*'nın başkarakteri *Joseph K.* bir gün ansızın tutuklanır, ancak tutuklanmasına neden olan dava sürerken normal yaşamına devam edebileceğini öğrenir. Buna karşın ne tutuklanma nedeni, ne de dava hakkında bilgi sahibi değildir. Bürokrasinin içerisinde sıkışmış bir arayış içindedir. *Joseph K.*'ya ilişkin veriler temel alınarak bir karar verilmiştir. Ancak bununla savaşılabilecek hiçbir bilgiye sahip değildir.

Veri bankalarında tutulan sayısız bilgiye ilgilinin erişim olanağının bulunmadığı bir ortamda, bunların olası kullanımlarına karşı bir mücadele geliştirmek söz konusu olamayacaktır. ABD'li hukukçu Daniel J. Solove bu ilişkiyi şu şekilde açıklar: "*Gözetim çoğunlukla kayıt sistemlerinde depolanan ve yeni amaçlar için kullanılan bilgiyi üretiyor. İzlenme ve birinin davranışını engelleme sorunun yalnızca bir yönüdür. Diğer tarafta ise verilerin bilinmeyen gelecek kullnımları için depolanması bulunur. İşte bu, Orwell ile Kafka'nın buluştuğu yerdir*"¹²⁶.

Orwell'in çizdiği tabloda bireysel özerkliğin yok olduğu "*son*" kaçınılmazdır. Kısa bir süreliğine de olsa sistemin dışına çıkabilmiş birey, eğitilmiş, ıslah edilmiş ve yine sistemin içine hapsedilmiştir. Bu niteliğiyle tasvir yalnızca karanlık olmakla kalmaz, umutsuzdur da. Ancak gerçek dünyada hâlen yapılabilecek bir şeyler vardır. Bu durumda "*1984*"ü olabileceklere ilişkin bir uyarı olarak kabul etmek yerinde olur. Kişisel verilerin etkili bir şekilde korunması bireyin devlet karşısında özerkliğini sürdürebilmesinin ve demokratik toplum yapısının devamı için

¹²⁴ Arthur R. MILLER, *The Assault on Privacy, Computers, Data Banks, and Dossiers*, The University of Michigan Press, ABD 1971, s. 50.

¹²⁵ Franz KAFKA, *Dava* (Oxford Metni), çev. Ahmet CEMAL, 5. Baskı, Can, İstanbul 2005.

¹²⁶ Daniel J. SOLOVE, *The Digital Person*, s. 42.

önemli gerekliliklerden biridir. Demokratik toplumsal yapı bu hakları savunabilmek için kullanılabilecek çeşitli yollar barındırmakta ve çeşitli araçlar sunmaktadır. Ancak bu yollara başvurulması için özel olarak bireylerde, genel olarak toplumda tehlikenin ciddiyetine ilişkin bir algı oluşması şarttır.

2. KÜÇÜK KARDEŞLER

Günümüz gözetim uygulamaları ile Orwell'ın tasviri arasındaki önemli bir farklılık da gözetimin kim tarafından yapıldığına ilişkindir. 1984'ün büyük biraderi tek bir büyük gücü, devleti simgeler. Oysa teknolojinin gelişmesiyle veri toplamanın yaygınlaşması yalnızca merkezî yapıyı güçlendirmemiştir. Merkez dışı çeşitli odaklarda da bir güç yoğunlaşması yaratmıştır¹²⁷. Artık bireyleri izleyen, onların hareketlerini kayıt eden ve bütün bunları, ve daha fazlasını, yapmaya olanak veren araçları elinde bulunduranlar yalnızca devletler değildir. İşte bu nedenle, günümüzde büyük biraderin yanında bizi izleyen pek çok “küçük kardeş”in olduğundan da söz edilmektedir.

1980'li yıllardan başlayarak, özellikle İnternet'in yaygınlaşmasıyla merkezî bir yapıdan çıkarak daha çok merkez dışı bir yapıya yönelim olduğu açıkça görülmüştür. Artık verileri toplayan ve işleyenler yalnızca devletler değildir. Bilişim teknolojilerin kullanılması pek çok alanda günlük hayatın bir parçası haline gelmiştir. Örneğin iş alanında işçilere ait bilgilerin elektronik ortamda tutulması ya da işyerine giriş çıkışlarının elektronik olarak denetlenmesi normalleşmiştir. 1990'lı yıllarda ise kredi kartları ve telekomünikasyon önemli bir tartışma konusu olmaya başlamıştır. ISDN gibi dijital ağlar sayesinde pek çok bilgi bağlanılabilir kılınmıştır. Artık “cam müşteriler”in kendileri vitrin haline gelmişlerdir. Gerçekten her bir müşteri adeta “veri süpermarketleri” gibi işletmelere sınırsız olanaklar sunan pek çok bilgiyi bünyelerinde barındırmaktadır¹²⁸.

Gözetlemeye ilişkin yapıları bugün için yaşamımızda daha çok “müşteri servisleri” adı altında görüyoruz. Bize daha iyi hizmet sunmak için telefon görüşmelerimizi kayıt altına alan şirketlerin sayısı her geçen gün biraz daha artıyor. Bazı oteller, müşterilerine en iyi hizmeti sunmak ve onları evlerinde gibi hissettirmek için, onların tercihlerini uluslararası veri tabanlarından takip ediyorlar. İnternet

¹²⁷ David LYON, **Elektronik Göz**, s. 78; Daniel J. SOLOVE, **Dijital Person**, s. 7.

¹²⁸ Alessandra Di MARTINO, s. 19-20.

üzerinden satış yapan şirketler farklı demografik grupların satın alma davranışlarını izliyorlar. Bunun yanında, kredi kartı şirketleri dolandırıcılığı önlemek için ayrıntılı kayıtlar tutarken, pek çok şirket çalışanlarının iş verimliliğini denetlemek için kameralar aracılığıyla onları gözetliyor, çeşitli havayolları güvenlik için park eden bütün araçların plakalarını kaydediyor¹²⁹. İşte bu uygulamalar ve daha fazlası dolayısıyla yakında dünyanın tam anlamıyla bir kişisel bilgi piyasası haline geleceği yönünde¹³⁰ öngörülerde bulunulması hiç de şaşırtıcı değildir.

Kimi yazarlar bu şekilde, bir anlamda işletmelerin devletin yerini aldığı¹³¹ ve hatta verilerin, ticaret için devletlere göre daha değerli olduğu görüşündedir. Örneğin Lessig'e göre, devletin amacı belli bazı kurallara uygun davranışları sağlamaktır. Oysa şirketler, kişilerin paralarını nasıl harcamak istedikleri ile ilgilenirler. Kişilerin ne yaptıkları ve ne söyledikleri ile ilgili veriler, pazarın onları doğrudan ve etkili şekilde yönlendirmesini sağlar¹³². Charlesworth ise kişisel verilerin korunması açısından özel sektörün, kamu sektörü ile karşılaştırıldığında gittikçe daha yüksek oranda potansiyel tehlike yaratmasının nedenlerini beş başlık altında belirlemiştir¹³³. Buna göre:

- Teknolojinin ucuzlaması ve yaygınlaşması ile özel teşebbüsler veri işlemede daha iyi bir konuma gelmiştir.
- Özel teşebbüslerin kişisel verilerin kullanımında daha çok nedeni vardır.
- Özel teşebbüsler üzerindeki kamusal denetim daha sınırlıdır.
- Özel teşebbüsler son yıllarda serbest pazar ve deregülasyon yaklaşımından yararlanmaktadır.
- Özel teşebbüsler uluslararası alanda gittikçe daha etkili olmaktadır.

¹²⁹ Bruce SCHNEIER, s.32.

¹³⁰ Louise CADAUX, s.116.

¹³¹ Alessandra Di MARTINO, s. 18-19; Andrew CHARLESWORTH, "Clash of the Data Titans? US and EU Data Privacy Regulation", **European Public Law**, C. 6, S.2, Y. 2000, s. 254. (253-274)

¹³² Lawrence LESSIG, **Code Version 0.2.**, s.216. Şirketlerin kişisel verileri toplama gerekçelerine ilişkin bir tartışma için bkz. John HAGEL III, Jeffrey F. RAYPORT, "The Coming Battle for Customer Information", **Creating Value in the Network Economy**, Harvard Business Review Book Series, ABD 1999, s.159-171.

¹³³ Andrew CHARLESWORTH, "Clash of the Data Titans? US and EU Data Privacy Regulation", s. 254.

- Modern teknolojiyle birlikte sayıları hızla artan çok uluslu şirketler, iş yerlerinde yaptıkları değişikliklerle bazı yasal zorunluluklardan kurtulabilmektedir.
- Özel teşebbüsler öncelikle uluslararası akışı kolay, maddi olmayan veriler ile ilgilidir.

İşte bu nedenlerle, bir zamanlar yalnızca ulus devletin idari işler açısından değerlendirdiği isim listeleri, şimdi uluslararası pazarda alınıp satılmaya başlamıştır¹³⁴. Ancak bu noktada bir sorunun cevaplanması gerekir: Hergün cep telefonlarımıza gelen onlarca mesaj, e-posta kutularımızı dolduran reklamlar ya da ev, ofis telefonlarımızı sürekli çaldıran müşteri temsilcileri, pazarlamacılar, müşterileri ile ilgili yakından ilgili tüccarları mı yoksa tacizi mi akla getirmektedir?

Şebekeleşmiş bir ortamda, bilginin kolaylıkla elde edilebilmesi, gönderilebilmesi ve analizi onun ciddi bir ticarî değer olarak gelişmesine neden olmaktadır. Bu devletlerin ve diğer aktörlerin kolaylıkla toplanan, tahlil edilen ve satılan kişisel verilerle artan oranda ilgilenmesine neden olmaktadır¹³⁵. Özellikle teknolojinin ucuzlaması, kullanımının yaygınlığı ve bunların iş çevrelerine sağladığı olanaklar dikkate alındığında, büyük biraderi yenebilsek bile, küçük kardeşler karşısında kazanmanın çok daha zor olacağı¹³⁶ uyarısına kulak vermek gerekir.

Bireylerin kişisel verilerini toplayan, depolayan, işleyen ve kullanan şirketler karşısında özel yaşamlarımızı korumamızın zorluğu, vaat edilenler nedeniyle bu paylaşım çoğu zaman gönüllü olarak katılmamızdan da kaynaklanır. Bireylerin bilgiye tutsak olmuş yeni düzenin bileşeni olmayı kitlesel olarak kabul etmelerinden dolayı, gelişmeye devam eden toplum yapısını Orwell'in "1984"ü yanında Huxley'nin "Cesur Yeni Dünya"sına¹³⁷ benzetmek de olanaklıdır. Büyük Birader,

¹³⁴ David LYON, **Elektronik Göz**, s. 249.

¹³⁵ Jeffrey H. MATSUURA, **A Manager's Guide to the Law and Economics of Data Networks**, Artech House, ABD 2000, s. 71-72.

¹³⁶ Bu saptama Schneier'in "belki büyük biraderi başarı ile yendik ama küçük biraderlere kaybederek" sözüne atfen yapılmıştır. Bkz. Bruce SCHNEIER, s.33.

¹³⁷ Aldous HUXLEY, **Brave New World**, Vintage Classics, Büyük Britanya 2004. Kitaba İnternet üzerinden de şu kaynaktan ulaşılabilir: <http://www.huxley.net/bnw/index.html> (s.y. 30 Ocak 2009). Türkçe çevirisi için bkz. Aldous HUXLEY, **Cesur Yeni Dünya**, İthaki, İstanbul 2000. Huxley, Cesur Yeni Dünya romanını 1931'de yazmış ve 1932'de yayınlamıştır. İnsanların şartlandırılması ve sosyal kontrol üzerine radikal bir eleştiri niteliğinde olduğu söylenebilir: "İnsan, bir şeye inanır, çünkü onlara inanmaya şartlandırılmıştır". Huxley'nin 1958 yılında yazdığı ve kendi romanı Cesur Yeni Dünya'yı değerlendirdiği makalesi için bkz. Aldous HUXLEY, "Brave New World Revisited", 1958, <http://www.huxley.net/bnw-revisited/index.html> (s.y. 30 Ocak 2009).

yurttaşları üzerindeki denetimi, kural dışı hareketleri sert yaptırımlara bağlayarak ve onları sürekli olarak izlenme tehditi altında bırakarak sağlamaktadır. Oysa kişisel verilerle artan oranda ilgilenen iş çevreleri böylesine bir yaptırım uygulamadıkları gibi, sürekli izlenme gibi bir korkunun oluşmasını da amaçlamamaktadır. Aksine onlar, sürekli izlemeyi olanaklı olduğu ölçüde bireyler fark etmeden gerçekleştirmeyi hedeflemektedir¹³⁸.

Bireylerin verilerinin toplanması, işlenmesi ve paylaşımına gönüllü katılımları çeşitli nedenlerden kaynaklanabilir. Burada ilk akla gelen bireysel ve kamusal güvenlik gerekçeleridir. Veri toplama teknolojisi öncelikli bir savunma mekanizması olarak bireylere sunulabilir. Suç işlendiği zaman başka bir yerde bulunulduğunu kanıtlamak için ya da kamu yararı söz konusu olduğunda, bu sistem oldukça işe de yarayabilir. Belki de ileride yaşam kaydetme aletini (life recorder) üzerinizde bulundurmadığınız gün şüphe altında kalacağımız günler gelebilir¹³⁹.

İkinci olarak bireyler verilerini paylaşırken ekonomik gerekçelerle de hareket edebilirler. Pek çok şirketin sunduğu çok çeşitli hizmetleri almak ve promosyonlardan yararlanabilmek için bireyler verilerini gönüllü bir şekilde paylaşmaktadır. Tüketicilerinin cüzdanlarındaki kredi ve indirim kartları enflasyonu da bundan kaynaklanır.

Üçüncü olarak bilişim teknolojilerinin gelişmesiyle ortaya çıkan yeni türdeki bazı sosyal ilişkilerin içine girebilmek için de bireyler verilerini, üstelik çoğu kez de fütursuz bir şekilde, tanıdıkları ya da tanımadıkları pek çok başka kullanıcıya ve kuruluşa açıklayabilirler. Burada en bilinen uygulamalar web 2.0 tabanlı, yani içerikleri kullanıcıların katılımıyla oluşturulan İnternet siteleri ve kullanıcıların gerçek kişilikleri ile varoldukları sosyal paylaşım siteleridir¹⁴⁰.

Dünyanın önde gelen teknoloji ve mahremiyet uzmanlarından Simon Davies'e göre kamusal ve özel örgütler arasındaki ayrım, bütün alanlarda kayıtlara ulaşılmasını belirsizleştirmekte; kilit oyuncular tarafından belirlenen pratik çözümlerle kamusal ilgi, bireysel haklar, mahremiyet gittikçe daha etkisiz hale gelmekte; buna

¹³⁸ Daniel J. SOLOVE, *The Dijital Person*, s. 7.

¹³⁹ Bruce SCHNEIER, s.32.

¹⁴⁰ Bu konuya ilişkin olarak bkz. *How to Use Web 2.0 and Social Networking Sites Securely*, IT Governance Research Team, IT Governance Publishing, Birleşik Krallık 2009; Nicholas A. CHRISTAKIS, James H. FOWLER, *Connected: The Suprising Power of Our Social Networks and How They Shape Our Lives*, ABD 2009.

karşın bütün bu akımlara karşı duyulan tedirginlik cılız kalırken, neredeyse hiçbir tartışma da yürütülmemektedir¹⁴¹. Kitle iletişim araçlarında ve kültürün bütününde özel ile kamu arasındaki sınırlar belirsizleşmesi ile gelecekte bizi sürekli gözetleyen büyük ağabeyden çok, en az onun kadar korkutucu küçük kardeşlerle karşılaşma olasılığımız yüksek görünmektedir¹⁴².

Castells ise asıl sorunun, devletin özel yaşama yönelik tehditlerinden çok, her türden örgütlenmenin bireyler hakkında bilgi toplayarak bir pazar yaratmasında olduğu görüşündedir. Ancak bunun yanında yazar, gözetim teknolojisinin yaygınlaşmasının bireylere bazı olanaklar sağladığını da savunur. Ona göre:

“Nüfus cüzdanı bir yana, kredi kartı bütün mahremiyeti ele vermektedir. Kredi kartı, insanların hayatlarının profilinin çıkarılmasını, analiz edilmesini, insanların pazarlama (ya da şantaj) amacıyla hedef seçilmesini sağlayan bir araçtır. Hayatın kamu kayıtlarına geçmesi anlamında kredi kartını kavrayışımız, uçağa sık binenlere yönelik programlardan her çeşit tüketim hizmetine, türlü derneklere üye olmaya uzanan bir yelpazede işletmelerin sunduğu çok çeşitli hizmetleri de kapsamaktadır. Baskıcı bir “Ağabey”den çok, her birimizle kişisel düzeyde ilgili iyi niyetli bir “küçük kız kardeşler” güruhu söz konusudur; evet kişisel düzeyde ilgilidirler, çünkü kim olduğumuzu, hayatın bütün alanlarını kimlerin işgal ettiğini bilirler. ... [Y]eni teknolojiler, denetimi merkezileştirmekten ziyade izlemeyi, takip altına almayı merkezin elinden almaktadır. ... Lyon’ın ‘elektronik göz’ dediği, ‘izleyen devlet’ten çok izleyen ‘toplum’dur ... [ve] Tarihi dikkate alan bir karşılaştırmaya gidecek olursak, bugünün devleti izleyenden çok izlenendir diyebiliriz”¹⁴³.

David Brin ise geleceğimizin mutlaka gözetim altında bulunacağını ve bunun çok geçerli nedenleri olacağını (suçluluğun önlenmesi gibi) düşünmekte, bu durumda ise bizi izleyenin polis olmasındansa sıradan insanların istedikleri zaman diğerlerini gözetleyebilmesinin daha akla uygun olduğunu savunmaktadır¹⁴⁴.

¹⁴¹ Simon DAVIES, **Big Brother, Britain’s Web of Surveillance and the New Technological Order**, Pan Books, İngiltere 1996, s.xii.

¹⁴² Simson GARFINKEL, “Privacy and the New Technology”, **The Nation**, S.270, s.11.

¹⁴³ Manuel CASTELLS, **Enformasyon Çağı**, II. Cilt, s. 433-434.

¹⁴⁴ David BRIN, **The Transparent Society (Will Technology Force Us to Choose Between Privacy and Freedom)**, Addison-Wesley, ABD 1998, s.3 vd.

Bu durumda, gözetimin kimden yöneldiği noktasında konunun üç boyutu olduğu söylenebilir. Birincisi devlet ile yurttaş arasındaki ilişkiden, ikincisi özel teşebbüs ile müşteri arasındaki ilişkiden, üçüncüsü ise birey ile birey arasındaki ilişkiden kaynaklanır. Bizim konumuz açısından ilk ikisini incelememiz gerekir. Buna göre, her iki ilişki de çift yönlüdür. Bir başka anlatımla birey, devlet organları ve özel teşebbüsler tarafından izlenebildiği gibi, teknolojideki gelişme sayesinde onlar da birey tarafından izlenebilmektedir. Demokratik yönetimlerin başlıca öğelerinden biri “şeffaflık” olduğuna göre, devletin bireylerce izlenmesi demokrasiye zarar vermemekte, aksine onu güçlendirmektedir. Buna karşın bireylerin şeffaflaşması temel haklarının zarar görmesi sonucunu doğurur.

İnsanın kişiliğine ilişkin değer yargıları oluşturabilecek bilgilerin kendisinden habersiz bir şekilde toplanması, bunları düzeltme ve/veya silme olanağından da yoksun bırakılması zayıfın güçlü karşısında ezilmesi sonucunu doğuracaktır. Bu ise çoğulcu demokratik sistemlerin öngördüğü temel haklara aykırıdır¹⁴⁵. Nitekim Orwell’in tasvirinde aşırı yoğunlaşmış devlet gücü karşısında kapana kısılmış birey bulunur. Büyük biraderin yanında küçük kardeşlerin de gözetim sürecine katılması durumunda bireyin konumu daha da zorlaşmaktadır. Yine, yukarıda kısaca değinilen aşağıda biraz daha ayrıntılı incelenecek, panoptikon metaforu bunların üzerine bir de bireyin kimler tarafından, ne zaman, nerede, nasıl izlendiğini bilememesinin tedirginliğini ekler. Bu noktada kişisel verilerin korunması bireysel özerkliğin tekrar kazanılmasında ya da kaybının önlenmesinde en önemli gerekliliklerden biridir.

3. PANOPTİK CESUR YENİ DÜNYA

Elektronik gözetim (uygulayıcıları tarafından pek çok kez dile getirildiği üzere) suçluların yakalanması ve suçluluğun önlenmesi için oldukça elverişli bir araç olarak görülmektedir. Ancak bu elverişlilik ilk aşamada fark edilmeyen ve bireysel özerklik açısından çeşitli tartışma noktalarının gelişmesine neden olacak başka özelliklerinden de kaynaklanır. Bu durumu açıklamada Foucault’nun Panoptikon’a ilişkin değerlendirmeleri oldukça yararlıdır.

¹⁴⁵ Durmuş TEZCAN, “Bilgisayar Karşısında Özel Hayatın Korunması”, **Anayasa Yargısı Dergisi**, Y.1991, C.8, s.386.

Nitekim “1984” ve “Cesur Yeni Dünya”nın yanında, “panoptikon” da gözetime ilişkin güncel tartışmaların pek çoğunda kullanılmaktadır¹⁴⁶. “Görünmeden her şeyi gören göz” olarak nitelendirilebilecek panoptik mimaride¹⁴⁷, mahkûmlar ne zaman ve kim tarafından izlendiklerini bilememektedirler. Panoptikonda amaç disiplin ya da eğitimidir. Mahkûmlar, sürekli olarak izlenebilecek olmalarından ve bu sırada işledikleri suçlardan dolayı cezalandırılacaklarından korktukları sürece, kurallara uyacaklar, hatta onları özümseyecekler böylece de gerçek anlamıyla bir yaptırıma gerek kalmayacaktır.

Kimi yazarlar panoptik yapının Bentham’ın tasvir ettiği dönemde gerçekleşemese de günümüzde bir başka düzlemde “siber panoptikon”¹⁴⁸ ya da “süper panoptikon”¹⁴⁹ olarak adlandırılacak bir gerçeklik olarak karşımıza çıktığını savunmaktadır. Çeşitli yorumcular, varsaydıkları panoptikonun işlediği farklı alanları vurgulamaktadır. Buna göre, panoptik uygulamaları işyerlerinde, özellikle elektronik izlemede, güvenlik güçlerinin çeşitli faaliyetlerinde ve özellikle, parmak izi, DNA ve sabıka kayıtlarında, tüketim faaliyetlerinde ve devletin çok çeşitli idari işlerinde görmek olanaklıdır¹⁵⁰. Derecesi üzerinde tartışmalar oluşabilse de günümüz gözetim ve veri toplama sistemlerinin panoptikonu andıran bazı öğeleri bulunduğu açıktır¹⁵¹. Ancak bu noktada bir ayırım yapmak gerekir.

¹⁴⁶ Reg WHITAKER, *The End Of Privacy*, The New Press, ABD 1999, s. 32. Örneğin Oscar H. Gandy, Jr., “*kişisel verilerin ekonomi politiği*” için bilgi teknolojileri uygulamalarını tartıştığı kitabının adını “*Panoptik Tür*” olarak belirlemiştir. Bkz. Oscar H. GANDY, Jr., *The Panoptic Sort, a Political Economy of Personal Information*, Westview Press, ABD 1993. Foucault’nun gözetim ve disipline ilişkin görüşlerinin İnternet ve devlet konusundaki güncel sorunlara ilişkin bir değerlendirmesi için bkz. James BOYLE, “Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwire Censors”.

¹⁴⁷ Panoptik hapishane mimarisinin yaratıcısı Bentham, planının temel yapısına uyumlu bir şekilde “*panopticon*” sözcüğünü kullanmıştır. Bu sözcük, Yunanca kökenlidir ve “göz önündeki yer” anlamına gelir. David LYON, *Elektronik Göz*, s. 92-93.

¹⁴⁸ Örneğin bkz. Shawn C. HELMS, “Translating Privacy Values with Technology”, *Boston University Journal of Science and Technology Law*, C.7, Y.2001, s.292.

¹⁴⁹ Mark POSTER, *The Second Media Age*, Polity Press, Büyük Britanya 1995, s. 86 vd. Bu çalışmaya ayrıca İnternet üzerinden şu kaynaktan ulaşılabilir: http://is.fhs.cuni.cz/th/6794/fhs_b/poster_second_media_age_original.pdf (s.y.: 6 Mart 2009). Poster’e göre süper panoptikonun, panoptikondan tek farkı, gözetim altındakilerin gözetime gönüllü olarak katılmalarıdır. Bkz. a.g.e., s. 86. Poster’in süper panoptikona ilişkin görüşlerinin kısa bir eleştirisi için bkz. Zygmunt BAUMAN, *Küreselleşme*, s.60-61.

¹⁵⁰ David LYON, *Elektronik Göz*, s. 98.

¹⁵¹ Şuna da işaret etmek gerekir ki, Foucault’nun değerlendirmeleri konusunda ilginç olan şeylerden biri, izleme ve insanları nesneleştirme süreci üzerinde durmasına karşın, bilişim teknolojilerinin mevcut ya da olası etkilerine hiç değinmemesidir. Foucault’nun analizlerini yeni gelişen bu teknolojilerin sosyal yönüne uyarlama işini ondan sonra gelen başka yazarlar yapmıştır.

Birincisi panoptik mimari, merkezde mahkûmları gözleyen bir büyük müfettişi öngörmüştür. Bu şekliyle “büyük birader”i anımsatan merkezileşmiş bir gözetim söz konusudur. Nitekim devletlerin bireyler üzerinde yoğunlaşan gözetimine ilişkin olarak Orwell’ın yanında Foucault’nun isminin de sıklıkla anıldığı görülmektedir¹⁵². Yukarıda açıklandığı üzere günümüzde yalnızca merkezde yoğunlaşan bir gözetimden söz etmek olanaklı değildir. Bir yandan devletler gözetimlerini arttırırken¹⁵³, öte yandan özel teşebbüsler de kendi panoptikonlarını yaratmaktadır¹⁵⁴.

Bunun yanında bireylerin de gözetim sürecine katıldıklarına ilişkin görüşleri dikkatten kaçırmamak gerekir. Thomas Mathiesen, panoptik gücün ortaya çıkmasını 1800’lerdeki büyük bir dönüşümle ilişkili olduğunu söylemektedir. Ona göre bu dönüşüm, çok fazla kişinin pek azı kişiyi gözlediği bir durumdan, pek azın çok fazlayı gözlediği duruma doğru olmuştur. Ancak Mathiesen Foucault’yu bundan sonraki aşamada gerçekleşen bir evrimi dikkate almaması nedeniyle eleştirir: televizyon ve diğer kitle iletişim araçları ile tekrar, azın çok tarafından seyredilmesini sağlayacak bir güç mekanizması ortaya çıkmıştır. “*Synoptikon*” adını verdiği bu mekanizma, panoptikonla birlikte durmaksızın yükselmektedir¹⁵⁵.

İkinci olarak, panoptikonda disiplin gözetleyenlerin görünmezliği ile sağlanmaktadır. Sürekli olarak izlenme olasılığı bulunduğunu bilen mahkûmların bu

¹⁵² LYON’a göre sıklıkla yanyana anılan büyük birader ve panoptikon metaforlarının arasında ilk başta dikkat çekmeyen bir farklılık da bulunur. Yazar ayrıca bu görüşlere sıklıkla atıf yapılmasına da eleştirel yaklaşmaktadır: “Orwell’in görüşüyle, Foucault’nun Bentham’ının görüşü arasında bazı farklar vardır. Orwell’inki “mümkün fakat önlenabilir” bir gelecek olarak görülebilirdi, oysa diyelim Rule’un ellerinde Foucault’nun panoptikonu sık sık yakın ve kaçınılmaz görünür. Orwell’in kara ütopyasının çağdaş yorumcuları, belirli koşullar altında eylemi ve direnişi canlandırabilirler-“Büyük Ağabey seni gözliyor” en ünlü gözetim karşıtı slogan olsa gerek-fakat Foucault’nun kara ütopyası daha ziyade insana paranoyayı ve donup kalmayı telkin ediyor gibi görünür. 1984 hala zayıf bir demokrasi ve görgü umudu taşıırken, Disiplin ve Cezalandırma her yere uzanan bir iktidar söyleminde bu umutları yok eder”. David LYON, **Elektronik Göz**, s. 282.

¹⁵³ James BOYLE göre devlet bir “*Internet panoptikonu*” yaratmak amacındadır. Bu ise, asıl sorumluluğu merkezden İnternet servis sağlayıcılara ve diğer kuruluşlara kaydırarak oluşturduğu “işlem mimarisi” ile gerçekleştirilmektedir. Bkz. James BOYLE, s. 180, 197-198.

¹⁵⁴ Paul M. SCHWARTZ, “Internet Privacy and the State”, **Connecticut Law Review**, Y.2000, C. 32, s. 852 vd. <http://www.paulschwartz.net/pdf/SCHWARTZ-CK1A.pdf> (s.y. 10 Şubat 2009).

¹⁵⁵ Thomas MATHIESEN, “The Viewer Society”, **Theoretical Criminology**, C.1, S.1, Y. 1997, s. 215-234; Zygmunt BAUMAN, **Küreselleşme**, s. 61-63. Foucault’nun görüşlerine karşı Mathiesen’in eleştirisinin 11 Eylül 2001 olayları sonrasında gelişen medya pratikleri ekseninde değerlendiren bir çalışma için bkz. David LYON, “9/11 Synopticon, and Scopophilia: Watching and Being Watched”, **The New Politics of Surveillance and Visibility**, haz. Kevin D. HAGGERTY, Richard V. ERICSON, University of Toronto Press, Kanada 2006, s. 35-54.

nedenle kurallara uygun davranmaları sistemin temel mantığını oluşturur. Bu niteliği dolayısıyla panoptik yapının, bilişim teknolojileri ile yaşama geçtiği söylenebilir. Veriler çoğu zaman bireyler farkında bile olmadan ve onların izni bulunmaksızın toplanmaktadır. Özel yaşamın gizliliğini savunanların üzerinde kuvvetle durdukları anonimlik hakkına rağmen bireylerin kimliklerinin ortaya çıkabilmesi de başka bir sorundur¹⁵⁶.

RFID yongaları ve CCTV kameraları bu bağlamda değerlendirilebilir. RFID yongaları ile bireyler “*nesnelerin İnternet’i*” olarak adlandırılan, birbiri ile iletişim kurabilen nesneler aracılığıyla hiç fark etmeden sürekli izlenmektedir¹⁵⁷. Benzer bir durum kapalı devre televizyon (CCTV) sistemleri için de söz konusudur. Hem devlet, hem özel teşebbüsler, hem de bireylerce sıklıkla kullanılan bu kameralar günümüzde artık her yerdedir ve genellikle panoptikondakine benzer bir amaca, güvenliği sağlamaya ve insanları kurallara uygun davranmaya zorlamaya yönelmiştir¹⁵⁸.

Sorun, bireyler için gözlem yapılmasından öte, bireylerin gözlenmesindedir¹⁵⁹. Güvenliğin sağlanması her yurttaşın devletinden beklediği bir gerekliliktir, ancak güvenlik gerekçeleri ile bireylerin devlet tarafından sürekli izlenmesi temel hakların zedelenmesine neden olur. Ayrıca bu sistemler, bireyler üzerinde sürekli olarak izlendikleri duygusu yaratmakta, kişilerin kendilerini potansiyel suçlu gibi hissetmelerine neden olmaktadır. Bunun sonucunda bireylerin sisteme küsmesi ve gitgide yabancılaşmaları söz konusu olabilir.

4. DİJİTAL KİŞİLİK

Kişilere ilişkin bilgilerin toplanma yöntemleri temelde ikiye ayrılarak değerlendirilebilir. Birincisi, doğrudan bir kişiye ya da kuruma ilişkin bilgilerin toplanması, ya da başka bir anlatımla belirli bir hedefe yönelmiş saldırılardır. İkincisi veri toplamaktır. İkinci yöntemde bir bağlantıdan yararlanıldığı görülür. Belirli bir

¹⁵⁶ Louise CADAOUX, s.115.

¹⁵⁷ Jeroen Van Den HOVEN, Pieter E. VERMAAS, “Nano-technology and Privacy: On Continuous Surveillance Outside the Panopticon”, **Journal of Medicine and Philosophy**, C.32, Y.2007, s. 283-297.

¹⁵⁸ Bert-Jaap KOOPS, Ronald LEENES, “ ‘Code’ and the Slow Erosion of Privacy”, s. 2, <http://law.bepress.com/expresso/eps/625> (s.y. 2 Şubat 2009).

¹⁵⁹ Sloganın “*büyük birader senin için diğerlerini izliyor*” mu, yoksa “*büyük birader seni izliyor*” mu olacağı önemlidir. Reg WHITAKER, s. 141.

İnternet sitesini ziyaret edenlerin listesinin çıkartılması, bankada belirli bir miktarın üzerinde parası olanların saptanması buna örnek olarak gösterilebilir¹⁶⁰.

Birincisi, özellikle modern devlet ile birlikte sıklıkla gördüğümüz bir uygulamaya işaret eder. Özellikle güvenlik gerekçesiyle pek çok kişinin hakkında araştırma yapıldığı, izlendiği ve “*fişlendiği*” bilinmektedir. Haberleşmenin gizliliğine ilişkin ilkelerin belirlenmesi, konut ya da üst aramanın hukuksal sınırlarının çizilmesi bir kişinin özel yaşamına yönetimin keyfî müdahalesini engellemek amacını taşımaktadır. Yeni teknolojilerin sağladığı olanak daha çok bu yöntemin etkinliğine ilişkindir. Artık telefon dinleme, hatta bir kişinin evinde ya da başka bir ortamda yaptığı konuşmaların dinlenmesi, günlük yaşamların ve pek çok tercihin izlenmesi ve toplanan bütün bu bilgilerin birbiriyle ilişkilendirmesi çok daha kolay, hızlı ve düşük maliyetlidir.

İkinci yöntemin yapılabilirliği ise teknolojiyle daha yakından ilişkilidir. Bilgisayar tabanlı ürünler ve diğer teknolojiler yaşamlarımızın içine girdikçe, birbirinden farklı merkezlerde verilerimizin toplanması ve bunlardan bütünlüklü profillerimizin çıkarılması, veri imgelerimizin oluşturulması olanaklı duruma gelmiştir. Bir başka anlatımla belirli ya da belirlenebilir bir kişiyi hedef almadan toplanan bu veriler ile ilgili kişilerin belirlenebilir kılınması, hatta bundan da öteye çok ayrıntılı bir şekilde tahlil edilebilecek bir bilgi topluluğuna ulaşılması olanaklıdır. Bu izleme, ekonomik, siyasal, sosyal gerekçelerle temellendirilebilmektedir. Doğrudan bir kişiyi hedef almadan veri toplama işlemi güvenlik ve benzeri gerekçelerle gerçekleştiriliyorsa masumiyet karinesinin ihlal edilmesi de söz konusu olacaktır. Nitekim bu uygulama, herkesin potansiyel suçlu olarak görülmesine neden olabilir.

Bunun yanında teknolojinin sağladığı olanaklarla devlet, bireyin sadece fiziksel varlığını değil, duygu, düşünce ve geleceğe yönelik planlarını da gözetleyip yönlendirme olanağına kavuşmuştur¹⁶¹. Özel girişimlerin kişisel verilere duydukları ilginin nedeni belirli açılardan farklılaşsa da bu hususta ortak noktalar bulunduğu açıktır. Özel teşebbüsler de müşterileri istedikleri gibi yönlendirme amacını

¹⁶⁰ Bruce SCHNEIER, s. 29-30.

¹⁶¹ İbrahim CERRAH, “Bilişim Teknolojileri ve Etik: Bilişim Teknolojilerinin Güvenlik Hizmetinde Kullanımının ‘Etik Boyutu’ ve ‘Sosyal’ Sonuçları”, **Uluslararası Polislik ve İç Güvenlik**, Haz. Tülin Günşen İÇLİ, Fatih KARAOSMANOĞLU, Nobel, Ankara 2003, s. 456.

taşımaktadır¹⁶². Noam Chomsky bu olguyu “rıza üretimi” olarak adlandırır. Bir başka anlatımla insanlara yüzeysel bir bireysellik ve bir öze sahip olduklarına ilişkin bir görüntü verilmektedir¹⁶³. Ancak görüntü her zaman gerçekliğe karşılık gelmeyebilir.

Bu anlamda, bireye yönelen tehdidin tek bir merkezden değil, işyeri, okul ve tüketim kültürünün bir arada oluşturduğu baskılardan kaynaklandığına dikkat çekilmeye başlanmıştır. Böylece insanın “öz”ünün, onu homojenleştirerek aşındırılabilmesi, her kişinin kendine özgü içsel yapısından kaynaklanan isteklerini ve hayallerini yeniden inşa ederek gölgelenebilmesi dikkate değer bir tehdittir ve gözetimin diğer yüzünü oluşturur. Bunun çok önemli sosyal sonuçları olabilir. Çünkü bu şekliyle gözetim, toplumun düzenlenmesine katkıda bulunmaktadır. Bunu ise sosyal ve ekonomik ayrımları destekleyerek, tercihleri kanalize ederek, istekleri yöneterek ve hatta kısıtlayıp denetim altında tutarak gerçekleştirir¹⁶⁴.

Nitekim, daha önce de işaret edildiği gibi, her yerde izlenme, gözetlenme olasılığı bulunduğunu bilen, bunu çok yakın potansiyel bir tehlike olarak algılayan bireyin hareketlerinde ne kadar özgür olabileceği şüphelidir. Ancak sorun bu noktada da bitmemektedir. Veri imgeleriyle eğilimleri, tercihleri, istekleri belirlenen bireyin, başta ticarî kaygılar olmak üzere, çeşitli nedenlerle yönlendirilmeye açık olduğu ortadadır. Bilgi güç verir ve kişisel bilgileri üzerinde denetimini kaybeden birey hızla güçsüzleşir. Bunun yanında eğer özel yaşamın gizliliği hakkı kişiliğe bağlı ise, benzersiz kişiliğin kaybı özel yaşamın gizliliği hakkını da anlamsız kılacaktır¹⁶⁵.

Ayrıca insanın kendine ilişkin bilgilerini ne oranda kimlere açıkladığı yakın zamana kadar karşılıklı bir güven ilişkisi içerisinde gerçekleşmiştir. Hekimlerle, psikologlarla, arkadaşlarla, aileyle yaşanan paylaşımın hep bu ilişki çerçevesinde gerçekleştiğini gözlemleyebiliriz. Teknolojideki gelişmeler sonucunda çok çeşitli kaynaklardan bilgiler toplanabilmesi ve üstelik de bunlar arasında kolaylıkla ve hızla bağlantı kurulabilmesi öncelikle bu güven ilişkisinin yok olmasına neden olabilir. Örneğin sağlığına ilişkin bilgilerin başkalarıyla paylaşılabilmesini düşünen kişi, tedaviden kaçınabilir.

¹⁶² Bert-Jaap KOOPS, Ronald LEENES, s.2.

¹⁶³ Harry HENDERSON, s.12.

¹⁶⁴ David LYON, **Günlük Hayatı Kontrol Etmek**, s. 16.

¹⁶⁵ Harry HENDERSON, s. 12; Simson GARFINKEL “Privacy and the New Technology”, s.11; Simon DAVIES, **Big Brother**, s.53.

Sorunun başka boyutları da bulunmaktadır. Artık bu bilgiler, tanımadığımız kişi ya da örgütlere elektronik araçlarla iletilmektedir. Bu kişiler ve makineler ise bizleri veri imgemiz üzerinden kavramaktadır¹⁶⁶. Doğum belgesinden ölüm kağıdına kadar, bir başka anlatımla dünya üzerindeki ilk gününden son gününe kişinin bilgileri çeşitli araçlarla kayıt altına alınmaktadır. Bu kayıtları ilişkilendirebilmek ve kullanabilmek için pek çok alanda sayılara başvurulur. Kaçınılmaz sonuç, 21. yüzyıl insanının artık yalnızca adı ile değil, kendisini niteleyen pek çok sayı ile tanımlanmasıdır. Vatandaşlık numarası, pasaport numarası, okul numarası, banka numarası, sigorta numarası yalnızca bir kaç örnektir¹⁶⁷.

Bu durumda ise, bireyin öznenen nesneye dönüşme sürecine girmesi de bir tehlike olarak karşımıza çıkabilir. Nitekim kişisel verilerin korunmasına ilişkin ilk dönem analizlerinde bu soruna işaret edildiği görülür. *Miller*'a göre, toplum, modern yaşamın bilgi merkezli yapısını ve kendileri hakkında çok büyük miktarlarda bilginin kayıt altına alındığını fark ettikçe, doğal olarak ana bilgisayarın koridorlarında depolanmış kendi elektronik profilleri dışında varlıklarının ya da kimliklerinin bulunup bulunmadığı konusunda şüpheye düşebilir¹⁶⁸. İnsanlar veri imgelerinin karşılaşacakları fırsatlar üzerinde nasıl bir etkiye bulunabileceği konusunda uyanık olmalıdır¹⁶⁹.

Kullanıcılar interaktif bir araçla etkileşime girdiklerinde sisteme kişiliklerine ilişkin çeşitli bilgiler aktarır. Zevkleri, tüketim tercihleri yanında, elektronik oyunlarla zekâ düzeyleri, tartışma gruplarıyla siyasal düşünceleri hakkında ayrıntılar da iletilebilmektedir¹⁷⁰. Bu bilgilerin sistem içerisinde bir yerlerde saklandığını saptadığımızda, bunların “nerede”, “ne için”, “kimler” tarafından kullanıldığını sormamız kaçınılmaz bir gerekliliktir. Bu gereklilik bilgilerin otomatik şekilde değerlendirilip mantıklı sonuçlara ulaşılabildiğinde daha da aciliyet kazanacaktır. Çünkü artık bir anlamda kişiliğimizin dijital bir yansımasının oluşabileceğini kavramış bulunuruz.

¹⁶⁶ David LYON, *Elektronik Göz*, s. 36.

¹⁶⁷ Peter SCHAAR, *Das Ende der Privatsphäre*, s. 98.

¹⁶⁸ Arthur R. MILLER, *The Assault on Privacy*, s. 49.

¹⁶⁹ Gary T. MARX, “For Sale: Personal Information About You”, *Washington Post*, 11 Aralık 1989, bu makaleye ayrıca şu kaynaktan ulaşılabilir: <http://web.mit.edu/gtmarx/www/forsale.html>.

¹⁷⁰ Lawrence EARLY, “Science, Technology and Human Rights: The Role of Data Protection”, *Human Rights in the Twenty-first Century, A Global Challenge*, C.2, haz. Katleen E. MAHONEY, Paul MAHONEY, Maritus Nijhoff Publishers, Hollanda 1993, s. 804-805.

Nitekim bilgisayar teknolojileri, kişisel verilerin kolaylıkla toplanması ve saklanmasına olanak tanıdığı gibi, veriler arasında ilişki kurarak bireyler hakkında ayrıntılı profiller oluşturulmasını da sağlamaktadır. Bu bağlamda “*veri eşleştirme*” (data matching) iki ya da daha çok kaynaktan elde edilen kişisel verilerin otomatik olarak karşılaştırılması ve analiz edilmesi sürecini ifade eder¹⁷¹. Veri eşleştirme, bütün toplum için geçerli bir genel yetki yasasının teknolojik eş değeridir. Bunun polisin bir evi aramasına, belgeleri incelemesine ve istediklerinin kopyasını almasına izin veren bir yetkilendirmeden farkı yoktur¹⁷². Kimileri bunu potansiyel olarak herkes için “*elektronik siciller*”in gelişimi olarak adlandırırken, kimileri de bu süreci “*verizilme*” (dataveillance)¹⁷³ olarak adlandırmaktadır¹⁷⁴. Gerçekten veri eşleştirme yönteminin akıllara getirdiği, ilk ve belki de en önemli soru, devletlerin verizleme olarak bilenen bir gözetim çeşidini kullanıp kullanmayacaklarıdır.

Verizleme, fiziksel gözlem yerine, bilgisayar verileriyle otomatik izleme anlamına gelir. Özellikle son otuz yılda gerçek kişiler yerine onların “*veri gölgeleri*”ni ya da dijital kişiliklerini izleyen yeni gözetim hızla gelişmiştir. Günümüzde birey, doğumundan ölümüne kadar ilişki içerisinde bulunduğu çeşitli kurum ve kuruluşlara kendisine ilişkin bilgiler vermektedir. Kamu kurumlarında bulunan, doğum, okul, sağlık, pasaport, sabıka...vb. kayıtları; özel kurumlarda bulunan müşteri eğilimlerine ilişkin bilgiler kişilere ilişkin önemli verileri oluşturur. Farklı kaynaklarda bulunan bu bilgilerin birleştirilmesi, işlenmesi, başka kurum ya da kuruluşlara gönderilmesi sonucunda bir kişinin yaşamına ilişkin önemli ayrıntıları da kapsayan bir veri profilinin oluşturulabileceği açıktır: “[B]u yeni aygıt ve yöntemlerle, istenirse kişiye, özel yaşamın gizliliğinin gerçekleştirilebilmesi konusunda hiç olanak bırakılmayabileceği anlaşılmaktadır. Artık insanlar Sartr’ın deyimiyle, tam anlamıyla birbirlerinin cehennemine dönüşmeye başlamışlardır”¹⁷⁵.

Verizleme yoluyla özel olarak belirli bir kişinin izlenmesi (kişisel verizleme) olanaklı olduğu gibi, aranan kişileri bulmak ya da kural dışı hareket etme olasılığı

¹⁷¹ Benzer bir tanım için bkz. Simon DAVIES, **Big Brother**, s. 83.

¹⁷² Simon DAVIES, 89.

¹⁷³ “*Dataveillance*” deyiimi Roger Clarke tarafından, “*data*” (veri) ve “*surveillance*”(gözetleme/izleme) kelimelerinin birleştirilmesiyle oluşturulmuştur. Bkz. <http://www.rogerclarke.com/DV/> (s.y. 10 Mart 2009).

¹⁷⁴ Ann CAVOUKIAN, Don TAPSCOTT, **Who Knows, Safeguarding Privacy in a Networked World**, McGraw-Hill, ABD 1997, s. 50.

¹⁷⁵ Oya ARASLI, s. 36-37, 39.

bulunanları caydırmak amacıyla, bir grubun ya da daha geniş kitlelerin izlenmesi (kitlesele verizleme) de olanaklıdır¹⁷⁶. Çünkü veri eşleme yöntemi, herhangi bir şüphe ya da neden olmaksızın yapılan keyfi soruşturmalara eş değerdir. Bunun yanında veri eşleştirme “suçluluk karinesi”ne dayanır. Bu sistemin temel mantığında herkes potansiyel suçludur. Bu ise insan haklarının ve hukuk düzeninin temel kavramlarından birine aykırılık oluşturur.

Ayrıca veri eşleştirme, özel yaşamın gizliliğinin ve kişisel verilerin korunmasına ilişkin bazı temel ilkelerin ihlal edilmesine de neden olmaktadır. Bunlardan belki de ilk akla gelen, belli bir amaç için elde edilmiş bir bilginin, ilgilinin rızası olmaksızın, başka bir amaç için kullanılamayacağı ilkesidir.

Uzun vadede söz konusu olabilecek başka bir tehlike ise evrensel bir nüfus numaralandırma sistemidir. Yalnız şunu da dikkatten kaçırmamak gerekir: kişiyi doğrudan niteleyen bir ulusal numaranın yokluğunda bile, eğer tam bir bağlantı kurulabilirse veri eşleştirme ile aynı sonuç yaratılabilir¹⁷⁷.

Bir başka önemli sorun eşleştirilen verilerin doğruluğuna ilişkindir. Farklı zamanlarda, farklı yerlerden toplanmış bilgiler birleştirildiği zaman gerçeği tam yansıtmayan sonuçlara da ulaşılabilir. Bir kişi araştırma için bir kez etiketlendiğinde istisnasız her olayda, devlete onun suçluluğunu kanıtlama yükü düşeceğine, suçsuzluğunu kanıtlama bu kişiye yüklenecektir. Yanlış bilgileri ve eşleştirmeleri düzeltmeye çalışan kişi, yalnız bu süreç yüzünden bile zarara uğrayabilir. Veri eşleştirmenin yaygınlaşması, çeşitli kuruluşlara her birey hakkında yargılamalara varılabilecek, ayrıntılı profiller oluşturma olanağı sunacaktır¹⁷⁸.

İnternet servis ve erişim sağlayıcılarının da elinde, mahremiyeti ihlal açısından önemli bir potansiyel güç bulunur. Sanal alışveriş yapılan siteler yalnızca satın alınanların değil, bakılıp alınmayanların da kaydını tutabilmektedir¹⁷⁹. Bunun yanında polislerin tuttuğu veritabanları suçluları yakalamakta oldukça yararlı olsalar da herhangi bir ticarî veri tabanından daha güvenli değildir, fakat onlardan çok daha hassas bilgileri içerir¹⁸⁰.

¹⁷⁶ Roger CLARKE, “Dataveillance: Delivering ‘1984’”, s. 4.

¹⁷⁷ Simon DAVIES, **Big Brother**, s. 89-91.

¹⁷⁸ Simon DAVIES, **a.g.e.**, s. 91-92.

¹⁷⁹ Bruce SCHNEIER, s.33.

¹⁸⁰ Bruce SCHNEIER, s.34.

Örnekler çoğaltılabilir. Ancak şurası açıktır: kişisel verilerin toplanması, kullanılması ve aktarılması çeşitli açılardan gereklidir. Amaca uygun rasyonel karar verebilme için elverişli bir araç olmaktadır. Bu gerekliliğe karşın olası yan etkiler konusunda dikkatli olunmalı ve insanı insan yapan değerlere zarar gelmemesi bir ön koşul olarak değerlendirilmelidir. İnsanı insan yapan biraz da yaşamın öngörülmezliği, rastlantısallığı içerisinde yolunu bulma arayışı değil midir? Yevgeni Zamyatin'in "*Biz*" adlı eserinde resmettiği yalnızca sayılardan ibaret bir toplumun parçalarını "*insan*" olarak nitelemeye devam edebilmek çok da kolay değildir. Matematiksel kesinlik ve mutlak rasyonelliğin katılığı burada yaşam olarak adlandırılan sürece insanın verdiği anlamı da dönüşüme uğratabilir. Hem "*1984*", hem "*Cesur Yeni Dünya*", hem de "*Biz*"de görülen sürekli izleyen devletin insana özgü değerleri yok edebileceğidir. Herşeyin matematiksel bir kesinlik içinde olduğu, planlanmış bir dünyada insanın ihtiyacı olan yaratıcılığa ya da rastlantısallığa yer yoktur.

Bütün bu gelişmeler, 20. Yüzyıla atfen kullanılan bilgi toplumunun üyesi olup olmama konusunda artık bireylerin bir seçim hakkı kalmadığını göstermektedir. Kişisel verilerin bir veya birden çok merkez tarafından, etkin ve etkili bir şekilde toplanabilmesi, işlenebilmesi, yayılabilmesi ve değerlendirebilmesi bireylerin sürekli izlendikleri duygusunu taşımalarına neden olmaktadır. Teknolojinin kuşattığı modern birey adeta çırlıçıplak kalmıştır ve hala kendine ait mahrem alanı koruyabilmek ve farklı kılıklar içinde toplumsal yaşamını sürdürmek için bir koruma alanına gereksinim duymaktadır. İşte kişisel verilerin korunmasının bireye sağladığı, ya da sağlamayı vaat ettiği değer, temelde budur.

II. KİŞİSEL VERİLERİN KORUNMASI HAKKI

A. GENEL OLARAK

Kişisel verilerin korunması, kendisinden daha köklü bir tarihe sahip başka hak alanları ile yakın ilişki içindedir. Bunların başında özel yaşamın gizliliği hakkı gelir. Bunun yanında, kişisel verilerin korunması düşüncüyü açıklama özgürlüğü, bilgi edinme hakkı, haberleşme özgürlüğü gibi başka bazı değerlerle de kimi zaman karşılıklı destekleme, kimi zaman çatışma halindedir. Ancak bu konulara ilişkin

açıklamalara geçmeden önce, kişisel verilerin korunmasının dayandığı temel çıkardan hareket eden bazı teorik tartışmalara değinmek gerekir.

B. BİR “HAK” ALANI OLARAK KİŞİSEL VERİLERİN KORUNMASI

Kişisel verilerin korunması ile amaçlanan çıkarın ne olduğu sorusu özellikle kıta Avrupa’ında ve ABD’de birbirinden farklı şekilde yanıtlanan, ya da en azından birbirinden çok farklı bir bağlamda tartışılan bir soruyu oluşturur: veri, üzerinde tasarrufta bulunulabilen bir mal olarak mı değerlendirilmelidir, yoksa bireylere doğal hukukça bahşedilmiş doğuştan gelen bir hak mı?

Yaklaşımlar çeşitli olsa da temelde ikiye ayrılabilir: birincisi kişisel verilerin korunmasını ekonomik bir hak olarak değerlendiren yaklaşım; ikincisi ise insan hakları kapsamında inceleyen yaklaşımdır.

1. EKONOMİK HAK YAKLAŞIMI

Kişisel verilerin korunmasına Avrupa yaklaşımı “sosyal değer” merkezli iken, Amerikan yaklaşımı, “ekonomik-teknolojik” bir yapı sergiler¹⁸¹. Bu, aslında her iki kıtanın bilgi altyapısına bakış açısındaki farklılığın bir uzantısıdır. Gerçekten Avrupa’da “bilgi toplumu”ndan söz edilirken, ABD’de daha çok “bilgi ekonomisi”nin tartışıldığı görülmektedir¹⁸².

ABD’de kişisel veriler son derece düşük düzeyde korunmaktadır. ABD’de kişisel verilerin korunması konusunda genel olarak Avrupa’daki gibi katı ve kapsayıcı bir düzenleme rejimi yerine sektörel çözümlerin tercih edildiği görülmektedir¹⁸³. Kişisel verilerin korunmasının bir hak alanı olarak tanınıp tanınmaması ve eğer tanınıyorsa bunun niteliği konusunda da görüş birliği bulunmamaktadır. Kimi hukukçular ve iktisatçılar, kişisel verilerin geniş oranda

¹⁸¹ H. BURKERT, “Privacy/Data Protection: A German/European Perspective”, Proc. 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council, Wood Hole, Mass. 1999’dan aktaran; Roger CLARKE, “Beyond the OECD Guidelines: Privacy Protection for the 21st Century, 4 Ocak 2000, <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html> (s.y. 2 Şubat 2009) .

¹⁸² 1993 yılından beri Avusturalya’nın da benzer bir yaklaşımı benimsediği söylenebilir. Roger CLARKE, “Beyond the OECD Guidelines”.

¹⁸³ Corien PRINS, “Property and Privacy: Perspectives and the Commodification of our Identity”, **The Future of the Public Domain**, haz. L. GUIBAULT, P.B. HUGENHOLTZ, Kluwer Law International, Hollanda 2006, s.224.

korunmasının ticarî ilişkilerin sağlıklı bir şekilde yürümesini engelleyeceği, bilgi edinmede sorun yaratacağı, işlem maliyetlerini yükselteceği gibi çeşitli sakıncaları olduğunu ileri sürmektedir¹⁸⁴.

Bunun yanında kanımızca, kişisel verilerin korunmasına ekonomik değeri temel alan yaklaşımda Amerikan hukukunun kendine özgü yapısı da etkili olmuştur. Amerikan hukukunda, kişisel verilerin korunması hakkını da içeren özel yaşamın gizliliği hakkı Anayasal bir hak değildir. Aşağıda inceleneceği üzere, bu hak alanı, 19. Yüzyılın sonlarında tartışılmaya başlanmış ve ilerleyen yıllarda içtihatlarla kabul görmüştür. Zaman içerisinde kişisel verilerin korunması gereksiniminin ortaya çıkması ile bu alan özel yaşamın gizliliği hakkı içinde değerlendirilmiştir¹⁸⁵. Korumanın derecesi ve şekline ilişkin hararetli tartışmalar sürse de Amerikalı hukukçuların kişisel verilerin korunması gerekliliğine işaret eden pek çok yayın yaptıkları görülmektedir¹⁸⁶. Bu durumda, yeni gelişen bu koruma alanına sağlam bir temel bulma arayışının da aşağıdaki teorilerin geliştirilmesinde etkili olduğu söylenebilir.

¹⁸⁴ Patricia L. BELLIA ve diğ., s.606-607. Bu sakıncaları ileri süren bazı çalışmalar için örneğin bkz. Richard A. POSNER, “The Right of Privacy”, **Georgia Law Review**, C.12, Y. 1978 s.393-422, 398; George J. STIGLER, “An Introduction to Privacy in Economics and Politics”, **Journal of Legal Studies**, C.9, Y.1980, s.623-644. Bu maliyetlerin fazlasıyla abartıldığına ilişkin karşı görüş için bkz. Richard S. MURPHY, “Property Rights in Personel Information: An Economic Defence of Privacy”, **Georgetown Law Journal**, C.84,Y. 1995, s. 2381-2417.

¹⁸⁵ Pek çok ABD’li yazar, kişisel verilerin korunması hakkını, “*özel yaşamın gizliliği hakkı*”nın (privacy right), özel bir türü olarak nitelemekte ve bu alanı işaret etmek için “*bilgisel gizlilik*” (informational privacy) deyimini kullanmaktadır. Bilgisel gizlilik ile iradi gizlilik gibi başka bazı özel türlerin arasındaki ilişkiye dair tartışma için bkz. Paul M. SCHWARTZ, “Property, Privacy and Personal Data”, **Harvard Law Review**, S.117, Y.2003-2004, s.2058.

¹⁸⁶ Fikri mülkiyet ve düşünceyi açıklama özgürlüğünün Amerikan ekonomisi ve politikası açısından önemi dolayısıyla siber uzayda telif hakkı ve pornografi konularına ilişkin daha fazla yayın yapılıyor olması da bunun bir göstergesi sayılabilir. Jerry KANG, Information Privacy..., s. 1196. Bunun yanında yapılan araştırmalar, Amerika’da özellikle İnternet ortamında özel yaşamın gizliliği hakkının sağlanmasına ilişkin kaygıların arttığını göstermektedir. 6486 Amerikalı tüketicinin katılımı ile gerçekleştirilen bir araştırma kişisel verilere verilen önemin önceki yıllara görece arttığını (2006 yılında kişisel mahremiyetlerini önemli yada çok önemli gören tüketicilerin oranı %69 iken 2008’de bu oran, %73’e çıkmıştır) ve kişisel verileri üzerinde kontrolleri olduğu düşüncesinin azaldığını (2006’da katılımcıların %56’sı, 2008’de ise %45’i kişisel verileri üzerinde kontrollerinin bulunduğu düşüncesindedir) ortaya koymuştur. Bkz. Ponemon Institut and TRUSTe Announce Results of Annual Report Most Trusted Companies for Privacy Survey, http://www.truste.org/about/press_release/12_15_08.php (s.y.6 Şubat 2009).

a. Mülkiyet Hakkı Teorisi

Özel yaşamın gizliliğini korumak için ortaya atılan görüşlerden biri kişisel bilgilerin bir mülkiyet türü olduğu görüşüdür¹⁸⁷. Ayrıca kişisel verilere mülkiyet hakkı temeline dayanan bir koruma sağlanırsa, veri öznesinin kendine ilişkin bilgiler üzerinde tam bir denetim hakkına sahip olacağı ve mülkiyet sahibine tanınan geniş yasal korumalardan da yararlanacağı düşünülmüştür.

Verilerin mülkleştirilmesini savunan yazarlar, bu yolla bireylerin uygun anlaşmalar yaparak verilerinin kullanımının karşılığını alabileceklerini, böylece kişisel veriler pazarının daha adil işleminin sağlanabileceğini ileri sürmektedir. Bu bağlamda bireyler istedikleri takdirde kişisel bilgilerini satabilmeli ya da açıklayabilmelidir¹⁸⁸. Bunun yanında bu yaklaşımın şirketleri kişisel verilerin toplanması ve işlenmesinden dolayı ortaya çıkan maliyetleri benimsemeye zorlayacağı ve bu yolla özel yaşamın gizliliğinin daha güçlü bir şekilde korunacağı da savunulmaktadır.

Mülkiyet hakkı yaklaşımı, bireylerin, verilerinin özel sektör tarafından kullanılmasına ilişkin değişen tercihlerine uyum sağlaması açısından yararlıdır. Çünkü kimi bireyler, özel yaşamlarının gizliliğini önemli görerek verilerin değiş-tokuşuna izin vermek istemeyeceği gibi, kimileri de bunları çeşitli şirketlere satmak konusunda istekli olabilir¹⁸⁹. Mülkiyet teorisinin güçlü yanı, bilgilerinin kötüye kullanılması durumunda ilgili kişiye doğrudan dava açma ya da zararın giderilmesi için talepte bulunma hakkını vermesidir. Ayrıca herkese kendine ilişkin profil üzerinde bir denetim olanağı verilirse ve bu hakkını mahkeme önünde savunması da sağlanırsa, mülkiyet hakkı yaklaşımı ilgili kişinin izni olmaksızın bilgilerinin paylaşımını önleyebilir¹⁹⁰.

¹⁸⁷ David BRIN, **The Transparent Society (Will Technology Force Us to Choose Between Privacy and Freedom)**, Addison-Wesley, ABD 1998, s.91. Ayrıca bkz. Kenneth C. LAUDON, "Markets and Privacy, **Communication of the ACM**, C.39, S.9, Y.1996, s.103 (s.92-104) ; Ann BARTOW, "Our Data, Ourselves: Privacy, Propertization and Gender", University of San Francisco Law Review, C.34, Y.2000, s. 633-695 (özellikle s. 683 vd.) ; Lawrence LESSIG, "Privacy as Property", **Social Research**, C.69, S.1, Y.2002, s. 247-269.

¹⁸⁸ Jerry KANG, "Information Privacy in Cyberspace Transactions", **Stanford Law Review**, C. 50, Y. 1998, s. 1256-1257.

¹⁸⁹ Pamela SAMUELSON, s. 1132-1134.

¹⁹⁰ Arthur R. MILLER, **The Assault on Privacy, Computers, Data Banks, and Dossiers**, The University of Michigan Press, ABD 1971, s. 211-212.

Bireylere kendilerine ilişkin verilerin sahibi olma düşüncesi doğal gelebilir¹⁹¹. Yasaların da bazı durumlarda verileri yetkisiz erişim ve kullanıma karşı korumaları kişisel veriler üzerinde mülkiyet hakkının bulunduğu düşüncesini güçlendirmektedir. Ancak bireylerin, verilerinin kullanılması ve yayınlanması konusunda korunduğu durumlarda da hukuksal temel, tarihsel olarak, kişilerin verileri üzerinde mülkiyet hakkı bulunduğu dayanamamaktadır¹⁹².

Mülkiyet yaklaşımı başka nedenlerle de kabul edilemez görülmektedir. Her şeyden önce, ilgili kişiye verileri üzerinde mülkiyet hakkını tanıma, hukukça, yalnız piyasanın ekonomik gerçeklerinin kabul edilmesi ve kişinin değerli şeyler üzerindeki sahipliğini korumayı tartışarak kabul edilebilir kılınamaz. Ayrıca mülkiyet hakkının tanınmasına güven, verileri isteyen kurumlara çeşitli sorumluluklar yüklemek yerine, kendi tercihlerini korumak konusunda her bireye sorumluluk verme yaklaşımında da istenmeyen sonuçlar doğurabilir.

Gerçekten pazarlıkta taraflar eşit olmadığından, örneğin birey bir devlet kurumunda çalışmak için başvuruda bulunduğu verileri üzerindeki mülkiyet hakkından gönüllü olarak vazgeçmesi doğaldır¹⁹³. Özel sektör açısından da durum pek farklı değildir. Kişisel bilgilerin alınıp satılan bir mal gibi değerlendirildiği bir ortamda, bireyler zarar görür. Bu durumdan yarar sağlayanlar ise şirketler olacaktır. Bir başka ifadeyle, ekonomik yaklaşım ile bireylerin verileri üzerindeki denetimi yeniden kazanabilmeleri olanaklı değildir. Böylesine bir yaklaşım, daha az varlıklı olan kesimin aleyhine olur¹⁹⁴.

Ayrıca mülkiyet hakkı yaklaşımını savunanlar, bunun bireylerin veri değiş-tokuşuna dahil olabildikleri ve pazarın rahatlıkla işleyebildiği bir ortam için gerekli olduğunu ileri sürmektedir. Ancak her ikisinin birden bu sistem içerisinde gerçekleşebilmesini sağlamak için yeni bir mülkiyet hakkı pazarı oluşturmak, bir alt yapı kurmak gerekir. Bunun ise hiç de kolay olmadığı açıktır. Pazarın karmaşıklığına

¹⁹¹ Bu konuda çeşitli alanlara ilişkin pek çok örnekle zenginleşmiş ayrıntılı bir çalışma için bkz. Anne WELLS BRANSCOMB, **Who Owns Information? From Privacy to Public Access**, Basic Books, ABD 1994. Kişisel veriler üzerinde “mülkiyet hakkı”na sahip olma konusunda bir değerlendirme için ayrıca bkz. Julie E. COHEN, “Examined Lives: Informational Privacy and the Subject as Object”, **Stanford Law Review**, C.52, Y.1999-2000, s. 1377-1394.

¹⁹² Pamela SAMUELSON, “Privacy As Intellectual Property?”, **Stanford Law Review**, C.52, s.1130-1132.

¹⁹³ Arthur R. MILLER, s. 213-214.

¹⁹⁴ Gary T. MARX, “For Sale: Personal Information About You”; David LYON, **Elektronik Göz**, s. 261.

özgü sorunlar dışında başka sıkıntılar da göze çarpmaktadır. Mülkiyet hakkının temel niteliklerinden biri, malın ilk sahibi bunu sattıktan sonra yeni hak sahibinin malı istediği gibi kullanabilecek ve dilediği gibi satabilecek olmasıdır. Devretme özgürlüğü, arabalara ya da gayrimenkullere ilişkin olarak iyi bir şekilde işleyebilirken aynı durumun bilgilerin gizliliği hakkı için de söz konusu olabileceğini söylemek güçtür. Ayrıca mülkiyet hakkını temellendirmede kullanılan en önemli hususlardan biri olan, pazarın kıt kaynaklarının bölüştürülmesinin kişisel verilere uygulanabilmesi de pek olanaklı görülmemektedir. Kıt olan, bilgilerin gizliliğidir, kişisel veriler değil¹⁹⁵.

b. Fikrî Mülkiyet Hakkı Teorisi

ABD’de kimi yazarlar kişisel verilerin, bir başka hak alanı olan fikrî mülkiyet hakkı ile ilişkilendirerek korunabileceğini ileri sürmektedir. Bu yaklaşımda genel olarak fikri mülkiyet hakkı ile kişisel verilerin korunması arasında benzerlik kurulduğu görülmekte ve bu noktadan hareketle kişisel verilerin telif hakkı benzeri bir yaklaşımla korunması önerilmektedir. Hem fikrî mülkiyet hakkında, hem de kişisel verilerin korunmasında bireye ait ve fakat denetimini kaybedebileceği bir veri vardır. Birinci durumda veri telif hakkı alınmış bir çalışmadan oluşurken, ikinci durumda bize ait bir bilgiyi temsil etmektedir. Her ikisinde de İnternet, denetimin kaybında etkili olabilir. İnternet, telif hakkıyla korunan ürün açısından tam ve bedava kopyalar çıkartmaya yardımcı olurken, kişisel verilerin korunması açısından, davranışlarımızın sürekli ve ucuz gözetimi sağlamaktadır.

Ancak Jonathan Zittrain’a göre Amerikan hukuku açısından, iki durum arasında önemli bir farklılık kendini ekonomi politikası yoluyla her iki soruna çözüm aramada gösterir. Telif hakkında korunan çıkarın ihlali tehlikesi yüksek ve düzenlidir, özel yaşamın gizliliğinde ise dağınık ve düzensizdir. Telif hakkında korumanın diğer tarafındaki değerler, zorlayıcı ya da iyi anlaşılmış değil iken, özel yaşamın gizliliği hakkında, korumanın diğer tarafındaki değerler (güvenlik, terörizmle savaş) zorlayıcı ve iyi anlaşılabilir niteliktedir. Bu farklılığın sonucu, Amerika’da her siyasal teorisyenin kabul edeceği gibi, bir süredir, telif hakkını

¹⁹⁵ Pamela SAMUELSON, s. 136-139.

çözmeye yönelik pek çok yasal ve teknik değişiklik görülürken, özel yaşamın gizliliğine ilişkin sorunları çözmeye yönelik çok az girişimle karşılaşılmasıdır¹⁹⁶.

Bu değerlendirmeler Amerikan hukuk sistemi açısından yerinde olabilir. Ancak daha geniş bir pencereden bakıldığında durum farklılaşır. Bilgiyi temel alan mülkiyet hakkı olarak da nitelendirilebilecek, fikrî mülkiyet gibi bir hak alanı ile de kişisel verileri korumak olanaklı değildir. Her şeyden önce fikrî mülkiyet hukukunun ekonomik temeli, fikri ürünlerle ilgili kamusal yarar sorunlarının üstesinden gelmektir¹⁹⁷. Oysa kişisel verilerimiz fikir ürünü olarak nitelendirilemez. Bunun yanında mülkiyet hakkı yaklaşımına getirilen eleştirilerin büyük çoğunluğunun fikrî mülkiyet hakkı yaklaşımı için de geçerli olacağı unutulmamalıdır.

c. Diğer Teoriler

Kişisel verilerin, bu yaklaşımlar çerçevesinde korunmasının sorunlu yanlarını gören çeşitli yazarlar, yukarıdaki görüşlere yakın ancak özellikle belirli noktalarda farklılaşan yaklaşımlar geliştirerek çözüm üretmeye çalışmıştır. Örneğin güven teorisi bunlardan biridir. Güven teorisine esas olan ilkeler, ABD’de Birleşik Planlama Teşkilatı’nda (United Planning Organization-UPO) uygulanmıştır. UPO, çeşitli yerlerden topladığı büyük miktardaki kişisel bilgileri güven içinde bilgisayara aktarmıştır. Bilgi üzerinde denetimi gerçekleştirmek için üç bağımsız yeddiemin görevlendirilmiş ve bunların verileri kullanımı ile ilgili kurallar yazılı bir anlaşma ile belirlenmiştir¹⁹⁸.

Kişisel verilerin, ticarî sırlara uygulanan bazı hükümlerle korunabileceği de ileri sürülmüştür. Örneğin, Samuelson’a göre yasa ile, mülkiyet kuramlarına

¹⁹⁶ Jonathan ZITTRAIN, “What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication”, The Berkman Center for Internet & Society at Harvard Law School, Research Publication No. 2000-01, <http://cyber.law.harvard.edu/publications> (s.y. 11.11.2007); Lawrence Lessig, **Code V2**, s. 200-201.

¹⁹⁷ Pamela SAMUELSON, “Privacy As Intellectual Property?”, s. 1141. Fikri ürün, tarihsel gelişimi içinde bir çeşit mülkiyet hakkı olarak değerlendirilmiş ve hatta bazı ülkelerde gayri maddi eşya olarak adlandırılmıştır. Ancak Türk hukukunda, müşterek hukuka paralel bir şekilde yalnızca maddi şeyler “eşya” sayılabilir. Bu nedenle fikrî ürün bir eşya değildir. Buna karşın Türk hukukunda da bu alanın “fikrî mülkiyet” adı altında korunmasının, bu deyim içinde “mülkiyet” sözcüğünün kullanılmasının nedeni fikrî ürün üzerindeki mutlak hakkın özel inhisarî niteliğini belirtmektir. Bkz. Ünal TEKİNALP, **Fikri Mülkiyet Hukuku**, 2. Baskı, Beta, İstanbul 2002, s. 5. Ayrıca bkz. Şafak N. EREL, **Türk Fikir ve Sanat Hukuku**, İmaj, 2. Baskı, Ankara 1998, s.9; Mustafa ATEŞ, **Fikir ve Sanat Eserleri Üzerindeki Hakların Kapsamı ve Sınırlandırılması**, Seçkin, Ankara 2003, s. 96-98.

¹⁹⁸ Arthur R. MILLER, s. 216 vd.

dayandırılmadan da bireylerin kişisel verilerine ilişkin çıkarları korunabilir. Bu da, kişiler aksine rıza göstermedikçe, verilerinin yetkisiz kişilerce örneğin kullanımını ya da yayınlanmasını yasaklayan kuralları kabul ederek yapılabilir. Yazara göre her ne kadar ticarî sır ile kişisel verileri düzenleyen kurallar birbirinden farklı olsa da bunların her ikisinin de temelde koruduğu çıkarlar aynıdır¹⁹⁹. Bu kuralların bir kısmı kişisel verilerin de lisansa bağlanmasında uygulanabilir. Ticarî sır lisanslarında uygulanan temel ilkeye göre, lisans sahibi başka bir kişiye belirli bir amaç için veri sağladığında, bu izinsiz bir şekilde başka amaçlar için kullanılamaz.

Ticarî sırların niteliği ile kişisel verilerin niteliği arasında ciddi farklılıklar bulunsa da yazara göre bu yöntem ile kişilerin verileri üzerinde denetimi sağlanabilir²⁰⁰. Ancak ekonomik hak yaklaşımının sorunlu yanları bu alternatif öneriler için de geçerlidir. Kişisel verilerin alınıp satılabilen bir mal olarak görülmesi, yalnızca nüfusun belirli bir bölümünün yararına olabileceği gibi, daha güçlü bir veri koruması sağlayıp sağlamayacağı da şüphelidir. Bunun yanında verilere “*sahip*” olma teorik açıdan da tartışmalıdır²⁰¹.

2. İNSAN HAKKI YAKLAŞIMI

Yukarıda kişisel verilerin korunması hakkına ekonomik temele dayanan yaklaşımların sorunlu yanlarına kısaca değindik. Ancak bunların yanında bu yaklaşıma en temel itirazın mülkiyet hakkının (ve fikri mülkiyet hakkı gibi diğer

¹⁹⁹ Samuelson’a göre temelde üç ortak çıkardan söz edilebilir. Bunlardan birincisi, gizli ya da özel bilgilerin yetkisiz kullanımını önleyerek hak sahibinin çıkarını korumaktadırlar. İkincisi, kişilere ya da şirketlere gizli ya da özel bilgilerin ticari kullanımları üzerinde denetim hakkı vererek ticari çıkarlarını korumaktadırlar. Üçüncüsü de bu çıkarlarda temel bulan hedefleri gerçekleştirebilmek için, ticari sırrı düzenleyen kurallar geçerli bazı lisans kurallarından gelişmiştir. Bkz. Pamela SAMUELSON, s. 1152.

²⁰⁰ Samuelson’a göre, ticari sır lisanslarında geçerli olan bazı kuralları bu alanda uygulamanın çok çeşitli faydaları görülebilir. Eğer bir kişi ile şirket kamuya açılmamış bazı kişisel bilgilerin belirli bir meblağ karşılığında verilmesi konusunda anlaşmışlarsa ve birey bu verilerin kullanımının gizli tutulmasını ve yalnızca belirli bir amaç için kullanılmasını istiyorsa bu sistem işe yarayacaktır. Bunun yanında, bu sistem yasanın uygun görmediği bazı durumlarda kişinin eğer istiyorsa kendine ilişkin veriler üzerinde özgürce karar vermesine de hizmet eder. Örneğin, yetkisiz gözetleme, hile ya da dolandırıcılık ile verilerin elde edilmesi durumunda bile, eğer kişi verilerinin kullanılmasını ve açığa çıkmasını istiyorsa buna olanak tanınabilecektir. Pamela SAMUELSON, s. 1151 vd. Kişisel verilerin tüketici lisansları ile korunmasına ilişkin değerlendirmeler için ayrıca bkz. Kalindo BASHO, “The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?”, *California Law Review*, C. 88, Y. 2000, s. 1507, 1509; Steven A. BIBAS, “A Contractual Approach to Data Privacy”, *Harvard Journal of Law & Public Policy*, C.17, Y. 1994, s. 591, 592

²⁰¹ Lee A. BYGRAVE, s. 120-121.

yaklaşımların) bu hak alanı ile korunmaya çalışılan kişisel değerlerle bağdaşmamasından kaynaklandığı belirtilmelidir. Kendimizi bize ilişkin bilgilerin pazarında herhangi bir alıcı/satıcı olarak mı yoksa birey olarak mı tanımladığımız bu noktada önem taşımaktadır.

Günümüzde bilgi, önceki dönemlerdekine göre çok daha önemli bir konuma gelmiştir. Bu bağlamda kişisel verilerin ekonomik bir değer taşıdığı da tartışmasızdır. Özellikle ticarî işlemler söz konusu olduğunda bu değer daha açık bir şekilde hissedilebilir. Bu anlamda bireylerin, başka çıkarlarının yanında, ekonomik çıkarlarının korunması gerekir. Ancak bu, kişisel veriler üzerinde mülkiyet hakkının kurulabileceği anlamına gelmez.

Gerçekten taşınır ya da taşınmaz mallara uygulanan kuralları elle ya da otomatik olarak işlenen kişisel verilere uygulamak, örneğin seçme hakkını ya da düşünceyi açıklama özgürlüğünü mal haline getirmekten farksızdır. Bir başka anlatımla mülkiyet hakkı ve benzeri yaklaşımlar yalnızca korumada yetersiz kalmaları, bu sistemlerin işleminin zor olması ya da iki hak alanı arasında ortak paydaların bulunmaması gibi nedenlerle değil, etik açıdan da yanlıştır. Bireyin özel yaşamının gizliliği hakkının temel amacı, duygusal ve psikolojik yapısını kişisel bilgilerinin istenmeyen şekilde yayılmasını önleyerek korumaktır ve hiçbir zaman, bilginin yasal adını tanımlamak ya da ticarî kullanım hakkına kimin sahip olduğunu belirlemek için bir araç olarak düşünülmemiştir. Oysa bunlar, mülkiyet hukukunun temel işlevlerini oluşturur²⁰².

Nitekim baskın görüş, kişisel verilerin korunmasının temel bir insan hakkı olduğu yönündedir²⁰³ ve bu yaklaşım özellikle Avrupa'da yaygındır²⁰⁴. Ayrıca bazı Amerikan yargı kararlarında da bu görüşün etkisi hissedilmektedir²⁰⁵. BM Evrensel

²⁰² Arthur R. MILLER, *The Assault on Privacy*, s. 212.

²⁰³ Roger CLARKE, "Beyond the OECD Guidelines".

²⁰⁴ Avrupa'da öğretinin büyük bir bölümünde, Avrupa kişisel verilerin korunması hukukunun özünün temel insan hakları yaklaşımı olduğu konusunda görüş birliği vardır. Bununla birlikte Avrupa veri koruma mevzuatı içerisinde, özellikle sözleşme haklarıyla ilişkili olarak, mülkiyet hakkı yaklaşımına uygun bazı özellikler de bulunabileceğine ilişkin farklı bir yaklaşım için bkz. Corien PRINS, "Property and Privacy", özellikle s. 234 vd.

²⁰⁵ Örneğin şu kararlara bkz. Kişinin özel haberleşmesinin özel yaşamının gizliliği hakkı kapsamında olduğuna ilişkin olarak: **Katz v. United States**, 389, U.S. 347 (1967); **Berger v. New York** 388 U.S. 41 (1967); İşyerinde işçilerin özel yaşamlarının gizliliğine ilişkin olarak; **O'Connor v. Ortega**, 480 U.S. 709 (1987). Cornell University Law School, Supreme Court Collection, <http://supct.law.cornell.edu/supct/search/index.html> (s.y. 3 Şubat 2009). Özel yaşamın gizliliği hakkı ve bu kapsamda kişisel verilerin korunmasına ilişkin ABD Yüksek Mahkemesi kararlarından çeşitli örnekler için ayrıca bkz. Harry HENDERSON, s.75-116.

İnsan Hakları Beyannamesi (m.17), BM Bireysel ve Siyasal Haklar Şartı (m.12), Avrupa İnsan Hakları Sözleşmesi (m.8) gibi pek çok önemli insan hakları metninde özel yaşamın gizliliği temel bir insan hakkı olarak kabul edilmiştir. Bunun yanında Avrupa Birliği Temel Haklar Şartı ve başka belgeleri, çeşitli devletlerin anayasaları gibi daha yeni bazı metinlerde kişisel verilerin korunması hakkının, özel yaşamın gizliliği hakkında bağımsız olarak da temel haklar kataloğu içerisinde yer aldığı görülmektedir.

Aşağıdaki açıklamalarda görüleceği üzere kişisel verilerin korunması hakkı, yalnızca kişisel çıkarların korunması ile ilişkili değildir. Kişisel verilerin korunması hakkı, insan onuru ve temel özgürlükler gibi çok daha geniş bir alana hizmet etmektedir.

C. İNSAN HAKKI OLARAK KİŞİSEL VERİLERİN KORUNMASI

1. İNSAN ONURU, BİREYSEL ÖZERKLİK VE BİLGİLERİN GELECEĞİNİ BELİRLEME HAKKI

Kişisel verilerin korunması, günümüz bilişim teknolojileri karşısında kişisel bilgileri sınırsız bir şekilde toplanan, kullanılan, devredilen bireyin korunmasını amaçlamaktadır. Bu bağlamda kişisel verilerin korunması hakkının ilk olarak insan onuru ve bu kapsamda kişiliğin serbestçe geliştirilmesi hakkına dayandırıldığı görülür. Nitekim Federal Almanya Anayasa Mahkemesi 1983 yılında verdiği etkisi ülke sınırlarını aşan²⁰⁶, Nüfus Sayımı (Volszählung) kararında bu duruma işaret etmiştir²⁰⁷.

Federal Almanya Anayasa Mahkemesi bu kararında parlamentonun her iki kanadının oy birliği ile kabul ettiği Nüfus Sayımı Yasasını (Volszählung Gesetz) Anayasaya aykırı bulmuştur. Belirtilen yasa uyarınca 1983 yılında memurların kapı

²⁰⁶ Hans H. WOHLGEMUTH, Jürgen GERLOFF, **Datenschutzrecht, Eine Einführung mit praktischen Fällen**, 3. Baskı, Almanya 2005, s.12; Flemming MOOS, **Datenschutz-recht**, Schnell Erfasst, Springer, Almanya 2006, s.7.

²⁰⁷ BVerfGE, 65, 1-Volszählung, 15 Aralık 1983. Kararın tam metni için bkz. **Entscheidungen des Bundesverfassungsgerichts**, C.65, Y. 1984, J.C.B.MOHR, Almanya 1984, s.1-71. Ayrıca İnternet üzerinden şu kaynaktan ulaşılabilir: http://www.datenschutz.rlp.de/downloads/bverfge_65_1_-_volkszaehlung.pdf (s.y. 12 Şubat 2009).

kapı dolaşarak yapacakları sayımda yurttaşların sayılmasından başka bilgilerin edinilmesi de hedeflenmişti ve yurttaşlara kapsamlı bilgileri açıklama yükümlülüğü getirilmekteydi. Bu yükümlülüğü yerine getirmeyenler için ise yaptırım öngörülüyordu²⁰⁸. Yasa, Anayasa Mahkemesinin önüne gelmeden önce devletin “*veri açlığı*”nı gösterdiği gerekçesiyle çeşitli eleştirilere uğramıştır. Sonuçta Anayasa Mahkemesi kararında yasanın dayanağı olan gerekçeler tek tek çürütülmüş ve devletin kişisel verilerle olan ilişkisi ayrıntılı bir şekilde tasvir edilmiştir²⁰⁹. Anayasanın insan onurunun korunmasıyla ilgili 1/1²¹⁰ ve kişiliğin korunması hakkına ilişkin 2/1²¹¹ maddeleri hükümlerini bir arada değerlendirerek, “*bilgilerin geleceğini belirleme hakkı*”nı (informationelle Selbstbestimmung) türetmiştir²¹².

Mahkemeye göre, anayasal düzenin merkezinde toplumun özgür bir üyesi olarak kişinin onuru bulunur. Günümüzdeki teknik gelişmeler ve buna bağlı olarak ortaya çıkan tehlikeler karşısında kişiliğin korunması özel bir önem kazanmaktadır. Hakkında edinilen bilgilerin neler olduğunu ve bu bilgilerin kimin elinde bulunduğunu öğrenebilme olanağına sahip olmayan bireyin kendi kararlarını verme özgürlüğü önemli ölçüde zarar görmüş demektir. Özellikle otomatik veri işleme araçları ile verilerin sınırsız bir şekilde kaydedilebilmesi, bu verilerin her zaman

²⁰⁸ Bkz. BVerfGE 65,1; Marie-Theres TINNEFELD ve diğ., s. 143-147; Oğuz ŞİMŞEK, s. 114-119; Gerrit HORNING, Christoph SCHNABEL, “Data Protection in Germany I: The Population census decision and the right to informational self-determination”, **Computer Law and Security Report**, C. 25, S. 1, Y. 2009, s. 84-88; Spiros SIMITIS, “Die informationelle Selbstbestimmung- Grundbedingung einer verfassungskonformen Informationsordnung”, **NJW**, Heft 8, Y. 1984, s. 398-405.

²⁰⁹ Alexander ROßNAGEL ve diğ., **Handbuch Datenschutzrecht, Die Neuen Grundlagen für Wirtschaft und Verwaltung**, Verlag C.H. Beck, Almanya 2003, s.8.

²¹⁰ Federal Almanya Cumhuriyeti Anayasası 1/1 maddesi şu hükmü içermektedir: “*İnsan onuru dokunulmazdır. Tüm devlet güçleri ona saygı göstermek ve onu korumakla yükümlüdür*”. Federal Almanya Cumhuriyeti Anayasası 1/1 hükmüne ilişkin değerlendirmeler için bkz. Horst DREIER ve diğ., **Grundgesetz Kommentar**, C.1 (Giriş, Madde 1-19), Mohr Siebeck, 2. Baskı, Almanya 2004, s. 139-231.

²¹¹ Federal Almanya Cumhuriyeti Anayasası 2/1 maddesi şu hükmü içermektedir: “*Herkes başkalarının haklarını ihlal etmemek, Anayasal düzene veya ahlak kurallarına aykırı düşmemek koşuluyla kişiliğini serbestçe geliştirme hakkına sahiptir*”. Federal Almanya Cumhuriyeti Anayasası m.2/1’e ilişkin değerlendirmeler için bkz. Horst DREIER ve diğ., s. 288-346.

²¹² Yalnız belirtmek gerekir ki, arada bazı benzerlikler bulunmakla birlikte buradaki genel kişilik hakkı kavramı, özel hukuk alanında bildiğimiz şekliyle kişilik hakkı kavramından farklıdır. Herşeyden önce ondan daha geniş bir alanı niteler. Nitekim Anayasa Mahkemesi, bireylerin kişiliklerini özel bazı durumlardaki saldırılardan korumak için genel kişilik hakkından bazı haklar türetmiştir. Örneğin, kişinin sözleri üzerindeki hakkı, **BVerfGE** 34, 238 (246), resmi üzerindeki hakkı **BVerfGE** 79, 256 (268), kendi kökeni hakkındaki bilgilere sahip olma hakkı **BVerfGE** 79, 256 (268) bu kapsamda sayılabilir. Kişilik hakkına ilişkin çeşitli değerlendirme ve tartışmalar için bkz. Aydın ZEVKLİLER, Beşir ACARBEY, Emre GÖKYAYLA, **Medeni Hukuk**, 6. Baskı, Seçkin, Ankara 1999, s.441-475.

ulařılabilir nitelięi ve bireyin ayrıntılı kiřilik profilinin oluřturulabilme olasılıęı da dikkate alındıęında, kiřinin üzerinde psikolojik baskı yaratılması ve onun kamusal yařama katılımlarını etkilemesi olanaklıdır.

Toplantı, gösteri yürüyüşü ya da sivil toplum örgütlerine katılımının resmi makamlarca kayıt altına alındıęını ve bundan dolayı çeřitli mağduriyetler yařayacaęını düşünen birey, bu haklarını kullanmaktan vazgeçebilir. Bu durum, yalnızca bireyin kendi kiřilięini geliştirme hakkını zedelemekle kalmaz, ayrıca kamu çıkarlarına da zarar verir, çünkü özgürlükçü bir demokrasinin işlemleri topluma katılma ve toplum içerisinde işlev görme becerisine baęlıdır. Bu nedenle, kiřilięin serbestçe gelişebilmesi ve demokratik toplum yapısının süreklilięi için devlet tarafından kiřisel verilerinin toplanılması, kaydedilmesi, kullanılması ve devredilmesi karşısında bireyin korunması bir gerekliliktir. Birey, yařam ilişkilerinin açığa çıkacaęı zamana ve bunun sınırına kendisi karar vermelidir. Nitekim bilgilerin geleceęini belirleme hakkı, ilke olarak bireyin kendi kiřisel verileri üzerinde tasarrufunu saęlamaktadır²¹³.

Sürekli izlenen, yařamına ilişkin bilgiler kayıt altına alınan, bütün bunların sonucunda adeta řeffaflařan, bireyin kiřilięini serbestçe geliřtirebilmesi olanaklı deęildir. Bu kiřinin toplumsal yařamda kiřilięini özgürce belirleyememesi, kendinden beklenen davranıř tarzına göre hareket etmesi de olasıdır. Bu noktada kiřisel verilerin korunması hakkı, bireye kiřisel verilerinin hukuka aykırı olarak sınırsız bir řekilde kaydedilmesi, işlenmesi, paylařılması karşısında temel bir hak vermekte ve onu basit bir veri nesnesi olmaktan korumaktadır²¹⁴. Kısacası verilerin geleceęini belirleme hakkı, bireye verilerinin kullanılması üzerinde karar verme hakkını tanır.

Verilerin korunması, yurttařın hakları, resmi makamların ve işletmelerin bilgilendirilmesi ile kiřilik haklarının korunması arasında bir denge öęesidir²¹⁵. Bu bağlamda kiřisel verilerin korunması hakkının sınırsız olmadıęını belirtmek gerekir. Verilerin geleceęini belirleme hakkı, ilgilinin “*kendi*” verileri üzerinde sınırsız bir hakka sahip olduęu anlamına gelmemektedir. Ancak sınırlamalar yalnızca belirli

²¹³ BVerfGE 65,1, 42 vd; Peter GOLA, Rudolf SCHOMERUS, **Bundesdatenschutzgesetz Kommentar**, Beck, Almanya 2007, s.77.

²¹⁴ Oęuz řİMŞEK, s. 112.

²¹⁵ Carl CREIFELDS ve dię., **Rechtswörterbuch**, Becks, Almanya 1997, s.277.

durumlarda söz konusu olmalı ve yasal temele dayanmalıdır. Bu sınırlamaların koşulları ve kapsamı yurttaş için açık ve anlaşılır bir şekilde saptanmalıdır. Anayasal haklar bireye, temelde kendi kişisel verilerinin kullanılması konusunda olanaklar tanımıştır. Bireyin kendi kişisel verileri üzerindeki tasarrufu ancak temel haklar izin verdiği ölçüde sağlanmıştır²¹⁶.

Öğretide pek çok yazar kişisel verilerin korunması hakkı ile bilgilerin geleceğini belirleme hakkını, ya da bir diğer ifadeyle “*enformasyonel özerklik*” hakkını eşdeğer olarak kullanmaktadır. Ancak örneğin *Jóri* bu kullanıma bir kaç açıdan karşı çıkmaktadır. Yazara göre öncelikle, verilerin geleceğini belirleme hakkı, 1983 yılında Federal Almanya Anayasa Mahkemesi’nin Nüfus Sayımı Kararı ile geliştirilmiş bir kavramdır. Oysa verilerin korunması hakkının gelişimi bundan çok daha önce başlamıştır. İlk veri koruma yasalarında bu yeni hakkın temelini oluşturan bireyin kendine ilişkin verileri düzenleme hakkı tanınmamıştır. Her ne kadar verilerin geleceğini belirleme hakkının geliştirilmesi, kişisel verilerin korunması hukuku açısından bir dönüm noktası olsa da konuya ilişkin ilkelerin bu hakkın belirlediği alanın ötesine gidemeyeceği düşüncesi yanlıştır. Nitekim yeni geliştirilen veri koruma düzenlemelerinde de korumanın bireylerin “*enformasyonel özerklik*” hakkını sağlayıp sağlamadığına bakılmaksızın hükümlerin geliştirildiği görülmektedir²¹⁷.

2. ÖZEL YAŞAMIN GİZLİLİĞİ HAKKI VE KİŞİSEL VERİLERİN KORUNMASI

Kişisel verilerin korunması hakkı, ilk aşamada özel yaşamın gizliliği hakkı içinde değerlendirilebilir. Ancak gelişen teknoloji, özel yaşamın gizliliği hakkına geleneksel yaklaşımla ve bu alanda benimsenen ilkelerle verilerimiz korunmasında yetersiz kalmaktadır. Bu nedenle tarihsel süreç içerisinde kendisinden daha köklü bir hak alanı olan özel yaşamın gizliliği hakkından ayrılmaya başlamıştır. Bu anlamda kişisel verilerin korunmasının özel yaşamın gizliliği hakkının özellik taşıyan bir türü olduğu ve kendine özgü bazı gereklilikleri nedeniyle ayrı bir alan olarak algılanmaya

²¹⁶ Peter GOLA, Rudolf SCHOMERUS, s. 78.

²¹⁷ András JÓRI, “dataprotection.eu”, <http://www.dataprotection.eu/>.

başlandığını söyleyebiliriz. Ancak iki hak alanı arasındaki yakın ilişki yadsınamaz²¹⁸. Kıta Avrupası hukukunun aksine özellikle ABD, Yeni Zelanda, Avustralya, Kanada gibi Anglo-Amerikan sisteminin geçerli olduğu ülkelerde konuya ilişkin düzenlemelerin özel yaşamın gizliliği hakkı başlığı altında yapılması da bunun en açık göstergesidir. Bu nedenle kişisel verilere neden gereksinim duyduğumuz sorusuna cevap ararken öncelikle özel yaşamın gizliliği hakkının koruduğu değere bakmamız gerekir.

a. Özel Yaşam

“Özel yaşam” üzerinde duran hemen hemen bütün eserlerde bu deyim tanımlama güçlüğünden söz edilir²¹⁹. Pek çok kişi, özel yaşamın ne olduğunu algılayabilir, ancak bunu kelimelere dökmeye zorlanır. Bir başka ifade ile özel yaşam, tanınması kolay, tanımlanması güç bir olgudur²²⁰. Bu güçlüğü aşabilmek için, bireyin çevresi ile ilişkileri iç içe geçmiş alanlara, çemberlere benzetilmiş ve bu şekilde özel yaşamın sınırlarını belirlemeye çalışılmıştır. Bu çemberler ortak özellikleri bakımından üç grupta toplanabilir. “Genel yaşam alanı” olarak adlandırılabilir dış çember, kişinin herkesle paylaşabileceği, kamuya açık yaşam alanlarını içerir. İkinci olarak “kişinin özel yaşam alanı”, belirli kimselerle ve belirli ölçüde paylaştığı yaşam parçalarını kapsar. En içte kalan “sır alanı” ise, kişinin yalnızca kendine saklamak istediği alanı oluşturur ve özel yaşam içinde değerlendirilir²²¹. Oya Araslı’ya göre “Bu durum sonuçta kişinin yaşam

²¹⁸ Buna karşın özel yaşamın gizliliğinin korunması ile kişisel verilerin korunmasını birbirlerinden tamamen ayrı iki alan olarak değerlendiren istisnai bir görüş de bulunmaktadır. Buna göre, kişisel verilerin korunmasının temel hak ve özgürlüklerle hiçbir ilişkisi bulunmamaktadır, yalnızca bilgi gücünü kontrolle ilişkilidir P. BLOK, **Het Recht Op Privacy (The Right to Privacy)**, Boom Juridische Uitgevers, Lahey 2002 s.326’dan akataran; Corien PRINS, “Property and Privacy”, s. 227-228.

²¹⁹ Nitekim Avrupa İnsan Hakları Mahkemesi (ve 11 Numaralı Protokol öncesi Avrupa İnsan Hakları Komisyonu) da kararlarında “özel yaşam”ın genel geçer bir tanımını yapmanın güçlüğüne işaret etmiştir. Mahkeme, bir tanım yapmaktansa her olayı kendi özel koşullarına göre değerlendirerek verdiği kararlarla kavrama açıklık getirmeye çalışmıştır. Örneğin *Niemietz, Almanya’ya karşı*, b.n. 13710/88, k.t.: 16 Aralık 1992, par. 29; *Costello Robert İngiltere’ye karşı*, b.n.: 13134/87, k.t.: 25 Mart 1993, par.36; *Murray İngiltere’ye karşı*, b.n.: 14310/88, k.t.: 28 Ekim 1994, par. 83 vd.

²²⁰ Ann CAVOUKIAN, Don TAPSCOTT, s. 11.

²²¹ Oya ARASLI, **Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi**, Ankara 1979 (yayımlanmamış doçentlik tezi), s.4 vd. Ayrıca bkz. Alan F. WESTIN, **Privacy and Freedom**,

parçalarının, çevreye açıklık derecesine göre ‘özel yaşam’ ve ‘genel yaşam’ olarak iki gruba indirgenebilmesine neden olmaktadır. Buna dayanarak ‘özel yaşam’ı, ‘kişinin mutlak olarak gizli tuttuğu yaşam parçaları ile herkesin bilmesini uygun bulmadığı, yalnız kendi seçeceği kişilerle, belirlediği ölçü ve biçimde paylaşacağı yaşam parçalarının birlikte oluşturdukları yaşam alanı’ olarak tanımlayabiliriz”²²².

Kişinin özel yaşamının çevreye açıklık derecesinin yararlanacağı korumanın oranı ve şekliyle ilgili olduğu söylenebilir. Nitekim kişinin sır alanı içerisinde yer alan, cinsel yaşamı, dinsel tercihleri, ırksal kökeni gibi konulara ilişkin veriler, hassas veri olarak kabul edilmekte ve daha özel bir korumaya tabi tutulmaktadır. Kişinin özel yaşam alanına müdahale ise ağırlıklı bir kamu yararının varlığı halinde söz konusu olabilir ve bu durumda da belirli ilkelere uygun hareket etmek bir zorunluluktur²²³. Kişinin özel yaşam alanı içerisinde yaptığı konuşmaların kayda alınması ya da telefonlarının dinlenmesi bu kapsamda incelenebilir.

Bunun yanında “*genel yaşam alanı*” olarak adlandırılan dış çemberde de birey korumasız değildir. Kişisel verilerin korunmasına ilişkin temel ilkelere bu alanda da uyulmalıdır. Kişinin kamuya açık yaşam alanında verilerinin toplanması, örneğin video ya da ses kaydının alınması ile söz konusu olabilir. Kapalı devre televizyon (CCTV) sistemleri ile kayıt altına alınan görüntülerin kişisel verilerin korunması açısından önemli tartışmalara neden olması da bundandır.

b. Özel Yaşamın Gizliliği Hakkı

Özel yaşamın gizliliği hakkı muğlâk, çok anlamlı ve tartışmalı bir deyimdir ve birbirinden oldukça farklı sorunlara, eğilimlere, haklara ve görevlere odaklanır²²⁴. Bu nedenle, özel yaşamın gizliliği hakkı farklı kişilerce farklı şekillerde anlaşılabilmektedir²²⁵.

Konut dokunulmazlığı; sebepsiz arama, izleme veya haberleşmeye müdahale; doğum kontrolü, gebeliğin iradi olarak sona erdirilmesi, giyim tarzı, cinsel tercih gibi

Atheneum, ABD 1970, s. 33 vd.; Aydın ZEVLİLER ve diğ., s.466 vd.; Bilge ÖZTAN, **Medeni Hukukun Temel Kavramları**, Turhan, Ankara 1995, s.260 vd.

²²² Oya ARASLI, **Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi**, Ankara 1979 (yayımlanmamış doçentlik tezi), s.4.

²²³ Oğuz ŞİMŞEK, s. 142-143.

²²⁴ Colin J. BENNET, s. 12-13.

²²⁵ Harry HENDERSON, s. 3. Özel yaşamın gizliliği hakkının kökenleri için bkz. Samuel H. HOFSTADTER, George HOROWITZ, **The Right of Privacy**, Central Book Company, ABD 1964, s. 9-16; Alan WESTIN, s.5-51; Oya ARASLI, s. 17 vd..

pek çok konu özel yaşamın gizliliği hakkı çerçevesinde tartışılmaktadır²²⁶. Bu hak, özel alanın korunmasından, özgür karar vermeye; bireysel özerklikten, kişisel bilgilerin korunmasına kadar uzanan geniş bir yelpazeyi kapsar. Bu nedenle özel yaşamın gizliliği hakkının tam ve kapsayıcı bir tanımını yapmak olanaksızdır. Bu hakkın tanımı ona nereden bakıldığına göre değişecektir. Temel ayrımın kimi tanımlarda “*özel yaşam*” olgusuna, kimilerinin ise “*özel yaşamın gizliliğini bozmaya yönelik davranışlar karşısında kişiye hukuken sağlanan korumaya*” dayanılmasından kaynaklandığı söylenebilir²²⁷. Oldukça sübjektif yapısı dolayısıyla da zamana, yere ve yazarın hakkın hangi boyutu üzerine odaklandığına bağlı olarak çok farklı tanımlar ortaya çıkmıştır²²⁸. Bu önemli hakkın yeni tanımları ile eskilerin bir arada değerlendirilmesi gerekir. Çünkü her birinde başka bir gerekliliğin hedef alındığı ya da başka bir gerekliliğe yöneldiği görülür. Ancak bu tanımların önemli bir bölümünde kişiye ilişkin bilgilerin vurgulandığı da dikkatten kaçmamalıdır.

Samuel D. Warren ve Louis D. Brandeis, 1890 yılında Harvard Hukuk Fakültesi Dergisi’nde yayınladıkları ünlü makalelerinde özel yaşamın gizliliği hakkını “*yalnız bırakılma hakkı*” olarak nitelemişler ve bu hak alanında yasal korumanın gerekliliğini tartışmışlardır²²⁹. Yalnız bırakılma hakkının temelinde bireyin kendisine ait bilgilerin paylaşılmasını denetlemesi düşüncesi yatar²³⁰.

Benzer şekilde Alan Westin’in tanımı da bireye ait bilgilere odaklanmıştır. Westin’e göre özel yaşamın gizliliği hakkı “*bireylerin, toplulukların ve kurumların kendileri hakkındaki bilgilerin ne zaman, nasıl ve hangi kapsamda başkaları ile ilişki içinde bulunacağına kendilerinin karar verme hakkı*”dır²³¹. Westin’in bu tanımında o dönemde telekomünikasyonda yaşanan gelişmelerin bu nedenle de iletişimin dinlenmesi olasılığının artması etkilidir. Bu tanım ayrıca, pek çok devletin özel yaşamın korunmasına ilişkin özel düzenlemeleri ve veri koruma yasaları gibi daha genel düzenlemeleri yürürlüğe soktukları dönemin de temsilcisi olarak

²²⁶ Sultan ÜZELTÜRK, s.5.

²²⁷ Oya ARASLI, s. 43-44.

²²⁸ Colin J. BENNET, s.13.

²²⁹ Samuel D. WARREN, Louis D. BRANDEIS, “The Right to Privacy”, **Harvard Law Review**, C. 4, S.5, 15 Aralık 1890, s.194-221. Makalenin yayınlanmasından kısa bir süre sonra pek çok Amerikan eyaletinde mahkeme kararlarında bu hak alanının tanınmaya başladığı dikkat çeker. Bu etkinin değerlendirilmesi ve örnek mahkeme kararları için bkz. Samuel H. HOFSTADTER, George HOROWITZ, **The Right of Privacy**, s. 17-24.

²³⁰ John GILLIOM, **Surveillance, Privacy and the Law, (Employee Drug Testing and the Politics of Social Control)**, The University of Michigan Press, ABD 1994, s. 91.

²³¹ Alan F. WESTIN, s.7.

değerlendirilmiştir²³². Westin'in tanımında dikkat çeken bir diğer özellik bireyin “denetim”ine vurgu yapmasıdır. Bu yaklaşımın pek çok başka yazar tarafından da kabul edildiği görülmektedir.

Denetime verilen özel önem yalnızca ABD yaklaşımına da özgü değildir. Alman Anayasa Mahkemesi'nin 1983 yılında verdiği nüfus sayımı kararı ile geliştirilen bilgilerin geleceğini belirleme hakkında da aslında aynı düşünceden hareket edilmiştir. Burada dikkat çekilmesi gereken konu, bireyin verileri üzerindeki denetiminden hareket eden yaklaşım ile ulaşılan sonuçların farklılaştığıdır. Kişisel verilere bir hak alanı olarak yaklaşımda yaptığımız değerlendirmelerden hatırlanacağı üzere, sonuçta Amerikalı hukukçular mülkiyet ve sözleşme hukukuna, Avrupalılar ise insan hakları düşüncesine dayanmışlardır.

O halde özel yaşamın gizliliği hakkına yönelik tanımların güncel gerekliliklerden etkilendiği söylenebilir. Bu durumda, özel yaşamın gizliliği hakkına, kişisel verilerin korunmasını temel alan bir tanım da getirilebilir. Nitekim Rodotà'ya göre özel yaşamın gizliliği hakkı, “*her türlü kamusal denetim ve sosyal damgalamaya karşı yaşam tercihlerimizin korunması*” olarak tanımlanabilir²³³.

Bu tanım denemelerine karşın özel yaşamın gizliliği hakkı kişisel verilerin korunması hakkından çok daha geniş bir alanı nitelediğini kabul etmek gerekir. Ancak günümüzde kazandığı önem dolayısıyla kişisel verilerin korunması hakkı, her ne kadar özel yaşamın gizliliği hakkına ilişkin temel ilkelerden beslense de ondan büyük oranda ayrılmıştır. Bu şekliyle haberleşme özgürlüğüne benzetilebilir. Nitekim haberleşme özgürlüğünde temelde özel yaşamın gizliliği hakkı kapsamındadır. Ancak özel önemi ve gereklilikleri dolayısıyla pek çok metinde ayrı olarak düzenlenilmesi tercih edilmiştir. Benzer bir ilişkinin düşüncüyü açıklama özgürlüğü ve basın özgürlüğü arasında bulunduğu da söylenebilir.

Avrupa kaynaklı iki önemli belge olan Avrupa İnsan Hakları Sözleşmesi ile Avrupa Birliği Temel Haklar Şartı'nın (ABTHŞ) karşılaştırılması bu durumu açıkça ortaya koyar. Nitekim 1950 yılında kabul edilen Avrupa İnsan Hakları

²³² Pieter KLEVE, Richard De MULDER, “Privacy Protection and The Right to Information: In Search of a New Symbiosis in the Information Age”, **Cyberlaw Security & Privacy**, haz. Sylvia Mercado KIERKEGAARD, The Second International Conference on Legal, Security and Privacy Issues in Information Technology (LSPI) 2007, Beijing, Çin, Ankara Barosu Yayınları, 2. Baskı, Ankara 2007, s. 339.

²³³ Stefano RODOTÀ, “Data Protection as Fundamental Right”, s.2.

Sözleşmesi'nde yalnızca (AİHS) özel yaşamın gizliliği hakkı düzenlenmiştir²³⁴. Ancak Avrupa İnsan Hakları Mahkemesi (AİHM) ve Avrupa İnsan Hakları Komisyonu(AİHK)²³⁵, pek çok ulusal mahkemenin benzer yorumlarına paralel bir şekilde, zaman içerisinde günün gerekliliklerine de uyum içinde, özellikle teknolojiadaki gelişmeleri dikkate alarak verdiği çeşitli kararlarla kişisel verilerin korunması hakkını bu kapsamda değerlendirdiğini ortaya koymuştur. Bu bağlamda AİHM, muhtemelen AİHS'nin hazırlayıcılarının aklında olmayan belge eşleştirme, kişisel verilere yetkisiz ulaşım, verilerin gereğinden uzun süre sistemlerde tutulması, DNA profillerinin değerlendirilmesi gibi kişisel verilerin korunması hakkı kapsamında incelenen alanlara özel yaşamın gizliliği hakkına ilişkin ilkeleri uygulamıştır²³⁶. Benzer şekilde BM İnsan Hakları Komitesi de 1988 yılında yayınlanan yorumunda kişisel verilerin korunması hakkına ilişkin temel ilkelerin BM Bireysel ve Siyasal Haklara İlişkin Uluslararası Sözleşmenin özel yaşamı korumaya ilişkin 17. maddesi çerçevesinde değerlendirilmesi gerektiğini belirtmiştir²³⁷.

Buna karşılık yine aynı coğrafyada hazırlanmış olan çok önemli, fakat daha yeni bir metinde: ABTHŞ'nda özel yaşamın gizliliği hakkı ile kişisel verilerin korunması hakkı farklı maddelerde ayrı ayrı hüküm altına alınmıştır²³⁸. Benzer bir

²³⁴ AİHS'nin 8. maddesi şu hükmü içermektedir: “(1)Herkes özel yaşamıyla aile yaşamına, konut ve haberleşmesine saygı gösterilmesi hakkına sahiptir. (2) Bu hakkın kullanılmasına demokratik bir toplumda kamu güvenliğinin gerekleri, kamu düzeninin korunması yada suçun önlenmesi, sağlık ve ahlakın, başkalarının hak ve özgürlüklerinin korunması için, gerekli olduğu ölçüde ve yasa uyarınca olan karışmalar dışında kamu makamlarınca karışılmaz”. Madde metninin Türkçe çevirisinde şu kaynaktan yararlanılmıştır: Muzaffer SENCER, **Belgelerle İnsan Hakları**, Beta, İstanbul 1988.

²³⁵ AİHS'nin ilk şeklinde koruma mekanizması iki organdan oluşuyordu: Avrupa İnsan Hakları Komisyonu (AİHK) ve Avrupa İnsan Hakları Divanı. 1 Kasım 1998 tarihinde yürürlüğe giren 11. Protokol ile AİHK kaldırılmış ve de iki organın yetkisi AİHM'nde toplanmıştır. Bu nedenle belirtilen tarih öncesinde AİHK tarafından başvurunun kabul edilebilirliğine ilişkin verilmiş pek çok karar bulunmaktadır. Ancak bu tarihten sonra hem kabuledilebilirlik kararları, hem de başvurunun esasına ilişkin kararların yalnızca AİHM tarafından verilebilmektedir.

²³⁶ **New Technologies: a Challenge to Privacy Protection?**, (Study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-Operation (CDCJ), Strasburg 1989, s. 41-42. Kişisel verilerin korunmasına ilişkin AİHM kararlarının değerlendirilmesi için bkz. aşağı. İkinci Bölüm, “AİHS” başlığı.

²³⁷ Bkz. BM İnsan Hakları Komitesi, 32. Oturum, Genel Yorum No.16, Y. 1988, Madde 17: Özel Yaşamın Gizliliği, par. 10.

²³⁸ ABTHŞ'nin 7. maddesi “Özel hayata ve aile hayatına saygı” kenar başlığı ile şu düzenlemeyi getirmiştir: “Herkes özel hayatına, konutuna ve haberleşme özgürlüğüne saygı gösterilmesini isteme hakkına sahiptir”. Bunu izleyen 8. madde ise “Kişisel verilerin korunması” kenar başlığı ile şu düzenlemeyi getirmektedir: “(1) Herkes, kendisini ilgilendiren kişisel verilerinin korunması hakkına sahiptir. (2) Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve düzelttirme hakkına sahiptir. (3) Bu kurallara uyulması, bağımsız

durum anayasal düzenlemeler açısından da kendini göstermektedir. Özel yaşamın gizliliği hakkı, hemen hemen bütün devletlerin anayasalarında temel bir hak olarak belirlenmiştir. Ancak kişisel verilerin korunması hakkının bağımsız olarak anayasal temelde korunduğu örnekler de artmaktadır²³⁹. Kişisel verilerin korunması, özünü özel yaşamın korunması hakkında bulsa da artık bağımsız bir hak olarak yeni bir temel değer oluşturmaya başlamıştır²⁴⁰.

Bunun yanında, özel ve aile yaşamına saygı hakkı ile kişisel verilerin korunması hakkı arasındaki ayrımın önemi yalnızca teoride kendini göstermemektedir. Nitekim özel ve aile yaşamına saygı hakkı bireyci yaklaşımı yansıtır. Statik bir hak olması dolayısıyla çoğu zaman negatif koruma gerektirir. Buna karşın veri korunması daha yüksek oranda dinamik bir koruma öngörmektedir. Bu koruma, veriyi her türlü hareketinde izler. Ayrıca kişisel verilerin korunmasına ilişkin hemen hemen bütün düzenlemeler bağımsız bir organ tarafından denetimi de öngörmektedir. ABTHŞ m.8/3 hükmü buna örnek olarak gösterilebilir. Bu anlamda korumanın bireye terk edilmediğini, kamusal bir otoritenin sürekli olarak bundan sorumlu tutulacağını söyleyebiliriz. Bu olgu, “*yalnız bırakılma hakkı*”ndan bilgi üzerinde denetim ve özel alanının nasıl şekilleneceğine karar verme hakkına doğru bir evrimin göstergesidir²⁴¹.

Bunun yanında verilerin korunması kapsamında değerlendirilen konuların karmaşıklığı özel yaşamın gizliliği hakkına ilişkin temel standartlardan türetilmesini güçleştirmektedir. AİHM ve pek çok ulusal mahkeme, kişisel verilerin korunmasına ilişkin özel bir hüküm olmamasına karşın, yorumlarıyla bu güçlüğü büyük oranda ortadan kaldırılabilmektedir. Ancak pek çok noktada bu koruma sınırlı kalabilir.

Örneğin AİHS’ne göre bireye ilişkin bilgiler toplanarak m. 8/1’deki özel yaşamın gizliliği hakkına müdahalenin m. 8/2 hükmünde yer alan sebeplerle hukuka uygun olduğunun kanıtlanması gerekir. Ancak, ikinci bölümde inceleneceği üzere, kişisel verilerin toplanmasının makul bir gerekçeye dayanması, bunların tutulmasını

bir makam tarafından denetlenir”. Metnin Türkçe çevirisi için bkz. Avrupa Birliği Temel Haklar Şartı, Avrupa Birliği İle İlişkiler Genel Müdürlüğü, Kasım 2001, www.dpt.gov.tr/DocObjects/Download/2962/temelhak.pdf, (s.y. 7 Şubat 2009).

²³⁹ Örneğin bkz. Hollanda Anayasası, m.10/2,3; Portekiz Anayasası m. 35; İspanya Anayasası m. 18/4.

²⁴⁰ Lawrence EARLY, “Science, Technology and Human Rights: The Role of Data Protection”, **Human Rights in the Twenty-first Century, A Global Challenge**, C.2, haz. Kathleen E. MAHONEY, Paul MAHONEY, Maritus Nijhoff Publishers, Hollanda 1993, s. 810.

²⁴¹ Stefano RODOTÀ, “Data Protection as Fundamental Right”, s. 3.

ve kullanılmasını mutlaka haklı kılmaz. Bunun gibi, veri hukuka uygun bir şekilde tutulduğunda bireyin buna ulaşımını sağlayan genel bir hak yoktur²⁴².

O halde şöyle söylenebilir; kişisel verilerin korunması her durumda bireylerin özel yaşamlarının korunması anlamına gelmektedir, ayrıca bu koruma bilişim teknolojilerindeki gelişimin bir sonucu olarak karşılaşılan elektronik veri işlemenin yarattığı tehlikelere bir cevap olarak ortaya çıkmıştır ve o günden bu güne içeriği değişmeye devam etmektedir. Kişisel verilerin korunması hakkı, en genel şekliyle bireye kişiliğine bağlı her türlü veri üzerinde tasarrufta bulunma hakkı vermektedir²⁴³. Ancak koruduğu temel değer açısından her iki hak alanının ortaklıkları çoktur. Bu nedenle özel yaşamın gizliliği hakkının gerekliliğine ilişkin değerlendirmeler kişisel verilerin korunması hakkı açısından da önemli bilgiler sunmaktadır.

c. Özel Yaşamın Gizliliği Hakkının Koruduğu Değer

Öncelikle şuna dikkat çekmek gerekir: özel yaşamın gizliliğinin bizim için neden önemli olduğunu basitçe açıklamak pek de kolay değildir. Bu nedenle konunun ilk olarak kişinin çıkarları üzerinden değerlendirildiği görülür. Nitekim özel yaşamın gizliliğinin ihlal edilmesinin kişilerin çeşitli çıkarlarına zarar verebileceği açıktır. Kişilerin kendilerine gizledikleri bazı taktiklerinin rekabet içinde bulundukları durumlarda ortaya çıkması onlara zarar verebileceği gibi, yaşamlarına ilişkin bazı konuların başkaları tarafından öğrenilmesinin onları utandırabileceği durumların varlığı da açıktır. Bunun yanında kişilerin sağlıklarına ya da mali durumlarına ilişkin bilgilerin istemedikleri kişilerce öğrenilmesinde maddi, manevi zararlar ortaya çıkabilir. Bu türdeki bilgilerin kimi kişilerce elde edilmesi evliliklerin sona ermesinden, işten çıkarılmaya kadar uzanan geniş bir yelpaze içinde çok çeşitli sonuçlar doğurabilir²⁴⁴.

Şirketlere ya da devlet organlarına kendilerine ait bilgileri veren birey, bu bilgilerin kötüye kullanılmasından dolayı mağdur olabilir. Bu, işlerini, kariyer tercihlerini ve yaşamlarının sonuna kadar mali durumlarını etkileyebilecek boyutta

²⁴² DJ HARRIS, M. O'BOYLE, C. WARBRICK, **Law of the European Convention on Human Rights**, Butterworths, Londra 1995, s. 310-311.

²⁴³ András JÓRI, "dataprotection.eu", <http://www.dataprotection.eu/>.

²⁴⁴ James RACHELS, "Why Privacy Is Important?", **Philosophy and Public Affairs**, C.4, S. 4, Y. 1975, s. 323-325.

zararlar doğurabilir. Ayrıca onların itibarlarının zedelenmesine de neden olabilir²⁴⁵. Bu nedenle örneğin eşcinsel birey, bu bilgiyi gizli tutmak isteyebilir. Kendisine ilişkin bilgilerin istemediği kişilerce öğrenilmesi, “damgalanma” ve dışlanma gibi sonuçlar doğurabilir. O halde özel yaşamın gizliliği ilk olarak ihlali durumunda oluşabilecek zarar açısından değerlendirilebilir.

Prosser’a göre özel yaşamın gizliliği hakkı dört tür haksız fiile karşı, dört tür çıkarı korumaktadır. Bunlar şu şekilde belirlenebilir²⁴⁶:

Haksız Fiiller	Çıkarlar
1. Kişinin sükunetinin, yalnızlığının, gizlerinin ve özel yaşamının ihlali	Kişinin manevi bütünlüğü
2. Kişinin özel yaşamına ilişkin utanç verici durumların kamuya açıklanması	Kişinin şeref ve onuru
3. Kişinin topluma yanlış tanıtılması	Kişinin şöhreti ve adı
4. Kişinin adının veya resminin çıkar sağlamak amacıyla kullanılması	Kişinin adından ve resminden doğan maddi çıkarları

Ancak Bloustein, Prosser’ın bu görüşünü eleştirerek, özel yaşamın gizliliğinin tek bir çıkarı “*insan onuru*”nu koruduğunu belirtmiştir²⁴⁷. Bizim de katıldığımız bu görüş, kişisel verilerin korunmasına ilişkin olarak Federal Alman Anayasa Mahkemesinin yukarıda değinilen değerlendirmesine de uygundur. Bu anlayışa koşut bir şekilde, Araslı da “*‘özel yaşamın gizliliği hakkı’nın bir tek temel değeri korumaya yönelik bulunduğu, bunun da ‘kişi dokunulmazlığı’, ‘insan onuru’, ‘kişilik’ gibi birbirinden farklı biçimlerde de ifade edilse ‘insanın insan olmasından doğan yüksek değeri’ olduğunu*” söylemektedir²⁴⁸.

Bu noktada özel yaşamın gizliliği hakkının ve kişisel verilerin korunmasının insanın insan olmasından doğan yüksek değeri için neden gerekli olduğu sorusu aklı gelir. Belirtilen çeşitli çıkarlar yanında, bu gerekliliğin antropolojik ve psikolojik

²⁴⁵ Michael ERBSCHLOE, John VACCA, **Net Privacy (A Guide To Developing and Implementing an Ironclad Ebusiness Privacy Plan)**, McGraw-Hill, ABD 2001, s.3.

²⁴⁶ William L. PROSSER, “Privacy”, **California Law Review**, Y. 1960, C.48, S.3, s. 383-423; Edward J. BLOUSTEIN, “Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser”, **New York University Law Review**, Y.1964, C.39, S.5, s. 965 vd.; Oya ARASLI, s. 43 vd.

²⁴⁷ Edward J. BLOUSTEIN, s. 962-1007.

²⁴⁸ Oya ARASLI, s. 48.

temelleri olduğu ileri sürülmüştür. Buna göre, antropoloji, biyoloji, sosyal bilim alanlarında yapılan çalışmalar, bütün canlılarda özel yaşamın gizliliği gereksinimi bulunduğunu ortaya koymaktadır. Bunun karşılanmadığı durumlarda ise bazı fiziksel ve psikolojik bozuklukların oluşabileceği belirtilmektedir²⁴⁹.

O zaman özel yaşamın gizliliğinin insanın sağlıklı bir fiziksel ve ruhsal yapıya sahip olması için gerekli olduğunu söyleyebiliriz. Ancak bununla da sınırlı kalmamaktadır: birey sosyal yaşam içerisinde ilişkilerini sürdürebilmek ve demokratik bir düzende siyasal haklarını tam anlamıyla kullanabilmek için de bu hakka gereksinim duyar. Özetle, konunun psikolojik, sosyal ve siyasal boyutlarının bulunduğu söylenebilir.

Özel yaşamın gizliliğine duyulan gereksinim, yalnızca kişilerin gizlemek isteyebilecekleri ya da onları utandırabilecek bilgiler çerçevesinde de düşünülmemelidir. Bireylerin, özel olarak utanç duymalarını ya da gizlemelerini gerektirmeyecek durumlarda, bunlar yalnızca “başkalarını ilgilendirmedeği” için kişilerin özel yaşamlarını gizli tutma hakları bulunmaktadır²⁵⁰. Garfinkel’in de belirttiği gibi;

“Özel yaşamın gizliliği hakkı, yalnızca bir şeyleri gizlemek ile ilgili değildir. İrade, özerklik ve bütünlük ile ilgilidir. 21. yüzyılın bilgisayarlaşmış dünyasına girdiğimizde özel yaşamın gizliliği hakkı en önemli bireysel haklarımızdan biri olacaktır. Ancak özel yaşamın gizliliği hakkı, belki de meşru olmayan ya da yasadışı etkinliklerde bulunmak istedikleri için, kapıları kapalı tutma ve perdeleri kapatma hakkı değildir. Bu, insanların yaşamlarına ilişkin hangi ayrıntıları evlerinin içinde tutacaklarını, hangilerini dışarı sızdıracaklarını kontrol etme hakkıdır”²⁵¹.

Evli bir çiftin cinsel yaşamına ilişkin son derece sıradan bilgilerin başkaları tarafından öğrenilmesini istememesi ya da mali bazı bilgilerin kendisine herhangi bir şekilde zarar vermeyecek de olsa (hatta bazı durumlarda bunların açıklanmasından dolayı iş yaşamında çeşitli çıkarlar da sağlayabileceği düşünülebilir) kendisine saklaması buna örnek olarak gösterilebilir.

²⁴⁹ Alan F. WESTIN, s.14 vd.; Oya ARASLI, s.20 vd.

²⁵⁰ James RACHELS, s. 326.

²⁵¹ Simson GARFINKEL, “Privacy and the New Technology”, s.11.

Rachels'a göre bir “*özel yaşamın gizliliği duygusu*”na sahibiz ve bu duygu çıkarlarımızın zedelenmesi ya da utanma korkumuzla açıklanamaz. Ona göre, özel yaşamın gizliliğinin asıl değeri, bize ve bizim hakkımızdaki bilgilere kimin ulaşabileceğini denetleyebilmemizle farklı kişilerle farklı ilişkiler kurabilme yeteneğimiz arasındaki ilişkide kendini bulmaktadır. Gerçekten bir kişi, çocuğuyla, eşiyle, patronuyla, çalışanıyla ya da çeşitli arkadaşlarıyla farklı kimliklerle ilişki kurar. Kimileri bunu sosyal ilişkilerde taktığımız çok çeşitli maskelerle “*gerçek*” kişiliğimizi gizlememizle açıklamaktadır. Ancak Rachels bu düşünceye aslında sosyal ilişkilerde takındığımız bütün rollerin en az diğerleri kadar “*gerçek*” olduğu düşüncesiyle karşı çıkmaktadır. Bize ve bize ilişkin bilgilere kimlerin ulaşabileceğini denetleyebildiğimiz ölçüde farklı kişilerle çeşitli ilişkiler kurabiliriz. İşte bu, özel yaşamın gizliliğine verdiğimiz önemin temel nedenidir²⁵² ve kişisel verilerin korunması hakkı da temelde bu amaca hizmet etmektedir.

Bu yaklaşım ayrıca temel hak ve özgürlükler anlayışıyla bağdaşmayacak bir şekilde özel yaşamın gizliliği hakkına müdahale oluşturan yaklaşımların savunucularının sıklıkla kullandığı “*saklayacak bir şeyin yoksa korkacak bir şeyin de yoktur*” sloganına da yanıt oluşturur. Özel yaşamın gizliliği hakkı ve kişisel verilerin korunması hakkı suçluların bilgilerine gizleyerek onların korunmasına hizmet etmemektedir. Bu iki önemli hak alanı “*insan*”ın yalnızca insan olması dolayısıyla sahip olduğu değerleri korumaya yönelmiştir ve bu şekliyle insanların kendileri hakkındaki bilgilere ilişkin bir denetim sağlar.

d. Özel Yaşamın Gizliliği Hakkının Sonu mu?

Özel yaşamın gizliliği hakkı, mutlak bir hak değildir. Konuya ilişkin ulusal ve uluslararası düzenlemelerde bu hakkın sınırları belirlenmiştir²⁵³. Üçüncü bölümde görüleceği gibi aynı durum kişisel verilerin korunması için de geçerlidir. Ancak özellikle son yirmi yıl içerisinde bu hak alanının hızla eridiği yönünde

²⁵² James RACHELS, s. 326-329.

²⁵³ Örneğin bkz. AIHS m.8/2 . Ayrıca özel yaşamın gizliliği hakkının başka bazı sosyal gerekliliklerle sınırlanabileceğine ilişkin olarak bkz. Amitai ETZIONI, **The Limits of Privacy**, Basic Books, ABD 1999. Etzioni bu çalışmada, devletin elinde kişisel bilgilerin toplanmasının pek çok alanda (terörizmle mücadele, genel sağlığın korunması, cinsel suçluluğun azaltılması gibi) gerekli olduğunu ve bu bağlamda pek çok özel yaşamın gizliliği savunucusunun karşı çıktığı çeşitli uygulamaların (gizli servisin özel e-mailleri okuması, çocuklara ana-babalarının izni olmaksızın HIV testi yapılması, ulusal kimlik kartları gibi) gerekli olabileceğini ABD hukuk sistemi çerçevesinde, çeşitli örnekler üzerinden tartışmaktadır. Bkz. **a.g.e.**

değerlendirmeler dikkat çekmektedir²⁵⁴. Bu bağlamda “*özel yaşamın gizliliğinin sonu mu?*” sorusu her geçen gün biraz daha fazla kişi tarafından dile getirilir olmuştur. Bunun başlıca nedeni yukarıda da tartışıldığı gibi bilişim teknolojilerinin gelişmesi ile bu alana çeşitli cephelerden pek çok saldırının olanaklı ya da kolay hale gelmesidir. Ancak bunun yanında, daha yakın bir zamanda özel yaşamın gizliliği hakkına yaklaşımda bir değişim olduğu da görülür.

Özel yaşamın gizliliği hakkı ile ilişkili sorunların sıklıkla tartışmalı ve zorlukla çözümlenebilir yapısı, bu alanının diğer bazı önemli hedeflerle arasındaki engellenemez çekişmeden kaynaklanır. Bu konudaki tartışmalarda, özel yaşamın gizliliği hakkının ihlal edildiğini iddia eden tarafın karşısına, hemen hemen her seferde, ihlalin asgari düzeyde olduğu ve amacın çok önemli sosyal, ticarî ya da yönetsel çıkarların korunması olduğunu söyleyen bir karşı taraf çıkmaktadır. Son yıllarda bu meşrulaştırma çabasının özellikle terörle mücadele merkezinde geliştiği de dikkat çekmektedir²⁵⁵. Burada 11 Eylül 2001’de ABD’ye karşı yapılan saldırı bir dönüm noktası olarak kabul edilebilir. Ardından Avrupa’da yaşanan çeşitli terör olayları bu sürecin devamı niteliğindedir.

Gerçekten 11 Eylül 2001 saldırıları öncesinde de küresel pazarın gereklilikleri dolayısıyla tüketicilerin davranış biçimlerinin saptandığı veri tabanlarının oluşturulması dolayısıyla “*özel yaşamın sona erdiği*” sıklıkla dile getiriliyordu. 11 Eylül sonrasında ise artık “*terör çağında özel yaşamın gizliliği*” ile karşı karşıya kaldık. Burada sorun yalnızca özel yaşamın gizliliğinin artık temel bir hak olarak bile görülmemesinin ötesindedir: bu hakkın güvenliğin önünde bir engel olarak değerlendirildiğine sıklıkla rastlanmaktadır²⁵⁶. Bu günde yaşananlar, uluslararası politikada önemli değişimlere neden olması yanında²⁵⁷, başta ABD olmak üzere, yeni teknolojilerin gelişmesi, yasama ve yürütme organlarının tasarrufları, toplumun özel

²⁵⁴ Bu çalışma içerisinde yararlandığımız birkaç kaynağın yalnızca adı bile bu endişeyi ortaya koymaktadır. Örneğin, Bert-Jaap KOOPS, Ronald LEENES, “‘Code’ and the Slow Erosion of Privacy” (‘Kod’ ve Özel Yaşamın Gizliliğinin Yavaş Erozyonu); Reg WHITAKER, **The End of Privacy** (Özel Yaşamın Gizliliğinin Sonu); Peter SCHAAR, **Das Ende der Privatsphäre** (Özel Yaşamın Gizliliğinin Sonu).

²⁵⁵ Harry HENDERSON, s. 4-5.

²⁵⁶ Stefano RODOTÀ, s.1.

²⁵⁷ 11 Eylül 2001 saldırılarının çeşitli açılardan değerlendirilmesine ilişkin olarak örneğin bkz. **The Age of Terror**, Amerika and the World After September 11, haz. Strobe TALBOTT, Nayan CHANDA, Basic Books, ABD 2001; **ABD, Terör ve İslam, 11 Eylül Üzerine**, der. Ahmet DEMİRHAN, Vadi, Ankara 2001; **11 Eylül**, Noam CHOMSKY, çev. Dost KÖRPE, OM Şimdi, İstanbul 2002.

yaşamın gizliliğini algılayışını ve hatta mahkeme kararlarını üzerinde etki yaratmıştır²⁵⁸.

Rotenberg, 11 Eylül sonrası Amerikalıların özel yaşamlarının artık eskisi kadar “gizli” olmadığını ve bu temel hakka yönelen saldırıların üç ayrı alanda kendini gösterdiğini savunmaktadır²⁵⁹. Birincisi, yasal düzenlemeler karşısında kişilerin koruma alanı zayıflamıştır. Bunun en açık göstergesi ise Amerikan Vatanseverlik Yasasının (U.S.Patriot Act) yürürlüğe girmesidir²⁶⁰. Bu yasa ile Amerikan özel yaşamın gizliliğinin korunması hukuku belki tamamen yerle bir olmamıştır, ancak pek çok önemli kural zayıflatılmıştır²⁶¹.

Burada bir noktaya dikkat çekmek gerekir: Amerikan Vatanseverlik Yasası ile 11 Eylül saldırıları, özel yaşamın gizliliğine ilişkin değerlendirmelerde sıklıkla birlikte anılmaktadır. Bunun nedeni, yasanın saldırıların hemen sonrasında yürürlüğe girmesidir. Vatanseverlik yasasının yanında, uçak yolcularına ilişkin kayıtların ABD’ye aktarılmasına ilişkin karar ve elektronik iletişim verilerinin tutulması dikkat çeken diğer uygulamalardır²⁶². Ayrıca sorunun, yalnızca Amerikan hukuku açısından geçerli olduğunu söylemek de olanaklı değildir. Nitekim 11 Eylül 2001 tarihinde Amerika’da yaşanan olaylar sonrasında, pek çok demokratik ülkede özel yaşamın gizliliği hakkına zarar verici düzenlemeler yapıldığı görülmektedir.

Bu düzenlemeleri 11 Eylül 2001 tarihinde bir anda ortaya çıkan yeni gerekliliklerin bir sonucu olarak da değerlendirmemek gerekir. Gerçekten bu düzenlemeler öncekilerden bağımsız değildir. Bunlar daha çok devletlerin geçmiş

²⁵⁸ Marc ROTENBERG, “Privacy and Secrecy After September 11”, *Minnesota Law Review*, Y. 2002, S.86, s. 1115. Bu tarihten sonra yapılan çeşitli araştırmalar, ABD’de güvenlik önlemlerin artırılmasını destekleyen bir eğilimin oluştuğunu göstermektedir. Ancak bunun yanında, kişilerde, özel yaşamlarına keyfi olarak müdahale edildiği yönünde bir kaygının da artan oranda geliştiği dikkat çekmektedir. Bkz. Robert POWER, “Changing Expectations of Privacy and Fourth Amendment”, *bepress Legal Series*, S. 1153, Y. 2006, <http://law.bepress.com/expresso/eps/1153> (s.y. 1 Mart 2008), s.2-4.

²⁵⁹ Marc ROTENBERG, s. 1115-1135.

²⁶⁰ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, 26 Ekim 2001, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107 (s.y. 5 Şubat 2009). Vatanseverlik Yasası, 11 Eylül’den yalnızca altı hafta sonra ve çok sınırlı bir tartışmanın ardından ABD Kongresi tarafından kabul edilmiştir. Yasada, özel yaşamın gizliliği hakkını zayıflatan pek çok hüküm bulunmaktadır. 2005 yılında yasanın çeşitli hükümleri yenilense de, kamuda, bu yasadaki kaynaklı, özel yaşamın gizliliği hakkının ihlaline ilişkin kaygılar sürmektedir. Harry HENDERSON, s. 35-36.

²⁶¹ Marc ROTENBERG, s. 1118.

²⁶² Stefano RODOTÀ, s.1.

daha eskilere dayanan niyetlerinin, girişimlerinin yeniden kurgulanmasının bir sonucudur²⁶³. Nitekim saldırıların öncesinde de gözetim hukukuna ilişkin benzer değişiklikleri içeren pek çok düzenleme gündemdedir²⁶⁴. Bu noktada 11 Eylül saldırılarının etkisinin Amerika’da özel yaşamın gizliliği açısından değiştirdiği şeyin bu konuya yaklaşım değil, bu yaklaşımın yaşama geçirilmesi noktasında olduğunu söylemek daha doğru olacaktır.

İkinci olarak özel yaşamın gizliliğine zarar verecek şekilde bazı yeni teknolojilerden yararlanılmaya başlandığı ya da yararlanma isteğinin daha açık ve güçlü bir şekilde ifade edildiği görülmektedir²⁶⁵. Nitekim terör olaylarının ardından gözetim sağlayıcı bazı uygulamalara halk desteğinin güçlendiği görülmektedir²⁶⁶. Yüz tanıma teknolojilerinin hızla yaygınlaşması ve sınır denetimlerinde güvenlik önlemlerinin fazlasıyla abartılması burada dikkat çekilebilecek birkaç örnektir²⁶⁷.

²⁶³ Avrupa’daki düzenlemelere ilişkin olarak bkz. Clive WALKER, Yaman AKDENİZ, “Anti-Terrorism Laws and Data Retention: War is Over?”, **Northern Ireland Legal Quarterly**, C.54, S.2, Y. 2003, s. 159-182. Bu kaynağa İnternet üzerinden şu adresten ulaşılabilir: http://www.cyber-rights.org/documents/data_retention_article.pdf (s.y. 2 Ocak 2009); Michael LEVI, David S. WALL, “Technologies, Security, and Privacy in the post-9/11 European Information Society”, **Journal of Law and Society**, C.31, S.2, Y. 2004, s. 194-220. Benzer uygulamaları yaşama geçiren Avrupa dışından bir örnek ise Kanada’dır. Nitekim 11 Eylül 2001 saldırıları pek çok yerde olduğu gibi Kanada da konuya yaklaşımın değişmesine neden olmuştur. Saldırılardan kısa bir süre sonra kabul edilen Terörle Mücadele Yasası (Anti-Terrorism Act) bunun en açık göstergesidir. Bu yasa uyarınca ile polisin elektronik gözetim yapmasını sağlayan araçlar ve bunların kapasiteleri ile ulusal güvenlik gerekçeleri ile verilere ulaşmayı sağlayan istisnalar arttırılmıştır. Buna karşın kamuyu aydınlatan bilgilerin açıklanmasına sınırlama getirilmiştir. **Privacy and Human Rights 2006**, s. 311. 11 Eylül saldırıları sonrasında gelişen güvenlik kaygısının yansıdığı bir diğer yasa ise 2002 yılında kabul edilen Kamu Güvenliği Yasasıdır (Public Safety Act). Bu yasada da terörle mücadele amacıyla getirilen ve kişilerin özel yaşamlarını doğrudan etkileyen hükümler bulunmaktadır. Havayolu taşımacılarına ve rezervasyon sistem operatörlerine yolcuların, rızaları bulunmaksızın, ayrıntılı kayıtlarını tutma yükümlülüğü getirilmesi bu kapsamda sayılabilecek örneklerden biridir. Jason M. YOUNG, s. 45.

²⁶⁴ Daniel J. SOLOVE, “Reconstructing Electronic Surveillance Law”, s. 1277-1278; Orin S. KERR, “Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn’t”, **Nortwestern University Law Review**, C. 97, Y. 2003, s. 607-637.

²⁶⁵ Stefano RODOTÀ, s.1.

²⁶⁶ Örneğin yapılan araştırmalar ABD’de 11 Eylül’ü izleyen günlerde ulusal bir kimlik kartının kullanılmasına yönelik halk desteğinin açık bir şekilde güçlendiğini göstermektedir. Marc ROTENBERG, s. 1119-1120.

²⁶⁷ Marc ROTENBERG, s. 1121-1122. Özellikle uçak yolcularına ilişkin güvenlik kontrollerinin hızla arttığı görülmektedir. Örneğin; 4 Ocak 2010 tarihinde ABD tamamı Müslüman on dört ülkeden gelen yolcuları “*tam vücut görüntüleme*” uygulamasına tabi tutma kararı bu uygulamaların ne kadar uç noktalara ulaşabileceğinin göstergesidir. Belirtilen yöntem ile kişilerin vücut hatlarına ilişkin ayrıntılı görüntüler alınması hak ve özgürlüklere zarar verici niteliktedir. Bunun yanında uygulamanın yalnızca belirli ülkelerden gelen yolculara yönelik olması ayrımcılık yasağının da ihlaline neden olmaktadır. Bkz. “Müslüman Yolcuya Ayrımcılık”, **Radikal**, 5 Ocak 2010. Tam vücut görüntüleme ve tarama teknolojisinin kişisel verilerin korunması açısından yarattığı çeşitli sorunlara ilişkin olarak bkz. “Whole Body Imaging

Bunların bir de, telefon dinleme gibi daha eski yöntemlerin artan oranda kullanılması, terörizm şüphesiyle özellikle Orta Doğulu kişilerin gözetim altında tutulması gibi uygulamalarla birleşmesi, bir paranoya ve şüphe ortamının yaratılmasına neden olmaktadır. Bu ise bireysel hakların ve özellikle de özel yaşamın gizliliği hakkının zedeleneceği konusunda ciddi bir kaygı oluşturmaktadır²⁶⁸.

Üçüncü olarak devletin gizlilik alanında bir genişleme gözlenmektedir. Kamusal kayıtlara ulaşma olanakları azaltıldığı gibi, normalde kamuya açık yapılan bazı görüşmelerin kapalı kapılar ardında yapılmaya başlanması da dikkat çekicidir²⁶⁹. Kişilerin özel yaşamlarına yönelen saldırılara rağmen alınan bu önlemlerin güvenlik açısından bir yarar sağlanıp sağlanmadığı ise kuşkuludur. Kimi yazarlar, saydamlık ve açıklığın mahremiyetle çatışan kavramlar olduğunu, bu nedenle daha yüksek bir kamusal değer için özel yaşamın gizliliği hakkından kısmen feragat edilebileceğini ileri sürer²⁷⁰.

Rotenberg'e göre ise bu ve benzeri görüşleri ileri süren yazarlar “gizlilik” (secrecy) ile “özel yaşamın gizliliği” (privacy) kavramları arasındaki ilişkiyi tam olarak kavrayamamıştır. Hem Avrupa, hem de Amerikan geleneği, özel yaşamın gizliliğini korurken, devletin kapalılığını sınırlandırmak üzerine kurulmuştur ve 11 Eylül sonrasında bu iki değer büyük bir risk altındadır²⁷¹. Bu risk kendini özellikle kişisel verilerin korunması hakkı açısından gösterir.

Gözetime yönelik bütün bu uygulamalar karşısında, pek çok demokratik devlette kişisel verilerin korunması hakkının ihlal edildiği görülmektedir. Örneğin toplanan verilerin yalnızca toplandıkları amaçla kullanılması ilkesinin pek çok kez ihlal edildiği görülmektedir. Belirli bir amaç için toplanan veriler, güvenlik gibi

Technology and Body Scanners”; Electronic Privacy Information Center, <http://epic.org/privacy/airtravel/backscatter/>.

²⁶⁸ Edwar SAID, “Şüpheliğin Zorunluluğu, Geri Tepki ve Geriye Dönüş”, **ABD, Terör ve İslam**, s. 33.

²⁶⁹ Marc ROTENBERG, s. 1123-1125.

²⁷⁰ Amitai ETZIONI, “Introduction: Rights and Responsibilities Post 9/11”, **Rights vs. Public Safety After 9/11, America in the Age of Terrorism**, haz. Amitai ETZIONI, Jason H. MARSH, Rowmann & Littlefield, İngiltere 2003, s. ix-xviii. Belirtmek gerekir ki ETZIONI, biyometrik yöntemleri ve gerçek kimlik kartlarının kullanımının yararlarını 11 Eylül saldırılarının öncesinde de dile getirmiştir. Bkz. Amitai ETZIONI, “Identification Cards in America”, **Society**, C.36, S.5, Temmuz 1999, s.70-76.David BRIN, “Some Notes About Calamity and Opportunity”, (Bu yazı ilk kez 2001 yılında 11 Eylül saldırılarından kısa bir süre sonra yayınlanmıştır), <http://www.futurist.com/archives/society-and-culture/calamity-and-opportunity/> . Ayrıca Marc ROTENBERG, s.1125-1127.

²⁷¹ Marc ROTENBERG, s. 1127-1128.

üstün sayılan gerekçelerle, farklı amaçlar için kullanılabildiği gibi, verildiği kuruluştan başka kuruluşlarca da elde edilebiliyor²⁷².

Özel yaşamın gizliliği hakkı ile yurttaş ve devlet arasındaki güç dengesinin yakın ilişkisi bulunduğu²⁷³ dikkatten kaçmamalıdır. Bu bağlamda, özel yaşamın gizliliği hakkını koruyan yasalar, güçler arasındaki dengesizliği gidererek bireyleri özel yaşamlarına müdahale edebilecek kurumlardan koruma amacını da taşımaktadır. Bu açıdan bakıldığında, 11 Eylül sonrasında tanık olunan gelişmeler, devletin gücü artarken bireylerin haklarının zayıflaması sonucunu doğurmuştur²⁷⁴. Bu noktada Benjamin Franklin'in ünlü sözünü hatırlamak gerekir: temel bir özgürlüğü, geçici güvenlik için terk edenler, ne özgürlük ne de güvenliği kazanacaklardır.

Bu aslında güvenlik kaygıları karşısında özgürlük taleplerinin cılızlaşmasının bir sonucudur. Hemen hemen her zaman güvenliklerinden endişe duyan bireyler, temel hak ve özgürlüklerinin bir kısmından ya da kimi zaman tamamından gönüllü olarak vazgeçmektedir²⁷⁵. Yukarıda da işaret edildiği gibi 11 Eylül 2001 saldırılarından sonra yalnızca ABD'de değil, başta batı Avrupa olmak üzere dünyanın pek çok yerinde gözetim artıyor. Demokratik yönetim altında yaşayan nüfusun çoğunluğu ise, özgürlüklerinin korunmasını güvence altına alma adına özel yaşamlarının sınırlandırılmasını kabule hazır görünüyor²⁷⁶.

Güvenlik elbette insanın çok temel bir gereksinimidir. Ancak burada karar verilmesi gereken asıl soru, bu vazgeçişin ne kadar gerekli olduğudur: Güvenliğin sağlanabilmesi için olağan dışı tedbirlerin alınması bir zorunluluk mudur, yoksa normal koşullarda bireylerin kabul etmeyeceği, ancak yönetimdekilerin istediği koşulların yaratılması için bir bahane midir?²⁷⁷ Bu, cevaplanması çok da kolay olmayan önemli bir sorudur. Elbette terörle mücadele ve güvenliğin sağlanması

²⁷² Stefano RODOTÀ, s. 2.

²⁷³ Raymond Shih Ray KU, "The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance", **Minnesota Law Review**, C.86, Y.2001-2002, s. 1326.

²⁷⁴ Marc ROTENBERG, s. 1132-1133.

²⁷⁵ Örneğin 2008 yılında açıklanan bir araştırma AB yurttaşlarının büyük bir çoğunluğunun uluslararası terörle mücadeleyi kişisel verilerin korunmasını sınırlandırmak için haklı bir gerekçe olarak gördüğünü ortaya koymuştur. Bkz. "Eurobarometer survey reveals that EU citizens are not yet fully aware of their rights on data protection", MEMO/08/249, 17 Nisan 2008, <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/249&format=HTML&aged=0&language=EN&guiLanguage=en>.

²⁷⁶ Peter SCHAAR, **Das Ende der Privatsphäre**, s. 97.

²⁷⁷ Bu konuya ilişkin olarak ayrıca bkz. Mithat SANCAR, "Kalıcı Global Olağanüstü Hal", **Birikim**, Kasım 2001, S.151, s.12-21.

devletin başlıca görevleri arasındadır. Ancak bu, belirtilen amaçlarla ölçsüz önlemlerin alınabileceği anlamına gelmez. Kanada Yüksek Mahkemesi bir kararında bu sorunu şu şekilde değerlendirmiştir²⁷⁸:

“Bir yanda terörün ve masum insanların canına tesadüfi ve keyfi bir şekilde kıymanın, giderek artan kayıp ve korku sarmalını tetikleyen apaçık kötülüğü durmaktadır. Yönetimler, yönetilenlerin isteğinin ifadesi olarak, bu sorunu karşılayacak etkili araçlara gereksinim duyarlar.

Diğer yanda ise bu araçların, demokratik toplumumuzun temelini oluşturan, özgürlük, hukukun üstünlüğü, adaletin temel ilkeleri gibi Kanada Anayasası hükmünün ve Kanada’nın imzaladığı uluslararası belgelerin kalbinde yatan değerleri zayıflatmamasının sağlanması gerekliliği bulunur. Sonunda eğer terörizm, bu değerlere olan bağlılığımız feda edilerek, mağlup edilirse bu ancak bir Pirus Zaferi olur. Parlamantonun çözmesi gereken sorun, terörizmle etkili bir şekilde mücadeleyi sağlayan ve uluslararası bağliliklarımız ve Anayasamızın gereklilikleri ile uyumlu yasalar hazırlamaktır”.

Elbette bu dengeyi sağlamak kolay değildir. Bu çalışmanın çeşitli yerlerinde de değinildiği üzere güvenlik gereksinimi karşısında özgürlüklerin korunması hem sanal hem gerçek dünyada çağımızın en önemli sorunlarından birini oluşturmaktadır.

Bilgi toplumunda koşulsuz özel yaşamın korunması hakkının giderek daha az önem verilen bir değer haline geldiği görülmektedir. Ancak bu özel yaşamın gizliliği hakkının artık önemsiz olduğu anlamına gelmez. Değerler arasında uygun bir denge bulunmalıdır. Bilgi teknolojileri kötüye kullanılabilir ve bu noktada unutulmaması gereken, insanlar hakkında bazı olguların bilinmesinin bunların her türlü amaç için kullanılabileceği anlamına gelmediğidir. Örneğin bir kişinin ciddi bir hastalığı olduğunu bilmek, sigorta şirketlerine risk ve maliyet hesaplamalarını daha doğru bir şekilde yapabilme olanağı verir. Ancak belirtilen bilgiler, bu kişilerin sigorta sözleşmesi yapma haklarının ellerinden alınması gibi bir sonuç doğurmamalıdır. Bunun yanında, yalnızca kötüye kullanılması yönündeki korkudan dolayı, kişisel verilerin toplanması ve birlikte işlenmesinden vazgeçmek de akla uygun görünmemektedir. Bilgi teknolojilerinin kötüye kullanılmasının önüne geçebilmek

²⁷⁸ Suresh Kanada’ya (Yurttaşlık ve Göçmenlik Bakanlığı) karşı, [2002] 1 S.C.R. 3, 2002 SCC 1, par. 3-4; Jason M. YOUNG, s. 46.

için ilk gereklilik şeffaflığın sağlanmasıdır. Birey, kendisiyle ilgili bilgilerin nasıl kullanıldığını bilme ve bu konuda harekete geçme olanağına sahip bulunmalıdır²⁷⁹.

Görüldüğü gibi özel yaşamın gizliliği hakkı, dolayısıyla kişisel verilerin korunması hakkı kaynağını öncelikle insan onuru, kişilik hakkı ve bireysel özerklikte bulmaktadır. Bunun yanında kişisel verilerin korunması pek çok başka hak ve özgürlükle de ilişkilidir. Bu ilişki kimi zaman çatışma, kimi zaman ise kesişme ve birbirini tamamlama şeklinde kendini gösterir. Aşağıda bu hak alanlarından en yakın ilişki içinde bulunanları kısaca değerlendirilecektir.

3. DÜŞÜNCEYİ AÇIKLAMA ÖZGÜRLÜĞÜ VE KİŞİSEL VERİLERİN KORUNMASI HAKKI

a. Düşünceyi Açıklama Özgürlüğü

Düşünceyi açıklama özgürlüğü, “*insanın serbestçe düşünce ve bilgilere ulaşabilmesi, edindiği düşünce ve kanaatlerden dolayı kınanaması ve bunları tek başına ya da başkalarıyla birlikte (dernek, toplantı, sendika vb.) çeşitli yollarla (söz, basın, sinema, tiyatro vb.) serbestçe açıklayabilmesi, savunabilmesi, başkalarına aktarabilmesi ve yayabilmesi anlamına gelir*”²⁸⁰. Düşünceyi açıklama özgürlüğü, bu kapsamda özgürce yayın yapan kitle iletişim araçları olmadan açık ve aydınlanmış bir toplumdan söz edilemez. Ancak Kant’ın da belirttiği gibi, sorumlulukla özgürlüğü birbirine bağlamak gerekir. Bu nedenle düşünceyi açıklama özgürlüğünün belirli sınırları olduğu kabul edilmektedir. Bu sınırlardan biri de kişisel verilerin korunması hakkının da temel dayanaklarından olan kişiliğin geliştirilmesine ilişkin anayasal ilkelerdir²⁸¹. Nitekim düşünceyi açıklama özgürlüğü, demokratik bir toplumun eksen özelliklerinden biri olsa da, bu özgürlük, “*bireylerin öğrenmek istedikleri her şeyi bilme hakkı olduğu anlamında yorumlanamaz*”²⁸².

²⁷⁹ Pieter KLEVE, Richard De MULDER, s. 348.

²⁸⁰ Bülent TANÖR, **Türkiye’nin İnsan Hakları Sorunu**, BDS Yayınları, 3. Baskı, İstanbul 1994, s.59.

²⁸¹ Marie-Theres TINNEFELD, Eugen EHMAN, Rainer W. GERLING, **Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht**, R. Oldenburg Verlag, Almanya 2005, s. 613-614.

²⁸² Nur ULUŞAHİN, “İnsan Onuru Kavramı Temelinde Mahremiyet, İfade Özgürlüğü ve Medya”, **II. Ulusal Uygulamalı Etik Kongresi Bildiriler Kitabı, 18-20 Ekim 2006**, Ankara 2007, s. 678. (s.675-682) .

b. Düşünceyi Açıklama Özgürlüğü ve Kişisel Verilerin Korunması Hakkı Arasındaki Gerilim Hattı

Kişisel verilerin korunması hakkı, düşünceyi açıklama özgürlüğü ile çatışma potansiyeli taşımaktadır. Böylesine bir çatışma özellikle düşünceyi açıklama özgürlüğü içerisinde değerlendirilen basın özgürlüğü açısından kendini gösterir. Özellikle magazin basını olarak adlandırılabilir yayınlar, meraklı bir okuyucu kitlesine başkalarına ilişkin, son derece mahrem bilgiler yazı, fotoğraf ya da görüntüler ile aktarılmaktadır²⁸³. Bu tür yayınların toplum üzerindeki etkileri sosyologlarca araştırılan bir konuyu oluşturur. Ancak bu yayınlarının önemli hukuksal sonuçları da olmaktadır ve özel yaşamın gizliliği hakkının ilk kez ortaya çıktığı zamandan beri tartışılmaktadır. Nitekim Warren ve Brandeis'in , “*yalnız bırakılma hakkı*”nı geliştirdikleri ünlü makalelerini bireyin özel yaşamından beslenen azgın basının insan onuru, bireysel özerklik gibi önemli değerleri yok etmesi korkusundan hareketle kaleme alındığı bilinmektedir²⁸⁴. O halde en azından Amerikan hukuku açısından özel yaşamın gizliliği hakkının koruma altına alınmasında magazin basınının tacizkar hareketlerinin etkisi bulunur.

Bir tarafta halkın ilgisini çeken konuları araştıran, değerlendiren, yayınlayan basın kuruluşları, diğer yanda, kişisel bilgilerinin paylaşılmamasını isteyen bireyler arasında adeta gerilim hattını andıran bir çekişme söz konusu olmaktadır. Amerikan hukukunda “*kamusal figür*” olarak nitelenen ve kapsamında politikacılardan, eğlence sektöründe çalışanlara, yöneticilerden, sporculara kadar oldukça geniş bir kesimi barındıran kategorinin bu anlamda, özel yaşamın gizliliği hakkını daha sınırlı oranda ileri sürebileceği kabul edilmektedir. Buradaki temel dayanak, bu kişilerin kendi istekleri ile kamunun gözü önünde bulunmalarıdır. Bu gerekçe bile tartışmalı olmakla birlikte, böyle bir iradi seçim söz konusu olmaksızın, yalnızca birinin çocuğu, eşi, arkadaşı ya da yankı uyandıran bir suçun mağduru olması dolayısıyla “*kamusal figür*” haline gelenlerin konumu ne olacaktır?²⁸⁵ Bu soruya verilecek cevap aslında basın özgürlüğü ile özel yaşamın gizliliği ve kişisel verilerin korunması hakkı arasındaki ilişkide hangisine ağırlık verileceği ile ilişkilidir.

²⁸³ Pieter KLEVE, Richard De MULDER, s. 339.

²⁸⁴ Edward J. BLOUSTEIN, s. 971.

²⁸⁵ Nur ULUŞAHİN, s.678.

O halde düşünceyi açıklama ve basın özgürlüklerinin kullanımının kimi zaman kişisel verilerin korunması hakkına bir müdahale yaratabileceği açıktır. Diğer yandan kişisel verilerin korunması hakkının düşünceyi açıklama ve basın özgürlüklerinin gereği gibi kullanımında bir engel oluşturabildiği yönünde eleştiriler de söz konusu olabilir. Bu durumda her bir olayda tartım ve değerlendirme yapılmalı ve somut olayın kendisine özgü koşulları içinde hangisine ağırlık verileceği saptanmalıdır.

Kişisel verilerin korunmasına ilişkin çeşitli düzenlemelerde “eğer gerekli” ise düşünceyi açıklama özgürlüğünü korumak için istisna getirilebileceğine dair hükümler yer alır²⁸⁶. Buradaki “gerekliklik” koşulu her devletin olayın kendine özgü koşullarına uygun bir değerlendirme yapması ile açıklık kazanacaktır. Aynı şekilde düşünceyi açıklama özgürlüğüne ilişkin çeşitli düzenlemelerde doğrudan kişisel verilerin korunmasına atıf yapılmasa da kişisel hakların korunmasının hakkın sınırları arasında yer aldığı görülmektedir²⁸⁷.

Buna karşın, her iki hakkın arasındaki ilişkiye dair tartışmalar sürmektedir. Örneğin İsveç’te düşünceyi açıklama özgürlüğü savunucuları İsveç hükümetinin veri koruma yasalarını İnternet’te istemedikleri görüşlerin ifade edilmesini önlemek amacıyla kullandıklarını iddia etmektedir²⁸⁸. Oysa yasal düzenlemeler açısından

²⁸⁶ Bkz. AB Kişisel Verilerin Korunması Yönergesi AT/95/46, m.9. Ayrıca bkz. Article 29 WP 1/97 , First report on implementation of the Data Protection Directiv. Konuya ilişkin pek çok düzenlemede basın özgürlüğünün kullanılması kapsamında gerçekleştirilen faaliyetlerin veri koruma yasalarında belirtilen kuralların istisnasını oluşturduğu dikkat çekmektedir. Örneğin bkz. İsveç Veri Koruma Yasası sec.7; Avustralya Özel Yaşamın Gizliliği Yasası, sec. 7B (http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s7b.html , s.y. 20 Şubat 2009);

²⁸⁷ AİHS’nin 10. maddesi 2. fıkrasında “*Kullanılması görev ve sorumluluk yükleyen bu özgürlükler, demokratik bir toplumda gerekli tedbirler niteliğinde olarak, ... başkalarının şöhret ve haklarının korunması ... için yasayla öngörülen bazı merasime, koşullara, sınırlamalara veya yaptırımlara bağlanabilir*” hükmü yer almaktadır. Federal Almanya Cumhuriyeti Anayasası’nın düşünce, basın ve bilim, sanat özgürlüklerini düzenleyen 5. maddesinin ikinci fıkrası ise benzer şekilde şu hükmü içermektedir: “*Bu haklar, ... kişisel şeref hakları ile sınırlıdır*”. Her iki hak alanı arasındaki gerilimi değerlendiren birkaç örnek için bkz. AİHM Goodwin Birleşik Krallığa karşı, (b.n. 17488/90, k.t. 27 Mart 1996-gazetecinin basın özgürlüğü ve haber kaynağı kişinin mahremiyetine ilişkin olarak); Alman AYM, (BVerfGE 20, 162, 216-basının işlevselliğini sürdürülebilmesi için basın organı ve haber kaynağı arasındaki güven ilişkisinin önemine ilişkin olarak); AAD, Linquist kararı (C101-01-İnternet ortamında yayınlanan bilgiler ve ilgili kişinin kişisel verilerin korunması hakkına ilişkin olarak)..

²⁸⁸ Ancak İsveç Anayasa Mahkemesi (Supreme Court) 2001 yılında verdiği bir kararda, özelde İnternet ortamında, iki hak alanı arasında çatışan değerlere açıklık getirmiştir. Mahkeme kararını geliştirirken, AB Veri Koruma Yönergesi’nin 9. maddesini, AİHS’nin de 8. ve 10. maddelerini dikkate almıştır. İsveç Yüksek Mahkemesi, gazetecilik amacıyla İnternet’te yapılan yayınların İsveç Veri Koruma Yasası’nın veri aktarımına ilişkin sınırlamalarına tabi olmayacağına karar vermiştir. Mahkemeye göre, davalı her ne kadar gazeteci olmasa da web sitesi “*kamunun ilgisini*

bakıldığında, İsveç mevzuatının kişisel verilerin korunması karşısında düşünceyi açıklama ve basın özgürlüğüne ağırlık verdiği görülür²⁸⁹.

Benzer şekilde özellikle radikal düşünceyi açıklama özgürlüğü savunucularından, kişisel verilerin korunması aleyhine sesler yükselmektedir. Elbette eğer herkes “*yalnız bırakılma hakkı*”nı kullanmak isterse, düşünceyi açıklama özgürlüğünün etkinliği büyük zarar görecektir. Ancak insanlar sosyal varlıklar olduğuna göre bu yalnızca teoride kalacak bir kaygıdır. Bunun yanında, kişisel verilerin korunmasındaki zayıflamanın düşünceyi açıklama özgürlüğünün güçlenmesini sağlayacağı yönünde bir düşünce oldukça yanıltıcı olur. Aşağıda da kısaca tartışılacağı üzere, beklenenin aksine bunun tam tersi bir etki yaratması bile söz konusu olabilir²⁹⁰.

Verilerin korunması hakkı ile düşünceyi açıklama özgürlüğü arasında kaçınılmaz bir gerilim bulunsa da her iki hakkın bir arada gerçekleşmeyeceğine dair her hangi bir neden bulunmamaktadır²⁹¹. 29. Madde Veri Koruma Grubu²⁹² da veri koruma hakkı ile düşünceyi açıklama özgürlüğünün özünde çelişkili olmadığına, üye

çeken konularda bilgilendirme, eleştirme ve tartışma yaratma” gibi gazetecilik amaçlarını taşıdığından bu kapsamda değerlendirilecektir. Public Prosecutor v. Ramsbro, k.t.: 12 Haziran 2001, S. B 293-00. Kararın orijinal metni için bkz. <http://www.bankrattsforeningen.org.se/HDdomslut.html> (s.y. 20 Şubat 2009). Bkz. Christopher KUNER, **European Data Protection Law, Corporate Compliance and Regulation**, 2. Baskı, Oxford University Press, Büyük Britanya 2007s. 85-86; Lee A. BYGRAVE, “Data Protection Law-Sweden: Balancing Data Protection and Freedom of Expression in the Context of Website Publishing-Recent Swedish Case Law”, **Computer Law and Security Report**, C.18, S.1, s. 56-58. İsveç Temyiz Mahkemesi’nin aynı yönde verdiği bir başka karar için bkz. Hovrätten för västra Sverige, Mål T2505-01, Haziran 2002. Bkz. **Constitutional Rights and New Technologies**, A Comparative Study Covering Belgium, France, Germany, Sweden, and the United States, haz. Bert-Jaap KOOPS, Ronald LEENES, Paul de HERT, Tilburg, Şubat 2007, <http://www.voxinternet.fr/IMG/crant-report-2007def-1.pdf> (s.y. 20 Şubat 2009). Ayrıca bkz. Linqvist kararı par. 88-90. Basın özgürlüğü ve kişisel verilerin korunması hakkı arasındaki gerilimin Avustralya hukuku açısından değerlendirmesi için bkz. Nigel WATERS, “Can the Media and Privacy Ever Get On?”, *Privacy Law and policy Reporter*, Y. 2002, C.8, S.8, <http://www.austlii.edu.au/au/journals/PLPR/2002/1.html> (s.y. 20 Şubat 2009).

²⁸⁹ İsveç anayasa hukuku açısından kişisel verilerin korunmasına yaklaşımın özellikleri ve Alman anayasa hukuku ile farklılıkları için bkz. Hans-Heinrich VOGEL, Comments on Draft No.4735 on Protection of Processing of Personal Data, European Commision for Democracy Through Law (Venice Commisison), Opinion No. 207/2002_lux, 17 Mayıs 2002, CDL(2002)67, [http://www.venice.coe.int/docs/2002/CDL\(2002\)067-e.pdf](http://www.venice.coe.int/docs/2002/CDL(2002)067-e.pdf) (s.y.: 18 Şubat 2009).

²⁹⁰ Jeremy Haris LIPSCHULTZ, **Free Expression in the Age of the Internet**, Social and Legal Boundaries, Westview Press, 2000, s. 234-235.

²⁹¹ Christopher KUNER, s. 84.

²⁹² 29. Madde Veri Koruma Grubu, Kişisel Verilerin Korunmasına ilişkin 95/46/AT sayılı Yönerge’nin 29. Maddesine göre kurulmuştur. Bu Grup hakkında bilgi II. Bölüm’de verilecektir.

devletlerin her iki hak alanının sınırlarını tanımlamaya yeterli düzeyde önem atfetmediklerine dikkat çekmiştir.

O halde şöyle söylenebilir; veri koruma ve düşünceyi açıklama özgürlüğü arasında temel bir çatışma yoktur, ancak her iki hakkın da diğeri karşısında dengelenmesi gerekir. Bu dengelenme ise orantılılık gibi temel ilkeleri ve olayın kendine özgü koşullarını dikkate alarak gerçekleştirilebilir²⁹³.

c. Düşünceyi Açıklama Özgürlüğü ve Kişisel Verilerin Korunması Hakkının Birbirini Destekleyici Nitelikleri

Bunun yanında her iki hak ve özgürlüğün birbirlerini desteklediği alanlar da bulunmaktadır. Düşünceyi açıklama özgürlüğü ile bireyin açıklamalarının içeriğini ve muhatabını belirleme hakkı güvence altına almaktadır. Bu ise bireyin kişisel verileri üzerindeki belirleme hakkının bir ögesidir. Aynı durum tam tersi için de söylenebilir. Yani kişisel verilerin korunması hakkı ile düşünceyi açıklama özgürlüğü korunur. Çünkü bu hak kapsamında, insanlar düşüncelerini kiminle ne zaman, nerede, paylaşacaklarını seçebilirler²⁹⁴.

Ayrıca, kimsenin düşüncelerini açıklamaya zorlanamayacağı kuralı düşünceyi açıklama özgürlüğü kapsamında değerlendirilirken, diğer yandan da kişisel verilerin korunması açısından kısmi bir güvence sağlamaktadır. Bu kural, bireyin gizli kalmasını istediği verileri açıklamaya zorlanamamasına ve özellikle hassas verilerinin kendisinde saklı tutması isteğine destek verir. Bu şekilde, kural olarak bireyin kişisel verilerinin ancak kendi rızası ile toplanabilmesi ilkesi ve kişisel verilerini açıklama konusunda bireyin belirleme hakkı düşünceyi açıklama özgürlüğü ile de desteklenmiş olmaktadır²⁹⁵.

Bunun yanında örneğin, düşünceyi açıklama özgürlüğü kapsamında değerlendirilebilecek derneklere, sivil toplum kuruluşlarına, toplantı ve gösteri yürüyüşlerine katılma hakkı açısından, kişisel verilerin korunması destekleyici bir nitelik taşımaktadır. Bireyin kamuya açık bir ortamda yapılan bir toplantıya ya da gösteri yürüyüşüne katılma özgürlüğünü kullanması onun tamamen anonimleştiği anlamına gelmez. Bir başka anlatımla, kamusal ulaşılır bir alanda bu hakkını

²⁹³ Christopher KUNER, s. 87.

²⁹⁴ Ann CAVOUKIAN, Don TAPSCOTT, s. 14.

²⁹⁵ Oğuz ŞİMŞEK, s.146-147.

kullanan kişi, kendisinin bu toplantıya ya da gösteriye katıldığının ve kimliğinin öğrenebilme olasılığını göz önüne almalıdır²⁹⁶. Ancak bu, belirtilen hareketlerine ilişkin ses kaydının ya da görüntülerinin kayıt altına alınıp her türlü amaç için kullanılabileceği anlamına gelmez. Buna karşın, her sözü, her türlü üyeliği, her protestosu bir şekilde kayıt altına alındığını düşünen kişi, muhalif görüşlerini açıklamaktan kaçınabilir. Bu, bazılarının demokratik süreçlere katılmasını, düşüncelerini açıklamalarını ya da karar alma organlarında yer almak için yarışmalarını engellerse son derece önemli bir kamusal yarar, zarar görür²⁹⁷. Bu noktada belirtilen sorunla da yakından ilgili son derece önemli bir konuya “anonimlik hakkı”na kısaca değinmekte fayda vardır.

d. Anonimlik Hakkı

Hem düşünceyi açıklama özgürlüğü, hem de özel yaşamın gizliliği hakkı ekseninde tartışılan²⁹⁸ anonimlik genel olarak, bir kişi ya da grubun görüş ve düşüncelerini kimliğini ortaya çıkarmadan açıklaması ve yayması olarak tanımlanabilir²⁹⁹. İhbarcılar, muhalifler, utangaç kişiler, görüşlerini açıklamalarının kendilerini olumsuz bir şekilde etkileyeceğini düşünenler, kişisel verilerinin

²⁹⁶ Oğuz ŞİMŞEK, s.147-148.

²⁹⁷ Jeremy Haris LIPSCHULTZ, s.235.

²⁹⁸ Belirli durumlarda anonimlik hakkı çeşitli mahkeme kararları ile de tanınmıştır. AmerikanYüksek Mahkemesinin İnternet ortamında kimliğini ortaya koymaksızın, anonim kalarak broşür yayınlamayı bir hak olarak tanıyan bir kararı için bkz. McIntyre v. Ohio Elections Commision, (93-986), 514 U.S. 334, (1995), <http://supct.law.cornell.edu/supct/html/93-986.ZO.html> ; Eyalet Yüksek Mahkemesi, Anayasanın Birinci Eki'ne dayanarak, gönderenin tam olarak belirlenemediği her türlü elektronik iletişimi yasaklayan bir eyalet yasasının iptaline ilişkin olarak Georgia karar için bkz. ACLU of Georgia v. Miller, US District for the Northern Distrct of Georgia, 977 F. Supp. 1228, 20 Haziran 1997, bkz. <http://www2.bc.edu/~herbeck/cyberlaw/acluvmillier.html> (s.y. 10 Mart 2009); özellikle basın organlarının haber kaynaklarının anonimliğini korumasına ilişkin AIHM'nin şu önemli karara bakılabilir: Goodwin Birleşik Krallığa Karşı, b.n. 17488/90, k.t. 27 Mart 1996. Bu konuda ayrıca bkz. Andrew NICOL, Gavin MILLAR, Andrew SHARLAND, **Media Law and Human Rights**, Oxford University Press, Birleşik Krallık 2001, s. 82-95.

²⁹⁹ Yunanca kökenli bir kelime olan “anonimlik”, isimsiz yada isimsizlik anlamına gelir. Günlük konuşma dilinde kişinin kimliğinin yada onu belirlenebilir kılan bilginin bilinmediği durumu ifade etmek için kullanılır. Bkz. <http://en.wikipedia.org/wiki/Anonymity> (s.y.: 1 Mart 2009). Anonim kayıt yada işlem ise, verinin kendisinden yada başka verilerle birlikte işlem görmesinden veri sahibinin kimliğinin belirlenemediği durumlarda söz konusu olur. Bkz. Roger CLARKE, “Identified, Anonymous, Psedonymous Transactions: The Spectrum of Choise”, 30 Nisan 1999, <http://www.rogerclarke.com/DV/UIPP99.html> (s.y.: 6 Mart 2009). Oya ARASLI, “anonimlik”i Türkçe'ye “tanınmazlık” olarak çevirmiştir. ARASLI'ya göre “tanınmazlık” özel yaşamın gizliliğinin gerçekleştirilebileceği dört durumdan biridir ve Alan WESTIN'a atıfla, “kişinin herhangi bir yabancı ile, onun kendisinin kim olduğunu bilmesine ve çevresinde sürekli olarak kalamayacağına güvenerek, özel yaşam olaylarını paylaşması durumu” olarak tanımlanabilir. Bkz. Oya ARASLI, s. 10-11; Alan WESTIN, s. 30-32.

toplanmamasını ve hareketlerinin izlenmesini istemeyenler için anonimlik oldukça yararlıdır³⁰⁰.

Anonimlik hakkı, özellikle İnternet kullanımının yaygınlaşmasıyla güncellik kazanmış ve tartışılmaya başlanmıştır. Özellikle yeni yeni yaygınlaşmaya başladığı dönemde İnternet ortamında kişilerin kimliklerini gizleyebilmelerinin kolaylığı dolayısıyla görüşlerini ortaya koymada daha özgürce hareket edebilecekleri dile getirilmiştir. Binlerce insan, İnternet’te kendi özel yaşamlarına ilişkin yalnızca kim oldukları bilinmediği takdirde söyleyebilecekleri şeyleri açıklamaktadır.

Bu yargı yalnızca kısmen doğrudur. Nitekim anonimliğin temelde iki çeşidi bulunur. Birincisi ilgilinin kimliğinin ortaya çıkarılma olanağının bulunmadığı tam anlamıyla anonimlik (complete anonymity). İkincisi ise daha çok takma isimlilik (pseudonymity) olarak adlandırılır. Takma isim kullanıldığında, yine kimse gerçek kimliği bilmez ancak farklı iletişimlerin aynı kişi tarafından yapıldığını bilebilir. Her iki çeşidi de siber uzayda sağlayabilmek zordur çünkü pek çok yapı bizi tanımlamaya olanak sunmaktadır. Bu nedenle siber uzayda yüzeysel bir anonimlik kolaydır, ancak gerçek anlamda bunu gerçekleştirebilmek belki de olanaksızdır³⁰¹.

Oysa anonimlik kişisel verilerin korunmasında elverişli bir araçtır³⁰². Gerçekten kişilere ilişkin verilerin anonim olarak tutulmasının bu hak alanı açısından çok çeşitli yararları bulunduğu söylenebilir. Yukarıdaki açıklamalarımızda kişilere ilişkin bilgilerin modern devlet ve diğer modern örgütlenmeler için ne derece önemli olduğuna kısaca değinmiştik. Ancak pek çok alanda bu bilgilerin mutlaka doğrudan somut kişilere bağlı olarak tutulmasına gerek yoktur. Özellikle istatistiksel verilerin yeterli olduğu, planlama gibi amaçlarla yapılan işlemlerde bu açıkça görülebilir. Bu durumda anonimlik bir yandan bu işlerin en iyi şekilde yerine getirilmesini sağlamaya yardımcı olurken, diğer yandan da bireylerin kişisel verilerinin korunması hakkının zarar görmemesini sağlayacaktır. Ayrıca anonimlik hakkı, bir yandan kişisel verilerin korunmasına, bir yandan düşüncüyü açıklama özgürlüğünün

³⁰⁰ Laurie Thomas LEE, “Privacy, Security, and Intellectual Property”, *Understanding the Web, Social, Political, and Economic Dimensions of the Internet*, haz. Alan B. ALBARRAN, David H. GOFF, Iowa State University Press, ABD 2000, s. 143.

³⁰¹ Bruce Schneier, *Secrets and Lies*, s.64; David BRIN, *The Transparent Society (Will Technology Force Us to Choose Between Privacy and Freedom)*, Addison-Wesley, ABD 1998, s. 221.

³⁰² Belirtmek gerekir ki özel yaşamın yanında siyasal açıdan da anonimlik son derece önemlidir. Dünyanın pek çok yerinde siyasal yakınmalar, yaşamsal bir tehdit altına girmeden, ancak bu şekilde yapılabilmektedir.

sağlanmasına destek verir yapısı ile iki hak alanı arasında ortak bir payda da oluşturmaktadır.

Ancak madalyonun bir de diğer yüzü vardır: anonimlik başkalarını tehdit etmek, nefret ifadelerini açığa vurmak, karalamada bulunmak gibi amaçlar için de kullanabilmekte³⁰³, tacizcilerden, teröristlere kadar pek çok suçlu grubu için elverişli bir araç olabilmektedir³⁰⁴. Bu nedenle teknik özellikler dolayısıyla sağlanmasının güçlüğü yanında, doğrudan devletlerin İnternet ortamında anonimliğin ortadan kaldırılması yönünde de girişimlerinin bulunduğu de belirtilmelidir.

4. BİLGİ EDİNME HAKKI VE KİŞİSEL VERİLERİN KORUNMASI

a. Bilgi Edinme Hakkı

Bilgi edinme hakkı en genel şekliyle idarenin tuttuğu bilgilere ulaşabilme hakkı anlamına gelir³⁰⁵ ve normatif temelini düşünceyi açıklama özgürlüğünde bulur³⁰⁶. Bu hak, bireyleri yönetimin etkinlikleri, yetkileri ve kararları konusunda bilgi sahibi yaparak, kamu otoritelerinin denetlenmesini ve kamu hizmetlerinin etkin bir şekilde güvence altına alınmasını sağlamaktadır³⁰⁷. Özellikle idarenin elindeki bilgilerin artması sonucunda, bir denge unsuru olmakta ve idarenin gücüne ve

³⁰³ Bruce Schneier, **Secrets and Lies**, s.63-64; Yaman AKDENİZ, “Anonymous Now”, **Index on Censorship**, Privacy Issue, S.3, Y.2000, s. 57-62, bkz. http://www.cyber-rights.org/documents/index_article.htm (s.y.: 10 Şubat 2009).

³⁰⁴ Laurie Thomas LEE, s. 143.

³⁰⁵ Tekin AKILLIOĞLU, **İnsan Hakları I**, Kavram, Kaynaklar ve Koruma Sistemleri, AÜSBF İnsan Hakları Merkezi Yayınları, No.17, Ankara 1995, s. 185. Bilgi edinme hakkının çeşitli yazarlarca yapılmış değişik tanımları için ayrıca bkz. Cemil KAYA, **İdare Hukukunda Bilgi Edinme Hakkı**, Seçkin, Ankara 2005, s. 41-42. Bilgi edinme, Türk mevzuatında bir “hak” olarak belirlenmişken, bu kavramın genel olarak bir “özgürlük” olarak nitelendiği dikkat çekmektedir. Nitekim kavramın İngilizce karşılığı “freedom of information” ve Almanca karşılığı “*Informationsfreiheit*”dır ve her iki deyim de bilgi/enformasyon özgürlüğü anlamına gelmektedir. Hak ve özgürlük kavramlarını birbirinden kesin çizgilerle ayırmak olanaksızdır. Özgürlüğün de bir hak olduğunu düşünecek olursak bu kavramsal farklılığın uygulama açısından bir ayrışmaya sebep olmadığını söyleyebiliriz. Hak ve özgürlük kavramları arasındaki ilişkinin kısa bir değerlendirmesi için bkz. Ahmet MUMCU, Elif KÜZECİ, **İnsan Hakları ve Kamu Özgürlükleri, Kavramlar, Evrensel ve Ulusal Gelişimleri, Bugünkü Durumları**, Turhan Kitabevi, 4. Baskı, Ankara 2007, s. 14-17.

³⁰⁶ Cavidan SOYKAN, “Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı”, s.3 <http://auhf.ankara.edu.tr/dergiler/auhfd-arsiv/AUHF-2007-56-02/AUHF-2007-56-02-soykan.pdf> (s.y.: 26 Şubat 2009).

³⁰⁷ Bilgi edinme hakkı, bu bağlamda son dönemde önem kazanan e-yönetim ile de yakından ilişkilidir. Bu konuya ilişkin olarak bkz. Herbert BURKERT, “Freedom of Information and Electronic Government”, **Governance and Information Technology, From Electronic Government to Information Government**, haz. Victor MAYER-SCHÖNBERGER, David LAZER, The MIT Press, İngiltere 2007, s. 125-143. Ayrıca bkz. aşağı. Dördüncü Bölüm.

iktidarına sınırlama getirmektedir³⁰⁸. Bu niteliğiyle ilk planda, kişisel verilerin korunması ile amaçları bakımından, en azından belirli bir noktada, paralellik olduğu söylenebilir. Nitekim özel yaşamın gizliliği hakkını da, devlet erkinin bir sınırı olarak algıladığımızda, anlamı insan onurunun korunması ve bu hakka karşı ihlallerin önlenmesinin ötesine geçer ve devletin yapabileceklerinin sınırı anlamına gelir³⁰⁹.

Günümüz demokratik toplumlarında “şeffaf” yönetimin gerçekleştirilmesi önemli bir gerekliliktir³¹⁰. Bunun için ise idarenin eylem ve işlemlerinde “gizlilik” yerine, “açıklık”ı benimsemesi gerekir³¹¹. Şurası açıktır: devletin özel yaşamı yoktur, yalnızca gizlilik isteği vardır. Ayrıca özel yaşamı haklı kılan değerlerle gizliliği haklı kılan değerler de birbirinden farklıdır³¹². İdarenin elindeki bilgilerin gereksiz ve usulsüz biçimde gizlenmesi demokrasinin işlerliği açısından sorun yaratabilecek niteliktedir. Bir başka sorun ise, bilgiyi tekeli altında bulunduranların, bu bilgileri imtiyazlı şekilde kullanma tehlikesidir³¹³.

b. Bilgi Edinme Hakkı ve Kişisel Verilerin Korunması: Bilgi Toplumunun İki Sütunu

Bilgi edinme hakkı ile kişisel verilerin korunması hakkı arasındaki ilişkiyi birkaç açıdan değerlendirmek olanaklıdır. Öncelikle bu yakın ilişkiyi yansıtan fiili bir durumdan söz etmek gerekir. Pek çok devlet, kişisel verilerin korunmasına ilişkin

³⁰⁸ Cemil KAYA, s. 42-44.

³⁰⁹ Lawrence Lessig, **Code Version 0.2**, Basic Books, ABD 2006, s. 213.

³¹⁰ “Şeffaflık”ın çeşitli işlevleri bulunmaktadır. Solove’a göre bunlar dört grupta toplanabilir: (i) devlet yönetiminin etkinliklerini ve işleyişini aydınlatmak; (ii) kamu çalışanları ve kamusal görevler için aday olanlar hakkında bilgi edinmek; (iii) bir malın satımı yada dava açma gibi bazı işlemlerin yapılmasını kolaylaştırmak; (iv) çeşitli gerekçelerle başka bireyler hakkındaki bilgilere ulaşmak. Bkz. Daniel J. SOLOVE, “Access and Aggregation: Public Records, Privacy and the Constitution”, **Minnesota Law Review**, C. 86, Y. 2001-2002, s. 1173 vd.

³¹¹ Mutlak gizlilik olanaklı değildir. Bu nedenle, gizliliği, “belli sayıda kişilere yönelik açıklık” olarak tanımlamak olanaklıdır. Tekin AKILLIOĞLU, “Yönetimde Açıklık-Gizlilik ve Bilgi Alma Hakkı”, s. 3. Eken’e göre, “Gizlilik, yönetimdeki bilgi, belge ve diğer verilerin açıklanmaması anlamındadır. Kapalılık ise, kamu kurum ve kuruluşlarının dıştan gelen her türlü etkiye karşı duyarsız kalmasını, çoğu işlem ve eylemlerinin dıştan görülememesini ve alınan kararların gerekçelerinin açıklanmamasını ifade eder. Kapalılık, yönetimin hizmet yürüttüğü çevre ya da halka karşı duyarsızlığını ifade ettiği halde, gizlilik, hem dış çevreye hem de yönetimin kendi içindeki kişi ve birimlere karşı izlediği bir politikadır. Aslında bunları çoğu zaman birbirinden ayırmak mümkün değildir. Çünkü gizliliği temel politika olarak benimseyen bir yönetim, kendini dışa kapayacak ve içine girilebilirliği güçleştirecektir. Kendini dışa kapayan yönetim ise, gizlilik alanlarını daha da genişletme imkanı elde edecektir”. Musa EKEN, “Kamu Yönetiminde Gizlilik Geleneği ve Açıklık İhtiyacı”, **AİD**, C.27, S.2, Haziran 1994, s.26.

³¹² Andrew CLAPHAM, **Human Rights in the Private Sphere**, Clarendon Press, ABD 1993, s.134.

³¹³ Nuri TORTOP, “İletişim ve Bilgi Edinme Hakkının Önemi”, **AİD**, C.37, S.1, Mart 2004, s. 36.

hukuksal düzenlemeler ile bilgi edinme hakkına ilişkin hukuksal düzenlemeleri birarada kabul etmiştir. Yani bunların hukuk düzenin bir parçası olması çeşitli yerlerde zaman açısından paralellik gösterir³¹⁴. Ayrıca çeşitli devletlerde her iki hakkın sağlanmasını denetleyen bağımsız kurulların aynı çatı altında toplandığı görülür³¹⁵. Burada her iki hak alanının birbirinin bütünleyicisi olduğu ve düzenlemelerin birbirleriyle uyumluluğunda yarar bulunduğu düşüncesi hâkimdir.

Nitekim çeşitli kaynaklarda bu iki hak arasındaki ilişkinin “*bir madalyonun iki yüzü*” ya da “*bilgi toplumu hukukunun iki sütunu*” olarak nitelendiği görülür. Bunlardan birincisi, her iki hakkın birbirini tamamladığına, ikincisi ise her iki hakkın birlikte bilgi toplumunun çatısını oluşturduğunu vurgulamaktadır³¹⁶.

Her iki hak alanı, birbirleriyle yakından ilişkili olmakla birlikte, bu ilişki her zaman birbirlerini destekler şekilde gelişmemektedir. Bu ilginin kendisini birbirine ters orantılı belli başlı iki alanda gösterdiği söylenebilir. Birincisi, kişisel veriler bilgi edinme hakkı çerçevesinde erişilebilecek bir bilgi kategorisini oluşturur. İkincisi ise, kişisel verilerin korunması, bilgi edinme hakkına sınır getirmektedir³¹⁷.

Gerçekten hem bilgi edinme, hem de kişisel verilerin korunması hakları açısından baktığımızda ikisinin birbirini bütünlediğini ve bu şekliyle de bir yandan bireylerin kendileri hakkındaki bilgilere ulaşmasını sağlarken, öte yandan özel yaşamların korunmasına hizmet ettiğini görüyoruz³¹⁸. Ayrıca kişisel veriler, bilgi edinme hakkı kapsamında erişilebilecek bir bilgi kategorisini de oluşturmaktadır. Kişiler kural olarak, bilgi edinme hakkı kapsamında başvuruda bulunarak kendilerine ilişkin idarenin tuttuğu verileri, öğrenebilirler. Ancak bilgi edinme hakkı, yalnızca bilgilere erişime yönelik ilkeler belirlediğinden, daha önceden işlenmiş verilerin varlığı gerekmektedir³¹⁹. Buradan iki sonuç çıkarılabilir.

Birincisi, kişinin idarece kendisine ilişkin tutulan verilere ulaşımında hem bilgi edinme hakkına, hem de kişisel verilerin korunmasına ilişkin düzenlemelerden

³¹⁴ Örneğin Kanada ve Macaristan’da bilgi edinme ile kişisel verilerin korunması haklarına ilişkin yasalar aynı paketin içinde yer almıştır. Bkz. Lee A. BYGRAVE, **Data Protection Law**, s. 122.

³¹⁵ David BANISAR, “Freedom of Information and Access to Government Record Laws Around the World”, **The Freedominfo.org Global Survey**, s.6, http://www.freedominfo.org/documents/global_survey2004.pdf (s.y. 25 Şubat 2009).

³¹⁶ Alexander ROßNAGEL, “Konflikte Zwischen Informationsfreiheit und Datenschutz?”, **MMR**, 2007, Heft 1, s.16.

³¹⁷ Cemil KAYA, s. 89-91.

³¹⁸ Barbara MEREDITH, “Data Protection and Freedom of Information”, **BMJ**, Y.2005, S.330, s. 491, <http://www.bmj.com/cgi/reprint/330/7490/490.pdf> (s.y.: 22 Şubat 2009) (490-491).

³¹⁹ Cemil KAYA, s. 89.

yararlanma olanağı bulunmasıdır. Bu durumu çeşitli hukuksal uyuşmazlıklarda bireylerin her iki hakka birden dayanarak talepte bulunduğu örnekler de ortaya koyar.

İkincisi ise bilgi edinme hakkı yoluyla yalnız daha önceden toplanmış ve/veya işlenmiş bazı kişisel verilere erişimin olanaklı bulunmasıdır. Oysa kişisel verilerin korunması hakkı, verilerin toplanmasına ilişkin ilkeler de getirmekte ve kişileri henüz zarar ortaya çıkmadan koruma altına almaktadır. Bu da iki hak alanı arasındaki kesişimin ne kadar sınırlı olduğunu bir kez daha ortaya koyar.

Bunun yanında şuna da dikkat çekmek gerekir: devletin topladığı verilerin büyük bir bölümü yurttaşın yönetime katılımını sağlamak için son derece önemlidir ve bilgi edinme özgürlüğü kapsamında korunmaktadır. Bu konuda şehir planlamasına, çevre kirliliği ve trafik sorunlarına ilişkin veriler örnek gösterebilir. Ancak bu sorunlara ilişkin bilgilerin kişisel veri niteliği taşımadığı açıktır. Burada kişisel verilerin korunması hakkı ile bilgi edinme hakkı ayrıştığı için aralarında bir çatışmadan söz etmek de olanaklı değildir. Başka bazı alanlarda ise yönetim kişilere ilişkin bilgileri toplamaktadır. Bunlar, yurttaşların ilgileri ile ilişkilendirilebilmesini sağlamaktadır. Ayrıca bütün bilgilerin, her zaman yönetimin esenliğine hizmet etmediğini de belirtmek gerekir³²⁰. Bunların da kişisel veriler kapsamında korunabilmesinin yanında, bilgi edinme özgürlüğünün kapsamına girmedikleri açıktır.

O halde şu saptamada bulunulabilir: bilgi edinme hakkı, bireyin kamusal organların elindeki verilere ulaşmasını sağladığından şeffaf yönetimin gerçekleşmesi açısından oldukça önemlidir. Kişisel verilerin korunması hakkı açısından ise bireyin kendisine ilişkin kamusal organlarca tutulan verilere erişimine yardımcı olur. Ancak kişisel verilerinin korunması kapsamında oldukça sınırlı bir alanı oluşturur³²¹.

Devlet, çok geniş bir kişisel bilgi hazinesine sahiptir. Bu gücün sınırlandırılmaması, özel yaşamın gizliliği hakkının özüne müdahale oluşturur³²². Kamu yönetiminin gizliliğinin sebeplerinden biri de özel yaşamın korunması olarak gösterilebilir. Kamunun elinde sosyal (doğum, ölüm, evlatlık edinme, sabıka, sağlık

³²⁰ Alexander ROßNAGEL, “Konflikte Zwischen Informationsfreiheit und Datenschutz?”, s. 18.

³²¹ Bu konuya ilişkin olarak bkz. aşa. Üçüncü Bölüm.

³²² Tekin AKILLIOĞLU, İnsan Hakları I’den aktaran; Cemil KAYA, **İdare Hukukunda Bilgi Edinme Hakkı**, Seçkin, Ankara 2005, s. 91.

kayıtları vb.), siyasal (seçmen kütükleri gibi) ve ekonomik (banka, sosyal güvenlik, vergi, iflas, malvarlığına ilişkin kayıtları gibi) öze sahip kayıtlar bulunur³²³. Bunların bir kısmının oldukça hassas nitelik gösterdiği ve bireyin isteği dışında, herhangi bir kamusal gereklilik olmaksızın, başkalarının eline geçmesi durumunda ortaya çıkabilecek zararlar da açıktır. Bu bilgilerin başka kişilere aktarılması bireylerin temel hak ve özgürlükleri ile özel yaşamlarına zarar verebileceği gibi, onların bağımsızlığını da zedeleyebilir. Ayrıca işletmelerin ve şirketlerin de üretim tekniklerinin, mali ve ticari bilgi ve stratejilerinin bu kapsamda değerlendirildiği görülmektedir³²⁴.

Herkese verilere ulaşma olanağı tanınırsa, veri öznelerinin verilere ulaşma, onları düzeltme, sildirtme gibi hakları zarar görür. Çünkü ilgili kişinin haberi olmadan verileri başkalarına aktarılabilirse bu kişiler, haklarını kime karşı ileri süreceklerini bilemezler. Ayrıca böylesine bir uygulama verilerin yalnızca belirli bir hedef için kullanılması ilkesine de aykırıdır. Eğer verilere ulaşım hiçbir sınırlamaya tabi tutulmazsa, bunlar her türlü hedef için kullanılabilir. Bireylerin genellikle kendi istekleri dışında ve belirli bir amaç doğrultusunda aktardıkları veriler, idare tarafından başka bir hedefe yönlendirilmemelidir³²⁵.

Son olarak şuna işaret etmek gerekir, tüm bu sorunlar, özellikle İnternet'in yaygınlaşmasıyla kamunun elinde bulunan kayıtların İnternet ortamında yayınlanmaya başlamasıyla daha da önem kazanmıştır. İdarenin elinde bulunan kayıtların çevrimiçi olarak yayınlanmaya başlamasının, bilgilere erişim konusunda sağladığı yararlar açıktır. Ancak bunların içerisinden kişisel veriler çıkarılmazsa, yukarıda işaret edilen sorunlar yanında, kimlik hırsızlığından, meraklı gözlerin hedefi olmaya kadar giden çok çeşitli başka zararların oluşması da söz konusu olabilir³²⁶.

³²³ Roger CLARKE, "Privacy and 'Public Registers'", Adres to the IIR Conference on Data Protection and Privacy, Mayıs 1997, <http://www.rogerclarke.com/DV/PublicRegisters.html> (s.y. 13 Mart 2008). Ayrıca bkz. Robert GELLMAN, "Public Records: Access, Privacy, and Public Policy", Center for Democracy and Technology, 21 Nisan 1995, <http://www.cdt.org/privacy/pubrecs/pubrec.html> (s.y. 20 Şubat 2009); "From Cradle to Grave: Government Records and Privacy", Privacy Rights Clearinghouse, Nisan 2002, <http://www.privacyrights.org/fs/fs11-pub.htm> (s.y.:20 Şubat 2009).

³²⁴ Musa EKEN, "Kamu Yönetiminde Gizlilik Geleneği ve Açıklık İhtiyacı", *AİD*, C.27, S.2, Haziran 1994, s.29-30.

³²⁵ Alexander ROßNAGEL, "Konflikte Zwischen Informationsfreiheit und Datenschutz?", s.18.

³²⁶ İnternet ortamında yer alan kamusal kayıtlar ve bunların karşısında kişisel verilerin korunması hakkının durumunda ilişkin bir değerlendirme için bkz. Sol BERMANN, "Privacy and Access to Public Records in the Information Age", *bepress Legal Series*, Y. 2006, <http://law.bepress.com/expresson/eps/1303> (s.y. 2 Mart 2008), s. 1-24.

Nitekim İnternet üzerinde, aralarında kamunun elinde bulunan kayıtlar da olmak üzere çeşitli kaynaklardan topladıkları kişisel verileri satan pek çok web sitesi bulunmaktadır.

Bu anlamda yönetimde gizliliğin gerekli olduğu alanlardan birinin kişisel veriler olduğunu belirtmek gerekir. Bireylere ilişkin olarak sicil ve disiplin kayıtları, vergiye ilişkin bilgiler, işletmelere ilişkin olarak ticari, ekonomik, sınai nitelikteki bilgiler bu kapsamda değerlendirilmelidir³²⁷. Elbette ki bu gerekçelerden hareketle getirilen sınırlamalarda, bilgi edinme hakkını işlevsiz kılacak bir düzeye ulaşılmamalı, iki hak alanı arasında dengenin korunmasına dikkat edilmelidir.

5. ÖZEL HABERLEŞMENİN GİZLİLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI

Özel haberleşmenin gizliliği³²⁸ ile kişilerin telefon, telgraf, mektup, elektronik posta gibi araçlarla gerçekleştirdikleri özel iletişiminin gizliliğini ve güvenilirliğini korumak hedeflenmektedir. Bu hak, normatif temelini özel yaşamın gizliliği hakkında bulur³²⁹. Özel haberleşmenin gizliliğinde ilke, bireyin dilediği kişilerle dilediği şekilde haberleşmesinin engellenmemesi ve bu haberleşmelerin ilgilinin onayı ya da yasal gereklilikler olmaksızın üçüncü kişilerin müdahalesinden korunmasıdır³³⁰. Nitekim özel yaşamın korunmasına ilişkin AİHS'nin 8. ve EİHB'nin 12. maddelerinde haberleşmenin gizliliği hakkından da söz edildiği görülür. Ancak önemi nedeniyle pek çok ulusal ve uluslararası düzenlemede haberleşmenin gizliliğine ilişkin özel hükümler de getirilmiştir.

³²⁷ Tekin AKILLIOĞLU, “Yönetimde Açıklık-Gizlilik ve Bilgi Alma Hakkı”, **AÜSBFD**, C.46, S.3-4, Haziran-Aralık 1991, s. 1-2.

³²⁸ Özel haberleşmenin gizliliği hakkı, haberleşme özgürlüğü kapsamında yer almaktadır. Ancak çeşitli kaynaklarda haberleşme özgürlüğü, kitlesel iletişim özgürlüğünü nitelemek için kullanılmıştır. Bu bağlamda haberleşme özgürlüğünün, “*haber, düşünce ve kanıların basın, radyo-televizyon, sinema, İnternet gibi kitle haberleşme araçları ile serbestçe alınması ve yayılması*” şeklinde tanımlandığı görülmektedir. Bkz. Kayıhan İÇEL, **Kitle Haberleşme Hukuku, Basın, Radyo-Televizyon, Sinema, İnternet**, 5. Baskı, Beta, İstanbul 2001, s.21 vd. Ayrıca bkz. Feyyaz GÖLCÜKLÜ, **Haberleşme Hukuku, Basın-Radyo-TV**, AÜSBF Yayınları, No.292, Ankara 1970. Herhangi bir kavramsal karışıklığa neden olmamak düşüncesiyle, her ne kadar Anayasamızın 22. maddesinde de haberleşme özgürlüğü özel haberleşmeyi niteleyecek şekilde kullanılmışsa da, burada “*özel haberleşmenin gizliliği*” deyiminin kullanılması tercih edilmiştir.

³²⁹ Feyyaz GÖLCÜKLÜ, Şeref GÖZÜBÜYÜK, **Avrupa İnsan Hakları Sözleşmesi ve Uygulanması**, 3. Baskı, Turhan, Ankara 2002, s. 341.

³³⁰ İbrahim Özden KABOĞLU, **Özgürlükler Hukuku, İnsan Haklarının Hukuksal Yapısı**, 6.Baskı, İmge, Ankara 2002, s. 297.

Hızla gelişen İnternet ve benzeri teknolojiler sayesinde bireyler, yazdıkları metinleri çok daha hızlı, kolay ve ucuz bir şekilde ilgililerine ulaştırabilmekte, her geçen gün biraz daha yaygınlaşan cep telefonları ile sesli ve hatta görüntülü konuşmaları dünyanın önemli bir kesiminden gerçekleştirebilmektedir. Elektronik posta ve telefon hizmetlerinin yaygınlığı neticesinde telgraf ya da geleneksel yazılı posta ile haberleşme her geçen gün biraz daha az başvuru alan yollar olmaktadır³³¹. Günümüzde iletişimin büyük oranda sayısal hale geldiğinin de göstergesidir. Bu ise iletişime müdahalenin artık daha kolay olduğu anlamına gelir. Nitekim geleneksel posta yoluyla gönderilen bir mektubun içeriğine ulaşmak için üzerinde fiziksel bir müdahalede bulunmak gerekirken, e-postada bu hedef dünyanın öbür ucundan gerçekleştirilebilmektedir.

Hukuka aykırı bir şekilde dinleme ya da kaydetme ile kişisel verilerin elde edilmesi hem özel haberleşmenin gizliliğinin, hem de kişisel verilerin korunması hakkının ihlali anlamına gelmektedir. Nitekim, verilerin toplanmasında ve işlenmesinde hukuka uygunluk ve dürüstlük kişisel verilerin korunmasına hakim olan temel ilkelerdendir. Özel haberleşmenin gizliliği, haberleşmenin içeriğinin üçüncü kişilerin (bu, kamusal organlar olabileceği gibi, telefon işletmeleri gibi özel teşebbüsler ya da başka kişiler olabilir) müdahalesinden korumakta, haberleşmenin içeriği ve muhatabını serbestçe belirleme özgürlüğünü desteklemektedir³³². Böylece özel haberleşmenin gizliliği hakkı, kişisel verilerin korunması hakkına da hizmet etmektedir.

Ancak gelişen bilişim teknolojileri, verilerin izlenmesi, toplanması, saklanması maliyetlerinin düşmesi ve kolaylaşması iletişimin içeriğinin dinlenmesi yanında yeni tartışma noktalarının da alevlenmesine neden olmuştur. Gerçekten özel haberleşmenin içeriği yanında, özel iletişime ilişkin çeşitli verilerin tutulması da önemli bir sorun olarak karşımıza çıkmaktadır. Bu noktada iletişimin doğrudan içeriğinin, bir başka ifade ile “ne” konuşulduğunun değil, telefon aramaları ya da posta gönderimleri kayıtlarının, yani “kiminle”, “ne sıklıkla” ve “ne kadar süreyle” konuşulduğunun merkezi önemde olduğu görülür. Bu, temel olarak alınan ve yapılan

³³¹ Hatta artık “el yazısı”nın neredeyse hiç kullanılmadığına ve el yazısı ile birlikte kültürel açıdan da bir kayıp yaşandığı dikkat çekmektedir. Bu konuya ilişkin olarak bkz. Kitty BURNS FLOREY, **Script and Scribble: the Rise and Fall of Handwriting**, Melville House, ABD 2009.

³³² Oğuz ŞİMŞEK, s.149.

telefon aramaları ya da elektronik postalarla, ziyaret edilen web siteleri ile ilişkilidir³³³.

Unutulmaması gerekir ki, çoğu zaman iletişimin şekli ve bu bağlamda iletişim trafiğinin analizi, en az içeriği kadar önemlidir. Örneğin II. Dünya savaşı sırasında Naziler trafik analizini, gözetimindeki kişilerin telefon faturalarını inceleyerek, iletişim halinde bulundukları kişilerin tespiti için kullanmışlardır. Burada asıl ilgilendikleri, ne konuşulduğu değil, kiminle konuşulduğudur. Günümüzde aynı yöntemi yalnızca telefon görüşmeleri için değil, çok daha geniş bir yelpazede gerçekleştirebilmek olanaklıdır. Örneğin kimi çalışmalar, bir kimsenin web trafiğinin analizinin, İnternet üzerinde “*neye*” bakıldığının saptanması için yeterli olduğunu göstermektedir³³⁴. Bu nedenle iletişimin içeriğini gizliliğinin korunması kadar, iletişim trafiğine ilişkin kayıtların gizliliğinin ve güvenliğinin sağlanması da önemlidir. Bu yöndeki ihlaller, yine özel yaşamın gizliliği hakkı ve haberleşme özgürlüğü kapsamında değerlendirilecektir. Kamu otoritesinin, içeriğine bakmadığı gerekçesiyle, keyfi olarak veri trafiğini izleme ve bundan kimi sonuçlar çıkarma hak ve yetkisi olamaz. Nitekim AİHM de bu konunun önemine işaret etmiştir³³⁵.

Görüldüğü gibi, özel haberleşmenin gizliliği, kişisel verilerin korunması hakkı açısından kısmi bir güvence sağlamaktadır ve bu güvence yalnızca iletişimin dinlenmesini değil, izlenmesini de kapsamaktadır.

³³³ Bart CUSTER, “Tapping and Data Retention in Ultrafast Communication Networks”, **Cyberlaw Security & Privacy**, haz. Sylvia Mercado KIERKEGAARD, The Second International Conference on Legal, Security and Privacy Issues in Information Technology (LSPI) 2007, Beijing, Çin, Ankara Barosu Yayınları, 2. Baskı, Ankara 2007, s. 290-291.

³³⁴ Bruce SCHNEIER, s.34; **Constitutional Rights and New Technologies**, s.9.

³³⁵ Kerem ALTIPARMAK, “Büyük Biraderin Gözetiminden Çıkış: Telefonların İzlenmesinde Devletin Sorumluluğu”, s.15, <http://80.251.40.59/politics.ankara.edu.tr/altipar/Yayinlar/Buyuk%20Birader.pdf> (s.y.: 20 Şubat 2009). Bu makaleye ayrıca şu kaynaktan ulaşmak olanaklıdır: TBB Dergisi, Y.2006, S.63, s. 29-66. Ayrıca bkz. AİHM’nin Malone Birleşik Krallığa karşı kararı (b.n.: 8691/79, k.t.: 2 Ağustos 1984). Bu kararda AİHM şu tespitte bulunmuştur: (par.84) “*Hükümetin haklı olarak belirttiği gibi, sayaç denetim yazıcısı, bir telefon hizmet vericisinin kural olarak meşru bir biçimde ve özellikle aboneye doğru ücret tahakkuk ettirebilmek veya hizmete ilişkin şikayetleri veya kötüye kullanma ihtimallerini araştırabilmek için, elde edebileceği bilgiyi kaydetmektedir. O halde niteliği gereği sayaçlama, haklı kılınmadıkça demokratik bir toplumda istenmeyen ve gayri meşru olan iletilerin izlenmesinden ayrı tutulmalıdır. Ne var ki Mahkeme, sayaçlamadan elde edilen verilerin ne şartlarda ve ne amaçlarla kullanılırsa kullanılsın, Sözleşme’nin 8. maddesine göre bir soruna yol açmayacağı görüşünü kabul edemez. Sayaçlama kayıtları, çevrilen numaralar gibi, telefonla yapılan iletişimin bütünleyici bir unsuru olan bilgiyi içermektedir. Sonuç olarak Mahkeme’nin görüşüne göre, abonenin rızası olmaksızın bu bilginin polise verilmesi de, Sözleşme’nin 8. maddesindeki bir hakka müdahaledir*”. Kararın burada kullanılan çevirisi şu kaynaktan alınmıştır: Osman DOĞRU, **İnsan Hakları Avrupa Mahkemesi İçtihatları**, C. 1, Legal, İstanbul 2004, s. 764-779.

6. BİLİM ÖZGÜRLÜĞÜ VE KİŞİSEL VERİLERİN KORUNMASI

Kişisel verilerin korunması hakkı ile yakından ilişkili bir diğer alan bilim özgürlüğüdür. Bilim özgürlüğü pek çok temel metinde güvence altına alınmıştır. EİHB'nin 27. maddesi, bilimsel ilerlemeye katılma hakkını güvence altına almıştır³³⁶. BM Ekonomik, Sosyal ve Kültürel Haklar Şartı'nın 15/3 hükmü devletleri “*bilimsel araştırma ve yaratıcı etkinlikler için vazgeçilmez olan özgürlüğe*” saygıya davet eder³³⁷. ABTHŞ'nin 13. maddesi ise “*Bilimsel araştırma ve sanat, sınırlamaya tabi tutulamaz. Akademik özgürlük gözetilmelidir*” ifadesi ile bu alana koruma getirmiştir. AİHS açısından bilim özgürlüğü kaynağını düşünceyi açıklama özgürlüğüne ilişkin 10. maddede bulur. Alman Anayasası'nın m.5/3 hükmü “*Sanat ve bilim, araştırma ve öğretim serbestir. Öğretim özgürlüğü Anayasaya sadakat borcunu ortadan kaldırmaz*” ifadesini içerir.

Bu hükümler, bir yandan bilim insanlarının (sosyal bilimciler, güncel tarih araştırmacıları, psikologlar, pedagoglar) devletten gelecek müdahalelerden korunmalarını sağlamaktadır, diğer yandan ise devlete bu kimseleri ve araştırmalarını koruma görevini yüklemektedir³³⁸. Örneğin Federal Alman Anayasa Mahkemesi, kendini “*kültür devleti*” olarak tanımlayan bir devletin görevleri arasında özgür bilimsel faaliyetlerin korunması ve desteklenmesinin zorunlu olarak bulunduğunu belirtmiştir³³⁹. Devletin bu görevi, yalnızca araştırma yapanın değil, toplumun da yararınadır. Çünkü bilimsel araştırmalar, toplumun kendisi hakkında bilgi sahibi olmasını sağlar³⁴⁰.

Bilim ve araştırma özgürlüğünün başlıca öğeleri: (i) araştırma özgürlüğü; (ii) araştırma için zorunlu araçlara ve ortama sahip olma hakkı; (iii) bilimsel üretim özgürlüğü ve (iv) bilme hakkıdır³⁴¹. Pek çok bilimsel araştırmada kişisel verilerin kullanılması gerekmektedir. Bu gerekliliğin kişisel verilerin korunmasına müdahale niteliğinde bazı sonuçları olabileceği açıktır. Bu sorunlar, araştırma sırasında veriler

³³⁶ EİHB'nin 27. maddesi şu hükmü içermektedir: “(1) Herkes, toplumun kültürel yaşamına serbestçe katılma, güzel sanatlardan yararlanma, bilimsel gelişmeye katılma ve bundan yararlanma hakkına sahiptir. (2) Herkesin yaratıcı olduğu, bilim, edebiyat ve sanat ürünlerinden doğan maddi ve manevi çıkarlarının korunmasına hakkı vardır”.

³³⁷ İbrahim Özden KABOĞLU, “Bilim ve Sanat Özgürlüğü”, **İnsan Hakları**, YKY, İstanbul 2000, s. 122.

³³⁸ Marie-Theres TINNEFELD ve diğ., s. 602.

³³⁹ BvergGE 35, 79, 114. Marie-Theres TINNEFELD ve diğ., s. 602.

³⁴⁰ BverfGE 47, 327, 368. Marie-Theres TINNEFELD ve diğ., s. 602.

³⁴¹ İbrahim Özden KABOĞLU, “Bilim ve Sanat Özgürlüğü”, s. 122.

toplanırken söz konusu olabileceği gibi, araştırmanın sonuçlanıp yayınlanması aşamasında da söz konusu olabilir. Bu durum araştırma özgürlüğü ile veri koruması arasında bir denge kurulmasını gerektirir.

Kişisel verilerin korunmasına ilişkin ilkeler bilimsel araştırmalar gerçekleştirilirken dikkate alınmalıdır. Nitekim bu ilkeler, araştırmanın yürütülmesi sırasında bazı sınırlamaları beraberinde getirecektir. Bilimsel ilerleme için araştırmada gereken her türlü bilginin kullanılabilmesi elbette oldukça önemlidir. Ancak temel haklar dolayısıyla bazı durumlarda bu alanın sınırlandırılmasını gerekebilir³⁴². Nitekim bilimsel araştırmalarda etik kuralların önemi de bu görüşü desteklemektedir. Kişisel verilerin korunmasına yönelik çeşitli ilkelerin bu kurallar kapsamında yer aldığı dikkatten kaçmamalıdır³⁴³.

Araştırmacı, bilimsel etkinliğini sürdürürken kişisel verilerin korunmasına da önem vermelidir. Bu noktada anonimleştirilmiş veriler bir yarar sağlayabilir. Nitekim daha önce de belirttiğimiz gibi, belirli ya da belirlenebilir bir kişi ile ilişkisi kurulmamış veriler, kişisel verilerin korunmasına yönelik pek çok metnin koruma kapsamı dışında yer alır. Bu nedenle eğer olanaklı ise araştırmanın anonim veriler ile yapılması gerekir.

Ne var ki pek çok araştırmanın anonim veriler ile yapılabilmesi olanaklı değildir. Özellikle tarihsel, tıbbi, kriminolojik, farmakolojik araştırmalarda kişisel verilere de gereksinim duyulur. Pek çok araştırma, aynı kişiler üzerinde uzun süreli gözlemlere dayanılarak yapılır. Çeşitli veri gruplarının birleştirilerek sonuca varılması uzun süreli araştırmaların en belli başlı özelliğidir³⁴⁴. Buna karşılık, kesitsel araştırmalar sırasında kişilerle ilgili veriler, araştırma belli bir noktaya geldiğinde anonimleştirilebilmektedir.

³⁴² Kimyasal silahların geliştirilmesini amaçlayan araştırmaların yasaklanması bilim özgürlüğünün sınırlanabilir yapısına ilişkin bir örnektir. Bunun gibi ırk ayrımcılığı sorunu yaratabilecek araştırmaların yasaklanması da söz konusu olabilir. Bkz. İbrahim Özden KABOĞLU, “Bilim ve Sanat Özgürlüğü”, s. 124. TANÖR’e göre ise “*Bilim ve sanatların toplumsal işlevi, bu alandaki yaratıların mutlak bir özgürlük rejiminden yararlanmalarını gerekli kılar. Çünkü bunlar fikir üretiminin en yüce değer ve biçimleridir. ... Niteliği gereği bilim ve sanat özgürlüğü hiçbir sınırlamaya tabi olmayan ve olmaması gereken mutlak bir özgürlüktür*”. Bkz. Bülent TANÖR, **Türkiye’nin İnsan Hakları Sorunu**, BDS Yayınları, 3. Baskı, İstanbul 1994, s. 90-91.

³⁴³ Avrupa’da Etik Komitelerinin sağlık verilerinin korunmasına ilişkin karar ve uygulamaları için bkz. **Research Ethics Committees, Data Protection and Medical Research in European Countries**, haz. Deryck BEYLEVELD, David TOWNEND, Jessica WRIGHT, Ashgate, İngiltere 2005.

³⁴⁴ Marie-Theres TINNEFELD ve diğ., s. 603.

Özellikle hassas verilerin kullanıldığı alanlarda (örneğin; tıbbi araştırmalarda) araştırmanın gereklilikleri ile veri konusu kişinin bilgilerinin gizli tutulması gerekliliği arasında yaşanacak gerilimden doğan hedef çatışmasına dikkat edilmelidir. Ayrıca bu gibi hassas verilerin yayınlanması (tıbbi araştırmalarda videolarla, kişinin cinsel yaşamına ilişkin görüntüler sergilenmesi gibi) olasılığı, yalnızca verilerin korunmasına ilişkin olarak değil, araştırmanın sağlıklı bir şekilde yürütülebilmesi açısından da sorunlar yaratır. Çünkü kendisine ilişkin son derece özel bilgilerin açıklanmasından çekinen birey, araştırmaya katılma konusunda çekingen olabilir³⁴⁵. Bu, araştırmacının kişisel verilerin korunmasına özen göstermesi gerekliliğinin yalnızca yasal bir zorunluluktan kaynaklanmadığının da göstergesidir. Araştırmaya katılımın sağlanması ve araştırma sırasında ulaşılan bilgilerin doğruluğu açısından gizliliğin sağlanması gerekir.

Kişisel verilerin korunması ile bilim özgürlüğünün bazı noktalarda çatışabileceği konuya ilişkin çeşitli metinlerde de dikkate alınmıştır. AB Kişisel Verilerin Korunması Yönergesi gibi çeşitli metinlerde bu nedenle bilimsel araştırma hedefine yönelmiş veri işlemlere bazı istisnalar getirildiği görülmektedir³⁴⁶. Örneğin, veri koruma hukukunun en önemli ilkelerinden biri olan hedefe sıkı sıkıya bağlılık ilkesinin bilimsel araştırmalarda biraz yumuşatılması söz konusu olabilir. İkincil hedeflere yönelik çalışma, ancak bunlar birincil olarak tespit edilmiş ve hukuka uygun bulunmuş hedef ile bağdaştırılabiliyorsa yapılabilir. Bunun yanında hassas verilerin korunması yönünde de bir olanak tanınmaktadır. Aynı durum, tarihsel, istatistiksel ya da bilimsel hedefler için de söz konusudur. Eğer bu konuda özel bir düzenleme varsa, o zaman bu tür bir düzenleme, araştırmacı için de verimli, sağlam bir bilgi kaynağı haline gelir. Ancak AB Yönergesi'nde, konuya ilişkin ayrıntılı hükümlere yer verilmemiştir. Aksine ulusal yasa koyuculardan veri konusu kişilerin korunması için yerinde ve uygun güvenceler sağlanması talep edilmiştir³⁴⁷.

Sonuç olarak kişisel verilerin korunması, bilimsel araştırmaların önünde bir engel olarak değerlendirilmemelidir. Her iki hak alanı arasında bir dengenin

³⁴⁵ Marie-Theres TINNEFELD ve diğ., 604.

³⁴⁶ Bkz. AB Kişisel Verilerin Korunması Yönergesi, m. 6; 8; 11/2. Özellikle tıbbi araştırmalarda Veri Koruma Yönergesi'nin uygulamasına ilişkin olarak bkz. **Implementation of the Data Protection Directive in Relation to Medical Research in Europe**, Deryck BEYLEVELD, David TOWNEND, Ségolène ROUILLE-MIRZA, Jessica WRIGHT, Ashgate, İngiltere 2005.

³⁴⁷ Marie-Theres TINNEFELD ve diğ., s. 604.

kurulabilmesi olanaklıdır ve bu her somut olayda ayrı bir değerlendirmeyi gerektirir. Ayrıca kişisel verilerin korunması bilimsel araştırmaların sağlıklı bir şekilde sürdürülebilmesi için de bir gerekliliktir.

7. DİĞER BAZI HAK VE ÖZGÜRLÜKLER İLE KİŞİSEL VERİLERİN KORUNMASI HAKKININ İLİŞKİSİ

Yukarıda kimi zaman çatışan, kimi zaman kesişen yönleriyle bazı temel hak ve özgürlüklerin kişisel verilerin korunması hakkı ile ilişkisini değerlendirdik. Bunların yanında kişisel verilerin korunmasının kısmi güvenceler sağladığı ya da kişisel verilerin korunmasına kısmi güvenceler sağlayan başka temel hak ve özgürlük kategorileri de bulunmaktadır.

Özellikle, “*hassas kişisel veriler*” olarak adlandırılan ve özel koruma gerektiren bazı veri türlerinin, kökenleri oldukça eskiye dayanan bazı ilkelerle korunduğu görülmektedir. Hassas kişisel verilerin özel olarak korunmasında hareket noktası, bu verilerin hukuka aykırı ve keyfi bir şekilde toplanmasının, saklanmasının, işlenmesinin ve yayılmasının doğurabileceği zararın daha büyük olduğu düşüncesidir.

Bu noktada ilk akla gelen “*ayrımcılık yasağı*”dır. Kişilerin etnik, dinsel, cinsel yapılarına dayanılarak ayrımcılık yapılamayacağı ilkesi, insan haklarının eksen kavramlarından “*eşitlik*”in bir gereğidir ve bu ilke, pek çok devlette anayasal düzeyde korunmaktadır. Özellikle genetik araştırmaların hız kazanması ve kişilerin genetik yapılarına ilişkin bilgilerin toplandığı gen bankalarının kurulması ile ayrımcılık yasağının yeni bir boyutta tartışılmaya başlandığını da belirtmek gerekir. Nitekim genetik mühendisliğindeki gelişmeler sonucunda, farklı olma hakkı, genetik temelden hareketle ayrımcılık yasağı, genetik kimlik hakkı gibi yeni tartışma alanlarının geliştiği görülmektedir³⁴⁸.

Hassas veriler kapsamında değerlendirilen önemli bir hak kategorisi de kişilerin dinsel inançlarına ilişkin verilerdir. Din ve inanç özgürlüğü, kişisel verilerin korunması hakkının tartışılmaya başlanmasından çok daha eskilere dayanan bir geçmişe sahiptir. Din özgürlüğü, “*inançsızlıkla insanlara önerilenler içinde bir dine katılma arasında tercih serbestliği ve dinin gereklerini bireysel ve toplu uygulama*

³⁴⁸ Lawrence EARLY, s. 802.

serbestliđi” olarak tanımlanabilir³⁴⁹. Din ve inanç özgürlüğünün kapsamında dinini açıklamaya zorlamama da yer alır³⁵⁰. Gerçekten kimsenin dini inanç ve kanaatlerini açıklamaya zorlanamayacağı konuya ilişkin pek çok metinde de belirtilmiştir. Böylece inanç ve kanaate öğrenme biçiminde bile olsa müdahale edilemeyeceđi saptanmıştır³⁵¹. Bu bağlamda din ve inanç özgürlüğü ile kişisel verilerin korunması hakkının birbirinin desteklediđi söylenebilir.

Bunun yanında örneğın sağık verilerinin gizli tutulması, hekimin sır saklama yükümlölüğü hasta-hekim arasındaki ilişkinin bir geređi olarak binlerce yıldır kabul edilen bir gerekliliktir. Hipokrat yemininde de yer alan bu ilke, sağık hizmetlerine ilişkin pek çok ölkedeki yasal düzenlemelere de yansımıştır.

Ancak bu temel hak ve özgürlüklerin kişisel verilerin korunmasına katkısı oldukça sınırlıdır: ayrımcılık yasağı, kişilerin hangi etnik kökene, dinsel gruba dahil olduklarının ya da cinsel tercihlerinin, genetik yapılarının ne olduđunun kayıt altına alınmasını değıl, bu bilgilerden hareketle farklı işlem görmelerini önlemeyi amaçlamaktadır. Sağık verilerine ilişkin hekimlerin ulaştıkları bilgileri gizli tutmaları gerekliliğı de kişisel verilerin korunması hakkı kapsamında yer alan ilkelerin yalnızca birinin güvencesini oluşturur. Bunun gibi din ve inanç özgürlüğünün getirdiğı koruma da bu konudaki verilerin işlenmesi karşısında zayıf kalmaktadır.

Kişisel verilerin korunmasına yönelik yasal düzenlemenin yokluğunda bunlar ve benzeri diğerk ilkeler sınırlı da olsa bir koruma sağlamaktadır. Ancak kişisel verilerin korunması hakkı ile tam bir güvence sağlanabileceğı gibi, bu güvence yukarıda belirtilen diğerk hak ve özgürlüklerin de etkin bir şekilde sağlanmasına hizmet edecektir.

³⁴⁹ İbrahim Ö. KABOĞLU, s. 364

³⁵⁰ Bülent TANÖR, s. 45 vd.

³⁵¹ İbrahim Ö. KABOĞLU, s. 366.

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN GELİŞİMİ VE ULUSLARARASI KAYNAKLARI

I. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUKUKSAL DÜZENLEMELERİN TARİHSEL GELİŞİMİ

A. GENEL OLARAK

Kişisel verilerin paylaşımdan uzak tutulmasına ve korunmasına yönelik bazı ilkelerin uzun zamandan beri kabul edildiğini söyleyebiliriz. Ancak bunlar, özellikle belirli meslek grupları ile bireyler arasındaki güven ilişkisinden kaynaklanmıştır. Bunun en bilinen örneği, M.Ö. 5. yüzyılda gelişen hekimin sır saklama yükümlülüğüdür. Günümüzde de halen geçerliliğini sürdüren ve Hipokrat Yemini'nde¹ yer alan bu ilke hekime, mesleği dolayısıyla elde ettiği bilgileri saklama yükümlülüğü getirmektedir. Hekimler yanında, din adamları, avukatlar, bankacılar gibi başka meslek grupları için de benzer ilkelerin gelişiminin oldukça eskiye dayandığı söylenebilir².

Buna rağmen günümüzde anladığımız şekliyle kişisel verilerin korunması, oldukça yeni bir alandır. Ancak bu kısa sürede kişisel verilerin korunması hukukunun hızla yayıldığı ve geliştiği görülür. Batı Avrupa başta olmak üzere

¹ Hipokrat Yemini'nde sır saklama yükümlülüğü “(g)erek sanatımın icrası sırasında, gerek sanatımın dışında insanlarla münasebette iken etrafımda olup bitenleri, görüp işittiklerimi bir sır olarak saklayacağım ve kimseye açmayacağım” olarak ifade edilmiştir. Hipokrat Yeminin Türkçe çevirisi için bkz. <http://www.ibtf.ibu.edu.tr/idari/and.htm> . Hipokrat Yemini'nin klasik ve modern versiyonları ve konuya ilişkin çeşitli tartışmalar için bkz. Peter TYSON, “The Hippocratic Oath Today”, <http://www.pbs.org/wgbh/nova/doctors/oath.htm> . Ayrıca bkz. “The Hippocratic Oath”, 20 Ağustos 2003, <http://www.bbc.co.uk/dna/h2g2/A1103798> .

² Oğuz ŞİMŞEK, s. 5-7.

dünyanın pek çok bölgesinde kişisel verilerin korunmasına yönelik hukuksal düzenlemeler kabul edilmektedir.

Kişisel verilerin korunması oldukça dinamik bir alandır: ortaya çıkan yeni sorunlar ve yeni gereksinimler, konuya ilişkin yaklaşımlarda ve düzenlemelerin içerik ve kapsamlarında sürekli bir değişimi ve çeşitli tartışmaları da beraberinde getirmektedir. Bu nedenle, kişisel verilerin korunması alanındaki ilk düzenlemeler ile daha sonra kabul edilenler karşılaştırıldığında bazı farklılıkların görülmesi şaşırtıcı değildir.

Her geçen gün hızla gelişen teknoloji dolayısıyla verilerin korunması için aranan çözüm yolları da çeşitlenmekte, konuya ilişkin tartışmalar yeni boyutlar kazanmaktadır. Bu durum, kimi yazarları kişisel verilerin korunması hukukunun gelişimini kuşaklara ayırarak incelemeye yöneltmiştir³. Elbette kişisel verilerin korunması hukuku dünyanın her yerinde aynı düzeyde ve doğrusal bir çizgi üzerinde gelişmemiştir. Ancak gelişimin kuşaklara ayrılarak incelenmesi anlatısal bir kolaylık sağladığı için yararlıdır.

Kişisel verilerin korunmasındaki değişimlerde farklı önceliklerden hareket edilmesi, bu kuşakların sayısının ve başlangıç noktalarının çeşitli yazarlarca farklı değerlendirilmesine neden olmuştur. Ancak hangi ayırım benimsenirse benimsensin, kişisel verilerin korunması hukukunun başlangıcı kaçınılmaz olarak ortaktır: bugün anladığımız şekliyle kişisel verilerin korunmasına yönelik hukuksal düzenlemeler, otomatik veri işleme teknolojilerinin gelişmesi ile, 1960'lı yıllarda tartışılmaya ve 1970'li yıllarda da hukuksal düzenlemelerin konusu olmaya başlamıştır.

B. İLK DÜZENLEMELER

1950'li ve 1960'lı yıllar şaşırtıcı olanaklar sunan bilgisayarların ortaya çıktığı, hızla geliştiği ve yaygınlaşmaya başladığı bir dönemdir. Ancak bu araçların kullanımının yaygınlaşması bazı sorunları da beraberinde getirmiştir. Bu bağlamda

³ Örneğin bkz. Alessandra Di MARTINO, **Datenschutz im europäischen Recht**, Nomos, Baden-Baden 2005, s. 17-20; András JÓRI, “dataprotection.eu”, <http://www.dataprotection.eu/> ; Viktor MAYER-SCHÖNBERGER, “Generational Development of Data Protection in Europe”, **Technology and Privacy: The New Landscape**, haz. Philip E. AGRE, Marc ROTENBERG, MIT Press, ABD 1998, s. 219-242. Viktor MAYER-SCHÖNBERGER, Ernst O. BRANDL, **Datenschutzgesetz, Grundsätze und europarechtliche Rahmenbedingungen Gesetzestext mit Materialien, Datenschutz-Verordnungen und Richtlinien im Anhang**, 2. Baskı, Avusturya 2006, s.12-13.

kişisel verilerin kaydı konusundaki yeni gelişmelere, hem toplumsal, hem akademik düzeyde temel hak ve özgürlükler açısından şüpheyile yaklaşmıştır. Birinci bölümde açıklamaya çalıştığımız gerekçelerden hareketle başta özel yaşamın gizliliği hakkının ciddi bir tehlike altında olduğu düşünülmüştür⁴. Özellikle batı toplumlarında görülen bu endişe, devletlerin kişisel verileri kötüye kullanma olasılığında yoğunlaşır. II. Dünya Savaşı'nın dehşet günlerinin anıları henüz çok tazedir ve Avrupa yurttışı sınırsız devlet gözetiminin, denetiminin ne gibi sonuçları olabileceğini yakından bilmektedir. Şimdi yeni gelişen bilgisayar teknolojisi potansiyel sorunu daha da ciddi bir noktaya taşımaktadır.

Bu atmosferin izlerini kişisel verilerin korunmasına ilişkin ilk çalışmalarda bulmak olanaklıdır. Bu çalışmalarda toplumun hızla gelişen bilgisayar merkezli yapısına ve bu yapının da “*kişisel veri*” olarak adlandırılan bilgilere dayandığı vurgulanır⁵. Bunun doğal bir sonucu olarak, 1970’li yıllarda hazırlanan ilk hukuksal metinlerde hareket noktası, yeni bir olgu olarak karşılaşılan bilgisayarların kullanılmasından dolayı bireyler açısından ortaya çıkabilecek sorunlara çözüm bulmaktır⁶.

Bu dönemde çeşitli devlet organları ve işletmeler ellerindeki bilgileri merkezi bir veri tabanında birleştirmeye yönelik ciddi hazırlıklar içindedir. İşte kimi yazarların birinci kuşak veri koruma yasaları olarak niteledikleri düzenlemelerin ortaya çıkışında bu düşünceye karşı oluşan tepki etkilidir⁷. Verilerin insan eliyle işlenmesinden otomatik işlemeye geçişin yeni ve ciddi riskler ortaya çıkaracağı düşünülmektedir. Devletin, çeşitli kaynaklardan elde ettiği bilgileri ilişkilendirerek bireylerin karşısında aşırı güçlenmesi tehlikesi fark edildiğinden, yasaları hazırlayanların, yeni teknolojilerin getirdiği bu olanakların kullanımını denetlenebilir ve şeffaf kılmaya özel bir dikkat göstermeleri gerektiği düşüncesi gelişmiştir⁸.

Verilerin korumasına ilişkin ilk yasal düzenleme, 1970 yılında Almanya’nın Hessen eyaletinde yapılmıştır. Bu yasanın kabulüne neden olan en önemli dinamik,

⁴ Daniel J. SOLOVE, **The Dijital Person**, s. 15.

⁵ **The Dimensions of Privacy, A National Opinion Research Survey of Attitudes Toward Privacy**, (Araştırma Louis Harris and Associates Inc. İle Dr. Alan F. Westin yönetiminde yürütülmüştür), Garland Publishing, ABD 1981, s.3.

⁶ **New Technologies: A Challenge to Privacy Protection?**, (Study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European on Legal Co-Operation (CDCJ), Fransa 1989, s. 5.

⁷ Viktor MAYER-SCHÖNBERGER, Ernst O. BRANDL, s. 12.

⁸ András JÖRI, “dataprotection.eu”, <http://www.dataprotection.eu/>.

“Hessen Planı” olarak adlandırılan bir program içerisinde 1960’lı yılların sonunda federe düzeyde merkezi bir veri bankasının kurulma tasarısıdır. Verilerin korunmasına ilişkin hükümlerin yasalaşmasında bu veri bankasının özel yaşamın gizliliği hakkı üzerindeki olası sonuçlarının etkili olduğu söylenebilir⁹.

Yükselen tartışmalar ve Hessen eyaletinin verilerin korunmasına ilişkin yaptığı düzenleme, kısa süre sonra Almanya’da federal düzeyde de bir koruma öngörülmesini de sağlamıştır. Bu doğrultuda 1977 yılında Federal Almanya Veri Koruma Yasası kabul edilir. Ancak bu yasa, verilerin korunması görevini, aynı zamanda milli istihbarat ve polis teşkilatından da sorumlu olan İçişleri Bakanlığına bırakması nedeniyle oldukça eleştirilmiştir¹⁰.

Almanya’nın Hessen eyaletinde kabul edilen bu yasadan sonra, ilk ulusal düzenleme 1973 yılında İsveç’te yapılır¹¹. İsveç’te veri koruması yasasının kabul edilmesine neden olan tartışmalar, Almanya’dakine benzerdir. Bu dönemde hızla ilerleyen teknolojinin bir parçası olan otomatik veri işleme sistemleri, özellikle Batı Avrupa’da yaygınlaşmıştır. Ancak sorunun İsveç’te bundan önce tartışılmaya başlandığı da belirtilmelidir.

1947 yılında İsveç’te her yurttaşa, cinsiyet ve doğum tarihi bilgilerini içeren, on haneli bir kimlik numarasının verilmesini sağlayan bir sistem oluşturulmuştur. Böylesine bir sistemin çeşitli yararları bulunmakla birlikte, verilerin korunmasının bir sorun olarak gündeme gelmesinde de önemli etkisi bulunur¹². 1960’lı yılların ortalarına gelindiğinde ise, İsveç’te nüfus kütüğüne ilişkin bilgilerin bulunduğu bir nüfus sicili ve ayrıca bir vergi sicili oluşturmak için çalışmalar başlar. Bu kapsamda verilerin kaydedileceği ortak bir veri bankasının oluşturulması temel hedeflerden biridir¹³.

⁹ Colin J. BENNETT, **Regulating Privacy**, s. 48. Bu dönem Almanya’da, devlet organlarınca çeşitli amaçlar doğrultusunda, bilgisayar sistemlerinin artan oranda kullanılmaya başlandığı görülür. Bunun en bilinen ve en çok tartışılmış örneklerinden biri, Bavyera eyalet yönetiminin, 1972 yılında Münih’te yapılan olimpiyatlar için kurmuş olduğu bilgisayar sistemini, daha sonra merkezi Bavyera bilgi sistemi olarak kullanmak istemesidir. Viktor MAYER-SCHÖNBERGER, s. 222.

¹⁰ Christian FRIEDRICH, “Fundamentals of Privacy”, Datenschutzaspekte im Umfeld des Pervasive Computing, Prof. H.-U. HEISS, Prof. B. LUTTERBECK, Yaz 2004, <http://ig.cs.tu-berlin.de/lehre/s2004/pvc/ablauf/01/Friedrich-PrivacyBackgroundtext-2004-07-21.pdf> s.15.

¹¹ 1973 İsveç Veri Yasası’nın (1 Ocak 1989’da yürürlüğe giren değişikliklerin işlendiği) metninin İngilizce çevirisine şu kaynaktan ulaşılabilir: <http://archive.bild.net/dataprSw.htm> .

¹² Colin J. BENNETT, **Regulating Privacy**, s. 49-50.

¹³ Oğuz ŞİMŞEK, s. 8-9; Viktor MAYER-SCHÖNBERGER, s. 222.

İsveç ve Almanya konuya ilişkin ilk örnekleri oluşturur. Ancak aynı dönemde, kişisel verilerin korunması, başka Avrupa ülkelerinde de tartışma konusu olmuş; Hessen ve İsveç veri koruma yasalarından kısa bir süre sonra, kişisel verilerin korunmasına ilişkin yasal düzenlemeler Avrupa’da pek çok ülkede kabul edilmiştir. Nitekim 1980 yılına gelindiğinde İrlanda, İtalya ve İngiltere dışında, Avrupa Ekonomik Topluluğu’nun bütün üyelerinin ya bu konuda düzenleme yaptıkları, ya da ciddi hazırlıklar içinde bulundukları görülür¹⁴.

Bu gelişim, kişisel verilerin korunması hukukunun anavatanının Batı Avrupa olduğunu açıkça ortaya koymaktadır. Ancak şunu da belirtmek gerekir: 1970’li yıllarda yalnızca Avrupa’da değil, ABD’de de kişisel verilerin korunması yönünde bazı girişimler bulunur. 1970 yılında ABD Kongresi, bireylere kendilerine ilişkin kredi raporlarını görme ve yanlış bilgileri çıkartma hakkı veren, Adil Kredi Raporlama Yasasını (Fair Credit Reporting Act) kabul etmiştir¹⁵. Dönemin Sağlık, Eğitim ve Sosyal Yardım Bakanı Eliot Richardson ise 1972 yılında bilgisayarların özel yaşamın gizliliği hakkı üzerindeki etkilerini araştıran bir komisyon kurmuş ve bu komisyon 1973 yılında Kongre’ye bir rapor sunmuştur¹⁶. Ancak Raporun etkisi ABD’den çok Avrupa’da görülür. Avrupa’da pek çok devlet bu temel ilkelere

¹⁴ Andrew CHARLESWORTH, “The Governance of the Internet in Europe”, **The Internet, Law and Society**, haz. Yaman AKDENİZ, Clive WALKER, David WALL, Pearson Education Limited, İngiltere 2000, s.63.

¹⁵ ABD’de federal düzeyde kabul edilen bir yasa olan Adil Kredi Raporlama Yasası (15 U.S.C. § 1681), müşteri kredi bilgilerinin toplanmasını, yayınlanmasını ve kullanılmasını düzenlemektedir. Yasada öncelikle, kredi raporlarının hangi hallerde meşru bir biçimde kullanılabileceği belirlenmektedir. Mahkeme emri, bilginin doğrudan rapora konu olan kişiden edinilmesi ve çeşitli “meşru ticari gereklilikler” bu kapsamda sayılabilir. Ayrıca yasa ile burada belirlenen meşru amaçlar bulunmaksızın “bilgi simsarlarının” (information brokers) kredi bilgilerini açıklamaları da yasaklanmaktadır. Bundan başka raporda bir bilgi dolayısıyla tüketici ile ihtilafa düğüldüğünde kredi acenteleri ve kurumlarının diğerlerini bilgilendirmesi gerektiği yer almıştır. Adil Kredi Raporlama Yasası’nı, Adil Kredi Faturalandırma Yasası (Fair Credit Billing Act, 1975, 15 U.S.C. § 1666), Adil Borç Toplama Uygulamaları Yasası (Fair Debt Collection Practices Act, 1977, 15 U.S.C. § 1692-1692) izlemiştir. Bkz. Harry HENDERSON, s. 52-53. Bu yasaların tam metinlerine İnternet üzerinden <http://www.ftc.gov> adresinden ulaşılabilir.

¹⁶ Richardson Raporu’nun en önemli katkısı, “bilgisayar çağının haklar bildirgesi” olarak nitelendirilebilecek beş ilkeyi saptamış olmasıdır. “Adil Enformasyon Uygulama Kuralları” (Code of Fair Information Practices) olarak adlandırılan bu ilkelere göre: 1. Mevcudiyeti gizli olan bir kişisel veri saklama sistemi olmamalıdır. 2. Kişilerin kendileri hakkında hangi bilgilerin kayıt altına alındığını ve bunların nasıl kullanıldığını öğrenme olanağı bulunmalıdır. 3. Kişilerin kendileri hakkında belirli bir amaç için toplanmış verilerin, rızaları olmaksızın başka amaçlar için kullanılmasını önleme hakları olmalıdır. 4. Kişilerin kendileri hakkındaki belirlenebilir bilgilerin kayıtlarını düzeltme ya da değiştirme olanakları bulunmalıdır. 5. Belirlenebilir kişisel verilerin kayıtlarını oluşturan, muhafaza eden, kullanan ya da yayınlayan herhangi bir kuruluş, verilerin kendilerinin hedefleri için kullanımındaki güvenliği sağlamak ve verilerin kötüye kullanımını önleyecek tedbirleri almak zorundadır. Simson GARFINKEL, **Database Nation, The Death of Privacy in the 21st Century**, O’Reilly, ABD 2000, s. 7.

dayanan yasalar çıkarırken, ABD’de, 1974’te kabul edilen Özel Yaşamın Gizliliği Yasası’nın sınırlı uygulama alanı bir yana bırakılırsa¹⁷, kurumsallaşmış bir veri koruma düşüncesi uygulamaya geçememiştir¹⁸.

Bu dönemde kabul edilen veri koruma düzenlemelerinin bazı ortak özellikleri saptanabilir. Öncelikle, yukarıdaki örneklerde de görüldüğü gibi bu dönemde özellikle devletin elindeki merkezi ve geniş kapsamlı veri bankalarına karşı gelişen bir tepki söz konusudur. Hemen belirtmek gerekir: bu veri bankalarının kurulmasına yönelik girişimler genelde başarılı olamamıştır¹⁹. Ancak bu tepkinin dönemin veri koruma yasalarının niteliklerinde önemli bir etkisi bulunduğu açıktır: bu yasalarda başta devletin elinde bulunanlar olmak üzere, geniş veri bankalarının şeffaflaşması temel amaçtır.

Bunun yanında 1970’li yılların başlarında yapılan düzenlemelerde verilerin yok edilmesi gibi, bugün kişisel verilerin korunmasında temel ilkeler arasında sayılan bazı haklara yer verilmemiştir. Ancak yine bugün temel ilkeler arasında kabul edilen verilere ulaşma ve onları düzeltme hakkı güvence altına alınmıştır. Kişisel verilerin toplandığı veri bankalarının kayıt altına alınması yükümlülüğünün de bu dönemde kabul edildiği görülür.

Yasa koyucu 1970’li yıllarda özel olarak bilgisayarlarla işlenmiş verilerin korunmasını hedef almıştır. Ayrıca bazı yasalar ile yasama organına, kamu yönetiminin elde edebildiği verilere ulaşma hakkı verilmiştir. Bu durum, birinci kuşak yasaların kişisel verilerin korunmasından çok “*enformasyonel güçler ayrımı*” oluşturma düşüncesinden kaynaklandığı iddiasını güçlendirmektedir. Çünkü bu şekilde yönetimin elindeki enformasyon gücü, devlet ve toplum arasında dağıtılmaktadır²⁰.

¹⁷ 1974 Özel Yaşamın Gizliliği Yasası (The Privacy Act of 1974, 5 U.S.C. § 552a) ile Richardson Raporu’nda yer alan ilkeler uygulamaya geçirilmeye çalışılmıştır. Bu yasada federal kurumlarda bulunan kişisel verilerin toplanması, kullanılması ve yayılmasına ilişkin bazı ilkeler belirlenmiştir. Ancak yasada yer alan çeşitli istisnalar bu hükümlerin etkili bir şekilde uygulanmasına engel oluşturacak niteliktedir. Özellikle kurumların görevleri dolayısıyla kişisel verileri “*rutin kullanım*”larının istisnalar arasında sayılması, özel yaşamın korunmasında önemli bir gedik açtığı için eleştirilmiştir. Bkz. Harry HENDERSON, s. 59-60.

¹⁸ Simson GARFINKEL, “Privacy and the New Technology”, s.13. Federal Almanya Cumhuriyeti, İsviçre, Fransa, Kanada ve ABD’de kişisel verilerin korunması hukukunda ilk düzenlemelerine ilişkin ayrıntılı bir değerlendirme için bkz. David H. FLAHERTY, **Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States**, The University of North Carolina Press, ABD 1992.

¹⁹ Viktor MAYER-SCHÖNBERGER, s. 223.

²⁰ András JÖRI, “dataprotection.eu”, <http://www.dataprotection.eu/>.

Birinci kuşak, veri koruma yasaları daha çok devletlerde görülen aşırı güç yoğunlaşması karşısında dengeyi sağlama amacını güder. Hatta öyle ki ilk düzenlemelerde özel yaşamın gizliliği gibi önemli bir değerin vurgulandığı, yalnızca veri bankalarındaki bilgilerin düzenlenmesinin hedeflendiği görülür²¹.

C. İNSAN HAKLARI KAPSAMINDA KİŞİSEL VERİLERİN KORUNMASI

Kişisel verilerin korunmasına yönelik olarak kabul edilen ilk yasalarda öngörülemeyen önemli bir gelişim, bilgisayarların yaygınlaşması ve devletin elinde bulunan merkezi veri bankalarının yanında, kamu ve özel sektörde pek çok veri bankasının kurulmasıdır. Bunun sonucunda bireyin kendisiyle ilgili bilgilerin toplanması ve işlenmesinin yaratacağı tehlikeleri açıkça ve doğrudan hissetmesi, yalnızca belirli bir veri işleme sürecinin düzenleme kapsamına alınmasının ötesinde veri koruma hakları talep etmesine neden olur²². Bu talep, kişisel verilerin korunmasında yeni bir dönemin de habercisidir: artık özel yaşamın gizliliği daha çok vurgulanmakta ve konu insan hakları ekseninde tartışılmaktadır. Ayrıca kişisel verilerin korunmasının yurttaşların hakları arasındaki yeri de belirginleşmektedir. Nitekim Portekiz, İspanya, Avusturya gibi ülkelerde kişisel verilerin korunması bu dönemde anayasal bir hak olarak tanınmıştır.

1976 tarihli Portekiz Anayasası, bu topraklara demokrasinin tekrar gelişinin müjdecisidir. Yeni anayasada kişisel verilerin korunması hakkının tanınması, 1974 yılında yeni düzenin kurulmasının ve otoriter devlet yapısından uzaklaşmanın belirtilerinden biri olarak değerlendirilebilir²³. 1976 Portekiz Anayasasının 35. maddesi kapsamında kamusal güçlerin veri işleme şekillerine anayasal sınırlamalar getirilmiştir²⁴. Bireylerin özel yaşamına müdahale teşkil edebilecek uygulamalara ihtiyatla yaklaşılmaktadır. Bunda şüphesiz otoriter yönetim altında sürekli izlenen bireylerin geçirdikleri travmanın da etkisi vardır. “*Bir daha yaşanmama*” isteği pek çok hak ve özgürlükte olduğu gibi kişisel verilerin korunmasında da etkili olmuştur.

²¹ Viktor MAYER-SCHÖNBERGER, s. 224.

²² A.g.e., s. 225.

²³ Aşağıda görüleceği üzere benzer bir durum, daha ileri bir tarihte çeşitli Latin Amerika ülkelerinde de, otoriter rejimlerin yıkılmasının ardından yapılan yeni anayasalarda görülecektir.

²⁴ 2 Nisan 1976 tarihli Portekiz Anayasası’nın İngilizce çevirisi için bkz. http://www.servat.unibe.ch/icl/po00000_.html . Anayasa’da, çeşitli tarihlerde kapsamlı değişiklikler yapılmıştır. Portekiz Anayasası’nın güncel metninin İngilizce çevirisi için bkz. http://www.portugal.gov.pt/Portal/EN/Portugal/Sistema_Politico/Constituicao/ .

Bu durum, Portekiz’le benzer bir süreci yaşamış İspanya’nın yeni Anayasası’nda da görülür. İspanya Anayasası’nın 18/4 hükmü uyarınca, yurttaşların onuru, kişisel ve ailevi mahremiyetleri ile haklarını tam anlamıyla kullanımlarını güvence altına almak için kişisel verilerin işlenmesi yasa ile sınırlanacaktır²⁵.

Kişisel verilerin korunmasının anayasal düzeyde tanınması olgusunun yalnızca demokrasi özlemi içerisindeki ülkelerde görülmediği de belirtilmelidir. Avusturya, Macaristan ve İsveç gibi demokratik ülkelerde de benzer düzenlemeler yapılmıştır. Bu yaklaşım birkaç açıdan önemlidir: Kişisel verilerin korunmasına anayasal düzeyde yer verilmesinin yanında, bu gelişmeler, kaynağını özel yaşamın gizliliğinde bulan kişisel verilerin korunmasının artık bağımsız bir hak olarak yükselmeye başladığının da işaretidir²⁶.

Artık tehlike yalnızca “büyük birader” değildir, dağınık ve çok merkezlidir. Bu durumda bireyler için en iyi koruma yolu da bireysel haklara ağırlık vermek olacaktır. Bu dönemde yapılan hukuksal düzenlemeler genel olarak öncekilere benzer. Ancak özünde önemli bir farklılık taşıyarak: artık kişisel verilerin korunmasına teknoloji merkezli bakış terk edilmeye başlanmıştır. Düzenlemelerde daha az teknik terim kullanılması da bunun bir göstergesidir²⁷.

Bireylerin kendilerine ilişkin bilgilere ulaşma ve eğer bu bilgiler yanlışsa onları düzeltme hakkı, konuya ilişkin ilk düzenlemelerde de tanınmıştır. Ancak o dönemde bu, daha çok merkezi veri bankalarında tutulan verilerin doğruluğunu sağlamaya yöneliktir ve birey kendisi hakkında hangi verilerin işleneceğine karar verememektedir. Artık bireylerin işleme sürecinde de ileri sürebilecekleri bazı hakları vardır²⁸. Bu dönemde kişisel verilerin korunması açısından bireyin mücadelesine ağırlık verilmiştir. Bu bağlamda, verilerin denetimi, ilgilinin kendisi tarafından gerçekleştirilecek subjektif bir savunma hakkı olarak görülmüştür²⁹.

İspanya Anayasası metninin İngilizce çevirisi için bkz. http://www.senado.es/constitu_i/index.html.

²⁶ Lawrence EARLY, “Science, Technology and Human Rights: The Role of Data Protection”, s. 809-810.

²⁷ Viktor MAYER-SCHÖNBERGER, s. 226.

²⁸ Örneğin Norveç Veri Koruma Yasası’nın 7. ve 33. maddeleri uyarınca, bireyler, doğrudan pazarlama ve pazar araştırması amaçlarıyla verilerinin işlenmesine itiraz edebilirler. Danimarka veri koruma hükümleri de bireylere, kendileri hakkındaki bilgilerin devlet bankalarından özel bankalara aktarılması gibi çeşitli konularda karar verme hakkı tanımaktadır. Viktor MAYER-SCHÖNBERGER, s. 226-227.

²⁹ Oğuz ŞİMŞEK, s. 9.

D. BİLGİLERİN GELECEĞİNİ BELİRLEME HAKKI

Kısa süre içerisinde kişisel verilere yönelik saldırıların yalnız önlenmesiyle yeterli koruma sağlanmadığı anlaşılmıştır. Bu, kişisel verilerin korunmasına yönelik düzenlemelerde bazı değişiklikler yapılması gereksinimi ortaya çıkarır. Bunda 1983 yılında Alman Anayasa Mahkemesi'nin Nüfus Sayımı Kararındaki saptamaları da etkili olmuştur³⁰. Karar, hem Almanya'da hem dışında büyük yankı uyandırır. Artık kişisel verilerin korunması, bireyin veri işleme sürecinin her aşamasına katıldığı "*bilgilerin geleceğini belirleme hakkı*" olarak anlaşılmaya başlanmıştır. Kararda ortaya konan felsefenin etkisi, Avusturya Verilerin Korunması Yasası'na 1986 yılında eklenen hükümlerde, Norveç, Finlandiya, Hollanda ve Macaristan'da yapılan düzenlemelerde görülebilir³¹.

Bu dönemde bilişim teknolojilerinde, yalnızca merkezi veri işleme modellerinin ötesine geçen gelişimlerin görülmesi de bireylerin sürece aktif bir şekilde katıldığı düzenlemelerin yapılmasında etkilidir. Bu gelişmeler birbirine eskisinden çok daha etkin bir şekilde bağlanmış bir toplum yapısını ortaya çıkarır. Bu ortamda artık bireylerin veri işleme süreçlerinin dışında kalma şansı bulunmamaktadır. O halde kişi, verilerinin paylaşılması yoluyla sosyal ilişkilere nasıl katılacağını belirleyebilmelidir. Yasa koyucular kişilerin üzerine düşen sorumluluğu vurgulamaya devam etseler de bu gelişmeler onların veri imgelerini denetleyebilmeleri için bireysel hakların bağlayıcı ve açık olmasının zorunluluğunu fark etmelerini sağlar.

1980'li yıllardaki bir diğer önemli gelişim, kişisel verilerin korunmasının uluslararası alanda da çözüm aranan bir konu haline gelmesidir. Aslında bu husus, bir süredir tartışılmaktadır. Nitekim her geçen gün sanal ve gerçek iletişim ağları ile birbirine biraz daha sıkı bağlanan bir dünyada, bilginin hızlı akışı sınır tanımaz bir niteliktedir. Etkin bir koruma ancak küresel düzeyde bir veri koruma sisteminin kabulü ile olanaklıdır.

Bu düşünceden hareketle BM, OECD, AK gibi etkili uluslararası kuruluşlar bir süredir gündemlerinde olan kişisel verilerin korunmasına ve özellikle kişisel verilerin uluslararası aktarımına ilişkin kurallar belirleme düşüncelerini ard arda

³⁰ BVerfGE, 65, 1-Volkszählung.

³¹ András JÓRI, "dataprotection.eu", <http://www.dataprotection.eu/> .

yaşama geçirmişlerdir. Bu bağlamda kişisel verilerin korunması, artık ulusal sınırları aşmış ve etki düzeyleri birbirinden farklı çeşitli uluslararası metinlerin konusu olmaya başlamıştır.

1980’li yılların sonlarında Orta ve Güney Amerika ülkelerinde konuya ilişkin ilginç bir gelişim daha yaşanır. Alman Anayasa Mahkemesi’nin geliştirdiği “*bilgilerin geleceğini belirleme hakkı*” ve AK’nin 1981 tarihli Veri Koruma Sözleşmesi bazı Latin Amerika ülkelerinde, konuya ilişkin düzenlemeler yapılmasını sağlamıştır³². Bu bağlamda Latin Amerika ülkelerinde, başka bölgelerde görülmeyen bir yöntemle: “*Habeas data*” hakkının tanınmasıyla kişisel verilerin korunması yolu seçilmiştir³³.

Latince bir kelime olan Habeas Data Türkçe’ye “*veriye sahip olmalısın*” şeklinde çevrilebilir. Habeas Data hakkı, ilk olarak 1988 Brezilya Anayasa’sında yer almıştır. Brezilya’nın yeni anayasasında böylesine bir hakka yer vermesini geniş bir çerçevede değerlendirmek gerekir. Gerçekten 1980’li yılların sonu ve 1990’lı yılların başı, Latin Amerika ülkeleri için, askeri diktatörlüklerin ve soğuk savaşın sona erip, yeni demokrasilerin kurulduğu bir dönemdir. Bu nedenle Anayasalarda temel hak ve özgürlükler güçlü bir şekilde vurgulanmaktadır. Bu dönemin bir ürünü olan Brezilya Anayasası’nda da daha önce görülmeyen yeni bir hakka yer verilmiştir: Habeas data bireysel şikayeti³⁴.

Uygulamada ülkeler arasında bazı farklılıklar bulunsa da genel olarak “*Habeas data*”, kişinin mahkemeye vereceği bir şikayet dilekçesi ile görüntüsünün, özel yaşamının, şerefının, kişisel bilgilerinin geleceğini belirleme ve bilgiye erişme haklarının korunmasını sağlamak için tasarlanmıştır³⁵. Kişisel verilerin korunmasına yönelik, Avrupa ve ABD sistemlerinden ayrılan bu yaklaşım şekli kısa zamanda başka Latin Amerika ülkelerine de yayılmıştır³⁶.

³² Andrés GUADAMUZ, “Habeas Data vs. European Data Protection Directive”, **Journal of Information Law and Technology**, Y. 2001, S.3, s.3, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/guadamuz (s.y. 20 Nisan 2009). (s.1-19)

³³ Cemil KAYA, s. 98-99.

³⁴ Andrés GUADAMUZ, “Habeas Data vs. European Data Protection Directive”, **Journal of Information Law and Technology**, Y. 2001, S.3, s. 4, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/guadamuz (s.y. 20 Nisan 2009). Bkz. 1988 Brezilya Anayasası m.5/LXXI.

³⁵ Andrés GUADAMUZ, s. 5.

³⁶ Paraguay 1992’de, Peru 1993’te, Arjantin 1994’te, Ekvator 1996’da, Kolombiya 1997’de anayasalarında kişisel verilerin korunması yöntemi olarak Habeas data bireysel şikayetini

Genel olarak Habeas data dilekçesi, hem kamu hem de özel sektörde, verileri otomatik ya da elle işleyenler hakkında verilebilir. Bu dilekçe kapsamında kişinin, kendisine ilişkin bilgilere ulaşma³⁷, onların düzeltilmesini, güncellenmesini ve ortadan kaldırılmasını isteme hakkı bulunmaktadır. Bu hak, çekişmesiz yargı konusu olur ve bireyin kişiliğine bağlı olduğundan, yalnızca kendisi tarafından kullanılabilir. Bu bakımdan mahkemenin resen inceleme başlatması olanaklı değildir³⁸. Bu niteliği ile habeas data bireysel şikayetin, bilgilerin geleceğini belirleme hakkının özündeki düşünceden etkilendiği açıkça görülmektedir.

E. YENİ GELİŞMELER KARŞISINDA KİŞİSEL VERİLERİN KORUNMASINI ETKİN BİR ŞEKİLDE SAĞLAMA ÇALIŞMALARI

Yasa koyucuların, bireylerin haklarını kullanırken zayıf konumlarını fark etmeleri, bu sorunun üstesinden gelmek üzere veri koruma kurallarında değişiklikler ve/veya eklemeler yapılması gerekliliğini ortaya çıkarmıştır. Her ne kadar Alman Anayasa Mahkemesi'nin geliştirdiği "*bilgilerin geleceğini belirleme hakkı*" veri koruma hukukunda Almanya'nın sınırlarını aşan bir dönüşüme neden olmuşsa da bu daha çok teoride kalmış, uygulamada beklenen etkiyi gösteremediği kısa sürede anlaşılır.

Geliştirilmiş ve güçlendirilmiş katılım haklarına karşın, bireyler bilgilerin geleceğini belirleme hakkının kullanımının neden olacağı bedelleri ödemekte istekli

benimsemişlerdir. 1997 yılından günümüze kadar da Latin Amerika ülkelerinde Habeas data bireysel şikayetin benimsenmesi yönündeki eğilim devam etmiştir. Andrés GUADAMUZ, s. 4. Bkz. 1992 Paraguay Anayasası, m.135; Peru Anayasası, m. 200/3; Arjantin Anayasası, m.43. Örneğin Filipinler'deki gelişmeler için bkz. Leila SALAVERRIA, "SC Drafting Writ of Habeas Data Invoking Right to Truth", 31 Ağustos 2007, **Inquirer.net**, http://newsinfo.inquirer.net/inquirerheadlines/nation/view/20070831-85704/SC_drafting_writ_of_habeas_data_invoking_right_to_truth (s.y. 23 Nisan 2009). Buna rağmen, Şili gibi bazı Latin Amerika ülkelerinin kendi bölgelerine özgü bu yöntem yerine,

Avrupa yaklaşımını benimsedikleri de görülmektedir. Andrés GUADAMUZ, s. 15.

³⁷ Habeas data bireysel şikayeti, bu sistemi benimseyen pek çok ülkede kişisel verilerin korunması yanında, kısmen bilgi edinme hakkının kullanılmasına da hizmet etmektedir. Nitekim Habeas data ile ulaşılacaklar yalnızca kişinin kendisi ile ilgili olan bilgilerdir. Bkz. David BANISAR, **Freedom of Information Around the World 2006, A Global Survey of Access to Government Information Laws**, Privacy International, s.17. Ayrıca bkz. Arjantin'e ilişkin olarak **a.g.e.**, s. 39, Kolombiya'ya ilişkin olarak **a.g.e.**, s. 58, Panama'ya ilişkin olarak **a.g.e.** s. 119-121.

³⁸ Andrés GUADAMUZ, s. 5; Cemil KAYA, s. 99.

ol(a)mamışlardır. Bu durum, veri korumanın ekonomik ve sosyal olarak haklarını kullanabilen ayrıcalıklı bir azınlığa terk edilmesine neden olmuştur. Bu noktada veri koruma kurallarını “*kâğıttan dışsız kaplanlara*” benzetmek abartılı olmayacaktır³⁹.

Gerçekten hukuksal metinlerde bireyler, pek çok hakka kavuşmuştur. Ancak gerçeklikte bunların hedeften, yani kişisel verilerin etkin korunmasından uzak sonuçları bulunur. İnsan hakları düşüncesinin ilk ortaya çıktığı günden bugüne yaşanan pek çok örnek gibi burada da bireyler için yeterli güvenceler tanınmadan verilen hakların etkin bir şekilde kullanılmıştır. Bireyler, kişisel verilerini işleyenlerle yaptıkları sözleşmelerde kişisel verileri üzerindeki haklarından sıklıkla vazgeçmişlerdir. Ayrıca sorun bununla da sınırlı kalmamıştır: doğrudan pazarlama gibi bazı alanlarda mevcut düzenlemelerle aşılamayan bazı sorunların ortaya çıktığı görülmüştür.

Bütün bunlara çözüm olarak geliştirilen yeni normlarda, ilgilinin haklarını korumak için ispat yükümlülüğünün taraflarını değiştirmek, sektörel şartlara uygun özel düzenlemeler getirmek gibi yeni yaklaşımlar benimsenir⁴⁰. Ayrıca aynı dönemde bilgiye erişimde daha güçlü kurumların geliştirilmesiyle pazarlıkta dengenin sağlanmasına çalışılmış ve bazı durumlarda mutlak bir korumanın sağlanması yaklaşımı benimsenmiştir. Buna göre, kimi alanlarda kişisel veriler mutlak olarak korunmalı ve birey pazarlığa oturamamalıdır. Hassas kişisel verilere işleme yasağı getirilmesi, bu düşüncenin ürünü olarak değerlendirilebilir⁴¹.

Kişisel verilerin korunmasının içinde bulunduğu krizi aşmak ve güvencelerin etkin bir biçimde uygulanmasını sağlamak amacıyla mevcut yasalarda değişiklikler yapmak, bazı sektörlerle ilişkin özel düzenlemeler geliştirmek yanında teknoloji tabanlı uygulamaların yaygınlaştırılması gibi başka bazı çözüm yolları 1990’lı yıllarda üzerinde durulan konular arasındadır. Ayrıca uluslararası düzeydeki çalışmalar da hızla gelişmiştir. Burada belki en önemli soru: bilginin özgür akışının önünde engel oluşturmada kişisel verilerin uluslararası düzeyde korunmasının nasıl sağlanacağıdır. Gelişen ve her geçen gün yeni ürünler sunmaya devam eden bilişim teknolojilerinin bilgiyi daha hızlı kullanma, işleme ve yayma olanakları sunması, bir

³⁹ Viktor MAYER-SCHÖNBERGER, s. 229-232.

⁴⁰ Viktor MAYER-SCHÖNBERGER, Ernst O. BRANDL, s. 13.

⁴¹ Viktor MAYER-SCHÖNBERGER, s. 229-232.

yandan kişisel verilerin üzerindeki tehdidi güçlendirirken, diğer yandan bireye sağlanan güvencelerin etkinliğini de azaltmaktadır.

1995 yılında AB bünyesinde kabul edilen 95/46/AT sayılı Verilerin Korunması Yönergesi ise kişisel verilerin korunmasına ilişkin krize yeni bir boyut kazandırmıştır. Aşağıda ayrıntılı olarak inceleneceği üzere bu Yönerge, kişisel verilerin korunması alanında AB sınırlarını aşan bir etkiye sahiptir ve şimdilik dünyada konuya ilişkin en baskın ve zorlayıcı modeli oluşturmaktadır.

Buraya kadar kişisel verilerin korunmasının hukuksal yolculuğu genel çizgileriyle açıklanmaya çalışılmıştır. Ancak şu konuyu bir kez daha anımsamak gerekir: bütün bu gelişimlerin dünyanın tamamı için aynı çizgi üzerinde geliştiğini söylemek olanaklı değildir. Herşeyden önce kişisel verilerin korunmasının dinamik yapısı, herhangi bir ülke uygulamasından bağımsız olarak konunun çeşitli boyutlarının ortaya çıkmasına neden olmaktadır. Bunun yanında sorunlara çözüm arayışında farklı yaklaşımlar çözüm yollarının da çeşitlenmesine neden olmaktadır.

Bireylerin özel yaşamlarına müdahale etmeyi ve yurttaşları gözetlemeyi, fişlemeyi ve sürekli takibi bir yönetim pratiği haline getiren devletlerde kişisel verilerin korunması hukuksal düzeyde ya hiç tanınmamıştır, ya da bu konuyu düzenleyen hükümler fiilen uygulanmamaktadır. Kimi ülkelerde ise devletin elindeki kişisel verilerin işlenmesine yönelik belirli güvenceler tanınırken, ekonomik gerekçelerle özel teşebbüslerin benzer uygulamalarına büyük oranda ılımlı yaklaşıldığı görülür. Ayrıca kişisel verilerin korunması yönünde güçlü adımlar atılan Avrupa’da da konuya ilişkin pek çok sorun halen sürmektedir. Bu bağlamda Avrupa yaklaşımı da dâhil, kişisel verilerin korunmasına yönelik benimsenen sistemlerin işlerliği önemli bir tartışma konusunu oluşturur. Bu tartışmalar, özellikle “*etkinlik*” ekseninde gelişmektedir.

Aşağıda kişisel verilerin korunması hukukunun tarihsel gelişimine ilişkin genel tablo çizilirken, üzerinde daha sonra ayrıntılı açıklamalar yapılacağı için bilinçli olarak ihmal edilmiş bir başka konuya, kişisel verilerin korunması hukukunun uluslararası kaynaklarına değinilecektir.

II. KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN ULUSLARARASI KAYNAKLARI

A. GENEL OLARAK

Kişisel verilerin korunması hukukunun normatif temelini oluşturan özel yaşamın gizliliği hakkı, pek çok önemli insan hakları metninde güvence altına alınmıştır. Bu kapsamda BM Evrensel İnsan Hakları Bildirisi, BM Uluslararası Bireysel ve Siyasal Haklar Sözleşmesi, Avrupa İnsan Hakları Sözleşmesi ve Amerikalılar Arası İnsan Hakları Sözleşmesi ilk akla gelenlerdir⁴². Birinci bölümde açıklandığı üzere, bu metinlerde koruma altına alınmış özel yaşamın gizliliği hakkı, kişisel verilerin korunmasının hedef ve ilkeleri ile yakından ilişkilidir⁴³.

Bunun yanında uluslararası alanda doğrudan kişisel verilerin korunmasına hasredilmiş metinler de bulunur. İlk veri koruma düzenlemelerinin yasalaşmasından kısa bir süre sonra, verilerin sınır ötesi aktarımında sorun yaşanmaması için ulusal yasaların uyumlaştırılması gereksinimi ortaya çıkmıştır. Bu doğrultuda 1980’li yılların başından itibaren verilerin korunması açısından yeni bir döneme girildiği söylenebilir. OECD, BM, AK, APEC gibi uluslararası kuruluşlar, kişisel verilerin korunmasına ilişkin temel ilkeleri ve verilerin sınırötesi aktarımını düzenleyen metinler kabul etmiştir. Bu metinler, hem ulusal hukuklarda genel olarak geçerli olan

⁴² 1981 tarihli Afrika İnsan ve Halkların Hakları Şartı’nda ise özel yaşamın gizliliği hakkından söz edilmediği görülür. (Metnin İngilizce çevirisi için bkz. http://www.achpr.org/english/_info/charter_en.html) Buna karşın batı demokrasilerini kapsamayan bölgesel metinlerde özel yaşamın gizliliği hakkının kesin olarak ihmal edilen bir alan olduğu da düşünülmemelidir. Örneğin 5 Ağustos 1990 tarihli Kahire İslam İnsan Hakları Bildirgesi’nin 18/b hükmünde özel yaşamın gizliliği hakkı bütün bireyler için tanınmıştır. (Metnin İngilizce çevirisi için bkz. <http://www.oicun.org/articles/54/1/Cairo-Declaration-on-Human-Rights-in-Islam/1.html>) 22 Mayıs 2004 tarihli İnsan Hakları Arap Şartı ise 21. maddesinde özel yaşamın gizliliği hakkını düzenlemiştir. (Bu metnin İngilizce çevirisi için bkz. Mohammed Amin Al-MIDANI, Matilde CABANETTES, Susan M. AKRAM, “Arab Charter on Human Rights 2004”, *Boston University International Law Journal*, C.24, Y. 2006, s. 147-164, http://www.acihl.org/res/Arab_Charter_on_Human_Rights_2004.pdf) Buna karşın özellikle İslam öğretisinin hakim olduğu bölgelerde kabul edilen insan hakları metinlerine ilişkin tartışmaların sürdüğü ve bunların çeşitli açılardan eleştirildiği de belirtilmelidir. Genel bir değerlendirme için bkz. Oktay UYGUN, “İnsan Hakları Kuramı”, *İnsan Hakları*, YKY, İstanbul 2000, s. 29 vd.

⁴³ Bkz. Lee A. BYGRAVE, “Privacy Protection in a Global Context-A Comparative Overview”, *Scandinavian Studies in Law*, Y. 2004, C. 47, s. 332, <http://folk.uio.no/lee/publications/Privacy%20in%20global%20context.pdf> (s.y. 20 Nisan 2009).

veri koruma ilkelerini belirlemektedir, hem de konuya ilişkin ulusal ve uluslararası girişimlerde örnek oluşturarak⁴⁴, veri koruma hukukunun gelişimini etkilemektedir.

Kişisel verilerin korunmasında etkili metinler kabul eden bir diğer önemli kuruluş ise AB'dir. Uluslarüstü bir kuruluş olan AB, kendi ilkelerini dünyanın geri kalanına ihraç etme konusunda oldukça başarılı sayılabilir. Nitekim pek çok bölgeden çok çeşitli devletlerin kişisel verilerin korunmasında Avrupa modelinden etkilendiği görülmektedir⁴⁵. Bunun önemli bir nedeni aşağıda inceleneceği üzere 95/46/AT sayılı Yönergenin kişisel verileri “yeterli” oranda korumayan devletlere verilerin aktarımını yasaklamasıdır.

Bunun yanında kişisel verilerin korunmasında uluslararası rejimin büyük oranda AB'nin tercih ettiği modele göre belirlenmesinin nedenlerinden bir diğeri, yeni gelişen bir konuda uluslararası alanda ilk aşamada kabul edilen normların, düşüncelerin, uygulamaların sonradan değiştirilmesinin zorluğudur. Bunun yanında AB'nin ABD'yle derin görüş ayrılığında bulunduğu bu konuda uluslararası bir model geliştirebilmesinin, bu alanda çok güçlü bazı devletlerin katılımı olmaksızın kurulabileceğine ilişkin önemli bir örnek olarak değerlendirilmelidir⁴⁶.

Bu belgelerin hepsi devletlere, belirlenen ilkeleri iç hukuklarına aktarmaları konusunda geniş bir takdir yetkisi tanımaktadır. OECD ve BM'nin Rehber İlkeleri bağlayıcı olmadığı için bu durum onlar açısından oldukça açıktır. Ancak AK Sözleşmesi ve AB Yönergesi de bu belgeleri kabul eden ülkelere önemli bir hareket alanı tanımaktadır. Bu belgelerin bir diğer ortak özelliği ise oldukça dağınık hükümlerine karşın, bunların nasıl yorumlanacağına ilişkin yol gösterici resmi belgelere çok sınırlı oranda yer vermeleridir⁴⁷. Tartışılabilir yönlerine karşın bu metinlerin uluslararası alanda kişisel verilerin korunması yönünde önemli adımlar olduğunu belirtmek gerekir.

⁴⁴ Lee A. BYGRAVE, **Data Protection Law**, s.30.

⁴⁵ Bu etkiyi örneğin Latin Amerika ülkelerinde hissetmek olanaklıdır. 95/46/AT sayılı Yönerge'nin 25. maddesi ile belirlenen, yeterli düzeyde koruma sağlamayan ülkelere veri aktarımının yasaklanması ilkesi, pek çok Latin Amerika ülkesinde, yukarıda açıklanan, Habeas data bireysel şikayetine ilişkin düzenlemelerde bu gereklilikle uyumlu değişiklikler yapma zorunluluğunu gündeme getirmiştir. Nitekim kişisel verilerin Habeas data bireysel şikayeti yoluyla korunduğu bazı ülkeler, AB'nin belirlediği asgari ölçüyü karşılayamamaktadır. Bu ise, küresel düzeyde elektronik ticarete rol oynamak isteyen devletler açısından önemli bir sorun oluşturmaktadır. Andrés GUADAMUZ, s. 14 vd.

⁴⁶ Dorothee HEISENBERG, **Negotiating Privacy, The European Union, The United States, and Personal Data Protection**, Lynne Rienner Publishers, Londra 2005, s. 161-164.

⁴⁷ Lee A. BYGRAVE, **Data Protection Law**, s. 33-35.

B. OECD

Kişisel verilerin korunmasının uluslararası bir konu olarak görülmesinde ilk adımı OECD atmıştır. 1961 yılında kurulan OECD'nin temel hedefleri arasında ekonomik büyümeyi desteklemek, iş alanlarını arttırmak, yaşam standardını yükseltmek, finansal dengeyi korumak, başka devletlerin ekonomik gelişimine yardımcı olmak, küresel ticaretin büyümesine katkı sağlamak ile demokrasiye ve pazar ekonomisine bağlı devletleri bir araya getirmek bulunur⁴⁸. Çalışmaları da doğal olarak bununla bağlantılı bir şekilde yürütülmektedir. Bu nedenle 1980 yılında “*Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler*”i⁴⁹ kabul etmesi kişisel verilerin korunmasının ekonomik boyutunun öneminin işareti olarak değerlendirilebilir.

OECD Rehber İlkeleri, hukuksal olarak bir tavsiye kararıdır ve üye ülkeler için bağlayıcılığı yoktur. Dolayısıyla OECD üyesi devletler, bu ilkeleri iç hukuklarının bir parçası haline getirip getirmemekte serbesttir. Konsey, temel olarak üye devletlere kişisel verilerin korunması ve bireysel özgürlüklerle ilgili bu ilkeleri, iç hukuklarında yapacakları yasal düzenlemelerde dikkate almalarını, sınır aşan veri trafiğinin haksız yere engellenmemesini, mevcut engellerin kaldırılmasını, bu ilkelerin yaşama geçirilmesinde iş birliği yapılmasını tavsiye etmektedir⁵⁰.

Bu kapsamda kabul edilen ilkeler verilerin korunmasına yönelik asgari gereklilikleri ortaya koyar. Bir başka anlatımla OECD Konseyi üye devletlerin verilerin korunmasını güvenceye almak için en azından bu ilkeleri benimsemesi gerektiğini belirtmektedir. Bu bağlamda kişisel verileri ve bireysel özgürlükleri

⁴⁸ Ekonomik İşbirliği ve Kalkınma Teşkilatı (Organization for Economic Co-operation and Development-OECD), 1947 yılında kurulan Avrupa Ekonomik İşbirliği Örgütü'nün (Organization for European Economic Co-operation-OEEC) ardıdır. 1961 yılında Türkiye'nin de içinde bulunduğu yirmi ülke ile kurulmuştur. Daha sonra on ülke daha OECD'ye katılmıştır. OECD'nin ürettiği tavsiyelerin bağlayıcılığı bulunmamaktadır. Ancak ortak anlayıştan kaynaklanan “*grup baskısı*” ile üye ülkelerin çeşitli konulardaki reform süreçlerini etkilediği söylenebilir. Bkz. İktisadi İşbirliği ve Kalkınma Teşkilatı ve Türkiye, <http://www.oecd.org/dataoecd/39/40/42122130.pdf> (s.y. 23 Nisan 2009).

⁴⁹ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 Eylül 1980, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (s.y. 23 Nisan 2009). Bundan böyle “*OECD Rehber İlkeleri*” olarak anılacaktır.

⁵⁰ Bkz. aynı yer.

korumak amacıyla bu ilkeleri güçlendirici daha kapsamlı düzenlemeler yapılması da olanaklıdır⁵¹.

OECD Rehber İlkeleri, kişisel verilerin korunmasına ilişkin politikaların belirlenmesi ve yasal düzenlemelerin yapılmasında ölçüt olarak kullanılan sekiz ilkeyi içermektedir. Bu ilkeler şunlardır:

- 1. *İLKE: Veri toplamanın sınırlı olması ilkesi* (m.7);
- 2. *İLKE: Verilerin belirli bir niteliği karşılaması (veri kalitesi) ilkesi* (m.8);
- 3. *İLKE: Amacın belirliliği ilkesi* (m.9);
- 4. *İLKE: Kullanımın sınırlı olması ilkesi* (m. 10);
- 5. *İLKE: Veri güvenliği ilkesi* (m. 11);
- 6. *İLKE: Açıklık ilkesi* (m.12);
- 7. *İLKE: Bireyin katılımı ilkesi* (m.13);
- 8. *İLKE: Hesap verilebilirlik ilkesi* (m.14).

OECD Rehber İlkelerinin bir kaç açıdan önemli olduğu belirtilmelidir. Öncelikle, bunlar, konuya ilişkin olarak uluslararası alanda yapılan ilk önemli girişimin ürünüdür⁵². Bu nedenle, kişisel verilerin korunmasını bazı devletlerin ulusal hukuk sistemlerinde bulunan bir alan olmasının ötesinde, uluslararası alanda da tartışılan ve çözüm aranan bir konu olduğunun ilk işaretidir.

İkinci olarak bu ilkelerin belirlenmesinde Kuzey Amerika, Avrupa, Asya gibi dünyanın çeşitli bölgelerinden pek çok temsilci katkıda bulunmuştur. Çeşitli kültürlerden gelen ve farklı yönetim biçimleri altında yaşayan temsilciler, kişisel verilerin korunmasına ilişkin bu sekiz ilkede birleşmişlerdir. Bu anlamda, OECD Veri Koruma İlkeleri, bilginin sınır tanımaz bir şekilde yayıldığı dünyamızda, kişisel

⁵¹ Bkz. OECD Rehber İlkeleri, par. 6.

⁵² OECD'nin özel yaşamın gizliliği ve kişisel verilerin korunmasına ilişkin çalışmaları, 1960'lı yıllarda, hatta bazı gözlemciler göre daha da önce başlamıştır. Michael ERBSCHLOE, John VACCA, **Net Privacy, A Guide to Developing and Implementing an Ironclad E-business Privacy Plan**, McGraw-Hill, ABD 2001, s. 30. 1974 yılında OECD'nin düzenlediği Veri Bankası Paneli'nde bir grup uzman günümüzde OECD Veri Koruma İlkeleri olarak bilinen kuralları oluşturmuşlardır. Bu ilkelerde ağırlık, farklı ülkelerdeki veri koruma yasalarını harmanlama, bilginin özgür dolaşımını sağlama gereksimine ve kişisel veriler ile özel hayatın gizliliğini ilgilendiren hakların garanti altına alınması zorunluluğuna verilmiştir. Robert BOND, **New Economy Equity (Navigating Security and Legal Issues in Digital Business)**, John Wiley & Sons, LTD, İngiltere 1988, s.137-138.

bilgilerin denetiminin nasıl yapılacağı, kullanım şekillerinin nasıl saptanacağı konusunda geniş kapsamlı bir uzlaşmayı yansıtmaktadır⁵³.

Üçüncü olarak OECD Rehber İlkeleri, her ne kadar üye ülkeler için bağlayıcı olmasa da konuya ilişkin pek çok ulusal ve uluslararası metnin kabul edilmesini ve bunların içeriğinin belirlenmesini önemli oranda etkilemiştir. AB Veri Koruma Yönergesi⁵⁴ yanında Japonya, Avustralya, Yeni Zelanda, Hong Kong gibi çeşitli ülkelerde bu etkiyi hissetmek olanaklıdır. Kuzey Amerika’da ise yasal bir zorunluluk olmasa da, pek çok şirket ve ticari kuruluş bu ilkelere uyacağını açıklamıştır⁵⁵. Asya Pasifik bölgesinde yapılacak düzenlemeler için, Asya Pasifik Birliği’nin ortak veri koruması ilkelerini belirlediği bir çerçeve karar hazırlamasında da OECD Rehber İlkelerinin etkisi bulunur⁵⁶.

OECD Rehber İlkeleri çeşitli devletlerde halen hem özel, hem de kamu sektöründe geniş oranda kullanılmaktadır. Türkiye’de Kişisel Verilerin Korunması Kanunu gerekçesinde de belirtilen ilkelere atıfta bulunulması, yapılan ulusal düzenlemelerde bu etkinin halen sürdüğünün bir göstergesidir.

OECD konuya ilişkin çalışmalarını, Kişisel Verilerin Korunması Rehber İlkeleri’nin kabul edilmesinden sonra da sürdürmüştür. Bu bağlamda, OECD Veri Koruma İlkeleri’ni destekleyici çeşitli çalışmalar yürütülmüş⁵⁷, kurumlara gizlilik politikalarını belirlemede yardımcı olacak çevrimiçi bir program oluşturulmuş⁵⁸, spam ile mücadeleye yönelik girişimlerde bulunulmuş⁵⁹ ve Veri Güvenliğine İlişkin Rehber İlkeler⁶⁰ yayınlanmıştır⁶¹. Ayrıca OECD’nin özellikle küresel ağlar ile

⁵³ WHOIS, <http://epic.org/privacy/whois/> Pek çok Avrupa ülkesi OECD üyesidir. Avrupa dışındaki üye devletler ise şunlardır: ABD, Avustralya, Kanada, Japonya, Kore, Meksika, Yeni Zelanda. Bkz.

http://www.oecd.org/document/58/0,3343,en_2649_201185_1889402_1_1_1_1,00.html (s.y. 1 Mayıs 2009).

⁵⁴ Michael ERBSCHLOE, John VACCA, s. 30.

⁵⁵ **Safeguarding Privacy in the Fight Against Terrorism**, Report of the Technology and Privacy Advisory Committee, Mart 2004 ABD.

⁵⁶ Lee A. BYGRAVE, “Privacy Protection in a Global Context”, s. 335.

⁵⁷ Örneğin bkz. **Declaration of Transborder Data Flows**, 11 Nisan 1985, http://www.oecd.org/document/25/0,3343,en_2649_34255_1888153_1_1_1_1,00.html (s.y. 20 Nisan 2009).

⁵⁸ Bkz. **OECD Privacy Statement Generator**, <http://www.oecd.org/sti/privacygenerator> (s.y. 20 Nisan 2009).

⁵⁹ Bkz. **Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommendation Policies and Measures**, 26 Nisan 2006, <http://www.oecd-antispam.org>.

⁶⁰ **OECD Guidelines for the Security of Information Systems and Networks, Towards a Culture of Security**, (25 Temmuz 2002’de OECD Konsey’inin 1037. oturumunda tavsiye

bağlanan dünyamızda sanal ortamda ortaya çıkabilecek ihlalleri de göz ardı etmediği görülür⁶². RFID gibi yeni gelişen teknolojilerin kullanılmasında kişisel verilerin korunmasına ilişkin ortaya çıkabilecek sorunların irdelendiği metinler de yayınlanmıştır⁶³.

C. BİRLEŞMİŞ MİLLETLER

İkinci dünya savaşının yarattığı acı ve dehşet ortamının bir daha yaşanmaması için en önemli girişimlerden biri Birleşmiş Milletler Örgütü'nün (BM) kuruluşudur. 24 Ekim 1945 tarihinde 51 devletin kurduğu örgütün günümüzde 192 üyesi bulunmaktadır⁶⁴. Bu üye devletler, aralarındaki ilişkilerin temel ilkelerini belirleyen BM Şartı'ndan⁶⁵ doğan yükümlülükleri kabul ederler. Bu metinde Örgüt'ün belirlenen dört amacından biri de herkesin insan hakları ve temel özgürlüklerine saygı gösterilmesinin geliştirilip desteklenmesidir⁶⁶.

BM'nin kuruluşundan kısa bir süre sonra 10 Aralık 1948 yılında kabul edilen BM Evrensel İnsan Hakları Bildirisi, Örgüt'ün insan haklarının korunması alanında dünya ölçeğinde standart belirleme sürecinin ilk adımıdır⁶⁷. Kısa sürede yaygın bir kabul gören bu metin, halen insan hakları alanında en önemli uluslararası belgelerden biridir. Bildirinin 12. maddesinde özel yaşamın gizliliği hakkı düzenlenmiştir. 12. madde hükmü şöyledir:

niteliğinde kabul edilmiştir), <http://www.oecd.org/dataoecd/16/22/15582260.pdf> (s.y. 20 Nisan 2009).

⁶¹ Christopher KUNER, *European Data Protection Law*, 49;

⁶² Özellikle bkz. **The OECD Ministerial Declaration on the Protection of Privacy on Global Networks, Privacy Online: Policy and Practica Guidance**, Committee for Information Computer and Communications Policy, Working Group on Information Security and Practice, 21 Ocak 2003, [http://www.oecd.org/olis/2002doc.nsf/LinkTo/NT000029C6/\\$FILE/JT00137976.PDF](http://www.oecd.org/olis/2002doc.nsf/LinkTo/NT000029C6/$FILE/JT00137976.PDF) (s.y. 20 Nisan 2009).

⁶³ **RFID, Radio Frequency Identification, OECD Policy Guidance, A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives**, OECD Ministerial Meeting on the Future of the Internet Economy, Seul, Güney Kore, 17-18 Haziran 2008, <http://www.oecd.org/dataoecd/19/42/40892347.pdf> (s.y. 20 Nisan 2009).

⁶⁴ Bkz. <http://www.un.org/en/aboutun/index.shtml>.

⁶⁵ BM Şartı'nın İngilizce tam metni için bkz. <http://www.un.org/en/documents/charter/>.

⁶⁶ Bkz. BM Şartı m. 1/3. BM sisteminin insan haklarını koruma ve denetim yöntemlerine ilişkin ayrıntılı bilgi için bkz. Mesut GÜLMEZ, **Birleşmiş Milletler Sisteminde İnsan Haklarının Korunması**, Türkiye Barolar Birliği Yayınları, Ankara 2004. Ayrıca bkz. Mehmet Semih GEMALMAZ, **Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş**, 6. Baskı, Legal 2007, s. 833-846; Turgut TARHANLI, "Birleşmiş Örgütü ve İnsan Haklarının Korunmasına İlişkin Başlıca Usuller", **İnsan Hakları**, YKY, İstanbul 2000, s. 407-436.

⁶⁷ Turgut TARHANLI, s. 408.

“Hiç kimse, özel yaşamına, ailesine, konutuna ya da haberleşmesine yönelik keyfi müdahalelere ya da onur ve şöhretine yönelik saldırılara maruz bırakılmayacaktır. Herkesin, bu tür müdahale ya da saldırılara karşı yasa ile korunma hakkı vardır”.

Bunun gibi BM Bireysel ve Siyasal Haklar Uluslararası Sözleşmesi’nin 17. maddesinde de, hemen hemen aynı ifade ile bu hak alanına yer verilmiştir. Ancak daha önemlisi, kişisel verilerin korunması hakkının bu Sözleşme’de yer alan özel yaşamın gizliliği hakkı kapsamında görüldüğünün BM İnsan Hakları Komitesi tarafından açıkça kabul edilmesidir. BM İnsan Hakları Komitesi 16. Genel Yorumu ile 17. maddenin kapsamına açıklık getirmiştir⁶⁸. Buna göre:

“Tüm insanların toplum içerisinde yaşamalarının sonucu olarak, özel hayatın gizliliğinin korunması kaçınılmaz şekilde görecelidir. Ancak, Sözleşme’den anlaşıldığı üzere yetkili kamu otoriteleri, bilinmesi toplumun çıkarlarının korunması açısından gerekli olan, bireyin özel hayatıyla ilgili bir bilgiyi öğrenme talebinde bulunabilmelidir. ... Kamu otoritelerinin, özel kişi ve kurumların bilgisayarlarda, veri bankalarında veya benzeri cihazlarda kişisel bilgileri toplaması veya saklaması hukuki düzenlemeye tabi olmalıdır. Devletler, bir kimsenin özel hayatına dair bilgilerin hukuken bu bilgilere sahip olma ve kullanma yetkisine sahip olmayanların eline geçmesini ve bu bilgilerin Sözleşme’nin amaçlarına aykırılık teşkil edecek şekilde kullanılmasını engellemek için etkili tedbirler almalıdır. Özel hayatın gizliliğinin en etkili şekilde korunabilmesi için, her birey kişisel dosyalarda veya veri tabanlarında kendisiyle ilgili bilgiler saklanmışsa bu bilgilerin ne tür bilgiler olduğunu ve ne amaçla saklandığını öğrenme hakkına sahiptir. Ayrıca, her birey hangi kamu otoritelerinin, özel kişilerin veya kurumların bu dosyaları kontrol altında tuttuğunu veya tutabileceğini öğrenebilmelidir. Söz konusu dosyaların, yanlış kişisel bilgilere yer vermesi halinde veya bu bilgilerin hukuka aykırı şekilde toplanması veya kullanılması halinde her

⁶⁸ BM İnsan Hakları Komitesi, Bireysel ve Siyasal Haklar Sözleşmesi’nin 40/4 hükmü uyarınca Sözleşme’nin çeşitli hükümlerini yorumlayarak kapsamlarını netleştirmektedir. Komite, Genel Yorumlarını belirli bir devlete değil, bütün taraf devletlere yönelik olarak geliştirmektedir. Bu Genel Yorumlar, aydınlatıcı bir niteliktedir ve taraf devletlere Sözleşmenin uygulamasını geliştirebilmeleri için Komitenin deneyimlerini öğrenebilme olanağı sunmaktadır. Bkz. Mehmet Semih GEMALMAZ, **Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş**, s. 434.

birey düzeltme veya bilgilerin ortadan kaldırılmasını talep etme hakkına sahiptir”⁶⁹.

Görüldüğü gibi İnsan Hakları Komitesi, 17. madde ekseninde geliştirdiği yorum ile kişisel verilerin korunmasını özel yaşamın gizliliği hakkı içerisinde gördüğünü açıkça ortaya koymuştur. Komite’nin 17. madde hükmünü değerlendirirken kişisel verilerin korunmasına ilişkin ulusal ve uluslararası düzenlemeleri dikkate aldığı görülmektedir. Bu kapsamda kişisel verilerin korunmasında hâkim olan pek çok temel ilkeye 16. Genel Yorum içerisinde yer verilmiştir.

Bununla birlikte bazı ilkelerin göz ardı edildiği belirtilmelidir. Örneğin kişisel verilerin toplanmasının belirli bir amaç ile sınırlandırılması öngörülmüşse de bu işlemin dürüstlük kurallarına uygun olacağına dair bir ifade Yorum’da yer almamaktadır. Ayrıca pek çok ulusal ve uluslararası belgenin aksine hassas kişisel veriler ile diğerleri arasında bir ayrıma gidilmediği ve bu nedenle belirtilen ilk kategoriye yönelik özel bir korumanın geliştirilmediği dikkat çekmektedir⁷⁰.

BM bünyesinde kabul edilen genel nitelikli insan hakları metinlerinde görülen bu düzenlemeler yanında, Örgüt’ün doğrudan kişisel verilerin korunmasına yönelik bazı girişimlerinin bulunduğu da belirtilmelidir. Bunlardan en önemlisi BM Genel Kurulu’nun, 1990 yılında kabul ettiği “*Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler*”dir⁷¹. BM Rehber ilkeleri hem üye ülkeleri kişisel verileri korumaya yönelik yasaları çıkarmaya teşvik etmeyi, hem de hükümet içi ve hükümet dışı uluslararası kuruluşları kişisel verileri bu temel ilkelere uygun bir şekilde işlemeye yönlendirmeyi amaçlamıştır⁷². Ayrıca BM, kendi personeline ilişkin

⁶⁹ BM İnsan Hakları Komitesi, 32. Oturum, Genel Yorum No.16, Y. 1988, Madde 17: Özel Yaşamın Gizliliği, par. 7, 10, **Birleşmiş Milletlerde İnsan Hakları Yorumları, İnsan Hakları Komitesi ve Ekonomik, Sosyal ve Kültürel Haklar Komitesi, 1981-2006**, der. ve çev. Lema UYAR, İnsan Hakları Hukuku Çalışmaları, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2006, s. 35-36.

⁷⁰ Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy in Human Rights Treaties” , s. 253.

⁷¹ United Nations guidelines concerning computerized personal data files, Genel Kurulca kabul tarihi: 14 Aralık 1990. Rehber ilkelerin tam metni için bkz. <http://www.unhchr.ch/html/menu3/b/71.htm> (s.y. 20 Nisan 2009).

⁷² Lee A. BYGRAVE, **Data Protection Law**, s. 33.

ve kendi personelinin erişebileceği kişisel veriler açısından da çeşitli ilkeler geliştirmiştir⁷³.

BM Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler⁷⁴ uyarınca, ulusal hukuk sistemlerinde tanınması gereken güvenceler şu konulara ilişkindir:

- Yasal ve dürüst yollarla toplama ve işleme ilkesi;
- Verilerin doğruluğu ilkesi;
- Amacın belirliliği ilkesi;
- İlgili kişinin erişimi ilkesi;
- Ayrımcılık yapmama ilkesi;
- Veri güvenliği ilkesi;
- Denetim ve yaptırım;
- Verilerin sınır ötesi akışı.

Belirtilen ilk dört ilkeye belirli durumlarda istisna getirilmesi olanaklıdır. Bu ilkelerin ilk olarak kamu ve özel sektördeki bilgisayarlarda bulunan, gerçek kişilere ilişkin bütün veri dosyalarına uygulanması gerekmektedir birlikte, isteğe bağlı olarak elle işlenen dosyalara ve tüzel kişilere ilişkin verilere uygulanmaları da söz konusu olabilir.

BM Rehber İlkeleri'nin bir bölümünün, başka bazı uluslararası metinlerden daha ileri hükümler içerdiği söylenebilir⁷⁵. Gerçekten BM'nin Rehber İlkeleri, kişisel verilerin korunmasına ilişkin ilkelerin uygulamasını denetleyecek yetkili ve bağımsız bir veri koruma organının kurulmasını öngören ilk uluslararası hukuk belgesidir⁷⁶. Ancak bu öncü rolüne karşın metnin, AK Sözleşmesi ve OECD Veri Koruma İlkelerine göre çok daha sınırlı bir etkisi olmuştur. Bu sınırlı etki, BM Örgütünün etki alanı düşünüldüğünde oldukça şaşırtıcıdır. Bu durumun nedenlerinden biri olarak ilkelerin hukuksal açıdan bağlayıcı olmaması, yalnızca tavsiye niteliğinde bulunması düşünülebilir. OECD Veri Koruma İlkelerinin de aynı şekilde bağlayıcılığının bulunmamasına karşın, bu alandaki ilk uluslararası düzenleme olması dolayısıyla daha geniş bir etki yarattığı söylenebilir.

⁷³ Bkz. Marie VICIEN-MILBURN, "The United Nations and Personal Data Protection", 3 Ekim 2005, <http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=4236> (s.y. 3 Nisan 2009).

⁷⁴ Bundan böyle "*BM Rehber İlkeleri*" olarak anılacaktır.

⁷⁵ Lee A. BYGRAVE, *Data Protection Law*, s. 73, 350.

⁷⁶ Marie-Theres TINNEFELD ve diğ., s. 99.

İleride BM'nin kişisel verilerin korunmasına yönelik daha güçlü metinler geliştireceği ve bu konuya daha fazla eğileceği düşünülmektedir. BM'nin kişisel verilerin korunmasına ilişkin geniş kapsamlı çeşitli toplantılara destek vermesi bunun bir göstergesidir. Ayrıca 2005 yılında Montrö'de yapılan “27. Uluslararası Veri Koruma ve Özel Yaşamın Gizliliği Temsilcileri Konferansı”nda (27th International Conference of Data Protection and Privacy Commissioners) açıklanan “Montrö Bildirgesi”nde BM'ye veri koruma ve özel yaşamın gizliliği haklarını ayrıntılı bir şekilde düzenleyen bağlayıcı bir uluslararası belge hazırlaması yönünde çağrıda bulunulmuştur⁷⁷. Bu, BM kapsamında daha etkin çalışmaların yapılmasının yalnızca kurum içindeki ilgili birimlerden gelen bir istek olmadığına da göstergesidir. Kurum dışından da böyle bir beklentinin bulunduğu görülmektedir.

D. AVRUPA KONSEYİ

1. Genel Olarak

Kişisel verilerin korunması yönünde önemli çalışmalar yürüten diğer bir uluslararası kuruluş Avrupa Konseyi'dir⁷⁸. II. Dünya Savaşı'nın hemen ardından kurulan AK'nin hedefi, Statüsü'nün⁷⁹ Başlangıç bölümünde belirtilmiştir. Buna göre:

“(...) halkların ortak varlığı olan ve her gerçek demokrasinin dayandığı kişi özgürlüğü, siyasal özgürlük ve hukukun üstünlüğü ilkelerine kaynaklık eden düşünce ve ahlaki değerlere, sarsılmaz bir şekilde bağlı olarak, aynı hisleri paylaşan ülkeler arasında sıkı bir birlik kurulması zorunlu görülmüştür”⁸⁰.

Bölgesel bir kuruluş olan AK'nin⁸¹ amaçlarından en önemlisi şüphesiz insan haklarının korunması ve geliştirilmesidir⁸². Konsey bünyesinde çeşitli hukuksal

⁷⁷ Christopher KUNER, s. 49-50. “Montrö Bildirgesi” için bkz. **The Protectin of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities (“Montreaux Declaration”)**, International Conference of Data Protection and Privacy Commissioners, 16 Eylül 2005, s.3, <http://www.unhcr.org/refworld/publisher,ICDPPC,,,435914f74,0.html> (s.y. 23 Nisan 2009).

⁷⁸ Bundan böyle “AK” veya “Konsey” olarak anılacaktır.

⁷⁹ Statute of the Council of Europe, Andlaşma sayı: 002, imza t.: 5 Mayıs 1949, yürürlük t.: 3 Ağustos 1949. Türkçe metni için bkz. Muzaffer SENCER, s. 384-394.

⁸⁰ Şeref GÖZÜBÜYÜK, Feyyaz GÖLCÜKLÜ, s. 8. AK'nin kurucu belgesi 5 Mayıs 1949'da imzaya açılan ve 3 Ağustos 1949'da yürürlüğe giren Avrupa Konseyi Statüsüdür.

⁸¹ AK, kişisel verilerin korunmasının da dahil olduğu pek çok konuda AB kurumları ile ortak çalışmalar yürütmektedir. AK, bir AB organı olmamakla birlikte AB üyesi devletlerin tamamının bu Konseyin üyesi olduğunu belirtmek gerekir.

⁸² Şeref GÖZÜBÜYÜK, Feyyaz GÖLCÜKLÜ, s. 8.

metinlerin kabulü ve çalışmaların yürütülmesi ile insan haklarının korunmasına katkı sağlanmaya çalışılmaktadır.

Kişisel verilerin korunmasının önemi ve gerekliliği AK içerisinde kısa sürede kavranmış ve bu konuda çeşitli girişimlerde bulunulmuştur. Bu doğrultuda somut sonuç veren ilk girişim, 1973 ve 1974 yıllarında görülür. Bu yıllarda otomatik veri bankalarındaki kişisel verileri korumaya yönelik ilki özel sektör, ikincisi kamu sektörünü kapsayan iki karar açıklanmıştır⁸³. Buradaki amaç, tavsiye kararlarında saptanan ilkeler çerçevesinde ulusal hukuk sistemlerinde kişisel verilerin korunmasına yönelik düzenlemeler yapılmasına ivme kazandırmaktır. Ancak kısa zamanda ulusal hukuklarda etkin bir korumanın ancak bağlayıcı uluslararası normlarla bunların güçlendirilmesi durumunda söz konusu olabileceği fark edilmiştir. Nitekim bu konuya 1972 yılında Avrupa Adalet Bakanları Konferansı'nda da işaret edilmiştir. Bunun üzerine dört yıl süren görüşmelerin ardından 1981 yılında 108 sayılı “*Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme*” kabul edilmiştir⁸⁴.

AK bünyesinde kişisel verilerin korunması yaklaşımının nasıl olduğu değerlendirilirken öncelikle bu Sözleşme'ye bakılmalıdır. Öte yandan Avrupa İnsan Hakları Sözleşmesi'nin ilgili hükümleri de oldukça önemlidir. Nitekim “*Avrupa kamu düzeninin anayasal belgesi*”⁸⁵ olarak kabul edilen AİHS'ne konuya ilişkin pek çok metinde atıf yapılmaktadır⁸⁶. Bu iki belgenin konumuza ilişkin ne oranda

⁸³ Bkz. Council of Europe Committee of Ministers, **Resolution (74) 29 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector**, adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies; Council of Europe Committee of Ministers, **Resolution (73) 22 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector**, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies. Bu metinler için bkz. <http://wcd.coe.int>.

⁸⁴ “Background”, http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/background/11Background.asp#TopOfPage (s.y. 20 Nisan 2009).

⁸⁵ *Loizidou Türkiye'ye karşı*, (ön itirazlar), 23 Mart 1995, Seri A No. 310, par. 75'den akataran Naz ÇAVUŞOĞLU, “Avrupa Konseyi: İnsan Hakları Avrupa Sözleşmesi'nin Denetim Sistemi”, **İnsan Hakları**, YKY, İstanbul 2000, s. 458.

⁸⁶ AK Kişisel Verilerin Korunması Sözleşmesi ya da aşağıda incelenecek olan AB düzenlemeleri yanında, pek çok anayasal, yasal düzenleme ve kişisel verilerin işlenmesine ilişkin hükümler içeren çeşitli Sözleşmeler örnek olarak gösterilebilir. AAD da 95/46/AT sayılı Kişisel Verilerin Korunması Yönergesi hükümlerinin yorumlanmasının temel haklar ışığında, özellikle de AİHS'de güvence altına alınan özel yaşamın gizliliği hakkı dikkate alınarak yapılması gerektiğine işaret etmiştir. *Rechnungshof, Österreichischer Rundfunk ve diğerlerine karşı*, C-465/00, par. 68; Mads ANDEAS, Stefan ZLEPTNIG, s. 779; Lee A. BYGRAVE, “International Agreements to Protect Personal Data”, *Global Privacy Protection: The First Generation*, haz.

koruma getirdiği aşağıda incelenecektir. Ancak ondan önce bir hususa daha değinmekte yarar vardır.

AK, insan hakları alanında çeşitli konulara ilişkin önemli belgeler üretmektedir. Bu kapsamda belirtilen Sözleşmelerin yanında başka metinlerde de kişisel verilerin korunmasına ilişkin hükümlerin bulunduğu görülür. Şüphesiz AK'nin çalışmaları konumuz açısından çok önemlidir. Ancak Konsey bünyesinde kabul edilen kimi metinlerde kişisel verilerin korunmasına yönelik yeterli hassasiyetin gösterilmediği de dikkat çekmektedir.

Burada ilk akla gelen, 1996 tarihli İnsan Hakları ve Biyotıp Sözleşmesi'dir⁸⁷. Sözleşme hızla gelişen biyoteknoloji alanında söz konusu olabilecek insan hakları ihlallerini, özellikle de insan onuruna yönelen saldırıları önlemek amacıyla kabul edilmiştir⁸⁸. Sözleşme'nin Başlangıç bölümünde EİHB ve AİHS yanında AK Verilerin Korunması Sözleşmesi'ne de atıfta bulunulmuştur⁸⁹. Ayrıca Sözleşme'de özel yaşamın ve kişisel verilerin korunmasına yönelik bazı hükümler de bulunmaktadır⁹⁰. Ancak Sözleşme'nin konusu yani Biyotıp, hassas veriler olarak adlandırılan ve pek çok düzenlemede özel olarak koruma altına alınan bir veri

James B. RULE, Graham GREENLEAF, Edward Elgar Publishing, Büyük Britanya 2008, s. 32. (15-49) Bu, AİHS'nin 8. maddesinin, aşağıda ayrıntılı olarak incelenecek AB Yönergesi'nin hükümleri ve ulusal hukuk sistemlerinde benimsenen ilkelerin yorumlanması ile doğrudan ilgili olduğunun bir işaretidir.

⁸⁷ 4 Nisan 1997 tarihli 164 sayılı Sözleşmenin tam adı, “*Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Haklarının ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesi*”dir. Sözleşme 1 Aralık 1999’da yürürlüğe girmiştir. Sözleşmenin orijinal metni için bkz. 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, <http://conventions.coe.int/Treaty/en/Treaties/Word/164.doc> . Türkiye bu Sözleşme’yi imzaya açıldığı tarihte imzalamış ve 3 Aralık 2003’de onaylamıştır. Bkz. 3 Aralık 2003 tarih, 5013 sayılı Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Haklarının ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesinin Onaylanmasının Uygun Bulunması Hakkında Kanun, RG t. 20 Nisan 2004, S. 25439. Sözleşme’ye ve ilgili metinlere ilişkin ayrıntılı bilgi için bkz. Mehmet Semih GEMALMAZ, s. 1219-1248.

⁸⁸ Bkz. m.1. Biyoteknoloji ve insan hakları ilişkisine dair ayrıntılı bilgi için bkz. Hürol ÇANKAYA, **Biyoteknoloji ve İnsan Hakları**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Genel Kamu Hukuku Anabilim Dalı, yayınlanmamış doktora tezi, Ankara 2008.

⁸⁹ Bkz. İnsan Hakları ve Biyotıp Sözleşmesi, Başlangıç bölümü par.2,3,6.

⁹⁰ Sözleşmenin III. Bölümü, “*Özel Yaşam ve Bilgi Edinme Hakkı*” kenar başlığını taşır ve yalnızca tek bir madde içerir. Bu kapsamda yer alan 10. madde hükmü şöyledir: “(1)Herkes, kendi sağlığı hususundaki bilgilerle ilgili olarak, özel yaşamına saygı gösterilmesi hakkına sahiptir. (2) Herkes, kendi sağlığı hususunda toplanmış her türlü bilgiyi öğrenme hakkına sahiptir. Bununla beraber bireylerin bilgilendirilmeme hakları da gözetilecektir. (3) İstisnai durumlarda, ikinci paragrafta belirtilen hakların kullanımına, hastanın yararı için kanuni kısıtlamalar getirilebilir”. Bkz. http://www.adlitabiplik.saglik.gov.tr/include/dosyalar/19_iphep_ETs164_trsb.pdf (s.y. 23 Nisan 2009). Sözleşmenin resmi çevirisine ilişkin bazı eleştiriler için bkz. Mehmet Semih GEMALMAZ, s. 1224-1225.

kategorisi ile yakından ilişkilidir. Her ne kadar Sözleşme’de verilerin korunmasına yönelik bazı hükümler bulunsun da, bunların yetersiz kaldığına ilişkin haklı itiraz ve eleştiriler yükselmektedir⁹¹.

Benzer sorunları taşıyan bir diğer metin ise AK Siber Suç Sözleşmesi’dir⁹². Sözleşme ile *“toplumun siber suçlara karşı korunması için atılacak diğer adımlarla birlikte gerekli mevzuatın kabul edilmesi ve uluslararası işbirliğinin geliştirilmesi yollarıyla ortak bir cezai politikanın öncelikli olarak kabul edilmesi”* hedeflenmiştir⁹³.

İnsan Hakları ve Biyotıp Sözleşmesi’nde olduğu gibi Siber Suç Sözleşmesi’nin başlangıç bölümünde de diğer pek çok önemli insan hakları metni ile birlikte AK Verilerin Korunması Sözleşmesi’ne atıfta bulunulmuştur. Bununla birlikte siber suçlulukla mücadelede izlenecek yol içerisinde kişisel verilerin toplanması, işlenmesi ve uluslararası işbirliği çerçevesinde başka devletlerle paylaşılması öngörülürken kişisel verilerin korunmasına yönelik hükümler oldukça zayıftır⁹⁴.

Nitekim Siber Suç Sözleşmesi henüz taslak halindeyken, çeşitli kuruluşlarca yayınlanan rapor ve görüşlerde Sözleşme’nin pek çok hükmünün özel yaşamın gizliliği ve kişisel verilerin korunması hakları üzerinde doğrudan etkisi bulunduğu, ancak bu etkinin Sözleşme’yi hazırlayanlarca yeterince dikkate alınmadığına işaret edilmiştir⁹⁵.

⁹¹ Örneğin bkz. Marie-Theres TINEFELD ve diğ., s. 104; Oğuz ŞİMŞEK, s. 20.

⁹² 23 Kasım 2001, 185 numaralı Avrupa Konseyi Siber Suç Sözleşmesi 1 Temmuz 2004’te yürürlüğe girmiştir. Sözleşmenin tam metni için bkz. Convention on Cybercrime, <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc>. Sözleşme’nin Türkçe çevirisi için bkz. **İnternet ve Hukuk**, der. Yeşim M. ATAMER, çev. İnternet ve Hukuk Platformu, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2004, s. 703-733. Daha sonra Sözleşme’ye eklenen 28 Ocak 2003 tarihli 189 numaralı bir protokolle siber alanda ırkçılık ve yabancı düşmanlığı ile mücadele hedeflenmiştir. Bu ek protokol 1 Mart 2006’da yürürlüğe girmiştir. Ek Protokolün tam metni için bkz. Additional Protokol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, <http://conventions.coe.int/Treaty/en/Treaties/Word/189.doc>.

⁹³ Bkz. 185 numaralı Sözleşme, Başlangıç bölümü.

⁹⁴ Marie-Theres TINEFELD ve diğ., s. 105.

⁹⁵ Bkz. **Opinion 4/2001 On the Council of Europe’s Draft Convention on Cybercrime**, Article 29 Data Protection Working Party, 22 Mart 2001, 5001/01/EN/Final WP 41, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp41en.pdf. Ayrıca bkz. International Working Group on Data Protection in Telecommunications **Common Position on data protection aspects in the Draft convention on cyber-crime of the Council of Europe**, 13-14 Eylül 2000, http://www.datenschutz-berlin.de/attachments/218/cy_en.pdf.

2009 Temmuz ayı itibariyle Sözleşme’yi 46 devlet imzalamış, 26 devlet ise onaylama sürecini tamamlamıştır. Bu anlamda Sözleşme’nin önemli bir etki alanına kavuştuğu söylenebilir. Sözleşme hükümlerinin somut olaylarda uygulanması kaçınılmaz olarak kişisel veriler ile ilişkili olduğundan, verilerin işlenmesinde bireylerin haklarına dikkat edilmesi önemli bir gerekliliktir. Bu bağlamda, özellikle amaç ile eylem arasındaki dengenin, bir başka anlatımla orantılılığın ve amaç ile sınırlılığın sağlanması, soruşturulan etkinlik ile ilgisi olmayan üçüncü kişilerin haklarının korunması gibi konulara dikkat edilmelidir⁹⁶.

Bu sorunlara karşın AK’nin kişisel verilerin korunmasına ilişkin farkındalığı arttırmak yönünde önemli çalışmaları bulunduğu da belirtilmelidir. Yapılan araştırmalar, Avrupa yurttaşlarının büyük bir bölümünün kişisel verilerinin korunmasına ilişkin haklarını yeterli oranda bilmediğini ortaya koymaktadır⁹⁷. Oysa kişisel verilerin korunmasının tam anlamıyla sağlanabilmesi için hukuksal düzenlemelerin yanında, bireylerin de haklarının neler olduğu ve bunları nasıl kullanacakları konusunda bilgilendirilmeleri gerekir⁹⁸.

Bu düşünceden hareketle AK bünyesinde, Avrupa yurttaşlarında konuya ilişkin bilinçlenme sağlamayı amaçlayan çalışmalar yürütülmektedir⁹⁹. Örneğin, AK,

⁹⁶ Ayrıca bkz. International Working Group on Data Protection in Telecommunications, **Recommendation on the Implementation and Application of the Council of Europe Convention No.185 on Cybercrime (a.k.a. “Budapest Convention”)**, 4 Mart 2008, http://www.datenschutz-berlin.de/attachements/218/cy_en.pdf.

⁹⁷ Avrupa Barometresi’nin, 17 Nisan 2008’de açıkladığı araştırması, Avrupa yurttaşlarının verilerin korunmasına ilişkin haklarını tam olarak bilmediklerini bir kez daha ortaya koymuştur. Bkz. “Eurobarometer survey reveals that EU citizens are not yet fully aware of their rights on data protection”, MEMO/08/249, 17 Nisan 2008, <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/249&format=HTML&aged=0&language=EN&guiLanguage=en>.

⁹⁸ Nitekim AK Genel Sekreteri Terry DAVIS da 2009 yılı Veri Koruma Günü’nde yaptığı açıklamada bu soruna işaret etmiştir. Bkz. 3. Data Protection Day, Statement by Terry Davis, Secretary General of the Council of Europe, 28 Ocak 2009, http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/DPD/DPD2009/Statement_CoE_2009_en.pdf.

⁹⁹ Nitekim yapılan araştırmalar bu yönde girişimlerin oldukça önemli ve gerekli olduğunu ortaya koymaktadır. Avrupa Barometresi’nin 2008 yılında açıkladığı bir araştırma bu durumu açıkça ortaya koymaktadır. Yirmi yedi AB üyesi ülkede 15 yaşının üzerindeki 27.000 kişiyle yapılan görüşmeler sonucunda elde edilen istatistikler, araştırmaya katılanların üçte ikisinin kişisel verilerin korunmasına ilişkin endişeleri bulunduğunu ve büyük bir çoğunluğunun (%82) İnternet’te paylaştıkları kişisel verilerin güvenliği konusunda kaygıları bulunduğunu ortaya koymaktadır. Buna karşın, Avrupa yurttaşları bazı veri koruma düzenlemeleri hakkında genel olarak bilgi sahibi olmakla birlikte, yalnızca dörtte biri Avrupalıların bu hakların tamamından yararlanabildiğini bilmektedir. “Eurobarometer survey reveals that EU citizens are not yet fully aware of their rights on data protection”, MEMO/08/249, 17 Nisan 2008,

AB Komisyonu’nun da desteğiyle, 2007 yılında ilk kez 108 sayılı Kişisel Verilerin Korunması Sözleşmesi’nin imzaya açıldığı gün olan 28 Ocak’ı Veri Koruma Günü olarak ilan etmiştir. Her yıl bu tarihte, kişisel verilerin korunmasına ilişkin çeşitli toplantılar, eğitim ve yurttaşları konuya ilişkin olarak bilinçlendirme amacı taşıyan başka bazı etkinlikler düzenlenmektedir¹⁰⁰.

2. Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme

a. Sözleşmenin konusu ve uygulama alanı

AK, 28 Ocak 1981 tarihinde 108 numaralı “*Kişisel Verilerin Otomatik İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme*”yi imzaya açmıştır¹⁰¹. Bu Sözleşmenin üye ülkelerin hukuk sistemleri üzerinde çok sınırlı bir etkisi olduğu kimi yazarlarca belirtilse de¹⁰² önemini ve güncelliğini halen korumasına neden olan bazı özellikleri dikkatten kaçmamalıdır.

Birincisi Sözleşme, AK üyesi olmayan devletlerin de imzasına açıktır. Bu nedenle, yalnızca üye devletler için değil¹⁰³, Sözleşme’ye taraf olan üçüncü ülkeler

<http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/249&format=HTML&aged=0&language=EN&guiLanguage=en>.

¹⁰⁰ Veri Koruma Günü kapsamında çeşitli devletlerde düzenlenen etkinlikler ve konu hakkında daha ayrıntılı bilgi almak için bkz. http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/Default_DP_Day_en.asp#TopOfPage. AK’nin veri koruma gününe benzer uygulamaların dünyanın çeşitli yerlerinde kabul edildiği görülmektedir. Bunun bir örneği Asya-Pasif bölgesinde 2006’dan beri her yıl düzenlenen Özel Yaşamın Gizliliği Farkındalık Haftasıdır. Bkz. <http://www.privacyawarenessweek.org>. Buradaki amaç, AK veri koruma gününde olduğu gibi kişisel verilerin korunmasına ilişkin farkındalığı arttırmaktır. Her ikisi de bölgesel nitelikte olan bu girişimlerin yanında çeşitli ülkelerde ulusal düzeyde benzer etkinlikler yapılmaktadır. Kapsamlı kişisel verilerin korunması düzenlemeleri bulunmayan ABD’de her yıl Amerikan Sağlık Bilgileri Yönetimi Derneği’nce düzenlenen Sağlık Bilgilerinin Gizliliği ve Güvenliği Haftası örnek olarak gösterilebilir. Bkz. <http://www.ahima.org/hipsweek/>. Bunun yanında, 30. Veri Koruma ve Özel Yaşamın Gizliliği Denetçileri Konferansı’nda küresel düzeyde geçerli olacak bir kişisel verilerin korunması gününün ya da haftasının saptanması için gereken çalışmaların yürütülmesi yönündeki kararını açıklanmıştır. Resolution to explore establishing an International Privacy/Data Protection Day or Week, 30. International Conference of Data Protection and Privacy Commissioners, Strasbourg, 17 Ekim 2008, http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_explore_establishing_en.pdf.

¹⁰¹ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Sözleşme, 1 Ekim 1985 beş devletin onaylama işlemini tamamlamasıyla yürürlüğe girmiştir. 1 Mayıs 2009 tarihine kadar Sözleşme’nin onaylama sürecini 41 devlet tamamlamıştır. Rusya, Türkiye ve Ukrayna ise Sözleşme’yi imzalamış ancak onaylama işlemini henüz gerçekleştirmemiştir. Bkz. <http://conventions.coe.int>.

¹⁰² Viktor MAYER-SCHÖNBERGER, s. 220.

¹⁰³ Örneğin Birleşik Krallık’ta özel yaşamın gizliliği hakkını koruyan herhangi bir yasal düzenleme ya da “common law” kuralı bulunmamasına karşın, Avrupa Konseyi’nin sözleşmesine uyum

için de konuya ilişkin bir çerçeve sunmaktadır. İkinci olarak Sözleşme, halen kişisel verilerin korunması alanında bağlayıcı olan tek uluslararası metindir¹⁰⁴. Bu nedenle konuya ilişkin en önemli kaynaklardan biri olma özelliğini sürdürmektedir.

AK bünyesinde AİHS Sözleşmesi gibi etkili bir metin bulunurken, kişisel verilerin korunmasına ilişkin özel bir Sözleşme'nin kabul edilme nedeni merak edilebilir. Öncelikle AİHS'de kişisel verilerin korunması bağımsız bir hak alanı olarak düzenlenmediği, yalnızca 8. maddede özel yaşamın gizliliği hakkının güvence altına alındığı hatırlatılmalıdır. Bu nedenle, aşağıda inceleneceği üzere, kişisel verilerin korunmasına yönelik ilkelerin ne oranda Sözleşme kapsamında görüldüğünü saptamak için AİHM'nin kararlarına başvurmak gerekir. Bu noktada çalışmamızın birinci bölümünde yapılan açıklamalar hatırlanmalıdır.

Yeni ancak hızla gelişen bir alan olarak kişisel verilerin korunması konusunda özel bazı düzenlemelere ve bu bağlamda yeni araçlara gereksinim duyulmaktadır. Bunun özel yaşamın gizliliği hakkının korunmasına yönelik geleneksel kurallarla sağlanabilmesi pek de olanaklı görülmemektedir. Nitekim AK Verilerin Korunması Sözleşmesi kabul edilirken de AİHS bünyesindeki güvencelerin sınırlı kalacağını düşünülüğünü belirtmek gerekir. Ayrıca özel sektörde kişisel verilerin bilgisayar ortamında işlenmesi durumunda AİHS'nin yeterli oranda güvence sağlayıp sağlayamayacağını da açık olmadığına işaret edilmelidir¹⁰⁵. 108 numaralı Kişisel Verilerin Korunması Sözleşmesi ile bu boşluğun doldurulması hedeflenmiştir¹⁰⁶. Nitekim Sözleşmenin amacı taraf devletlerde her gerçek kişinin temel hak ve özgürlüklerini ve özellikle kişisel bilgilerinin otomatik bilgi işleme tabi tutulması karşısında özel yaşamın gizliliği haklarını, kısacası kişisel verilerinin korunmasını güvence altına almaktır¹⁰⁷.

AK Sözleşmesinin koruma kapsamında hem kamusal hem de özel sektör tarafından işlenen veriler bulunur¹⁰⁸. Bununla birlikte yalnızca otomatik yolla işlenen veriler için güvence öngörüldüğünden, elle işlenen veriler kapsam dışında

sağlamak amacıyla 1984 yılında veri koruma yasası yürürlüğe girmiştir. Robert BOND, s. 138; Peter CAREY, **Data Protection, A Practical Guide to UK and EU Law**, Oxford University Press, 2. Baskı, Büyük Britanya 2004, s. 3.

¹⁰⁴ Bkz. "Privacy versus Information", http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/background/12Presentation.asp#TopOfPage (s.y. 12 Nisan 2009).

¹⁰⁵ Lee A. BYGRAVE, **Data Protection Law**, s. 123-124.

¹⁰⁶ Marie-Theres TINEFELD ve diğ., s. 100 vd.; Oğuz ŞİMŞEK, s. 21.

¹⁰⁷ Bkz. AK Verilerin Korunması Sözleşmesi, m.1.

¹⁰⁸ Bkz. AK Verilerin Korunması Sözleşmesi, m. 3/1.

kalmaktadır. Ancak bunu mutlak bir dışlama olarak düşünmemek gerekir. Nitekim Sözleşme’ye göre “*otomatik işleme*”den söz edebilmek için sürecin tamamının otomatik olması gerekmemekte, kısmen otomatik işlenen veriler de güvenceden yararlanmaktadır¹⁰⁹. Bu, Sözleşme’nin uygulama alanını oldukça genişletmektedir¹¹⁰.

Sözleşme uyarınca, taraf devletler kendi ülkelerinde bulunan herkes için geçerli olacak şekilde bu metinde yer alan ilkeleri iç hukuk düzenlerinin bir parçası durumuna getirmelidir. Bu yalnızca bir öneri değil, bir yükümlülüktür. Sözleşme uyarınca, her taraf devlet, en geç bu Sözleşme kendisi açısından yürürlüğe girinceye kadar, burada yer alan ilkelere etkinlik kazandırmak için kendi ulusal hukukunda gerekli düzenlemeleri yapacaktır¹¹¹.

b. Sözleşmenin Kapsamı

Sözleşme ile kişisel verilerin korunmasına yönelik “*asgari*” gereklilikler belirlenmiştir. Bu nedenle taraf devletlerin daha geniş bir koruma getirmesinin önünde herhangi bir engel bulunmamaktadır¹¹². Sözleşmede belirlenen temel ilkeler şöyle sıralanabilir:

- *Verilerin belirli bir nitelikte olması* (m.5): Buna göre otomatik olarak işlenecek kişisel verilerin meşru ve yasal yoldan elde edilmesi ve işlenmesi; belirli ve meşru amaçlar için tutulması ve bunlarla bağdaşmayan amaçlar için kullanılmaması; bu amaçlar için yalnızca ilgili ve gerektiği kadar verinin saklanması; doğru ve gerektiğinde güncel olması; ilgili kişinin kimliğini

¹⁰⁹ Bkz. m.1, 2/c. Açıklayıcı Rapor’da da veri işleme teknolojilerindeki hızlı gelişim dikkate alınarak Sözleşmenin 2/c hükmünde “*otomatik veri işleme*” deyimine yorumlamaya olanak tanıyacak şekilde oldukça geniş bir tanım verildiği belirtilmektedir. Bkz. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 185, Explanatory Report**, (bundan sonra “açıklayıcı rapor” olarak anılacaktır) <http://conventions.coe.int/Treaty/en/Reports/Html/108.htm> . Her ne kadar burada, büyük olasılıkla, yeni teknoloji ürünlerinin de kapsama alınması ilk hedef olarak belirlenmişse de, Sözleşme’nin kabul ediliş amacı dikkate alındığında “*kısmi otomatik işleme*”yi de geniş yorumlama kapsamında düşünmenin önünde bir engel görülmemektedir.

¹¹⁰ Bunun yanında bir taraf devletin Sözleşme’nin uygulama alanını genişlettiğini belirtmesi de olanaklıdır. Sözleşme’nin otomatik veri işleme kapsamına girmeyen kişisel veri dosyaları hakkında da uygulanacağı bildirilebileceği gibi (m.3/2,b), gerçek kişiler yanında topluluklar, dernekler, vakıflar, şirketler, tüzel kişiliğe sahip olan ya da olmayan ve gerçek kişileri doğrudan ya da dolaylı olarak bünyesinde toplayan diğer kuruluşlarla ilgili bilgiler de kapsam dâhiline alınabilir (m. 3/2,c).

¹¹¹ Bkz. m.4. Nitekim Türkiye Sözleşmeyi 28 Ocak 1981 tarihinde imzalamış olmasına karşın, halen iç hukukta gereken düzenlemeler yapılmadığı için Sözleşmenin onaylanması işlemi tamamlanmamıştır.

¹¹² Bkz. m.11.

belirtecek şekilde amaç için gerekli olandan uzun süre saklanmaması, kısaca “kaliteli” olması gerekir.

- *Hassas kişisel verilerin özel olarak korunması* (m.6): Kişilerin ırksal kökenleri, siyasal düşünceleri, dinsel inançları gibi hassas veriler ilgili devletin ulusal hukukunda uygun güvenceler sağlanmadığı takdirde otomatik olarak işlenemez.

- *Veri güvenliği* (m.7): Verilere yetkisiz erişimin, bunların değiştirilmesinin ya da ortadan kaldırılmasının önlenmesi için veri güvenliği sağlanmalıdır.

- *İlgili kişinin bilgi alma, verilere ulaşma ve gerektiğinde onları düzeltme hakkı* (m. 8): İlgili kişinin kendisine ilişkin otomatik olarak işlenmiş veriler hakkında bilgi alma, eğer bu veriler hukuka aykırı bir şekilde işlenmişse onları sildirtme, yanlış verileri düzeltme, eğer bu taleplerine uyulmazsa hukuksal yollara başvuru hakkı bulunmaktadır.

Sözleşmede bu hakların kullanımına bazı sınırlamalar getirildiği görülmektedir. Ancak burada sınırlamanın sınırlarına da yer verilmiştir. Buna göre, sınırlamalar ancak yasa ile devletin ya da kamunun güvenliği, devletin ekonomik çıkarlarının korunması, suçlarla mücadele veya ilgili kişinin ya da başkalarının hak ve özgürlüklerinin korunması amacıyla ve eğer demokratik bir toplumda gerekli ise yapılabilir¹¹³. Burada AIHS’nin özel yaşamın gizliliği hakkını düzenleyen 8. maddesinin 2. fıkrasındaki sınırlamalara koşut bir düzenleme getirildiği görülmektedir.

Sözleşme ayrıca, taraf devletler arasında kişisel verilerin serbest aktarımını öngörmektedir. Buna göre taraf devletler arasında, özel yaşamın gizliliğinin korunması gerekçesiyle, veri aktarımı yasaklanamaz ya da özel bir izne tabi tutulamaz¹¹⁴. Ancak bu kurala iki durumda istisna getirilmiştir: (i) belirli veri kategorileri için özel bir koruma getirilmiş olması ve aktarımın yapılacağı Sözleşmecî devlette buna “eşdeğer” korumanın bulunmaması veya (ii) aktarımın Sözleşme’nin tarafı olmayan üçüncü bir devlet aracılığıyla yapılacak olması¹¹⁵.

¹¹³ Bkz. AK Sözleşmesi, m. 9.

¹¹⁴ Bkz. AK Sözleşmesi, m.12/1,2. Bu, başka gerekçelere dayanarak (örneğin gizli ticari bariyerler gibi) veri aktarımında bulunmak istemeyen devlete karşı bu hükme sığınılmasını engelleyici bir ifadedir. Bkz. Açıklayıcı Rapor, par. 67.

¹¹⁵ Bkz. AK Sözleşmesi, m.12/3.

Sözleşme ile bu metinde yer alan hükümleri yorumlamaktan ve uygulamaları geliştirmekten sorumlu bir Danışma Komitesi de oluşturulmuştur. Komitede Sözleşmeciler devletlerin temsilcileri yanında, belirli koşulların gerçekleşmesi durumunda, AK üyesi olan ya da olmayan başka devletlerden gözlemcilerin bulunması da olanaklıdır¹¹⁶. Bu Komite'nin bir diğer görevi, kişisel verilerin korunmasına ilişkin raporlar hazırlamak ve rehber ilkeler geliştirmektir. Bu kapsamda özellikle belirli sektörlerle ilişkin tavsiye kararları yayınlanmıştır¹¹⁷.

Danışma Komitesi, 108 sayılı Sözleşme'ye yaptığı bir ekle buradaki ilkelere Avrupa Topluluklarının da uymasına olanak tanımıştır. Bu değişiklik ile AB düzenlemeleri ile uyumluluk hedeflenmiş ve orijinal metninde yalnızca devletlerin taraf olabildiği Sözleşme'ye Avrupa Topluluklarının da taraf olabilmesi sağlanmıştır¹¹⁸.

Danışma Komitesi'nin bir başka önemli etkinliği ise 108 numaralı Sözleşme'ye ek bir Protokol kabul etmesidir¹¹⁹. Bu Protokol ile Sözleşme'deki önemli bir eksiklik giderilmeye çalışılmış ve veri işleme etkinliklerini denetleyecek bağımsız bir organ öngörülmüştür. Ancak belirtmek gerekir ki Ek Protokol'ün bağımsız bir veri koruma organı kurulmasına ilişkin hükümleri özgün değildir, büyük oranda AB'nin aşağıda incelenecek 95/46/AT sayılı Yönergesi ile koşuttur¹²⁰. Protokol'de ayrıca Sözleşme'nin üçüncü ülkelere veri aktarımına ilişkin hükümlerinin geliştirildiği de görülmektedir. Yine AB Yönergesine benzer bir

¹¹⁶ Bkz. m.18.

¹¹⁷ Biyometrik verilerin toplanması ve işlenmesinde 108 numaralı Sözleşme'de belirlenen ilkelerin uygulanmasına ilişkin gelişme raporu örnek olarak gösterilebilir. Raporun tam metni için bkz. **Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data**, 2005, http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/.

¹¹⁸ AK Bakanlar Komitesi tarafından 15 Haziran 1999 tarihinde uygun bulunan ve Sözleşme'nin kimi hükümlerinde değişiklik öngören bu metin bütün Sözleşmeciler devletlerin onayı ile yürürlüğe girecektir. Sözleşmeye ek hükümler ve açıklayıcı beyan için bkz. http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/.

¹¹⁹ 181 sayılı Ek Protokol, imzaya 8 Kasım 2001'de açılmış ve beş taraf devletin onaylaması ile 1 Temmuz 2004'te yürürlüğe girmiştir. 1 Mayıs 2009 itibarıyla 23 devlet onaylamış, aralarında Türkiye'nin de bulunduğu 14 devlet ise imzalamış ancak onaylama sürecini henüz tamamlamamıştır. Bkz. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=1&DF=&CL=E> NG.

¹²⁰ Bkz. Ek Protokol m. 1.

şekilde Protokol ile “yeterli” düzeyde veri koruma sağlamayan üçüncü ülkelere kişisel verilerin aktarımı yasaklanmaktadır¹²¹.

Çalışmamızın çeşitli yerlerinde belirttiğimiz üzere, kişisel verilerin korunması dinamik bir alandır ve AK Kişisel Verilerin Korunması Sözleşmesi’nin 1981 yılında kabul edilmesinden bu yana, kişisel verilerin korunmasına ilişkin sorunlar çeşitli açılardan değişime uğramıştır. AK Sözleşmesi, belirli bir sektöre hasredilmiş bir metin değildir. Dolayısıyla yeni gelişen alanlarda ya da otomatik veri işlemenin 1980’li yıllardan bugüne çok daha kapsamlı bir şekilde kullanılmaya başladığı sektörlerde Sözleşme’de belirlenen ilkelere uyulması gerekir. Ancak bu uygulamaların şekil ve araçları farklılaşabilir. Bankacılık, sigortacılık, reklamcılık, sosyal güvenlik, bilimsel araştırmalar, işyeri etkinlikleri, telekomünikasyon gibi farklı sektörlerin kimilerinde ilkelerin daha esnek uygulanması gerekebilir. Kimilerinde ise işin niteliği gereği kendiliğinden düzenleme gibi yöntemlerin daha etkin sonuç vereceği düşünülmektedir. Bütün bu değerlendirmeleri dikkate alan AK, Sözleşme’ye Ek Protokoller kabul etmektense daha kolay bir yolu seçmiş ve Bakanlar Komitesi Tavsiye Kararları ile ulusal yasa koyuculara ve uygulayıcılara yol göstermeye çalışmıştır¹²². Bunlar Sözleşme’deki ilkeleri destekleyici ve geliştirici bir nitelik taşımaktadır¹²³.

3. Avrupa İnsan Hakları Sözleşmesi

a. Genel Olarak

AK bünyesinde kişisel verilerin korunmasına ilişkin düzenlemeler incelenirken dikkate alınması gereken bir diğer önemli metin Avrupa İnsan Hakları Sözleşmesi’dir¹²⁴. AİHS, imzaya açıldığı 1950 yılından bugüne, insan hakları alanında en önemli kaynaklardan biri olma özelliğini korumaktadır¹²⁵.

¹²¹ Bkz. Ek Protokol m. 2.

¹²² Bu konuya ilişkin olarak bkz. http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/background/11Background.asp#TopOfPage. AK Bakanlar Komitesi tarafından hazırlanan bu tavsiye kararlarında sağlık veri bankalarının düzenlenmesinden sigorta amacıyla kişisel verilerin toplanması ve işlenmesine kadar çok çeşitli alanların yakından incelendiği ve öneriler geliştirildiği görülmektedir. Bkz. http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/.

¹²³ Lee A. BYGRAVE, “Privacy Protection in a Global Context”, s. 335.

¹²⁴ Bundan böyle “AİHS” veya “Sözleşme” olarak anılacaktır.

¹²⁵ Sözleşmenin tam adı “İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi”dir. Sözleşme 4 Kasım 1950’de Roma’da imzalanmış, 3 Eylül 1953’de on devletin onaylama sürecini tamamlaması ile yürürlüğe girmiştir. Türkiye Sözleşme’ye ilk imzalayan devletlerden biridir,

Öncelikle AİHS’nde kişisel verilerin korunmasının bağımsız bir hak alanı olarak yer almadığını hatırlatmak gerekir. Ancak Sözleşme’nin 8. maddesinde özel yaşamın gizliliği hakkı düzenlenmiştir¹²⁶. AİHS’nin “Özel ve aile yaşamına saygı hakkı” kenar başlıklı 8. maddesi şu hükmü içerir:

“1. Herkes özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önelenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda gerekli olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir”.

Görüldüğü gibi AİHS’nin 8. maddesi dört alanda koruma getirmektedir: kişinin (i) özel yaşamı, (ii) aile yaşamı, (iii) evi ve (iv) haberleşmesi¹²⁷. Özel yaşamın korunması hakkı bu dört alan içerisinde en geniş kapsamlı olanıdır¹²⁸. Bu kapsama kişisel verilerin korunmasına ilişkin temel ilkelerin dâhil olup olmadığını saptayabilmek için Avrupa İnsan Hakları Mahkemesi’nin¹²⁹ (ve 11. Protokol

ancak onaylama süreci 18 Mayıs 1954’te tamamlanmıştır. Bu tarihten itibaren Türkiye’nin Sözleşme’ye taraf olmaktan kaynaklı yükümlülükleri işlerlik kazanmıştır. AİHS’nin kurduğu sisteme ilişkin ayrıntılı bilgi için bkz. Mehmet Semih GEMALMAZ, s. 965 vd.

¹²⁶ AİHS’nin 6, 10 ve 13. maddeleri başta olmak üzere başka bazı hükümleri de kişisel verilerin korunması ile ilgili içtihatların oluşmasına kaynaklık edebilir. Ancak konumuz açısından merkezi öneme sahip hüküm 8. maddede yer almaktadır. Bkz. Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy in Human Rights Treaties”, **International Journal of Law and Information Technology**, C.6, S.3, s.254, d.n.55.

¹²⁷ Mahkeme, önüne gelen somut olaylardaki değerlendirmesinde bu dört koruma alanına ilişkin her zaman kesin bir ayırım belirlememektedir. Bu somut olayların nitelikleri dolayısıyla da kaçınılmaz bir sonuçtur. Nitekim bu deyimler, öz olarak “özel yaşam”ın çeşitli unsurlarını oluşturmaktadır ve iç içe geçmiş bir niteliktedir. Bunun bir sonucu birine ilişkin düşüncelerin diğerleri için de geçerli olmasıdır. Feyyaz GÖLCÜKLÜ, Şeref GÖZÜBÜYÜK, s. 333. Örneğin gizli telefonların dinlemesi konusunda, “özel yaşam” yanında “haberleşme” de ön plana çıkmaktadır. AİHM de “telefon görüşmeleri” 8. maddenin 1. fıkrasında açıkça belirtilmese de bu deyimmin yine aynı hüküm içerisinde yer alan “özel yaşam” ve “haberleşme” deyimlerinin kapsamında bulunduğunu belirtmiştir. Bkz. *Klass ve diğ., Almanya’ya karşı*, b.n. 5029/71, k.t. 6 Eylül 1978, par. 41. Ayrıca bkz. *Malone, Birleşik Krallık’a karşı*, b.n. 8691/79, k.t. 2 Ağustos 1984, par. 64.

¹²⁸ Robert UERPMANN-WITTZACK, “Personal Rights and Prohibition of Discrimination”, **European Fundamental Rights and Freedoms**, haz. Dirk EHLERS, Ulrich BECKER, De Gruyter Rechtswissenschaften Verlags-GmbH, Almanya 2008, s. 68, par. 3.

¹²⁹ Bundan böyle “AİHM” veya “Mahkeme” olarak anılacaktır.

öncesindeki sistem açısından Avrupa İnsan Hakları Komisyonu'nun¹³⁰) kararlarına başvurmak gerekir.

b. AİHS m.8/1 Hükmü Kapsamında Kişisel Verilerin Korunması

Hemen belirtelim: AİHM, özellikle 1980'li yılların ortalarından beri ve gittikçe artan bir yoğunlukta, kişisel verilerin korunmasını, Sözleşme'nin sağladığı güvenceler kapsamında değerlendirmiştir¹³¹. Nitekim Mahkeme'nin bireysel özerkliği ve bilgilerin geleceğini belirleme hakkını, 8. madde ile getirilen güvencelerin yorumlanmasında önemli bir temel ilke olarak belirlediği görülür¹³². Bu bağlamda AİHM, bireylerin kişisel verilerinin kullanımı ve kaydı konusunda denetim hakkının bulunduğunu kabul etmektedir¹³³.

AİHM'nin kişisel verilerin korunmasını 8. madde kapsamında görmesi oldukça önemlidir¹³⁴ ancak, buradaki yorumunun belirli açılardan sınırlı kalmaya

¹³⁰ Bundan böyle “AİHK” veya “Komisyon” olarak anılacaktır. AİHS'nin ilk şeklinde koruma sistemi iki organdan oluşmaktaydı: Avrupa İnsan Hakları Komisyonu ve Avrupa İnsan Hakları Mahkemesi. Bu dönemde denetim süreci Komisyon'a başvuru ile başlıyor ve Komisyon başvuruları “*kabul edilir*” bulduğu takdirde denetim sisteminin ikinci ve üçüncü organı olan Mahkeme ve Bakanlar Komitesi devreye giriyordu. Ancak daha sonra 1 Kasım 1998 tarihinde yürürlüğe giren 11. Protokol ile denetim sistemi önemli ölçüde değiştirilmiştir. 11. Protokol Komisyon ve Mahkeme'yi birleştirmiş ve bunun sonucunda denetim sistemi tek organlı duruma gelmiştir. Aşağıda incelenecek kararlarda, 11. Protokol öncesi dönemde verilmiş kararlar açısından Mahkeme yanında ikinci bir organ olarak Komisyon'dan da söz edilmesi bu nedenledir.

¹³¹ Lee A. BYGRAVE, “Where have all the judges gone? Reflections on judicial involvement in developing data Protection law”, **Privacy Law and Policy Reporter**, Y. 2000, C. 7, s. 11- 14, 33- 36, http://folk.uio.no/lee/oldpage/articles/Judges_role.pdf, s. 4.

¹³² Bkz. *Pretty, Birleşik Krallık'a karşı*, b.n. 2346/02, k.t. 29 Temmuz 2002, par. 61.

¹³³ Paul De HERT, Serge GUTWIRTH, “Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action”, **Reinventing Data Protection**, haz. Serge GUTWIRTH, Yves POULLET, Cécile de TERWANGNE, Sjaak NOUWT, Springer 2009, s.19.

¹³⁴ Kişisel verilerin korunmasına ilişkin AİHM'nin geliştirdiği içtihat bir kaç açıdan önemlidir. Öncelikle konuya ilişkin pek çok metinde AİHS'ne atıf yapıldığı görülür. Bu durumda kişisel verilerin korunmasına ilişkin çeşitli ulusal ve uluslararası metinlerin yorumlanmasında AİHM içtihatlarının da dikkate alınması gerektiği söylenebilir. Fakat AİHM'nin etkisi bununla da sınırlı kalmamaktadır. Bu durum AB mevzuatı açısından kendini açıkça gösterir. Aşağıda incelenecek 95/46/AT sayılı Kişisel Verilerin Korunması Yönergesi, AB ülkelerinde kişisel verilerin korunması alanında uyumlaştırmayı hedefleyen ve bu konuda kabul edilmesi gereken asgari koşulları belirleyen bir metindir. Ancak 1 Aralık 2009 tarihinde Lizbon Antlaşması yürürlüğe girmeye kadar uygulaması sınırlıdır. Nitekim Sözleşme yürürlüğe girmeden önce AB'nin üçüncü sütununda düzenlenen konular Yönerge'nin kapsamı dışında kalmaktaydı. Oysa AİHM'nin kararları konusunda böylesine bir ayırım yoktur. Dolayısıyla üçüncü sütun içerisinde yer alan adli ve cezai konularda işbirliği alanında da AİHM'in kararlarını dikkate almak gerekecektir. İkinci olarak, AB üyesi olmayan, AK'nin 108 sayılı Sözleşmesini de kabul etmemiş olan ancak AİHS tarafı devletler açısından da AİHM'nin kararları oldukça önemlidir. Bu noktada Türkiye örneği düşünülebilir. Türkiye, AİHS'nin tarafıdır. Ayrıca 1982 Anayasasının 90/5 hükmü uyarınca bu Sözleşme yasa hükmünde olduğu gibi, yasalarla arasında bir uyumsuzluk olması durumunda da Sözleşme hükümleri esas alınacaktır. Türkiye'de kişisel verilerin

mahkûm olduğu unutulmamalıdır. Öncelikle burada taraf devletlerin organlarının işlenen verilere yönelik bir koruma getirilmektedir. Bu nedenle, özel kişilerce ya da özel sektörde işlenen verilerin koruma kapsamında olup olmadığı tam anlamıyla açık değildir¹³⁵.

İkincisi AİHS'nin kabul edildiği 1950 yılında kişisel verilerin korunmasına ilişkin tartışmalar henüz gelişmediğinden, Sözleşme'de kişisel verilerin korunmasının özel gerekliliklerine ilişkin bir düzenleme bulunmamakta, koruma alanı yalnızca AİHM'nin "özel alan"a ilişkin yorumları çerçevesinde geliştirilebilmektedir¹³⁶. Bu bağlamda Mahkeme'nin Sözleşme'yi günün koşulları içerisinde yorumlama görevini üzerinde görmesine karşın¹³⁷, yine de hareket alanının

korunmasına yönelik bir yasanın bulunmadığı dikkate alındığında AİHM kararlarında saptanana ölçütlerin ne derece önemli olduğu sanırsanız daha iyi anlaşılabilir.

¹³⁵ AİHS'nin 8. maddesinin kimler tarafından gerçekleştirilen müdahalelere karşı bir güvence getirdiğinin saptanması oldukça önemlidir. Bilindiği gibi AİHM'ne başvurular, Sözleşme hüküm ya da hükümlerini ihlal ettiği iddia edilen taraf devlete karşı yapılır. Bu bağlamda devlet organları eliyle gerçekleştirilen eylem ve işlemler şüphesiz bu kapsamda değerlendirilir. Ancak bunun yanında, AİHM'nin de çeşitli kararlarında işaret ettiği üzere, Sözleşme'nin 8. maddesinde güvence altına alınan hak, taraf devletlere yalnızca kişilerin özel yaşamlarına müdahale etmeme gibi negatif bir yükümlülüğü değil, özel yaşamın gizliliğini sağlayacak önlemleri almayı, yani pozitif bir yükümlülüğü de getirmektedir. Buna göre taraf devlet, bu hakların fiilen ve gerçekten kullanılmasına olanak tanıyacak tedbirleri almalıdır. *Leander, İsveç'e karşı*, b.n. 9248/81, k.t. 26 Mart 1987; *Gaskin, Birleşik Krallık'a karşı*, b.n. 10454/83, k.t. 7 Temmuz 1989; *Airey, İrlanda'ya karşı*, b.n. 6289/73, k.t. 9 Ekim 1979 ; Feyyaz GÖLCÜKLÜ, Şeref GÖZÜBÜYÜK, s. 332. Bu yorum, en azından bazı koşullar altında, koruma altına alınan haklara karşı özel kişi ya da kurumlardan gelecek müdahalelerde de devletin sorumlu tutulmasını olanaklı kılar. Örneğin, X ve Y'nin Hollanda'ya karşı yaptığı başvuru üzerine verdiği kararda Mahkeme, "(Devletin) buradaki yükümlülükleri, bireylerin arasındaki ilişki alanında da özel yaşama saygıyı koruyacak önlemlerin kabulünü de içermektedir" ifadesine yer vermiştir. *X ve Y, Hollanda'ya karşı*, b.n. 8978/80, k.t. 26 Mart 1985, par.23; Andrew CLAPHAM, **Human Rights in Private Sphere**, Oxford University Press, ABD 1996, s. 212-214; Francis G. JACOBS, Robin C. A. WHITE, s. 174. Özel veri bankalarının ve kişisel verilerin satılmasının hak ve özgürlükler açısından ciddi sorunlar yarattığı açıktır. Buna, özel kişi ya da kurumlarca yapılan gizli dinlemeler, işverenlerin çalışanların özel yaşamlarına müdahale oluşturacak çeşitli etkinlikleri de eklenebilir. Mahkeme kararlarında bu ve benzer örneklerin tamamına yönelik kapsamlı ve açık cevaplar bulmak henüz olanaklı değildir. Ancak devletin pozitif yükümlülüğüne ilişkin yukarıda belirtilen içtihadından hareketle bu türdeki eylemleri önleyecek yasal düzenlemeleri ihmal etmiş devletin doğrudan sorumlu tutulabileceği söylenebilir. Ayrıca bkz. Andrew CLAPHAM, s. 215.

¹³⁶ AİHM yargıçlarından Pettiti, bir kararda yer alan mutabık görüşünde bu değişimi şu şekilde dile getirmiştir: "1950'de özel hayata müdahale teknikleri hala antikti; müdahale deyiminin içerik ve etkisinin bu dönemdeki anlamı, günümüzdeki anlamına üstün kabul edilemez". Bkz. *Malone, Birleşik Krallık'a karşı*, b.n. 8691/79, k.t. 2 Ağustos 1984, Concurring Opinion of Judge Pettiti.

¹³⁷ Kişisel verilerin korunması hakkının 8. madde kapsamında değerlendirilmesi, Sözleşme hükümlerinin yorumlanmasında yeni gelişmelere açık bir bakışın hâkim olduğunun da göstergesidir. Nitekim AİHM'ne göre Sözleşme, "güncel koşullar ışığında yorumlanması gereken yaşayan bir enstrüman"dır. Bkz. *Tyrer, Birleşik Krallık'a karşı*, b.n. 5856/72, k.t. 28 Nisan 1978, par. 31. Mahkeme'nin görevi, Sözleşme'yi yorumlarken sosyal değişimleri de yansıtmaktır. Bkz. *Cossey, Birleşik Krallık'a karşı*, b.n. 10843/84, k.t. 27 Eylül 1990, par. 35. AİHM'nin çeşitli kararlarında da belirttiği üzere, Sözleşme ile güdülen amaç, hakların hayali ya da teorik olarak değil, etkili ve elverişli bir şekilde güvence altına alınmasıdır. "Balancing

sınırlı kalmaya mahkûm olduğu söylenebilir. Mahkeme, kaçınılmaz olarak bu konuda önüne gelen her bir başvuruda ilk olarak somut olayın özel yaşamın kapsamında yer alıp almadığını değerlendirmektedir. Bunun sonucu, konuya ilişkin değerlendirmelerin her bir başvurunun kendi özel koşulları ile sıkı sıkıya bağlı olmasıdır. Bu durumda ise hem genel kuralların belirlenmesi güçleşmekte¹³⁸, hem de Mahkeme'nin “*özel alan*” dışında gördüğü konular, koruma kapsamının dışında kalmaktadır¹³⁹. Bu, verilerin korunmasında hakim olan temel ilkelerin bir bütün olarak bu kabul edilip edilmediğini de belirsiz kılmaktadır¹⁴⁰.

AİHM (ve 11. Protokol öncesinde AİHK ile birlikte) önüne gelen olaylarda üç aşamalı bir inceleme yapmaktadır. Buna göre;

- (i) Başvuru konusu olayın 8/1 hükmünün koruma kapsamında olan kavramlardan birine (özel yaşam, aile yaşamı, konut veya haberleşme) dâhil bulunup bulunmadığı incelenmekte;
- (ii) Olayın AİHS'nin 8/1 hükmü kapsamında görülmesi durumunda yapılan işlem ya da alınan önlemin bu hükme bir müdahale oluşturup oluşturmadığı değerlendirilmekte ve son aşama olarak da;
- (iii) İşlem veya önlemin müdahale teşkil ettiğine karar verilirse, bunun 8/2 hükmü çerçevesinde meşruluk kazanıp kazanmadığı saptanmaktadır¹⁴¹.

Öncelikle “*özel yaşam*”ın tanımlanmasının oldukça güç bir kavram olduğunu belirtmek gerekir. Zorluk özellikle kamusal alan ile özel alan arasındaki sınırların belirsizliğinden kaynaklanır. Bu ise her somut olayda olayın kendi

Security and Liberty Within the European Human Rights Framework, A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11”, **Security and Civil Liberties**, haz. Antonie M. HOL, John A. E. VERVAELE, Intersentia, İngiltere 2005, s.45. Bu bağlamda 1969 Viyana Antlaşmalar Hukuku Sözleşmesi'ni de dikkate almak gerekir. Antlaşmanın 31/1 hükmüne de uygun olarak, Mahkeme ve Komisyon, AİHS'ni yorumlarken metnin temel hedef ve amaçlarına ağırlık vermiştir. Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s.255.

¹³⁸ Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s. 255.

¹³⁹ Mahkeme, “*özel yaşam*” ile ilgisini dikkate alarak kişisel verileri, 8. maddenin kapsamında değerlendirilenler ve değerlendirilmeyenler olmak üzere ikiye ayırmıştır. Mahkeme'ye göre kimi kişisel veriler, “*özel yaşam*” kapsamında değerlendirilemeyeceğinden, Sözleşme'nin koruma alanından da yararlanamayacaktır. Bu türdeki bir ayırım, kişisel verilerin korunması mevzuatında görülmemektedir.

¹⁴⁰ Örneğin kişilerin yanlış verileri sildirme hakkının 8. maddede korunan özel yaşamın bir parçası olarak görülüp görülmediği henüz açık değildir. Paul J. A. De HERT, s. 46-48.

¹⁴¹ Feyyaz GÖLCÜKLÜ, Şeref GÖZÜBÜYÜK, s. 331.

koşullarına göre bir değerlendirme yapma zorunluluğunu beraberinde getirir. Mahkeme'nin çeşitli kararlarında özel yaşamı kişinin özel yaşamının iç çemberi dışında başkaları ile ilişki kurduğu alanları da kapsar şekilde yorumladığı görülmektedir¹⁴².

Bu yorum, kişisel verilerin korunması açısından önemli sonuçlar getirir. Öncelikle Mahkeme'nin özel yaşamı kişinin mahrem alanı ile sınırlı görmemesi kişinin ev telefonu yanında, iş telefonunun dinlenmesinin 8. maddenin korumasından yararlanmasını sağlar¹⁴³. Bunun yanında örneğin, bir kişinin kamusal bir alanda görüntüsünün kayıt edilmesi de korumadan yararlanacaktır¹⁴⁴.

¹⁴² Mahkeme, "... "özel hayat" kavramının kapsamlı bir tanımını yapmanın ne mümkün, ne de gerekli olduğunu düşünmektedir. Ancak, bu kavramı bireyin kendi özel hayatını istediği gibi yaşayabileceği bir "iç alan" ile kısıtlamak ve bu alandan söz konusu alanın içinde olmayan dış dünyayı olduğu gibi hariç tutmak aşırı kısıtlayıcı olur". Bkz. Niemietz, Almanya'ya karşı, par. 29; çeviri için bkz. Gilles DUTERTRE, s. 285. Komisyon ise bu yaklaşımı şu şekilde ifade etmiştir: "(Özel yaşama saygı hakkı), bir kişinin kendi kişiliğini geliştirmesi ve gerçekleştirmesi için, özellikle duygusal alanda diğer insanlarla ilişkiler kurma ve geliştirme hakkını da belirli bir düzeyde içermektedir". X, İzlanda'ya karşı, b.n. 6825/74, 18 Mayıs 1976. Mahkeme, özel yaşamın dış dünyadaki diğer insanlarla ilişki kurma ve bu ilişkiyi geliştirmeyi de kapsadığını daha sonra pek çok kararında yinelemiştir. Örneğin bkz. Z., Finlandiya'ya karşı, par. 66. Bu husus, AİHS'nin 8 ile 10. maddeleri arasındaki bağlantıyı da ortaya koymaktadır. P. Van DİJK, G.J.H. Van HOOFF, **Theory and Practice of the European Convention on Human Rights**, Kluwer Law International, Hollanda 1998, s. 490.

¹⁴³ Örneğin bkz. Niemitz, Almanya'ya karşı, b.n. 13710/88, k.t. 16 Aralık 1992, par. 29; Halford, Birleşik Krallık'a karşı, par. 42- 46; Rotaru, Romanya'ya karşı, par. 43. Mahkeme, bir avukatın bürosunun aranmasına ilişkin olan Niemietz kararında kişilerin iş yaşamlarını "özel yaşam" alanı kapsamında gördüğünü açıkça ortaya koymuştur. Mahkeme'ye göre "Özel yaşama saygı hakkı, belirli düzeyde başka kişilerle ilişki kurma ve bunu geliştirme hakkını da kapsamalıdır. Ayrıca, "özel yaşam" deyiminin bu anlamından profesyonel veya iş mahiyetindeki etkinliklerin dışlanması gerekliliği konusunda temelde herhangi bir neden bulunmamaktadır. Çünkü her şeyden öte, insanların büyük bir bölümü, dış dünyayla ilişkilerini geliştirme konusunda, en önemli değilse, önemli bir olanağa iş yaşamları sırasında kavuşmaktadır. Bu yaklaşım, Komisyon tarafından da doğru bir biçimde işaret edildiği üzere, kişinin profesyonel veya iş yaşamını oluşturan etkinlikleri ile bu kapsamda olmayanlar arasında açık bir ayrım yapmanın her zaman olanaklı olmaması gerçeği ile desteklenmektedir"(par. 29). Daha sonra Mahkeme, Halford kararında da görüldüğü üzere, bu saptamasını, işyerindeki izleme, dinleme etkinlikleri açısından da sürdürmüştür. Bkz. Halford, Birleşik Krallık'a karşı, b.n. 20605/92, k.t. 25 Haziran 1997.

¹⁴⁴ Kamusal alandaki etkinliklerin ne oranda "özel yaşam" kapsamında değerlendirileceğini Mahkeme çeşitli kararlarında incelemiştir. Friedl kararına konu olan olayda başvuranın fotoğrafları kamusal bir gösteri sırasında alınmıştır. Komisyon'a göre, fotoğraflar kamusal bir eyleme ilişkin bir gösteride alınmaları ve yalnızca o gün güvenliği sağlamak için kullanılmaları dolayısıyla kişinin özel yaşamının iç çemberine ilişkin değildir. Ayrıca burada Komisyon, fotoğrafların anonim olarak bırakıldığına, herhangi bir isim ile ilişkilendirilmediklerine, kayıt edilen verilerin ve çekilen fotoğrafların herhangi bir veri işlem sürecinden geçmediğine ve veri işleme ile fotoğrafları çekilenlerin kimliklerinin belirlenmeye çalışılmadığına dikkat çekmiştir. Bkz. Friedl, Avusturya'ya karşı, b.n. 15225/89, k.t. 31 Ocak 1995. Lupker kararında ise daha önceden kamusal otoritelere gönüllü olarak verilen fotoğrafların öngörülemeyen kullanımı söz konudur. Burada Komisyon, polisin fotoğrafları yalnızca cezai kovuşturma sırasında failleri belirlemek için kullandığına ve fotoğrafların kamuya paylaşılması veya başka amaçlar için kullanılmasına yönelik herhangi bir girişimin bulunmadığına dikkat çekmiştir. Bkz. Lupker ve

Ayrıca Mahkeme'nin günün koşullarının gerisinde kalmama düşüncesini koruma alanı açısından kararlarına yansıtmasının olumlu sonuçlarının bulunduğu belirtilmelidir. Örneğin bu yaklaşımla Mahkeme, geleneksel haberleşme araçlarının yanında modern iletişim araçlarını da koruma kapsamında görmektedir. Bu bağlamda kişilerin İnternet aracılığıyla kurdukları iletişimin, e-postalarının izlenmesi ya da içeriklerinin saptanması da 8. madde çerçevesinde değerlendirilmektedir¹⁴⁵.

AIHM 8. madde çerçevesinde, kişisel verilerin korunması ile ilişkili olarak, ilk önemli kararını Klass ve diğerlerinin Almanya'ya karşı yaptığı başvuru üzerine vermiştir. Bu kararda Mahkeme, gizli telefon dinlemelerini özel yaşam kapsamında değerlendirir¹⁴⁶. Daha sonra verdiği pek çok kararla Mahkeme'nin temel olarak

diğ., Hollanda'ya karşı, b.n. 18395/91, 7 Aralık 1992. Friedl ve Lupker kararlarında Komisyon, fotoğrafların başvuranın özel yaşamına ne oranda müdahale oluşturduğuna, fotoğrafların kamusal mı yoksa özel konularla mı ilişkili olduğuna, toplanan verilerin sınırlı kullanımının mı tasarlandığı yoksa kamunun ulaşılabilirliğinin mi sağlandığı gibi sorulara önem vermiştir. Mahkeme, kamusal alanda kapalı devre televizyon sistemleriyle yapılan kayıtları da değerlendirmiştir. Bkz. Peck, Birleşik Krallık'a karşı, b.n. 44647/98, k.t. 28 Nisan 2003. AIHM'ne göre kamusal alanların kişilerin görüntülerini alan araçlarla izlenmesi ancak bu görüntülerin kayıt edilmemesi durumunda özel yaşama müdahale söz konusu değildir. Ancak verilerin kayıt edilmesi ve bu kaydın sistemli ya da kalıcı olarak yapılması bu durumu değiştirir (par. 59).

¹⁴⁵ Örneğin Copland kararına Mahkeme, başvuranın iş telefonundan yaptığı görüşmelerin gizliliğine ilişkin “*makul bir beklenti*” içerisinde olmasının doğal olduğuna, aynı beklentinin e-posta ve İnternet kullanımı açısından da geçerli olduğuna işaret etmiştir. Bkz. Copland, Birleşik Krallık'a karşı, par. 42.

¹⁴⁶ *Klass ve diğ., Almanya'ya karşı*, b.n. 5029/71, k.t. 6 Eylül 1978. *Klass ve diğerleri* kararına konu olan olayda başvuranlar, Alman Anayasası'nın 10/2 hükmünün ve bu hükmeye dayanılarak çıkartılan Mektup, Posta ve Telekomünikasyonun Gizliliğinin Sınırlandırılması Yasası'nın (kısaca G-10 yasası olarak adlandırılmaktadır) Sözleşme'ye aykırı olduğunu ileri sürmüşlerdir. Buna göre başvuru sahiplerinin itirazı devletin bir yasayla denetim önlemleri alması değildir. İtiraz, kendilerini bilgilendirme yükümlülüğü bulunmaksızın, haberleşmelerini ve telefon görüşmelerini izleyebilme ve kendileri hakkında önlemler alabilme yetkisinin getirilmesinden ve bu uygulamaya karşı da mahkeme önünde hak arama özgürlüğünün tanınmamasından kaynaklanmaktadır (par. 10). Her ne kadar AIHS sisteminde “*actio popularis*” yani halkın hakkını arama tanınmasa da doğrudan mağdur oldukları belirli olmayan başvuranlar hem Komisyon, hem de Mahkeme'nin görüşüyle “*potansiyel mağdur*” olarak kabul edilmiştir. AIHM bu yorumunu daha sonra başka kararlarında da yinelemiştir. Örneğin Malone kararında, Mahkeme'ye göre başvuran, telefon görüşmelerini kimlerle yaptığına ilişkin bilginin devlet organlarıncı elde edilebilmesine olanak tanıyan uygulama dolayısıyla “*kendisine karşı somut bir işlemin yapılmasından ayrı olarak, ... sırf bu uygulamanın varlığı nedeniyle, Sözleşme'nin 8. maddesinin ihlalinden ötürü 25. madde bakımından ‘mağdur’ olduğunu iddia edebilir*”. Bkz. Malone, Birleşik Krallık'a karşı, b.n. 8691/79, k.t. 2 Ağustos 1984, par. 86. Bu, özellikle izleme ve dinlemenin doğası gereği gizli gerçekleştirilen etkinlikler olmaları dolayısıyla önemlidir. Bu karar, dinlendiğine ilişkin elinde somut bir bilgi bulunmayan kişinin, kendisini potansiyel mağdur konumuna düşüren bir yasal düzenlemeye ilişkin itirazını AIHM önünde dile getirebileceği anlamına gelir. Henüz Mahkeme içtihatlarında örneği bulunmasa da bir İSS'nin kullanıcının hangi siteleri ziyaret ettiğini ya da cep telefonu operatörünün abonesinin yer bilgilerini hükümet organları ile paylaşma potansiyel tehlikesini üzerinde hisseden kişinin durumunun da bu kapsamda değerlendirilebileceğini söyleyebiliriz. Bu açıdan bakıldığında, Klass davası

konumuza ilişkin önemli bazı ilkeleri Sözleşme'nin 8. maddesi kapsamında değerlendirdiğini görmekteyiz.

Buna göre:

- Bireylere ilişkin kişisel bilgilerin resmi makamlarca toplanarak arşivlenmesi¹⁴⁷;
- Telefon görüşmelerine ilişkin kayıtları izleme¹⁴⁸;
- Toplanan verilerin toplanma amacı dışında kullanılması¹⁴⁹;
- Sağlık verilerinin gizliliği¹⁵⁰;
- Emniyet güçleri tarafından parmak izi ve fotoğrafların alınması¹⁵¹;
- Kişisel verilere erişim hakkı¹⁵²;
- Kişisel verilerin gerektiğinden uzun süre tutulması¹⁵³ gibi konular

Mahkeme'nin çeşitli kararlarında 8/1 hükmü kapsamında değerlendirilmiştir. Bunun yanında Mahkeme'nin içtihadı uyarınca “*özel yaşam*”, kimlik hakkını¹⁵⁴ ve 8. maddedeki güvencelerin yorumlanmasında oldukça önemli olan, kişilik¹⁵⁵ ve bireysel özerklik ilkeleri dolayısıyla¹⁵⁶, kişisel gelişim hakkını da kapsamaktadır¹⁵⁷.

Ancak belirtmek gerekir: AIHM, konuya ilişkin pek çok kararında, m.8/1'in ihlalini 2. fıkra hükümleri uyarınca meşru görmüştür¹⁵⁸. Buna karşın hangi konuları “*özel yaşama saygı hakkı*” kapsamında değerlendirdiğini saptamak, en az Mahkeme'nin somut olaylarda ihlale ilişkin verdiği karar kadar önemlidir. Nitekim Mahkeme'nin Sözleşme'nin 8/1 hükmü kapsamında özel yaşama müdahale olarak değerlendirdiği bir durumun, 8/2 hükmünde yer alan koşullara uygun olarak meşruluk kazanmadığı durumlarda ihlal kararının doğacağı açıktır.

bağlamında geliştirilen yorum, kişisel verilerin korunması açısından ciddi kazanımlar yaratabilecek niteliktedir.

¹⁴⁷ *Amann İsviçre'ye karşı*, b.n. 27798/95; k.t. 16 Şubat 2000; *Rotaru Romanya'ya karşı*, b.n. 28341/95, k.t. 4 Mayıs 2000.

¹⁴⁸ *Malone, Birleşik Krallığa karşı*, b.n. 8691/79, k.t. 2 Ağustos 1984; *P.G. ve J.H., Birleşik Krallığa karşı*, b.n. 44787/98, k.t. 25 Eylül 2001 .

¹⁴⁹ *Leander, İsviçre'ye karşı*, b.n. 9248/81, k.t. 26 Mart 1987.

¹⁵⁰ *Z., Finlandiya'ya karşı*, b.n. 22009/93, k.t. 25 Şubat 1997; *M.S., İsveç'e karşı*, b.n. 20837/92, k.t. 27 Ağustos 1997.

¹⁵¹ *Murray, Birleşik Krallık'a karşı*, b.n. 14310/88, k.t. 28 Ekim 1994.

¹⁵² *Gaskin, Birleşik Krallık'a karşı*, b.n. 10454/83, k.t. 7 Temmuz 1989.

¹⁵³ *S. ve Marper, Birleşik Krallığa karşı*, b.n. 30562/04, 30566/04, k.t. 4 Aralık 2008.

¹⁵⁴ *Wisse, Fransa'ya karşı*, b.n. 71611/01, k.t. 20 Aralık 2005, par. 24.

¹⁵⁵ *Christine Goodwin, Birleşik Krallık'a karşı*, b.n. 28957/95, par. 90.

¹⁵⁶ *Evans, Birleşik Krallık'a karşı*, b.n. 6339/05, par. 71.

¹⁵⁷ *Reklos ve Davourlis, Yunanistan'a karşı*, b.n. 1234/05, k.t. 15 Nisan 2009, par. 39.

¹⁵⁸ Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s. 270.

c. AİHS m. 8/2 Kapsamında Müdahalenin Meşruluğu

AİHS'nin 8. maddesinde düzenlenen özel yaşama saygı hakkının sınırları, aynı maddenin 2. fıkrasında yer alır. Bu özel yaşama saygı hakkına bir müdahale olduğu saptandığında, Mahkeme bu müdahalenin meşruiyet kazanıp kazanmadığını değerlendirir. Bu değerlendirme 2. fıkrada belirlenen koşul ve ölçütlere uygunluk açısından yapılmaktadır.

AİHS 8/2 hükmü uyarınca özel ve aile yaşamına müdahale, (i) burada sınırlı sayımla belirtilmiş amaçlardan bir ya da bir kaçına yönelik; (ii) yasada öngörülmüş ve (iii) aynı zamanda demokratik toplum için gerekli ve öngörülen amaç ile orantılı olması durumunda meşrudur.

Sınırlı sayımla belirlenen ve özel ve aile yaşamına saygı hakkına istisna getiren meşru amaçlar şunlardır: ulusal güvenlik; kamu güvenliği; ülkenin ekonomik refahı; dirlik ve düzenin korunması; suç işlenmesinin önlenmesi; sağlığın veya ahlakın veya başkalarının haklarının korunması. Görüldüğü gibi meşru amaçlar oldukça geniş bir şekilde belirlenmiştir. O kadar ki herhangi bir müdahalenin burada belirlenen meşru amaçları karşılayamaması oldukça zordur¹⁵⁹.

Mahkeme, çeşitli kararlarında ayrıntılı bir değerlendirme yapmaya gerek görmeden müdahalenin milli güvenlik ve/veya suçluluğun önlenmesi hedeflerine yöneldiğini saptamıştır¹⁶⁰. Bazı kararlarında ise, bunların yanında müdahalenin “başkalarının haklarının korunması” gibi meşru bir amaca da yöneldiğine karar vermiştir¹⁶¹.

Özel yaşama yönelik müdahalelerde ulusal güvenliğin ve kamu güvenliğinin korunmasına yönelik gerekçeler öne çıkmaktadır. Mahkeme, suçlulukla, özellikle de organize suçlar ve terörizmle, mücadelenin günümüzde Avrupa toplumlarının karşı karşıya kaldığı önemli bir sorun olduğuna işaret etmektedir¹⁶². Bu bağlamda Mahkemenin özellikle terörle mücadele amacıyla gerçekleştirilen müdahalelere daha

¹⁵⁹ Dirk EHLERS, Ulrich BECKER, s. 75; Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s. 270.

¹⁶⁰ *Leander, İsveç’e karşı*, par. 49; *P.G. ve J.H., Birleşik Krallık’a karşı*, par. 49; *Murray, Birleşik Krallık’a karşı*, par. 89.

¹⁶¹ *Niemietz, Almanya’ya karşı*, par. 36; *Z., Finlandiya’ya karşı*, par. 76; *Pretty, Birleşik Krallık’a karşı*, par. 69. Bu noktada şu husus da dikkatten kaçmamalıdır: Mahkeme, müdahaleye ilişkin olarak hükümetin ileri sürdüğü gerekçenin inandırıcılığını da dikkate almıştır. Örneğin Copland kararında, hükümetin okul yönetiminin yaptığı izlemenin daha ileri ve yüksek bir eğitim sağlama amacıyla “gerekli ve yararlı herhangi bir şeyi” yapma düşüncesinden kaynaklandığına yönelik iddiasını inandırıcı bulmamıştır. *Copland, Birleşik Krallık’a karşı*, par. 34, 47.

¹⁶² *S. ve Marper, Birleşik Krallık’a karşı*, par. 105.

ılımlı baktığı söylenebilir¹⁶³. Ancak bu hedefe yönelik etkinliklerde de demokratik toplum düzeninin gerekliliklerine vurgulanmıştır¹⁶⁴.

Müdahalenin yasal temelini bulunması ile ise resmi makamların keyfi müdahalelerini önlemek amaçlanmıştır¹⁶⁵. Bunun yanında Mahkeme'nin yerleşmiş içtihadı uyarınca bu hukuksal temel yalnızca bulunması yeterli değildir; ayrıca bunun ulaşılabilir ve öngörülebilir olması da gerekir¹⁶⁶. Mahkeme yasal düzenlemenin kalitesine ilişkin gerekliliği, müdahalenin ağırlığı ile bağlantılı olarak değerlendirmektedir¹⁶⁷. Ayrıca “yasa ile öngörülme” kuralının karşılanabilmesi için ulusal hukukta dava yollarının ve güvencelerin sağlanması gerektiğine de işaret edilmiştir¹⁶⁸.

¹⁶³ Sultan ÜZELTÜRK, s. 193.

¹⁶⁴ Bu noktada Klass ve diğ. kararında Mahkeme'nin saptaması şu şekildedir: “*Demokratik toplumlar son zamanlarda kendilerini casusluğun ve terörizmin hayli gelişmiş biçimlerinin tehdidi ile karşı karşıya bulmuşlardır. Bu da Devletin, bu tür tehditlerle etkin bir biçimde müdahale edebilmek için kendi egemenlik alanı içinde faaliyet gösteren yıkıcı unsurları gizli izlemeye almasını gerektirmiştir. Bu nedenle, Mahkeme'nin istisnai koşullar çerçevesinde mektup, posta ve telekomünikasyon üzerinde gizli izleme yetkisi veren bir yasanın, ulusal güvenlik nedeniyle ve/veya suç ve düzensizliği önlemek için demokratik bir toplumda gerekli olduğunu kabul etmesi gerekir*” (par.48, çev. için bkz. Osman DOĞRU, s. 259). Ancak AİHM aynı kararda bu müdahalenin sınırlarına da işaret etmiştir. Buna göre Mahkeme: “... bunun Sözleşmeciler Devletin kendi yetki alanındaki kişileri gizli izlemeye tabi tutmasında sınırsız takdir yetkisi olduğu anlamına gelmeyeceğini vurgular. Mahkeme, böyle bir yasanın onu savunma adına demokrasiyi zedeleme, hatta onu ortadan kaldırma tehlikesini içerdiğinin bilincinde olarak, sözleşmeciler devletlerin, casusluk ve terörizmle mücadele adına uygun gördükleri her türlü önlemleri alamayacaklarını kabul eder¹⁶⁴. Mahkeme, hangi izleme sistemi benimsenirse benimsensin, kötüye kullanmaya karşı yeterli ve etkili güvencelerin bulunduğuna ikna olmalıdır. Bu değerlendirmenin yalnızca göreceli bir niteliği vardır. Değerlendirme, olası önlemlerin niteliğine, kapsamına ve süresine; bu önlemleri emretmek için gerekli sebeplere; bu önlemler için emri veren, uygulayan ve denetleyen yetkili makamlara ve ulusal hukukta tanınan iç hukuk yollarının türü gibi, olayın bütün koşullarına dayanır”(par.50).

¹⁶⁵ Feyyaz GÖLCÜKLÜ, Şeref GÖZÜBÜYÜK, s. 375. Burada “yasa” ile münhasıran yasama organının tasarruflarının kastedilmediği, İngilizce “law” (yasa/hukuk) deyiminin geniş anlamıyla değerlendirildiği görülmektedir. Bu nedenle yasa yanında, diğer düzenleyici tasarruflar ve Anglo-sakson hukukundaki yazılı olmayan hukuk kuralları da bu kapsamdadır. *Sunday Times, Birleşik Krallık'a karşı*, par. 47; *Kruslin ve Huvig Fransa'ya karşı*, par. 29; *Kopp, İsviçre'ye karşı*, par. 60; *Malone, Birleşik Krallık'a karşı*, par. 66. Feyyaz GÖLCÜKLÜ, Şeref GÖZÜBÜYÜK, s. 376; Dirk EHLERS, Ulrich BECKER, s. 75.

¹⁶⁶ Yasanın ulaşılabilirliği ilkesi, vatandaşların bu hukuk kuralının varlığı konusunda yeterli bilgiye sahip olmasını, öngörülebilirlik ise, yasaların açıklığını gerektirir. Buna göre, yasa, eğer gerekli ise danışma ile, ilgili kişinin somut olayda belirli bir hareketinin ne tür sonuçlar doğurabileceğini makul bir düzeyde öngörebilmesini sağlamalıdır. *Sunday Times, Birleşik Krallık'a karşı*, par. 49; *Silver ve diğ. Birleşik Krallık'a karşı*, par. 87-88; *Malone, Birleşik Krallık'a karşı*, par. 66.

¹⁶⁷ Örneğin Mahkeme'ye göre, “*telefon görüşmelerinin dinlenmesi özel yaşama ve haberleşmeye ciddi bir müdahale oluşturur ve özellikle açık bir “yasa”ya dayalı olmak zorundadır. Konuya ilişkin kuralların açık ve ayrıntılı olması, özellikle kullanılan teknoloji gittikçe daha karmaşık bir hale geldiğinden, mutlak bir gerekliliktir*”. *Kruslin, Fransa'ya karşı*, par. 33; *Huvig, Fransa'ya karşı*, par. 32; Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s. 271.

¹⁶⁸ Bkz. *Kruslin, Fransa'ya karşı*, b.n. 11801/85, 24 Nisan 1990; *Huvig, Fransa'ya karşı*, b.n. 11105/84, 24 Nisan 1990. Bu kararlarda Mahkeme Fransız hukuk sistemini değerlendirmiş ve şu

Mahkeme'ye göre yasada suistimallere karşı uygun güvenceler belirlenmelidir¹⁶⁹. Buna göre yasada en azından müdahalenin usulü ve koşulları saptanmış olmalıdır. Telefon dinleme, gizli gözetim ve haberalma, DNA, hücre örnekleri ve parmak izi alınması gibi etkinliklerin amacına ve uygulama şekline ilişkin ayrıntılı kurallar ve asgari güvencelerin belirlenmesi gerekir. Bunlar içerisinde belirtilen yollarla elde edilen bilgilerin tutulma süresi, depolanması, kullanılması, üçüncü kişilerce erişimi, doğruluğunun ve gizliliğinin korunması, yok edilmelerine ilişkin usullerin belirlenmesi gibi konulara ilişkin kurallar bulunmalıdır. Bu idarenin keyfi müdahalelerine ve bu bilgilerin kötüye kullanılmasına karşı bir güvence sağlayacaktır¹⁷⁰. Mahkeme'nin kimi kararlarında işaret ettiği bir diğer güvence ise özel yaşamın gizliliğini ihlal edecek etkinlikleri izleyecek bağımsız bir denetim organının bulunmasıdır¹⁷¹.

AIHM, özel ve aile yaşamına müdahalenin meşruluğunu incelerken üçüncü olarak bunun demokratik bir toplumda gerekli olup olmadığı sorusuna yanıt arar. Buna göre müdahalenin meşru olduğundan söz edebilmek için 8/2 hükmünde sınırlı sayıda belirtilen amaçlardan birine yönelmesi ve yasal bir temeli bulunması yanında demokratik bir toplum için gerekli olması da bir zorunluluktur. Ancak Mahkeme'nin genellikle bu son değerlendirmeye kuşkulu ve isteksiz yaklaştığı görülmektedir. Somut olaydaki müdahalenin demokratik bir toplumda gerekli olup olmadığı sorusunu Mahkeme çoğu zaman yanıtsız bırakmış, diğer iki koşuldan birinin gerçekleşmediği durumlarda bir de bu üçüncü koşul açısından değerlendirme

saptamada bulunmuştur: “(Fransız sistemi) zamanında çeşitli muhtemel suistimallere karşı **yeterli güvence** sağlamamaktadır. Örneğin, mahkeme kararı ile telefonları dinlemekten sorumlu olacak kişi grupları ve böyle bir emre neden olabilecek suçların niteliği hiçbir yerde tanımlanmamıştır. Yargıcı telefon dinlemelerin süresini belirlemede sınırlayacak bir zorunluluk bulunmamaktadır. Benzer şekilde, müdahale edilen görüşmeyi içeren özet raporların tanzim usulü; orjinal bantların sayısını ve uzunluğunu zorlukla doğrulayacak, yargıç ve savunma tarafından gerçekleştirilecek muhtemel inceleme için kayıtların tam ve bütünlük içerisinde iletilmesini sağlayacak önlemler; özellikle zanlının yargıç kararı ile tahliye edilmesi veya mahkeme tarafından beraat edilmesi hallerinde, kayıtların silinmesini veya teyblerin yok edilmesini gerektirecek durumlar belirlenmemiştir”. Kruslin, Fransa'ya karşı, par. 35; Huvig, Fransa'ya karşı, par. 34; P. Van DIJK, G.J.H. HOOF, s. 536.

¹⁶⁹ Iain CAMERON, 34.

¹⁷⁰ Kruslin, Fransa'ya karşı, par. 33, 35; Rotaru, Romanya'ya karşı, par. 57-59; S. ve Marper, Birleşik Krallık'a karşı, par. 99.

¹⁷¹ Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s. 275.

yapmamıştır. Bu bağlamda şüphesiz müdahalenin yasal bir temele dayanıp dayanmadığının saptanması daha güvenli bir yoldur¹⁷².

Mahkeme içtihadında “gerekli” deyimini “zorlayıcı toplumsal gereksinim” (pressing social need) ve yöneldiği amaç ile “orantılılık” a karşılık gelmektedir¹⁷³. Mahkeme, bunun belirlenmesinde üye devletlere bir “takdir marjı” tanır¹⁷⁴. Bu gerekliliğin saptanmasında Mahkeme’nin yetkisi ikincildir. Mahkemeye göre “ülke ve toplum gerçekleriyle dolaysız ve devamlı temasta olan ulusal merciler” ilk olarak bu değerlendirmeyi yapar¹⁷⁵. Ancak bu takdir yetkisi sınırsız olmayıp Sözleşme organlarının denetimine tabidir.

Takdir yetkisinin kapsamı, her somut olayda ayrı ayrı değerlendirilir ve Mahkeme burada çeşitli unsurları dikkate alır. Müdahalenin ciddiliği, müdahaleye neden olan meşru amacın önemi, ilgili hak ve özgürlüğün niteliği bunlardan bir kaçıdır¹⁷⁶. Bu durumda hassas verilerin işlenmesinde demokratik toplum için gereklilik koşulunun daha katı bir şekilde uygulanacağı söylenebilir¹⁷⁷.

Özellikle son yıllarda hem Avrupa’da hem diğer bölgelerde güvenliğe ilişkin kaygıların yükselmesinin, temel hak ve özgürlüklere yönelik sınırlamaların artmasında etkili olduğu görülmektedir. Son dönemde pek çok devlet, “*demokratik bir toplumda gereklilik*” ölçütünü ihmal eden uygulamalar içerisinde¹⁷⁸. Bu bağlamda hem ulusal hem uluslararası alanda kişisel verilerin korunmasına ve özel yaşamın gizliliği hakkına çeşitli açılardan müdahaleyi öngören hukuksal düzenlemelerdeki artış da dikkat çekicidir.

¹⁷² Paul De HERT, Serge GUTWIRTH, s. 20.

¹⁷³ Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s. 273; Paul De HERT, Serge GUTWIRTH, s. 21-22.

¹⁷⁴ AİHS’nin 8. maddesi çerçevesinde konuya ilişkin bir değerlendirme için bkz. Yutaka ARAI-TAKAHASHI, **The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR**, Intersentia, Birleşik Krallık 2001, s. 60-91. Ayrıca bkz. Howard Charles YUROW, **The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence**, Martinus Nijhoff Publishers, Hollanda 1996.

¹⁷⁵ Feyyaz GÖLCÜKLÜ, Şeref GÖZÜBÜYÜK, s. 378.

¹⁷⁶ S. ve Marper, Birleşik Krallık’a karşı, par. 102; Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s. 273; David John HARRIS, Michael O’BOYLE, Colin WARBRICK, **Law of the European Convention on Human Rights**, Birleşik Krallık 1995, s. 290-301; Pieter DIJK ve diğ., s. 540, Robert UERPMANN-WITZACK, s. 76.

¹⁷⁷ Örneğin, AİHM, Z., Finlandiya’ya karşı kararında bir kişinin HIV taşıyıcısı olup olmadığına ilişkin bilginin “mahrem ve hassas” niteliğine işaret etmiştir. Bu durumda Mahkeme, daha dikkatli bir inceleme yapma gerekliliğini üzerinde görmektedir. Z., Finlandiya’ya karşı, par. 96, Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s. 274. Ayrıca bkz. S. ve Marper, Birleşik Krallık’a karşı, par. 103.

¹⁷⁸ Paul J. A. De HERT, s. 63.

Görüldüğü gibi kişisel verilerin korunmasına ilişkin ilkeler büyük oranda AİHS kapsamında güvence altındadır. Ancak Mahkeme, önüne gelen olaylarda, somut duruma ilişkin yorumunu geliştirirken genel uygulanabilir ilkeler belirleyememiştir. Bunun doğal bir sonucu, yukarıda yapmaya çalıştığımız gibi, dağınık ve çeşitli saptamalardan ortak görüşlerin çıkarılmaya çalışılmasıdır. Bununla birlikte genel olarak, ilgili kişinin izni ya da icazeti olmaksızın kişiliğine ilişkin verilerin işlenmesi, toplanması, verilerin sınırsız ya da gerektiğinden uzun süre tutulması, meşru amacın açık bir şekilde belirtilmemesi ve gereken güvencelerin sağlanması durumunda ihlalin gerçekleştiğini söyleyebiliriz.

Ayrıca Mahkeme'nin kişisel verilerin korunmasına ilişkin yaklaşımının belirli oranda değiştiğini de gözlemlemekteyiz. Mahkeme, konuya ilişkin ilk kararlarıyla karşılaştırıldığında, kişisel verilerin korunması hakkına esas teşkil eden ilkeleri, Sözleşme'nin 8. maddesi kapsamında değerlendirmeye daha istekli görünmektedir. Daha önce de belirttiğimiz gibi burada özel olarak 8. maddenin dinamik yapısını, genel olarak da AİHS'nin yeni gelişmelere açık niteliğini dikkate aldığını söyleyebiliriz.

E. APEC

Dünyanın geri kalanı gibi, Asya-Pasifik ülkeleri de hızla gelişen küresel ticaretin sunduğu olanaklardan yararlanmak istemektedir. Kişisel verilerin korunması ise hem tüketicilerin bu konudaki bilincinin artması, hem AB ve çeşitli uluslararası şirketler gibi yapılanmaların bu konudaki baskısı dolayısıyla, daha önce de işaret edildiği gibi, görünmez ticari ilişkileri açısından oldukça önemlidir¹⁷⁹.

Nitekim Asya-Pasifik ülkelerinde kişisel verilerin genel yasalar ile korunması yönünde ciddi bir eğilimin geliştiği dikkat çekmektedir. Özellikle Asya ülkelerinde elektronik ticareti geliştirme amacıyla ve AB Yönergesinin zorlayıcı hükümleri dolayısıyla Avrupa ile olan veri akışının zedelenmemesini için bu yasaların kabul edildiği görülür¹⁸⁰.

¹⁷⁹ Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., "Data Protection in the Asia Pasific Region", *Computer Law and Security Review*, Y. 2009, S. 25, s. 59.

¹⁸⁰ David BANISAR, "Privacy and Data Protection Around the World", s. 3, <http://www.pcpd.org.hk/english/infocentre/files/banisar-paper.doc> (s.y. 3 Nisan 2009).

Kişisel verilerin korunması açısından bölgesel düzeyde en önemli girişimin Asya-Pasifik Ekonomik İşbirliği Örgütü tarafından gerçekleştirildiğini belirtmek gerekir. 1989 yılında kurulan Asya Pasifik Ekonomik İşbirliği (Asia-Pacific Economic Cooperation-APEC) kendisini, bu bölgedeki ekonomik gelişme, işbirliği, ticaret ve yatırımların en önemli destekleyicisi olarak tanımlamaktadır¹⁸¹. 21 üyesi olan bu örgüt¹⁸², dünya ekonomisinin önemli bir bölümünü temsil etmektedir¹⁸³. Pek çok başka konudaki çalışmaları yanında, APEC son dönemde kişisel verilerin korunması açısından önemli bir girişimde bulunmuş ve Asya Pasifik bölgesinde konuya ilişkin farklılıkları makul bir düzeye indirmek ve verilerin korunması alanında asgari ölçütleri belirlemek amacıyla 2004 yılında bir çerçeve belge kabul etmiştir.

APEC Özel Yaşamın Gizliliği Çerçeve Belgesi (Privacy Framework)¹⁸⁴, AB'nin 1995 yılında kabul ettiği Veri Koruma Yönergesinden sonraki dönemde konuya ilişkin en önemli uluslararası girişim olarak değerlendirilebilir¹⁸⁵. Bu Belge'nin hazırlanması ile APEC üyesi ülkelerin, kişisel verilerin korunması konusunda, AB'nin belirlediği ölçütlerden bağımsız olarak, kendi yaklaşımlarını oluşturmayı amaçladıkları görülmektedir¹⁸⁶. Nitekim aşağıda görüleceği üzere kişisel verilerin korunmasının farklı bir bakışla değerlendirildiği bu belgede, 95/46/AT sayılı Verilerin Korunması Yönergesi'nde olduğu gibi başka bir uluslararası belgede görülmeyen yeni bazı ölçütler geliştirilebilmiştir¹⁸⁷. Ancak bu girişimin ne oranda başarılı olduğu tartışmaya açıktır: pek çok olumlu yönü yanında, oldukça sorunlu yanları da bulunmaktadır.

¹⁸¹ http://www.ekodialog.com/ekonomi_kurumlari/apec_asya_pasifik_ekonomik_isbirligi.html.

¹⁸² APEC üyesi devletler şunlardır: Avustralya, Brunei, Kanada, Endonezya, Japonya, Malezya, Filipinler, Yeni Zelanda, Singapur, Güney Kore, Tayland, ABD, Tayvan, Hong Kong, Çin, Meksika, Papua Yeni Gine, Şili, Peru, Rusya, Vietnam.
http://www.apec.org/apec/about_apec.html.

¹⁸³ Bkz. APEC resmi İnternet sayfası: <http://www.apec.org>.

¹⁸⁴ Asia-Pacific Economic Cooperation, APEC Privacy Framework, 2004/AMM/014rev1, 29 Ekim 2004. Bundan böyle “Belge” ya da “Çerçeve Belge” olarak anılacaktır. Belge'nin tam metni için bkz. http://www.apec.org/apec/news__media/fact_sheets/apec_privacy_framework.html.

¹⁸⁵ **Privacy and Human Rights 2006**, s. 13.

¹⁸⁶ Lee A. BYGRAVE, “International Agreements to Protect Personal Data”, s. 43.

¹⁸⁷ Aşağıda inceleneceği üzere, “zararın önlenmesi ilkesi” tartışmalı niteliğine karşın, kişisel verilerin korunması alanında yeni bir ilke olarak karşımıza çıkmaktadır.

Öncelikle şunu belirtelim: APEC Çerçeve Belgesi üzerinde OECD Rehber İlkeleri'nin etkisi açıkça hissedilmektedir¹⁸⁸. Bu Belge ile güdülen temel amaç, kişisel verilerin yeterli düzeyde korunmasını sağlayacak ilkeler geliştirmek ve bölgedeki ekonomik kalkınmayı sağlamak üzere üye ülkeler arasındaki sınır ötesi veri akışını serbestleştirmektir. Ancak Çerçeve Belge'de belirlenen ilkeler zorlayıcı değildir. Bu metin, üye devletler için yalnızca yol gösterici ilkeler içerir. Bu ilkelere uyum sağlayıp sağlamama ya da bu ilkeleri geliştirme tamamen üye devletlerin takdirine bırakılmıştır¹⁸⁹.

Bunun yanında Çerçeve Belge'nin hazırlandığı alt komisyona Çin Halk Cumhuriyeti, Kanada gibi yaklaşımları birbirinden oldukça farklı olan devletlerin katılımı bölgede konuya ilişkin ortak bir paydada buluşulduğunun belirtisi olarak değerlendirilebilir¹⁹⁰. Bu belki de Belge'nin en olumlu yönünü oluşturur. Asya Pasifik bölgesinde bulunan ülkelerin, genel olarak insan hakları konusundaki yaklaşım farklılıkları, elbette kişisel verilerin korunması gibi özel alanlara da yansımaktadır. Bu durumda Çerçeve Belge, özellikle konuya ilişkin herhangi bir düzenleme öngörmeyen ve böylesine bir düzenleme konusunda hevesli olmayan ülkeleri kişisel verilerin korunması yönünde destekleyici bir metin olarak nitelendirilebilir.

Hedefiyle de bağlantılı olarak, APEC Çerçeve Belgesi, biri kişisel verilerin korunmasında hâkim olacak temel ilkeleri belirleyen, diğeri sınır ötesi veri akışının kurallarını düzenleyen iki ana bölümden oluşur. Ancak Çerçeve Belge'de yer alan ilkelerin, özellikle AB veri koruma sistemi ile karşılaştırıldığında çeşitli açılardan eksik kaldığı görülür. Bu bağlamda öncelikle metinde belirlenen ilkelerin değerlendirilmesi gerekir. Çerçeve Belge'de yer alan dokuz veri koruma ilkesi şunlardır¹⁹¹:

¹⁸⁸ Lisa S. NELSON, "Constructing Policy: The Unsettled Question of Biometric Technology and Privacy", **Privacy and Technologies of Identity, A Cross-Disciplinary Conversation**, haz. Katherine STRANBURG, Daniela Stan RAICU, Springer, ABD 2006, s. 168. (151-173)

¹⁸⁹ Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 60; Lee A. BYGRAVE, "International Agreements to Protect Personal Data", s. 43.

¹⁹⁰ Taslak Alt Komisyonunda şu ülkelerden temsilciler yer almıştır: Avustralya, Kanada, Çin, Hong Kong, Japonya, Kore, Malezya, Yeni Zelanda, Tayland ve ABD. **Privacy and Human Rights 2006**, s. 13.

¹⁹¹ Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 60-61.

- *Zararın önlenmesi ilkesi*: Koruma, kişisel verilerin yanlış toplanmasından ve kötüye kullanılmasından doğabilecek zararların önlenmesini içermelidir¹⁹². “*Zarar ilkesi*” olarak adlandırılabilir bu kural, AB Verilerin Korunması Yönergesi gibi başka önemli metinlerde yer almamaktadır¹⁹³. Bu nedenle bu ilke, APEC Taslağı’na özgün bir nitelik vermektedir. Bu ilkeye göre, kişisel verilerin toplanması, kullanılması ve aktarılması dolayısıyla ortaya çıkabilecek zarar riski ve zararın ciddiyeti, konuya ilişkin yükümlülükler belirlenirken dikkate alınmalı ve giderim de bununla orantılı olmalıdır. Bu durumda iki önemli soru ile karşılaşılır. Birincisi, zarar ile anlatılmak istenilenin tam olarak ne olduğudur. Bu ilke ile zarar, koruma düzeyine ve giderime ilişkin uygulamalarda bir değerlendirme ölçütü olarak değerlendirilmektedir. Oysa “*zarar*” gibi sübjektif bir kavramı, objektif bir ölçüt olarak değerlendirme kapsamına almak oldukça güçtür¹⁹⁴. İkinci olarak, zararın meydana gelmediği durumda korumanın ne olacağı belirsizdir. Kişisel verilerin korunmasını zarar ölçütü ile belirleyen bir sistem hukuksal açıdan “*zarar*” olarak tanımlanacak bir durumun yokluğunda korumanın ortadan kalkmasına neden olacaktır. Nitekim Çerçeve Belge’deki “*kişisel verilerin toplanması, kullanılması veya yayınlanmasından kaynaklanan tehlike, özel yükümlülüklerde dikkate alınmalıdır*” hükmü yer alır. Bu durumda herhangi bir zarar görülüyorsa, diğer ilkelerin uygulamasında da ciddi sorunlarla karşılaşılabilir. Örneğin ilgili kişinin kendisine ilişkin kişisel verilere ulaşma isteğinin, zarar tehlikesinin çok düşük olması nedeniyle, reddedildiği bir durumu düşünelim. Kişinin verilerine ulaşma amacı işlemenin kendisine zarar verip vermeyeceğini öğrenmek olduğunda böylesine bir yaklaşım, bu araştırmanın önünde bir engel oluşturacaktır¹⁹⁵. Bu ise kişisel verilerin korunmasının özü ile bağdaşmamaktadır.

- *Bildirim*: Veri denetçisi, ilgiliye belirli bilgileri içeren bir bildirimde bulunmalıdır. Bu bildirimin, kişisel veriler toplanmadan ya da verilerin

¹⁹² APEC Çerçeve Belgesi’ne özgü olarak gördüğümüz “*zararı önleme*” ilkesini, Google’a özel yaşamın gizliliği konusunda danışmalık yapan Peter Fleisher, yaygınlaştırılması gereken bir ilke olarak değerlendirmiştir. Fleisher’a göre küresel mahremiyet standartları zararın önlenmesi hedefine odaklanmalıdır. Bkz. **Washington Internet Daily**, 15 Kasım 2007.

¹⁹³ Chris POUNDER, “Why the APEC Privacy Framework is Unlikely to Protect Privacy”, s. 2.

¹⁹⁴ Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 61.

¹⁹⁵ Chris POUNDER, s. 3.

toplanma anında veya işlemin gerçekleşmesinden sonra olanaklı bulunan en kısa zamanda sağlanması konusunda makul adımlar atılmalıdır. Bu durumda APEC Taslağı'nda AB Yönergesi'nde olduğu gibi kişisel verilerin toplanmasından önce ya da toplama anında bildirimin bir zorunluluk olmadığını söyleyebiliriz. Olayın kendi koşullarında bazen “*uygun*” olanın toplanmanın ardından yapılan bir bildirim olacağı da söylenebilir¹⁹⁶. Ayrıca Taslak, bu ilkedeki bildirim yükümlülüğünün “*APEC üyesi ekonomilerin konsensusuna dayanmasını*” öngörmektedir. Bu yaklaşım ilgili kişinin çıkarları yerine, ticari yararın önde tutulmasına neden olabilir¹⁹⁷.

- *Toplamanın sınırlandırılması*: Kişisel veri toplamanın yasal ve meşru olması için belirli oranda, özellikle toplama amacıyla bağlı olarak, sınırlandırılması gerekmektedir. Ancak burada Verilerin Korunması Yönergesi'nde olduğu gibi amacı gerçekleştirmek üzere gerekli olandan fazla veri toplanamayacağına ilişkin kurala yer verilmemiştir¹⁹⁸.

- *Kişisel verinin kullanımı*: Kişisel verilerin kullanımı toplama amacı ve buna uygun diğer amaçlar ile sınırlandırılmıştır. Taslak ile kişisel verilerin kullanımına getirilen sınırlandırmanın AB Yönergesi ile karşılaştırıldığında oldukça gevşek olduğu dikkat çekmektedir. Taslak'ta kişisel verilerin kullanımının toplama amacı ve bu amaca uygun ya da bu amaçla ilgili diğer amaçlar ile sınırlandırılması, haklı olarak “*uygun ve ilgili amaçların*” neler olduğu sorusunu akla getirmektedir. İlgili kişinin iznine gerek bulunmaksızın verilerin uygun ve ilgili amaçların meşru görülmesi, kullanım alanının önemli oranda genişlemesine neden olacaktır. Bu durumda pek çok ticari amacın kendiliğinden “*uygun*” hale geleceği ve yasallaşacağı dikkate alınmalıdır¹⁹⁹.

-*Seçim*: Uygun koşullar bulunduğunda bireylere, kişisel verilerinin toplanması, kullanımı ve yayınlanmasında seçim hakkı veren mekanizmalar kurulmalıdır. Bu kuralda elbette ilk dikkat çeken seçim hakkının yalnız “*uygun koşullar bulunduğunda*” tanınmış olmasıdır. Ancak bunun dışında kamusal ulaşılabilir verilere ilişkin herhangi bir seçim hakkının

¹⁹⁶ Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 61.

¹⁹⁷ Chris POUNDER, s. 5.

¹⁹⁸ Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 61.

¹⁹⁹ Chris POUNDER, s. 7.

tanınmadığına, ayrıca ilgili kişinin daha sonra fikrini değiştirmesi durumunda ne olacağına ilişkin yol gösterici bir hüküm içermediğine dikkat çekmek gerekir²⁰⁰. Bunun gibi Taslak, seçim ilkesinin ilgili kişinin verilerinin silinmesi için söz konusu olup olmadığını da belirtmemektedir. Oysa böylesine bir seçeneğin bulunması, özellikle verilerin toplanması zamanında düşük olan risk düzeyinin daha sonra yükselmesi durumunda önem kazanmaktadır²⁰¹.

- *Kişisel verinin tamlığı*: Kişisel veriler doğru, tam ve güncel olmalıdır. Kişisel verilerin güncelliğini yitirmesi durumunda “*erişim ve düzeltme*” ilkesi uyarınca ilgili kişinin bunların silinmesini talep etmesi olanaklıdır. Ancak, kişisel verilerin tutulmasının haklı nedeninin ortadan kalkması halinde bunların silinmesini gerektirecek bir kural bu ilke çerçevesinde belirlenmemiştir²⁰².

- *Güvenlik önlemleri*: Tehlikenin düzeyine ve kişisel verilerin hassasiyetine uygun şekilde güvenlik önlemlerinin alınması gerekmektedir.

- *Erişim ve düzeltme*: Bireylere kişisel verilerin doğruluğunu sağlamak amacıyla onlara ulaşma ve gerekli durumlarda düzeltme olanağı sağlanmıştır. Ancak kişisel verilere erişimin ve bunları düzeltme olanağının AB Yönergesi ile karşılaştırıldığında çok daha fazla istisnası olduğu dikkat çekmektedir. Özellikle erişim ve düzeltme isteğinin gerçekleştirilmesi durumunda ortaya çıkacak yükün ve bu işlemin maliyetinin bireyin kişisel verileri üzerinde oluşan risk ile karşılaştırıldığında orantısız ve mantıksız olması durumunda reddedilmesinin olanaklı bulunması dikkat çekicidir²⁰³. Ayrıca gizli ticari bilgilerin (confidential commercial information-ticari sır) korunması amacıyla

²⁰⁰ Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 61; Chris POUNDER, s. 6.

²⁰¹ Bunun belki en açık ve bilinen örneği olarak 1930’lu yıllarda Almanya’daki Yahudilerin ad ve adreslerinin toplanmasının riski düşük iken ilerleyen yıllarda Nasyonal Sosyalist yönetim altında bu bilgilerin gerçek anlamda yaşamsal önem taşımaya başlaması gösterilebilir. Ancak bunun yanında örnekleri çoğaltmak da olanaklıdır. Nitekim siyasal değişimler yanında teknolojideki gelişim de ilk aşamada ciddi risk taşımayan bazı bilgi gruplarının daha sonra oldukça önemli bir konuma gelmesine neden olabilir. Örneğin İnternet, ilk ortaya çıktığı dönemde sınırlı sayıdaki kişi tarafından kullanılır iken günümüzde oldukça yaygın ve kolay erişilebilir bir konuma yükselmiştir. İnternet ilk ortaya çıktığı dönemde bu ortamda çeşitli kişisel verilerinin yayınlanmasına izin veren bir kişinin maruz kalabileceği zarar ile günümüzdeki kıyaslanamaz. Chris POUNDER, s. 6.

²⁰² Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 61.

²⁰³ Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 61.

ya da yayının “güvenlik riski” yaratması durumunda erişim ve düzeltme isteklerinin reddedilmesi olanaklıdır²⁰⁴.

- *Hesap verilebilirlik*: Veri denetçisi, bu metinde belirlenen ilkelere işlerliğini kazandıracak önlemlerin alınmasını denetlemekten sorumludur. Kişisel veriler aktarılırken, alıcının bilgileri burada belirtilen ilkelere uygun bir şekilde koruyacağı yönünde gereken adımların atılması gerekir.

Görüldüğü gibi Çerçeve Belge’nin veri güvenliği ve veri tamlığına ilişkin hükümleri dışındaki bütün ilkeler özellikle 95/46/AT sayılı Veri Koruma Yönergesi ile karşılaştırıldığında oldukça zayıf kalmaktadır²⁰⁵. Bu ilkelerin önemli bir yenilik getirmediği, çoğunun uluslararası metinlerde yer aldığı, bu ilkeleri asgari düzeyde kabul etmenin AB’nin “yeterli” koruma ölçütünü karşılayamayacak kadar zayıf kalacağı gibi çok çeşitli eleştirilerin ileri sürüldüğü görülmektedir²⁰⁶. Ayrıca kamusal ulaşılabilir verilere ilişkin olarak da metnin oldukça sınırlı bir koruma getirdiği belirtilmelidir²⁰⁷.

Çerçeve Belge’de dikkat çeken bir diğer eksiklik kişisel verilerin saklanması (data retention) ilişkin herhangi bir sınırlama getirmemesidir. Belgeyi hazırlayanların, işlenen kişisel verilere artık gereksinim duyulmaması durumunda veri denetçilerinin bunları sileceklerini bekledikleri düşünülebilir. Ancak kişisel verilerin korunmasına ilişkin, özellikle belirli bir yol kat etmiş Avrupa uygulamasına bakıldığında bu beklentinin gerçeklikle uyuşmadığı kolaylıkla görülebilir²⁰⁸.

Bu noktada metnin verilerin sınırötesi aktarımına ilişkin hükümleri üzerinde de kısaca durmak gerekir. APEC bünyesinde bu Belge’nin hazırlanması sırasında kimi yazarlar, sistemin AB’nin “yeterli” koruma ölçütü karşısında yeni bir blok oluşturabileceğine ilişkin endişelerini dile getirmiştir. Ancak metnin son hali, bundan oldukça uzak bir yapı sergilemektedir.

Kişisel verilerin korunmasına yeni bir uluslararası standart getirmek ya da AB’nin sistemi karşısında bir bloklaşma yaratmaktan öte, APEC Çerçeve Belgesi mevcut metinlerdeki korumanın da oldukça gerisinde kalmaktadır. Metnin son

²⁰⁴ Chris POUNDER, s. 7.

²⁰⁵ Chris POUNDER, s. 3.

²⁰⁶ Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 61.

²⁰⁷ Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 62.

²⁰⁸ Chris POUNDER, s. 7.

halinde oldukça düşük düzeyde belirlenen standart, zorlayıcı hükümlerin ve veri aktarımına ilişkin bağımsız hükümlerin yokluğu bu bağlamda dikkat çekmektedir. Ayrıca APEC Çerçeve Belgesi'nde kişisel verilerin korunması hakkının geride kaldığı, merkeze alınan asıl konunun ise ekonomik kaygılar olduğu söylenebilir²⁰⁹.

Bütün bu nedenlerle APEC Çerçeve Belgesi'nin en olumlu ifadeyle OECD Rehber İlkeleri'ne yaklaşan hükümler getirdiği ve kişisel verilerin korunması konusunda uluslararası alanda geliştirilen en düşük düzeydeki standardı belirlediği söylenebilir²¹⁰. Bütün bu eleştirilere katılmayanlar da bulunmaktadır. Örneğin, 2007 yılı Eylül ayında Google'ın küresel özel yaşamın gizliliği danışmanı Peter Fleischer girişimi “*umut vaat edici*” olarak nitelemiştir. Fleischer'a göre eğer 21 APEC üyesi ülke, kişisel verilerin korunmasına ilişkin ilkeler üzerinde anlaşılırsa benzer ilkeler küresel düzeyde de uygulanabilir²¹¹.

Yukarıda kısaca işaret etmeye çalıştığımız sorunlar dolayısıyla APEC Çerçeve Belgesi, ideal bir standart oluşturma noktasında oldukça gerisindedir. Ancak küresel düzeyde bir model oluşturmaya bile kişisel verilerin korunması konusunda isteksiz olan bazı APEC üyesi ülkeleri etkileyebileceği düşünülebilir²¹². Bu bakımdan APEC Taslak'ının esnek hükümleri, kabulünü de kolaylaştırabilir.

Farklı gerekçelerden hareketle de olsa kişisel verilerin korunmasına ilişkin ulusal düzeyde bir düzenleme getirmemiş Çin ve ABD bu noktada dikkat çekici örnekler oluşturabilir. ABD'de Google, Yahoo!, Microsoft gibi Amerikan ekonomisindeki güçlü aktörlerin APEC Çerçeve Belgesi ile benimsenen sisteme ılımlı yaklaşımları benzer hükümlerin iç hukukun bir parçası durumuna gelmesini sağlayabilir. Nitekim özellikle, yukarıda incelenen, 11 Eylül saldırıları sonrası uygulamalar dolayısıyla ABD'de pek çok politikacı kişisel verilerin korunmasına yönelik bir şeyler yapılması gerektiğinin farkındadır. Ancak diğer taraftan bu kişiler, muhaliflerince bu konuyu ulusal güvenliğin önünde görmekle eleştirilmekten çekinmektedirler. Bu ortamda APEC'in Özel Yaşamın Gizliliği Çerçeve Belgesi'nin

²⁰⁹ Lee A. BYGRAVE, “International Agreements to Protect Personal Data”, s. 43.

²¹⁰ Graham GREENLEAF, “APEC Privacy Framework Completed: No Threat to Privacy Standards”, **Privacy Law and Policy Reporter**, S.5, Y. 2006, <http://www.worldlii.org/au/journals/PLPR/2006/5.html>.

²¹¹ Bkz. <http://www.peterfleischer.blogspot.com/>, 14 Eylül 2007.

²¹² Julian LIGERTWOOD, Margaret JACKSON, “Transborder Data Protection and the Effects on Business and Government”, **Usability and Internationalization, Global and Local User Interfaces**, haz. Nuray AYKIN, Springer, Almanya 2007, s. 143.

kabulü “*bir şeyler*” yapıldığının kanıtı olarak sunulabilir²¹³. Ancak insan hakları kapsamındaki diğer bütün alanlarda da geçerli olduğu üzere, yalnızca “*bir şeyler*” yapmanın yeterli olmadığı unutulmamalıdır. Burada gereksinim duyulan gerçek anlamda etkin korumadır.

III. AVRUPA BİRLİĞİ’NDE KİŞİSEL VERİLERİN KORUNMASI

A. GENEL OLARAK

Avrupa’nın bütünleşmesi düşüncesinin gelişimi oldukça eskiye dayansa da bunun bir sürece dönüşmesi 20. yüzyıla rastlar. Bu dönemde artık bu amacın gerçekleştirilmesi için somut adımlar atılmaya başlanır. 1995 yılında kurulan Avrupa Birliği (AB), ekonomi, sanayi, siyaset, yurttaş hakları ve dış politika alanlarını kapsayan bütünleşme sürecinin en ileri biçimidir²¹⁴.

Kendine özgü ekonomik ve siyasal bir ortaklık olarak nitelendirilebilecek AB, doğrudan uygulanabilen bir mevzuat oluşturabilmekte ve yurttaşları lehine özel haklar ihdas edilebilmektedir. Ancak niteliği bakımından ABD gibi federal devlet yapılanmasından farklıdır: üye devletler egemenlik haklarına sahip olduğu gibi, uluslararası alanda da kendilerini temsil edebilir.

²¹³ Chris POUNDER, s. 9.

²¹⁴ Üye devletleri geleneksel uluslararası antlaşmalardan daha sıkı bir şekilde birbirine bağlayan AB’nin hukuksal temellerini ilk aşamada Avrupa Kömür ve Çelik Topluluğu’nu (AKÇT) kuran Paris Antlaşması (1951), Avrupa Ekonomik Topluluğu’nu (AET) ve Avrupa Atom Enerjisi Topluluğu’nu (Euratom) kuran Roma Antlaşmaları (1957), Avrupa Tek Senedi (1986), bir sonraki aşamada Amsterdam, Nice, Maastricht ve Lizbon Antlaşmaları oluşturmaktadır. Bkz. http://europa.eu/abc/12lessons/index_en.htm . Avrupa bütünleşmesinin tarihine ilişkin olarak bkz. Paul CRAIG, Gráinne de BÚRCA, s. 1-37; Martin HOLLAND, **European Integration: From Community to Union**, Pinter Publishers, Birleşik Krallık 1993. Ekim 2009 itibariyle AB’ye üye 27 devlet bulunmaktadır. Bunlar, Avusturya, Belçika, Bulgaristan, Güney Kıbrıs, Çek Cumhuriyeti, Danimarka, Estonya, Finlandiya, Fransa, Almanya, Yunanistan, Macaristan, İrlanda, İtalya, Letonya, Litvanya, Luksemburg, Malta, Hollanda, Polonya, Portekiz, Romanya, Slovakya, Slovenya, İspanya, İsveç ve Birleşik Krallık’tır. Böylelikle AB’nin yaklaşık 498 milyon yurttaşı bulunmaktadır. Hırvatistan, Makedonya ve Türkiye ise aday ülke statüsündedir. Aday ülkelerin de üyelik süreci içerisinde diğer konular yanında kişisel verilerin korunması hukuku açısından da uyumlaştırmaya gitmeleri gerekmektedir. Bkz. http://europa.eu/abc/european_countries/eu_members/index_en.htm . Bunun yanında AB üyesi olmayan bazı Avrupa ülkeleri de Birlik’in veri koruma hukukundan etkilenmektedir. Bunun özellikle dört üyesi bulunan Avrupa Serbest Ticaret Birlik’i (EFTA) üyesi ülkeler açısından görmek olanaklıdır. İzlanda, Lihtenştayn ve Norveç, Verilerin Korunması Yönergesi’ni onaylamıştır. Dolayısıyla burada yer alan kurallar onlar açısından da geçerli olacaktır. EFTA’ya üye dördüncü devlet olan İsviçre ise Yönerge’nin tarafı değildir. Christopher KUNER, s. 4.

Kişisel verilerin korunmasının anavatanı olarak nitelendirilebilecek Avrupa’da, bu alanda hem Avrupa Birliği (AB), hem de ulusal hukuk sistemleri düzeyinde oldukça gelişkin bir mevzuat bulunmaktadır²¹⁵. Almanya’nın Hessen eyaletinde ilk yasal düzenlemenin yapıldığı günden bugüne bölgede kişisel verilerin korunması hukuku yayılmış, gelişmiş ve olgunlaşmıştır. Konuya ilişkin devam eden sorunlara çözüm bulma arayışı ise halen sürmektedir.

Belirtmek gerekir: 1 Aralık 2009’da Lizbon Antlaşmasının onaylanması ile Birlik bünyesinde kişisel verilerin korunması daha da önemli hale gelmiştir. Bunun bir nedeni, aşağıda inceleneceği üzere kişisel verilerin korunmasının ayrı bir hüküm altında düzenlendiği, ABTHŞ’nin hukuksal bağlayıcılığa kavuşmasıdır. Diğer bir nedeni ise AB’nin İşleyişine İlişkin Sözleşmenin (Treaty on the Functioning of the EU-TFEU) verilerin korunması için yeni bir hukuksal temel sunmasıdır. Sözleşmenin 16. maddesi uyarınca artık polis ve adli işbirliğine ve ortak dış politika ve güvenlik politikasına ilişkin alanlar dahil özel ve kamu sektöründeki bütün veri işlemlerde Yönerge hükümlerine uygun hareket etmek gerekecektir²¹⁶.

Birlik düzeyinde kabul edilen çeşitli metinler içerisinde öncelikle AB Temel Haklar Şartı’nda ve AB Veri Koruma Yönergesi’nde konunun nasıl düzenlendiği üzerinde durmak gerekir. Ancak ondan önce kişisel verilerin korunmasına Birlik bünyesindeki kurumların nasıl katıldığına ilişkin kısa bir açıklama yapmak gerekecektir.

B. AB KURUMLARI

AB ile üye devletler arasındaki hukuksal ilişkileri düzenleyen çeşitli kural ve kurumlar bulunmaktadır²¹⁷. Bu bağlamda AB üyesi ülkelerde kişisel verilerin korunması hukukunu incelerken ikili bir ayırım yapmak gerekir: birincisi, Birlik

²¹⁵ AB düzeyinde kişisel verilerin korunmasının tarihsel gelişimine ilişkin ayrıntılı bir değerlendirme için bkz. Alexander VIETHEN, **Datenschutz als Aufgabe der EG-Bestandsaufnahme des datenschutzspezifischen Sekundärrechts und Analyse anhand der Kompetenzordnung des EG-Vertrages**, Kölner Schriften zum Internationalen und Europäischen Recht Band 5, LIT Verlag, Almanya 2003, s. 20-69.

²¹⁶ Article 29 Working Data Protection Working Party, **Working Party on Police and Justice, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data**, WP 168, 1 Aralık 2009, s. 5.

²¹⁷ Christopher KUNER, s. 5. Ayrıca bkz. Marie-Theres TINNEFELD ve diğ., s. 113-119. Ayrıntılı bilgi için bkz. Heinrich NEISSER, Bea VERSCHRAEGEN, **Die Europäische Union, Anspruch und Wirklichkeit**, Springer, Avusturya 2001, s. 133-239.

düzeyindeki düzenlemeler, ikincisi ise üye ülkelerin iç hukuklarında kabul ettikleri düzenlemelerdir. Üye devletlerin iç hukuk sistemlerinde kişisel verilerin korunmasına ilişkin kuralların uygulanmasını izleyen ve denetleyen bağımsız veri koruma otoriteleri bulunmaktadır. Birlik düzeyinde ise çeşitli organların kişisel verilerin korunması sürecinde rol oynadığı görülmektedir.

1. AB Komisyonu

AB'nin idari organı olan Avrupa Komisyonunun, kişisel verilerin korunmasında merkezi bir rol oynadığı belirtilmelidir. Nitekim Komisyon, Birlik düzeyinde hukuksal düzenlemeler önermekle yetkili tek organdır. Ayrıca Avrupa Komisyonu, üye devletlerde düzenlemelerin uygulamasını izlemek ve bir sorun olduğunda müdahale etmekten de sorumludur. Bunun yanında üye devletler de Veri Koruma Yönergesi uyarınca bazı girişimleri konusunda Komisyon'u bilgilendirirler²¹⁸.

2. AB Konseyi

İkinci olarak AB Konseyi (eski adıyla Bakanlar Konseyi) kişisel verilerin korunmasına ilişkin hukuksal düzenlemelerde bazen doğrudan etkili olabilmektedir. Bu bağlamda Konsey'in üye devletlerin Birlik düzeyinde karar alma ve uygulama süreçlerine siyasal açıdan etki edebildikleri bir forum oluşturması yanında, Veri Koruma Yönergesi ile kurulan ve üye devletlerin konuya ilişkin sorunlarında danışma organı olarak görev yapan 31. Madde Komitesi aracılığıyla bu etkiyi hissetmek olanaklıdır. Bunun yanında Konsey, veri koruma konuları ile uğraşan bir Çalışma Grubu da oluşturmuştur²¹⁹.

3. Avrupa Parlamentosu

AT organlarının üçüncü temel ayağını oluşturan Avrupa Parlamentosu da günümüzde veri koruma hukukuna ilişkin konularda merkezi bir role sahiptir. Veri koruması sorunları ile ilgilinin çeşitli Parlamento komitelerinin bulunması bunun açık göstergesidir²²⁰.

²¹⁸ Christopher KUNER, s. 5-6. Bkz. 95/46/AT sayılı Veri Koruma Yönergesi, m. 8/6, 25/3.

²¹⁹ Christopher KUNER, s. 6.

²²⁰ Christopher KUNER, s. 7.

4. Avrupa Adalet Divanı (AAD)

AT'nin yargı organı AAD ise kişisel verilerin korunmasına ilişkin sorunlara uygulamada iki temel yolla müdahil olmaktadır. İlk önce, bir üye devletin AB hukuku kapsamında bir düzenlemeyi uygulamasındaki sorunlara ilişkin olarak Mahkeme'de dava açılabilir. Bu başvuru AB Komisyonu ya da başka bir üye devletçe yapılabilir. Nitekim Komisyon bu yetkisini, 11 Ocak 2000 tarihinde Veri Koruma Yönergesi'ni uygulamada çeşitli sorunların bulunduğunu düşündüğü, Fransa, Almanya, İrlanda, Lüksemburg ve Hollanda'ya karşı kullanmıştır²²¹. İkinci olarak, bir Üye Devlet'in ulusal yargı organı AB hukukuna ilişkin bir konuda Mahkeme'nin yorumuna başvurabilmektedir²²². Bu doğrultuda AAD'nin verdiği çeşitli kararlar bulunmaktadır. Bu kararlar, Topluluk'un yargı organının uyumlaştırmada önemli bir görev üstlendiğinin de göstergesidir²²³.

Görüldüğü gibi kişisel verilerin korunması mevzuatı üzerinde AB temel organlarının çeşitli açılardan önemli etkileri bulunmaktadır. Ancak bunların yanında Birlik içerisinde çeşitli çalışmaları doğrudan bu konuya hasredilmiş bazı birimler de bulunur. Bu kapsamda özellikle Avrupa Veri Koruma Denetçisi, 29. Madde Çalışma Grubu ve 31. Madde Komitesi üzerinde durmak gerekir²²⁴.

5. Avrupa Veri Koruma Denetçisi

Avrupa Veri Koruma Denetçisi (European Data Protection Supervisor-EDPS), AB kurum ve organları tarafından kişisel verilerin işlenmesini denetlemek ile sorumludur. Ancak kurumun etkisi bu temel görevi ile sınırlı değildir. Bu bağımsız organ, AB düzeyinde kişisel verilerin korunması konusunda politikaların geliştirilmesinde oldukça etkilidir. Ayrıca, özellikle ticaret ile ilgili kişisel verilerin korunması sorunlarında görüş bildirdiği görülmektedir²²⁵. Bunun yanında Avrupa

²²¹ Christopher KUNER, s. 7.

²²² Christopher KUNER, s. 7.

²²³ Paul De HERT, Serge GUTWIRTH, s. 29.

²²⁴ AB içerisinde temel çalışma alanı kişisel verilerin korunması olmayan başka bazı birimlerin de zaman zaman konuya ilişkin sürece dahil oldukları görülmektedir. Örneğin, Avrupa Ombudsman'ının bir yurttaş ile Avrupa Komisyonu arasındaki çekişme dolayısıyla verdiği konuya ilişkin bir kararı bulunmaktadır. Bkz. **Decision of the European Ombudsman on complaint 2467/2004/PB against the European Commission**, 9 Haziran 2006; Christopher KUNER, s. 12.

²²⁵ Avrupa Veri Koruma Denetçisini etkinliklerine ilişkin olarak bkz. resmi İnternet sitesi: <http://www.edps.europa.eu/>.

Veri Koruma Denetçisi, AAD önünde veri korumasına ilişkin davalara müdahil olabilmektedir²²⁶.

6. 29. Madde Veri Koruma Grubu

AB bünyesinde verilerin korunmasına ilişkin bir diğer önemli organ, 29. Madde Veri Koruma Grubu'dur. 95/46/AT sayılı Veri Koruma Yönergesi'nin 29. maddesi uyarınca kurulan bu Grup, bağımsız bir danışma organı olarak görev yapmaktadır²²⁷. Kişisel verilerin korunmasına ilişkin çeşitli konularda görüşlerini belirten ve yorum geliştiren Veri Koruma Grubu, uygulamada oldukça önemli bir görev üstlenmiş bulunmaktadır²²⁸. Kişisel verilerin korunmasına ilişkin çok çeşitli konularda hazırladığı rapor, görüş ve öneriler hem teoriye, hem uygulamaya ışık tutacak niteliktedir.

7. 31. Madde Komitesi

Yine Veri Koruma Yönergesi ile kurulmuş bir diğer önemli organ 31. Madde Komitesi'dir. Yönerge'nin 31. Maddesi uyarınca *"Komisyon'a, Üye Devletler'in temsilcilerinden oluşan ve başkanlığını Komisyon temsilcisinin yaptığı bir Komite yardımcı olacaktır"*²²⁹. 29. Madde Çalışma Grubunun aksine 31. Madde Komitesi

²²⁶ Christopher KUNER, s. 7-9.

²²⁷ Veri Koruma Yönergesi, m. 29/1. Veri Koruma Grubu, her bir Üye Devlet'in belirlediği birer temsilci, Topluluk kurum ve organlarınca belirlenen birer temsilci ve bir Komisyon temsilcisinden oluşur. Bkz. Veri Koruma Yönergesi, m.29/2. Ayrıca bkz. Article 29 Data Protection Working Party, Working Party on the protection of individuals with regard to the processing of personal data, Rules of Procedure, 18 Şubat 2008.

²²⁸ Christopher KUNER, s. 9. Çalışma Grubu'nun görevleri Yönerge'nin 30. maddesinde belirlenmiştir. Buna göre şu hususlar Veri Koruma Grubu'nun görev alanına girmektedir: 1. Yönerge uyarınca ulusal hukuk sistemlerinde kabul edilen önlemlere ilişkin her türlü soruyu, uygulamadaki uyumu sağlamak amacıyla incelemek(m.30/1,a); 2. Diğer ülkelerde ve Topluluk bünyesinde koruma düzeyine ilişkin Komisyon'a görüş sunmak(m.30/1,b); 3. Yönerge'de değişiklik önerilerine ilişkin olarak Komisyon'u bilgilendirmek(m.30/1,c); 4. Topluluk düzeyindeki düzenlemelere (codes) ilişkin görüş bildirmek(m.30/1,d); 5. Üye Devletler'in kişisel verilerin korunmasına ilişkin düzenlemelerinde dengesizlik görmesi durumunda Komisyon'u haberdar etmek(m.30/2); 6. Topluluk bünyesinde kişisel verilerin korunmasına ilişkin dilediği herhangi bir konuda tavsiye sunmak(m.30/3); 6. Komisyon'a, Parlamento'ya ve Konsey'e iletmek üzere üçüncü ülkelerde ve Topluluk bünyesinde kişisel verilerin korunmasına ilişkin durumu saptayan yıllık raporlar hazırlamak(m.30/6).

²²⁹ Bkz. Yönerge m.31/1. Yönerge'nin bu hükmü, metnin kabulünden bugüne değişikliğe uğrayan tek hükümdür. 29 Eylül 2003 tarihli 1882/2003 sayılı Tüzük (Regulation) ile 1999/468 sayılı Konsey Kararı'nın Komite ile ilgili hükümleri uyarınca bu değişiklik kabul edilmiştir. Bkz. **Regulation (EC) No. 1882/2003 of the European Parliament and of the Council of 29 September 2003 adapting to Council Decision (EC) 1999/468 the provisions relating to committees which assist te Commission in the exercise of implementing powers laid down in**

yalnızca bir danışma organı değildir, pek çok önemli düzenlemenin kabulünde bu Komite'nin onayı gerekmektedir. Ayrıca Komite'nin üyeleri, Üye Devletlerin temsilcilerinden oluştuğundan siyasal bir kimlik de taşımaktadır. Ancak Komite şeffaf bir nitelikte bulunmadığından çalışmalarına ilişkin kolaylıkla bilgi alınmadığını da belirtmek gerekir²³⁰.

Çalışmamızın birinci bölümünde açıklamaya çalıştığımız üzere kişisel verilerin korunması çeşitli açılardan türlü zorluklarla mücadeleyi gerektiren bir alandır. Küresel bilgi akışına zarar vermeden bireylerin gittikçe daralan özel alanlarını ya da belki daha doğru bir anlatımla öz benliklerini korumak gittikçe güçleşmektedir. Hızla ilerleyen teknolojinin koruma mekanizmalarını işlevsiz ve hantal sistemler haline getirme tehlikesi bir yana, özellikle 11 Eylül 2001 ve bunu izleyen Londra ve Madrid saldırıları sonrasında artan güvenlik kaygılarının bu koruma alanına çeşitli açılardan zarar verdiği açıktır. Aşağıda kendi modelini yalnızca üye ülkelere değil, küresel düzeyde bütün dünya ülkelerine sunan AB hukuk sisteminde kişisel verilerin korunmasına ilişkin temel metinler üzerinde durulacaktır.

C. AB TEMEL HAKLAR ŞARTI

7 Aralık 2000 tarihinde Fransa'nın Nice kentinde imzalanan AB Temel Haklar Şartı ile Birlik'in tarihinde ilk kez Avrupa vatandaşlarının ve AB'de yaşayan bütün insanların bireysel, siyasal ve ekonomik hakları tek bir metinde toplanmıştır²³¹. Resmi bir beyan niteliğindeki bu belge, bazı değişikliklerle, 2004 yılında AB Anayasasının II. Bölümüne temel haklar katalogu olarak dâhil edilmiştir²³². Bu

instruments subject to the procedure referred to in Article 251 of the EC Treaty [2003] OJ L284/1. Ayrıca bkz. Christopher KUNER, s. 11-12.

²³⁰ Christopher KUNER, s. 12.

²³¹ Matthias Christoph SCHWENKE, **Individualisierung, Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung**, Deutscher Universitäts-Verlag, Almanya 2006, s.64. Nitekim belge, AİHS, AB üyesi devletlerin anayasal gelenekleri, AK Sosyal Şartı, AB İşçilerin Temel Sosyal Hakları Şartı ve üye ülkelerin taraf oldukları uluslararası sözleşmeler temel alınarak hazırlanmıştır. Daha geniş bilgi için bkz. AB Temel Haklar Şartı'nın resmi İnternet sitesi: http://www.europarl.europa.eu/charter/default_en.htm. AB Temel Haklar Şartı kabul edilinceye kadar Birlik'in hukuk sisteminde temel hakların korunmasının gelişimine ilişkin olarak bkz. Damien CHALMERS, Adam TOMKINS, **European Union Public Law**, Cambridge University Press, Birleşik Krallık 2007, s. 232-246; Jürgen KÜHLING, "Fundamental Rights", **Principles of European Constitutional Law**, haz. Armin von BOGDANDY, Jürgen BAST, Hart Publishing, 2. Baskı, ABD 2007, s. 504-507. (501-548)

²³² AB Temel Haklar Şartı'nın AB Anayasası'na eklenmesinde yapılan değişikliklere ve genel olarak bu eklemenin biçimsel niteliğine ilişkin eleştirel bir yaklaşım için bkz. Bertil Emrah

metin, eğer AB Anayasası beklendiği gibi 2005 yılında onaylansaydı, onun önemli bir parçası olarak yürürlüğe girecek ve bağlayıcı olacaktı²³³. Ancak AB Anayasa Antlaşmasının onaylanmamasının²³⁴ ve Şarta atıfta bulunan 2007 tarihli Lizbon Antlaşmasının da İrlanda tarafından reddedilmesinin ardından metnin hukuksal ve siyasal açıdan, Anayasa öncesindeki durumuna geri döndü²³⁵. Bununla birlikte, AB Temel Haklar Şartı, hem ATAD²³⁶ hem de diğer siyasal kurumlarca yol gösterici ve önemli bir belge olma özelliğini sürdürdü²³⁷. Ancak bu durum, Lizbon Antlaşmasının 1 Aralık 2009 tarihinde yürürlüğe girmesi ile değişmiştir. Artık ABTHŞ hukuksal açıdan tam anlamıyla bağlayıcıdır²³⁸.

AB Temel Haklar Şartı'nda hakların altı bölüm altında incelendiği görülür: (i) saygınlık, (ii) özgürlükler, (iii) eşitlik, (iv) dayanışma, (v) yurttaş hakları, (vi) adalet. Şartın “özgürlükler” başlığı altında yer alan 7. maddesinde “(h)erkes özel ve aile yaşamına, evine ve iletişimine(communicação) saygı gösterilmesini isteme hakkına sahiptir” hükmü yer alır. Buradaki düzenlemenin, uluslararası metinlerde ve çok sayıda devletin Anayasasında yer alan özel yaşamın gizliliği hakkının geleneksel düzenleme şekline uygun olduğu açıktır. Bu bağlamda Şartı hazırlayanlar, AİHS m.8/1 hükmünü temel almışlardır. Ancak iki metin arasında ilk bakışta dikkatten kaçabilecek bir farklılık bulunmaktadır.

Şartı hazırlayanların AİHS'nin 8. maddesini temel almakla birlikte, bu hükmü yeni gelişmelere ve teknolojik değişime de uyumlu hale getirmeyi

ODER, **Avrupa Birliği'nde Anayasa ve Anayasacılık**, Anahtar Kitaplar, İstanbul 2004, s. 318-337.

²³³ Judith RAUHOFFER, “Intrusion in the Sphere of Personal Communications”, **Socioeconomic and Legal Implications of Electronic Intrusion**, haz. Dionisios POLITIS, Phaeton KOZYRIS, Ionnis IGLEZAKIS, Information Science Reference, 2009, s. 32. (25-46).

²³⁴ 29 Ekim 2004 tarihinde Roma'da imzalanan Avrupa Anayasası, 29 Mayıs 2005 tarihinde Fransa'da (%54,8 “hayır” oyuyla), 1 Haziran 2005 tarihinde ise Hollanda'da (%61,7 “hayır” oyuyla) yapılan referandumlar sonucunda veto edilmiştir. Bkz. Haluk GÜNUĞUR, **Avrupa Birliği'nin Hukuk Düzeni**, Avrupa Ekonomik Danışma Merkezi, Ankara 2007, s. 248, d.n. 1.

²³⁵ Lizbon Antlaşması, Üye Devletlerce 13 Aralık 2007'de imzalanmıştır. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 13 Aralık 2007, O.J. No. C 306, 17 Aralık 2007, s.1-271. Ayrıca Lizbon Antlaşması'na tam metni ve konuya ilişkin çeşitli bilgilere şu kaynaktan ulaşılabilir: http://europa.eu/lisbon_treaty/index_en.htm.

²³⁶ ATAD kararlarında AB Temel Haklar Şartı'nın etkisine ilişkin olarak bkz. Thomas SCHMITZ, “Die EU-Grundrechtecharta aus grundrechtsdogmatischer und grundrechtstheoretischer Sicht”, **Juristenzeitung**, Y. 2001, s. 833-843.

²³⁷ Paul CRAIG, Gráinne de BÚRCA, s.413. Ayrıca bkz. Roland WINKLER, **Die Grundrechte der Europäischen Union**, Springer, Avusturya 2006.

Lizbon Antlaşmasının tam metni ve konuya ilişkin genel bilgi için bkz. http://europa.eu/lisbon_treaty/index_en.htm.

hedefledikleri görülmektedir. Bunun işareti, AİHS'nin 8. maddesinde yer alan “haberleşme” (correspondence) deyiminin yerine, “iletişim”in (communication) tercih edilmesidir²³⁹. Böylelikle metnin iletişim alanında yaşanan hızlı gelişmeler sonucunda ortaya çıkan yeni araçları da kapsamına aldığı görülmektedir²⁴⁰. Ancak AB Temel Haklar Şartı’nın, konumuz açısından, AİHS’nin kabul edildiği 1950’li yılından bugüne farklılaşan gereklilikleri dikkate aldığı tek işareti bu değişiklik değildir. Bunun yanında Şartı hazırlayanlar, her geçen gün önemi biraz daha anlaşılan kişisel verilerin korunması hakkını ayrı bir hüküm altında düzenlemeyi tercih etmişlerdir.

AB Temel Haklar Şartı’nın “*Kişisel verilerin korunması*” kenar başlıklı 8. maddesi şöyledir:

“(1) Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir.

(2) Bu veriler, dürüst bir şekilde(fairly), 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 düzeltirme hakkına sahiptir. (3) Bu kurallara uyulması bağımsız bir makam tarafından denetlenir”²⁴¹.

²³⁹ Council of the EU, **Charter of Fundamental Rights of the European Union, Explanations relating to the complete text of the Charter**, Aralık 2000, Luxembourg Office for Official Publications of the EC 2001, s. 25. AİHS’nin 8/2 hükmü de Şartın 52/3 hükmü uyarınca bu metinde de korunmuştur.

²⁴⁰ Jürgen KÜHLING, Christian SEIDEL, Anastasios SIVRIDIS, **Datenschutzrecht**, Verlag Recht und Wirtschaft GmbH, Almanya 2008, s. 44.

²⁴¹ AB Temel Haklar Şartı’nın AB ile İlişkiler Genel Müdürlüğü tarafından yapılan Türkçe çevirisinde 8. maddeye ilişkin olarak ilk bakışta ufak gibi gözüken ancak temelde önemli anlam farklılıkları yaratan bazı hataların yapıldığı görülmektedir. Öncelikle bu çeviride 8/2 hükmü 1. fıkrada yer alan koşullarda veriler “*tutulur*” ifadesi yer almaktadır. Oysa orjinal İngilizce metinde “*processed*” yani “*işleme*” ifadesi kullanılmıştır. Çalışmamızın çeşitli yerlerinde belirtildiği üzere, kişisel verilerin işlenmesi, verilerin tutulmasını (retention) da kapsayan geniş bir kavramdır. Yapılan çeviri hatası, AB Temel Haklar Şartı’nda mevcut olandan daha sınırlı bir koruma öngörüldüğü gibi bir görünüm yaratmaktadır. Benzer şekilde yine aynı hükmün çevirisinde “*fairly*” ifadesinin karşılığı olarak dürüstlük kuralı değil, “*adil*” olma anlaşılmıştır. Oysa “*adil*” işleme, kişilik haklarının korunmasında daha dar bir alana işaret etmektedir. Bu ikinci hatanın başka bir metinde, Türkiye Bilişim Şurası’nın Sonuç Raporu’nda da bulunduğu görülmektedir. Bu raporda AB Yönergesi’nin 6. maddesine ilişkin olarak “*adil ve kanunlara uygun işleme*” ifadesi yer alır. Oysa metinde “*hukuka ve dürüstlük kuralına uygun işleme*”den söz edilmektedir. AB Temel Haklar Şartı’nın AB ile İlişkiler Genel Müdürlüğü tarafından Kasım 2001 tarihli çevirisi için bkz. <http://ekutup.dpt.gov.tr/ab/hukuk/temelhak.pdf> (s.y. 1 Temmuz 2009). Türkiye Bilişim Şurası’nın Sonuç Raporu’na ilişkin değerlendirme için bkz. Kesmez, “*Kişisel Verilerin Korunması Üzerine*”, <http://2002.bilisimsurasi.org.tr/dosyalar/102.doc>, 25 Şubat 1992, der.Başbakanlık, Türkiye Bilişim Şurası, **Bilgi Toplumuna Doğru, Türkiye Bilişim**

Görüldüğü gibi hükümde ilk olarak “herkes”in kişisel verilerin korunması hakkına sahip olduğuna işaret edilmiştir. Burada “herkes” deyiminin kapsamına gerçek kişilerin yanında tüzel kişilerin de girip girmediği açık değildir. Ancak kişisel verilerin korunması hukukunun temel mantığı ve Temel Haklar Şartı’na kaynaklık oluşturan 95/46/AT sayılı Yönerge dikkate alındığında koruma alanının öncelikle gerçek kişilere yönelik olduğunu söylemek sanıyoruz yanlış olmaz²⁴².

Belirtilen hükmün temelini, Avrupa Toplulukları’nı kuran Antlaşmanın 286. maddesi, 95/46/AT sayılı Yönerge, 108 sayılı AK Sözleşmesi ve AİHS’nin 8. maddesi oluşturur. Ayrıca kişisel verilerin korunması hakkı Yönerge’de belirtilen koşullar çerçevesinde kullanılacağı gibi, Şartın 52. maddesinde yer alan hükümlerle de sınırlandırılmıştır²⁴³. Şartın belirtilen hükmünde geçen “*kişisel veri*”, “*işleme*” gibi deyimlerde ve 8/2 hükmünde yer alan temel gerekliliklerde aşağıda incelenecek AB Yönergesi’nin etkisi açıkça hissedilmektedir. Bu açık etkinin yanında Şartın AB Yönergesi’nden ayrılan önemli bir özelliği vardır: 8. madde hükmü yalnızca iç pazar düşüncesine dayanmamakta, bu nedenle Yönerge’nin ötesine geçmektedir²⁴⁴.

AB Temel Haklar Şartı’nda özel yaşamın gizliliği hakkı ile kişisel verilerin korunması hakkı arasında bir ayrımın öngörülmesi, ulusal hukuk sistemlerinde yapılacak yeni anayasal çalışmalara da örnek oluşturacak niteliktedir. Kişisel verilerin korunması hakkı, özel yaşamın gizliliği hakkının çekirdeği içerisinde değerlendirilemeyecek bazı konuları koruma kapsamına almaktadır. Aşağıda ayrıntılarıyla incelenecek kişisel verilerin işlenmesinde dürüstlük kuralına uygunluk

Şurası Sonuç Raporu, s.336’dan aktaran; Nilgün BAŞALP, **Kişisel Verilerin Korunması ve Saklanması**, s. 37.

²⁴² Oğuz ŞİMŞEK, s. 73.

²⁴³ Council of the EU, **Charter of Fundamental Rights of the European Union, Explanations relating to the complete text of the Charter**, Aralık 2000, Luxembourg Office for Official Publications of the EC 2001, s. 26. Şartın 52. maddesinde güvence altına alınan hakların kapsamı düzenlenmiştir. Buna göre; “(1) Bu Şartla tanınan hak ve özgürlüklerin kullanılmasının sınırlandırılması yasa ile olmalı ve söz konusu hak ve özgürlüklerin özü korunmalıdır. Sınırlamalar, orantılılık ilkesi de dikkate alınarak, ancak gerekli olduğu ve Birlik tarafından tanınan genel yarar amacını veya başkalarının hak ve özgürlüklerini koruma gereksinimi gerçekten karşıladığı zaman gerçekleştirilebilir. (2) Bu Şartla tanınan ve Topluluk Antlaşmalarına veya Avrupa Birliği Antlaşmasına dayanan haklar, söz konusu Antlaşmalarda belirlenen koşullar ve sınırlar dahilinde kullanılır. (3) Bu Şartta yer alan haklardan, İnsan Haklarının ve Temel Özgürlüklerin Korunması Avrupa Sözleşmesinde yer alan haklarla örüntülerin anlamı ve kapsamı söz konusu Sözleşmedekiyle aynıdır. Bu hüküm, Birlik hukukunun daha geniş bir koruma getirmesini engellemez”.

²⁴⁴ Mads ANDENAS, Stefan ZLEPTNIG, “Surveillance and Data Protection: Regulatory Approaches in the EU and Member States”, **European Business Law Review**, Y. 2003, s. 780.

gerekliliği, ilgili kişinin rızasına ya da meşruluğa ilişkin kurallar bu kapsamda sayılabilecek bir kaç örnektir²⁴⁵.

Bunun gibi AB Temel Haklar Şartı'nın 8. maddesinde herkesin kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahip olduğunun belirtilmesi, AİHM'nin özel yaşamın gizliliği hakkına dayanarak oluşturduğu içtihatlarında tam anlamıyla cevaplayamadığı bazı hukuksal sorunları çözmektedir²⁴⁶. Sonuç olarak AB Temel Haklar Şartı'nda kişisel verilerin korunmasının özel yaşamın gizliliği hakkından ayrı olarak düzenlenmesi, kişisel verilerin korunmasının artık bağımsız bir hak olarak kabul edildiğinin önemli bir işaretidir. Ayrıca Şart'ın 8. maddesi, aşağıda incelenecek 95/46/AT sayılı Kişisel Verilerin Korunması Yönergesi'nin temel haklar boyutunu da vurgulamaktadır²⁴⁷.

D. 95/46/AT SAYILI KİŞİSEL VERİLERİN KORUNMASI YÖNERGESİ

1. YÖNERGENİN AMACI

Kişisel verilerin korunmasına ilişkin en önemli metinlerden biri “*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*”dir²⁴⁸. Aşağıda görüleceği üzere bu metin, AB üyesi ülkelerin sınırlarını aşan bir etki yaratmıştır.

²⁴⁵ Paul de HERT, Serge GUTWIRTH, “Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power”, **Privacy and the Criminal Law**, haz. Erik CLAES, Anthony, DUFF, Serge GUTWIRTH, Intersentia, 2006, s. 81. (61-109)

²⁴⁶ Paul de HERT, Serge GUTWIRTH, s. 81. Bu noktada ABTHŞ'nın 42. maddesi de dikkatten kaçmamalıdır. Nitekim 42. maddede “(b)irliğin her vatandaşı ve bir üye devlette ikamet eden veya kayıtlı iş merkezine sahip her gerçek ya da tüzel kişi, Avrupa Parlamentosu, Konsey ve Komisyon belgelerine erişim hakkına sahiptir” hükmü düzenlenmiştir.

²⁴⁷ Commission of the European Communities, **Report From the Commission, First report on the implementation of the Data Protection Directive (95/46/EC)**, 15 Mayıs 2003 Brüksel, COM(2003) 265 final, s. 3-4.

²⁴⁸ 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 data, Official Journal of the European Communities of 23 November 1995, No L. 281, s. 31. Bundan böyle “AB Yönergesi” veya “95/46/AT sayılı Yönerge” olarak anılacaktır. Yönerge'ye göre üye devletlerin 24 Ekim 1998'e kadar iç hukuklarındaki düzenlemeleri Yönerge ile uyumlaştırmaları gerekiyordu. Ancak bu üye devletlerin büyük bir bölümü bu süreye kadar gereken düzenlemeleri tamamlayamamışlardır. Peter CAREY, **Data Protection**, s. 5. AT Antlaşması'nın 249. maddesine göre “Yönergeler, şekil ve yöntemler bakımından yetkiyi ulusal kurumlara bırakarak, yöneldiği devletleri varılacak sonuçlar bakımından bağlar”. Bu bakımdan yönergeler, AB üyesi ülkeler açısından bağlayıcı nitelik taşımaktadır. Üye devletler, yönergelerde belirlenen hedeflere ulaşılabilmesi için ulusal düzeyde bir düzenleme yapma yetkisine sahiptirler. Bu bağlamda, Yönergenin hedeflerini iç hukuklarına aktarırken düzenlemenin türünü (örneğin bir

1995 yılında AT bünyesinde Kişisel Verilerin Korunması Yönergesi kabul edilmeden önce de pek çok Avrupa ülkesinde konuya ilişkin hukuksal düzenlemeler bulunmaktaydı. Nitekim yukarıda bu alandaki ilk düzenlemelerin 1970’li yıllarda Avrupa’da yapılmaya başlandığından ve bölgede hızla yayıldığından söz etmiştik. 1990’lı yıllara gelindiğinde özellikle küresel ağların gelişmesiyle kişisel verilerin korunmasının önemi daha yoğun bir şekilde hissedilmeye başlanmıştır.

Gelişen teknoloji, uluslararası ticaretin ve bilgi paylaşımının sınır tanımaz bir şekilde hızlanmasına, bu kapsamda bireylerin karşılaşabileceği sorunların öneminin artmasına ve bu sorunlara ilişkin algının güçlenmesine neden olmuştur. Avrupa ise hızlı bir dönüşüm içerisinde. 1991 yılının Aralık ayında kabul edilen Maastricht Antlaşması 1 Kasım 1993’te yürürlüğe girmiştir. Antlaşmada öngörüldüğü üzere, Avrupa, kişilerin, hizmetlerin, sermayenin ve malların serbestçe dolaştığı bir bölge olma yolunda hızla ilerlemektedir²⁴⁹. Pek çok alanda olduğu gibi, kişisel verilerin korunması da bir uyumlaştırma gereksiniminin hissedildiği alanlardan biridir. Özellikle “*tek iç pazar*” düşüncesi bu noktada etkilidir.

AK bünyesinde 108 sayılı Kişisel Verilerin Korunması Sözleşmesi kabul edilmişken AB düzeyinde neden yeni bir metnin hazırlandığı düşünülebilir. Nitekim ilgili bölümde de belirtildiği üzere, AK Sözleşmesi’nin 4. maddesi uyarınca Sözleşme tarafı devletlerin bu metinde yer alan ilkeleri iç hukuklarının bir parçası haline getirme zorunluluğu bulunmaktadır.

Yönerge’nin çıkarılmasına duyulan gereksinim, farklı ulusal yasaların tek bir iç pazar oluşumunu engelleme tehlikesinin önüne geçme düşüncesinde kaynağını bulur. Nitekim yapılan çalışmaların verilerin korunmasına ilişkin ulusal hukuk sistemlerinde ciddi farklılıklar bulunduğunu ortaya koyması, AB içerisinde bir uyumlaştırma gerekliliğini ortaya çıkarmıştır²⁵⁰. Gerçekten bu dönemde üye devletlerin konuya ilişkin yasal düzenlemelerinde belirgin bir çeşitlilik dikkat çeker. Örneğin Almanya, Fransa ve İskandinav ülkeleri konuyu insan haklarının bir bileşeni

yasa ile mi, yoksa bakanlar kurulu kararı ile mi) yapılacağını saptamakta serbesttirler. Yönergelerin hukuksal niteliğine ilişkin olarak bkz. Haluk GÜNUĞUR, **Avrupa Birliği’nin Hukuk Düzeni**, Avrupa Ekonomik Danışma Merkezi, Ankara 2007, s. 184-190. Kimi yazarlar, Yönerge’nin bazı dillere resmi çevirilerinde ufak farklılıklar bulunduğuna dikkat çekmektedir. Örneğin bkz. Christopher KUNER, s. 23-24. Bizim çalışmamızda Yönerge’nin resmi İngilizce metni esas alınmıştır.

²⁴⁹ Avrupa’daki gelişime ilişkin olarak bkz. Marie-Theres TINNEFELD ve diğ., s. 105-119.

²⁵⁰ Viktor MAYER-SCHÖNBERGER, s. 220.

olarak değerlendirirken, Birleşik Krallık Sözleşmede belirtilen hükümleri asgari düzeyde sağlayarak uluslararası ticaretini korumayı hedeflemiştir. Sözleşmenin 1995 yılına kadar onaylanmadığı Yunanistan'da ise bu dönemde kişisel verilerin korunması yasası bile bulunmamaktadır²⁵¹.

Komisyon, bu çeşitliliği “*tek pazar*” düşüncesine karşı ciddi bir engel olarak görmüştür. Bu nedenle AB Komisyonu'nun hazırladığı Yönerge'nin birincil amacı, üye devletler arasındaki veri korunmasına ilişkin farklılıkların ortadan kaldırılmasıdır. Nitekim AB'yi Kuran Antlaşmanın 7a maddesi uyarınca malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımına olanak tanıyan bir iç pazar oluşturulmalı ve işleyebilmelidir. Ancak kişisel verilerin bir üye devletten diğerine serbestçe dolaşımının yanında bireylerin temel haklarının korunması gerektiği de unutulmamalıdır²⁵².

Yönerge'nin 1. maddesi, kişisel verilerin korunmasının temel bir insan hakkı olduğunu açıkça ortaya koymaktadır. Bu hükme göre: “*Üye Devletler, gerçek kişilerin temel hak ve özgürlüklerini ve özellikle kişisel verilerin işlenmesi ile ilgili özel yaşamın gizliliği hakkını koruyacaktır*”. AAD de Yönerge'nin yalnızca iç pazarı geliştirme amacına yönelmediğini, temel hedeflerinden bir diğerinin insan haklarını korumak olduğunu teyit etmiştir²⁵³.

Bir yanda bilişim teknolojilerindeki gelişmeler ile kişisel verilerin işlenmesi ve devrinin kolaylaşması, diğer yanda Avrupa'da gelişen ekonomik ve sosyal bütünleşmenin sınır aşan kişisel veri akışını arttırması bu uyumlaştırmanın gerekliliğini ortaya koymaktadır. Bu bağlamda üye devletlerde kişisel verilerin korunma düzeyindeki farklılıkların Topluluk içerisinde pek çok ekonomik etkinliğin izlenmesini engelleyebileceğine, rekabeti bozacağına, Topluluk hukuku uyarınca yetkililerin sorumluluklarını ifa etmelerine engel olacağına işaret edilmiştir²⁵⁴.

Yönerge ile güdülen bir diğer amaç ise bütün üye devletlerde geçerli olacak asgari veri koruma ölçütlerini belirlemektir²⁵⁵. Bu bağlamda, sonuçta ortaya çıkan Yönerge, üye devletlerin kapsamlı bir veri koruma rejimi oluşturmalarını

²⁵¹ David I. BAINBRIDGE, *EC Data Protection Directive*, Butterworths, Birleşik Krallık 1996, s. 17; Andrew CHARLESWORTH, s. 256.

²⁵² Bkz. 95/46/AT sayılı Yönerge, Gerekçe, par. 3.

²⁵³ Bkz. *Österreichier Rundfunk ve Lindqvist kararları*; Lee A. BYGRAVE, “Global Privacy Protection: The First Generation”, s. 32.

²⁵⁴ Bkz. 95/46/AT sayılı Yönerge, Gerekçe, par. 4-7.

²⁵⁵ Christopher KUNER, s. 20.

gerektirmiştir²⁵⁶. Bir başka anlatımla, Yönerge ile ulusal hukuk sistemlerinde konuya ilişkin kuralları belirleyerek Avrupa içerisinde serbest veri akışını sağlamak hedeflenmiştir.

Hedef üye devletlerin iç hukuk sistemleri olduğundan, Veri Koruma Yönergesi Topluluk kurum ve organları tarafından işlenen veriler için geçerli değildir. Topluluk kurum ve organları tarafından kişisel verilerin işlenmesi sırasında gerçek kişilerin korunması 18 Aralık 2000 tarihli 45/2001/AT sayılı bir tüzük ile sağlanmıştır²⁵⁷. Kısaca AT Organlarında Verilerin Korunması Tüzüğü olarak adlandırılabilir bu metin, Avrupa Parlamentosu, AB Konseyi, Avrupa Komisyonu, Avrupa Adalet Divanı ve Sayıştay ile Topluluk hukuku çerçevesinde yaratılmış diğer organ ve kurumları bünyesinde kişisel verilerin işlenmesinde uyulacak esasları saptamaktadır. Bir başka ifade ile Tüzüğün Topluluğun kendi kurum ve organlarının etkinlik alanında kişisel verileri işlemeleri durumunda uyacakları ilkeleri belirlediğini söyleyebiliriz²⁵⁸.

2. KAPSAMI VE UYGULAMA ALANI

95/46/AT sayılı Yönerge yalnızca mevcut veri koruma hukukunu güçlendirmekle kalmayıp yeni bazı haklarla onu pekiştiren ortak bir çerçeve sunmaktadır²⁵⁹. Yönergede belirlenen temel ilkeler kısaca şöyle özetlenebilir: verinin kaynağını bilme hakkı, yanlış verileri düzeltme hakkı, hukuk dışı işlemlere karşı

²⁵⁶ Andrew CHARLESWORTH, “The Governance of the Internet in Europe”, **The Internet, Law and Society**, haz. Yaman AKDENİZ, Clive WALKER, David WALL, Pearson Education Limited, İngiltere 2000, s. 64.

²⁵⁷ **Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data**, OJ L 8, 12.1.2001, p. 1–22 Tüzüğün hukuksal dayanağı Avrupa Toplulukları Antlaşmasında bulunmaktadır. Bkz. m. 286.

²⁵⁸ Oğuz ŞİMŞEK, s. 65.

²⁵⁹ Kolaylıkla tahmin edilebileceği gibi Yönerge’nin kapsamı konusunda uzlaşının sağlanması kolay olmamıştır. Üye ülkelerin kişisel verilerin korunmasına farklı yaklaşımları, Yönerge taslak halindeyken süren tartışmalara da yansımıştır. Örneğin Almanya, kendi ülkesinde uygulanan yüksek düzeydeki korumayı düşürecek hükümlere isteksiz yaklaşmıştır. Birleşik Krallık, Hollanda, İrlanda ve Danimarka ise Üye Devletlerin AK Veri Koruma Sözleşmesi’ni onaylaması zorunluluğunun yeterli olacağını savunmuştur. Bunun yanında bankacılık, tıbbi araştırma, pazarlama gibi alanlarda etkinlik gösteren, kişisel verilerin kullanımına getirilecek sınırlamalara ilişkin kaygıları dile getirilmiştir. Sonuçta ortaya çıkan metinde belirli bir ulusal sistemin oransız etkisi görülmemektedir. Bu bağlamda Almanya, Birleşik Krallık, Hollanda ve Fransa’da Yönerge öncesi benimsenen sistemlerin ortak hususlarının metne yansıtıldığı söylenebilir. Andrew CHARLESWORTH, s. 256-257. Yönerge’nin kabul edilmesi öncesindeki tartışmalara ilişkin olarak ayrıca bkz. Spiros SIMITIS, “From the Market to the Polis: The EU Directive on Protection of Personal Data”, **Iowa Law Review**, C.80, Y. 1994, s. 445.

başvuru hakkı, doğrudan pazarlama gibi bazı konularda verilerin kullanılmasına izin vermeme hakkı²⁶⁰. Ayrıca AB Yönergesi'nin hassas kişisel veriler için daha güçlü bir koruma öngördüğünü de belirtmek gerekir.

AB veri koruma modelinin kilit özelliği ise “zorlayıcılığı”dır. AB üyesi devletlerin tamamında kişisel verilerin korunmasını güvence altına alan kuralların uygulanmasını sağlayacak birimler bulunmaktadır²⁶¹. Görüldüğü gibi Yönerge ile özellikle önleyici bir korumanın sağlanması hedeflenmektedir.

Veri Koruma Yönergesi'nin uygulama alanı birkaç açıdan sınırlandırılmıştır. Buna göre Yönerge, tamamı ya da bir bölümü otomatik olarak işlenen kişisel verilere ve otomatik olmayan yollarla işlenen verilerden bir dosyalama sistemine kaydedilenler veya kaydedilebilecek olanlar için uygulanır²⁶². Biraz karmaşık şekilde dile getirilmiş olsa da bu hükümden veri işleme usulünden bağımsız olarak neredeyse bütün kişisel verilerin korunması istendiği çıkarılabilir²⁶³. Nitekim günümüzde kişisel veriler, başta bilgisayarlar aracılığıyla olmak üzere, büyük oranda otomatik yollarla işlenmektedir²⁶⁴. Arşivdeki dosyaların ise pek çok yerde hızla elektronik ortama aktarıldığı görülmektedir.

Bununla birlikte Yönerge'nin uygulama alanı, verileri işleyen kişiye ve işleme amacına ilişkin olarak da bazı konularda sınırlandırılmıştır. İlk olarak AB'nin üçüncü sütununda yer alan ve topluluk hukukunun alanına girmeyen, kamu güvenliği, savunma, devlet güvenliği ve ceza hukuku alanında devletin etkinliklerinde Yönerge hükümleri uygulanmayacaktır²⁶⁵. Yönerge'nin 3/2 hükmü bu sınırı açıkça belirler. Buna göre, metinde yer alan hükümler, Avrupa Birliği Kurucu Antlaşması'nın²⁶⁶ V. ve VI. Başlıkları altında düzenlenen konular gibi topluluk hukukunun dışında bulunan alanlarda ve her halükarda genel asayiş, savunma,

²⁶⁰ AB Veri Koruma Yönergesi'nde belirlenen ilkeler çalışmamızın üçüncü bölümünde ayrıntılı olarak değerlendirileceği için burada belirtilmemiştir.

²⁶¹ **Privacy and Human Rights 2006**, s. 10.

²⁶² 95/46/AT, m. 3/1.

²⁶³ Oğuz ŞİMŞEK, s. 43.

²⁶⁴ Christopher KUNER, s. 99.

²⁶⁵ 95/46/AT, m.3/2, I. ATAD'a göre bu tür sınırlamaların dar yorumlanması gerekir. Bu bağlamda Mahkeme, “*asgari uyum*” düşüncesini reddetmekte, bunun Yönerge'nin bütüncül uyum hedefine ters düştüğünü savunmaktadır. Bkz. Yves POULLET, “EU data protection policy, The Directive 95/46/EC: Ten years after”, **Computer Law and Security Report**, 2006, s. 206-217.

²⁶⁶ Maastricht Antlaşması olarak da anılan Avrupa Birliği'ni Kuran Antlaşma, 7 Kasım 1992'de imzalanmış ve 1 Kasım 1993'te yürürlüğe girmiştir.

devletin güvenliği ve devletin ceza hukukuna ilişkin etkinliklerde kişisel verilerin işlenmesinde uygulanamaz.

AB Andlaşmasının V. başlığı “*Ortak Dış Politika ve Güvenlik Politikasına İlişkin Hükümler*” i içermektedir. VI. Başlık altında ise “*Adli Konularda Polis ve Adli İşbirliğine İlişkin Hükümler*” düzenlenmiştir. Oldukça önemli olan bu alanlarda Yönerge’nin zorlayıcılığı bulunmamaktadır. Polis ve adliye makamları arasındaki işbirliğinin amacı, suçluluk, ırkçılık ve yabancı düşmanlığı ile ortaklaşa mücadele ederek, vatandaşlara özgürlük, güvenlik ve adalet sağlamaktır²⁶⁷. Bu amacı gerçekleştirmek için çeşitli düzenlemeler yapıldığı görülür.

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.

Ancak 1 Aralık 2009 tarihinde Lizbon Antlaşmasının yürürlüğe girmesi Yönergenin uygulama alanına ilişkin bu önemli sorunun çözülmesini sağlamıştır. Özellikle bu Antlaşma ile AB’de Üçüncü Sütun’un kaldırılması kişisel verilerin korunması açısından olumlu bir etki yaratmıştır. Bu şekilde AAD’nin da çeşitli kararlarında oldukça zorlandığı bir konu olan, sütunlar arasındaki sınırların belirlenmesi gerekliliği ortadan kalkacaktır²⁶⁸.

İkinci bir istisna, gerçek kişilerce tamamen kişisel ya da ailevi etkinlikler çerçevesinde yapılan veri işlemlere Yönerge’nin uygulanamayacak olmasıdır²⁶⁹. Buna göre örneğin bir adres defteri, ticari ya da profesyonel amaçla değil, tamamen kişisel amaçlarla tutulmuşsa Yönerge’nin uygulama alanı dışında kalmaktadır. Bu,

²⁶⁷ Bkz. AB Antlaşması m.29-30. AB Antlaşması m.29/1 şöyledir: “*Avrupa Topluluğunun yetkilerine zarar vermeksizin, Birliğin amacı, üye devletler arasında cezai konularda polis ve adli işbirliği alanında ortak eylem geliştirerek, ırkçılığı ve yabancı düşmanlığını engelleyerek ve bunlara karşı mücadele ederek, vatandaşlara özgürlük, güvenlik ve adalet alanında üst düzey bir koruma sağlamaktır*”. Burada ve aşağıda AB Antlaşmasının Türkçe çevirisinde şu kaynaktan yararlanılmıştır: Haluk GÜNUĞUR, **Avrupa Birliği’nin Kurucu Antlaşmaları**, Avrupa Ekonomik Danışma Merkezi, Ankara 2005.

²⁶⁸ Kişisel verilerin korunması açısından Lizbon Antlaşması’nın değerlendirilmesine ilişkin olarak bkz. Peter HUSTINX, “Data Protection in the Light of the Lisbon Treaty and the Consequences for Present Regulation”, 11th Conference on Data Protection and Data Security-DuD 2009, Berlin 8 Haziran 2009, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2009/09-06-08_Berlin_DP_Lisbon_Treaty_EN.pdf, s. 1-10.

²⁶⁹ 95/46/AT, m.3/2,II.

sınırlarının kolaylıkla belirlenebileceği bir alan değildir. Örneğin hızla artan kullanımıyla pek çok kişinin günlük yaşamının bir parçası haline gelen sosyal ağlar üzerinde yer alan verilerin durumu ne olacaktır? Bu bağlamda Facebook, Twitter, MySpace gibi sosyal ağların kullanıcı etkinliklerinin bu istisna kapsamında değerlendirilip değerlendirilmeyeceği saptanmalıdır. Bu mecralarda pek çok kişi²⁷⁰ özel yaşamlarına ilişkin, kimi zaman oldukça ayrıntılı ve hassas, bilgileri kendi istekleri ile paylaşmaktadır.

29. Madde Veri Koruma Grubu'na göre sosyal ağ hizmetinden yararlanan kullanıcıların bazı etkinlikleri “*kişisel veya ailevi*” nitelikte bulunmamaktadır. Kullanıcının bir şirket ya da kurum adına hareket ettiği, ekonomik veya siyasi hedefler taşıdığı durumlar buna örnek olarak gösterilebilir. Bu durumda kullanıcının veri denetçisi olarak bazı yükümlülükleri bulunacaktır²⁷¹. Bu örnekte de görüldüğü gibi, Veri Koruma Yönergesi'nin uygulama alanının sınırlarını belirlemek kimi konularda yoruma muhtaç bir nitelik gösterir. Bu yorumu pek çok kez AAD kararlarından elde etmekteyiz.

AAD'nin bu bağlamda verdiği *Österreichischer Rundfunk* ve *Lindqvist* kararları üzerinde kısaca durmak gerekir²⁷². Mahkeme, her iki kararında da Yönerge'nin genel kural olarak uygulanması gerektiğine ve uygulama alanının bulunmadığı durumların istisnai nitelikte olduğuna ve bu nedenle dar yorumlanması gerektiğine işaret etmiştir²⁷³.

Österreichischer Rundfunk kararı, AAD'ın Kişisel Verilerin Korunması Yönergesi'ne ilişkin verdiği ilk karardır²⁷⁴. Kararda Avusturya kamusal yayın

²⁷⁰ Sosyal ağlar içerisinde en yüksek sayıda kullanıcıya hizmet sunan facebook Eylül 2008'de yüz milyon kullanıcıya ulaştığını açıklamıştır. facebook, kendi Internet sitesinde de şirket tanımını şöyle yapmaktadır: “*Facebook, insanlara paylaşma gücü verir ve dünyayı daha açık ve daha bağlı hale getirir. Milyonlarca insan, arkadaşlarıyla iletişim halinde olmak, sınırsız sayıda fotoğraf yüklemek, bağlantıları ve videoları paylaşmak ve tanıştıkları kişiler hakkında daha çok şey öğrenmek için her gün facebook'u kullanmaktadırlar*”. Bkz. <http://tr-tr.facebook.com/facebook>

²⁷¹ Bkz. Article 29 Data Protection Working Party, **Opinion 5/2009 on online social networking**, 01189/09/EN WP 163, 12 Haziran 2009.

²⁷² ECJ, Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauer mann (C-139/01) v Österreichischer Rundfunk, 20 Mayıs 2003, joined cases C-465/00, C-138/01, C-139/01; Lindqvist, C-101/01, 6 Kasım 2003.

²⁷³ Paul de HERT, Serge GUTWIRTH, s. 30.

²⁷⁴ Jane K. WINN, Benjamin WRIGHT, **Law of Electronic Commerce**, 4. Baskı, Aspen Law & Business, ABD 2000, § 15-05[A]. Karara ilişkin olarak ayrıca bkz. H. KHLERT, “Einheitliches Schutzniveau für personbezogene Daten in der Gemeinschaft”, European Law Reporter, 2003, s. 286-287.

organının, çalışanların ücretlerine ilişkin bilgiyi iletip iletemeyeceği tartışılmıştır. Bu bilgi herhangi bir üçüncü kişi tarafından değil, bir kamusal organ tarafından istenmiştir: Ulusal Muhasebe Kurumu (national accounting office), Parlamento’ya sunacağı yıllık rapor için bu bilgiye gereksinim duymaktadır.

AAD, kararında Veri Koruma Yönergesi’nin AİHS’nin 8. maddesi ışığında yorumlanması gerektiğine işaret etmiştir. Bu bağlamda ilgili kurumun çalışanlarının kişisel verilerinin üçüncü kişilere aktarılmasının özel yaşama bir müdahale oluşturacağını saptamıştır²⁷⁵. Ulusal mahkemeler, bu müdahalenin meşru olup olmadığını incelerken AİHS’nin 8/2 hükmünde yer alan ölçütleri dikkate almalıdır²⁷⁶. Ayrıca AAD’na göre Veri Koruma Yönergesi’nin Topluluk Hukuku’nda kaynağını iç pazar ve serbest dolaşımda bulması, somut olayda uygulanmayacağı anlamına da gelmemektedir²⁷⁷. Mahkeme’ye göre her türlü veri aktarımı kural olarak Verilerin Korunması Yönergesi’nin kapsamında yer almaktadır²⁷⁸.

AAD’ın Yönerge’nin uygulama alanına ilişkin önemli bir başka değerlendirmesi Lindqvist kararında bulunabilir²⁷⁹. Bu karar, İnternet ortamında bulunan kişisel veriler açısından Yönerge’nin uygulama alanına ilişkin genel kuralı belirlemektedir. AAD burada ilk olarak, “*veri işleme*”nin kapsamı hakkında bir değerlendirmede bulunmuştur. Buna göre Divan, kişilerin adları ve telefon

²⁷⁵ *Österreichischer Rundfunk kararı*, par. 21, 73-75.

²⁷⁶ *A.g.k.*, par. 76-90.

²⁷⁷ Paul de HERT, Serge GUTWIRTH, s. 30.

²⁷⁸ *A.g.k.*, par. 41-42. Bu konuda Mahkeme, Hukuk Sözcüsü (Advocate General) TIZZANO’nun görüşünü benimsememiştir. Nitekim TIZZANO’ya göre Verilerin Korunması Yönergesi, kişisel verilerin üye ülkelerde serbest dolaşımını sağlayacak bir uyumu hedeflemektedir. Temel hakların korunması ise Yönerge’nin müstakil bir hedefi değildir. Bkz. Opinion of Advocate General TIZZANO, Case C-465/00, 14 Kasım 2002.

²⁷⁹ Davaya konu olan olayda İsveçli bir kadın olan Lindqvist, bir kilisedeki gönüllü çalışmalarıyla ilgili bir İnternet sayfası hazırlamıştır. Burada yer alan yazılar içerisinde kilisede birlikte çalıştığı arkadaşlarına ilişkin kişisel veriler de yer almaktadır. Bunların arasında, bu kişilerin adları ve telefon numaraları yanında, hobilerine ve bir kişinin sağlık durumuna ilişkin bilgiler de bulunur. Lindqvist, bu bilgileri yayınlamadan önce ilgili kişilerin iznini almamıştır. Ancak eski çalışma arkadaşlarından bu bilgilerin kaldırılmasına yönelik bir uyarı alır almaz buna uymuş ve sitenin içeriğinden bunları çıkarmıştır. Buna karşın İsveç veri koruma yetkilileri tarafından Lindqvist hakkında soruşturma başlatılmış ve otomatik olarak kişisel verileri işlemesi ve bunları İsveç veri koruma yetkililerinden ve ilgili kişilerden izin almadan transfer etmesi nedeniyle tazminat ödemesine karar verilmiştir. Kararı temyiz eden Lindqvist, bilgileri bir İnternet sitesinde yayınlamanın bir “işleme” olamayacağını ve üçüncü ülkelere veri transferi anlamına da gelmeyeceğini belirtmiştir. Ayrıca Veri Koruma Yönergesi’nin kar amacı gütmeyen etkinliklere uygulanamayacağını, veri koruma yasasını ihlal ettiği gerekçesi ile ödemesine hükmedilen tazminat nedeniyle asıl kendisinin düşüncüyü açıklama özgürlüğünün ihlal edildiğini iddia etmiştir. Bunun üzerine Gota Temzyiz Mahkemesi, Yönerge’nin doğru yorumunu elde etmek amacıyla bu iddiaları ön sorun yaparak Divana sormuştur. Bkz. Case C-101/01.

numaraları gibi bilgilerin bir İnternet sitesinde yayınlanmasının, başka bir etkinliğe gerek görülmeksizin, “*verilerin otomatik yolla işlenmesi*” anlamına geleceğine hükmetmiştir. Divan’a göre her ne kadar Bayan Lindqvist’in verileri işlemesi, ekonomik bir amaca yönelmese de Yönerge’nin 3/2 hükmü kapsamında yer alan istisnalar içerisinde değerlendirilemez. İşlemenin bir hayır işi dolayısıyla olması, “*bireyin özel veya aile yaşamı*”na ilişkin bir etkinlik olarak görülmesini gerektirmemektedir. Kişisel verilerin İnternet ortamında yayınlanması, onları belirsiz sayıda kişinin erişimine açık hale getirilmesi bu istisnanın kapsamı dışına çıkmasına neden olmaktadır²⁸⁰.

İkinci olarak Divan, bu bilgilerin bir İnternet sitesinde yayınlanmasının üçüncü ülkelere veri aktarımı anlamına gelip gelmeyeceğini incelemiştir. Divan’a göre veriler, yalnızca İnternet ortamında yayınlanmaları dolayısıyla üçüncü ülkelere aktarılmış sayılmazlar. Ancak (i) eğer bu kişisel veriler, bu sayfaları özel olarak aramayan kişilere de gönderiliyorsa ve (ii) İnternet sunucu alt yapısı AB üyesi olmayan bir ülkede bulunuyorsa bu durum geçerli değildir. Üçüncü olarak Divan, Yönerge’nin kar amacı gütmeyen etkinliklere de uygulanacağına karar vermiştir.

Görüldüğü gibi Divan’ın saptamaları Avrupa veri koruma rejiminin oldukça geniş bir kapsama ulaştığını ortaya koymaktadır²⁸¹. Yönerge’nin etki alanı AB toprakları ile de sınırlı kalmamıştır. Nitekim Yönergenin AB üyesi olmayan pek çok ülkenin konuya ilişkin hukuksal düzenlemelerini de etkilediği bilinmektedir. Bu durum ilk olarak AB üyesi olmayan Avrupa ülkeleri açısından kendini gösterir. 1999 yılında Liechtenstein, Norveç, İzlanda gibi AET üyesi ülkeler de Yönerge ile bağlı kılınmıştır²⁸².

²⁸⁰ Bkz. **A.g.k.**, par. 27, 38, 43-48. Kimi yazarlar Divan’ın bu yaklaşımını Yönerge’nin yapılış amacının ötesinde bir uygulama alanını benimsediğini ortaya koyduğunu belirtmektedir. Örneğin Phillip LEITH’a göre Bayan Lindqvist’in İnternet sayfasında yer alan bilgiler, basılı bir iletişim aracı ile kilise üyeleri arasında paylaşılsaydı herhangi bir sorun oluşmayacaktı. Bu karar bağlamında artık yalnızca hayır işlerine ilişkin sayfaların içerik sağlayıcıları değil, İnternet’te her gün yeni bilgiler ekleyen pek çok gencin de dikkatli olması gerekir. LEITH’a göre bu yaklaşım şekli, başka bağlamlarda yasal kabul edilecek etkinliklerin suç haline getirilmesi sonucunu doğurmaktadır. Bkz. Philip LEITH, “The Socio-legal context of Privacy”, **International Journal of Law in Context**, C. 2, S. 2, Y. 2006, s. 128-129.

²⁸¹ Jaqueline Klosek, “European Court Establishes Broad Interpretation of Data Protection Law”, <http://library.findlaw.com/2004/Mar/19/133351.html>.

²⁸² Application to the EFTA countries Norway, Iceland and Liechtenstein under the EEA AGREEMENT Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement OJ L 296/41, 23 Aralık 2000.

İkinci olarak Yönerge'nin, yeterli koruma sağlamayan ülkelere veri aktarımını yasaklayan hükmü nedeniyle Avrupa dışındaki pek çok ülke de benzer içerikteki düzenlemeleri kabul etmiştir. Dolayısıyla Yönerge'nin AB sınırlarını aşan bir etkiye sahip olduğunu söylemek sanırız yanlış olmayacaktır. Bu. Yönerge'nin hazırlanma aşamasında öngörülen bir sonuç olabilir. Nitekim metnin aşağıda incelenecek 25. ve 26. maddeleri ve 4/1,c hükmü yalnızca AB ülkeleri için değil, küresel düzeyde bir sistem önerdiği izlenimi yaratmaktadır.

3. KİŞİSEL VERİLERİN ÜÇÜNCÜ ÜLKELERE AKTARILMASI

a. Genel Olarak

Gerçek ve sanal ağlarla bağlanmış dünyamızda bilgi sürekli hareket eder. Çağımızın koşullarının bir gereği olan bu durum kişisel verilerin korunması açısından önemli sonuçlar doğurmaktadır. Bu konunun siyasal ve sosyal boyutuna birinci bölümde değinmiştik. Hukuksal açıdan bakıldığında ise kişisel verilerin korunmasını etkin bir şekilde sağlayabilmek açısından bu durumu dikkate almak oldukça önemlidir. Çünkü herşeyden önce ulusal ya da bölgesel düzeyde korunan kişisel veriler, bu alanın sınırlarını aştıktan sonra korumasız mı kalacaklar sorusu akla gelir. Nitekim dünyanın her yerinde bu konuya, en azından günümüzde, aynı hassasiyetle yaklaşılmadığı bilinmektedir.

AB bünyesinde kişisel verilerin korunmasına ilişkin düzenlemeler hazırlanırken bu sorun dikkate alınmıştır. Kişisel Verilerin Korunması Yönergesi'ne bu engelin aşılması için yeterli düzeyde veri koruması sağlamayan ülkelere veri akışının yasaklanmasına ilişkin oldukça tartışmalı hükümlerin yerleştirildiği görülmektedir.

Bu tartışmalara girmeden bir temel ilkeyi hatırlatmak gerekir. AB üyesi pek çok ülkede aktarım, bir çeşit veri işleme olarak kabul edilmektedir. Bu nedenle belirtilen işlemin yasal bir temelini bulunması her durumda gereklidir. Bu, aktarımın üye devletler arasında yapılması halinde de geçerlidir²⁸³.

²⁸³ Örneğin İspanya'da bir Peugeot satıcısı firmanın, müşteri bilgilerini yine İspanya'da bulunan başka bir Peugeot satıcısı firmaya aktarması İspanya Veri Koruma Otoritesi tarafından değerlendirilmiştir. Müşterilerinin verilerinin yine aynı gruptaki başka bir satıcı firmaya aktarılabilmesine ilişkin genel ifadelerle bilgilendiren firmanın bu eylemini Veri Koruma Otoritesi yetersiz bulmuştur. Bkz. Christopher KUNER, s. 79-80.

İkinci olarak veri aktarımı konusunda teknolojik gelişmeler ile ortaya çıkan yeni özellikler dikkatten kaçmamalıdır. Nitekim verilerin aktarımı günümüzde konuya ilişkin ilk düzenlemelerin yapıldığı zamanla karşılaştırıldığında çok daha önemli bir duruma gelmiştir. Artık verilerin somut araçlarla aktarımı zorunluluğu kalmamıştır.

1990'lı yıllara gelinceye kadar bilgisayar ortamındaki verilerin aktarımı büyük oranda somut araçlarla gerçekleştirilmekteydi. Günümüzde ise her geçen gün daha yüksek miktarda veri, daha kısa zamanda sanal ortamda aktarılabilir. Saniyeler içerisinde kişinin bütün bir yaşamını kapsayan profil dünyanın öbür ucuna gönderilebilir. Ayrıca bu işlemin mutlaka fiilen yapılması da gerekli değildir²⁸⁴. Çoğu zaman İnternet ortamında bilgi belirli bir yerde bulunmaktadır. Bu bilgiye gereksinim duyan kişi ya da kurum, ilgili yere ulaşabildiği ölçüde onu elde edecektir. Bu noktada bir bilginin yalnızca İnternet ortamında bulunmasının veri aktarımı olarak nitelendirilip nitelendirilmeyeceği sorusu akla gelebilir. Bu, özellikle AB veri koruma mevzuatı açısından önemlidir.

b. 95/46/AT sayılı Yönerge Uyarınca “Veri Aktarımı”

Veri Koruma Yönergesi “aktarım”a ilişkin bir tanım geliştirmemiştir. Bu, hangi durumların veri aktarımı olarak değerlendirileceğini saptamayı güçleştirir. AAD’a göre ise bir bilginin yalnızca İnternet ortamında bulunması ile üçüncü ülkelere veri aktarımının gerçekleştiği söylenemez²⁸⁵.

AB Kişisel Verilerin Korunması Yönergesinde üçüncü ülkelere kişisel verilerin aktarımına ilişkin kurallar 25. ve 26. madde hükümlerinde düzenlenmiştir²⁸⁶. Yönerge uyarınca, kural olarak, üçüncü ülkelere veri aktarımı ancak bu ülkelerde kişisel verilerin “yeterli düzeyde” korunması durumunda olanaklıdır. Hemen belirtelim: Yönerge’nin bu hükmü Avrupa dışındaki ülkelere tepkiyle karşılanmıştır²⁸⁷. ABD başta olmak üzere pek çok ülkede hukukçuların ve iş çevrelerinin bu zorlayıcı hükme tepki gösterdikleri görülür.

²⁸⁴ Christopher KUNER, s. 80.

²⁸⁵ C-101/01, par. 52-71.

²⁸⁶ Üçüncü ülkelere veri aktarımının kurallarını belirleyen tek hukuksal düzenlemenin Veri Koruma Yönergesi olmadığı da unutulmamalıdır. AK Veri Koruma Sözleşmesi’nin 12. maddesi, OECD Rehber İlkelerinin 17 ve 18. paragrafları, BM Rehber İlkeleri kapsamında 9. ilke aynı konuya ilişkin kuralları belirlemektedir.

²⁸⁷ Andrew CHARLESWORTH, s. 65.

Kişisel Verilerin Korunması Yönergesi'nin temel amaçlarından biri, yukarıda da belirtildiği gibi, iç pazarda serbest veri akışını sağlamaktır. Nitekim Yönerge'nin gerekçe bölümünde de bu duruma *"kişisel veri akışının önündeki engelleri ortadan kaldırmak için, bu gibi verilerin işlenmesinde bireylerin hak ve özgürlüklerinin koruma düzeyinin bütün Üye Devletler'de eşit olması gerektiğinden"* ifadesiyle yer verilmiştir. Ancak yalnızca bu uyumlaştırmanın sağlanması yeterli değildir. Ayrıca veri koruma ilkelerinin etkin bir şekilde uygulamaya da geçirilmesi gerekir. Yeterli düzeyde koruma sağlamayan ülkelere veri akışının yasaklanması da bu kapsamda değerlendirilmelidir. Bu ilkenin benimsenmesindeki temel amaç, veri denetçilerinin kişisel verilerin korunması ilkelerini uygulamaktan kaçınmak amacıyla veri işleme operasyonlarını daha düşük koruma getiren, *"veri cennetleri"* olarak adlandırılacak, ülkelere kaydırmalarına engel olma²⁸⁸.

Buna rağmen, Avrupa iç pazarında verilerin serbest dolaşımına yönelik bu düzenlemede, üçüncü ülkelerle veri değişiminde böylesine ağır bir koşulun getirilmesi AB'nin buradaki gerçek niyetine ilişkin kuşkuların yükselmesine de neden olmuştur. Bu doğrultuda Avrupa'yı kendi sistemini dünyaya dayatmaya ve sanal ticarete ABD ile yarışabilmek için vakit kazanmaya çalışmakla, ayrıca tüketicileri serbest rekabet ortamından yoksun bırakmakla suçlayanlar bulunmuştur²⁸⁹. Bu iddiaların ne oranda haklı olduğu tartışmaya açıktır. Ancak şu bir gerçektir: Avrupa, uygulamada yaşadığı pek çok sıkıntıya ve soruna karşın, kişisel verilerin korunması konusunda kendi sistemini uluslararası alanda etkili bir model olarak kabul ettirmiştir.

c. "Yeterli Düzeyde Koruma" Koşulu

Uluslararası ticaretin ve küresel bilgi akışının günümüz ekonomik düzeninin en önemli bileşenlerinden olduğu ve Avrupa'nın da hem üretim hem de tüketim

²⁸⁸ Lee A. BYGRAVE, **Data Protection Law**, s. 79-80.

²⁸⁹ Tansuğ, bu tepkileri şu şekilde özetlemektedir: *"Bu durum ABD hukukçularının çoğunluğu ile yeni ekonomiye yön vermeye alışık iş çevrelerini teoride ve pratikte Avrupa'ya karşı tavır almaya itiyor. Onlar Avrupa'yı "perderşahi" bir tavrıla "değişime" karşı durmakla, "bilgiye erişim özgürlüğü"nü engellemekle, pahalı yeni bürokratik kurumlar yaratmakla, en önemlisi Avrupalı tüketiciyi kötü ve niteliksiz ürünleri pahalıya almaya mahkum etmekle suçlarken, "süzülmüş bir demokrasi ve insan hakları yaklaşımı" ile küresel bilgi trafiğine kırmızı ışıklar koyan Avrupa yoksa zaman mı kazanıyor?"*. Bkz. Avniye TANSUĞ, "AB'nin Yeni Ekonomi Silahı: "Veri Saklama Hukuku"..., **Bilişim Hukuku**, der. Mete TEVETOĞLU, Kadir Has Üniversitesi Yayınları, İstanbul 2006, s. 533. Konuya ilişkin kapsamlı bir değerlendirme için bkz. Peter P. SWIRE, Robert E. LITAN, **None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive**, the Brookings Institution Press, ABD 1998.

açısından dünyanın en değerli bölgeleri arasında yer aldığı gerçeğinden hareketle hangi durumda AB üyesi ülkelere üçüncü ülkelere veri aktarımı yapılabileceği üzerinde kısaca durmak gerekir.

Öncelikle kişisel verilerin “yeterli” düzeyde korunduğu ülkelere veri aktarımının gerçekleşmesinin olanaklı bulunduğu belirtilmelidir. Ancak “yeterli” düzeyin ne olduğunun saptanması pek de kolay değildir. Yönerge’ye göre, bir veri aktarımında ya da veri aktarımı grubunda, koruma düzeyinin yeterliliği bütün koşullar göz önüne alınarak değerlendirilecektir. Bu bağlamda, verinin niteliği, işlemenin (ya da işlemelerin) amacı ve süresi, çıkış yeri ülkesi ve varacağı ülke, üçüncü ülkede geçerli genel ve sektörel hukuk kuralları, bu ülkede uyulan mesleki kurallar ve uygulanan güvenlik önlemleri özellikle dikkate alınacaktır²⁹⁰. “Yeterli” düzeyin ne olduğu saptanırken, yalnızca ilgili hukukta konuya ilişkin olarak belirlenmiş kurallara değil, bu kuralların işlerliğini sağlamak için oluşturulmuş sisteme de bakmak gerekir.

Veri aktarımının gerçekleşmesi istenilen üçüncü ülkede verilerin yeterli düzeyde korunup korunmadığının saptanmasında hem üye devletlerin hem de Komisyon’un üzerine düşen çeşitli görevler bulunmaktadır. Yapılan inceleme sonucunda yeterli düzeyde korumanın sağlanmadığı fark edilirse Komisyon’un ve üye devletlerin birbirlerini durumdan haberdar etme yükümlülükleri bulunur²⁹¹.

Bu noktada bir hususa dikkat çekmek gerekir: her ne kadar Yönerge, üye devletlerde kişisel verilerin korunmasına ilişkin hükümleri uyumlaştırma amacı taşısa da, bu devletlerin tamamında birebir aynı koruma düzeyinin bulunduğu beklentisi gerçekçi değildir. Bu durumda ortaya çıkabilecek farklı uygulamalar, veri koruma düzeyinin en düşük olduğu ülkenin “AB veri koruması limanına” dönüşmesine neden olabilir. Üçüncü ülkelerde yeterli düzeyde veri korumanın bulunup bulunmadığının saptanmasında üye devletlere verilen görevler yanında, Komisyon’a da mutlak yetki tanınmasında bu kaygının etkili olduğu düşünülmektedir²⁹².

²⁹⁰ Veri Koruma Yönergesi, m. 25/2.

²⁹¹ Veri Koruma Yönergesi, m. 25/3.

²⁹² Nilgün BAŞALP, s. 69.

d. İstisnalar

Yönerge'nin 25/1 hükmünün katılığı, 26. maddede belirlenen bazı istisnalarla yumuşatılmıştır. Bu ise kişisel veri aktarımının Verilerin Korunması Yönergesi'nden sonra da büyük oranda aksamadan sürmesini sağlar²⁹³. Verilerin Korunması Yönergesi'ne göre eğer verilerin aktarılacağı ülkede yeterli düzeyde koruma yoksa aktarımın yapılabilmesi ancak istisnai bazı durumlarda söz konusu olabilir. Buna göre aşağıdaki durumlarda yasaktan muafiyet tanınmıştır²⁹⁴;

- *İlgili kişinin aktarım için açık rızasının bulunması*²⁹⁵: Yalnızca rızanın varlığı bu koşulun karşılanması için yeterli değildir. Ayrıca rızanın açık ve ilgili kişinin isteği konusunda şüphe bırakmayacak nitelikte; özgürce verilmesi ve ilgili kişinin bilgilendirilmiş olması gerekir.

- *Aktarımın bir sözleşmenin ifası veya ilgilinin talebi ile sözleşme öncesi bir ilişkinin yürütülmesi için gerekli olması*²⁹⁶: oldukça geniş kapsamlı bu istisna “gereklilik” ölçütü ile sınırlandırılmıştır. Gereklilik testinde, veri öznesi ile sözleşme arasında yakın ve gerçek bir bağ bulunması aranır. Bu durumda örneğin bir seyahat acentası ile yapılan sözleşme neticesinde, ilgili kişinin bilgilerinin kalacağı otele aktarılması bu istisna kapsamında değerlendirilebilir. Çünkü bu veri aktarımı seyahat acentasının yüklendiği işi gerçekleştirmesi için bir gerekliliktir.

- *Aktarımın ilgili kişinin çıkarlarının korunması doğrultusunda, veri kontrolörü ve üçüncü bir kişi arasında yapılan bir sözleşmenin sonuçlandırılması ve uygulanması için gerekli olması*²⁹⁷: Bir önceki istisnada olduğu gibi burada da aktarımın “gereklilik”i koşulu öne çıkmaktadır.

- *Aktarımın önemi bir kamusal çıkarın korunması; hukuksal taleplerin tesisi, ileri sürülmesi ve korunması için gerekli veya yasa gereği zorunlu olması*²⁹⁸: Buradaki “kamusal çıkar” ölçütünün dar yorumlanması gerekir. Aksi

²⁹³ Nilgün BAŞALP, s. 68.

²⁹⁴ Veri Koruma Yönergesi, Gerekçe par. 58, m. 26. Bu istisnai durumlara ilişkin kısa açıklamalarda 29. Madde Veri Koruma Grubunun, Yönerge'nin 26/1 hükmüne ilişkin yorumundan yararlanılmıştır: **Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995**, Article 29 Working Party, 25 Kasım 2005, 2093/05/WP 114.

²⁹⁵ Veri Koruma Yönergesi, m. 26/1,a.

²⁹⁶ Veri Koruma Yönergesi n. 26/1,b.

²⁹⁷ Veri Koruma Yönergesi, m. 26/1,c.

²⁹⁸ Veri Koruma Yönergesi, m. 26/1,d.

takdirde istisnanın sınırları özü ile bağdaşmayacak oranda genişleyebilir²⁹⁹. Veri Koruma Yönergesi'nin Başlangıç Bölümü'nde bu duruma örnek olarak vergi veya gümrük kurumları arasında veya sosyal güvenlik konularında yetkili birimler arasında uluslararası veri aktarımı gösterilmiştir³⁰⁰. Bunun yanında hukuksal taleplere ilişkin istisnanın da dar yorumlanması gerekir³⁰¹.

- *Aktarımın ilgili kişinin yaşamsal bir çıkarının korunması için gerekli olması*³⁰²: Bu istisna, ilgili kişinin sağlığına ilişkin acil bir durumda, tıbbi yardım alması için verilerin aktarılmasının gerekli olması halinde söz konusu olur.

- *Aktarımın herkese (ya da ilgisini kanıtlayan herkese) açık olan kamu sicillerinden yapılması ve veri koruma mevzuatının aradığı şartları taşıması*³⁰³: Bu istisna, mantıksal temelini kayıtların herkese açık olmasında bulur. Eğer ilgili ülkede meşru çıkarı olan herkes bu bilgilere ulaşabiliyorsa, üçüncü ülkelerde bulunan kişilerin de onlara ulaşmasında bir engel bulunmamalıdır. Ancak bu, verilerin veya veri kategorilerinin tamamının aktarılabileceği şeklinde yorumlanmamalıdır. Aktarım meşru çıkarı olanların talebi üzerine ya da bu kişiler alıcı konumunda ise söz konusu olacaktır³⁰⁴.

Belirtilen istisnaların dar yorumlanması gerekir³⁰⁵. Bu yorum şekli, istisnanın kural haline gelmesini önlemek açısından önemlidir. Ayrıca Yönerge'nin 26/1 hükmünün diğer hükümlerinden bağımsız olmadığı da unutulmamalıdır. Bu

²⁹⁹ Örneğin, 29. Madde Veri Koruma Grubu, aşağıda incelenecek Yolcu İsim Kayıtlarının (PNR) ABD'ye aktarılmasına ilişkin olarak açıkladığı görüşünde, bu aktarımın “önemli kamusal çıkar” temeline dayandığı görüşünü benimsememiştir. **Opinion 6/2002 on transmission Passenger Manifest Information and other data from airlines to the United States**, Article 29 Data Protection Working Party, WP 66, 24 Ekim 2002.

³⁰⁰ Veri Koruma Yönergesi, baş. par. 58. Yönerge'de yer verilen bu örnek, belirtilen istisnanın söz konusu olabilmesi için yalnızca üçüncü ülkenin kamusal menfaatinin bulunmasının yeterli olmadığını, AB üyesi ülkenin de somut olayda kamusal bir çıkarının bulunması gerektiğini ortaya koymaktadır. Bkz. **Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995**, s. 15.

³⁰¹ Örneğin merkezi AB toprakları dışında bulunan uluslararası bir şirketle, AB yurttaşı çalışanı arasındaki hukuksal çekişme dolayısıyla bu kişinin bilgileri aktarılabilir. Ancak bu istisna, bütün işçilerin kişisel dosyalarının, bir gün böyle bir uyuşmazlığın oluşması olasılığına karşılık, aktarılması durumunda geçerliliğini korumayacaktır. Bkz. **Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995**, s. 15.

³⁰² Veri Koruma Yönergesi, m. 26/1,e.

³⁰³ Veri Koruma Yönergesi, m. 26/1,f.

³⁰⁴ Veri Koruma Yönergesi, baş. par. 58.

³⁰⁵ **Working Document, Transfer of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive**, WP 12, 24 Temmuz 1998.

bağlamda örneğin özel nitelikteki (hassas) veriler için geliştirilen nitelikli koruma burada da dikkate alınacaktır³⁰⁶.

Gerçekleştirilmek istenen aktarıma, yeterli önlemlerin eşlik etmesi durumunda da izin verilebilir. Veri denetçisinin, ilgili kişinin temel haklarını korumak üzere “*uygun sözleşme hükümleri*” benimsemesi buna örnek olarak gösterilebilir³⁰⁷. Bu bağlamda Komisyon’un Yönerge’nin 31. maddesinde belirlenen usule uygun olarak yeterli güvenceyi sağlayacak, standart sözleşme hükümleri (standard contractual clauses) önermesi de olanaklıdır³⁰⁸.

Komisyon’un olumlu sonuçlanan bazı yeterlilik değerlendirmeleri bulunmaktadır. Bu bağlamda İsviçre, Kanada, Arjantin gibi bazı ülkelerin kişisel verilere “*yeterli*” düzeyde koruma getirdiği kabul edilmiştir. Bunun yanında veri aktarımı konusunda Amerika ile yapılan Bağımsızlık Sözleşmeleri ve yine Amerika’ya PNR verilerinin aktarılmasının kabulüne ilişkin kararlar bulunmaktadır³⁰⁹.

Son dönemde ise bazı iş çevrelerinin, “*yeterli koruma*” biçimi olarak “*bağlayıcı müşterek kurallar*”ın (Binding Corporate Rules-BCRs) kabulünü

³⁰⁶ **Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995**, s. 8.

³⁰⁷ Veri Koruma Yönergesi, m.26/2. Kişisel verilerin uluslararası aktarımını düzenlemede sözleşmelerin kullanılması elbette Yönerge ile getirilmiş bir yenilik değildir. 1992 yılında AK, Milletlerarası Ticaret Odası(ICC) ve Avrupa Komisyonu bu konuda ortak bir çalışma yapmışlardır. Bkz. “Modal Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows, with Explanatory Memorandum”, study made jointly by the Council of Europe, the Commission of European Communities and the International Chamber of Commerce, Strasburg 2 Kasım 1992; **Working Document, Transfer of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive**, s. 15.

³⁰⁸ Veri Koruma Yönergesi, m.26/4. **Decision 2001/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC**, OJ L 6, 10 Ocak 2002, s. 52-62; **Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC**, OJ L 181, 4 Temmuz 2001, s. 19-31; **Commission Decision of 27 December 2004, Amending Decision 2001/497/EC as regard to introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries**, OJ L 385, 29 Aralık 2004, s. 74-84.

³⁰⁹ **Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland**, OJ L 215, 25 Ağustos 2000; **Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate Protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act**, OJ L 2, 4 January 2002; **Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate Protection of personal data in Argentina**, OJ L 168, 5 July 2003. İsviçre, Kanada ve Arjantin’in yanında Birleşik Krallık’a bağlı olmayan küçük ada devletleri Guernsey, Isle of man ve Jersey için de Komisyon benzer kararlar vermiştir. AB ile ABD arasında kabul edilen Bağımsızlık Sözleşmeleri ve PNR verilerinin aktarımına ilişkin açıklamalar ise aşağıda yapılacaktır.

destekledikleri görülmektedir³¹⁰. Buradaki temel düşünce bir grup şirketin kendi veri koruma ilkelerini belirlemesi ve bu kuralların her bir şirket için zorlayıcı olmasıdır. Yetkili bir veri koruma otoritesi tarafından bu kurallar kabul edildiğinde şirket grubu içerisinde uluslararası veri aktarımı da olanaklı hale gelmektedir³¹¹.

e. Bağışıklık Sözleşmeleri (Safe Harbor)

Veri Koruma Yönergesi'nin 25. ve 26. maddelerinin “yeterli düzeyde” koruma sağlamayan ülkelere veri aktarımını yasaklamasına ilişkin tartışmalar yalnızca teorik düzeyde kalmamaktadır. Bu kural, uygulamada özellikle iki bölge arasında ciddi sorunların yaşanmasına neden olmuştur: nitekim AB ve ABD'nin kişisel verilerin korunmasına yaklaşımları oldukça farklıdır³¹².

ABD, kişisel verilerin korunmasına ilişkin ilk tartışmaların gündeme geldiği günden beri federal düzeyde bir yasa çıkarmaya olumlu bakmamıştır. Üstelik bu tutumunu birkaç farklı gruptan yönelen ciddi baskılara karşın sürdürmüştür. Bir yanda AB'nin dünyaya sunduğu model, diğer yanda Amerikan yurttaşlarından yükselen özel yaşamlarının ve kişisel verilerin korunmasına yönelik istemler³¹³, konuya ilişkin birkaç düzenleme önerisinin ötesinde bir sonuç getirmemiştir.

³¹⁰ Lee A. BYGRAVE, “International Agreements to Protect Privacy”, s.38.

³¹¹ Christopher KUNER, s. 219. Lee A. BYGRAVE, “International Agreements to Protect Privacy”, s.38-39. 29. Madde Veri Koruma Grubu, şirket gruplarının uyacakları davranış kurallarını saptamalarının oldukça sık görüldüğüne işaret etmiştir. Bu bağlamda özellikle uluslararası şirketler, kayıtların sistemlerinde ne kadar süreyle tutulacağına, gizli bilgilerin korunması, şirket aktiflerinin kötüye kullanılmasının yasaklanması gibi konuları içerdiği görülmektedir. Ayrıntılı değerlendirme için bkz. Article 29 Working Party, **Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers**, WP 74, 3 Haziran 2003.

³¹² CHARLESWORTH bu farklılığın temel nedenini şu şekilde açıklamaktadır: kişisel verilerin korunmasına Avrupa yaklaşımı, temelde özel sektörün hükümetçe düzenlenmesi şeklinde işlerken, ABD'de anayasa ile temellendirilen özel yaşamın gizliliği hakkının neredeyse bütün unsurları devlete karşı geliştirilmiştir. Andrew CHARLESWORTH, s. 66. Kişisel verilerin korunmasına ilişkin AB ve ABD yaklaşımlarının farklılığına ilişkin karşılaştırmalı bir değerlendirme için bkz. Alexendar GENZ, **Datenschutz in Europa und den USA, Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung**, Deutscher Universitäts-Verlag, Almanya 2004.

³¹³ Gerçekten yapılan araştırmalar, ABD vatandaşlarının gittikçe özel yaşamlarına ve kişisel verilerine yönelen saldırılardan daha çok rahatsız olduklarını ortaya koymaktadır Bkz. Dorothee HEISENBERG, s. 161. ABD'de gündemi meşgul etmiş pek çok önemli olay, toplumu kişisel veri piyasasının düzenlenmediği ve verilerin korunmadığı bir ortama ilişkin uyardır. Bu, özellikle sanal ortamda, sakıncalı görülen ürünlere ve sitelere karşı tüketici kampanyalarının yürütülmesine ve çok çeşitli kapsamlarda protestolarda bulunulmasına neden olmaktadır. Andrew CHARLESWORTH, s. 70. ABD'de Lotus MarketPlace ve Clipper çipine karşı yürütülen protestolara ilişkin olara bkz. Laura J. GURAK, **Persuasion and Privacy in cyberspace (The Online Protests over Lotus Market Place and the Clipper Chip)**, Yale University Press, ABD 1997.

ABD’de özel yaşamın gizliliğinin ve kişisel verilerin zayıf korunmasının nedenlerine ilişkin çeşitli görüşler bulunmaktadır. Öncelikle tarihsel ve kültürel etmenler dikkate alınabilir. ABD’de yalnızca kişisel verilerin korunması değil, daha genel olarak özel yaşamın gizliliği hakkı da oldukça zayıf bir şekilde korunmaktadır³¹⁴.

Ancak ABD’de kişisel verilerin korunmasının yetersiz düzeyde bulunmasının asıl nedeni pek çok yazara göre oldukça farklıdır: telekomünikasyon ve ileri teknoloji endüstrisinin bu düzenlemeleri istememeleri ve yürüttükleri güçlü lobicilik faaliyetleri ile genel ve kapsayıcı düzenlemeler yerine, kendiliğinden düzenlemenin propagandasını yürütmeleri. Bu nedenle çeşitli zamanlarda bazı Kongre üyeleri özel yaşamın gizliliğini ve kişisel verileri koruyan yasal düzenlemeleri destekleseler de bu girişimler endüstrinin baskısı sonucu engellenmiştir³¹⁵.

Sonuçta ortaya çıkan tablo, kişisel verilerin korunması açısından ABD’nin adeta “*vahşi batı*” olarak görülmesine neden olmaktadır. Ancak kimi yazarlar böylesine bir tanımlamanın çok abartılı olacağına, nitekim ABD’de kişisel verilerin korunmasına yönelik bazı girişimlerin bulunduğuna işaret etmektedir³¹⁶.

ABD’nde en olumlu ifadeyle verilerin oldukça sınırlı bir şekilde korunduğu söylenebilir. 1974 tarihli Özel Yaşamın Gizliliği Yasası (Privacy Act)³¹⁷, hükümetlerin elindeki bilgisayarlarda işlenen kişisel bilgileri kapsamına almaktadır. Bunun yanında, bazı sektörlerle ilişkin hukuksal düzenlemeler bulunsada bunlar yeterli düzeyin oldukça altında kalmaktadır. Birkaç istisnai konu dışında İnternet kullanımına ilişkin olarak da sınırlı bir koruma dikkat çekmektedir³¹⁸. Bunun yanında ABD’de konuya ilişkin olarak daha çok öz-düzenlemelerin (self regulation) desteklendiği görülmektedir³¹⁹. Ancak bütün bu yapı, Veri Koruma Yönergesi’nin 25. maddesi uyarınca aranan “*yeterli*” korumanın oldukça altındadır.

³¹⁴ Bruce SCHNEIER, s. 29.

³¹⁵ İçine AOL, Amazon.com, Yahoo!, e Bay, DoubleClick gibi sanal dünyanın güçlü temsilcilerini de alan bir lobicilik gurubu olan NetCoalition.com kendi kendine düzenlemeye ağırlık vermektedir ve bu yönde propaganda yapmaya devam etmektedir. Bkz. Bruce SCHNEIER, s. 35. Bu Ayrıca bkz. Dorothee HEISENBERG, s. 161.

³¹⁶ Axel SPIES, “USA: Datenschutz im Internet”, **MMR** 2002, Heft 7, s. 12-13. (KONTROL)

³¹⁷ Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579.

³¹⁸ David BANISAR, “Privacy and Data Protection Around the World”, s. 3.

³¹⁹ Öz düzenlemenin temeli “*güven*”dir. Bu bağlamda öz düzenleme yapacak olan tarafın doğru olanın ne olduğunu bileceğine ve dışarıdan zorlamaya gerek olmaksızın buna uyacağına güven duyulur. Öz düzenlemeden ayrıca, belirli bir sektörün uyacağı kuralları sektör içinde belirlemesi de anlaşılabilir. Buradaki temel düşünce, düzenlemeyi yapanların sektörün uygulamalarını,

Öte yandan dünyanın en önemli güçlerinden biri olan ABD, uluslararası ticarete de en etkin ülkelerdendir. Sınır ötesi bilgi akışının günümüz ticari ilişkilerindeki önemi göz önüne alındığında, AB ülkelerinden ABD'ye kişisel bilgi akışının durdurulmasının yaratabileceği sorunlar kolaylıkla anlaşılabilir. Bu durumda örneğin Avrupa'da yan kuruluşları bulunan bir Amerikan şirketi, ABD'deki merkezinde pazar kaynak bilgilerini değerlendiremeyecek ya da Avrupa'daki çalışanlarına ilişkin bilgilere ulaşamayacaktır. Bunun her iki bölge arasında ticareti olanaksız kılabileceğine ilişkin kaygılar, Yönerge'nin kabul edilmesinden kısa bir süre sonra soruna çözüm bulmaya yönelik görüşmelerin başlamasına neden olmuştur. 1998 yılında başlayan görüşmelerde kişisel verilerin korunmasına ilişkin yaklaşımları keskin bir şekilde ayrılan iki taraf arasında bir uzlaşa sağlanmaya çalışılmıştır³²⁰.

“Yeterli” düzeyde korumaya ilişkin pek çok tartışma yapıldıktan sonra 2000 yılında ABD ile AB sui generis³²¹ bir anlaşmaya varmışlardır³²². Komisyon'un en bilinen “yeterlilik” kararı olan bu uzlaşa “Bağımsızlık Sözleşmesi” (Safe Harbor) olarak Türkçe'ye çevrilebilir. “Safe Harbor”, kişisel verilerin korunması alanında farklı sistemler arasında uzlaşa sağlanmasının önemli bir örneğidir.

Bu, ABD ve AB arasında kabul edilen bir dizi veri koruma ilkesinden oluşur ve Amerikan Ticaret Bakanlığı yardımıyla yürütülecek bir program öngörür. Bu kapsamda kabul edilen ilkeler uyarınca, Amerikan ticari şirketlerinden, antlaşmada

gerekliliklerini en iyi şekilde bilecekleri ve bu nedenle kuralları belirlemede ve kendi belirledikleri kuralların uygulanmasını sağlamada en etkili yolu bulacaklardır. Ji Lian YAP, “The Regulation of Data Privacy in Hong Kong”, **Cyberlaw, Security and Privacy**, haz. Sylvia Mercado KIERKEGAARD, The Second Conference on Legal, Security and Privacy Issues in Information Technology (LSPI) 2007, China, 2. Baskı, Ankara Barosu Yayınları, Ankara 2007, s. 318. (317-330) Öz düzenleme yolu AB veri koruma hukuku kapsamında da desteklenmektedir. Bkz. Veri Koruma Yönergesi, m. 27. Bu noktada AB yaklaşımı ile ABD yaklaşımı arasındaki farklılık, ilkinde bu yöntem kapsayıcı koruma mekanizmasını destekleyen bir yan unsur olarak düşünülürken, ikincisinde kişisel verilerin korunmasının temelini oluşturmasından kaynaklanmaktadır. Öz düzenlemeye ilişkin olarak ayrıca bkz. **Self Regulation and Personal Data Protection**, haz. Working Group Meeting at Santa Cruz de la Sierra, Bolivya, 3-5 Mayıs 2006, Red Iberoamericano de Proteccion de Datos.

³²⁰ Robert BOND, s. 165.

³²¹ Mireille M. CARUANA, Joseph A. CANNATA, s. 102.

³²² Bkz. **2000/520/EC, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441)**, OJ L215, 25 Ağustos 2000. Safe Harbor sisteminin benimsenmesine götüren sürecin gelişimi için bkz. Andrew CHARLESWORTH, s. 260 vd.

belirtilen ilkelere³²³ bağlı olacaklarını belirterek, yeterli düzey koruma sağlayanlar, AB tarafından sanki bu ilkeyi gerçekleştirmiş bir ülkede işlem yapıyormuş gibi değerlendirileceklerdir. Böylece Bağışıklık Sözleşmesi kapsamında olan şirketlerle AB arasında veri aktarımı gerçekleştirilebilecektir³²⁴. Şirketlerin gerekliliklere uygun hareket etmeleri ise Amerikan yönetimi tarafından sağlanacaktır³²⁵.

Safe Harbor temel olarak verilerin işlenmesine ilişkin yedi ilkeyi içermektedir. Bunlar bildirim, seçim, aktarım, güvenlik, doğruluk, erişim ve uygulamaya ilişkindir³²⁶. Safe Harbor uyarınca özel nitelikli (hassas kişisel veriler) söz konusu olduğunda, özel bazı gerekliliklerde öngörülmüştür. Bu durumda eğer bu türdeki veri toplandığı sırada belirtilen amaçtan başka nedenlerle kullanılacaksa ya da üçüncü kişiye aktarılacaksa şirketin mutlaka rızayı “opt-in” alması gerekir³²⁷.

Safe Harbor uyarınca veri koruma otoritesi öngörülmemiştir. Ayrıca bu ilkelere bağlılığını açıklamak Amerikan şirketleri açısından bir zorunluluk da değildir. Ancak şirketlerin bağışıklık sözleşmesine katılımı tamamen gönüllük esasına dayansa da sözleşmeyi ihlal etmelerini engelleyecek bir sistem bulunmaktadır³²⁸.

³²³ Bkz. <http://www.export.gov/safeharbor/> (s.y. 23 Nisan 2009).

³²⁴ Bir şirketin bu sisteme katılabilmesi için şu basamakları izlemesi gerekir: 1. İlk olarak Amerikan şirketi, Safe Harbor’a katılmaya uygun olup olmadığını belirlemelidir. Amerikan Federal Ticaret Komisyonu (Federal Trade Commission-FTC) veya Ulaştırma Bakanlığı’nın (Department of Transportation) yetki alanına giren şirketler safe harbor’a katılabilmektedir. 2. İkinci olarak ilgili şirket, hangi uyumsuzluk çözüm yoluna ve uygulama sistemine (enforcement mechanism) bağlı olmak istediğini değerlendirmelidir. Genel olarak bu seçim hakkının (i) öz-düzenleme sistemi ile (ii) yasal ya da yönetsel bir sistem arasında kullanılabileceği söylenebilir. 3. Daha sonra ilgili şirketin ABD Ticaret Bakanlığı’na yetkili kişi tarafından imzalanmış ve safe harbor ilkelerine bağlılığın ifade edildiği yazılı bir onay belgesi göndermesi gerekir. 4. Ardından şirket, safe harbor ilkelerine bağlılığını ilan etmelidir. 5. Bundan sonra şirketin, ABD’de işlediği verilere ilişkin olarak safe harbor ilkelerini uygulaması gerekir. 6. Son olarak her yıl safe harbor’a üyeliğini tekrar onaylamalıdır. Bkz. Christopher KUNER, s. 180-185.

³²⁵ Andrew CHARLESWORTH, s. 68; András JÓRI, “dataprotection.eu”, <http://www.dataprotection.eu/>.

³²⁶ Christopher KUNER, s. 185-187. Bunların en azından beşi, AB Veri Koruma Yönergesi’nin 2 ile 14. maddeleri arasında düzenlenen kurallara işaret etmektedir. Hossein BIDGOLI, *The Internet Encyclopedia* (Cilt II), John Wiley and Sons Inc., ABD 2003, s. 224.

³²⁷ William G. STAPLES, *Encyclopedia of Privacy*, Greenwood Pres, ABD 2007, s.476.

³²⁸ William G. STAPLES, *Encyclopedia of Privacy*, s.475. Bununla birlikte Bağışıklık Sözleşmeleri’nin yeterli oranda zorlayıcı olmadığı yönünde önemli eleştirilerin bulunduğu da belirtilmelidir. Bu konuda bir değerlendirme ve çözüm önerisi için bkz. Daniel R. LEATHERS, “Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement”, *Case Western Reserve Journal of International Law*, C. 41, S. 1, Y. 2009, s. 193-242.

Safe Harbor, ABD merkezli şirketlerin AB ile veri akışını sağlayabilmesi açısından kullanışlı bir araç olarak değerlendirilebilir³²⁹. Ancak sistemin uygulanmasına ve etkinliğine ilişkin tartışmaların halen sürdüğü belirtilmelidir³³⁰. İş çevreleri bu sistemi, külfetli ve karmaşık olarak nitelendirmektedir. Bu nedenle Amerikan şirketlerinin Safe Harbor'a sınırlı katılımı dikkat çekmektedir³³¹. Ayrıca pek çok sivil toplum kuruluşu hazırladıkları raporlarda safe harbor'u AB'nde geçerli olan koruma düzeyine yaklaşmadığı ve ABD yurttaşlarının verilerinin korunmasını da sağlayamadığını ileri sürerek eleştirmiştir³³².

f. Havayolu Yolcu Kayıtlarının ABD'ye Aktarımı

AB Veri Koruma Yönergesi'nin uygulama alanına ilişkin önemli tartışmalardan bir diğeri, havayolu yolcu kayıtlarının (Passenger Name Records-PNR verileri) ABD idari makamlarına aktarılması ekseninde gelişmiştir. Aslında bu konu, yalnızca Yönerge'nin uygulama alanı açısından değil, hedefleri ve işlerliği açısından da çeşitli sorunların varlığını gözler önüne sermiştir.

11 Eylül 2001 saldırılarını izleyen günlerde ABD'de ulusal güvenliği arttırmaya yönelik çeşitli hukuksal düzenlemeler kabul edilir. Bu tarihte gerçekleştirilen terör saldırılarında sivil uçakların kullanılması, özellikle havayolu taşımacılığında güvenliğin artırılması isteğini gündeme getirmiştir³³³. ABD'nin PNR verilerinin aktarılmasına ilişkin talebi de bu kapsamdaki yasal düzenlemelerde öngörülmektedir.

³²⁹ Christopher KUNER, s. 191.

³³⁰ İlkelerin uygulanmasına ilişkin AB bünyesinden gelen bir değerlendirme için bkz. **The implementation of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce**, Commission Staff Working Document, Commission of the European Communities, 20 Ekim 2004, SEC(2004) 1323.

³³¹ 2005 yılında yalnızca 811 şirket safe harbor'a bağlılık listesinde yer almaktadır. William G. STAPLES, s. 476. Bu ilkelere uyacağını taahhüt eden şirketlerin güncel listesi için bkz. <https://www.export.gov/safeharbr/list.aspx>.

³³² William G. STAPLES, s. 476. Ayrıca bkz. Chris CONNOLLY, *The US Safe Harbor: Fact or Fiction?*, Galexia, 2008, http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/print-index.html.

³³³ Sivil havayolu taşımacılığında güvenlik gereksinim aslında bu tarihten çok daha önce, 1968 yılında siyasal gerekçelerle uçak kaçırmanın önemli bir tehlike olarak gündeme gelmesiyle başlamıştır. Bu konuya ilişkin ayrıntılı bilgi için bkz. Bruce HOFFMAN, **Inside Terrorism**, Columbia University Press, 2. Baskı, ABD 2006, s. 65 vd. Bu tehlikeye karşılık, ABD'de uçuş öncesi yolcu ve bagaj denetimi uygulaması başlamıştır. Bu denetim halen dünyanın dört bir tarafında sürdürülmektedir. Bkz. Ioannis NTOUVAS, "Air Passenger Data Transfer to the USA: the Decision of the ECJ and Latest Developments", **International Journal of Law and Information Technology**, C.16, S. 1, s. 72. (72-95)

İlgili yasa uyarınca çıkış ya da varış yeri ABD olan ya da ABD üzerinden yapılan uçuşlarda, hava yolu taşıma şirketinin ABD makamlarına bu uçuşlarda bulunan yolcuların kişisel bilgilerine elektronik ortamda ulaşma olanağı tanınması öngörülmüştür³³⁴. Buna göre hem Amerikan, hem yabancı hava taşıyıcıları iki tür veriyi yetkili birime sunmak zorundadır: (i) yolcu ve mürettebat listeleri(bu kapsamda havayolu ve uçuş bilgileri de yer almaktadır); (ii) PNR verileri. Her iki bilgi türü de kişisel nitelik taşımakla birlikte, ikinci türün daha hassas olduğu belirtilmelidir³³⁵.

Kısaca “PNR” olarak adlandırılan yolcu isim kayıtları, uçuşlara yer ayırtan her yolcuya ilişkin olarak havayollarının oluşturduğu dosyalara verilen genel addır. Bunlar havayolunun ilgili veri tabanlarında yer alır. Bu kayıtlar hava sanayine dâhil çeşitli kuruluşların (örneğin seyahat acentaları ya da bilgisayar rezervasyon sistemleri) yolcuyu tanımasını ve bu kişinin seyahatine ilişkin gerekli bilgilere (örneğin gidiş ve dönüş uçuşları, varsa aktarmaları, uçuşuna ilişkin özel talepleri) ulaşmasını sağlar³³⁶. PNR verilerinin kapsamında, kişinin uçuşu ile ilgili sağlık verilerine ya da yiyecek tercihleri dolayısıyla dini inançlarına ilişkin verilere ulaşılabilmesi olanaklıdır.

Bir başka anlatımla, PNR verileri, kimi hassas olan, kişisel nitelikteki verilerdir. ABD’nin yasal düzenlemeler ile bu verilerin kendi ülkesindeki ilgili birime aktarılmasını öngörmesi, AB veri koruma mevzuatı açısından sorun yaratmaktadır. Nitekim yukarıda işaret edildiği üzere AB’den üçüncü ülkelere veri aktarımı ancak “yeterli” koruma sağlandığı durumlarda olanaklıdır.

Bu, havayolu taşıyıcıları açısından ciddi bir sorun yaratmıştır. Gerçekten havayolu taşıyıcıları, verilerin aktarımını reddetmeleri durumunda Amerikan otoriteleri karşısında, verileri aktarmaları durumunda ise AB Üye Ülkeleri karşısında hukuksal sorunlar yaşama olasılığı ile karşı karşıya gelmiştir³³⁷. Nitekim AB veri koruma hukuku ile bu düzenleme arasında ortaya çıkabilecek potansiyel çatışmayı

³³⁴ Christopher KUNER, s. 22. Bkz. The Aviation and Transportation Security Act, Public Law 107-71, 19 Kasım 2001.

³³⁵ Ioannis NTOUVAS, s. 73.

³³⁶ Airline passenger data transfers from the EU to the United States (Passenger Name Record)-Frequently asked questions, MEMO/03/53, 12 Mart 2003 Brüksel. Ayrıca bkz. Katja WALETZKO, **Der gläserne Passagier - Datenüberwachung im amerikanischen Flugverkehr**, GRIN Verlag, Almanya 2007.

³³⁷ Ioannis NTOUVAS, s. 77.

fark eden AB Komisyonu, bu uygulamanın başlamasından kısa bir süre sonra, ABD hükümeti ile görüşmelere başlamıştır³³⁸.

Bu görüşmeler sonucunda varılan anlaşma ile AB'deki hava yolu şirketlerinin ABD'ye yapılan uçuşlarda PNR verilerini paylaşması kabul edilmiştir. Ancak Antlaşma'nın kabul ediliş sürecinde bazı sorunlar bulunmaktadır. 14 Mayıs 2004'te Avrupa Komisyonu bu antlaşmada belirlenen korumanın yeterli düzeyde olduğunu kabul etmiştir³³⁹. Konsey ise Parlamento'nun görüşünü beklemeden 17 Mayıs 2004'te bu kararı onaylamıştır³⁴⁰. Komisyon'un ve Konsey'in kararları Avrupa Parlamentosu ile çatışma yaşamalarına neden olmuştur. Bunun sonucunda Parlamento, Konsey ve Komisyon'a karşı AAD'da dava açmıştır³⁴¹.

Parlamento'nun iddiaları eylemin yasal temeline ve neticede varılan anlaşmanın içeriğine ilişkindir. Parlamento, Yönerge'nin kapsamı dışında kalan bir konuda Yönerge'ye dayanılarak karar verildiğini ve ayrıca ABD hükümetinin "yeterli" korumayı sağlamadığını ileri sürmüştür³⁴².

30 Mayıs 2006'da kararını açıklayan AAD, Konsey ve Komisyon'un işlemini geçersiz bulmuş ve Parlamento'nun istemi yönünde karar vermiştir³⁴³. Yalnız Antlaşma'nın kendisi yanında, Divan'ın kararı da birkaç açıdan tartışmaya açıktır.

³³⁸ Bkz. European Commission, MEMO/03/53, 12 Mart 2003.

³³⁹ **Commission decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (2004/535/EC)**, OJ L 235, 6 Temmuz 2004, s. 11.

³⁴⁰ **Council Decision of 17 May 2004 on the conclusion of an agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriersto the United States Department of Homeland Security, Bureau of Customs and Border Protection (2004/496/EC)**, OJ L 183, 20 Mayıs 2004, s. 83. Konsey bu noktada yaptığı değerlendirmede Komisyon'un ABD'nin taahhütlerini yeterli gördüğüne ilişkin bulguları dikkate almıştır. Bkz. Mehmet ÖZCAN, Fatma YILMAZ, "AB'nin Amerikanlaşan Terörle Mücadelesi", <http://www.usak.org.tr>.

³⁴¹ Divan, Parlamento'nun 9 Temmuz 2004'te açtığı iki davayı birleştirerek incelemiştir. Bunlardan birincisi Parlamento'nun "AB ve ABD arasında hava taşımacıları tarafından PNR verilerinin Amerikan Anavatan Güvenlik Bölümü, Gümrükler ve Sınır Koruma Bürosu'na akatarılması hakkındaki Antlaşma'nın akdedilmesi kararının iptali istemlidir. Bkz. C-317/04. İkincisi ise aktarılan PNR verilerinin yeterli düzeyde korunduğuna ilişkin Komisyon kararının iptali istemlidir. Bkz. C-318/04. Konsey'e karşı açılan davada Parlamento'yu Avrupa Veri Koruma Denetçisi, Konsey'i ise Komisyon ve Birleşik Krallık desteklemiştir. Ioannis NTOUVAS, s. 83, d.n. 73. Ayrıca bu süreç içerisinde çeşitli sivil toplum örgütleri de anlaşmaya tepki göstermiştir. Örneğin bkz. Privacy International, **Transferring Privacy: the Transfer of Passenger Records and the Abdication of Privacy Protection, The First Report on "Towards an International Infrastructure for Surveillance of Movement"**, Şubat 2004, <http://www.privacyinternational.org/issues/terrorism/rpt/transferringprivacy.pdf>.

³⁴² Christopher KUNER, s. 22.

³⁴³ **Joined Cases C-317/04 and C-318/04, European Parliament v Council of the European Union and Commission of the European Communities**, 30 Mayıs 2006, OJ C178/1, 29 Temmuz 2006.

Nitekim Divan, antlaşmayı Topluluk hukukunun kapsamı dışında kaldığı gerekçesiyle iptal ederken temel hak ve özgürlüklerin ihlaline ilişkin bir değerlendirme yapmaktan kaçınmıştır³⁴⁴. Bu noktada iki sorunun belirdiği görülmektedir.

Birincisi, Divan'ın bu kararı AB'de kişisel bilgileri toplayan ve daha sonra kamu güvenliği gibi amaçlarla ABD'ye aktarma olasılığı bulunan özel teşebbüslerin durumunu belirsiz kılmıştır. Çünkü böylece, AB Veri Koruma Yönergesi'nde güvenlik gerekçeleri için özel teşebbüslerce toplanan kişisel verilerin koruma dışı bırakılmasına neden olan açık bir kapı oluşturmuş gibi görünmektedir³⁴⁵. Bu nedenle AB'nin üçüncü sütununda yer alan konularda verilerin korunmasını sağlayacak araçlar geliştirilmesi yönünde tartışmalar başlamıştır.

İkincisi bu Antlaşma'ya ilişkin sorun yalnızca bir yetki sorunu değildir, Antlaşma'nın içeriği AB veri koruma hukukunun temel ilkelerine aykırılık oluşturacak niteliktedir. Benzer içerikteki bir antlaşmanın yetkili organ tarafından kabul edilmesi durumunda ATAD'ın tutumunun ne olacağı halen belirsizliğini korumaktadır³⁴⁶.

AAD'nin kararında değinmediği bazı sorunlar, kişisel verilerin korunması açısından oldukça önemlidir. İlk olarak bu kararlar neticesinde paylaşılan verilerin miktarı, terörle mücadele için gerekli olanın ötesindedir. Bunu orantılılık ilkesi ile bağdaştırmak olanaklı değildir. Verilerin havayolu taşımacılığının güvenliğini sağlamak dışında başka amaçlarla da kullanılabilmesi aktarımın sorunlu yanlarından bir diğerini oluşturur. Ayrıca PNR verilerinin aktarılması düşüncesi, mevcut bir terörizm olayıyla mücadeleye değil, olasılık üzerinden bir değerlendirmeye

³⁴⁴ Mehmet ÖZCAN, Fatma YILMAZ, "AB'nin Amerikanlaşan Terörle Mücadelesi", <http://www.usak.org.tr>. Mahkemeye göre antlaşmanın amacı, güvenliği güçlendirmek ile terörizm ve diğer ciddi suçları önlemektir. Bu nedenle AB Veri Koruma Yönergesinin uygulama alanının dışında kalmaktadır. Bkz. Veri Koruma Yönergesi, m.3/2. Dava konusu olan Konsey ve Komisyon kararları, AB Veri Koruma Yönergesi'ne dayanılarak verildiğinden, Mahkeme her ikisini de geçersiz bulmuştur. Christopher KUNER, s. 22; Spiros SIMITIS, "Übermittlung der Daten von Flugpassagieren in die USA: Dispens vom Datenschutz?" *NJW* 2006, Heft 28, s. 2012. Ayrıca bkz. Vanessa SERRANO, "Comment: The European Court of Justice's Decision to Anul the Aggrement Between the United States and European Community Regarding the Transfer of Personal Name Record Data, Its Effects, and Recommandations for a New Solution", *ILSA Journal of International and Comparative Law*, S.13, Y. 2006-2007, s. 453 vd.

³⁴⁵ Christopher KUNER, s. 22.

³⁴⁶ Nitekim ATAD kararının açıklanmasının ardından Avrupa Komisyonu'nca yapılan basın açıklamasında da Divan'ın Antlaşma'nın içeriğine ve ABD'nin taahhütlerinin "yeterli"liğine ilişkin bir konuda iptale gitmediğine dikkat çekildiği görülmektedir. Bkz. Commission's reaction to the ECJ judgement on Passenger Name Records, 30 Mayıs 2006 Brüksel.

dayanmaktadır. Bunun ise temel haklar açısından ciddi bir tehlike yarattığı ortadadır³⁴⁷. Yalnızca uçuş bilgilerine dayanılarak yapılan bir inceleme yolcuyla kişisel tercihleri dolayısıyla bir soruşturmanın eksenine yerleştirebilir³⁴⁸. Ayrıca antlaşmanın içeriğine ilişkin sorunlar bununla da sınırlı kalmamaktadır: verilerin AB'den ABD'ye doğru tek taraflı akışı ve verilere erişimin tekniği de tartışmalı konular arasındadır.

Divan, hukuksal bir karmaşayı önlemek ve iki tarafın da karara uygun önlemleri alması için makul bir süre tanımış ve kararın uygulamasını 30 Kasım 2006'ya ertelemiştir. Bu tarihten kısa bir süre önce, 16 Kasım 2006'da iptal edilen Antlaşma yerine önce geçici bir metin kabul edilmiş, ardından asıl Antlaşma ise 23 Temmuz 2007'de AB, 26 Temmuz 2007'de de ABD tarafından imzalanmıştır³⁴⁹.

Yeni uzlaşıda kişisel verilerin korunmasına ilişkin bazı kazanımların olduğu söylenebilir. Örneğin ABD ilgili birimlerine aktarılan veri miktarında azalma dikkat çekmektedir³⁵⁰. Ancak Antlaşma'nın geneline bakıldığında pek çok sorunun halen devam ettiği görülür. Özellikle verilerin ABD'de hangi birimlere aktarılacağına ilişkin kesin bir sınırlama belirlenmemiş olması önemli sorunların devam ettiğini göstermektedir. Bunun yanında ABD otoritelerince verilerin tutulma süresi 3,5 yıldan 7 yıla çıkarıldığı gibi, verilerin kötüye kullanılması durumuna karşın sağlam bir hukuksal yol da belirlenmemiştir³⁵¹.

³⁴⁷ Mehmet ÖZCAN, Fatma YILMAZ, "AB'nin Amerikanlaşan Terörle Mücadelesi", <http://www.usak.org.tr>.

³⁴⁸ Darjia MOROZOVA, "EU-US Passenger Name Record Data Transfer: Most Privacy Rights be a Casualty of the War on Terrorism", **EuroJournal.org**, Journal of Foreign Policy of Moldova, S. 6, Y. 2004, s. 4. Nitekim PNR verileri ABD'de özel bir dosyalama sisteminde tutulmaktadır. Bu sistem, kapsamında yer alan bilgilere dayanarak bir risk değerlendirmesi yapmakta ve yolcuları "kabul edilebilir risk", "bilinmeyen risk" ve "kabul edilemez risk" olarak üç gruba ayırmaktadır. Birinci grup yolcular açısından bir sorun bulunmazken, ikinci grubun kontrolleri daha sıkı yapılmakta, üçüncü grup ise polis tarafından incelenmektedir. Ioannis NTOUVAS, s. 75-76.

³⁴⁹ Antlaşma uyarınca taraflar uygulamaya ilişkin düzenli raporlar hazırlamak konusunda antlaşmışlardır. Amerikan Anavatan Güvenlik Bölümü 2008 yılında yayınladığı rapor'da daha önce yayınlanan 2005 raporundan beri PNR verilerinin kötüye kullanımına ilişkin hiçbir bildirim alınmadığına, bu verilere ulaşabilen birim ve kişilere yönelik eğitimlerin sürdüğüne, ilgililerin bu verilerin kullanımında gereken özeni gösterdiklerine ilişkin bilgiler yer almaktadır. U.S. Department of Homeland Security, **A Report Concerning Passenger Name Record Information Derived From Flights Between the U.S. and the European Union, Privacy Office U.S. Department of Homeland Security**, 18 Aralık 2008.

³⁵⁰ Mehmet ÖZCAN, Fatma YILMAZ, <http://www.usak.org>.

³⁵¹ Belirtilen sorunlara, AB Veri Koruma Denetçisi Peter HUSTINX, ilgili görüşmelerde yetkili olan Alman İçişleri Bakanı Wolfgang SCHAUBLE'ye gönderdiği ve kamuoyu ile de paylaşılan mektupta açıkça yer vermiştir. Bkz. "New PNR Agreement with the United States of America", 27 Haziran 2007 Brüksel, <http://epic.org/privacy/pdf/hustinx-letter.pdf>. Ayrıca AB veri koruma hukuku açısından çeşitli sorunların sürdüğü de belirtilmektedir. Öncelikle, aşağıda veri koruma

Bütün bu sorunlar, her iki bölge arasında kişisel verilerin korunmasına yönelik yaklaşım farkında kaynağını bulmaktadır. İlginç bir gelişme ise, yolcu bilgilerinin aktarımı konusunda ABD'nin AB organları yerine doğrudan bazı üye ülkelerle anlaşması olmuştur. Şubat 2008'de bu konuda Çek Cumhuriyeti ile imzalanan ve yolcu bilgilerinin ABD'ye akatarımını gerektiren mutabakat tutağını³⁵² başka ülkelerle aynı konuda yapılan görüşmeler izlemiştir³⁵³. Her ne kadar bütün bu süreç boyunca AB ile ABD arasında havayolu taşımacılığında fiilen bir sorun yaşanmasa da belirtilen eksenlerdeki hukuksal sorunlar bir süre daha tartışılacak gibi gözükmektedir. PNR verilerine ilişkin yaşanan bu gelişmeler, iki önemli ekonomik gücün kişisel verilerin korunması konusundaki farklı yaklaşımlarının uygulamada yaratabileceği sorunlara ilişkin güncel bir örnek oluşturmaktadır. Ancak daha da önemlisi ne yazık ki Avrupa'da veri koruma hukukunun naifliğini ortaya koymuş olmasıdır.

C. TELEKOMÜNİKASYON ALANINDA DÜZENLEMELER

1. 2002/58/AT sayılı Özel Yaşamın ve Elektronik İletişimin Korunması Yönergesi

Yukarıda işaret edildiği üzere 95/46/AT sayılı Yönerge, kişisel verilerin korunmasına yönelik genel ve kapsayıcı hükümler içermektedir. Ancak bu alanda öne çıkan bazı sektörlerde özel düzenlemeler yapma gerekliliği de hissedilmiştir.

hukukunda hâkim olan temel ilkeler kapsamında inceleneceği üzere, veri kontrolünün üçüncü kişilere aktarılan kişisel verilere ilişkin olarak ilgili kişiyi bilgilendirme yükümlülüğü bulunmaktadır. Havayolu yolcu kayıtlarının aktarımına ilişkin durumda veri kontrolü bir ya da birden çok havayolu yanında, ilgili durumlarda seyahat acentası ya da bilgisayar rezervasyon sistemi de olabilir. Bu konuya ilişkin olarak bkz. Article 29 Data Protection Working Party, Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities, kabul tarihi: 15 Şubat 2007, yeniden gözden geçirilme ve güncellenme tarihi: 24 Haziran 2008, 00345/07/EN WP 132, 00345-01/07/EN WP 151.

³⁵² Memorandum of understanding between the Ministry of the Interior of the Czech Republic and the Department of Homeland Security of the United States of America regarding the United States visa waiver program and related enhanced security measures, <http://www.statewatch.org/news/2008/mar/us-czech-mou-visas-etc.pdf> . Dönemin Çek Cumhuriyeti İçişleri Bakanı, diğer pek çok AB üyesi devlette olduğu gibi Çek Cumhuriyeti yurttaşlarının da Amerika yolculuklarında vize muafiyetinden yararlanmaları isteğinin bu tutanağın imzalanmasındaki itici güç olduğunu belirtmiştir. Bkz. "A divided Europe wants to protect its personal data wanted by the US", <http://www.rue89.com/2008/03/04/a-divided-europe-wants-to-protect-its-personal-data-wanted-by-the-us> . AB içerisinde ise Amerika'nın Birlik'i devreye sokmadan doğrudan üye devletlerle bu konuda görüşmeler yapması tepki uyandırmıştır. Bkz. "Brussels attacks new US security demands", 14 Şubat 2008, <http://euobserver.com/9/25657#> .

³⁵³ Bkz. <http://www.statewatch.org/news/archive2008.htm> .

Özellikle telekomünikasyon sektörünün kendine özgü niteliğini dikkate alan ve bu konuda AB Veri Koruma Yönergesi'ni tamamlayan bir düzenleme yapılması gereksinimi 1997 yılında 97/66/AT sayılı Telekomünikasyonun Gizliliği Yönergesi'nin³⁵⁴ kabul edilmesinde etkili olmuştur.

Bu Yönerge, telefon, dijital televizyon, mobil ağlar ve diğer telekomünikasyon sistemlerini kapsayan özel hükümler içermektedir. Telekomünikasyon Gizlilik Yönergesi, kullanıcının iletişiminin gizliliğini sağlamak için kullanıcı ve taşıyıcılara geniş kapsamlı yükümlülükler getirmiştir³⁵⁵. Bu bağlamda 97/66/AT sayılı Yönerge, daha önce veri koruma hukukunun boşluklarının bulunduğu alanları doldurmuştur. Örneğin, pazarlama etkinliklerinde olduğu gibi, fatura verilerine ulaşma ciddi oranda sınırlandırılmıştır³⁵⁶.

2000 yılı Temmuz ayında Avrupa Komisyonu elektronik iletişim sektöründe verilerin korunması için yeni bir yönerge tasarısı hazırlamıştır. Avrupa içerisindeki elektronik iletişim pazarında rekabeti güçlendirmeyi amaçlayan bu Yönerge, geniş kapsamlı bir paket olarak sunulmuştur. İlk önerildiği şekliyle Yönerge, telekomünikasyona ilişkin mevcut düzenlemeleri geliştirerek, kişisel verilerin korunmasını güçlendirmekteydi. Ancak daha sonra Bakanlar Konseyi, İnternet servis sağlayıcılara ve telekomünikasyon operatörlerine güvenlik gerekçeleriyle bütün telefon aramalarının, e-postalarının, faksların ve İnternet hareketleri kayıtlarının(logs) depolanmasını öngören veri tutma (data retention) hükümlerinin eklenmesi için baskı yapmıştır. Parlamentonun ise büyük bir çoğunluğu buna karşı çıkmıştır³⁵⁷. Ancak kısa bir süre sonra dengenin değiştiği görülecektir.

11 Eylül 2001 saldırıları Avrupa'yı da etkilemiş ve üye devletlerin Konsey'in veri tutmaya ilişkin tasarısı için Parlamento'nun üzerinde oluşturdıkları baskı artmıştır. Oylama Konsey'in lehine sonuçlanır³⁵⁸. Böylece 25 Haziran 2002'de AB Konseyi, Parlamento'da oylandığı şekliyle 2002/58/AT sayılı Elektronik İletişim Alanında Özel Yaşamın Gizliliğinin Korunması ve Kişisel Verilerin İşlenmesine

³⁵⁴ Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.

³⁵⁵ Bu konuda bkz. Nilgün BAŞALP, s. 87-90.

³⁵⁶ **Privacy and Human Rights 2006**, s. 10.

³⁵⁷ **Privacy and Human Rights 2006**, s. 11.

³⁵⁸ Jody R. WESTBY, **International Guide to Privacy**, American Bar Association, ABD 2005, s. 104. Ayrıca bkz. J. E. J. PRINS, M. J. M. Van DELLEN, **Digital Anonymity and the Law: Tensions and Dimensions**, Asser Press, ABD 2003, s. 170 vd; Clive WALKER, Yaman AKDENİZ, s. 167.

İlişkin Yönerge'yi³⁵⁹ kabul eder³⁶⁰. Bu Yönerge'nin kabulü ile 97/66/AT sayılı Yönerge, 30 Ekim 2003 itibariyle yürürlükten kalkmıştır³⁶¹.

Elektronik İletişim Yönergesi, yerini aldığı Telekomünikasyon Veri Koruma Yönergesi'nde olduğu gibi, belirli bir sektöre ilişkin düzenlemeler getirmektedir, bununla birlikte uygulama alanının çok daha genişlediğini belirtmek gerekir. Yönerge'nin bazı bölümleri ise Veri Saklama Yönergesi ile eklenmiştir³⁶².

Artık üye devletler, cep telefonları, kısa mesajlar(SMS), telefon hatları, fakslar, e-postalar, sohbet odaları, İnternet ya da başka herhangi bir araç üzerinden yapılan iletişimin trafik ve yer verilerini tutacak yasaları kabul edebileceklerdir. Bu, ulusal güvenlikten, suçluluğun önlenmesi, araştırılması ve takibine kadar çeşitli gerekçelerden kaynaklanabilir³⁶³.

Elektronik İletişim Yönergesi, Verilerin Korunması Yönergesi'nin aksine gerçek kişiler yanında tüzel kişileri de koruma kapsamına almaktadır³⁶⁴. Yönerge, kamusal ulaşılabilir elektronik iletişim araçlarınca işlenen verilere uygulanacaktır³⁶⁵.

29. Madde Veri Koruma Grubu'nun yorumuna göre, özel ağlar Yönerge'nin uygulama alanı dışındadır. Ancak uygulamada bazı durumlarda üye devletlerde kapalı ağlar operatörlerinin de bu ilkelerle sorumlu tutulduğu görülmektedir³⁶⁶.

Bunun yanında Yönerge'nin belirtilen amacına uygun bir şekilde AB Verilerin Korunması Yönergesi'ni tamamlayan ve bazı açılardan verilerin korunmasını güçlendiren hükümleri de bulunmaktadır. Nitekim Elektronik İletişim Yönergesi'nde özel olarak düzenlenmeyen konularda AB Verilerin Korunması

³⁵⁹ Bundan böyle Elektronik İletişim Yönergesi olarak anılacaktır.

³⁶⁰ **Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and protection of privacy in the electronic communications sector**, OJ (Official Journal of the European Communities), 31 Temmuz 2002, L201/37, http://www.dataprotection.ie/documents/legal/directive2002_58.pdf (s.y. 20 Nisan 2009). Yönergenin Türkçe çevirisi için bkz. Hayrunnisa ÖZDEMİR, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin, Ankara 2009, s. 243-260.

³⁶¹ Bkz. 2002/58/AT sayılı Yönerge, Gerekçe par. 4, m. 19.

³⁶² Christopher KUNER, s. 24; Jody R. WESTBY, s. 102.

³⁶³ Bkz. 2002/58/AT sayılı Yönerge m. 15. **Privacy and Human Rights 2006**, s. 12.

³⁶⁴ 2002/58/AT sayılı Yönerge, m. 1/2.

³⁶⁵ Bkz. 2002/58/AT sayılı Yönerge, m.3/1.

³⁶⁶ Bu konuda Almanya'nın yaklaşımı için bkz. Christopher KUNER, s. 25. 29. Madde Veri Koruma Grubu'nun değerlendirmesi için bkz. Article 29 Working Party, 'Opinion 7/2000 on the European Commission Proposal for a Directive of the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM(2000)385, WP 36, 2 Kasım 2000, s.2-3.

Yönergesinin uygulanacağı belirtilmiştir³⁶⁷. Bu bağlamda çeşitli konularda 95/46/AT Yönergesi'ne atıfta bulunulduğu görülmektedir³⁶⁸. Ancak bu bazı sorunlara da neden olur. Öncelikle uygulamada ne zaman Verilerin Korunması Yönergesi'nin, ne zaman Elektronik İletişim Yönergesi'nin uygulanacağı belirlenmelidir. Temel olarak Verilerin Korunması Yönergesi'nin genel bir düzenleme olduğu, Elektronik İletişim Yönergesi'nin ise belirli alanlarda uygulanacak özel bir düzenleme olduğu söylenebilir³⁶⁹.

Bu noktada 29. Madde Veri Koruma Grubunun yorumu yol göstericidir³⁷⁰. Buna göre, Veri Koruma Yönergesi, Elektronik İletişim Yönergesi'nin kapsamadığı alanlarda uygulanacaktır. Kamusal açıdan ulaşılabilir olmayan iletişim hizmetleri bunun bir örneğidir. Ayrıca kişinin İnternet bağlantısı sırasında gönüllü olarak paylaştığı kişisel bilgiler her zaman bu Yönerge'nin kapsamında değerlendirilecektir. Bu durumda hangi Yönerge'nin uygulanacağı araştırılırken bu metinlerin kapsamına dikkat etmek ve bunun sonucunda yalnızca birinin mi yoksa her ikisinin birden mi uygulama alanına girdiğini saptamak gerekir. Nitekim bazı durumlarda aynı anda gerçekleştirilen birden fazla etkinlik her iki Yönerge'nin birden kapsamına girebilir. Bir İSS'nin İnternet erişimi, web sitesi yöneticiliği(hosts websites) ve kendi web sitelerini işlettiği durumlar buna örnek olarak gösterilebilir³⁷¹.

Ayrıca Yönerge'de AB Temel Haklar Şartı'nda yer alan özel yaşamın gizliliği ve kişisel verilerin korunması haklarına saygı gösterilmesi gerektiğine, uluslararası sözleşmelere ve AİHS'nde düzenlenen haberleşmenin gizliliği hakkının önemine de özel olarak işaret edilmiştir³⁷². Yönerge'de düzenlenen belli başlı konular şöyle sıralanabilir³⁷³:

³⁶⁷ Bkz. 2002/58/AT sayılı Yönerge, Gerekçe par. 10.

³⁶⁸ Oğuz ŞİMŞEK, s. 58; Marie-Theres TINNEFELD, s. 128, 130.

³⁶⁹ Elektronik İletişim Yönergesi'nin uygulama alanına ilişkin kapsamlı bir değerlendirme için bkz. Christopher KUNER, s. 135-141.

³⁷⁰ 29. Madde Veri Koruma Grubu'nun raporu her ne kadar Elektronik İletişim Yönergesi'nin yürürlükten kaldırdığı Telekomünikasyon Gizlilik Yönergesi'ne ilişkin olsa da bu yeni düzenleme açısından da değerlendirilmeye alınabilir. Christopher KUNER, s. 27; Article 29 Working Group, "Privacy on the Internet", s. 22-23.

³⁷¹ Christopher KUNER, s.28.

³⁷² Bkz. 2002/58/AT sayılı yönerge, Gerekçe par. 2, 3.

³⁷³ Christopher KUNER, s. 25-26. Elektronik İletişim Korunması Yönergesi'ne paralel bir düzenleme Türkiye'de bir yönetmelik kapsamında yapılmıştır. 2004 tarihli Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik çalışmamızın III. Bölümünde değerlendirilecektir. Bu değerlendirmeler Elektronik İletişimin

- *Güvenlik*: Kamusal olarak ulaşılabilir bir elektronik iletişim hizmet sağlayıcı, hizmetinin güvenliğini sağlamak için gereken önlemleri almalı, sistemde bir güvenlik açığı bulunduğunda da abonelerini bu konuda bilgilendirmelidir³⁷⁴.

- *İletişimin Gizliliği*: Üye devletler ulusal hukuklarında yapacakları düzenlemeler ile iletişimin gizliliğini sağlamak zorundadırlar. Bu kapsamda özellikle, kişilerin rızası olmaksızın, iletişimin ve trafik verilerinin dinlenilmesi, izlenilmesi, kaydedilmesi gibi içeriğine ulaşma ve gözetleme yöntemlerine karşı gerekli önlemlerin alınması zorunludur³⁷⁵. Ancak ulusal güvenlik gibi bazı gerekçelerle, her durumda demokratik toplumda zorunluluk ve ölçülük ilkelerine uyularak, bu güvenceye istisna getirilebilir³⁷⁶. Burada Klass kararından beri AİHM'nin yerleşik olarak kabul ettiği bir ilkeye atıf yapıldığı görülmektedir³⁷⁷.

-*Veri İşlemenin Sınırlandırılması*: Trafik verilerinin ve fatura bilgilerinin işlenmesi belirli açılardan sınırlandırılmıştır³⁷⁸. Kamusal olarak ulaşılabilir elektronik iletişim hizmetlerin kullanıcıları ayrıntılı faturalama, arayan kişinin numarasının görülmesi, arama aktarma ve rehberlerde yer alan kayıtlar konusunda çeşitli haklara sahiptir. Örneğin, kullanıcı faturalarının ayrıntılı olmasını istememe hakkı bulunmaktadır³⁷⁹. Eğer arayan numaranın gösterilmesi hizmeti sunuluyorsa, hem arayan açısından numarasının gizlenmesi, hem de aranan açısından gizliliği kaldırma haklarının tanınması gerekir³⁸⁰. Abonenin, üçüncü bir kişiye otomatik arama aktarmayı önleme olanağı bulunmalıdır³⁸¹. Ayrıca kişilerin onayı alınmaksızın telefon numaralarının ve adreslerinin rehberlere kaydedilmemesi gerekir. Bu

Korunması Yönergesi ile karşılaştırmalı olarak yapılacağından, Yönerge'nin kapsadığı ilkelere burada yalnızca özet olarak değinilmiştir.

³⁷⁴ 2002/58/AT sayılı Yönerge, m. 4.

³⁷⁵ 2002/58/AT sayılı Yönerge, m. 5.

³⁷⁶ 2002/58/AT sayılı Yönerge, m. 15/1.

³⁷⁷ Bkz. Klass ve diğ, Almanya'ya karşı. Ayrıca bkz. yuk. "AİHS" başlıklı bölüm.

³⁷⁸ 2002/58/AT sayılı Yönerge, m. 6,7.

³⁷⁹ 2002/58/AT sayılı Yönerge, m. 7.

³⁸⁰ 2002/58/AT sayılı Yönerge, m. 8/1.

³⁸¹ 2002/58/AT sayılı Yönerge, m. 11.

gereklilik hem sabit telefon ve posta adresi, hem de cep telefonu ve elektronik posta adresi için geçerlidir³⁸².

- *İstenmeyen İletiler*: “Spam” adı verilen istenmeyen iletilere ilişkin düzenleme de bulunmaktadır. Otomatik arama makinelerinin, faksların ya da elektronik postaların doğrudan pazarlama amacıyla kullanılması ancak ilgilinin “opt-in” rızası ile olanaklıdır³⁸³.

- *Çerezlerin (cookies) ve Casus Yazılımların (spyware) Kullanımı*: Çerezler veya benzeri araçların kullanılabilmesi ancak Verilerin Korunması Yönergesi’ne uygun bir şekilde açık ve tam olarak bilgilendirilmesi ile olanaklıdır³⁸⁴.

- *Yer Bilgileri* : Kamusal ulaşılabilir iletişim ağlarını ve hizmetlerini kullananların yer bilgileri ancak anonim hale getirilirse ya da kullanıcı buna izin verirse işlenebilir³⁸⁵.

- *Verilerin Saklanması*: Üye devletler, belirli nedenlerle Yönerge’de güvence altına alınan bazı hakların koruma alanını azaltabilirler. Burada verilerin saklanmasına ilişkin süreler örnek olarak verilebilir. Verilerin saklanması hükümleri, aşağıda incelenecek olan, Veri Saklama Yönergesi ile değiştirilmiştir³⁸⁶.

Elektronik İletişim Yönergesi’nin daha etkin hale getirmek amacıyla bir değişiklik önerisi ise halen görüşülmektedir³⁸⁷. Bu öneride özellikle Yönerge’nin veri güvenliğine ilişkin hükümlerini güçlendirmek ve zorlayıcılığını arttırmak hedeflenmiştir³⁸⁸.

³⁸² 2002/58/AT sayılı Yönerge, m. 12.

³⁸³ 2002/58/AT sayılı Yönerge, m. 13.

³⁸⁴ 2002/58/AT sayılı Yönerge, m. 5/3.

³⁸⁵ 2002/58/AT sayılı Yönerge, m. 9.

³⁸⁶ 2002/58/AT sayılı Yönerge, m.15/1; Christopher KUNER, s. 26-27.

³⁸⁷ 13 Kasım 2007’de Komisyon 2002/58/AT sayılı Yönerge’de değişiklik öngören tasarımı kabul etmiştir. İlk değerlendirmenin ardından 24 Eylül 2008 tarihinde Parlamento, Komisyon’un görüşleri doğrultusunda, tasarıda uygun gördüğü değişiklikleri kabul etmiş ve ardından 27 Kasım 2008’de AB Konseyi siyasal uzlaşya (political agreement) ulaşmıştır. 29. Madde Veri Koruma Grubu’nun bu sürecin çeşitli aşamalarında görüşünü açıkladığı görülmektedir. Bkz. **Opinion 8/2006**, 26 Eylül 2006; **Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)**, WP 150, 15 Mayıs 2008; **Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)**, WP 159, 10 Şubat 2009.

³⁸⁸ **Article 29 Data Protection Working Party, Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)**, 15 Mayıs 2008, s. 2.

2. İletişim Trafik Verilerinin Saklanması Yönergesi

15 Mart 2006'da AB Konseyi, 2006/24/AT sayılı İletişim Trafik Verilerinin Saklanması Yönergesi'ni kabul etmiştir³⁸⁹. 2005 yılı Temmuz ayında İngiltere'de yaşanan terör eylemi Yönerge'nin kabul edilmesine hız kazandırmıştır³⁹⁰. Yönerge'nin çıkarılmasında terörizmle mücadele amacıyla trafik verilerine ulaşılmasını sağlamak için üye devletlerde veri saklama kurallarını uyumlaştırma düşüncesi etkilidir³⁹¹.

Bu Yönerge, üye devletlerin hizmet sağlayıcıları, iletişim verilerini altı ayla yirmi dört ay arasında tutmaya zorlamaktadır³⁹². Yönerge'nin uygulama alanı yalnızca iletişim trafik verileri ve bulunulan yer bilgileri için geçerlidir. Bunun ne anlama geldiğini biraz açmak gerekir. Kaydedilmesi öngörülen veriler sabit ya da mobil telefon görüşmeleri, kısa mesaj gönderimi, İnternet bağlantısı gibi etkinlikleri kullanan kişinin adı, soyadı, posta, e-posta ya da IP adresi, iletişimi gerçekleştirdiği saat, tarih, iletişimin süresi gibi bilgilerdir. Bu kapsamda iletişimin içeriğine ilişkin bilgiler yer almamaktadır³⁹³. Nitekim içeriğe ilişkin bilgilerin bu kapsamda kayıt edilemeyeceği Yönerge'de de açık bir şekilde belirtilmiştir³⁹⁴. Verilerin

³⁸⁹ **Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in the connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC**, OJ L 105, 13 Nisan 2006. Yönerge'de Üye Devletlere burada yer alan ilkeleri iç hukuklarına aktarmaları için 15 Eylül 2007'ye kadar süre tanınmıştır. Ancak bu sürenin 15 Mart 2009'a kadar ertelenebileceği de belirtilmiştir. Bkz. 2006/24/AT sayılı Yönerge, m. 15. Ayrıca belirtmek isteriz ki burada, "verilerin saklanması", İngilizce "*data retention*", Almanca "*Vorratsdatenspeicherung*", Fransızca "*Conservation de données*" deyimlerinin karşılığı olarak kullanılmıştır. Her ne kadar kimi Türkçe kaynaklarda farklı ifadeler yer verilmiş olsa da (örneğin bkz. Oğuz ŞİMŞEK, s. 66 vd.) bu deyim konuyu daha iyi ifade ettiği düşünüldüğü için tercih edildiğini belirtmek gerekir.

³⁹⁰ Christopher KUNER, s. 28, 2006/24/AT sayılı Yönerge, Gerekçe, par. 10.

³⁹¹ Ancak şu da belirtilmelidir: güvenlik gerekçeleriyle kişilerin iletişimlerinin izlenmesi yeni bir yöntem değildir. 1920'li yıllardan bugüne çeşitli amaçlarla devlet organları bu yöntemle başvurulmuştur. Bkz. Peter SHAAR, **Das Ende der Privatsphäre**, s. 117.

³⁹² 2006/24/AT sayılı Yönerge, m. 6. Bu zorunluluğu gerçekleştirmesi gereken kuruluşların Yönerge'de belirtilenden daha geniş yorumlanabileceğine de dikkat çekilmektedir. Bu noktada Fransa'daki uygulamaya ilişkin bir örnek için bkz. Christopher KUNER, s. 29.

³⁹³ 2006/24/AT sayılı Yönerge, m. 5. Yönerge'nin 5. maddesi uyarınca Üye Devletlerin iletişim trafik verilerinin saklanması sağlayacağı kategoriler tek tek sayılmıştır. Buna göre temel olarak şu alanlardaki verilerin saklanması gerekmektedir: (i) iletişimin kaynağını tespit ve takip için gerekli veriler; (ii) iletişimin istikametini belirlemek için gerekli olan veriler; (iii) iletişimin süresini, zamanını ve tarihini belirlemek için gerekli olan veriler; (iv) iletişimin türünü belirlemek için gerekli olan veriler; (v) kullanıcıyı iletişim araçlarını belirlemek için gerekli olan veriler; (vi) mobil iletişim aracının yerini belirlemek için gerekli olan veriler.

³⁹⁴ 2006/24/AT sayılı Yönerge, m. 1/2, 5/2.

saklanmasıdaki amaç ise ciddi suçların araştırılması, soruşturulması ve kovuşturulmasıdır³⁹⁵.

İletişim Trafik Verilerinin Saklanması Yönergesi, kişisel verilerin korunması alanında en çok tartışılan hukuksal metinlerden biridir. Herşeyden önce kişileri iletişim ve trafik verilerinin suç işlediklerine ilişkin somut bir belirti bulunmaksızın kayıt altında tutulması AİHS ve diğer pek çok insan hakları metni ile belirlenen özel haberleşmenin gizliliği ve masumiyet karinesine aykırılık oluşturmaktadır³⁹⁶. Üstelik temel hak ve özgürlükler açısından ciddi sorunlar yaratabilecek bu metinde yer alan hükümlerin uygulama alanı da adeta sınırsızdır. Verilerin saklanması için belirlenen “ciddi suç” ölçütü içeriği tam olarak belirlenemeyen, geniş bir alanı nitelemektedir.

Nitekim 29. Madde Veri Koruma Grubu da verilerin yalnızca belirli amaçlar için saklanması gerektiğine işaret etmiştir. Bu nedenle “*ciddi suç*” deyiminin içeriği belirlenmeli ve sınırlandırılmalıdır. Veri Koruma Grubuna göre Yönerge’nin uygulama alanı başka açılardan da sınırlandırılmalıdır. Buna göre, verilere yalnızca bu iş için görevlendirilmiş güvenlik birimleri ulaşabilmeli, bir suçtan dolayı şüpheli olmayan kişiler hakkında veri tabanı içerisinde araştırma yapılmamalıdır³⁹⁷. Bunun yanında hizmet sağlayıcıları böylesine bir zorunluluk altında tutmanın mali yükleri de dikkate alınmalıdır. Yönerge’ye göre hizmet sağlayıcıların masraflarının kendilerinin ya da devletin tarafından karşılanacağına kararı üye devletlere bırakılmaktadır.

İletişim Trafik Verilerinin Saklanması Yönergesi ayrıca şöyle bir ikilem içermektedir: verilerin saklanması kamu düzeni açısından öngörülmüş bir konuyken, verileri saklayanlar, pek çok durumda, iletişim hizmet sağlayıcıları yani özel teşebbüslerdir. Bu durumun yaratabileceği sakıncaları önlemek için Veri Koruma Grubu’nun da önerdiği üzere, iletişim hizmet sağlayıcılarının Yönerge kapsamında

³⁹⁵ 2006/24/AT sayılı Yönerge m. 1/1.

³⁹⁶ İletişim Trafik Verilerinin Saklanması Yönergesi’nin özel yaşamın gizliliği hakkını koruyan yeterli güvenceleri sağladığına ilişkin karşı görüş için bkz. Francesca E. BIGNAMI, “Privacy and Law Enforcement in the European Union: The Data Retention Directive”, **Chicago Journal of International Law**, C.8, S. 1, Y. 2007, s. 233-255. Ayrıca bkz. https://www.datenschutzzentrum.de/allgemein/061004_vdspeicherung.htm.

³⁹⁷ Article 29 Data Protection Working Party, **Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC**, WP 119, 25 Mart 2006.

yer alan durumlar dışında verileri işleyebilmelerinin kesin olarak önüne geçilmelidir³⁹⁸.

Ayrıca Yönerge bazı belirsizlikler de içermektedir. Örneğin hangi şirketlerin bu Yönerge'deki ilkelere uygun olarak verileri saklaması gerektiği tam olarak açık değildir. Bunun yanında temel hedeflerinden biri Üye Devletler'de konuya ilişkin düzenlemeler arasındaki uyumu sağlamak olan Yönerge'de, devletlere geniş takdir alanı bırakan hükümlerin yer alması bu hedefin gerçekleştirilebilirliğine ilişkin kuşku yaratmaktadır. Yönerge'ye göre üye devletler verilerin tutulacağı süreye ilişkin altı ayla yirmi dört ay arasında bir sınır belirlemelidirler. Verilerin asgari süre olan altı ay tutulmasına karar veren bir devlet ile azami süre olan yirmi dört ay tutulmasına karar veren bir devlet arasında uygulamada ne oranda bir uyum gerçekleşebileceği şüphelidir.³⁹⁹

Bu açıklamalar ışığında şu saptamayı yapmak sanırız yanlış olmayacaktır: Avrupa'da veri özneleri birbirleriyle ilişkili iki sistem ile karşı karşıya olduklarını kavramalıdır. Bunlardan bir verilerin korunması sistemi, diğeri ise verilerin saklanması sistemidir. İletişim verilerine uygulanan ikinci rejimde veri öznelerinin herhangi bir denetim olanağı bulunmamaktadır⁴⁰⁰. Bu durum temel hak ve özgürlükler açısından ciddi bir sorun yaratmaktadır. Nitekim trafik verilerinin analizi bir kişinin siyasal, ekonomik, cinsel, dini tercihlerine ilişkin ayrıntılı bilgiler sunabilmektedir. Bir başka anlatımla iletişimin içeriğine ilişkin herhangi bir kayıt tutulmaksızın, yalnızca iletişimin hangi araçla, nerede, kiminle, ne zaman ve ne

³⁹⁸ Wim SCHREURS, Mireille HILDEBRANDT, Els KINDT, Michaël VANFLETEREN, **Profiling the European Citizen, Cross-Disciplinary Perspectives**, haz. Mireille HILDEBRANDT, Serge GUTWIRTH, Springer, 2008, s. 266. (241-270)

³⁹⁹ Christopher KUNER, s. 31.

⁴⁰⁰ Wim SCHREURS, Mireille HILDEBRANDT, Els KINDT, Michaël VANFLETEREN, s. 267; Peter SHAAR, **Das Ende der Privatsphäre**, s. 119. Bunun yanında Yönerge'nin hukuksal temelden yoksun olduğuna ilişkin itirazlar da bulunmaktadır. İletişim Trafik Verilerinin Saklanması Yönergesi, yukarıda incelenmiş olan Havayolu Yolcu Bilgilerinin (PNR) Aktarılması kararıyla aynı hukuksal temele dayanmaktadır. Gloria Gonzalez FUSTER, Pieter PAEPA, "Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects", **Security versus Justice?**, haz. Elspeth GUILD, Florian GEYER, Ashgate, İngiltere 2008, s. 135. (129-152) Bu karar ise bilindiği gibi, ATAD tarafından hukuksal temelden yoksun bulunmuştur.

uzunlukta yapıldığının saptanmasının özel yaşama müdahale oluşturacak çok önemli bilgiler barındırabildiği unutulmamalıdır⁴⁰¹.

⁴⁰¹ Nitekim AİHM de çeşitli kararlarında bu duruma işaret etmiştir. İletişimin izlenmesine ilişkin değerlendirmede bulunduğu Malone, Birleşik Krallık’a karşı kararında (b.n. 8691/79, k.t. 2 Ağustos 1984) Mahkeme şu saptamada bulunmuştur: “*Hükümetin haklı olarak belirttiği gibi, sayaç denetim yazıcısı, bir telefon hizmet vericisinin kural olarak meşru bir biçimde ve özellikle aboneye doğru ücret tahakkuk ettirebilmek veya hizmete ilişkin şikâyetleri veya kötüye kullanma ihtimallerini araştırabilmek için, elde edebileceği bilgiyi kaydetmektedir. O halde niteliği gereği sayaçlama, haklı kılınmadıkça demokratik bir toplumda istenmeyen ve gayrimeşru olan iletilerin izlenmesinden ayrı tutulmalıdır. Ne var ki Mahkeme, sayaçlamadan elde edilen verilerin hangi şartlarda ve hangi amaçlarla kullanılırsa kullanılsın, Sözleşme’nin 8. maddesine göre bir soruna yol açmayacağı görüşünü kabul edemez. Sayaçlama kayıtları, çevrilen numaralar gibi, telefonla yapılan iletişimin bütünüleyici bir unsuru olan bilgiyi içermektedir. Sonuç olarak Mahkeme’nin görüşüne göre, abonenin rızası olmaksızın bu bilginin polise verilmesi de Sözleşme’nin 8. maddesindeki bir hakka müdahaledir*”(par. 84). Mahkeme daha sonra verdiği Copland Copland, Birleşik Krallık’a karşı (b.n. 62617/00, k.t. 3 Nisan 2007) kararında aynı yorumun e-postaların izlenmesi açısından da geçerli olduğunu ortaya koymuştur (par. 41). Ayrıca bkz. Patrick BREYER, “Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with ECHR”, **European Law Journal**, C. 11, S. 3, Y. 2005, s. 365-375.

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL İLKELERİ

I. GENEL OLARAK

Yukarıda uluslararası alanda kişisel verilerin korunmasına ilişkin çeşitli düzenlemelerden söz etmiştik. Yaklaşımlardaki farklılığa karşın konuya ilişkin düzenlemelerde, ortak olan bazı temel ilkeler bulunmaktadır. Bu doğrultuda aşağıda kişisel verilerin korunmasında hakim olan temel ilkeler, belli başlı düzenlemelerdeki farklılıklara dikkat çekilerek biraz daha yakından tanıtılmaya çalışılacaktır. Ancak bu ilkeler belirlenirken ve kapsamaları değerlendirilirken diğerlerine göre daha yüksek oranda ağırlık Avrupa sistemine verilmiştir.

Bunun bir nedeni, pek çok sorunlu yönüne karşın, şu an için hem ulusal, hem uluslararası düzenlemeler açısından kişisel verilerin korunması konusunda dünyadaki en gelişmiş modelin Avrupa’da görülmesidir. Bir diğer nedeni ise, bu bölgedeki düzenlemelerin Türkiye açısından önemidir. Nitekim bu başlık altında yapılacak açıklamaların bir amacı, bir sonraki bölümde incelenecek Türkiye’de kişisel verilerin korunması konusuna temel oluşturmaktır.

Kişisel verilerin korunması hukukunda hâkim olan temel ilkelere ilişkin açıklamalara geçmeden önce son olarak şuna işaret etmek isteriz: belirtilen ilkelerin birbirlerinden kesin çizgilerle ayrılması oldukça zordur. Aşağıda görüleceği gibi, kimi ilkeler diğerlerine kaynaklık eden genel bir nitelik sergilerken, pek çoğu da birbirini tamamlamaktadır. Bu nedenle yapılan açıklamalar değerlendirilirken bu ilkelerin birbirleri ile olan yakın ilişkisi unutulmamalıdır.

II. KİŞİSEL VERİLERİN NİTELİĞİNE İLİŞKİN İLKELER

Konuya ilişkin pek çok metinde, kişisel verilerin işlenmesinde belirli bir niteliğin karşılanması gerektiğine yönelik ilkeler belirlenmiştir. “*Verilerin kaliteli*

*olması ilkesi*¹ olarak da ifade edilebilecek bu gerekliliğin içeriği, 95/46/AT sayılı Yönerge'nin 6. maddesinde beş ayrı fıkrada belirlenir. Buna göre kişisel veriler, (i) hukuka ve dürüstlük kurallarına uygun işlenmeli, (ii) belirli, açık ve meşru amaçlar için toplanmalı, (iii) toplanma ve daha sonrasında işlenme amaçlarına uygun, ilgili bulunmalı ve aşırı olmamalı, (iv) doğru ve eğer gerekli ise güncel olarak tutulmalı, (v) amacın gerektirdiğinden daha uzun bir süre tutulmamalıdır. Şimdi bu gereklilikleri biraz daha yakından inceleyelim.

A. HUKUKA VE DÜRÜSTLÜK KURALLARINA UYGUN İŞLEME

Konuya ilişkin pek çok önemli metinde, birbirine yakın ifadelerle, kişisel verilerin hukuka ve dürüstlük kurallarına uygun işlenmesi ilkesinin yer aldığı görülür². Bu, kişisel verilerin korunması hukukunun birincil ilkesi olarak değerlendirilebilir. Çünkü bu ilke temelde aşağıda incelenecek diğer bazı ilkeleri de kapsar ve bunların kaynağını oluşturur³. Bu ilişkiyi açıklayabilmek için öncelikle ilkenin iki parçasını ayrı ayrı değerlendirmemiz gerekir. Bunlar ise (i) kişisel verilerin *hukuka* ve (ii) *dürüstlük* kurallarına uygun işlenmesidir.

Hukuka uygun olma gerekliliği kendi kendini açıklar niteliktedir. Kolaylıkla anlaşılabilceği gibi bu gereklilik, kişisel verilerin işlenmesinde yasalarla ve diğer hukuksal düzenlemelerle getirilen ilkelere uygun hareket edilmesi zorunluluğunu ifade eder. AB Yönergesi'nde işleme oldukça geniş bir şekilde tanımlanmıştır. Buna göre:

¹ “Verilerin belirli bir niteliği karşılması” burada İngilizce “*data quality*”, deyiminin karşılığı olarak kullanılmıştır. Bu deyim tam Türkçe karşılığı “*verilerin kaliteli olması*”dır. Nitekim pek çok çalışmada, belirtilen ilkenin karşılığı olarak bu deyim tercih edildiği görülür. Örneğin bkz. Oğuz ŞİMŞEK, s. 83 vd. Ancak burada “*Verilerin belirli bir niteliği karşılması*” deyiminin anlatılmak isteneni daha iyi karşılayacağı düşüncesiyle tercih edildiği belirtilmelidir. Nitekim öğretide bu deyim tercih eden kimi yazarlar bulunmaktadır. Örneğin bkz. Leyla KESER BERBER, Mahir M. ÜLGÜ, Cüneyd ER, **Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği**, İstanbul 2009, s. 126 vd.

² Bkz. AB Yönergesi m. 6/1,a, 108 sayılı AK Sözleşmesi m. 5/a, BM Rehber İlkeleri 1. ilke. Bunun yanında OECD Rehber İlkeleri par.7’de ve APEC Çerçeve Belge, par.18’de olduğu gibi kimi metinlerde başka bazı ilkelerle birlikte anıldığı da görülmektedir. Ayrıca pek çok ulusal düzenlemelerde de yine kişisel verilerin hukuka ve dürüstlük kurallarına uygun işlenmesi ilkesine yer verilmektedir. Örneğin bkz. İtalyan Veri Koruma Yasası m. 9, İsviçre Veri Koruma Yasası m. 4/2, 1998 Birleşik Krallık Veri Koruma Yasası, B.1, ek 1. Federal Alman Veri Koruma Yasası’nda ise dürüstlük kuralına yer verilmemiş olmakla birlikte 4/1 hükmünde şu ifade yer alır: “(k) *kişisel verilerin toplanması, işlenmesi ve kullanımı ancak bu yasa ile ya da başka bir yasal hükümle öngörülmüşse veya izin verilmişse ya da veri öznesinin rızası bulunuyorsa kabul edilebilir*” ifadesi yer almaktadır.

³ Lee A. BYGRAVE, **Data Protection Law**, s. 58.

“‘kişisel verinin işlenmesi’ (‘işleme’) toplama, kaydetme, düzenleme, saklama, uyarlama veya değiştirme, geri alma, danışma, kullanma, ileti ile açığa çıkarma, yayma veya başka şekilde oluşturma, sıraya koyma veya birleştirme, engelleme, silme veya yok etme gibi otomatik olan veya olmayan araçlarla, kişisel veri üzerinde uygulanan her türden işlem veya işlem dizisi anlamına gelir”⁴.

AK Sözleşmesi’nde de işleme bütün bu süreçleri kapsar şekilde tanımlanmıştır⁵. Öyleyse sürecin tamamında hukuka uygun hareket edilmesi temel bir gerekliliktir. Aşağıda belirtilen ve hukuksal düzenlemelerde öngörülen diğer ilkeler de hukuka uygun hareket etmenin doğal bileşenlerini oluşturacaktır.

İkinci olarak kişisel verilerin işlenmesine ilişkin her türlü eylemde dürüstlük kuralına uyulmalıdır. Yalnız dürüstlük kuralına uygun hareket etmenin kapsamını belirleyebilmek biraz daha güçtür. Dürüstlük (fair) ile anlatılmak istenenin ne olduğu zaman içerisinde değişebilmektedir⁶. Ancak en genel şekliyle, konumuz açısından dürüstlük kuralına uygun olma ilkesi ile veri denetçilerinin, veri işlemedeki hedeflerine ulaşmaya çalışırken, ilgili kişilerin çıkarlarını ve makul beklentilerini dikkate almaları gerektiğinin ifade edildiği söylenebilir⁷. Bu, işlemin ilgili kişi için şeffaf olması ve veri koruma görevlisinin bilgilendirme ve uyarı yükümlülüklerine uygun hareket etmesi gerekliliğini de kapsar⁸. Yasal bir temele

⁴ AB Yönergesi m. 2/b.

⁵ AK Sözleşmesi’ne göre otomatik işleme “bütünüyle ya da bir bölümü otomatik şekilde olmak üzere: şu işlemleri kapsar: verilerin depolanması, bu verilerin üzerinde mantıksal ya da aritmetik işlemlerin uygulanması, bunların değiştirilmesi, silinmesi, düzeltilmesi veya yayınlanması” Bkz. AK Sözleşmesi m. 2/c.

⁶ Medeni hukukun temel kavramlarından biri dürüstlük kuralı şu şekilde tanımlanabilir: “Dürüstlük kuralı, bir kimseden namuslu, dürüst bir insan olarak beklenen davranışı ifade eder. Bir davranışın bu nitelikte olup olmadığı, toplumda egemen olan ahlaki ölçülere, geçerli adetlere, hakları sağlayan ilişkilerin amacına göre tayin edilir”. Bkz. Kemal OĞUZMAN, Nami BARLAS, **Medeni Hukuk (Giriş, Kaynaklar, Temel Kavramlar)**, 15. Baskı, Vedat Kitapçılık, İstanbul 2008, s. 222.

⁷ Lee A. BYGRAVE, **Data Protection Law**, s. 58.

⁸ Leyla KESER BERBER, Mahir M. ÜLGÜ, Cüneyd ER, s. 126. Nitekim Birleşik Krallık’ta Veri Koruma Mahkemesi (the Data Protection Tribunal), katalog siparişleri ve kitle iletişim araçlarında yer alan ilanlarına verilen cevaplarla posta siparişi alan bir şirketin müşterilerini, toplanan kişisel bilgilerin hangi amaçlarla kullanılacağına ilişkin olarak sipariş anında bilgilendirmediği gerekçesi ile dürüstlük kuralına aykırı hareket ettiğine karar vermiştir. Bkz. Innovations (Mail Order) v Data Protection Registrar (DA92 31/49/1), Peter CAREY, **Data Protection**, s. 66.

dayanmadan ya da yasada belirtilen ilkelere aykırı bir şekilde kişisel verilerin gizli kayıt altında tutulması ve işlenmesi dürüstlük ilkesine aykırılık oluşturur⁹.

O halde bu ilkenin veri denetçilerini, kişisel verileri işleme sürecinde ilgili kişinin özel yaşamının gizliliği hakkını, maddi ve manevi bütünlüğü ile özerkliğini makul olmayan nedenlerle ihlal eden bir hareket tarzını benimsememesine zorladığını söyleyebiliriz. Bu bağlamda dürüstlük kuralı, denge ve orantılılık gerekliliklerini de beraberinde getirmekte¹⁰ ve aşağıda incelenecek diğer veri koruma ilkelerine kaynaklık etmektedir.

B. BELİRLİ, AÇIK VE MEŞRU AMAÇLAR İÇİN TOPLANMA

Kişisel verilerin işlenme sürecinin tamamında belirli, açık ve meşru amaçlar doğrultusunda hareket edilmelidir. Bir başka anlatımla, verilerin hem toplanma, hem de daha sonraki bütün işlenmelerinde bu ilkeye uyulmalıdır. Bu ilke dolayısıyla hangi verilerin işlenip hangilerinin işlenemeyeceğinin sınırları belirleneceğinden ve belirli bir amaç için toplanan verinin başka hangi amaç için kullanılabileceği bu kapsamda saptanacağından, amacın sınırlandırılmasını öngören bu ilke, iş çevreleri için merkezi öneme sahiptir¹¹.

Bütün temel veri koruma düzenlemelerinde kabul edilen¹² bu ilkenin üç parçadan oluştuğu görülmektedir:

- verilerin toplanma amacının belirli ve açık olması;
- verilerin toplanma amacının meşru olması;
- verilerin daha sonra işlenme amaçlarının, toplanma amacı ile uyumlu olması.

⁹ Ulrich DAMMANN, Spiros SIMITIS, **EG-Datenschutzrichtlinie Kommentar**, Almanya 1997, Art 6 RN 3'den aktaran; Oğuz ŞİMŞEK, **Anayasa Hukukunda Kişisel Verilerin Korunması**, s. 85.

¹⁰ Lee A. BYGRAVE, **Data Protection Law**, s. 58.

¹¹ Christopher KUNER, s. 99-100.

¹² Bkz. AB Veri Koruma Yönergesi m. 6/1,b; AK Sözleşmesi m. 5/b, OECD Rehber İlkeleri par.9, BM Rehber İlkeleri 3. İlke, APEC Taslağı, par. 18. Bu ilkeyi tanımlamak için kimi metinlerde “*amacın belirlenmesi*”(purpose specification) ifadesinin kullanıldığı (Örneğin OECD ve BM Rehber İlkeleri'nin belirtilen hükümleri), kimilerinde ise “*kesinlik*” (finality) deyimini ile karşılandığı görülmektedir. Örneğin bkz. Article 29 Data Protection Working Party, **Privacy on the Internet: an Integrated EU Approach to On-line Data Protection**, Working Document adopted 21 Kasım 2000; Lee A. BYGRAVE, **Data Protection Law**, s. 61.

1. Verilerin Toplanma Amacının Belirli ve Açık Olması

Verilerin toplanma amacının belirli ve açık olması, her şeyden önce bu konuya ilişkin hukuksal düzenlemelerde belirsiz ifadelerden kaçınılmasını gerektirir. Ayrıca verilerin anonimleştirilmeden yalnızca depolanmak üzere, bir başka anlatımla olası kullanımdan hareketle tutulması da bu ilkeye aykırılık oluşturur¹³.

Nitekim çalışmamızın birinci bölümünde de açıklamaya çalıştığımız üzere, kişisel verilerin belirli bir amaç olmaksızın “*bir gün gerekli olursa*” düşüncesiyle tutulması, bütün bir toplumu potansiyel suçlu konumuna sokar. Bu, kişileri kendilerini özgürce ifade etmekten alıkoyabilir. Sonuçta zarar görecektir olan kişinin maddi ve manevi bütünlüğü, kişiliğini geliştirme hakkı, bireysel özerkliği ve masumiyet karinesi gibi çağdaş demokratik toplumun temel değerleridir.

AB Veri Koruma Yönergesi’ne göre veri denetçileri, kişisel verilerin işleme amacını tam olarak belirlemeli ve bunu ilgili kişi ile ulusal denetim birimine bildirmelidir¹⁴. Dolayısıyla bu gereklilik ilgili kişinin bilgilere erişim hakkı ve veri koruma görevlisinin bildirim yükümlülüğü ile de yakından ilişkilidir. Bu nedenle örneğin kullanıcılarının kişisel bilgilerini toplayan bir web sitesi, onları toplama amacı konusunda bilgilendirmeli ve verileri bu amaç dışında kullanmamalıdır. Bu kapsamda web sitesinin bilgileri pazarlama amacıyla kullanacağını belirtmediği durumlarda, kullanıcılarına e-posta reklamları göndermesi ilkenin ihlali anlamına gelecektir¹⁵.

2. Verilerin Toplanma Amacının Meşru Olması

İkincisi verilerin toplanma amacının meşru olmasıdır. Verilerin toplanmasının meşru olabilmesi için yasal bir temele dayanması, bütün yasal gereklilikler ile uyum içinde olması ve verilerin işlenmesinden kaynaklanan çıkar ile dengeli olması gerekir¹⁶. Bir başka anlatımla, veriler toplanırken yalnız ilgili düzenlemede

¹³ Oğuz ŞİMŞEK, s. 84; Nilgün BAŞALP, s. 38.

¹⁴ Leyla KESER BERBER, Mahir M. ÜLGÜ, Cüneyd ER, s. 126.

¹⁵ Christopher KUNER, s. 100.

¹⁶ Christopher KUNER, s. 90. Belirtmek gerekir ki bu ilkenin yer aldığı kimi metinlerde “*meşru*”, kimilerinde ise “*yasal*” deyimini kullanılmıştır. Örneğin OECD Rehber İlkeleri ve 1998 Birleşik Krallık Veri Koruma Yasası’nda toplama amacının “*yasal*” olması gerektiği belirtilmiştir. AB Yönergesi ve AK Sözleşmesi’nde ise “*meşru*” deyimini yer almaktadır. Her iki kavram arasında bir ayrım olduğu açıktır. Meşruluk baskın sosyal kabulle ilişkili bir kavram olduğundan, meşru işlemeyi söz edebilmek için bu moral değerlere uygun hareket edilmesi gerekir. Ancak kişisel verilerin “*meşru*” amaçlarla toplanabileceğinin kabul edildiği metinlerin büyük bölümünde de bu deyim dayanağı olarak yasallık öngörülmüştür. Bu bağlamda çok az sayıda örnekte sosyal gerekçelerden hareket edilmiştir. Burada belki de tek örnek 1988 Hollanda Kişilerin Kaydı

belirlenen bir ya da birkaç amaca yönelinmesi yeterli değildir. Bunun yanında konuya ilişkin diğer ilkelere de uygun hareket edilmeli ve amacı aşan bir eylem gerçekleştirilmemelidir.

AB Veri Koruma Yönergesi'nde veri işlemeyi meşru kılan ölçütler belirlenmiştir¹⁷. Buna göre kişisel verilerin işlenmesi şu durumlardan bir ya da bir kaçının bulunması ile meşru kabul edilecektir:

- ilgili kişinin rızasının bulunması¹⁸;
- ilgili kişinin taraf olduğu bir sözleşmenin ifa edilmesi ya da ilgili kişinin bir sözleşmenin tarafı olmadan önceki istemleri dolayısıyla işlemenin gerekli olması¹⁹: bir servis sağlayıcının sunduğu hizmeti yerine getirebilmesi için veri öznesinin ad, telefon numarası, e-posta adresi gibi bilgilerini sağlaması burada örnek olarak gösterilebilir²⁰;
- denetçinin tabi olduğu yasal bir yükümlülüğe uymak için işlemenin gerekli olması²¹: Bu hükümde söz konusu olan yalnızca vergi, sosyal sigorta ya da mahkemeye delil sunma gibi yasal yükümlülüklerdir. Bu nedenle sözleşmeden kaynaklı yükümlülükler bu kapsamda değerlendirilemez. Ayrıca genel kabul gören görüş uyarınca bu hüküm, üçüncü devletlerin hukuk sistemlerinden kaynaklı yasal yükümlülükler açısından da geçerli olmayacaktır²²;
- ilgili kişinin yaşamsal çıkarlarının korunması için işlemenin gerekli olması²³: bu istisna ancak ilgili kişinin yaşamı için elzem bir çıkarının korunması söz konusu ise uygulanabilir²⁴. Özellikle acil tıbbi müdahaleler bu kapsamda değerlendirilmektedir²⁵;

Yasası idi(Registration of Persons Act). 2000 yılında Kişisel Verilerin Korunması Yasası'nın kabulü ile ilga edilen bu düzenlemenin 4/2 hükmü, “*Kişisel veri dosyasının amacı yasayla, kamu düzeninin korunmasıyla veya ahlakla(morality) çatışma halinde olamaz*” hükmü yer almaktadır. Bkz. Lee A. BYGRAVE, **Data Protection Law**, s. 61-62, dn. 226.

¹⁷ AB Yönergesi, m.7.

¹⁸ AB Yönergesi m. 7/a. Kişisel verilerin korunmasında ilgilinin rızası aşağıda incelenecektir.

¹⁹ AB Yönergesi m. 7/b.

²⁰ Lucas BERGKAMP, Jan DHONT, s. 81.

²¹ AB Yönergesi m. 7/c.

²² Christopher KUNER, s. 76.

²³ AB Yönergesi m. 7/d.

²⁴ AB Yönergesi, baş. par. 31.

²⁵ Lucas BERGKAMP, Jan DHONT, s. 81.

- işleminin kamu yararının bulunduğu bir hizmetin gerçekleştirilmesi ya da denetçinin veya verinin açıklandığı üçüncü kişinin resmi bir yetkisini kullanması için gerekli olması²⁶: burada geçen “kamu yararı” deyimini geniş yorumlamayı olanaklı kılan niteliği dolayısıyla istisnanın sınırlarının belirsizleşmesine neden olmaktadır. Örneğin Belçika’da salgın hastalıklara ilişkin araştırma yapmada kamu yararı görüldüğünden, bu amaç için gerekli olan işlemler veri öznesinin öncel izni (prior consent) olmaksızın gerçekleştirilebilir²⁷;

- Yönerge’nin 1/1 hükmü uyarınca ilgili kişinin temel hak ve özgürlüklerinden kaynaklı çıkarlarının baskın olduğu durumlar hariç, denetçi veya verinin açıklandığı üçüncü kişinin meşru çıkarlarından kaynaklanan amaçlar için gerekli olması²⁸: Bu hüküm ile ilgili kişinin çıkarları ile veri denetçisinin çıkarları arasında bir denge öngörüldüğü söylenebilir²⁹. AB Yönergesi’nde “meşru çıkar”ın ne olduğu tanımlanmamıştır. Ancak Yönerge’nin Başlangıç bölümünde “şirketlerin ve diğer organların meşru olağan etkinlikleri” ifadesi yer almaktadır³⁰. Bu bağlamda “meşru çıkarlar”ın “meşru ticari çıkarlar” olarak algılanması olanaklıdır. Bu ise doğrudan pazarlama gibi bazı etkinliklerin kapsam dahilinde bulunduğu sonucunu yaratır³¹. Eğer bu istisna doğrudan pazarlama için oluşturulmuş bir veri tabanına uygulanacaksa, ilgili kişinin temel hak ve özgürlüklerinden kaynaklı çıkarlarının veri denetçisinin ticari çıkarlarından baskın olup olmadığının değerlendirilmesi gerekir. Bu ise ulusal hukuk sistemindeki (AB Yönergesi açısından üye devletlerdeki) veri koruma düzenlemeleri dikkate alınarak yapılabilir³².

Kişisel verilerin korunmasında verilerin toplanmasının meşru olması gerekliliğinin uygulamada nasıl değerlendirildiği birkaç örnek üzerinden açıklığa kavuşturulabilir: Çevrimiçi bir tartışma grubuna katılan bir kişinin e-posta adresinin, web sitesinin sunucusu aracılığıyla ya da kullanıcının yazılımı dolayısıyla

²⁶ AB Yönergesi m. 7/e.

²⁷ Lucas BERGKAMP, Jan DHONT, s. 82.

²⁸ AB Yönergesi m. 7/f.

²⁹ Bu istisna hükmünün uygulanıp uygulanmayacağına saptanması bazı üye ülkelerin ulusal hukuk sistemleri açısından özellikle önemlidir. Örneğin bkz. Federal Almanya Veri Koruma Yasası, m. 28; Christopher KUNER, s. 76.

³⁰ AB Yönergesi baş. 30.

³¹ Lucas BERGKAMP, Jan DHONT, s. 81.

³² Lucas BERGKAMP, Jan DHONT, s. 81-82.

istenmeden paylaşıma açılmasını 29. Madde Veri Koruma Grubu meşruluk ilkesinin ihlali olarak yorumlamıştır. Benzer şekilde aynı Grup casus yazılımların kullanıcıların bilgisi olmaksızın verilerini aktarmaları dolayısıyla meşruluk ilkesiyle bağdaşmadığı yönünde görüşünü açıklamıştır³³.

3. Verilerin Daha Sonra İşlenme Amaçlarının Toplanma Amacı İle Uyumlu Olması

Bu ilkenin üçüncü gerekliliği olan verilerin daha sonra işlenme amaçlarının toplanma amacı ile uyumlu olması, ilke ile hedeflenen hukuksal yararın gerçekleşebilmesi için de bir zorunluluktur. Kişisel verilerin sonraki kullanımlarının toplanma amacı ile bağdaşmaması durumunda ilgili kişinin verileri üzerindeki denetimini kaybedeceği açıktır. Ancak burada “*uyumlu olmayan amaç*”ın saptanması çok da kolay değildir. Nitekim AB üyesi devletlerin neyin uyumlu olmayan amaç olduğu konusunda geliştirdikleri yorumlar da farklılaşmaktadır.

İlk amaç ile sıkı sıkıya bağlı sonraki amaçlar genel olarak “*uyumlu*” görülmektedir. Örneğin Avusturya yasalarına göre, bir şirketin muhasebe bölümünün satış verilerini işlemesi, satışın kendisi ile “*uyumlu*” bulunmaktadır. Oysa pek çok olayda mahkemeler, veri denetçilerinin ilgili kişiye işleme amaçlarına ilişkin tam bilgi sağlamasını beklemekte ve bunun gerçekleşmediği durumlarda işlemeyi meşruiyet ve yasallık koşullarına aykırı bulmaktadır³⁴.

Kişisel verilerin korunmasına yönelik AB Yönergesi bu noktada bir istisna tanımıştır. İlgili hüküm uyarınca “*üye devletlerin uygun önlemleri alması koşuluyla, tarihsel, istatistiksel ve bilimsel amaçlarla sonradan işlemlerin uygunsuz olduğu düşünülmeyecektir*”³⁵. Bu varsayım ile Yönerge’yi hazırlayanların, tarihsel, bilimsel ve istatistiksel amaçlarla yapılan araştırmalar ile belirtilen ilke arasında yaşanabilecek çatışmaya bir ölçüde de olsa çözüm bulmayı amaçladıkları söylenebilir. Ancak burada üye devletlerin uygun önlemleri almasının bir zorunluluk olduğu dikkatten kaçmamalıdır.

³³ Birinci örnek için bkz. Article 29 Working Party, **Privacy on the Internet: A Comprehensive EU Approach to Online Data Protection**, WP 37, 21 Kasım 2001, s. 39. İkinci örnek için bkz. Article 29 Working Party, **Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites**, WP 56, s.12. Ayrıca bkz. Christopher KUNER, s. 90.

³⁴ Christopher KUNER, s. 100.

³⁵ AB Veri Koruma Yönergesi, m. 1/b, 2. cümle.

Kişisel verilerin hangi amaçlarla kullanılacağını ilgili kişi tarafından bilinmesi önleyici bir koruma sağlamaktadır. Nitekim verilerinin kullanılacağı amacı bilmeyen kişi, hem işlemeye izin verip vermeyeceğini sağlıklı bir şekilde kararlaştıramaz, hem de verileri üzerindeki denetimini kaybeder.

C. TOPLANMA VE SONRASINDA İŞLENME AMAÇLARINA UYGUN, İLGİLİ BULUNMA, AŞIRI OLMAMA

95/46/AT sayılı Yönerge'nin 6/1,c hükmü uyarınca kişisel veriler, *“toplanma ve/veya bunu izleyen işleme amaçları açısından yeterli ve onlarla ilgili olacak ve aşırı olmayacaktır”*. 108 sayılı AK Sözleşmesi'nde ise bu ilkenin, AB Yönergesi ile hemen hemen aynı ifadelerle yer aldığı görülür. Ancak her iki hüküm arasında dikkat çekilmesi gereken bir farklılık da bulunur. Sözleşme'nin 5/c hükmüne göre otomatik yollarla işlenen kişisel veriler *“saklanma amacı için yeterli, onunla ilgili olacak ve aşırı olmayacaktır”*. 108 sayılı AK Sözleşmesi'nin yalnızca otomatik işlenen verilerin korunmasına hasredildiğinden daha önce söz etmiştik. Buradaki farklılık AB Yönergesi'nde ölçüt, *“toplama ve/veya daha sonra işleme amaçları”* ile bağlantısı açısından geliştirilirken, AK Sözleşmesi'nde *“saklanma amacı”* dikkate alınarak belirlenmesidir. Ancak her iki hüküm de henüz kişisel verilerin toplanması aşamasında bu ilkenin dikkate alınmasını öngörmektedir³⁶. Bunun yanında aşağıda inceleneceği üzere her iki metin de verilerin saklanma amaçları açısından artık gerekli olmadıkları zamanda anonimleştirilmelerine ya da silinmelerine ilişkin hükümler içermektedir³⁷.

Bununla birlikte pek çok metinde bu ilkenin AB Yönergesi ve AK Sözleşmesi'nde olduğu kadar açık bir şekilde düzenlenmediği de belirtilmelidir. Ne OECD, ne BM Rehber İlkelerinde bu ilkeye açıkça yer verilmemiştir. Yine de bu metinlerde belirtilen ilkenin tamamen dışlandığı düşünülmemelidir. Nitekim bu ilkeyi, yukarıda değindiğimiz dürüstlük kuralının bir bileşeni olarak değerlendirmek olanaklıdır³⁸.

³⁶ Lee A. BYGRAVE, **Data Protection Law**, s. 60.

³⁷ Bkz. AB Yönergesi m. 6/e; AK Sözleşmesi m. 5/e.

³⁸ Lee A. BYGRAVE, **Data Protection Law**, s. 60.

Çeşitli metinlerde kabul edilmiş bu ilkenin³⁹, kimi yerlerde “*yeterlik ilkesi*”(adequacy principle)⁴⁰, kimi yerlerde ise “*verileri asgarileştirme*” (data minimization)⁴¹ olarak ifade edildiği de görülür⁴². Bu ilke uyarınca veri denetçisi, öncelikle amaçlarına ulaşabilmek için kişisel verilerin mutlaka gerekli olup olmadığını saptamalıdır. Eğer kişisel veriler kullanılmadan da hedefe ulaşılabilecekse öncelikle bu yol tercih edilmelidir.

Ancak elbette kişisel verilerin kullanımının hedefe ulaşılması için zorunlu olacağı durumlar da bulunacaktır. Böylesi durumlarda ise veri denetçisi amaca ulaşmak için gerekli olan en az sayıda veriyi kullanmalıdır. “*Veri ekonomisi*” olarak da ifade edebileceğimiz bu yaklaşımla gerekli olandan fazla miktardaki kişisel verinin kullanımı önlenmektedir. Eğer aynı veri birden fazla amaç için kullanılıyorsa yine bunların gerekli olan kadarıyla sınırlandırılması gerekir⁴³.

Veri denetçisinin amaca bağlılık ilkesinin gerektirdiği değerlendirmeyi kişisel verilerin toplandığı her durumda tekrarlamalıdır. Örneğin iş başvurusu formları, müşteri bilgi kartları ya da İnternet ortamında kayıt sayfaları hazırlanırken bu ilkeye dikkat edilmeli ve amaca ulaşmak için gerekli olandan fazla bilgi istenmemelidir⁴⁴.

³⁹ Bkz. AK Sözleşmesi, m. 5/c.

⁴⁰ Peter CAREY, **Data Protection**, s. 55.

⁴¹ Örneğin bkz. Christopher KUNER, s.73-74.

⁴² Bu ilkeyi niteleyen başka bazı deyimler de bulunmaktadır. Örneğin Federal Almanya Veri Koruma Yasası’nda “*veri azaltma*” (Datenvermeidung) ve “*veri ekonomisi*” (Datensparsamkeit) deyimlerinin kullanıldığı görülmektedir. Bkz. Federal Almanya Veri Koruma Yasası m. 3a. AK’nin çeşitli metinlerinde ise “*orantılılık*” deyiminin kullanıldığı görülmektedir. Örneğin bkz. **Recommendation R (97) 18 on the Protection of Personal Data Collected and Processed for Statistical Purposes**, 30 Eylül 1997. Ayrıca bkz. Lee A. BYGRAVE, **Data Protection Law**, s. 60, d.n. 213.

⁴³ Örneğin bir okulda kullanılan “*akıllı kart*” (smart card) hem kantinde, hem kütüphanede geçerli olabilir. Bu durumda ancak bu iki amaç için ortak olan veriye bu kart üzerinde yer verilmelidir. . **Guiding principles for the protection of personal data with regard to smart cards (2004)**, as adopted by the CDCJ at its 79th Plenary, 11-14 Mayıs 2004, s. 3, http://www.coe.int/t/legaffairs/legal_co-operation/data_protection/documents/ . Bu bağlamda öğrencinin adı ve sınıfına ilişkin bilgi, her iki amaç için de ortaktır. Oysa öğrencinin hangi tür yemeklere alerjisi olduğu ya da hangi türdeki kitapları ödünç aldığına ilişkin bilginin kartın belleğine kayıt edilmemesi gerekir.

⁴⁴ İngiltere’de uygulanan özel bir vergi türü olan toplumsal vergi (community charge/poll tax) usulü dolayısıyla bu ilkenin çeşitli zamanlarda dava konusu olduğu görülmüştür. Pek çok kişi, belirtilen vergilendirme usulü dolayısıyla edinilen bilgilerin amacı aşan bir miktarda olduğu konusunda itirazda bulunmuştur. Örneğin Veri Koruma Sicil Amiri (“*Data Protection Registrar*”- daha sonradan “*Information Tribunal*” adını almıştır), bir idari makamın toplumsal vergi formunda yurttaşların doğum tarihlerini talep eden bilginin çıkarılmasını istemiştir. Buna karşın idari makam, formda doğum tarihinin bulunmasının gerekçesini aynı bölgede aynı ad ve soyadı taşıyan kişileri ayırmak olarak ifade etmiştir. Bu konuda istatistiksel bir bilgi bulunmamasına karşın Mahkeme, bu saptamanın doğru olabileceğine karar vermiştir. Ancak Mahkeme’ye göre idari makam, oluşturduğu veri bankasını yalnızca aynı ad ve soyada sahip ve aynı adreste

Bu durum özellikle “iş sözleşmesi” açısından değerlendirilebilir. İşveren ile işçi arasında yapılan bu sözleşmenin konusu doğal olarak işe alınacak “kişi”dir. Bu durumda elbette işveren (olası) işçisine ilişkin bazı bilgileri edinecektir. Ancak işverenin işçiden isteyebileceği bilgilerin de bir sınırı vardır. Bu bilgiler, iş ilişkisi açısından gerekli olanla sınırlı tutulmalıdır. Bu noktada işin niteliğinin dikkate alınması gerekecektir. Kimi yazarlara göre iş ilişkisi için gerekli olandan fazla bilgiyi edinme talebinde bulunması, işçinin “yalan söyleme hakkı”nı beraberinde getirir⁴⁵. Nitekim işçinin soruları yanıtsız bırakması olası bir iş olanağını kaçırmaması sonucunu doğurabilir. Benzer şekilde ücretsiz e-posta hizmeti sağlayıcısının, herhangi bir gereklilik yokken ilgili kişiden yaş, cinsiyet gibi bilgilerini istemesi de bu kapsamda değerlendirilebilir.

Kişisel verinin doğrudan ilgili kişiden ve onun bilgisi dâhilinde sağlandığı bu durumlar dışında, olanaklı olan en az sayıda verinin elde edilmesi ilkesi, konuyla ilgili diğer teknoloji ürünleri açısından da dikkate alınmalıdır. Güvenlik gerekçeleriyle gizli kamera kurulmuş bir işletmeyi düşünelim. Mağaza içindeki kameraların, mağazanın dışını da görüş alanı içine alması durumunda amacı aşan oranda veri toplanması söz konusu olacaktır. Nitekim Almanya’da görülen bir davada mahkeme, market önündeki kaldırımın en fazla bir metre çapında izlenebileceğini karara bağlamıştır. Bu durum, denetlenen yer işletmecinin kendi malı olsa bile geçerlidir. Mahkemeye göre sokakta yürüyenlere gözetlenmedikleri bir alan bırakılmalı ve sosyal yaşam burada korkusuz bir şekilde akmaya devam etmelidir. Aksi halde verilerin korunması hukuku zedelenir⁴⁶.

Ulusal düzenlemeler incelendiğinde bu ilkenin yaşama geçirilmesine yönelik hükümlerde çeşitlilik olduğu söylenebilir. Ancak bu noktada özellikle, konuya ilişkin Almanya’daki düzenlemeyi biraz daha yakından incelemek gerekir. Federal Almanya Veri Koruma Yasası’nın 3a hükmünde ilke şu şekilde formüle edilmiştir:

yaşayan kişilerin doğum tarihleri ile sınırlandırmamıştır. Bu nedenle Mahkeme, veri tabanında yer alan bilgilerin amaç ile ilgisiz ve aşırı olduğuna karar vermiştir(Community Charge Registration Officer of Rhondda Borough Council v Data Protection Registrar (DA/90/49/2)). Oysa bu “aşırı”lığı önlemek için veri denetçisinin, toplumsal vergi formunda doğum tarihinin istendiği bölüme “*lutfen yalnızca eğer aynı evde yaşadığınız ve sizinle aynı ad ve soyada sahip bir kişi bulunuyorsa, ayırt edebilmemizi sağlamak üzere doğum tarihinizi bildiriniz*” biçiminde bir bilgi notu eklemesi yeterlidir. Bkz. Peter CAREY, **Data Protection**, s. 56.

⁴⁵ Marie-Theres TINNEFELD ve diğ., s. 68.

⁴⁶ Marie-Theres TINNEFELD ve diğ., s. 315.

“(1)Veri işleme sistemleri, hiçbir verinin veya olanaklı bulunan en az miktarda kişisel verinin toplanması, işlenmesi veya kullanılması amacı doğrultusunda tasarlanmalı ve seçilmelidir. (2) Özellikle olanaklı bulunduğu ve maliyeti ile zahmeti korunmaya çalışılan amaç ile makul bir ilişki içinde olduğunda anonimleştirme ve takma adlaştırma kullanılır”.

Her ne kadar veri koruma hukuku içerisinde bu ilkenin kabulü yeni bir gelişme olmasa da Federal Almanya Veri Koruma Yasası’ndaki bu hüküm önceki düzenlemelerin ötesine geçen yeni bir yaklaşımı sergilemektedir. Yasanın 3a maddesinin 1. fıkrasında dile getirilen veri azaltma ilkesi, 2. fıkarda somutlaştırılmıştır. Buna göre olanaklar ölçüsünde verilerin anonimleştirilmesi veya takma adlar altında tutulması gerekliliğine işaret edilmiştir. Bunun gerçekleşebilmesi için elbette bazı teknik olanaklar sağlanmalıdır⁴⁷. Ancak verilerin anonim olarak ya da takma adlar altında toplanması, tutulması ve kullanılması her durumda söz konusu olacak bir zorunluluk olarak belirtilmemektedir. Teknik olanaklar, maliyet, gereklilik, bu yöntemi kullanacak kişinin bu işi yapabilirliliği bu noktada dikkate alınması gereken hususlar olarak karşımıza çıkar⁴⁸. Ayrıca belirtilen hükümde bu işlemin ne zaman gerçekleştirileceğine ilişkin bir açıklık da bulunmamaktadır. Bu anlamda verilerin anonimleştirilme veya takma adlaştırılma zamanı her olayın kendi koşullarına göre belirlenecektir. Ancak bu işlemin, olanaklar çerçevesinde en erken zamanda (toplanma, kullanma ya da daha sonra yararlanılması aşamasında) gerçekleştirilmesi gerekir⁴⁹.

Federal Almanya Veri Koruma Yasası’nda yer alan bu iki yol, yani anonimleştirme ve takma adlaştırma arasındaki farklılığa da dikkat çekilmelidir. Nitekim birbirlerine yakın olan bu iki yöntem farklı sonuç ve sorunları beraberinde getirir.

Federal Almanya Veri Koruma Yasası’na göre anonimleştirme, *“kişisel verilerin, belirli ya da belirlenebilir gerçek kişiyle, kişisel ya da olgusal bağımsız*

⁴⁷ Fleeming MOOS, s. 58. Nitekim Almanya’da yasa koyucu Teleservisler Veri Koruma Yasası’nda da bu duruma işaret etmiştir. Yasanın 4. maddesi hükmüne göre, bu hizmet sağlayıcılara düşen bir görevdir. Bkz. Gesetz über den Datenschutz bei Telediensten, Bundesgesetzblatt, 1997 I 1871. Ayrıca bu konuya ilişkin olarak bkz. Lee A BYGRAVE, “Germany’s Teleservices Data Protection Act”, **Privacy Law and Policy Reporter**, C. 5, Y. 1998, s. 53-54; Peter SCHAAR, **Datenschutz im Internet, Die Grundlagen**, Verlag C.H. Beck, Almanya 2002, s. 121-123.

⁴⁸ Peter GOLA, Rudolf SCHOMERUS, s.138-139, par. 8.

⁴⁹ Peter GOLA, Rudolf SCHOMERUS, s. 139, par. 9.

*bilginin bağlanamamasını veya bunun ancak fahiş oranda zaman, maliyet ve emek kaybı ile bağlanabilmesini sağlayacak şekilde değiştirilmesidir*⁵⁰. Takma adlaştırma ise, “bir kişinin adının veya diğer belirlenebilir özelliklerinin, veri öznesinin kimliğinin saptanmasını engellemek veya kimliğin saptanmasını oldukça güç duruma getirmek amacıyla bir etiket ile değiştirilmesi”⁵¹ anlamına gelir.

Tam anlamıyla anonim olan verilerin gerçek kişilerle ilişkisi koptuğu, yani belirlenebilir bir birey ile arasında bir bağ kurmak olanaklı bulunmadığı için bunlar, kişisel veri olarak değerlendirilemezler⁵². Dolayısıyla anonim veriler, kişisel verilerin korunması mevzuatının dışında yer alır. Buna karşın, takma adların birey ile bağlantısı bulunduğu için bunlar, halen veri koruma hukukunun konusu olmayı sürdürür⁵³. Örneğin Almanya’da takma adıyla çevrimiçi hizmet alan bir kişi, burada tutulan bilgilere erişim hakkını yine takma adı ile kullanabilmektedir⁵⁴.

İnternet ortamına ilişkin önemli bir soru ise IP⁵⁵ ya da kullanıcının kimliğini gizleyen başka sembollerin takma ad olarak değerlendirilip değerlendirilmeyeceğidir. Örneğin eğer bir web sitesi kullanıcının çevrimiçi etkinliklerini izleyerek bir profil oluşturursa, IP numarası takma ad olarak mı kabul edilecektir? Bu soruya kesin bir cevap verebilmek olanaklı bulunmasa da pek çok veri koruma yetkilisi, bunların kullanıcı tarafından seçilmemesi ve IP adresinin ötesine geçerek kullanıcının gerçek kimliğine ulaşılmasının ne kadar kolay olduğunun bilinmemesi nedeniyle bu soruyu olumsuz bir şekilde yanıtlamakta, yani IP adreslerinin takma ad olarak kabul edilmesini benimsememektedir⁵⁶.

Alman Veri Koruma Yasasında yer aldığı şekliyle bu ilke, e-ticaret açısından da bazı sonuçlar getirmektedir. Çünkü bu kural, veri işleme ve bilgisayar sistemlerinin iş görme ve kişisel verileri işleme şekillerine ilişkin özel yasal ölçütler

⁵⁰ Federal Almanya Veri Koruma Yasası m. 3/6.

⁵¹ Federal Almanya Veri Koruma Yasası m. 3/6a.

⁵² Fleeming MOOS, s. 59; Christopher KUNER, s. 66.

⁵³ Anonimleştirme ve takma adlaştırma arasındaki derecelendirme farkına ilişkin olarak bkz. Bernhard C. WITT, **Datenschutz Kompakt und Verständlich, Eine praxisorientierte Einführung**, Vieweg, Almanya 2008, s. 77-78. Ayrıca bkz. Alexander ROßNAGEL, Philip SCHOLZ, s. 721-731.

⁵⁴ Christopher KUNER, s. 66.

⁵⁵ IP (yani İnternet Protokol) adresi, TCP/IP(Transmission Control Protocol/İnternet Protokol-İletim Denetim Protokolü/İnternet Protokolü)’nin bir bileşenidir. Bu bağlamda IP, TCP/IP standardını kullanan bir ağdaki cihazların birbirlerini tanımaları, birbirleriyle iletişim kurmaları ve veri alışverişinde bulunmalarını sağlayan benzersiz bir numaradır. İnternet’e bağlı her cihazın yalnızca kendine özgü bir IP numarası bulunur. Bkz. <http://www.ip-numaram.com/ipadres.html>.

⁵⁶ Christopher KUNER, s. 66-67.

geliştirilmesini olanaklı kılar. Bu durumda, belirtilen hüküm dolayısıyla yazılım, donanım, veri bankası ve diğer veri işleme sistemlerinde, kişisel verileri savurgan bir şekilde işlenmemesini, asgari olarak gerektiği kadar verinin işlenmesini sağlamak ve ilgili kişilerin bu gibi sistemleri anonim olarak ya da takma isim altında kullanmalarını olanaklı kılmak potansiyel olarak zorunludur⁵⁷.

Verilerin anonim olarak ya da takma adlar altında toplanması, tutulması, kullanılması ya da aktarılması, verinin arkasındaki kişinin maskelenmesi anlamına gelir. Bu çeşit maskeler, bireylerin sosyal hayata katılmalarını kolaylaştırdığı gibi, kişisel verilerin korunmasının temel mantığına uyumlu sonuçları da bulunur. Alman veri koruma mevzuatında olduğu gibi anonimleştirme ve takma adlaştırma gibi yöntemlerin desteklenmesi ve bunların yaygınlık kazanması önemli yararlar sağlayacaktır. Nitekim çeşitli ülkelerde benzer yaklaşımların kabul edildiği görülür. Örneğin Avusturya’da “*dolaylı kişisel veri*” kavramı benimsenmiştir. Bu durumda veri denetçisi ya da işleyicisi, veri aktarımı söz konusu ise alıcısı, ilgili kişinin kimliğini saptayamamaktadır. Bu nedenle “*dolaylı kişisel veri*”nin bir anlamda takma ad olduğu söylenebilir. Avusturya veri koruma mevzuatı uyarınca bu şekildeki verilere bazı yasal ayrıcalıklar tanındığı, böylece kullanımının desteklendiği görülmektedir⁵⁸.

Son olarak şu hususa dikkat çekilmelidir: kişisel verilerin toplanması, kullanılması ya da başkalarına aktarılması meşru ve çeşitli gerekliliklerden kaynaklanabilir. Ancak verilerin bir kez toplanmasının ardından her türlü amaç için kullanılabileceği düşünülmemelidir. Eğer verilerin daha sonra başka bir amaç için kullanılması gerekiyorsa, diğer hususların yanında bunun meşru bir temele dayanması da gerekir⁵⁹. Bu, özellikle DNA profilleri gibi oldukça hassas nitelik

⁵⁷ Christopher KUNER, s. 74. Kişisel verilerin İnternet ortamında görünmez ve otomatik olarak işlenmesinde yazılım ve donanımların etkisi ve bu teknolojilerde kişisel verilerin korunması için dikkat edilmesi gereken hususlarda 29. Madde Veri Koruma Grubu’nun görüşü için bkz. Working Party on the Protection of Individuals with regard to the Processing of Personal data, **Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware**, WP 17, 23 Şubat 1999.

⁵⁸ Austrian Data Protection Act, 2000, m.4/1, 12/3,2; Christopher KUNER, s. 67.

⁵⁹ AİHM de çeşitli kararlarında bu durumu değerlendirmiştir. Örneğin Malone kararına konu olan olayda başvuranın itirazları hem telefonların dinlenmesi ve mektupların okunmasını, hem de kendisinin yaptığı aramaların otomatik olarak kaydeden bir cihazla iletişimin izlenmesine ilişkindir. Bkz. Malone, Birleşik Krallık’a karşı, b.n. 8691/79, k.t. 2 Ağustos 1984, par. 15, 17. AİHM burada iletişimin izlenmesi ile dinlenmesi arasında bir ayrım öngörmüştür. Buna göre, iletişimin dinlenmesi her durumda kişinin özel yaşamına bir müdahale oluşturur. İzleme ise her durumda müdahale olarak değerlendirilemez. Burada önemli olan izleme etkinliğinde güdülen

taşıyan veriler açısından önemlidir. Bir suçun soruşturulması, bir kişinin kimliğinin belirlenmesi gibi bir amaçla toplanmış hücre örnekleri ve DNA profillerinin başka bir amaç için kullanılmasının oldukça ağır sonuçları olabilir.

D. DOĞRU VE EĞER GEREKLİ İSE GÜNCEL OLARAK TUTULMA

Kişisel verilerin doğru olması, hem ilgili kişinin, hem de veriyi çeşitli amaçlarla işleyen kişinin çıkarları açısından son derece önemlidir. Kişisel verilerin yanlış olarak tutulması bireyin temel hak ve özgürlüklerini, ekonomik çıkarlarını ve/veya manevi bütünlüğünü zedeleyici sonuçlar doğurabilir. Diğer yandan kişisel verileri toplayan, kullanan, değerlendiren taraf da bütün bu işlemleri belirli bir hedefe ulaşmak için yapmaktadır. Bu hedef, kamusal bir işlemin gerçekleştirilmesinden, müşteri eğilimlerinin saptanmasına; istatistiksel bilgilerin oluşturulmasından, karlılığın arttırılmasına kadar çok geniş bir yelpaze içinde yer alan pek çok konuya yönelik olabilir. Ancak hangi alana ilişkin olursa olsun yanlış bilgilerden hareketle verilecek kararlar, yanlış sonuçlara ulaşılmasına neden olacaktır. Bu ise yalnızca ilgili kişinin değil, veri denetçisinin de çıkarlarının zedelenmesi sonucunu doğurur.

AB Yönergesi'nin 6/1,d, Avrupa Konseyi Sözleşmesi'nin 5/d maddesinde bu ilke hüküm altına alınmıştır. Her iki metinde de kişisel verilerin “*doğru ve gereken durumlarda güncel olması*” gerektiğinden söz edilmektedir. Ancak kişisel verilerin korunmasına ilişkin her metinde ilkenin bu şekilde ifade edilmediği de belirtilmelidir. İsviçre Veri Koruma Yasası'nda (m.5) yalnızca “*doğruluk*” (Richtigkeit) ifadesi kullanılırken⁶⁰, OECD Rehber İlkeleri'nin 8. ve APEC Taslak'ının 21. paragrafında “*doğruluk*” ve “*güncellik*”in yanında, kişisel verilerin “*tamlığı*”na da (completeness) da bir zorunluluk olarak yer verilmiştir.

amaçtır. Mahkemeye göre izlemenin meşru amacı “*bir telefon hizmet sağlayıcının kural olarak meşru bir biçimde ve özellikle aboneye doğru ücret tahakkuk ettirebilmek veya hizmete ilişkin şikâyetleri veya kötüye kullanma olasılıklarını araştırabilmek için*” bilginin kayıt edilmesidir. Mahkemenin görüşüne göre, abonenin rızası olmaksızın bu bilginin polise verilmesi de Sözleşme'nin özel yaşamın gizliliğini güvence altına alan 8. maddesine müdahaledir. **A.g.k.**, par. 84. Belirtmek gerekir: müdahalenin daha sonraki aşamalarına geçilmesinden sonra ise ihlalin söz konusu olması için bu bilgilerin kişilerin aleyhine kullanılması mutlaka aranan bir koşul değildir. Yalnızca bu bilgilerin toplanması ve depolanması elbette diğer koşulların da varlığı durumunda, ihlale hükmedilmesi ile sonuçlanır. “*Amaç ile sınırlama*” ilkesi ayrıca makul beklenti ile de bir arada değerlendirilebilir. Bkz. Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s. 263. Nitekim telefon kayıtları faturalama amacıyla tutulan bir kişi, doğal olarak bu bilginin başka amaçlarla kullanılmayacağı makul beklentisi içinde olacaktır.

⁶⁰ Lee A. BYGRAVE, **Data Protection Law**, s. 62.

Burada işaret edilmesi gereken belki de ilk husus: belirtilen ilkenin erişim hakkı ile yakın ilişkisidir. Nitekim aşağıda da üzerinde durulacağı gibi, bilgilere erişilememesi durumunda, kişisel verilerin doğruluğunun saptanması da hemen hemen olanaksızdır. Kişisel veriler, bağlantılı olduğu kişiyi niteleyen, onun kişiliği ile sıkı sıkıya bağlı bilgiler olduğuna göre şurası açıktır: bu bilgilerin doğruluğunu en iyi şekilde denetleyebilecek taraf yine ilgili kişi olacaktır. Bilgilerine ulaşamayan kişinin ise bunların doğruluğunu denetleyebilmesi olanak dışıdır.

İkinci olarak kişisel verilerin güncel tutulmasının ne zaman “*gerekli*” olacağı belirlenmelidir. Bu saptamayı yaparken şu nokta gözden kaçmamalıdır: kişisel verilerin doğru ve güncel tutulması veri denetçisine yönelik bir yükümlülüktür ve devredilemez. Ancak bu ilkeyi kişisel verilerin güncelliğini saptayabilmek için veri denetçilerinin zorla ve sürekli olarak ilgili kişilerin içinde bulunduğu yeni durumları araştırması olarak algılamak makul değildir. Bu durumda ilgilinin kişisel bilgilerine ilişkin bir değişiklik oluştuğunda veri denetçisini bilgilendirmesi gerektiğini söylemeliyiz. Bu ilkeye uyumluluğu sağlayabilmek için veri denetçileri ilgili kişilerin bilgilerine ulaşabileceği ve onları denetleyebileceği bir sistem oluşturabilirler⁶¹.

Bu noktada AB Yönergesi’nin 6/1,d hükmünün ikinci parçasını dikkate almalıyız. Burada kişisel verilerin, “*doğru ve eğer gerekli ise güncel olarak tutulması*” zorunluluğunun hemen ardından ikinci bir gereklilik daha belirlenmiştir: buna göre üye devletlerde “*toplanma amaçları veya sonradan işleme için yanlış veya eksik verinin silinmesi veya düzeltilmesi için makul olan bütün adımlar atılacaktır*”⁶².

Bu makul adımları atan, yanlış verilerin silinmesine ya da eksikliklerin giderilebilmesine olanak tanıyan bir sistemi oluşturmuş veri denetçisi, üzerine düşen görevi yapmış sayılacaktır. Pek çok web sitesinde bulunan, kullanıcıların bir şifre ile kişisel bilgilerine ulaşabildikleri sayfalar burada örnek olarak gösterilebilir. Bir şirketin belirli aralıklarla müşterisine gönderdiği beyanlarda bu bilgilere yer vermesi ve müşteriyi yanlış olan bilgileri düzeltme yolları hakkında yönlendirmesi ise bir diğer örnektir.

⁶¹ Peter CAREY, **Data Protection**, s. 57.

⁶² AB Yönergesi m. 6/1,d.

E. AMACIN GEREKTİRDİĞİNDEN DAHA UZUN SÜRE TUTULMAMA

Kişisel verilerin gerektiğinden uzun süre tutulmaması gerekir. AB Veri Koruma Yönergesi'nin 6/1,e hükmü uyarınca, ilgili kişinin teşhis edilmesine olanak tanıyacak şekilde, kişisel verilerin toplandığı veya daha sonra işlendiği amaçlar için gerekli olandan daha uzun süre tutulmaması gerekir. Bu, kişilerin unutulma hakkı olarak nitelendirilebilir. Konuya ilişkin pek çok metinde kabul edilmiş⁶³ bu ilke kişisel verilerin korunması hukukunu temel değerleri ile yakından ilişkilidir.

Her şeyden önce kişisel verilerin tutulmasının kendi başına potansiyel bir risk yarattığı unutulmamalıdır. Aşağıda da değinileceği üzere veri güvenliği sağlanması zorunlu, ancak pek de kolay olmayan bir gerekliliktir. Bu durumda verilerin tutulduğu sürecin tamamında veri güvenliğine ilişkin tehlikeler varlığını sürdürecektir. Ancak kişisel verilerin gerektiğinden uzun süre tutulmaması ilkesinin benimsenmesinin tek nedeni bu değildir. Bu ilke ayrıca kişisel verilerin korunması düşüncesinin özünde kaynağını bulur. Çünkü bu ilkenin kabul edilmediği bir ortamda, haklı gerekçelerle de olsa, bir kez kişisel verileri edinilen bir kişi yaşam boyu bu bilginin bir yerlerde kayıt altında tutulmayı sürdüreceğini ve “*yeri geldiği zaman*” kullanılmak üzere bekletileceğini düşünür. Böylesine bir ortamda kişisel verilerin korunması hukukunun dayanağını oluşturan, bireysel özerklik, bireyin maddi ve manevi bütünlüğü ve özel yaşamın gizliliği gibi çok önemli değerlerin zarar göreceği açıktır.

Kişisel verilerin amaç açısından gereksiz duruma gelmesi birkaç olasılıkta söz konusu olabilir: (i) kişisel verilerin işlenmesi ile hedeflenen amaç ortadan kalkabilir; (ii) amaca ulaşmak için kişisel verinin işlenmesinin gereksiz olduğu anlaşılabilir ya da (iii) amaca ulaşıldığı için artık kişisel verinin tutulması gerekliliği ortadan kalkabilir. Her üç durumda da kişisel veri ile amaç arasındaki illiyet bağı sona ermiştir. Ancak bu ayrılmanın ne zaman gerçekleştiğini saptamak pek de kolay değildir. Bu ilkenin yaşama geçirilmesi için veri denetçisinin işlemin her aşamasını ve her aşamada söz konusu olan amaçları dikkate alması ve her bir veri türü için ilgili amaca göre ne kadar süre saklanması gerektiğini saptaması gerekir. Elbette böylesine bir yükümlülüğün altından kalkılabilmesi oldukça zordur. Ancak veri denetçisinin bu

⁶³ AK Sözleşmesi m.5/e; OECD Rehber İlkeleri, par. 8.

ilkeye uygun bir şekilde hareket etmesi için bazı kullanışlı yöntemler de bulunmaktadır. En çok kullanılan yöntem, çeşitli kategorilerde bulunan verilerin ne kadar süre tutulacağını ortaya koyan bir veri tutma politikası (data retention policy) geliştirmektir.

Kişisel verilerin korunmasında Avrupa sisteminde verilere artık gereksinim duyulmadığı noktada iki yoldan biri tercih edilebilir: kişisel veriler, (i)ortadan kaldırılır ya da (ii) anonimleştirilerek saklanır. Bu kapsamda verileri silme ya da anonimleştirme işlemini gerçekleştirecek veri denetçisi, kendi başına bu hareketin de veri işleme kapsamında olduğunu, dolayısıyla bu işlemler yapılırken de diğer ilkelere uyulması gerektiğini unutmamalıdır⁶⁴.

Bunun yanında AB Yönergesi, üye devletlerin uygun güvenceleri sağlamaları kaydıyla bilimsel, tarihi ve istatistikî amaçlarla verilerin daha uzun süre saklanmasını da olanaklı kılmıştır⁶⁵. Çeşitli yerlerde işaret ettiğimiz üzere kişisel verilerin korunması, kimi zaman diğer hak ve özgürlüklerle çatışma halinde olabilir. Bu açıdan Yönerge'nin belirtilen hükmünün bilim ve sanat özgürlüğü ile kişisel verilerin korunması arasında dengenin sağlanmasına hizmet ettiği söylenebilir.

Son olarak şuna da işaret etmek gerekir: AİHM de çeşitli kararlarında verilerin gerekenden uzun süre tutulmasının sakıncalarına dikkat çekmiştir. Şüphelilerin parmak izi, DNA profili ve hücre örneklerinin ulusal bir veri tabanına aktarılmasına ilişkin bir başvuruyu değerlendirdiği kararında⁶⁶ Mahkeme, herhangi bir kayıt altına alınabilir suç dolayısıyla herhangi bir yaştaki herhangi bir kişinin parmak izi ve DNA örneklerinin belirsiz bir süre saklanmasına izin veren uygulamayı Sözleşme'nin 8/1 hükmüne aykırı bulmuştur⁶⁷.

⁶⁴ Peter CAREY, **Data Protection**, s. 58.

⁶⁵ AB Yönergesi, m. 6/1,e.

⁶⁶ *S. ve Marper, Birleşik Krallık'a karşı*, b.n. 30562/04, 30566/04, k.t. 4 Aralık 2008.

⁶⁷ Kararda da işaret edildiği üzere pek çok Sözleşmecî Devlet, belirli ağırlıktaki suçları işlediğinden şüphelenilen kişilerden cezai kovuşturma dolayısıyla hücre örnekleri alınmasına izin vermektedir. Sözleşmecî Devletlerin büyük çoğunluğu, veri tabanlarında yer alan örneklerin ve DNA profillerinin ilgili kişilerin tahliye edilmeleri veya aklanmalarının hemen sonrasında veya sınırlı bir sürenin geçmesinin ardından kaldırılmasını veya yok edilmesini öngörmektedir. İngiltere ve Galler'deki uygulama ise oldukça geniş kapsamlıdır ve herhangi bir ayırım da öngörmemektedir. Özellikle somut olayda veriler, özlerine bakılmaksızın, bireyin işlediğinden şüphelenilen suçla orantı kurulmaksızın veya bu kişinin yaşı dikkate alınmaksızın tutulabilmekte, verilerin tutulma süresine bir sınırlama getirilmemekte, aklanan kişinin bilgilerinin ulusal veri bankasından çıkarılmasını veya bu bilgilerin yok edilmesini sağlamak için ise çok sınırlı bir olanak tanınmaktadır. **A.g.k.**, par. 119. Birleşik Krallık'ta diğer Avrupa ülkeleri ile karşılaştırıldığında veri tabanlarına ilişkin yeterli düzenlemenin bulunmamasına karşın, bu

III. İLGİLİ KİŞİNİN KATILIMI VE DENETİMİNE YÖNELİK İLKELER

Kişisel verilerin korunması hukuku kapsamında, ilgili kişiye, sürece çeşitli aşamalarda müdahale etme olanağı tanıyan bazı haklar verilmiştir. Kişisel verilere erişim hakkı, verilerin düzeltilmesini isteme hakkı ve bazı durumlarda veri işlemeye itiraz hakkı bu kapsamda sayılabilir. Bunların ilgili kişinin verileri üzerinde denetimini sağlaması ve yukarıda belirtilen kişisel verilerin niteliğine ilişkin ilkelerin gerçekleşebilmesi için son derece önemlidir. Bireyin aktif konumda olduğu bu hakların yanında, yine ilgili kişinin verileri üzerindeki denetimini sağlamak amacıyla veri denetçisinin de bazı yükümlülükleri bulunur. Bunlardan ilk akla gelen kuşkusuz ilgilinin bilgilendirilmesi zorunluluğudur.

OECD Rehber İlkelerinin 13. paragrafında bireyin katılımına yönelik ilkeler topluca düzenlenmiştir. Ancak genel olarak bakıldığında diğer metinlerde ilgili kişinin katılımı ve denetimine yönelik ilkelerin tek bir başlık altında toplanmadığı, çeşitli hükümlerin içine serpiştirildiği görülmektedir⁶⁸.

Aşağıda biri ilgili kişinin aktif, diğeri pasif konumda bulunduğu ancak her ikisi de kişinin verilerinin geleceğini belirleyebilmesi açısından son derece önemli olan “*ilgilinin bilgilendirilmesi*” ve “*erişim hakkı*” üzerinde durulacaktır. Bunların

yönteme, yine diğer Avrupa ülkeleri ile karşılaştırıldığında, daha sık başvurulduğu bir gerçektir. Örneğin İsveç'te yalnızca iki seneden uzun süreyi hapiste geçiren suçluların profilleri tutulmaktadır. Norveç'te ve Almanya'da DNA örneklerinin kalıcı olarak tutulabilmesi için mahkeme kararı gerekmektedir. ABD'de ise 2005 yılından beri FBI yakalanan kişilerin DNA örneklerini alabilmektedir. Ancak eğer kişi suçsuz bulunursa ya da üzerindeki şüphe kalkarsa istek üzerine bu verilerin silinmesi olanaklıdır. İngiltere'de ise 5 milyondan fazla kişinin DNA profili ilgili veri tabanında yer almaktadır ve bu konuda dünya üzerindeki en geniş veri tabanını oluşturmaktadır. Bu veri tabanında bilgileri yer alanların yaklaşık bir milyonu hiçbir suçtan mahkum edilmediği gibi, yaklaşık yarım milyonunu da çocuklar oluşturmaktadır. Bkz. “Throw it out”, The Economist, 4 Aralık 2008, http://www.economist.com/world/britain/displaystory.cfm?story_id=12726053 Karara karşı Birleşik Krallık'tan gelen tepkiler ise umut vericidir. Yazılı ve görsel iletişim araçlarında yer alan ve AİHM'nin kararını destekleyen çeşitli yorumların yanında, Hükümet de özellikle verilerin tutulma süresini sınırlayan hükümler içeren yasal düzenlemelerin hazırlığındadır. Karara yönelik tepkiler için bkz. David MERY, “Don't Delay: Delete Your DNA Today”, 17 Aralık 2008, http://www.theregister.co.uk/2008/12/17/david_mery_reclaim_your_dna/. James STURCKE, “DNA Pioneer Alec Jeffreys: drop innocent from database”, The Guardian, 15 Nisan 2009. Hükümetin 7 Ağustos 2009'a kadar kamunun görüşüne açtığı konuya ilişkin raporu için bkz. Keeping the Right People on the DNA Database, Science and Public Protection, Homeoffice, Mayıs 2009, <http://www.homeoffice.gov.uk/documents/cons-2009-dna-database/dna-consultation?view=Binary>. Ayrıca bkz. George J. ANNAS, “Protecting Privacy and the Public-Limits on Police Use of Bioidentifiers in Europe”, The New England Journal of Medicine, 361;2, 9 Temmuz 2009, s. 196-201.

⁶⁸ Lee A. BYGRAVE, Data Protection Law, s. 63.

doğal bir sonucu olarak kaşımıza çıkan ilgilinin düzeltme, sildirme ve engelleme hakları ile AB Yönergesinde tanınan başka bazı haklar da aşağıda incelenecektir.

A. İLGİLİNİN BİLGİLENDİRİLMESİ

Kişinin verilerinin işlenmesi hakkında bilgilendirilmesi özellikle iki açıdan önemlidir. Birincisi, kişinin haklarını gerçek anlamda kullanabilmesi için kişisel verilerinin işlenmesi hakkında bilgi sahibi olması gerekir. Bu anlamda ilgili kişinin veri denetçilerince bilgilendirilmesi bu gerekliliğin sağlanabilmesi açısından en önemli koşullardan biridir. İkincisi, bu ilke özellikle kamusal organların ellerinde tuttukları kişisel veriler düşünüldüğünde idarenin şeffaflığının da önemli bir gereğidir. Ayrıca yukarıda da belirtildiği gibi kişinin bilgilendirilmesi dürüstlük kuralı ile de yakından ilişkilidir⁶⁹. Bütün bu nedenlerden ötürü, ilgilinin bilgilendirilmesi veri koruma hukukunda merkezi öneme sahiptir⁷⁰.

Veri denetçisinin ilgili kişiyi bilgilendirme yükümlülüğü AB Yönergesi'nin 10 ve 11. maddelerinde düzenlenmiştir. Diğer uluslararası metinlerde ise bu ilkenin AB Yönergesi'ndeki gibi açık ve kapsamlı bir şekilde düzenlenmediği görülür. APEC Çerçeve Belgesi'nin 15. paragrafında ilgili kişinin hangi verilerinin toplandığı ve bunların ne gibi amaçlarla kullanılacağına ilişkin bilgilendirilmesini öngören bir hüküm yer almaktadır. AK Sözleşmesi'nin 8. maddesinde, OECD Rehber İlkeleri'nin 12. paragrafında, BM Rehber İlkeleri içerisinde 3. ilkede dolaylı olarak ilgili kişinin bilgilendirilmesine değinildiği söylenebilir. Ulusal düzenlemelerin bir bölümünde ise verilerin doğrudan ilgili kişiden elde edildiği durumlarda AB Yönergesi'nin 10. maddesine benzer yükümlülüklerin getirildiği görülmektedir⁷¹.

⁶⁹ Oğuz Şimşek, s. 88.

⁷⁰ Deryck BEYLEVELD, "The Duty to Provide Information to the Data Subject: Articles 10 and 11 of Directive 95/46/EC", **The Data Protection Directive and Medical Research Across Europe**, Ashgate, İngiltere 2004, s. 70. Kişinin kendisine ilişkin verilerin işlenmesi hakkında bilgilendirilmesini öngören kurallar üçe ayrılarak incelenebilir: (i) belirli durumlarda veri denetçisinin doğrudan ilgili kişiden verileri toplamasını gerektiren kurallar; (ii) ilgili kişinin rızası (consent) olmaksızın kişisel verilerin işlenmesini yasaklayan kurallar; (iii) veri denetçilerini veri işlemeye ilişkin belirli bilgiyi doğrudan ilgili kişiye vermeye yönelten kurallar. Lee A. BYGRAVE, **Data Protection Law**, s. 63. Birinci ayırım örnekleri son derece sınırlı nadir bir uygulamaya işaret ettiğinden (Örneğin bkz. 1982 Kanada Federal Özel Yaşamın Gizliliği Yasası m. 5/1), ilgili kişinin rızası konusuna ise aşağıda değinileceğinden burada yalnızca üçüncü başlık üzerinde durulacaktır.

⁷¹ Örneğin bkz. US Act 552a(e)(3), Australian Act IPP 2, Swiss Act 18(1). Bunun yanında elbette AB ya da AET üyesi olan devletlerin büyük bir bölümünde Yönerge'ye uyumlu bir şekilde

AB Yönergesi'nde bilgilerin doğrudan ilgili kişiden elde edildiği durum ile üçüncü kişilerden sağlandığı durum arasında bir ayrım yapıldığı görülür. İlgili hüküm uyarınca 10. maddesi uyarınca veri denetçisinin veya temsilcisinin ilgili kişiye, kendisinin zaten bunları bildiği durumlar hariç, en azından şu bilgileri sunması gerekir⁷²:

- veri denetçisinin veya duruma göre temsilcisinin kimliği;
- veri işleme amacı; ayrıca
- veri alıcıları veya alıcı kategorileri;
- sorulara cevap vermenin zorunlu veya isteğe bağlı olduğu ve olası bir cevap vermeme durumunun sonuçları;
- ilgili kişinin kişisel verileri hakkında bilgi alma ve düzeltme hakkının mevcudiyeti;
- son olarak, veri işlemede özel bazı durumların varlığı halinde (hassas kişisel verilerin işlenmesi gibi) dürüst işlemeyi temin edecek gerekli bilgiler.

Kişisel verilerin ilgili kişiden alınmadığı, başka kaynaklardan elde edildiği durumlarda da ilgili kişinin bu kapsamda bilgilendirilmesi, eğer ilgili kişiden elde edilen bilgiler üçüncü kişiyle paylaşılmışsa bu konuda da haberdar edilmesi gerekir. Ancak bu kurala karşın, eğer bu bilgilerin sağlanması olanaksız ise, oransız bir çaba gerektiriyor ise ya da işlem açıkça yasadan kaynaklanıyorsa bu bilgilerin sağlanması gerekmeyecektir⁷³.

İlgili kişinin bilgilendirilmesi özellikle İnternet ortamında kullanılan çeşitli araçlar ve iletişim şekilleri açısından tartışılan bazı konuları beraberinde getirir. Nitekim pek çok donanım ve yazılım kişisel bilgileri toplamakta, değerlendirmekte ve çeşitli amaçlar için kullanmaktadır. Hiperbağlar (Hyperlinks), çerezler (cookies) ya da tarayıcıların (browser) karşılıklı iletişimi bu kapsamda düşünülebilir. Bu gibi uygulamalar, yukarıdaki açıklamalar ışığında, servis sağlayıcıların ilgili kişinin yapılan işlemin farkında olduğunu kanıtlaması hariç, kullanıcının yeterli oranda bilgilendirilmediği durumlarda kabul edilemez. Ancak ilgili kişinin durumun

benzer yükümlülükler iç hukuk düzeninin bir parçası haline getirilmiştir. Son dönemlerde kabul edilen bazı ulusal yasalarda ise AB Yönergesi'nden de daha kapsamlı düzenlemeler getirilmiştir. Bu kapsamda özellikle kişi profillerinin kullanımı ve video ile izlemeye ilişkin yeni yükümlülükler getirildiği görülmektedir. Bkz. Lee A. BYGRAVE, **Data Protection Law**, s. 64, d.n. 239, 240.

⁷² AB Veri Koruma Yönergesi, m. 10.

⁷³ Bkz. AB Yönergesi, m. 11; Lucas BERGKAMP, Jan DHONT, s. 84.

farkında olduğunu ispatlamanın hemen hemen olanaksız olduğu da belirtilmelidir⁷⁴.

29. Madde Veri Koruma Grubu da İnternet yazılım ve donanım ürünlerinin kullanıcılara hangi bilgilerin toplanma, saklanma ve aktarılma niyetinde olunduğu ve hangi amaçlarla bu verilerin gerekli olduğu konusunda bilgilendirilmelerini sağlayacak bir sistemin gerekliliğine işaret etmektedir⁷⁵.

B. İLGİLİNİN BİLGİLERİNE ERİŞİM HAKKI

Pek çok metinde ilgili kişinin başka kişi ve kurumların elinde bulunan kişisel verilere ulaşma hakkı kabul edilmiştir. Ancak özellikle AB Yönergesi'ndeki düzenleme dikkat çekicidir. Nitekim benzer hükümler, AK Sözleşmesi⁷⁶, OECD Rehber İlkeleri⁷⁷ ve BM Rehber İlkeleri'nde⁷⁸ bulunsa da Yönerge'deki düzenleme daha geniş kapsamlıdır⁷⁹. AİHM de kişinin bilgilerine erişim hakkını Sözleşme'nin 8. maddesinin güvence alanı kapsamında görmektedir⁸⁰.

AB Yönergesi'nin 12. maddesi, ilgili kişinin kişisel verilerinin işlenmesine ilişkin veri denetçisinden bazı temel bilgileri sağlamasına olanak vermektedir.

⁷⁴ Lucas BERGKAMP, Jan DHONT, s. 84.

⁷⁵ Lucas BERGKAMP, Jan DHONT, s. 84; Working Party on the Protection of Individuals with regard to the Processing of Personal data, **Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware**, WP 17, 23 Şubat 1999.

⁷⁶ AK Sözleşmesi m. 8.

⁷⁷ OECD Rehber İlkeleri par. 13-14.

⁷⁸ BM Rehber İlkeleri 4. İlke.

⁷⁹ Lee A. BYGRAVE, **Data Protection Law**, s. 65.

⁸⁰ Bilgilere erişim hakkına ilişkin Mahkeme'nin ilk kararı Leander'in İsveç'e karşı yaptığı başvuru (b.n. 9248/81, k.t. 26 Mart 1987) üzerine verilmiştir. Başvuruya konu olan olayda, hakkındaki güvenlik soruşturması nedeniyle İsveç'li bir marangoz olan Leander'in askeri bir deniz üssü yakınındaki müzedeki işine son verilmesi söz konusudur. Ayrıca Leander'in kendisine ilişkin güvenlik kayıtlarına ulaşmasına da izin verilmemiştir. Mahkeme'ye göre başvuranın kişisel verilerinin ulusal güvenlik gerekçeleriyle gizli olarak tutulması ve yayımı özel yaşama müdahale oluşturmaktadır. Bu nedenle 8. maddenin kapsamında değerlendirilmelidir (par.48). Nitekim Leander'e ilişkin bilgi, yalnızca güvenlik güçlerince tutulmakla kalmamış, ayrıca kendisi hakkındaki güvenlik soruşturması nedeniyle ilgili birime de aktarılmıştır. Ancak Mahkeme'nin ve Komisyon'un bu olaya ilişkin açıklamaları oldukça belirsizdir. Burada Mahkeme'nin bilgilerin gizliliği ile tutulmaları ve aktarılmalarına ilişkin sorunlara değinmediği görülmektedir. Mahkeme, Sözleşme'nin düşüncüyü açıklama özgürlüğüne ilişkin 10. maddesi çerçevesinde yaptığı değerlendirmede, bu hükmün, somut olaydakine benzer şartlarda, bireye kendi kişisel durumuna ilişkin kayıtlara erişim hakkı tanımadığı gibi, devlete de bu tür bilgileri bireye iletme yükümlülüğü getirmediğine karar vermiştir (par. 74). Mahkeme, 10. madde çerçevesinde Sözleşmeciler Devletin böylesine bir pozitif yükümlülüğünün bulunmadığı belirtilse de, bu hakkın 8. madde kapsamında değerlendirilebileceğine hükmetmiştir. İlk kez Gaskin Birleşik Krallık'a karşı, kararında (b.n. 10454/83, k.t. 7 Temmuz 1989) dile getirilen bu yaklaşım, daha sonraki başka kararlarda da tekrarlanmış ve devlet tarafından tutulan kişisel verilere erişim talepleri 8. maddenin kapsamında görülmüştür.

Burada şu noktaya dikkat çekmek gerekir: belirtilen hükümde kişiye yalnızca kendisine ilişkin verilere ulaşma hakkı tanınmamış, bunun yanında verilerin nasıl kullanıldığı, işleme amaçları, verinin kaynağı ve alıcıları gibi başka bilgilerin alınmasına da olanak verilmiştir⁸¹. Bu bilgilerin ilgili kişiye gereksiz yere geciktirilmeden ve gereksiz masraflardan kaçınılarak bildirilmesi gerekir⁸².

İlgili kişinin erişim hakkı uygulamada çözülmesi gereken bazı sorunlara neden olur. İşlem karşısında makul bir ücretin takdir edilip edilmeyeceği, eğer edilecekse bu ücretin “makul”lük derecesinin ne olduğu, ne oranda bilginin sağlanması gerektiği, istenilen bilginin başkalarına ilişkin kişisel veriler de içermesi durumunda hangilerinin çıkartılacağı bu sorunlardan bazılarıdır.

Bu sorunlar ancak AB üyesi devletlerin kendi ulusal düzenlemeleri uyarınca yapılacak yorumlar ile çözülebilir⁸³. Burada AB Yönergesi’nin hedeflerini tekrar hatırlamak gerekir. Yukarıda da belirtildiği üzere Yönerge’nin yöneldiği temel amaçlardan biri Avrupa’da verilerin korunmasına ilişkin farklı yaklaşımları uyumlaştırmaktır. Ancak ilgilinin haklarını kullanabilmesi açısından kendi sınırlarını aşan bir öneme sahip olan erişim hakkında masraflara ve makul süreye ilişkin farklı uygulamalar dikkat çeker. Avrupa Komisyonu, bilgilere erişim hakkı açısından üye devletler arasında “tatmin edici” düzeyde uyum bulunduğu görüşündedir⁸⁴. Ancak uygulamadan örnekler bu saptamaya şüpheyi yaklaştırmayı gerektirir.

⁸¹ AB Yönergesi’nin 12. maddesi şu hükmü içermektedir:

“Üye devletler her ilgili kişinin veri denetçisinden şunları edinmesini sağlar:

(a) makul aralıkları sınırlama ve aşırı gecikme ve masraf olmaksızın:

- kendisine ilişkin verilerin işlenip işlenmediğinin teyidi ve an azından işlemenin amacını (belirten) bilgi, ilgili veri kategorileri ve verinin açıklandığı alıcılar ya da alıcı kategorileri;

- işlenmekte olan verinin kaynağına ilişkin her türlü bilginin anlaşılır bir şekilde iletilmesi;

- en azından m. 15/1’de düzenlenen otomatikleştirilmiş kararlar durumunda, kendisine ilişkin verinin her tür otomatik işlenmesinin temelini içeren bilgi;

(b) özellikle verinin yapısının eksik veya yanlış olmasından dolayı, işlenmesi bu Yönerge’nin hükümlerine göre uygun olmayan verinin düzeltilmesi, silinmesi veya engellenmesine uygun olarak;

(c) olanaksız olduğunun kanıtlanması veya oransız bir çaba gerektirmesi durumları hariç olmak üzere, (b) fıkrasına uygun olarak her tür düzeltme, silme veya engellenmenin verinin açıklandığı üçüncü kişilere bildirilmesi”.

⁸² Her ne kadar yalnızca 1. maddenin (a) bendinde gereksiz masraf ve gecikmelerden kaçınılması gerekliliği belirtilmişse de uygulamada ve AB üyesi ülkelerin ulusal hukuk sistemlerinde bunun (b) ve (c) bentlerinde yer alan düzeltme, silme, engelleme ve üçüncü kişilerin bilgilendirilmesi haklarına da uygulanacağı kabul edilmektedir. Christopher KUNER, s. 63-64.

⁸³ Christopher KUNER, s. 64.

⁸⁴ European Commission, **First Report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final, Analysis and impact study on the implementation of Directive 95/46/EC in Member States**, par. 20; Christopher KUNER, s. 64, d.n. 3.

Bu noktada Birleşik Krallık ile Avrupa Komisyonu arasında, önemli tartışmalara neden olan *Durant davası*ndan kısaca söz edilmelidir⁸⁵. Birleşik Krallık Temyiz Mahkemesi, Durant’ın Finansal Hizmetler mercisine karşı açtığı davada ilgilinin erişim haklarını oldukça sınırlayan bir karar vermiştir. Mahkeme, başvuru Durant’ın bir banka tarafından kendisine ilişkin olarak bilgisayar ortamında yer alan düzenlenmemiş belgeleri ile elle tutulmuş kayıtlarının açıklanması yönündeki isteğini reddetmiştir. Mahkemenin bu kararında iki dayanağından biri kayıtların “*kişisel veri*” niteliğini taşıması, diğeri ise elle tutulan kayıtların Birleşik Krallık Veri Koruma Yasası uyarınca “*ilgili dosyalama sistemi*” sayılamayacağı yönünde yorumudur. Bu kararda geliştirilen yorumun AB veri koruma hukuku ile uyumlu olup olmadığı ise tartışmaya açıktır⁸⁶.

İlgilinin kişisel verilerine erişim hakkı, onların doğruluğunu denetleme ve onları düzeltme, sildirme ve engelleme hakkının da bir gerekliliğidir. Ancak erişim hakkını yalnızca bu amaca hizmet eder şekilde de düşünmemek gerekir. Nitekim birey ancak hangi verilerinin, kimlerin elinde, ne gibi amaçlarla tutulduğunu ve kullanıldığı bilerek bilgilerinin geleceğini belirleme hakkından yararlanabilir⁸⁷.

⁸⁵ *Durant v Financial Services Authority* [2003] EWCA Civ 1746, Court of Appeal (Civil Division), par. 2.84-2.85; ayrıca bkz. *Johnson v Medical Defence Union* [2006] EWHC 321(Ch); Christopher KUNER, s. 64.

⁸⁶ Christopher KUNER, s. 64-65.

⁸⁷ Avusturya Anayasa Mahkemesi de önüne gelen bir olayda bu duruma işaret etmiştir. Başvuruya konu olan olayda ilgili kişi, bir doğrudan pazarlama şirketinin elinde bulunan verilere erişim hakkını kullanmak istemiştir. Şirket, kişilerin adları, adresleri, özel ilgi alanları, gelirleri gibi pazarlama ile ilgili bilgilerini bir CD içerisinde tutmakta ve bunların ticari amaçlarla satışını yapmaktadır. Belirtilen şirket, CD’nin içeriği hakkında ilgili kişiyi bilgilendirmekle birlikte, bu bilgilerin alıcıları hakkında bilgi vermekten kaçınmış ve yalnızca kendileri ile sözleşmesel bir ilişki içinde bulunanlara bu bilgileri verdiklerini açıklamıştır. Avusturya Veri Koruma Mercisi de ilgili kişinin kendisine yaptığı başvuru üzerine, alıcıların somut olarak adlarının açıklanmamasını doğrudan pazarlama şirketi ile alıcılar arasındaki veri koruma ilişkisi açısından yerinde görmüştür. Ayrıca Avusturya Veri Koruma Mercisi’ne göre ilgili kişinin haklarını kullanabilmesi için alıcıların somut olarak adlarını bilmesine de gerek yoktur. İlgili kişi verilerinin daha sonra işlenmesini istemiyorsa, bunun için yalnızca şirketi bilgilendirmesi yeterlidir. CD’nin sürekli güncellenen yapısı dolayısıyla bu, alıcıların sonraki işlemlerini de önleyecektir. Avusturya Anayasa Mahkemesi, bu noktada ilgili kişiye erişim hakkı tanınmanın tek hedefinin daha sonraki işlemlerin engellenmesi olmadığına işaret etmiştir. Erişim hakkı, ilgili kişinin verilerinin nerede bulunduğunu bilme hakkını da güvencelemektedir. O halde, erişim hakkını yalnızca bilgilerin sonraki işlemlerini önleme hedefine yönelmediğini bilmek, bu hak alanının kapsamı konusunda doğru bir değerlendirme yapabilmek için gereklidir. Belirtilen olaya ilişkin olarak bkz. Alexander FLENDROVSKY, “The Scope of the Right to Access Under the Fundamental Right of Data Protection, Austrian Constitutional Court Judgement of October 2nd, 2007, (B227/05)”, *International Constitutional Law Journal*, C. 2, S. 3, Y. 2008, s.213-217, <http://www.icl-journal.com>.

C. İLGİLİNİN VERİLERİNİ DÜZELTME HAKKI

95/46/AT sayılı Yönerge'nin 12/b hükmü uyarınca ilgili kişinin Yönerge'nin hükümlerine uygun olmayan, özellikle de eksik ve yanlış olan verileri düzeltme hakkı bulunur. İlgili kişinin verilerinin düzeltilmesini, silinmesini veya engellenmesini sağlama hakkı, bilgilere erişim hakkının bir uzantısıdır⁸⁸. Ayrıca yukarıda incelenen verilerin doğru ve güncel tutulması gerekliliği ile de yakından ilişkilidir.

Yönerge'de bu etkinlikler tanımlanmadığı gibi hangi durumlarda “engelleme”nin söz konusu olacağı da belirtilmemiştir. Ancak burada engelleme daha çok önleyici bir koruma olarak düşünülebilir. Örneğin bir işlemin hukuka aykırı olup olmadığı henüz netlik kazanmadığı dönemde veriye erişimin engellenmesi yoluna gidilebilir⁸⁹.

D. İLGİLİNİN DİĞER HAKLARI

Yukarıda ilgili kişinin veri işleme sürecine müdahalesini sağlayan önemli haklarından kısaca söz ettik. İlgilinin bilgilendirilmesi, bilgilere erişim ve verileri düzeltme hakları kişisel verileri üzerindeki denetimini sürdürebilmesi açısından gereklidir. Ancak bunun yanında çeşitli metinlerde ilgiliye tanınmış başka bazı haklar da dikkat çeker.

Örneğin AB Yönergesi'nde ilgili kişiye belirli durumlarda veri işlemeye itiraz hakkı⁹⁰ ve otomatik bireysel kararların konusu olmama hakkı⁹¹ tanınmıştır. Bu haklar diğer temel veri koruma metinlerinde yer almamaktadır. Hatta Avrupa'da pek çok ulusal hukuk düzenlemesinde de, AB Yönergesi'nde kabul edilen ilkeler olmalarına rağmen, bunlara yer verilmediği görülür⁹². Sınırlı uygulama alanı bulunmasına karşın kişilerin bilgilerinin geleceğini belirleme hakkı açısından önemli nitelikleri dolayısıyla bunlara kısaca değinmek gerekir.

⁸⁸ Oğuz ŞİMŞEK, s. 92.

⁸⁹ Alfred BÜLLESBACH, Yves POULLET, Corien PRINS, **Concise European IT Law**, Kluwer Law International, Hollanda 2006, s. 66-67.

⁹⁰ AB Yönergesi m. 14.

⁹¹ AB Yönergesi m. 15.

⁹² Lee A. BYGRAVE, **Data Protection Law**, s. 66.

1. İlgilinin İtiraz Hakkı

İlgili kişinin itiraz hakkı oldukça geniş bir şekilde yorumlanmaktadır⁹³. AB Yönergesi'nin 14. madde hükmü içerisinde ilgili kişinin genel olarak verilerin işlenmesine ve doğrudan pazarlamaya itiraz hakkı düzenlenmiştir.

Yönerge'nin 14/a hükmü uyarınca ilgili kişi belirli durumlarda verilerin işlenmesine itiraz edebilir⁹⁴. 14/b hükmünde ise ilgili kişinin verilerinin doğrudan pazarlama amacıyla işlenmesi durumunda bedelsiz itiraz hakkı yer alır⁹⁵. Bundan başka ilgili kişinin, üçüncü kişilere verilerinin ilk kez açıklanmasından önce veya bu üçüncü kişilerin adına doğrudan pazarlama amaçlı kullanılmasından önce haberdar edilmek ve böylesi açıklamalara veya kullanımlara bedelsiz olarak itiraz etme hakkı tanınmıştır⁹⁶. Ayrıca ilgili kişinin bu hakkı konusunda bilgilendirilmesi de gerekir.

2. İlgilinin Otomatik Kararların Konusu Olmama Hakkı

İlgilinin otomatik kararların konusu olmama hakkı bireysel özerklik ile yakından ilişkilidir. AB Yönergesi'nin 15/1 hükmü, her bireye kendisine yönelik hukuksal sonuçlar yaratan, kendisini önemli ölçüde etkileyen ve işindeki performansı, kredi itibarı, güvenilirliği, davranışları gibi kişisel durumların değerlendirilmesi amacıyla yalnızca otomatikleştirilmiş veri işlenmesine dayanan bir karara tabi olmama hakkı tanımaktadır. 1978 tarihli eski Fransız Veri Koruma Yasası'ndan Yönerge'ye aktarılan bu hüküm Üye Devletlerin tamamında kabul

⁹³ Avrupa Ombudsmanı, Avrupa Komisyonu'na karşı yapılan bir başvuruda AB Yönergesi'nin 14/b hükmü kapsamında düzenlenen ilgili kişinin verilerin işlenmesine itiraz hakkının yalnızca verileri kendi doğrudan pazarlama amaçları için kullanacak organlar ile sınırlandırmanın “veri işleme”nin kapsamını daraltan bir yorum olduğuna karar vermiştir. Oysa aktarım ile açıklama, yayınlama ya da başka herhangi bir yolla ulaşılabilir kılma da “işleme” kapsamında değerlendirilmektedir. Ayrıca Avrupa Ombudsmanı, Avrupa Komisyonu'nun 14/b hükmünde sözü geçen veri denetçilerini kamu iktisadi teşebbüsleri ile sınırlandırmasını da uygun bulmamıştır. Bkz. **Decision of the European Ombudsman on complaint 2467/2004/PB against the European Commission**, 9 Haziran 2006, par. 1.6; Christopher KUNER, s. 65.

⁹⁴ Bu özel durumlar, Yönerge'nin 7(e) ve (f) hükümlerinde belirlenen işlemenin kamusal otorite tarafından veya kamu yararı için yapılması veya veri denetçisinin meşru çıkarına hizmet etmesi durumlarıdır. Bkz. Veri Koruma Yönergesi, m. 14/a. İtiraz hakkı kaynağını eski Fransız Veri Koruma Yasası'nda (1978) bulmaktadır. Bu hakkın uygulamasının da Üye Devletler arasında çeşitlilik gösterdiği görülmektedir. Fransa gibi kimi ülkeler inandırıcı ve meşru nedenler için genel bir itiraz hakkı tanıırken, Finlandiya kimi ülkeler, doğrudan pazarlama gibi belirli konulara yönelik, özel itiraz hakkı tanımaktadır. Bkz. Alfred BÜLLESBACH ve diğ., s. 73.

⁹⁵ Belirtmek gerekir: AT bünyesinde kabul edilen genel ve özel Yönergelerde “doğrudan pazarlama”nın tanımı yapılmamıştır. Yalnızca 95/46/AT sayılı Yönerge'nin Başlangıç bölümü 30. paragrafında “*ticari olarak veya bir yardım kuruluşu veya örneğin, siyasal nitelikli başka bir dernek veya vakıf tarafından gerçekleştirilen pazarlama amacıyla kişisel verilerin üçüncü bir kişiye açıklanması koşulları*”ndan söz edilmektedir.

⁹⁶ Veri işlemeye itiraz hakkı geniş yorumlanmalıdır. Bkz. **Decision of the European Ombudsman on complaint 2467/2004/PB against the European Commission**, 9 Haziran 2006, par. 1.6.

edilmiş olmakla birlikte, uygulamasına nadiren rastlanmaktadır⁹⁷. Oysa bu hüküm kişisel verilerin korunmasındaki temel düşünce ile yakından ilişkilidir. Nitekim burada kişiye otomatikleştirilmiş, bir başka anlatımla insan müdahalesinin bulunmadığı kararların konusu olmama seçeneği sunulmaktadır. Çalışmamızın birinci bölümünde bu türdeki kararların kişiliğin zarar görmesi gibi ciddi sonuçları olabileceğinden söz etmiştik.

Bu noktada ilgili hükmün uygulamasının bazı durumlarda sınırlandırıldığı da belirtilmelidir. Buna göre: Üye Devletler, iki durumda ilgili kişinin böyle bir kararın konusu olmasına izin verebilir. İlk olarak, eğer bu karar ilgili kişinin bir sözleşmenin tarafı veya sözleşmenin işlerliği için alınıyorsa, ilgilinin meşru çıkarlarının korunması için tatmin edici veya uygun önlemlerin alınması koşuluyla kabul edilebilir⁹⁸. İkinci olarak veriye konu olan kişinin meşru çıkarlarını korumak için önlemler saptayan bir yasa tarafından öngörülmüşse otomatik bir kararın konusu olabilir⁹⁹. Burada dikkat çekici bir nokta: her iki istisnada görülen “*tatmin edici*” ve “*meşru çıkar*” ifadelerinin özelleştirilmemiş olmasıdır. Bu, hükmün uygulaması açısından bir belirsizliğe neden olabileceğidir¹⁰⁰.

Bu hüküm, verilerin korunmasında yeni bir ilkenin temelini oluşturur. Buna göre, kişinin karakterinin tamamen otomatik yollardan değerlendirilmesi onun çıkarlarını önemli ölçüde etkileyecek kararların temelini oluşturmamalıdır¹⁰¹. Bu yönetime ilişkin tipik bir örnek kişilerin kredi istemlerinin değerlendirilmesi konusunda verilebilir. Yalnızca rakamsal bazı bilgilere dayanılarak bir bilgisayar sistemince, herhangi bir insanın müdahalesi olmaksızın, kişi kredi derecelendirilmesine tabi tutulmamalıdır¹⁰². Bu noktada ortaya çıkabilecek sorunların giderilmesi için şirketler, en son kararın her zaman bir bilgisayar yerine bir insan tarafından verilmesini sağlayabilirler¹⁰³.

⁹⁷ BÜLLESBACH ve diğ., s. 74.

⁹⁸ AB Veri Koruma Yönergesi m.15/2,a.

⁹⁹ AB Veri Koruma Yönergesi, m.15/2,b.

¹⁰⁰ Federico FERRETTI, **The Law and Consumer Credit Information in the European Community, The Regulation of Credit Information Systems**, Routledge-Cavendish, ABD-Kanada 2008, s. 174.

¹⁰¹ Lee A. BYGRAVE, **Data Protection Law**, s. 66.

¹⁰² Federico FERRETTI, bu hükmün kredi raporlamayı değil, onunla yakından ilişkili başka bir işlemi: kredi derecelendirmeyi etkileyeceğini belirtmektedir. Bkz. Federico FERRETTI, s. 175.

¹⁰³ Christopher KUNER, s. 65.

IV. İLGİLİNİN RIZASI

Kişisel verilerin korunması hukukunda ilgili kişinin rıza beyanında bulunması da veri işleme sürecine katılmasını sağlayan önemli unsurlardan biridir. Ancak niteliği gereği yukarıda incelenen “*ilgili kişinin katılımı ve denetimine yönelik ilkeler*”den farklılaşan yönleri bulunur. Bu nedenle burada ayrıca değerlendirilmesi tercih edilmiştir. Nitekim ilgilinin rızası, verilerin işlenmesinin en önemli meşruluk temellerinden biridir. Bu bağlamda “*rıza*” ilgili kişinin kendisiyle ilgili veriler üzerinde denetimini sağlamasının önemli bir aracı ve “*bilgilerin geleceğini belirleme*” düşüncesinin bir yansımasıdır¹⁰⁴.

Ancak bu noktada hemen belirtmek gerekir: kişisel verilerin korunmasına ilişkin düzenlemelerden bir bölümünde bireyin rıza vermesi koşulu yer almadığı gibi¹⁰⁵, AB Yönergesi gibi başka metinlerde verilerin işlenmesinin tek meşru koşulu olarak değerlendirilmemiş, yalnızca veri işlemeyi meşru kılan durumlar içerisinde sayılmıştır. Bunun yanında diğer koşulların geniş yorumlara olanak veren yapısı, rızanın aranmasının zorunlu olduğu durumların oldukça sınırlı kalmasına neden olmaktadır¹⁰⁶. Buna karşılık “*doğrudan pazarlama*” gibi bazı konularda veri işlemenin meşruiyet kazanabilmesi için ilgilinin rızası şarttır¹⁰⁷.

A. RIZA BEYANININ NİTELİĞİ

AB Temel Haklar Şartı’nda da yer almış bu ilkenin¹⁰⁸, AB Yönergesi’ndeki ve üye devletlerin ulusal hukuk sistemlerindeki düzenlenme şekli konumuz açısından oldukça önemlidir. AB Yönergesi’nde rıza, kişinin kendisiyle ilgili verilerin işlenmesini kabul ettiğini gösteren, belirli ve aydınlatılmış özgür iradesinin her türlü işareti¹⁰⁹ olarak tanımlanmıştır. Ayrıca yine Yönerge’ye göre bunun bir hukuka uygunluk koşulu olarak değerlendirilebilmesi için, ilgili kişinin rızasının “*şüpheye*

¹⁰⁴ Lucas BERGKAMP, Jan DHONT, “Data Protection in Europe and the Internet: An Analysis of the European Community’s Privacy Legislation in the Context of the World Wide Web”, **The EDI Law Review**, s.7, Y. 2000, s. 78.

¹⁰⁵ Örneğin AK Sözleşmesi’nde bu konuda herhangi bir hüküm bulunmamaktadır.

¹⁰⁶ Lee A. BYGRAVE, **Data Protection Law**, s. 66. Ayrıca bkz. Veri Koruma Yönergesi m. 7.

¹⁰⁷ Peter CAREY, s. 250.

¹⁰⁸ ABTHŞ m.8.

¹⁰⁹ AB Yönergesi m.2/h.

yer bırakmayacak” nitelikte, bir başka anlatımla “kesin” olması gerekir¹¹⁰. Hassas kişisel verilerin söz konusu olduğu durumlarda ise ayrıca rızanın “açık” olması da gerekmektedir¹¹¹. Görüldüğü gibi AB Yönergesi’nde nitelikli bir rıza beyanı aranmaktadır. Buna göre rıza beyanının geçerli sayılabilmesi için dört durumun bir arada bulunması gerekir:

- Rıza, ilgili kişinin isteminin açık ve kesin bir göstergesi olmalı, bir başka ifadeyle ilgili kişinin rıza gösterip göstermediği konusunda herhangi bir şüphe bulunmamalıdır. Bu durumda beyanın içeriğine ilişkin herhangi bir kuşku varsa bu ölçüt sağlanmamış olur. Şüpheyi yer bırakmayan rızanın aranması, hem açık hem de örtülü beyanın kabul edilebileceği sonucunu getirir¹¹². Nitekim öğretide “(b)eyanın anlam ve konusu hiçbir yoruma ve karışıklığa yer vermeyecek şekilde beyan vasıtalarından, yani kullanılan söz, yazı ve işaretlerden anlaşılıyorsa”¹¹³ bu açık bir irade beyanı olarak kabul edilmektedir. Bu durumda açık irade beyanının buradaki ölçütü karşılayacağına şüphe yoktur¹¹⁴. Sorun, örtülü irade beyanının bu koşulu sağlayıp sağlamayacağıdır.

Örtülü irade açıklamasında, kişi isteğini başka davranış biçimleriyle veya bunların yorumuyla ortaya koyar. Burada ilgili kişinin susmasının nasıl değerlendirileceği önemli bir tartışma konusudur. Kural olarak (Türk hukuk sisteminde) susma kabul değil red anlamına gelir, ancak bunun istisnaları da bulunur¹¹⁵. Konumuz açısından ise, Yönerge’de hüküm altına alınan “şüpheyi yer bırakmayacak” ifadesini hatırdan çıkarmamak gerekir. Şüpheyi yer bırakmayacak şekilde ilgili kişinin iradesini ortaya koyan örtülü bir beyan, bu koşulu sağlamış olacaktır. Ancak ilgili kişinin susması, başka herhangi bir belirti olmaksızın iradenin kesin ifadesi olarak değerlendirilemez¹¹⁶.

¹¹⁰ AB Yönergesi m. 7/a.

¹¹¹ Bu konu aşağıda “Hassas kişisel verilerin nitelikli korunması” başlığı altında incelenecektir.

¹¹² Nilgün BAŞALP, **Kişisel Verilerin Korunması ve Saklanması**, s. 40.

¹¹³ Fikret EREN, **Borçlar Hukuku, Genel Hükümler**, Beta, 9. Baskı, İstanbul 2006, s. 124.

¹¹⁴ Bkz. aynı yönde Nilgün BAŞALP, **Kişisel Verilerin Korunması ve Saklanması**, s. 40.

¹¹⁵ Örtülü irade beyanına ilişkin açıklamalar için bkz. Ahmet KILIÇOĞLU, s. 29-30; Fikret EREN, s. 124 vd.

¹¹⁶ Bkz. aynı yönde Nilgün BAŞALP, **Kişisel Verilerin Korunması ve Saklanması**, s. 40. Federal Almanya Veri Koruma mevzuatına göre sürekli susma halinin bazı durumlarda kabul olarak nitelendirilebileceği yönünde görüşler bulunmaktadır. Buna göre, sürekli bir iş ilişkisi içinde bir kez verilerin korunmasına izin verilmişse ve daha sonra koşullar değişmemişse, sürekli susmanın kabul edilebileceği belirtilmektedir. Bkz. Peter GOLA, Rudolf SCHOMERUS, s. 180, par. 13.

- Rıza, ilgili kişinin özgür iradesinin yansıması yani serbest ve özgür bir zihinsel etkinliğinin ürünü olmalıdır¹¹⁷. Bunun için de ilgili kişi rıza göstermeye mecbur bırakılmamalı, üzerinde dışsal herhangi bir baskı yani kişinin iradesini bozacak herhangi bir hal bulunmamalıdır. Ancak burada hukuksal açıdan yalnız hata, hile ve tehdidin unsurları dikkate alınmamalıdır. İki taraf arasında dikey ilişkinin söz konusu olduğu çeşitli durumlarda bağımlı tarafın özgür iradesinin oluşup oluşmadığı sorgulanabilir. Örneğin işçi ile işveren arasındaki ilişki bu kapsamda düşünülebilir¹¹⁸.

Her durumda rızanın özgür iradenin bir sonucu olarak verilmesi gerekir. İşçinin de teoride kişisel verilerinin işlenmemesini isteme hakkı bulunur. Ancak bu durumda, işçinin bir iş olanağını kaybetmesi sonucu doğabileceğinden, üzerinde bir baskı oluşabileceği dikkate alınmalı ve ek bazı güvenceler sağlanmalıdır. İşçi ile işveren arasındaki ilişkinin niteliği dolayısıyla, işverenin işçinin rızasına dayanması yanıltıcı olabilir. Bu nedenle işlemenin meşruluğunda rızaya dayanılması sınırlandırılmalıdır¹¹⁹. Bu noktada işçinin sahipsiz özgür seçimine dayanılması ve daha sonradan çıkarları zedelenmeksizin rızasını geri alabilmesi oldukça önemlidir.

Kimi AB üyesi ülkelerin ulusal hukuk sistemlerinde işçilerin kişisel verilerinin korunması için temsilcilerinden yardım alındığı görülmektedir. Örneğin bazı ülkelerde işyerinde denetim sistemleri kurulmadan önce işçi konseyleri ile işverenin bir anlaşmaya varması gerekir¹²⁰. Bunun yanında dikey/hiyerarşik ilişkiyi yalnızca işçi-işveren ile sınırlı düşünmemek gerekir. İlgili kişinin veri denetçisine önemli oranda bağlı olduğu diğer durumlarda da rızanın “özgürce verilmiş” sayılabilmesi için bazı ek güvenceler tanınmalıdır. Örnek olarak hekim-hasta ilişkisi

¹¹⁷ Ahmet KILIÇOĞLU, **Borçlar Hukuku, Genel Hükümler**, Turhan, 7. Baskı, Ankara 2006, s. 28.

¹¹⁸ Christopher KUNER, s. 68.

¹¹⁹ Nitekim İngiltere’de veri koruma otoritesi, işverenlerin işçilerin kişisel verilerini işlerken meşruiyet temeli olarak nadiren rıza beyanına dayanabileceklerine işaret etmiştir. Bkz. Peter CAREY, s. 72-73.

¹²⁰ Article 29 Working Party, **Opinion on the Processing of Personal Data in the Employment Context**, (Opinion 8/2001, WP 48), 13 Eylül 2001, s. 23. Kişisel veri içeren e-postaları işverenin incelemesi açısından da bu kural geçerlidir. E-posta görüntülemenin meşruluk dayanağı, 95/46/EC m. 7/f olabilir. Ancak şunu belirtmek gerekir, eğer işçiye e-posta hesabı tamamen kişisel kullanım için verilmişse veya web-mail hesabına ulaşımına izin verilmişse bu hesaptaki postaların işveren tarafından açılmasına kural olarak m.7/f altında meşruluk kazanabileceği durumlar oldukça sınırlıdır. Bu, örneğin cezai bir etkinlik dolayısıyla postalara ulaşılması gerekmesi gibi sınırlı durumlarda söz konusu olabilir. Normal koşullarda ise virüslerin araştırılması için hesaba ulaşılması kabul edilebilir bir nedendir. Article 29 Working Party, **Working Document on the Surveillance of Electronic Communications in the Workplace**, WP 55, 29 Mayıs 2002, s.21, d.n. 23.

gösterilebilir. Bu durumda hekimin, hastanın verilerinin işlenmesine rıza göstermemesinin kendisine sağlanacak tedavi hizmetini etkilemeyeceğini açıkça belirtmesi gerekir¹²¹.

Ayrıca reddin bir yaptırımının bulunduğu durumlarda da rıza, özgürce verilmiş sayılmaz. Buna örnek olarak rızanın anlaşma için koşul olarak görüldüğü durumlar verilebilir. Ancak bu noktada külfetin ağırlığına bakmak gerekir. Rıza göstermeme sonucunda karşılaşılabilecek külfet son derece hafif ise rıza, özgür iradenin bir ürünü olarak düşünülebilir. Bir örnek vermek gerekirse, parasız elektronik posta hizmetlerinin bir bölümünü kullanabilmek için çerezlere (cookies) izin vermek bir zorunluluktur. Bu durumda eğer İnternet ortamında aynı hizmetin bedavaya, üstelik de çerezlere izin vermeye gerek olmaksızın alınabileceği başka siteler varsa, rızanın özgürce verildiğini kolaylıkla söyleyebiliriz¹²².

- *Rıza genel nitelikli olmamalı, belirli bir duruma özgülenmiş olarak verilmelidir.* Bu ilke özellikle az önceki değerlendirmede de belirtildiği gibi bazı durumlarda daha öncelikli bir önem kazanmaktadır. Rızanın belirli bir duruma özgülenmiş sayılması için kişisel verinin işlenmesine rıza gösterilen somut olayın çok iyi bir şekilde tanımlanmış olması gerekir¹²³. Ayrıca bu koşul uyarınca kişinin kendisine ilişkin her türlü veri işlemeyi kapsar şekilde genel nitelikli bir rıza beyanında bulunması koşulun gerçekleşmesi için yeterli değildir.

- *Aydınlatılmış bir rıza beyanı bulunmalıdır.* Yani kişinin neye rıza gösterdiği konusunda bilgilendirilmiş olması gerekir. Kişisel verilerin daha sonraki işlemelerine ilişkin rıza beyanı da gerektiğinden bu konuda da bazı bilgiler sunulmalıdır¹²⁴. İlgili kişinin neye rıza gösterdiği konusunda bilgilendirilmesi, rızanın “*şüpheye yer bırakmayacak*” şekilde verilmesi gerekliliği ile de yakından ilişkilidir. Örneğin, ilgili kişinin verilerinin yeterli düzeyde koruma getirmeyen üçüncü bir ülkeye aktarımı riski varsa bu konuda uygun şekilde bilgilendirilmesi gerekir. Eğer böyle bir bilgi sağlanmamışsa ilgili kişinin rızasının şüpheye yer bırakmayacak nitelikte olduğu

¹²¹ Lucas BERGKAMP, Jan DHONT, s. 77.

¹²² Lucas BERGKAMP, Jan DHONT, s. 78.

¹²³ Article 29 Working Party, **Working Document on the processing of personal data relating to health in electronic health records (EHR)**, WP 131, 15 Şubat 2007, s. 9.

¹²⁴ Christopher KUNER, s. 67.

söylenemez¹²⁵. Bunun yanında kimi ulusal düzenlemelerde aydınlatma yükümlülüğünün içeriği hakkında da bilgi verilmiştir. Örneğin Federal Almanya Veri Koruma Yasası'na göre rızası istenen ilgili kişi, verilerin toplanma, işleme ve kullanma amaçları ve somut olayda, zorunluluk ya da istek gereği, elden geldigince rıza vermekten çekinmenin sonuçları konusunda bilgilendirilmelidir¹²⁶.

Ayrıca kişiyi rıza gösterdiği konuda bilgilendirirken anlaşılır bir dil kullanılması da gerekir. Kişinin, anlayamayacağı terimlerin ya da okumakta güçlük çekeceği oranda küçük puntolarla basılmış ve sıkışık ifadelerin yer aldığı matbu bir formu imzalaması ile aydınlatılmış rıza beyanı alınmış olmayacaktır. Aynı şekilde ilgili kişiyle yapılan bir sözleşmenin içine sıkıştırılmış, kişinin gözünden kaçabilecek ifadeler de kabul edilemez¹²⁷.

AB Yönergesi'nde bu koşulları taşıyan rıza beyanının şekline ilişkin ise herhangi bir koşul aranmamaktadır. Belirtilen koşulları içeren iradenin "*her türlü işareti*" kabul edilmektedir. Kişisel verilerin korunmasında ilgili kişinin rıza beyanına ilişkin olarak AB üyesi ülkelerin kimisinde rıza beyanına yer verilmemesine karşın, kimi ulusal düzenlemelerde ise nitelikli bir rıza beyanı aranmaktadır. Bunun yanında AB Yönergesindeki Hatta Almanya gibi kimi ülkelerde "*rıza*"nın koşulları oldukça ayrıntılı bir şekilde düzenlenmiştir. Federal Almanya Veri Koruma Yasası'na göre, rızanın yazılı olması gerekir. Elektronik ortamda yapılan kabullerde de yazılılık koşulu gerçekleştirilmiş olmaktadır¹²⁸.

Bu noktada elektronik ortamda verilen rıza beyanlarının geçerli olup olamayacağı değerlendirilmelidir. Kural olarak koşulları taşıyan ve fakat elektronik ortamda açıklanmış bir rıza beyanının geçerli sayılmaması için herhangi bir neden bulunmamaktadır¹²⁹. Ancak özellikle elektronik ortamdaki ticari etkinliklerde kişinin

¹²⁵ Working Party on the Protection of Individuals with regard to the Processing of Personal Data, **Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive**, WP 12, 24 Temmuz 1998, s.24

¹²⁶ Bkz. Federal Almanya Veri Koruma Yasası, m. 4a/1.

¹²⁷ Alman hukukundaki duruma ilişkin olarak bkz. Peter GOLA, Rudolf SCHOMERUS, s. 180, par. 12, 13. Federal Almanya Veri Koruma Yasası'nda bunun gibi sıkıntıları önlemek amacıyla "*Eğer rıza başka yazılı beyanlarla birlikte veriliyorsa, görünüşünde ayırt edilebilir olmalıdır*" hükmü düzenlenmiştir. Bkz. Federal Almanya Veri Koruma Yasası, m. 4a/1, son cümle.

¹²⁸ Peter GOLA, Rudolf SCHOMERUS, **Bundesdatenschutzgesetz Kommentar**, s. 180, par. 13.

¹²⁹ Aynı yönde bkz. Nilgün BAŞALP, **Kişisel Verilerin Korunması ve Saklanması**, s. 40. Elektronik ortamda yapılan rıza beyanları açısından son yıllarda kullanım alanları ve yaygınlığı hızla artan elektronik imzanın da önemli bir yeri bulunmaktadır. Diğer hukuksal işlemlerde olduğu gibi, bu konuda da rıza beyanında bulunan kimliğinin işareti olan ve kimi zaman yalnızca ispat, kimi zaman ise geçerlik koşulu olan ıslak imzanın, elektronik ortamdaki karşılığı olarak

rızasının alınması bazı riskleri beraberinde getirir. Bunlar daha çok ilgili kişinin neye rıza gösterdiği konusunda tam olarak bilgilendirilmemesi ve neye rıza gösterdiğini tam olarak anlayamaması tehlikesinden kaynaklanır¹³⁰.

Özellikle İnternet ortamında toplanan ve işlenen veriler açısından ilgili kişinin rızasının ne şekilde alınacağı üzerinde durulmalıdır. Bu konuda öncelikli sorun belki her geçen gün daha fazla sayıda verinin aktığı siber uzayda, ilgili kişilerin haberi bile olmaksızın toplanan ve işlenen verilerdir¹³¹. Ancak bunun yanında kişilerin rızasının alınması ile verilerin işlenmesini yasallaştıma girişiminde olan sitelerin bunu ne oranda gerçekleştirebildikleri, özellikle Avrupa veri koruma sistemine uyum açısından değerlendirilmesi gereken bir konudur.

Öncelikle İnternet sitesinde rızası istenen kişinin verilerinin işlenmesine ilişkin bilginin anlaşılabilirliği üzerinde durmak gerekir. Metinde yer alan ve kabulü beklenen bilgiler; fazla uzunsa, ifadeler açık değilse, sitenin içerisindeki yönlendirmelerle bunlara ulaşılması zorlaştırılmışsa ya da ortalama bir kişinin anlayamayacağı teknik bir dilde yazılmışsa geçersiz olacaktır¹³².

İkinci olarak İngilizce “*opt-in*” ve “*opt-out*” olarak ifade edilen rıza türleri üzerinde durmak gerekir. Bu ayrımı pazarlama amacıyla yapılan işlemlere ilişkin bir örnek ile açıklayabiliriz. İnternet’i ve e-posta hizmetini kullanan kişiler, çeşitli şirketlerden pazarlama amacıyla gönderilen iletiler ile sıklıkla karşılaşmaktadır. İnternet üzerinden alışveriş yapan kişilerin tercihleri çoğu zaman kaydedilir ve kullanıcıların isteklerine paralel olduğu düşünülen ürünler ise e-posta yoluyla bu kişilere iletilir. Eğer bu postalarda “*bu iletileri istemiyorsanız aşağıdaki kutuyu işaretleyiniz*” gibi bir ifade yer alıyorsa bu, “*opt-out*” rıza beyanına örnek oluşturur. Yine aynı şirket, kullanıcılarına ilişkin verileri üçüncü kişilerle paylaşmak isteyebilir. Bu durumda ilgilinin onayını alması gerekir. Eğer bu şirket ilgili kişilere “*sizin tercihlerinize uygun fırsat ve seçenekler sunacak (...) Şirketi ile bilgilerinizi*

nitelendirilebilecek dijital imzaya ilişkin ayrıntılı bilgi için bkz. Leyla KESER BERBER, **İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza**, Yetkin, Ankara 2002, s. 119 vd.

¹³⁰ Christopher KUNER, s. 68.

¹³¹ AB Veri Koruma Grubu 2000 yılında yayınladığı bir çalışma raporunda İnternet ortamında pek çok kişisel verinin ilgisinin haberi bile olmaksızın toplandığına ve işlendiğine işaret etmiş ve bu durumun kişisel verilerin korunması açısından yarattığı sakıncaları ayrıntılı bir şekilde değerlendirmiştir. Bkz. Article 29 Data Protection Working Party, **Working Document: Privacy on the Internet-An Integrated EU Approach to On-line Data Protection-**, WP 37, 21 Kasım 2000.

¹³² Christopher KUNER, s. 68.

paylaşmamıza izin veriyorsanız aşağıdaki kutuyu işaretleyiniz” gibi bir içerik taşıyan posta gönderirse bu, “*opt-in*” rıza beyanı istendiğinin göstergesidir¹³³.

Bir başka anlatımla “*opt-in*” rıza beyanı, ilgili kişinin kabule yönelik iradesini ortaya koyan müspet bir hareketini gerektirir. Oysa “*opt-out*” rıza beyanında kişinin hareketsizliğinden onay verdiği sonucu çıkarılır. İkinci durumda kişi, rıza göstermediği durumda bunun için özel bir çaba gösterecektir. Dolayısıyla ilgilinin hakları açısından daha zayıf bir korumayı öngörmektedir.

AB Veri Koruma Yönergesi’nin 14. maddesi uyarınca pazarlamaya ilişkin olarak “*opt-out*” bir standart belirlemiştir¹³⁴. Elektronik İletişim Yönergesi’nde de doğrudan pazarlamaya yönelik bir hüküm bulunur¹³⁵. Buna göre otomatik arama sistemlerinin, fax makinelerinin ve e-postaların doğrudan pazarlama amacıyla kullanılması ancak ilgilinin önceden izin vermesi ile olanaklıdır. Görüldüğü gibi Veri Koruma Yönergesi’nin tersine burada “*opt-in*” bir standart belirlenmiştir. Yönerge, diğer türdeki pazarlama etkinliklerinde ise Üye Devletleri “*opt-in*” ya da “*opt-out*” rıza koşulu açısından serbest bırakmıştır¹³⁶.

B. RIZA BEYANINDA BULUNMA EHLİYETİ

Üzerinde durulması gereken bir diğer konu, rıza gösterme ehliyetidir. Bir başka anlatımla kimler rıza gösterebilir? Elbette rıza beyanında bulunacak olan işlemenin konusu olan kişidir. Ancak bu noktada bazı özel durumların üzerinde durulması gerekir.

Burada ilk akla gelen çocukların durumudur. Çocukların hukuksal konularda ehliyeti çeşitli devletlerde farklı şekillerde düzenlenmiştir. Konunun hukuksal boyutu yanında sosyal, siyasal yönünün de bulunduğu ve bunların yaklaşımların

¹³³ Ayrıca bkz. Peter CAREY, s. 254 vd.

¹³⁴ Christopher KUNER, s. 309.

¹³⁵ Bkz. Elektronik İletişim Yönergesi, m. 13. Veri Koruma Grubu, 95/46/AT sayılı Yönerge’nin Baş. Par. 30 hükmüne de uygun olarak bu maddede sözü geçen doğrudan pazarlama etkinliklerine her türlü satış promosyonu yanında siyasal organizasyonların ya da yardım kuruluşlarının benzer etkinliklerinin de dahil olduğu yönünde görüşünü açıklamıştır. Bkz. Article 29 Data Protection Working Party, **Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC**, WP 90, 27 Şubat 2004, s. 7.

¹³⁶ Elektronik İletişim Yönergesi, m.13/3. Opt-in ve opt-out rıza çeşitlerinin yarar ve sakıncalarının RFID teknolojisi özelinde değerlendirilmesi için bkz. Gerd WORFLAM, Birgit GAMPL, Peter GABRIEL, **The RFID Roadmap: The Next Steps for Europe**, Springer, Almanya 2008, s. 92-95.

belirlenmesine etki ettiği açıktır. Kişisel verilerinin işlenmesine çocukların rıza gösterebilip gösteremeyeceği de bu kapsamda değerlendirilmelidir.

Çalışmamızın çeşitli yerlerinde belirtildiği üzere kişisel verilerin korunması bireysel özerklik ile yakından ilişkilidir. Kişinin kendisine ilişkin verilerin kullanımına rıza göstermesi de bunun bir uzantısıdır. Buna karşın ebeveynlerin çocuklarının yerine velayeten rıza göstermesi daha çok “*üstün çıkar*” ve “*çocukların korunması*” düşünceleri ile ilişkilidir¹³⁷. O halde çocuğun iradesine mi yoksa veli ya da vasisinin tercihinine mi dayanılacağına karar verilmelidir. Burada hatırdan çıkarılmaması gereken konu, rıza ile korunmak istenenin kişinin yararı olmasıdır. Şüphesiz rıza, bireysel özerklikten yola çıkılarak ilgili kişinin kişi hak ve özgürlüklerinin korunmasına yönelmiştir. Bu durumda çocuklara ilişkin verilerde de korunan, ebeveynlerinin değil çocukların çıkarı olacaktır. Üstelik çocukların korunmasının yetişkinlere göre daha önemli olduğu pek çok alanda kabul edilmektedir¹³⁸.

Çocuklar pek çok haklarını kullanabilmek için yasal bir temsilciye gereksinim duyarlar. Ancak bu, temsilcilerin çocuklar üzerinde kesin bir üstünlükleri bulunduğu anlamına gelmez. Eğer çocuğun verilerinin işlenmesine temsilcisinin rızası ile başlanmışsa, çocuk reşit olduğunda bu rızayı geri alabilmesi gerekir. Bunun yanında işlemenin devam etmesini isterse, bazı durumlarda açık izin de vermesi de beklenebilir. Örneğin, sağlık verilerini içeren bir davada çocuğun verilerinin kullanılmasına temsilcisi rıza göstermişse, çocuk reşit olduğunda veri denetçisi ilgili kişinin açık rızası olup olmadığının saptanmasına özel önem vermelidir. Çünkü bu

¹³⁷ International Working Group on Data Protection in Telecommunications Working Paper, **Childrens' Privacy Online: The Role of Parental Consent**, adopted at the 31st meeting, Auckland (New Zealand), 26-27 Mart 2002, s. 1. Özellikle İnternet ortamındaki bazı unsurların çocuklar ve gençler üzerindeki olası kötü etkilerine karşı, anne-babaların izni ve gözetimi ile bir denge kurulmaya çalışıldığı görülmektedir. Bunun bir örneğini ABD’nde Çocukların Özel Yaşamının Çevrimiçi Ortamda Korunması Yasası’nda (Children’s On-line Privacy Protection Act) görmekteyiz.

¹³⁸ Kişisel verilerin korunması açısından da çocukların durumunun özellikli olması temel olarak, biri statik diğeri dinamik, iki nedenden kaynaklanır. Statik açıdan çocuk henüz fiziksel ve zihinsel olgunluğa erişmemiş kişidir. Bu nedenle korunmaya muhtaçtır. Dinamik açıdan ise çocuk, bir yetişkin olmak üzere hem fiziksel hem de zihinsel açıdan geliştiği bir sürecin içindedir. Gelişimini en iyi şekilde tamamlayabilmesi özel bir dikkati gerektirir. Kişisel verilerin korunması da dahil çocukların haklarına ilişkin uygulamalarda bu iki durumun bir arada değerlendirilmesi gerekir. Bkz. Article 29 Data Protection Working Party, **Opinion 2/2009 on the protection of children’s personal data (General Guidelines and the special case of schools)**, WP 160, 11 Şubat 2009, s. 3.

durumda hassas kişisel veriler söz konusudur. Unutulmamalıdır: veri koruma hakkı, onu kullanan yasal temsilciye değil, doğrudan çocuğa aittir¹³⁹.

O zaman, en azından teorik düzeyde, velinin rızasını olmazsa olmaz bir koşul olarak değerlendirmemek, somut olayda eğer çocuk mantıklı kararı kendisi verebilecek durumdaysa bunu ona bırakmak gerekir. Ancak elbette kararın yalnızca çocuğa bırakılamayacağı durumlarda anne-babası da çocuğun çıkarları için sürece katılmalıdır. Şuna da işaret etmek gerekir: teoride bu saptamaların yapılması, uygulamada bunun kolaylıkla sağlanabileceği anlamına gelmez. Her şeyden önce bütün çocuklar aynı yaşta aynı yeteneklere sahip değildir¹⁴⁰.

Özellikle uygulamada örneğin bir İnternet sitesinin veri denetçisinin çocukların eriştikleri olgunluğu değerlendirip veli ya da vasilerinin iznine gerek olup olmadığını değerlendirmesi olanaksızdır. Bu durumda çocukların kişisel verilerinin toplanması, işlenmesi, daha sonra doğrudan pazarlama gibi farklı amaçlarla kullanılmasında veli ya da vasilerin izninin aranması gerekir. Ancak biraz önce yukarıda belirttiğimiz gerekçeler dolayısıyla, bir çocuğun İnternet üzerinden kişisel verilerine erişim hakkını kullanırken veli ya da vasisinin rızasının gerekli olmadığını söyleyebiliriz¹⁴¹.

Rızanın gerekli olduğu durumlarda çözüm belki yalnızca çocuğunun rızasının alınması değil, temsilcisiyle çocuğun paralel olarak rızalarının alınması şeklinde geliştirilebilir. Eğer çocuk, olgunluk düzeyine erişmişse yalnızca onun rızası da alınabilir. Son ilke, danışılma hakkı olarak belirlenebilir. Buna göre, uyulması zorunlu olmasa da çocukların görüşleri de dikkate alınmalıdır. Örneğin bu danışma

¹³⁹ Article 29 Data Protection Working Party, **Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)**, WP 160, 11 Şubat 2009, s. 5.

¹⁴⁰ International Working Group on Data Protection in Telecommunications Working Paper, **Children's Privacy Online: The Role of Parental Consent**, adopted at the 31st meeting, Auckland (New Zealand), 26-27 Mart 2002, s. 1.

¹⁴¹ International Working Group on Data Protection in Telecommunications Working Paper, **Children's Privacy Online: The Role of Parental Consent**, adopted at the 31st meeting, Auckland (New Zealand), 26-27 Mart 2002, s. 2. Örneğin İngiltere'de 12 yaşını doldurmuş çocuklar verilere ulaşma hakkını kendi başlarına kullanabilmektedirler¹⁴¹. 29. Madde Veri Koruma Grubu, çocuğun verilerine ulaşma hakkını kullanıp kullanamayacağı belirlenirken yalnızca yaşına değil, olgunluk ve özerklik seviyesinin de dikkate alınmasını tavsiye etmektedir. Article 29 Data Protection Working Party, **Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)**, WP 160, 11 Şubat 2009, s. 11.

coğrafi yer belirlemede ya da çocukların görüntülerinin kullanılmasında söz konusu olabilir¹⁴².

AİHM de rızanın verilme anı ve anne-babanın çocuk adına rıza beyanında bulunması konularını değerlendirmiştir¹⁴³. Başvuruya konu olan olayda henüz bir günlük bir bebeğin bulunduğu steril klinikte profesyonel bir fotoğrafçı tarafından görüntülenmesi söz konusudur. Çocuğun anne ve babası bu eylem dolayısıyla şikâyetle bulunmuş ve fotoğrafların negatiflerini istemiş olmalarına karşın hastane yönetiminden ve daha sonra ulusal mercilerden istekleri doğrultusunda bir yanıt alamamıştır. Mahkemeye göre *“Bir kişinin görüntüsü, kişiliğine bağlı niteliklerinden biri olduğuna göre, bunun etkili koruması (...) basitçe eğer yayınlanacaksa ya da yayınlanacağı zaman değil, fotoğraf çekilirken ilgili kişinin izninin alınmasını gerektirir. Aksi takdirde kişiliğin temel bir özelliği üçüncü bir kişinin ellerine bırakılmış olacak ve ilgili kişi görüntüsünün izleyen kullanımları üzerindeki denetimini kaybedecektir”*¹⁴⁴.

Ayrıca kamusal ilgi temelinden hareketle fotoğrafların çekilmesine meşru bir zemin bulmak da olanaklı değildir. Aksine ilgili kişi küçüktür ve görüntüsünü koruma hakkının kullanımı ebeveynlerince denetlenmektedir. Bu nedenle ailesinden önceden izin alınması zorunludur. Buna karşın ilgili kliniğin yönetimi anne-babanın rızasını almamış, ayrıca fotoğrafçının normalde yalnızca doktor ve hemşirelerin girebildiği steril bölümde bulunan çocuğun fotoğrafının çekilmesine izin vermiştir¹⁴⁵. Sonuç olarak AİHM somut olayda 8. maddenin ihlal edildiğine karar vermiştir¹⁴⁶.

Son olarak şuna değinmek gerekir: Amerikan hukukunda verilerin korunması müzakere edilebilir bir *“çıkart”* olarak görülürken, Avrupa’da temel bir hak olarak benimsenmiştir. Bu durum rıza beyanı konusunda da etkilerini gösterir. Bu yaklaşım farklılığı Avrupa’da ilgili kişinin haklarının ihlali sayılacak hareketlere rıza

¹⁴² Article 29 Data Protection Working Party, **Opinion 2/2009 on the protection of children’s personal data (General Guidelines and the special case of schools)**, WP 160, 11 Şubat 2009, s. 6. Ancak bunun yanında başka sorunlar da bulunmaktadır. Örneğin Alman veri koruma hukukuna göre, kişinin rıza gösterebilmesi için medeni hakları kullanma ehliyetine sahip olması yeterlidir. Ayrıca temsilci aracılığıyla verilebilir. Yalnız bu durumda temsilciye yetkinin oldukça açık bir şekilde verilmesi gerekir. Bkz. Peter GOLA, Rudolf SCHOMERUS, s. 178, par. 10.

¹⁴³ Bkz. Reklos ve Davourlis, Yunanistan’a karşı, b.n. 1234/05; k.t. 15 Nisan 2009.

¹⁴⁴ A.g.k., par. 40.

¹⁴⁵ A.g.k. par. 41.

¹⁴⁶ A.g.k., par. 43.

gösterememesi sonucunu getirir¹⁴⁷. ABD’de ise bu gibi sorunların teknoloji tabanlı bazı araçlarla çözülmesine öncelik verilmektedir. Kişisel verilerin korunması için benimsenen P3P¹⁴⁸ ve OPS¹⁴⁹ gibi standartlar da bu bağlamda incelenebilir.

Bu standartlar altında İnternet kullanıcısı ile verileri toplayan hizmet sağlayıcı arasında özel yaşamın gizliliğinin korunması konusunda bir anlaşmaya varılmaktadır. P3P, tarayıcıdaki bir seçim hizmeti ile ilgili kişinin verilerinin hangi amaçlar için işlenmesine izin verdiğini belirlemesine olanak tanır¹⁵⁰. P3P ise, İnternet uygulamalarında rıza ve bilgilerin geleceğini belirleme ilkesinin bulunduğu bir teknoloji ürünüdür. Ancak bu, Avrupa veri koruma sistemindeki “*meşru işleme*”nin koşullarını sağladığı anlamına gelmez. Çünkü veri koruma otoritelerine göre başka ek güvenceler de bulunmalıdır. Tek başına P3P ya da OPS gibi sistemlerin kabul edilmesi kişisel verilerin korunmasına yeterli değildir, bunun yanında yasal yükümlülüklerin düzenlendiği bir çerçeve de bulunmalıdır. Yalnızca bu gibi sistemlere dayanıldığında ilgili kişinin rızası ile meşru işlemenin gerçekleştiği ve veri denetçilerinin bir sorumluluğu kalmadığı yanılgısına düşülebilir¹⁵¹. Bu ise Avrupa veri koruma sisteminin temel mantığı ile uyuşmayacaktır.

¹⁴⁷ Lucas BERGKAMP, Jan DHONT, s. 78.

¹⁴⁸ Özel Yaşamın Gizliliği Tercihleri Düzlemi (Platform for Privacy Preferences-P3P), web sitelerinde yer alan gizlilik politikalarını ortak bir dilde algılamaya yarayan standartlar bütünüdür. Ayrıca bkz. <http://www.w3.org/P3P/>.

¹⁴⁹ Açık Profilleme Standartı (Open Profiling Standard-OPS) ise kullanıcıların web siteleri ile kişisel bilgilerini nasıl paylaşacaklarının denetimini sağlayacak bir standart önerisidir.

¹⁵⁰ Lucas BERGKAMP, Jan DHONT, s. 78.

¹⁵¹ Bkz. Working Party on the Protection of the Individuals with regard to the processing of Personal Data, Opinion 1/98 **Platform for Privacy Preferences (P3P) and the Open Profiling Standard(OPS)**, WP 11, 16 Haziran 1998. Başka bazı çalışmalarda da P3P’nin yararları yanında dikkatle izlenmesi gereken yönleri de bulunduğu dikkat çekilmektedir. Örneğin, bkz. International Working Group on Data Protection in Telecommunications, **Common Position on Essentials for privacy-enhancing Technologies (e.g. P3P) on the World Wide Web**, adopted at the 23rd meeting in Hong Kong SAR, China, 15 Nisan 1998.

V. ÖZEL KATEGORİDEKİ (HASSAS) KİŞİSEL VERİLERİN NİTELİKLİ KORUNMASI

A. KAPSAMI

Bu ilke, ilgili kişi açısından “*hassas*” sayılan bazı veri türlerinin işlenmesini diğerlerine göre daha sıkı bir denetim altına alma düşüncesine dayanır¹⁵². Pek çok uluslararası ve ulusal metinde hassas verilerin özel olarak korunması yaklaşımı benimsenmiştir. AB Yönergesi¹⁵³, AK Sözleşmesi¹⁵⁴, BM Rehber İlkeleri¹⁵⁵ hassas verilere özel koruma öngörürken, OECD Rehber İlkeleri¹⁵⁶ ve APEC Çerçeve Belgesi’nde¹⁵⁷ belirli türdeki verilere yönelik özel bir koruma geliştirilmemiştir.

AB Yönergesi’nin 8. maddesine göre özel kategorideki kişisel verilerin işlenmesi kural olarak yasaktır. Bunlar ilgili kişinin,

- ırksal veya etnik kökenini,
- siyasal görüşünü,
- dinsel ya da felsefi inancını,
- sendika üyeliğini,

- sağlık ya da cinsel yaşamını¹⁵⁸ belirli eden verilerdir. Bunun yanında kişilerin ceza mahkumiyetine ilişkin veriler de her durumda korumadan yararlanırken, idari ve adli mahkumiyetlere ilişkin verilerin bu kapsamda sayılıp

¹⁵² Lee A. BYGRAVE, **Data Protection Law**, s. 68. Her ne kadar AK Sözleşmesi, AB Yönergesi gibi metinlerde bu ilke “*özel kategorideki veriler*” başlığı altında düzenlenmişse de, bu veri türlerini nitellemek için daha sıklıkla “*hassas veriler*” deyimini kullanılmaktadır. Deyim Almanca’da “*sensibel Daten*”, İngilizce “*sensitive data*” kelimelerinin Türkçe karşılığıdır.

¹⁵³ AB Yönergesi m. 8.

¹⁵⁴ AK Sözleşmesi m. 6.

¹⁵⁵ BM Rehber İlkeleri 5. İlke.

¹⁵⁶ OECD Rehber İlkeleri’ni hazırlayan uzman heyet, çeşitli hassaslık ölçütlerini değerlendirmiştir. Buna karşın OECD Rehber İlkelerinde hassas kişisel veri kategorisinin belirlenmemesinin nedeni, heyetin evrensel düzeyde “*hassas*” olarak nitelendirilebilecek bir veri kategorisi bulunmadığı yönündeki görüşüdür. “Guidelines’ Explanatory Memorandum”, **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**, 27 Şubat 2002, s.40, par. 51.

¹⁵⁷ APEC Çerçeve Belgesinde hassas kişisel veriler için özel bir koruma getirilmemekle birlikte veri güvenliğine ilişkin önlemleri düzenleyen hükümde (par.22), alınan önlemlerin, diğerleri yanında, bilginin hassaslığı ile de orantılı olması gerektiği belirtilmiştir. Bu yaklaşım aslında APEC Çerçeve Belgesinde zarar ile koruma arasında çeşitli yerlerde kurulmaya çalışılan denge ile de uyumludur.

¹⁵⁸ İlk beş kategori 8. maddenin 1. fıkrasında hüküm altına alınmış ve bunların işlenmesinin kural olarak yasak olduğu belirlenmiştir. Bu kuralın istisnaları ise Yönerge’nin 8/2 hükmünde yer alır ve bu hüküm aşağıda değerlendirilecektir.

sayılmayacağı üye devletin takdirine bırakılmıştır¹⁵⁹. Çeşitli metinlerde bu sayımda farklılıklar dikkat çekse de genel olarak bu konulara ilişkin bilgilerin hassas veriler olarak kabul edildiği görülür¹⁶⁰.

Burada öncelikle sayılan veri kategorileri ile ilişkili her türlü bilginin bu kapsamda değerlendirilip değerlendirilmeyeceği belirlenmelidir. Nitekim bazı durumlarda hassas verilerin içine dâhil olan veri türlerinin özel bir koruma altına alınmadığı görülebilir. Örneğin; gözlüklü bir insanın resmi o kişinin sağlık durumuna ilişkin bir bilgi içermektedir, ancak bu, özel koruma gerektirdiği anlamına gelecek midir? Kişilerin adları açısından benzer bir soru yöneltilebilir: bir kişinin dinsel inancını yansıtan bir adının olması, bunun geçtiği her türlü bilgiyi hassas nitelikte kılar mı?

Bir kişinin gözlüklü fotoğrafı ya da dini inancını yansıtan adı ancak herhangi bir değerlendirme söz konusu olduğunda (görme bozukluğu olan kişiye ya da İslam inancına sahip tüketicilere yönelik ilanlar gibi) bu kapsamda değerlendirilebilir. O halde öncelikle somut olayın özellikleri dikkate alınmalıdır. Nitekim benzer olaylar, farklı sonuçları getirebilir. Örneğin siyasal bir toplantıya katılma üzerindeki söylemlerin ne oranda siyasal nitelik taşıyacağı o toplantının anlamından çıkarılabilir. Bu kapsamda herhangi bir partinin taraftarı olmayan bir kişinin, Başbakanın seçim kampanyası kapsamında düzenlediği bir toplantıya katılması saf bir bilgi edinme eylemi iken bir siyasal partinin düzenlediği protesto yürüyüşüne katılması bu şekilde değerlendirilemez¹⁶¹.

¹⁵⁹ Kişinin ceza mahkûmiyetine ilişkin bilgilerinin özel olarak korunması ilkesi Yönerge'nin 8/5 hükmünde şu şekilde düzenlenmiştir: *"Suçlara, ceza mahkûmiyetine ya da güvenlik önlemlerine ilişkin verilerin işlenmesi yalnızca resmi mercinin denetimi altında veya eğer uygun, özgül(spesifik) koruma önlemleri, bu uygun koruma önlemlerini sağlayan Üye Devlet tarafından ulusal hükümler uyarınca tanımlanan derogasyonlara tabi olmaları şartıyla verilmişse gerçekleştirilebilir. Ancak ceza mahkûmiyetlerinin tam kaydı yalnızca resmi mercinin gözetimi altında tutulabilir. Üye Devletle, idari yaptırımlara ya da adli davalardaki hükümlere ilişkin verilerin de resmi otoritenin denetimi altında işlenebileceğine karar verebilirler"*.

¹⁶⁰ Ancak AB Yönergesi ile AK Sözleşmesi arasında bu noktada bazı farklılıklar bulunduğu dikkat çekmek gerekir. AK Sözleşmesi'nde, AB Yönergesi'nin aksine kişinin sendika üyeliği hassas veriler arasında sayılmamıştır. Bu, iki metin arasında hassas kişisel verilerin kapsamına ilişkin en önemli farklılıktır. Belirtmek gerekir ki AK Sözleşmesi'nin sendika üyeliğini kapsamdan dışlayan yaklaşımına karşın, BM Rehber İlkeleri'nde ilgili kişinin yalnızca sendika üyeliği değil, her türlü dernek üyelikleri hassas veri kategorileri içerisinde sayılmıştır. Bkz. BM Rehber İlkeleri, 5. İlke. Bunun yanında kişinin etnik kökenine ilişkin veriler de Sözleşme'de bu kategori içerisinde yer almamaktadır. Ancak kişinin ırksal kökenine ilişkin verilerin korunacağından hareketle yapılacak bir yorum ile bu kapsamda değerlendirilebilir. Bu konuya ilişkin olarak ayrıca bkz. aşağı. Dördüncü Bölüm, Tablo 4.2.

¹⁶¹ Peter GOLA, Rudolf SCHOMERUS, s. 132, par. 56a.

Ulusal hukuk sistemleri açısından düşündüğümüzde bu noktada elbette önemli olan veri koruma otoritesinin ve nihai olarak da mahkemenin yorumudur. Yorum geliştirilirken bir bilginin yalnızca belirlenen hassas veri kategorisinde yer almasının mı yoksa bilginin öz olarak hassas nitelikte olmasının mı gerektiği arasında bir tercih yapılmalıdır. En sağlıklı yöntem, her ikisini de birlikte dikkate almak ve makul bir sonuca ulaşmak olacaktır. Yukarıda da işarete edilen, kişinin dinsel inançlarını belirli eden isimlerin doğrudan bu içeriğin kullanıldığı zamanlarda hassas sayılırken, yalnızca bir isim veri tabanında yer aldığında hassas sayılmaması bunun en açık örneğini oluşturur¹⁶².

Hassas kişisel verilerin korunmasına ilişkin sorunların özellikle İnternet kullanımının ve çevrim-içi bilgi paylaşımının artmasıyla daha da büyük önem kazandığını belirtmek gerekir¹⁶³. Bu kapsamda örneğin “tıklama akışlı veriler”in (clickstream data) hassas kişisel veriler kapsamında değerlendirilip değerlendirilemeyeceği düşünülebilir. O zaman öncelikle tıklama akışlı verilerin hassas kişisel verileri içerdiği durumları düşünmemiz gerekir. Bu türdeki veriler, bir İnternet sitesini ziyaret eden bir kişinin profilinin oluşturulmasını sağlayabilir. Ancak bunun içerisine hassas bazı verilerin girip giremeyeceği tartışmaya açıktır. Örneğin bir kişinin düzenli olarak bir kilisenin web sayfasını ziyaret ediyor olması, kesin bir şekilde onun dinsel inançlarına ilişkin bir veri oluşturmaz. Nitekim bu kişinin

¹⁶² Peter CAREY, **Data Protection**, s. 87. Nitekim Birleşik Krallık'ta görülen Naomi Campbell davasında da (*Campbell v Mirror Group Newspapers [2002] EWHC 299*) yargıç bu yaklaşımı benimsemiştir. Buna göre siyahı bir manken olan Bayan Campbell'in fotoğrafları doğal olarak kendisinin etnik kökenine ilişkin hassas kişisel veriler içermektedir, ancak bu fotoğrafların yayınlanma amacı ile ilişkili değildir. Bkz. **a.g.e.**, s.87. Bunun yanında belirtilen davada haberin içeriğinde yer alan ve Bayan Campbell'in fiziksel ve ruhsal sağlığına ilişkin olarak gördüğü tedaviye ilişkin yapılan haberde hassas verilerin yer aldığı kabul edilmiştir. Bu konuya ilişkin olarak bkz. Joshua ROZENBERG, **Privacy and the Press**, Oxford University Press, ABD 2005, s. 66-67. Benzer yaklaşımları başka bazı ulusal hukuk sistemlerinde de görmek olanaklıdır. Örneğin İsveç'te ilgili kurum, kişinin cilt rengi, giyim tarzı gibi ırksal ya da etnik kökenini belirli kılan görüntülerin hassas kişisel veri kategorisinde olup olmadığı değerlendirirken, yayının amacını ve somut olayın kendine özgü koşullarını dikkate almaktadır. Bkz. Mads ANDENAS, Stefan ZLEPTNIG, “Surveillance and Data Protection: Regulatory Approaches in the EU and Member States”, **EBLR**, Y.2003, s. 777. (765-813) Ayrıntılı bilgi için bkz. British Institute of International and Comparative Law, **The Implementation of Directive 95/46/EC to the Processing of Sound and Image Data**, Londra 2003, http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/biiclstudy-soundimage_en.pdf.

¹⁶³ Joel R. REIDENBERG, Paul M. SCHWARTZ, **Data Protection Law and On-line Services: Regulatory Responses**, s. 9-10. Çevrim-içi profillerin oluşturulmasında hassas kişisel verilerin korunmasına ilişkin Belçika, Fransa, Almanya ve Birleşik Krallık uygulamalarına ilişkin açıklama ve değerlendirmeler için bkz. **a.g.e.**, s. 83 vd.

ziyaretleri yalnızca araştırma amaçlı da olabilir. Buna karşın, AAD'nın *Lindqvist* kararında işaret ettiği hassas kişisel veri kategorilerinin geniş yorumlanması gerekliliğini de hatırdan çıkarmamak gerekir¹⁶⁴. Bu durumda veri öznesinin ziyaret ettiği web siteleri aracılığıyla oluşturulan profilinde hassas verilerin bulunuyor olması bu kapsamda değerlendirileceği anlamına gelebilir¹⁶⁵.

B. HASSAS OLAN VE HASSAS OLMAYAN VERİLERİN AYRIMI

Hassas kişisel verilerin bazı ek güvencelerle korunmasındaki temel mantık, bu türdeki verilerin, ayrımcılık başta olmak üzere, diğer verilere göre ilgili kişi açısından daha ciddi zararlar ortaya çıkarabilmesidir. Ancak bu görüşün genel kabul gördüğünü söylemek güçtür. Örneğin Federal Almanya Anayasa Mahkemesi, 1983 yılında verdiği Nüfus Kararı'nda bu şekilde bir ayırım yapılamayacağını karara bağlamıştır. Mahkemeye göre kişisel verilerin tamamı önemlidir. Bu nedenle “önemliler” ve “daha az önemliler” gibi bir ayrıma gidilmemelidir. Başlangıçta tehlike taşımayan, basit bir bilgi, otomatik işleme sistemleri ile oldukça hassas bir nitelik kazanabilir¹⁶⁶. Benzer şekilde, Avusturya, Almanya, Birleşik Krallık gibi bazı Avrupa ülkelerinin önceki sistemlerinde bu yaklaşımı benimsedikleri bilinmektedir¹⁶⁷.

Nitekim öğretilerde kimi yazarlar bu görüşü paylaşmaktadır. Buna göre hangi verilerin korunmaya değer olup olmadığı konusunda ayırımda bulunmak adil değildir.

¹⁶⁴ AAD, AB Yönergesi'nin amaçları çerçevesinde yaptığı değerlendirmede 8/1 hükmünün geniş bir şekilde yorumlanması gerektiğine ve bu kapsamda örneğin sağlık verilerinin, kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgiyi içerdiğine işaret etmiştir. Bu nedenle, karara konu olan olayda geçen, kişinin ayağının incinmesine ilişkin bilgi de sağlık verisidir ve hassas veri kategorileri içerisinde değerlendirilecektir. Bkz. *Case C-101/01, Bodil Lindqvist (ECJ) [2003]*, par. 49-51. Ayrıca bkz. Rebecca WONG, “Data Protection Online: Alternative Approaches to Sensitive Data”, C.2, S. 1, Y. 2007, <http://www.jiclt.com>, s. 10-12.

¹⁶⁵ Daniel B. GARRIE, Rebecca WONG, “The Future of Consumer Web Data: A European/US Perspective”, *International Journal of Law and Information Technology*, Y. 2006, C. 15, S. 2, s. 145-146.

¹⁶⁶ BVerfGE 65, 1, 45.

¹⁶⁷ Lee A. BYGRAVE, *Data Protection Law*, s. 69. AB Yönergesi'nin 8. maddesi 2000 yılında çıkarılan Avusturya Veri Koruma Yasasının da 9. maddesine yansımıştır. Buna göre gerçek kişilerin etnik kökenleri, sendikal faaliyetleri, sağlık durumları ve cinsel yaşamlarına ilişkin veriler bu hassas verilerin kapsamında yer almaktadır. Nitekim 1978 Federal Almanya Veri Koruma Yasası'nda bazı veri çeşitlerinin özel hükümlerle korunması öngörülmemiştir. Buna karşın, AB Yönergesi'ne uyum zorunluluğu dolayısıyla bu gelenek yıkılmıştır. Viktor MAYER-SCHÖNBERGER, Ernst O. BRANDL, s. 33; Peter GOLA, Rudolf SCHOMERUS, s. 131, par. 56.

Bir verinin korunmaya değer olup olmadığının olayın özel şartlarından çıkarılabildiğini düşünürsek ilk bakışta son derece önemsiz gibi görülen bazı verilerin de çok ciddi sorunlara neden olabileceğini kolaylıkla fark edebiliriz. Her verinin olayın özel koşulları içinde değerlendirilmesi gerektiğinden dolayı da belirli bazı verilere ayrıcalık tanınmaması gerekir¹⁶⁸.

Ayrıca böylesine bir ayırım, başka bazı sorunları da getirir. Örneğin bazı veri kategorilerine özel koruma öngörülmesi diğerlerinin tam anlamıyla korunmadığını mı ortaya koymaktadır? Eğer bu soruya olumlu yanıt verilirse “*hassas*” olarak nitelendirilmeyen kişisel verilerin düşük oranda korunduğunu ve bunlara yönelen bazı müdahalelere izin verildiğini kabul etmek gerekecektir.

İçinde bulunduğumuz bilgi çağında pek çok alanda, hatta belki hemen hemen her alanda, verilere gereksinim duyulduğu açıktır. O halde verilerin işlenmesinden doğacak zarar ile yarar arasında bir dengenin kurulması gerekir. Nitekim çeşitli yerlerde belirttiğimiz üzere, kişisel verilerin korunması hukukunun temeli de bu düşüncedir. Bu saptamadan hareketle, kişisel verilerin mutlak olarak korunmasından söz edilemez. Dengenin sağlanabilmesi, yararın derecesi ve tehlikenin şiddetini de dikkate almayı gerektirdiğinden, bazı verilerin diğerlerine göre daha yüksek oranda korunmasını yadırgamamak gerekir.

Ancak sorun bu noktada bitmemektedir. Bazı veri kategorilerinin özel olarak korunması gerekliliğini kabul ettiğimizde başka bazı soruların da yanıtlanması gerekecektir. Birincisi AB Veri Koruma Yönergesi’nde ve bu ayrımı benimseyen diğer metinlerde hassas kişisel veriler, sınırlı sayım esasına göre belirlenmiştir. Yani hassas kişisel veri kategorilerini genişletmek olanaklı değildir. Yukarıda işaret edildiği gibi çeşitli metinlerde belirlenen özel veri kategorileri kişinin ırksal veya etnik kökeni, siyasal görüşü, dinsel ya da felsefi inancı, sağlık bilgileri, adli kayıtları gibi çeşitli bilgileri kapsamaktadır. Ancak bu bilgi kategorileri nitelikleri dolayısıyla farklı özelliktedir. Bir başka anlatımla bu bilgilerin tamamına aynı rejimi uygulamanın çeşitli sakıncaları bulunur. Nitekim aşağıda inceleneceği üzere hassas kişisel verilerin işlenmesi kural olarak yasaktır, ancak bazı istisnaları da

¹⁶⁸ Viktor MAYER-SCHÖNBERGER, Ernst O. BRANDL, s. 33. Ayrıca bkz. Spiros SIMITIS, Revisiting Sensitive Data, 1999, http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/reports%20and%20studies%20by%20experts/1Experts%20Studies.asp#TopOfPage, s. 1-11.

bulunmaktadır. Oysa kişinin dinsel inancı, etnik kökeni gibi bilgi gruplarının işlenme yasağına hangi durumlarda istisna getirilebileceği ayrıca değerlendirilmelidir.

Bir an için hukuksal düzenlemelerden bağımsız olarak, kişinin dinsel inancı, ırksal kökeni gibi bilgilerin belirli ya da belirlenebilir bir kişi ile ilişkili olarak tutulmasının ve işlenmesinin bireysel, sosyal ya da siyasal düzeyde ne gibi amaçlara veya yararlar hizmet edebileceğini düşünelim. Bir kişinin dinsel inancı ya da inançsızlığı onun maneviyatına ilişkindir. Bu bilgiyi bir ya da birden fazla kişiyle ya da daha geniş kitlelerle paylaşmak yalnızca onun özgür iradesinin bir yansıması olarak ortaya çıkabilir. Bu durumda kişinin paylaşmama yönündeki iradesine karşın bu bilgilerin işlenmesinin sağlayacağı yararın ne olacağı sorulmalıdır.

Burada belki de ilk akla gelen idarenin yurttaşlarının dinsel gereksinimlerini karşılama yükümlülüğüdür. Örneğin idarenin ibadethane yapma görevini yerine getirirken ülkedeki dinsel çeşitliliği ve bunların oranlarını dikkate alması gerekebilir. Ancak bunlar istatistiksel rakamlarla ulaşılabilecek bilgilerdir. Bir başka ifade ile kimin hangi dine inandığının değil, yaklaşık olarak ne kadar kişinin hangi dine inandığının bilinmesi yeterlidir¹⁶⁹.

Demokratik bir devlet yapılanmasının kişinin dinsel inançları gibi konular karşısında “*gözlerinin bağlı*” olması gerekir. Aksi durumda bireyler örtülü ayrımcılık tehlikesi ile karşı karşıya kalabilir. Bu yaklaşım amaç için gerekli olandan fazla verinin tutulmaması ilkesi ile de bağdaşan sonuçlar yaratır. Sorun o kadar önemlidir ki kanımızca bu türdeki bilgilerin anonimleştirilmiş olarak tutulmasının bile kimi zaman sorun yaratabilir. Nitekim grup profilleri de kimi zaman tehlikeli olabilir. Belirli bir sokakta oturan ya da belirli bir gruba dahil olan kişilerin dinsel inançlarına ya da etnik kökenlerine ilişkin belirleme yapılması buna örnektir.

Bütün bunlara rağmen dinsel tercihlerin kişisel veri niteliğinde tutulmasının sağlayabileceği yararlar ise oldukça sınırlıdır. Kimsesiz bir kişinin ani ölümü durumunda bu kişinin cenaze işlemlerinin dinsel tercihlerine uygun bir şekilde gerçekleştirilebilmesi için bu bilgilere gereksinim duyulabilir. Ancak açıktır ki bu oldukça sınırlı bir alana işaret etmektedir.

¹⁶⁹ Benzer bir durum özel sektör açısından da söz konusu olabilir. Örneğin, yurtdışında bir ülkeye ilk kez ihracat yapacak bir gıda firması, o ülkedeki dinsel dağılıma ilişkin bilgilere ihtiyaç duyabilir. Bu, hem pazarlama yöntemleri, hem de sonuçtaki satış grafiği açısından yaşamsal önemde olabilir. Ancak bu konuda yapılacak pazar araştırmalarında belirtilen türdeki bilgilerin anonim tutulması halinde de beklenen yararın sağlanabileceği unutulmamalıdır.

Benzer bir durum, kişinin ırksal veya etnik kökenine ilişkin olarak da geçerlidir. Eşitlik, demokratik bir hukuk devletinin önemli bileşenidir. Bu durumda hangi ırksal veya etnik kökenden gelirse gelsin yasa önünde herkesin eşit olması, eşit hizmet alması gerekir. Bu durumda, yine kişinin istemesi durumunda bu bilgileri özgürce paylaşabilme olanağının gerekliliğini bir yana koyarsak, idarenin planlama görevi açısından bu bilgilerin bir öneminin bulunmaması gerekir. Aynı şekilde kişi, siyasal görüşünü de bir siyasal partiye üye olmak gibi çeşitli şekillerde açıklayabilir. Ancak buna ilişkin kayıtların tutulmasının idarenin eylemleri için bir yararı bulunmayacaktır. Nitekim kapalı oy, açık sayım döküm esası demokratik siyasal sistemlerde seçimlerin gerektiği gibi yürüyebilmesi için en önemli bileşenlerden biridir ve yine aynı düşünceye dayanır.

O halde kişilerin etnik veya ırksal kökenine, siyasal görüşüne, dinsel ve felsefi inancına ilişkin bilgilerin kişisel veri niteliğinde tutulması ve işlenmesinin yararlarının oldukça sınırlı olduğu söylenebilir. Oysa kişinin sağlık verileri, adli, idari sicilleri açısından durum biraz daha farklıdır.

Nitekim sağlık verilerinin kişi ile ilişkili olarak tutulmasının hasta açısından da çok çeşitli yararları olacaktır. Hekimler doğru müdahalelerde bulunabilmek için çoğu zaman hastalarının tıbbi geçmişlerine ilişkin bilgilere gereksinim duyar. Bunun yanında tıbbi araştırmalar için de kişisel veriler gerekli olabilir¹⁷⁰. Ancak diğer taraftan tıbbi bilgiler oldukça kişiseldir. İnsanların kendilerine ait tıbbi bilgileri gizli tutma hakları vardır. Bu bilgiler dolayısıyla kişilerin tehdide maruz kalabilecekleri, eşleri tarafından terk edilebilecekleri, işlerinden kovulabilecekleri düşünüldüğünde bunların başkalarının eline geçmesinin ne kadar tehlikeli olduğu kolaylıkla fark edilebilir¹⁷¹.

Bunun yanında ilgili kişinin sağlık verilerinin yeterli düzeyde korunmadığına ilişkin şüpheye düşmesi, sağlık hizmetlerinden yararlanmaktan çekinmesine de neden olabilir. Bunun sonuçları ise hem bireysel, hem de toplumsal düzeyde oldukça ağır

¹⁷⁰ Hantal ve katı kişisel verilerin korunması hukuku kurallarının tıbbi araştırmaların önünde bir engel oluşturduğu yönünde görüşler de bulunmaktadır. Tıbbi araştırmalar ve kişisel verilerin korunmasına ilişkin, araştırmacılar tarafından kaleme alınmış, bir değerlendirme için bkz. **Personal Data for Public Good: using health information in medical research**, haz. The Academy of Medical Sciences, Ocak 2006.

¹⁷¹ Bruce SCHNEIER, s.66. Ayrıca unutulmamalıdır: tıbbi sırrın açıklanması yalnızca hukuksal değil, aynı zamanda bir tıp etiği sorunudur. Hasta-hekim arasındaki ilişkinin mahremiyeti Hipokrat yemininde de yer almaktadır. Bkz. Sultan ÜZELTÜRK, s.112.

olacaktır. Nitekim AİHM de Z. Finlandiya'ya karşı kararında¹⁷² bu tehlikeye işaret etmiştir. Mahkeme'ye göre¹⁷³:

“Tıbbi verilerin gizliliğine saygı göstermek, AİHS'ne taraf olan bütün Sözleşmecî devletlerin yasal sistemlerinin temel prensibidir. Sadece hastanın özel hayatına saygı göstermek değil, hastanın tıp mesleğine ve genel olarak sağlık hizmetlerine duyduğu güveni de korumak şarttır. Böyle bir koruma olmazsa, tıbbi yardıma ihtiyacı olanlar doğru tedavi görmek için ve hatta tıbbi yardım almak için gerekli olan kişisel veya mahrem bilgileri açıklamaktan cayabilir; bu durum da hem kendi sağlıklarını, hem de bulaşıcı hastalıklar söz konusu olduğunda toplum sağlığını tehlikeye atar”.

AİHM'ne başvuru konusu olan olay, HIV enfeksiyonu ile ilgilidir. Mahkeme, bulaşıcı niteliği olan bu enfeksiyonla ilgili verilerin gizliliğinin korunmasının özellikle önemli olduğuna işaret etmiştir. Mahkeme'ye göre bu tür bilgilerin açıklanması, kişinin özel ve aile yaşamının yanında sosyal durumunu ve iş durumunu da ciddi oranda etkileyebilir, bunun sonucunda da adının lekelenmesi ve toplumdan dışlanması riski ortaya çıkabilir. Bu ise ilgili kişiye tanı konmasını ve onun tedavi edilmesini engelleyebilir ve salgını önleme çabalarına zarar verebilir. Bu nedenle, yapılan müdahalenin meşru amaçla orantılı olup olmadığı belirlenirken, bu tür bilgilerin gizliliğinin korunması terazide ağırlıklı taraf olmalıdır. Mahkeme'ye göre bu tür müdahaleler, önemli bir kamu yararı olmadığı durumlarda, AİHS 8. madde ile uyumlu olamaz¹⁷⁴.

Ceza hukukundaki kuralların uygulanabilmesi için kişilerin adli sicillerinin tutulması da sağlık verilerine benzer şekilde değerlendirilebilir. Ancak bu bilgiler kişilerin sosyal yaşamları ve ekonomik durumları açısından ciddi sonuçlara neden olabilecek önemli bilgilerdir. Bu nedenle belirtilen veri kategorileri için özellikli bir korumanın öngörülmesi şaşırtıcı değildir. Burada bizim dikkat çekmek istediğimiz, birbirinin peşi sıra sayılmış bu veri kategorilerinin niteliklerinin kendi içinde farklılaşabileceğidir.

¹⁷² Z, Finlandiya'ya karşı, b.n. 22009/93, k.t. 25 Şubat 1997.

¹⁷³ A.g.k., par. 95. Çeviri şu kaynaktan alınmıştır: Gilles DUTERTRE, **Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler**, Avrupa Konseyi Yayınları, Ankara 2007, s. 310-312.

¹⁷⁴ A.g.k., par. 96.

Son olarak belirtmek gerekir ki AİHM de kişisel verilerin arasında, neden olabileceği zararın derecesine göre bir ayırım yapılmasını makul görmektedir. Nitekim Mahkeme, *S. ve Marper Birleşik Krallık'a karşı* kararında¹⁷⁵ kişisel verilerin önem derecesine ilişkin ayırımı kabul etmiştir. Mahkemeye göre hücre örnekleri, DNA profili ve parmak izi belirli ya da belirlenebilir bir kişi ile ilişkilendirildiğinde tartışmasız bir şekilde kişisel veridir, ancak aralarındaki nitelik farkı dolayısıyla hücre örnekleri ve DNA profili, ile parmak izi kayıtlarını ayrı ayrı değerlendirmek gerekir¹⁷⁶. Hücre örnekleri kişinin sağlığına ilişkin oldukça hassas bilgileri içerirken, DNA profili kişinin genetik bağlarını ve etnik kökenini ortaya koyabilir. Oysa parmak izi kayıtlarının böylesine bir etkisi bulunmamaktadır. Bu nedenle AİHM'ne göre ilgili kişinin hücre örneklerinin ve DNA profilinin bir veri bankasında tutulmasının sonuçları, parmak izi kayıtlarının tutulmasına göre çok daha ağırdır¹⁷⁷.

Benzer bir tartışma biyometrik yöntemlerin kullanımı açısından da söz konusudur. Bu bağlamda kimi yazarlar, biyometrik yöntemlerin aralarında herhangi bir ayırım yapılmadan değerlendirilmelerinin yanlış olacağı görüşündedir. Buna göre, örneğin iş yerinde ses tanıma ve yüz tanıma teknolojilerinin kullanılmasının yaratacağı sorunlar, parmak izi ve DNA kayıtlarının tutulmasından farklı değerlendirilmelidir. Çünkü burada, kişinin çehre görüntüsü gibi, herkes tarafından bilinen, görünen, kamuya açık unsurlarının, iş sözleşmesi çerçevesinde kayıt altına alınması söz konudur¹⁷⁸. Bu nedenle kişinin parmak izi kaydı ile karşılaştırıldığında özel yaşamına daha sınırlı bir müdahalenin söz konusu olduğu düşünülebilir.

Bu konuda bir saptamada bulunurken öncelikle somut olayın koşulları dikkate alınmalıdır. Yukarıda da işaret edildiği gibi ilk aşamada oldukça önemsiz gibi görünen bir bilgi, bazı koşulların altında ilgili kişi açısından yaşamsal öneme kavuşabilir. Bununla birlikte bazı veri türlerinin nitelikleri dolayısıyla özel koruma gerektirdiği de kabul edilmelidir. Bu gereklilik birkaç nedenden kaynaklanır.

Kanaatimizce kişisel verileri hassaslık derecesine göre özel bir korumaya tabi tutmak yerindedir. Ancak bu kapsama nelerin dahil olacağını belirlemek oldukça

¹⁷⁵ *S. ve Marper Birleşik Krallık'a karşı*, b.n. 30562/04 ve 30566/04, k.t. 4 Aralık 2008.

¹⁷⁶ **A.g.k.**, par. 69.

¹⁷⁷ **A.g.k.**, par. 70 vd.

¹⁷⁸ Cüneyd ER, **Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı**, İstanbul 2005 (yayımlanmamış yüksek lisans tezi), s. 115 vd.'dan (aynen) aktaran; Leyla KESER BERBER, Murat LOSTAR, **Bilişimde Biyometrik Yöntemler**, Yetkin, Ankara 2006, s. 105-106.

güçtür. AB Yönergesi'nde ya da hassas kişisel verilere nitelikli koruma öngören diğer ulusal ya da uluslararası metinlerde belirli veri grupları yer almaktadır. Kişinin ırksal, etnik kökeni, dinsel, felsefi inançları, siyasal görüşleri gibi kategorilerin bu kapsamda yer almasında, yukarıda açıkladığımız gerekçelerden ötürü, şaşılacak bir yan bulunmamaktadır. Sağlık verilerinin, adli, idari sicil bilgilerinin önemi de yadsınamaz. Ancak bu verilerle hemen hemen aynı nitelikteki başka bilgilerin kapsam dışında tutulması ayrımın nedenlerini anlaşılamaz kılmakta ve hassas verilerin özel olarak korunması ile amaçlanan hedefin gerçekleştirilebilirliğine şüphe düşürmektedir. Nitekim bu durum, Yönerge'nin kimi çevrelerce eleştirilmesine de neden olmaktadır.

Bu eleştirilere göre, belirtilen durum Yönerge'deki kişisel veri kavramı ile gerçek zarar arasındaki bağın belirsizliğinin bir kanıtıdır. Örneğin finansal bilgiler ya da yer verileri bu kategoriler içerisinde sayılmadığından özel korumadan yararlanamayacaktır. Oysa belirtilen türdeki verilerin işlenmesinin oldukça ciddi sonuçlar yaratabileceğine ve öneminin gün geçtikçe arttığına çeşitli kaynaklarda işaret edildiği görülmektedir. Kişinin bulunduğu yer bilgisi bir örnek olarak incelenebilir. Bu türdeki verilerin işlenmesi yalnız kişiliğin değişik görünümelerini açığa çıkararak (hassas kişisel veri kategorileri için söz konusu olduğu gibi) ayrımcılık tehlikesini berberinde getirmemekte (ilgili kişinin kumarhanede, içkili mekanda, şehrin ayrılmış bölgelerinde bulunması gibi), ayrıca, bu bilgilerin adam kaçırmaya, soygun gibi cezai etkinliklerde kullanılması durumunda, güvenlik sorunlarını da ortaya çıkarabileceği unutulmamalıdır¹⁷⁹.

¹⁷⁹ Bkz. Yves POULLET, Sophie LOUVEAUX, María Verónica Pérez ASINARI, "Data Protection and Privacy in Global Networks: A European Approach", Meda Conference, Atina, 25 Nisan 2001, **The EDI Law Review**, Y. 2001, S.8, s. 157. Bu konuya ilişkin olarak ayrıca bkz. Roger CLARKE, "Person Location and Person Tracking-Technologies, Risks and Policy Implications", **Information Technology and People**, Y. 2001, C. 14, S. 2, s. 206-231. Kişinin yer bilgilerine kişisel verilerin korunmasına ilişkin bazı değerlendirmelerde daha az önem atfedildiği de görülmektedir. Federal Almanya Anayasa Mahkemesi önüne gelen bir olayda, "*küresel yer belirleme sistemlerinin*"(global positioning systems-GPS) polis tarafından kullanımının Anayasa'ya aykırı olmadığına karar vermiştir. Bkz. BverfG, 2 BvR 581/01, 12 Nisan 2005. Mahkeme bu kararında, GPS ile izlemenin şüphelinin kişilik hakları üzerinde bir etkisi bulunmasına karşın, bu ihlalin insan onurunu ve özel yaşamın gizliliği hakkının özünü zedeleyecek düzeyde olmadığına karar vermiştir. Bkz. **a.g.k.** par. 56. Mahkemenin buradaki değerlendirmesi, diğerlerinin yanında, GPS'in kapalı mekanlarda ve kalabalık ortamlarda tam bir etkinlik gösterememesine dayanmaktadır. Bkz. **a.g.k.** par. 53. Bu nedenle GPS ile izlemenin örneğin kişinin evinde ya da kitle iletişim araçlarıyla gerçekleştirdiği görüşmelerin dinlenmesi ile aynı ağırlıkta değerlendirilmesi olanaklı değildir. Anayasa Mahkemesinin bu kararında GPS teknolojisinin sınırlı yapısına dikkat çektiği ancak hızla gelişen teknoloji dolayısıyla yasa

Sonuç olarak asıl sorunun kişisel verilerin etkin korunması olduğu dikkatten kaçmamalıdır. Kişisel verilerin toplanmasına, kullanılmasına ve paylaşımına ilişkin uygulanabilir ve etkili kuralların belirlenmesi, bunların denetimini sağlayacak bağımsız kurumların oluşturulması, ihlallere karşı yaptırımların öngörülmesi ve konuya ilişkin bilincin gelişmesi “*hassas*” ya da değil bireylerin kişiliğini etkileyen her türlü verinin korunmasını sağlayacaktır.

C. İSTİSNALAR

AB Yönergesindeki düzenleme şekline geri dönecek olursak, öncelikle Yönergeye göre hassas kişisel verilerin işlenmesinin kural olarak yasaklandığını anımsatmamız gerekir. Ancak bu kuralın istisnaları bulunmaktadır. Nitekim Yönerge’nin 8/2 hükmü hassas kişisel verilerin işlenebileceği durumları belirlemiştir¹⁸⁰. Buna göre bu türdeki verilerin işlenmesine izin verilebilecek özel koşullar şöyledir:

- *İlgili kişinin açık rızası bulunuyorsa*.¹⁸¹ Özel nitelikteki kişisel verilerin işlenmesinde belki de en önemli meşruiyet koşulu ilgili kişinin rıza beyanında bulunmasıdır. Nitekim bu türdeki veriler, ilgilinin kişiliği ile yakından ilişkilidir ve verilerinin işlenmesi kararını öncelikle kendisi vermelidir. Hassas kişisel verilerin işlenmesi için aranan rızanın, yukarıda değinilen diğer işlemlerdeki gerekliliklerden farklı olarak bir de “*açık*” bir şekilde verilmesi zorunluluğu bulunur. Bu ise ilgili kişinin kabule yönelik iradesini ortaya koyan müspet bir hareketini (“*opt-in consent*”) gerektirir. Kişinin hareketsizliğinden rıza gösterdiği sonucunun çıkarılması

koyucuların, bilgilerin geleceğini belirleme hakkını ihlal edebilecek yeni uygulamalara karşı uyanık olması gerektiğine işaret ettiği de dikkatten kaçmamalıdır. Bkz. **a.g.k.** par. 51. Ancak kararın verildiği tarihten bugüne belirtilen teknolojinin gelişim hızını düşünürsek Alman Anayasa Mahkemesi’nin bu değerlendirmesinin günümüz koşullarını karşılamadığını rahatlıkla söyleyebiliriz. Yalnızca şüphelinin cep telefonuna gönderilen bir mesajla yer takibinin yapılabildiği günümüzde, önüne gelen yeni olaylarda Alman Anayasa Mahkemesi’nin değerlendirmesinin de farklı olacağı düşünülebilir. Bkz. Nicole JACOBY, “The Decision of the Bundesverfassungsgericht of April 12, 2005-Concerning Police Use of Global Position Systems as a Surveillance Tool”, **German Law Journal**, C. 6, S.7, Y. 2005.

¹⁸⁰ Bu noktada AK Sözleşmesi’nde özel veri kategorilerinin yani hassas verilerin işlenmesinin olanaklı olduğu istisnai durumlar Ab Yönergesi’ndeki gibi ayrıntılı bir şekilde belirlenmediğini hatırlamak gerekir. Bunun yerine Sözleşme’de bu türdeki verilerin ancak ulusal hukuk sisteminde “uygun önlemler” alınarak işlenebileceği belirtilmiştir. Bkz. AK Sözleşmesi m.6.

¹⁸¹ AB Yönergesi m. 8/2,a.

ise söz konusu değildir¹⁸². Bu durumda, veri öznesine katılmamayı tercih edebileceği bir araç sunulması ile m.8/1,a'da aranan açık rıza koşulu gerçekleşmiş olmayacaktır. Bazı üye ülkelerde pazarlama amacıyla kişisel verilerin işlenmesi, rıza gösterilmemiş olsa bile, meşruluk testini aşabilmektedir. Ancak bu durum hassas kişisel veriler için söz konusu değildir. Bu kategorilerdeki veriler için rıza gösterilmiş olması zorunludur. Bunun gibi, tıbbi ya da eczai ürünler ya da hizmetler sunan bir web sitesini ziyaret eden bir kişiye doğrudan pazarlama amacı dolayısıyla sunulan anlaşmada rızasının geçerli olabilmesi için pasif değil aktif bir tutumda bulunması gerekir. Bir başka anlatımla kişi, iradesinin katılmama yönünde belirttiğini göstermek için değil, katılma yönündeki iradesini ortaya koyabilmek için bir harekette bulunmalıdır¹⁸³.

- *Veri işleme, veri koruma görevlisinin iş hukukundan kaynaklanan özel hak ve yükümlülüklerini yerine getirmesi için zorunluysa*:¹⁸⁴ Örneğin böylesi bir zorunluluk, işçinin sendika kesintisini yapmak işverenin yasal göreviyse söz konusu olabilir. Bu istisnanın kapsamına yorum yoluyla ulaşmak olanaklı değildir. Bu koşulun sağlanabilmesi için verinin toplanması ve işlenmesi mutlaka gerekli olmalı ve yasal bir zorunluluktan kaynaklanmalıdır¹⁸⁵.

- *Veri öznesinin ya da diğer bir kişinin yaşamsal çıkarlarının korunması için gerekliyse*:¹⁸⁶ Bu istisnadan söz edebilmek için ilgili kişinin hukuken veya fiziksel olarak rıza göstermesinin olanaksız olması gerekir. Aksi takdirde kararı verecek olan yine ilgili kişidir ve burada "rıza"ya ilişkin kurallara uyulması gerekir.

- *işlemenin ilgili kişi tarafından kamuya açıklanan verilere ilişkin ya da hakların kurulması, kullanılması ve korunması için gerekli olması*¹⁸⁷;

- *kar amacı gütmeyen bir kurum tarafından yasal etkinliklerini yerine getirebilmesi için işlemenin gerekli olması*¹⁸⁸: Bu istisnanın geçerli olabilmesi için uygun önlemlerin alınması, verilerin kurumun üyeleri ya da bağlantılı kişilerle ilgili olması ve veri öznesinin rızası olmaksızın üçüncü kişilere açıklanmaması gerekir.

¹⁸² Christopher KUNER, s. 102. Ayrıca bkz. Article 29 Working Party, **Working Document on the processing of personal data relating to health in electronic health records (EHR)**, WP 131, 15 Şubat 2007, s. 9.

¹⁸³ Lucas BERGKMP, Jan DHONT, s. 83.

¹⁸⁴ AB Yönergesi m. 8/2, b.

¹⁸⁵ Christopher KUNER, s. 102.

¹⁸⁶ AB Yönergesi m. 8/2,c.

¹⁸⁷ AB Yönergesi m. 8/2,e.

¹⁸⁸ AB Yönergesi, m.8/2, d.

Burada belirtilen kar amacı gütmeyen kuruluş; dernek, vakıf... vb. olabileceği gibi bu örgütlenme siyasal, felsefi ya da sendikal bir amaca da yönelmiş olabilir.

- *veri işlemenin önleyici hekimlik, tıbbi teşhis, tıbbi yardım veya bakım veya sağlık hizmetlerinin idari olarak yürütülmesi için gerekli olması ve bu verilerin ya sağlık personeli veya sağlık personeli gibi sır saklama yükümlülüğüne tabi kişiler tarafından işlenmesi*¹⁸⁹: Burada sağlık hizmetinin sağlanması açısından geçerli olan bazı veri türlerinin işlenmesine istisna getirildiği görülmektedir. Ancak burada da verileri işleyebilecek olanlar, sır saklama yükümlülüğüne tabi olan kişiler ile sınırlandırılmıştır.

- Bütün bunların yanında Yönerge uyarınca üye devletler, uygun önlemleri almak koşuluyla kamu yararı için başka bazı istisnalar da belirleyebilir¹⁹⁰.

Bu özel durumlara ilişkin dikkatten kaçmaması gereken önemli bir konu, bunların AB Yönergesinde belirlenen diğer kurallara uygun davranma zorunluluğunu ortadan kaldırmadığıdır. Burada istisna getirilen yalnızca hassas kişisel verilere yönelik özel korumadır¹⁹¹. Nitekim hassas kişisel verilerin işlendiği durumlarda diğer güvencelerin de daha sıkı bir şekilde uygulanması söz konusu olacaktır. Hassas kişisel verilerin, veri koruma görevlilerine yönelik getirdiği fazladan yükler, özel ve kamu kuruluşlarının pek çok kez bu türdeki verilerin işlenmesinin gerekli olup olmadığını tekrar gözden geçirmeye yöneltmektedir. Şüphesiz bu değerlendirmelerin bir kısmında hassas verilerin toplanmasının veya işlenmesinin mutlaka gerekli olmadığı sonucuna varılmaktadır¹⁹².

VI. VERİ GÜVENLİĞİ İLKESİ

Veri güvenliği ilkesi kişisel verilerin korunması hukukunun ayrılmaz bir parçasıdır. Bu ilke veri denetçilerinin kişisel verilerin kazara ortadan kaldırılmasını,

¹⁸⁹ AB Yönergesi m. 8/3.

¹⁹⁰ AB Yönergesi m. 8/4.

¹⁹¹ Christopher KUNER, s. 101; Lucas BERGKMP, Jan DHONT, s. 83.

¹⁹² Christopher KUNER, s. 102.

bunlara yetkisiz erişimi, değiştirilmelerini, silinmelerini ve yayınlanmalarını engelleyecek önlemleri almalarını gerektirir¹⁹³.

Çalışmamızın giriş bölümünde de belirtildiği üzere kişisel verilerin korunması ile veri güvenliği eş anlamlı değildir. İlkinde amaç, bireylerin korunması iken, ikincisinde verilerin korunması hedeflenmektedir. Ancak bunlar kişisel nitelikte olduğunda veri güvenliği kişisel verilerin korunmasının bir aracı haline gelmektedir. Verilere yetkisiz erişim ve bunların yetkisiz kullanımının önüne geçilmesinde kurum ve kuruluşların da çıkarı bulunur. Bu, bankacılık, sigortacılık ve sağlık hizmetleri gibi güven ilişkisinin önemli olduğu alanlarda daha da açıkça görülebilir¹⁹⁴. Bir bankaya parasını yatırmayı, sigorta şirketiyle sözleşme yapmayı ya da tanı ve tedavi için bir sağlık kuruluşuna başvurmayı düşünen kişi verilerinin güvende olduğunu bilmek isteyecektir. Bu konuda endişe duyması halinde ise belirtilen hizmetleri almamayı tercih edebilir. Bunun ilgili kişi açısından yaratacağı sorunlar yanında, kurumun ekonomik kaybına neden olacağı da açıktır. Bu durum, veri güvenliğinin ekonomik olarak ölçülebilir çıkarları da güvence altına aldığını ortaya koymaktadır.

Veri güvenliği ilkesi konuya ilişkin metinlerin tamamında yer alır. 108 sayılı AK Sözleşmesinin 7. maddesi uyarınca *“Yetkisiz erişim, değiştirme veya yayımlama yanında kazara veya yetkisiz tahribe karşı otomatik veri dosyalarında yer alan kişisel verilerin korunması için uygun güvenlik önlemleri alınacaktır”*. Hükümde yer alan *“uygun güvenlik önlemleri”* ifadesini, somut olaydaki verinin tutulma amacı, taşıdığı riskin şiddeti gibi konuları dikkate alarak yorumlamak gerekir. BM Rehber İlkelerinde ise: *“Hem kazara kayıp veya tahrip gibi doğal tehlikelere karşı, hem de yetkisiz erişim, verilerin dolandırıcılık amacıyla kötüye kullanımı gibi insan kaynaklı tehlikelere ya da bilgisayar virüslerinin bulaşmasına karşı dosyaları koruyacak uygun önlemler alınmalıdır”* ifadesi yer alır¹⁹⁵.

Veri güvenliği ilkesi OECD Rehber İlkeleri ve APEC Çerçeve Belgesinde de düzenlenmiştir. OECD Rehber İlkelerinde: *“Kayıp veya yetkisiz erişim, tahrip, kullanım, değiştirilme ya da yayımlamaya karşı”* kişisel verilerin *“makul güvencelerle”* korunması gerektiğine işaret edilmiştir¹⁹⁶. APEC Çerçeve Belgesi’nde

¹⁹³ Lee A. BYGRAVE, **Data Protection Law**, s. 67.

¹⁹⁴ Marie-Theres TINNEFELD ve diğ., s. 384.

¹⁹⁵ BM Rehber İlkeleri, par. 7.

¹⁹⁶ OECD Rehber İlkeleri, par. 11.

ise biraz daha ayrıntılı bir düzenleme yer alır¹⁹⁷. Buna göre “*Kişisel veri denetçisi, tuttukları kişisel verileri ... risklere karşı uygun önlemlerle korumalıdır*”. Bu riskler, ilgili hükümde kişisel verilerin kaybı, yetkisiz erişim, yetkisiz silinme, kullanılma, değiştirilme ve yayınlanma ya da diğer kötüye kullanımlar olarak sayılmıştır. Ayrıca belirtilen hükümde bu önlemlerin “*zarar tehdidi olasılığı ve önemiyle, bilginin hassaslığıyla ve somut durumuyla orantılı ve düzenli inceleme ve yeniden değerlendirme konusu*” olması gerektiği belirtilmiştir.

AB Veri Koruma Yönergesi’nde ise şu düzenleme yer alır: “*Üye Devletler denetçinin, kişisel verilerin kazara veya hukuka aykırı tahribine veya kazara kaybolmasına, değiştirilmesine, yetkisiz yayımı veya erişimine, özellikle işlemin bir şebeke ağı üzerinden nakli yoluyla yapılması durumunda, ve hukuka aykırı diğer hukuka aykırı işleme biçimlerinden korunması için gerekli teknik ve örgütsel önlemleri almasını sağlayacaklardır*”¹⁹⁸.

Bu önlemlerin hem ilgili sistem kurulurken, hem de daha sonra veriler işlenirken alınmalıdır¹⁹⁹. Bu sırada teknik olanaklar ve uygulama masrafları göz önünde tutularak işlemeyen kaynaklı riske ve korunan verinin niteliğine uygun düzeyde güvenlik sağlanmalıdır²⁰⁰. Veri denetçisi ayrıca, bir sözleşme veya yasal hüküm uyarınca²⁰¹, veri işleyen çalıştırdığında teknik ve örgütsel güvenlik önlemleri bağlamında yeterli güvenceyi sağlamalıdır²⁰². Bunun yanında belirtilen hükümlere uygun olarak alınan önlemlerin belgelendirilmesi de gerekir²⁰³.

Veri güvenliğine yönelik yukarıda işaret edilen önlemler, birkaç açıdan değerlendirilebilir. Öncelikle konu, tehdidin kaynağı açısından irdelenmelidir. BM Rehber İlkelerinin ilgili hükmünde de açıkça belirtildiği gibi tehlike kazara oluşabileceği gibi, bir ya da daha fazla kişiden de kaynaklanabilir. Her iki durum da teknik önlemler alınmalıdır. Veriler, kazara kaybolmalarına ya da değiştirilmelerine karşı yedeklenmeli, bilgisayar virüslerinden korunmayı sağlayacak bir sistem kurulmalıdır. İnsan kaynaklı tehlikelere karşı da dışarıdan gelebilecek müdahalelerin önlenmesi için bilgisayar sistemlerine güvenlik duvarları kurulması yararlı olacaktır.

¹⁹⁷ APEC Çerçeve Belgesi, par. 22.

¹⁹⁸ AB Veri Koruma Yönergesi, m. 17/1.

¹⁹⁹ AB Veri Koruma Yönergesi, baş. Par. 46.

²⁰⁰ AB Veri Koruma Yönergesi, m.17/1, 2. cümle; baş. par. 46.

²⁰¹ AB Veri Koruma Yönergesi, m. 17/3.

²⁰² AB Veri Koruma Yönergesi, m. 17/2.

²⁰³ AB Veri Koruma Yönergesi, m. 17/4.

Özellikle uzaktan bankacılık hizmetleri gibi alanlarda veri güvenliğinin sağlanması oldukça önemlidir. Banka, müşterilerle iletişiminin teknikle aynı düzeyde olmasına özen göstermelidir. Hem müşterilere hem de bankaya karşı müdahale olasılığının yok edilmesi gerekir. Telefon görüşmelerinde iletişimin dinlenmesi önlenmelidir. Veriler, değiştirilmeyecek şekilde saklanmalıdır²⁰⁴.

Bunun yanında, böylesine bir müdahalenin verileri işleyenlerden kaynaklanabileceği de göz ardı edilmemelidir. Verileri işleyenlerin olanaklı olan en az miktarda veriye ulaşmasının sağlanması ve bu kişilerin etkinliklerinin uygun araçlarla denetimi olumlu sonuçlar sağlayabilir. Dikkatten kaçmaması gereken bir diğer husus ise verilere müdahalenin hem gerçek, hem de sanal dünyada gerçekleşebilecek olmasıdır.

Kişisel verilerin bulunduğu belgeler maddi olarak elde edilebileceği gibi, bilgisayarlarda tutulan bilgilere sanal ortamda uzaktan erişim de söz konusu olabilir. Teknik açıdan programlara ve bilgi işlem sistemlerine yönelebilecek her türlü tehdite karşı koruma sağlanmalıdır²⁰⁵. Bu kapsamda hem yazılım hem de donanım korunmalıdır²⁰⁶.

Veri güvenliğine ilişkin ilkeler uygulamaya geçirilirken somut durumun kendi koşulları da dikkate alınmalıdır. Örneğin kişisel verilerin yer aldığı bir akıllı kartın ödeme yapma özelliği de bulunması, bu bilgilerin kötüye kullanılma riskini artırır. Bu nedenle veri güvenliğini sağlayabilmek için, kart sahibin hassas verilerinin kayıtlı olduğu bir akıllı kartın ödeme özelliği ile birleştirilmesi önerilmemektedir²⁰⁷.

Veri güvenliği önemli ancak hızla gelişen teknoloji dolayısıyla sağlanması zor bir konudur. Veri güvenliğini sağlayan araçlar ile bunların aşılmasını sağlayan yöntemler paralel bir şekilde gelişmektedir. Bu nedenle alınan teknik önlemlerin sürekli güncellenmesi, yenilenmesi bir zorunluluktur.

Veri güvenliğinin yeteri düzeyde sağlan(a)maması dünyanın pek çok yerinde yankı uyandıran skandalların yaşanmasına neden olmuştur. Hatta ABD’de özellikle müşteri veri tabanlarından çeşitli bilgilerin çalınması olayları, ülkenin kişisel

²⁰⁴ Marie-Theres TINNEFELD ve diğ., s. 384.

²⁰⁵ Marie-Theres TINNEFELD ve diğ., s. 384.

²⁰⁶ Peter GOLA, Rudolf SCHOMERUS, s. 344.

²⁰⁷ **Guiding principles for the protection of personal data with regard to smart cards (2004)**, as adopted by CDCJ at its 79th Plenary, 11-14 Mayıs 2004, s. 4.

verilerin korunması politikasını çeşitli zamanlarda önemli bir tartışma konusu haline getirmiştir²⁰⁸.

Kişisel verilerin yetkisiz kişilerin eline geçmesi ekonomik, siyasal, sosyal ve hatta fiziksel zararlara neden olabilir. Yaklaşık on yıl önce Cambridge Üniversitesi'nde çalışanların adres bilgilerinin sızması sonucunda, evlerinin hayvan hakları savunucularınca hedef alındığı bilinmektedir. Birkaç yıl önce yine İngiltere'de kredi kartı verilerinin basına sızması sonucunda politikacıların iddia edilen ölçüsüz alkol tüketimlerine ilişkin kişilik haklarına zarar verici bilgiler basında yayınlanmıştır²⁰⁹. Kimlik bilgileri, banka hesap numaraları gibi bilgilerin çalınması sonucunda oluşan ekonomik zararın boyutu ise her geçen gün artmaktadır²¹⁰.

Bu noktada şu hususa da işaret etmek gerekir: veri güvenliğinin hem verileri işleyen kişiler tarafından, hem de verilerin öznesi tarafından sağlanması gerekir. Verileri toplayan ve işleyen sistemlerin korunması yanında, bireyler de kendilerini korumalıdır. Teknoloji tabanlı güvencelerin kişisel verilerin etkin korunması için oldukça önemli olduğu unutulmamalıdır. Bireylerin kendi özel bilgisayarlarında ya da kullandıkları başka elektronik araçlarda gereken önlemleri almaları, hem temel hak ve özgürlüklerine hem bütçelerine yönelecek pek çok saldırının önlenmesine yardımcı olacaktır.

Nitekim gelişen teknoloji, kişilerin özel yaşamlarını korumaya yardım edecek ürünleri de sunmaktadır. Fiziksel alandaki bazı uygulamalar ve İnternet iletişiminde, çeşitli düzeylerde koruma sağlayan pek çok teknoloji bulunur. Şifreleme, kullanıcının kimliğini anonim hale getiren yeniden postalayıcılar (anonymous remailers), vekil sunucular (Proxy servers), dijital para (digital cash) ve akıllı kartlar (smart cards) birkaç örnektir. Ancak bu sistemlerin güvenliği ve güvenilirliğine ilişkin çeşitli tartışmaların sürdüğü de belirtilmelidir²¹¹.

²⁰⁸ Bu konuya ilişkin olarak bkz. Maarten PEETERS, "Identity Theft Scandals in the U.S. : Opportunity to Improve Data Protection", **MMR**, Y. 2005 Heft 7, s. 415-420.

²⁰⁹ **Dilemmas of Privacy and Surveillance, Challenges of Technological Change**, The Royal Academy of Engineering, Mart 2007, s. 22.

²¹⁰ Konuya ilişkin çeşitli örnekler için bkz. "The Scary New World of Identity Theft", **Newsweek**, 5 Eylül 2005; "Büyük Gözaltı: İzleniyoruz, Gözleniyoruz, Dinleniyoruz", **NTV Bilim**, 2 Nisan 2009.

²¹¹ David BANISAR, "Privacy and Data Protection Around the World", s. 2; **Privacy and Human Rights**, s. 4.

Bireylerin haberleşmesinin gizliliği ve bu iletişimin yetkisiz kişilerin müdahalesinden uzak tutulması, özel yaşamın gizliliği hakkının önemli bileşenleridir. Bu gereklilik, pek çok durumda kişisel verilerin korunması açısından da söz konusudur. Birey, özel haberleşmenin gizliliğinin sağlanmasında, elbette, ilk önce hukuksal güvencelerle korunmalıdır. Ancak fiilen bu gizliliği sağlayabilmek için teknoloji de etkili bir araç olabilir. Bu noktada, özellikle şifreleme teknolojilerinin öne çıktığı görülmektedir²¹².

Şifreleme en genel tanımıyla *“İnternet üzerinden yayın yapan veya iletişim kuran bazı kişi ve grupların, yayınlarının ya da iletişimlerinin tamamını veya bir kısmını belirli şifre teknolojileri kullanarak gizlemelerini sağlayan bir teknolojidir”*²¹³. Çeşitli şifreleme tekniklerinin kullanılması bilgi çağı olarak nitelendirilen günümüze özgü bir uygulama değildir. Sırların saklanması amacıyla şifreleme tekniği Antik Çağlardan günümüze hep kullanılan bir yöntem olmuştur²¹⁴. Günümüzde de çok çeşitli amaçlarla bu yöntemden yararlanılmaktadır. Özellikle elektronik ticaretin şifreleme teknolojisinin yokluğunda işlemesi olanaksızdır.

Ancak devletlerin özellikle güvenlik gerekçesiyle bu türdeki uygulamaların kullanımına sınırlama getirme yönünde eğilimleri dikkat çeker. Oysa şifreleme araçlarına ilişkin herhangi bir düzenlemenin, ciddi suçlarla mücadeleye yardımcı olacağı düşüncesine pek çok kesim kuşkuyla yaklaşmaktadır²¹⁵. Suçlulukla mücadele için, şifreleme yazılımlarını lisansa bağlamak, bunların ihracına ve ithaline sınırlamalar getirmek, şifre anahtarlarının depolanmasına zorlamak, arka kapılar sağlayan donanımlar kullanmak gibi devletlerin kimi zaman başvurduğu yöntemlerin orantısız önlemler olacağı dikkatten kaçmamalıdır²¹⁶.

²¹² Şifreleme gibi bazı teknolojilerinin siyasal alandaki potansiyel etkilerine ilişkin bir değerlendirme için bkz. Olaf WINKEL, “The Democratic Potentials of Interactive Information Technologies under Discussion-Problems, Viewpoints, and Perspectives”, **Elektronische Demokratie (Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis)**, haz. Bernd HOLZNAGEL, Andreas GRÜNWALD, Anika HANSSMANN, s. 29.

²¹³ Hasan SINAR, **İnternet ve Ceza Hukuku**, Beta, İstanbul 2001, s. 58.

²¹⁴ Antik Çin’de, yalnızca üst sınıfların okuma yazma öğrenmesi sağlanarak, yazının kendisi bile bir şifreleme yöntemi olarak kullanılmıştır. Şifrelemenin belgeli olarak ilk kullanımına ise M.Ö.1900 yılında Mısır’da rastlanmıştır. Bkz. Bruce SCHNEIER, s. 86. Ayrıca bkz. Alparslan BABAOĞLU, “Kriptolojinin Geçmişi: Bir Şifre Algoritması Kullanmadan Önce Son Kullanma Tarihine Bakın!”, **Bilim ve Teknik**, Y. 42, S. 500, Temmuz 2009, s. 24-27.

²¹⁵ Örneğin bkz. **Common Statement on Cryptography**, 12 Eylül 1997, International Working Group On Data Protection in Telecommunications.

²¹⁶ Özellikle dijital ortamda kişisel verilerin korunmasını sağlamak için pek çok kişi güçlü şifreleme teknolojilerinin kullanılmasının etkili bir araç olduğu görüşündedir. Başta ABD olmak üzere

Şifreleme teknolojisinin devletin müdahalesinden bağışık olarak, ulaşılabilir olmasının çok çeşitli yararları bulunduğuna işaret edilmektedir. Şifreleme tek başına güvenliğin sağlanması için yeterli değildir. Ancak oldukça etkili araçlardan biridir²¹⁷. Öncelikle e-posta ya da para transferi gibi iletişim etkinlikleri şifreleme ve kimlik denetimi (authentication) ile sağlanacak güvenli bir ortamda sağlıklı bir şekilde yürütülebilir. Özel iletişimin yanında şifreleme, bilginin anonim olarak yayılmasına da yardımcı olacaktır. Örneğin insan haklarına ilişkin raporların anonim bir şekilde yayınlanması bu sayede sağlanabilir. Bunun yanında şifreleme, dijital ortamda yayınlanan belgelerin sonradan değiştirilmesini ya da tahrif edilmesini de engelleyecektir. Ayrıca veri güvenliğine ilişkin pek çok sorunun yaşandığı günümüzde, şifreleme, sağlık bilgileri, mali veriler, e-postalar gibi kişisel verilerin gizliliğini sağlar. Ağlarla örülmüş bir ortamda bu türdeki bilgilerin çalınma ve kötüye kullanılma riski taşıdıkları unutulmamalıdır²¹⁸. Avrupa Komisyonu da bu yöntemlerin yasal bir çerçevenin yerini alamayacağı, ancak mevcut yasaların tamamlayıcısı olabileceği yönünde görüşünü açıklamıştır²¹⁹.

Sonuç olarak veri güvenliğinin sağlanmasının kişisel verilerin korunması açısından oldukça önemli olduğu unutulmamalıdır. Bu, yukarıda işaret edilen metinlerde de yer aldığı üzere veri denetçi ve işleyicileri üzerine düşen bir yükümlülüktür. Ancak bunun yanında kişilerin de verilerinin güvenliğini sağlayacak önlemleri almaları çıkarlarının korunmasına yardımcı olacaktır. Yetkisiz erişim ve benzeri müdahaleler pek çok hukuk sisteminde suç olarak tanımlanmış ve bu

çeşitli ülkelerde bu konuya ilişkin girişimlerin devletler tarafından sınırlandırılma eğilimi olduğu dikkat çekmektedir. Örneğin, bir dönem ABD’de askeri silahlanmaya ilişkin bir yasa ile bu teknolojiler sınıflandırılmış ve 64 bittin büyük bir anahtar gerektiren şifreleme teknolojileri askeri mühimmat sayılarak satışları katı kurallara bağlanmıştır. Bu gibi sınırlamaların aşılmasında ya da daha doğru bir deyimle gevşetilmesinde 2000’li yılların başında çeşitli hacker grupları önemli bir rol oynamıştır. Bu gruplardan en çok bilinenlerinden biri “*Cypherpunks*”dır. John Gilmore, Tim May ve Eric Hughes tarafından kurulan bu grubun amaçları, Hughes’ın yayınladığı “*A Cypherpunk’s Manifesto*”da açıklanmıştır. Bu metinde, elektronik çağda kişisel verilerin korunmasının özel olarak önemli olduğuna işaret edilmiş ve bu korumayı sağlayabilmek için herkesin kullanımına açık bir kod oluşturdıkları duyurulmuştur. Bkz. Pekka HIMMANEN, **The Hacker Ethic and the Spirit of the Information Age**, Vintage, Büyük Britanya 2001, s.103-105; Eric HUGHES, “A Cypherpunk’s Manifesto”, 9 Mart 1993, <http://activism.net/cypherpunk/manifesto.html> , (s.y. 18 Şubat 2008); John GILMORE, “Privacy, Technology and the Open Society”, Conference on Computers, Freedom and Privacy, 28 Mart 1991, <http://www.toad.com/gnu/cfp.talk.txt> (s.y. 18 Şubat 2008).

²¹⁷ Bruce SCHNEIER, s. 85.

²¹⁸ **Cryptography and Liberty 2000, An International Survey of Encryption Policy**, Electronic Privacy Information Center, Washington DC, ABD 2000, s. 5.

²¹⁹ David BANISAR, “Privacy and Data Protection Around the World”, s. 2.

eylemleri gerçekleştirenler karşı yaptırımlar öngörölmüştür. Ancak böylesi bir suçun mağduru olmadan veri güvenliğinin sağlanması önleyici bir koruma oluşturacağı dikkatten kaçmamalıdır.

VII. İSTİSNALAR VE SINIRLAMALAR

Kişisel verilerin korunması hakkı, sınırsız bir hak alanı değildir. Yukarıda incelenen temel ilkelere belirli durumlarda istisna getirilmesi olanaklıdır. Bu, her şeyden önce buradaki temel hakkın göreceli yapısından kaynaklanır. Kişisel verilerin korunmasına temel oluşturan hakkın, diğer hak ve özgürlüklerle ayrıca bireysel ya da kolektif olarak başkalarının hak ve özgürlükleriyle dengeli olması gerekir²²⁰. Bu denge ise ancak yukarıda incelediğimiz temel ilkelere belirli durumlarda istisna ve sınırlamaların getirilmesi ile olanaklıdır.

Nitekim kişisel verilerin korunmasına hâkim olan temel ilkelere yönelik sınırlama ve istisnalar konuya ilişkin bütün belgelerde yer alır. Bu anlamda AK Verilerin Korunması Sözleşmesi, OECD ve BM Rehber İlkeleri ve APEC Çerçeve Belgesi'nde hem ilkelere getirilen sınırlamalara, hem de sınırlamanın sınırlarına ilişkin hükümler bulunur²²¹. AİHS'in de 8/2 hükmünde aynı maddenin 1. fıkrasında güvence altına alınan özel yaşamın gizliliği hakkına müdahalenin meşru kabul edileceği durumlar belirlenmiştir²²².

AB sistemi açısından baktığımızda özellikle 95/46/AT sayılı Yönerge'yi dikkate almak gerekir. Yönerge'nin 9. ve 13. maddelerinde yukarıda değerlendirilen ilkelerin sınırlandırılmasına ilişkin hükümler yer almaktadır. “*Kişisel verilerin işlenmesi ve düşünceyi açıklama özgürlüğü*” kenarbaşlıklı 9. madde uyarınca kişisel verilerin işlenmesi yalnızca gazetecilik amacıyla veya sanatsal ya da edebi açıklamalar için söz konusu olduğunda özel yaşamın gizliliği hakkı ile düşünceyi açıklama özgürlüğüne hakim olan ilkelerin dengelenmesini gerektiren durumlarda sınırlandırılabilir ve istisnalar getirilebilir.

²²⁰ David TOWNEND, “Overriding Data Subjects’ Rights in the Public Interest”, **The Data Protection Directive and Medical Research Across Europe**, Ashgate, İngiltere 2004, s. 89.

²²¹ AK Verilerin Korunması Sözleşmesi, m. 9; OECD Rehber İlkeleri, par. 4; BM Rehber İlkeleri, par. 6; APEC Çerçeve Belgesi, par. 13.

²²² Bkz. yuk. “AİHS” başlığı.

AB Yönergesi'nin 13. maddesinde ise “*istisnalar ve sınırlamalar*” başlığı altında bu konu düzenlenmiştir. Buna göre, bazı durumlarda verinin niteliğine ilişkin ilkelere, ilgili kişinin bilgilendirilme hakkına, erişim hakkına, işleme eyleminin kamuya ilan edilmesine sınırlandırma getirilebilir. Ancak bunun şu konuların korunması için mutlaka zorunlu bulunması gerekir:

- (a) *ulusal güvenlik;*
- (b) *savunma;*
- (c) *kamu güvenliği;*
- (d) *suçların ya da düzenlenmiş etik kuralların ihlalinin önlenmesi, araştırılması, soruşturulması ve kovuşturulması;*
- (e) *para, bütçe ve vergiyle ilgili konular dahil olmak üzere, Avrupa Birliğinin veya Üye Devletin önemli bir ekonomik veya mali çıkarı;*
- (f) *yukarıda (c), (d) ve (e)'de belirtilen resmi yetkinin kullanılmasıyla bağlantılı olarak izleme, soruşturma veya düzenleme;*
- (g) *ilgili kişinin veya diğerlerinin hak ve özgürlüklerinin korunması.*

Görüldüğü gibi kamu çıkarının ağır bastığı bazı durumlarda kişisel verilerin korunmasına yönelik ilkelere istisna getirilmesi olanaklıdır. İstisnaları oluşturan kavramların sınırları belirsizdir. Bu nedenle istisna ve sınırlamaların geniş yorumlanması kişisel verilerin korunması ilkelerinin özüne müdahale getirebilir. Ancak temel hak ve özgürlüklere ilişkin bütün metinlerde olduğu gibi burada da sınırlamaların dar yorumlanması gerektiği unutulmamalıdır.

Burada altı çizilmesi gereken husus, kişisel verilerin korunmasının temel bir insan hakkı olduğudur. Bu nedenle temel hak ve özgürlüklerin sınırlandırılmasına ilişkin ilkeler burada da uygulanacaktır. AİHS'nde ve demokratik devletlerin Anayasalarında temel hak ve özgürlüklerin ancak yasa ile sınırlandırılabilceği ilkesi benimsenmiştir. Bunun yanında ölçülülük ilkesine uygun olarak, meşru amacın gerektirdiğinden daha yüksek oranda sınırlama getirilmemesi gerekir. Kişisel verilerin korunmasına istisna getiren hükümlerin açık ve öngörülebilir olması ve belirlenen amacın aşılması da oldukça önemlidir. Aksi takdirde hukuk devleti ile bağdaşmayacak keyfi uygulamalarla karşılaşılabilir. Örneğin belirsiz ya da henüz belirlenmemiş bir amaç için kişisel verilerin bir yerde depo edilmesi bu ilkelere aykırılık oluşturacaktır.

Çalışmanın birinci bölümünde de belirtildiği üzere bazı durumlarda kişisel verilerin korunmasının bilim özgürlüğü ile çatışma halinde olacağı düşünülebilir. Ancak kişisel verilerin korunmasına ilişkin düzenlemelerde genel olarak bu konuya ilişkin özel bazı hükümlerin kabul edildiği görülmektedir²²³. Bilimsel, tarihsel ve istatistiksel araştırmalar bu kapsamda değerlendirilmektedir. Ancak araştırma etkinliklerinin kişisel verilerin korunmasının sınırı olarak değerlendirmemek gerekir. Burada önemli olan her iki meşru amaç arasındaki dengenin sağlanmasıdır. Bu bağlamda bilimsel etkinlikler için bilgileri toplanılacak, işlenilecek ve kullanılacak kişilerin konuya ilişkin olarak aydınlatılmalı ve rızalarının alınması, doğrudan kişilerle ilişkili olarak tutulması gerekmeyen bilgilerin ise anonim olarak saklanması dengenin sağlanmasında önemli araçlardır²²⁴.

VIII. DENETİM VE YAPTIRIM SİSTEMLERİ

Yukarıda kişisel verilerin korunabilmesi için kabul edilen temel ilkelerin neler olduğundan söz ettik. Kişisel verilerin korunması öncelikle bu algının gelişmesiyle ilgilidir. Bireylerin haklarını, veri denetçilerinin sorumluluklarını bildikleri bir ortamda yukarıda belirtilen ilkelere uyum büyük oranda sağlanır. Yine yukarıda işaret edildiği üzere teknik bazı araçların kullanımı da kişisel verilerin korunması açısından yararlı olabilmektedir. Ancak pek çok örnek göstermiştir ki bu ilkelerin yalnızca kâğıt üzerinde tanınması hedefe ulaşılabilmesi için yeterli değildir. Belirtilen ilkelere uygun davranmaya zorlayan, bunların ihlal edilmesi durumunda yaptırım öngören ve bireylerin şikâyetlerini dile getirebildikleri, zararlarını tazmin edebildikleri bir sistemin oluşturulması da gerekir.

Kişisel verilerin korunmasının uluslararası kaynaklarında genel olarak bu türdeki güvencelere yer verilmediği ya da sınırlı olarak değinildiği görülür²²⁵. 95/46/AT sayılı Veri Koruma Yönergesi'nde ise sorumluluk, yaptırım, tazminat, bildirim gibi konular düzenlenmiştir. Bu güvencelere ilişkin açıklamalara geçmeden

²²³ Örneğin bkz. AB Verilerin Korunması Yönergesi, Başlangıç, par. 29, 34, 40; m. 6/1,b,e; 11/2; 13.

²²⁴ Ayrıca bkz. Oğuz ŞİMŞEK, s. 126.

²²⁵ Diane ROWLAND, Elizabeth MACDONALD, **Information Technology Law**, 3. Baskı, Cavendish Publishing, ABD 2005, s. 339.

önce kişisel verilerin etkin bir şekilde korunabilmesi için kuralların uygulanabilir nitelikte olması yanında, bunların uygulamasının sağlanmasının da son derece önemli olduğunu hatırlatmak isteriz.

A. BAĞIMSIZ ORGANLARCA DENETİM (VERİ KORUMA OTORİTELERİ)

Kişisel verilerin korunması açısından oldukça önemli bir güvence, veri koruma yasaları ile belirlenen ilkelere uygun hareket edilip edilmediğini denetleyen bağımsız bir organın oluşturulmasıdır²²⁶. Kimi yazarlarca bu, kişisel verilerin korunmasına ilişkin düzenlemeleri diğerlerinden ayırt edici bir özellik olarak bile değerlendirilir²²⁷.

Nitekim veri koruma yasalarını iç hukuk düzenlerinin bir parçası haline getirmiş devletlerin büyük bir bölümü, bu yasaların uygulanmasını denetleyecek organlar kurmuştur²²⁸. Özellikle kişisel verilerin korunmasına Avrupa yaklaşımında bu gerekliliğin altı çizilmektedir. Nitekim AB Yönergesi'nde bağımsız denetim organları kişisel verilerin korunmasının "*temel bir bileşeni*" olarak nitelenir²²⁹. Ancak Yönerge'nin aksine diğer uluslararası metinlerde, bağımsız denetim organlarına daha sınırlı yer verildiği görülür.

OECD Veri Koruma Rehber İlkeleri ve APEC Çerçeve Belgesi bağımsız bir denetim organı kurulmasını öngörmemiştir. Benzer bir durum, yakın zamana kadar AK Sözleşmesi için de geçerlidir. Nitekim Sözleşme'nin orijinal metninde böylesine

²²⁶ Bağımsız veri koruma organının (independent data protection authority), kimi yerlerde denetleyici organ (supervisory authority), veri koruma görevlisi (data protection commissioner) ve ombudsman olarak adlandırıldığı da görülmektedir. Simone Fischer-Hübner, **IT Security and Privacy-Enhancing Security Mechanisms**, Springer 2001, s. 11. Bu organı nitelemek üzere farklı deyimlerin tercihi kimi zaman niteliklerindeki farklılıktan da kaynaklanmaktadır.

²²⁷ Lee A. BYGRAVE, **Data Protection Law**, s. 3; Peter HUSTINX, "The Role of Data Protection Authorities", **Reinventing Data Protection**, haz. Serge GUTWIRTH, Yves POULLET, Paul de HERT, Cécile de Terwangne, Sjaak NOUWT, Springer, Almanya 2009, s. 133.

²²⁸ Bağımsız organlarca denetim Avrupa dışındaki pek çok ülkede de benimsenmiştir. Örneğin Kanada'da 1983 yılında yürürlüğe giren ve federal hükümet organlarının elinde bulunan kişisel verilerin korunmasına yönelik hükümler içeren Özel Yaşamın Gizliliği Yasasında 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 değişikliklerde önerilerde bulunmak ve parlamentoya yıllık rapor sunmak ile görevlidir. **Privacy and Human Rights 2006**, s. 309. Bu çoğunluğun dışında kalan ayrıksı örneklerin başında ise ABD ve Japonya gelmektedir. Lee A. BYGRAVE, **Data Protection Law**, s. 70.

²²⁹ Bkz. AB Veri Koruma Yönergesi, baş. par. 62.

bir organın kurulmasını öngören bir hüküm bulunmamaktadır²³⁰. Ancak AK Bakanlar Komitesi tarafından kabul edilen bir ek protokol ile AB Yönergesi'nde belirlendiği şekliyle bir bağımsız denetim organının kurulması benimsenmiştir²³¹. Protokol'ün “*Açıklayıcı Rapor*”unda (Explanatory Report) belirtildiği üzere, bu metnin kabul edilişindeki amaç 108 sayılı Sözleşme’de yer alan ilkelerin uygulamasını geliştirmektir²³². AB Temel Haklar Şartı’nda da kişisel verilerin korunmasını sağlayan ilkelerin uygulamasının bağımsız bir makam tarafından denetleneceği hüküm altına alınmıştır²³³.

BM Rehber İlkeleri’nde ise ulusal düzeyde veri koruma otoritelerinin gerekliliğine dikkat çekilmiştir. Buna göre belirtilen otorite, tarafsız, bağımsız ve teknik olarak yeterli olmalıdır²³⁴. BM’nin 8. rehber ilkesi şu hükmü içermektedir:

“Her ülke yasa ile kendi ulusal hukuk sistemine uygun olarak, yukarıda belirtilen ilkelerin yerine getirilmesini denetlemekten sorumlu bir merci atamalıdır. Bu merci, verileri işlemekten ve oluşturmaktan sorumlu ve teknik yeterlikteki kişi ve kurumlar karşısında tarafsızlığına ve bağımsızlığına ilişkin güvenceler sunmalıdır. Sözü edilen ilkelerin yerine getirildiği ulusal yasa hükümlerinin ihlali halinde, cezai ya da diğer yaptırımlar, uygun bireysel yasal yollarla birlikte öngörülmelidir”.

Diğer uluslararası metinler ile karşılaştırıldığında, bağımsız denetim organına ilişkin en ayrıntılı düzenlemenin AB Veri Koruma Yönergesi’nde bulunduğu görülür. Yönerge’ye göre her üye devlet, Yönerge’de belirlenen hükümlerin uygulamasını izlemek üzere bir ya da birden çok resmi makam oluşturacaktır²³⁵. Bir

²³⁰ Sözleşmede bu hususa yalnızca çok sınırlı bir şekilde değinildiği söylenebilir. Nitekim 108 sayılı Sözleşmenin 10. maddesi “*ulusal hukukta verilerin korunmasının temel ilkelerine etkinlik kazandırmak için gerekli önlemlerin alınması*” öngörülmektedir.

²³¹ **Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows**, ETS No. 181.

²³² **Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows**, ETS No. 181, Explanatory Report, par. 1.

²³³ AB Temel Haklar Şartı, m. 8/3.

²³⁴ BM Rehber İlkeleri, par. 8.

²³⁵ Avrupa Toplulukları kurum ve organlarında kişisel verilerin korunmasını öngören 45/2001 sayılı düzenlemede Birlik düzeyinde bir veri koruma otoritesi öngörmüştür. “*Avrupa Veri Koruma Otoritesi*” olarak adlandırılan bu kuruluş, AB kurum ve organlarının veri koruma ilkelerini doğru uygulamasının izlenmesinden sorumludur. Bkz. **Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with**

başka anlatımla, Yönerge ile en az bir denetim mercinin oluşturulması zorunlu tutulmuştur²³⁶.

Her ne kadar metinde üye devletlere veri koruma otoritelerine ilişkin sistemlerini seçerken bir takdir payı bırakılmış olsa da bazı asgari koşullar belirlenmiştir. Bunların başında mercinin kendisini kuran yürütme ve/veya yasama organından bağımsızlığı gelir²³⁷. Yönerge’de “*tam bağımsızlık*” ifadesi yer almakla beraber, bu gerekliliğin koşullarına yer verilmemiştir²³⁸. Bu nedenle kavramın içeriğinin yorumlanması gerekir.

Bağımsızlık denetim organının görüşüne ulaşırken, başka bir organdan somut olaya yönelik talimat alınmamasını gerektirir. Denetim organı, bunun gerçekleştiği oranda bağımsızdır. Bunun yanında elbette denetim organının yasal olarak bağlayıcı kararları, siyasal ve hukuksal incelemeden geçirildiği gibi, başka organlara ilişkin yasa ve düzenlemeler ile de bağlıdır²³⁹. Bu noktada asıl önemli olan denetim organının özerk bir statüye ve siyasal müdahaleleri önleyecek ve görevini uygun bir şekilde yerine getirmesini sağlayacak finansman ve personel kaynağına sahip olmasıdır²⁴⁰.

regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 008 , 12 Ocak 2001, m.41-48.

²³⁶ AB Veri Koruma Yönergesi, m. 28/1. AB üyesi devletlerin büyük bir bölümü tek bir ulusal veri koruma yasası ve tek bir denetim kurumu öngörmüştür. Ancak örneğin Federal Almanya’da Federal düzeyde bir veri denetçiliğinin yanında, her bir federe devlet için de ayrı bir resmi makam bulunmaktadır. İtalya’da ise, veri koruma otoritesinin yanında bankacılık sisteminde özel yaşamın gizliliğine ilişkin sorunları denetlemek üzere ayrı bir makam 2006 yılında oluşturulmuştur. Christopher KUNER, s. 13, d.n. 50. Veri Koruma Otoriteleri, Avrupa dışındaki kimi ülkelerin de hukuk sistemlerinde benimsenmiştir. Ancak bu kurum ve kuruluşların yetkilerinin Avrupa sistemi ile kıyaslandığında çoğu zaman sınırlı kaldığı görülmektedir. Örneğin Dubai’deki uygulamaya ilişkin olarak bkz. 2007 Veri Koruma Yasası, m.21-25. Dubai Veri Koruma Yasası’nın İngilizce metni için bkz. http://dp.difc.ae/legislation/dp_protection/. Kanada Özel Yaşamın Gizliliği Komiserliği’nin görev ve yetkilerine ilişkin olarak bkz. <http://www.priv.gc.ca/>. Avustralya’daki uygulamaya ilişkin olarak bkz. <http://www.privacy.gov.au/>.

²³⁷ Yönerge’nin başlangıç bölümünde de Üye Devletler’de bir denetim organının kurulmasının ve işlevlerini bağımsız olarak gerçekleştirmelerinin bireylerin korunmasının önemli bir parçası olduğuna işaret edilmiştir(par. 62).

²³⁸ Oysa 45/2001 sayılı AB kurum ve organlarında verilerin korunmasını düzenleyen düzenlemede Avrupa Veri Koruma Denetmeni’nin bağımsız olması gerektiği ifadesiyle yetinilmemiş, bunu koşulları da belirlenmiştir. Belirtilen metin uyarınca bu otorite, görevlerini tam bir bağımsızlık içinde yerine getirmeli (m.44/1); kimseden talimat almamalı ve aramamalıdır (m.44/2). Göreviyle uyuşmayan her türlü etkinlikten kaçınmalı, görev süresi boyunca ücretli ya da ücretsiz hiçbir işte çalışmamalıdır (m.44/3). Görev süresinin bitiminden sonra da dürüst ve menfaatlerden yararlanmada ihtiyatlı olmalıdır (m.44/4).

²³⁹ Lee A. BYGRAVE, **Data Protection Law**, s. 70.

²⁴⁰ Christopher KUNER, s. 17.

Denetim organının bağımsızlığını sağlayacak unsurlar açısından da üye devlet uygulamalarının farklılaştığı görülür²⁴¹. Kimi ülkelerde denetim organı tam anlamıyla özerk bir statü içerisindeyken, kimilerinde başka devlet organlarına bağlı, kimilerinde ise adalet ya da içişleri bakanlıklarının bir organı konumundadır. Başka organlara bağlı olduğu uygulamalar kurumu, siyasal etkilere açık hale getirmekte, bu nedenle eleştirilmektedir²⁴². Bazı üye ülkelerin ise kaynak ya da personel yetersizliği içinde olduğu görülür²⁴³. Bunun yanında Avrupa'daki veri koruma makamlarının hem kurumların yapısı, hem yetkileri açısından da bazı farklılıklar taşıdıkları dikkat çekmektedir²⁴⁴.

AB sisteminde bu organların yetkileri Yönergenin 28. maddesinde düzenlenmiştir²⁴⁵. Buna göre bağımsız denetim organlarının yetkileri üç temel başlık altında toplanabilir:

- *araştırma yetkisi*;
- *etkili müdahalede bulunma yetkisi*;

²⁴¹ Almanya'daki uygulamaya ilişkin olarak bkz. David H. FLAHERTY, **Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States**, The University of North Carolina Press, ABD 1989, s. 40 vd., ayrıca bkz. <http://www.datenschutz.de> ; Yunanistan uygulamasına ilişkin olarak bkz. Phillipos C. SPYROPOULOS, Theodore P. FORTSAKIS, **Constitutional Law in Greece**, Kluwer Law International, Hollanda 2009, s. 150-151; Çek Cumhuriyeti'ndeki uygulamaya ilişkin olarak bkz. <http://www.uoou.cz/uoou.aspx> .

²⁴² Christopher KUNER, s. 17.

²⁴³ First report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final, Analysis and impact study on the implementation of Directive 95/46/EC in Member States, European Commission, par. 13-14.

²⁴⁴ AB ülkelerinden kimileri kamu denetçisi(ombudsman) modelini benimserken, kimileri düzenleme modelini benimsemiştir. Birincisine örnek olarak Finlandiya, Macaristan ve İsveç gösterilebilir. İkincisi ise Fransa, Polonya ve İspanya gibi ülkelerde uygulanmaktadır. Her ikisinin arasında yer alan karma sistemlerin benimsenmesi de olanaklıdır. Bkz. David SMITH, "The Supervisory Authority: Ombudsman or Regulator", Proceedings of the Council of Europe Conference on Data Protection, Varşova, 19-20 Kasım 2001, [http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/events/conferences/2DP\(2001\)Proceedings_Warsaw_EN.pdf](http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/events/conferences/2DP(2001)Proceedings_Warsaw_EN.pdf) , s. 143-144; Christopher KUNER, s. 14-15. AB ülkelerinin ulusal hukuk sistemlerinde veri koruma makamlarına tanındıkları yetkiler de önemli farklılıklar içermektedir. Bu konuya ilişkin Avrupa Komisyonu'nun değerlendirmesi için bkz. First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, Analysis and impact study on the implementation of Directive 95/46/EC in Member States, European Commission, par. 39-41.

²⁴⁵ Ancak belirtmek gerekir ki veri koruma otoriteleri Yönerge'de yalnızca 28. madde ile yetkilendirilmemiştir. Metnin bazı hükümlerinde veri koruma otoritelerinin çeşitli konularda görevlendirildiği görülmektedir. Bunlar şöyle sıralanabilir: özel nitelikteki (hassas) kişisel verilerin açıklanmasına ilişkin karar vermek (m.8/4); veri denetçilerinin işleme etkinlik bildirimlerinin yönetimi (m. 18); öncel denetim etkinlikleri (m.20); işleme etkinlik sicilinin tutulması (m.21); sektörel etik kurallar (codes of conduct) görüş bildirmek (m.27). Bkz. Alfred BÜLLESBACH ve diğ., s. 122-123.

- *ihlal durumunda dava ve şikayet yetkisinin kullanılması.*

Veri koruma otoritelerinin araştırma yetkisi, somut olayda konu olan veriye erişim ve denetim görevini yerine getirebilmek için gerekli olan bilgileri toplama gibi hususları içerir. Etkili müdahalede bulunma yetkisi ise bu organın zorlayıcı niteliğinin bir bileşenidir. Buna göre veri koruma otoritesi, verilerin silinmesini, ortadan kaldırılmasını veya bloke edilmesini emredebileceği gibi, kimi durumlarda verilerin işlenmesini de yasaklayabilir. Veri denetçisini uyarma ya da konuyu parlamento veya başka siyasal kurumların önüne götürme yetkisi de bulunur. Son olarak Yönerge'ye uygun olarak ulusal hukukta kabul edilmiş ilkelere aykırılık bulunduğu hukuksal yollara başvurulması da olanaklıdır²⁴⁶.

AB Veri Koruma Yönergesi, veri koruma otoriteleri arasında işbirliği yapılmasını da öngörür. Bu, bilgilerin paylaşımı ve kimi durumlarda da yetkilerin kullanımı açısından söz konusudur²⁴⁷. Veri koruma hukuku kapsamına giren pek çok olayın uluslararası nitelik taşıması, işbirliğinin benimsenmesini bir zorunluluk haline getirmektedir. Örneğin ilgili kişi ile veri denetçisinin farklı ülkelerde ikamet etmesi halinde bu ülkelerin ulusal organlarının bir arada hareket etmesi gerekecektir.

Bunun yanında veri koruma otoritelerinin konuya ilişkin farkındalığın artırılması ve ilgili kişilerin haklarının kullanılmasının sağlanması yönünde de çalışmaları olmalıdır. Bu yaklaşım, veri denetçilerinin hareketlerinde daha sorumlu olmaları yönünde de olumlu sonuçlar verecektir²⁴⁸. Veri koruma otoritelerinin zorlayıcı yetkilerini kullanmaları çeşitli durumlarda söz konusu olur. Örnek olarak şikayet ya da basın yoluyla veri koruma düzenlemelerinin ihlal edildiğine ilişkin bir bilgi alınması verilebilir. Bunun yanında veri koruma otoriteleri kendi araştırma ve denetleme programlarını da kurmuş olabilirler. Bu sistemler kapsamında veri denetçilerinin ilkelere uygun hareket edip etmediği denetlenebilir ve veri denetçilerinin üzerlerine düşen yükümlülükleri daha iyi anlamaları sağlanabilir²⁴⁹.

Gelişen teknoloji ile kişisel verilerin korunmasının zorluğu veri koruma otoritelerinin üzerine düşen görevi daha önemli hale getirmektedir. Nitekim çeşitli bölgelerden pek çok önemli sivil toplum kuruluşunun imzasını taşıyan 2007

²⁴⁶ AB Veri Koruma Yönergesi, m. 28/3.

²⁴⁷ AB Veri Koruma Yönergesi, m.28/6.

²⁴⁸ Peter HUSTINX, "The Role of Data Protection Authorities", s. 135.

²⁴⁹ Article 29 Data Protection Working Party, **Declaration of the Article 29 Working Party on Enforcement**, WP 101, 25 Kasım 2004, s. 3.

Montreal Bildirgesi'nde bu soruna işaret edilmiş ve veri koruma otoritelerinin *"toplumun temel değerlerinin ve özel yaşamın gizliliği hakkının savunulmasında benzersiz bir konumda"* olduğuna işaret edilmiştir. Bu bağlamda artan tehditler karşısında daha etkin mücadelelerin bir gereklilik olduğuna işaret edilmiştir²⁵⁰.

B. BİLDİRİM VE LİSANS VERME UYGULAMALARI

Avrupa'da konuya ilişkin ulusal düzenlemelerde verileri toplayan ve işleyenlerin hareketlerini denetlemeyi sağlayacak özel kurallara yer verilmiştir²⁵¹. Bu kurallar ülkeden ülkeye çeşitlilik gösterir. Veri Koruma Yönergesi'nde benimsenen sistem ise kişisel verilerin işlenmesi düşünüldüğünde, bu konuda veri koruma otoritesinin bilgilendirilmesini öngörmektedir²⁵². Bildirim yükümlülüğü çoğu zaman bir kayıt sistemi içerisinde gerçekleştirilmektedir²⁵³. Sınırlı uygulaması olan bir diğer yöntem ise veri denetçisinin veri koruma otoritesinden bir kayıt sistemi oluşturmadan veya veri işleme etkinliği yapmadan önce özel bir izin, lisans almasıdır. Bu ikinci yöntemin uygulamasının daha çok, kredi raporlama, uluslararası veri aktarımı, veri eşleştirme gibi özel bazı alanlarda tercih edildiği görülmektedir²⁵⁴.

Yönerge, hem verileri işleyen ve toplayanların, hem veri işleme etkinliğinin kaydını öngörmektedir. Bunun sonucunda, Avrupa'da kural olarak, tamamen özel ve kişisel faaliyetler dışında, hiç kimse devletin haberi olmaksızın verileri toplayamayacak ve işleyemeyecektir²⁵⁵. Ancak belirtmek gerekir: üye devletler bildirim yükümlülüğüne bazı durumlarda istisna getirilmesini öngörebilir²⁵⁶. Yine

²⁵⁰ Declaration of Civil Society Organizations on the Role of Data Protection and Privacy Commissioners Montréal, September 25, 2007, <http://thepublicvoice.org/events/montreal07/declaration.pdf> par. 8.

²⁵¹ Buna karşın verilerin korunmasına ilişkin uluslararası belgelerde genel olarak bildirim ve lisans gibi konulara ilişkin özel düzenlemelerden kaçınıldığı görülmektedir.

²⁵² Lee A. BYGRAVE, **Data Protection Law**, s. 75.

²⁵³ Örneğin Birleşik Krallık'ta konuya ilişkin sicil, ICO tarafından tutulmaktadır. Veri denetçileri bu kuruma bazı bilgileri, belirli bir ücret ile birlikte vermekle yükümlüdürler. Bu bilgi telefon ya da kurumun web sitesinde yer alan form aracılığıyla iletilebilmektedir. Ardından ICO, bu bilgileri Birleşik Krallık veri denetçileri sicilene işlemektedir. Bu bildirimin amacı ise, veri denetçileri ile ilgili bilgilere kamunun rahatlıkla ulaşabilmesini sağlamaktır. Bkz. Peter CAREY, **Data Protection**, s. 125.

²⁵⁴ Lee A. BYGRAVE, **Data Protection Law**, s. 76.

²⁵⁵ Fred H. CATE, **Privacy in the Information Age**, s. 47.

²⁵⁶ Veri Koruma Yönergesi, m. 18/2. Üye devletlerin yaklaşımlarındaki çeşitliliğe ilişkin olarak bkz. Article 29 Data Protection Working Party, **Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union**, WP 106, 18 Ocak 2005.

bildirim kapsamında sunulacak bilgilerin içeriğini saptamakta da üye devletlerin takdir hakkı bulunur. Bu bağlamda Yönerge yalnızca bildirim kapsamında sunulması gereken asgari bilgileri belirlemiştir²⁵⁷. Buna göre bildirimde en azından şu hususlar yer almalıdır:

- denetçinin ve, eğer varsa, temsilcisinin adı ve adresi;
- veri işlemenin amaçları;
- ilgili kişinin kategorileri;
- verinin iletileceği alıcıların kategorileri;
- üçüncü ülkelere önerilen ver transferleri;
- işlemenin güvenliğini sağlayan önlemlerin genel tanımı.

Veri Koruma Yönergesi'nin 18. maddesinde düzenlenen "*bildirim*" konusunu, 20. maddede düzenlenen "*ön denetim*"den ayırmak gerekir. Ön denetim, bazı veri türlerinin özel bir risk taşıyıp taşımadığının önceden incelenmesini gerektirmektedir²⁵⁸. Bildirim, kimi zaman veri işlemenin incelenmesi sonucunu getirebilir. Ancak bu, her durumda söz konusu değildir. Ön denetim ise, özel risk taşıdığı düşünülen bazı durumlarda işlemenin önceden incelenmesi anlamına gelir²⁵⁹. Bu bağlamda ön denetimin sınırlı bir uygulama alanının bulunduğu da belirtilmelidir²⁶⁰.

²⁵⁷ Veri Koruma Yönergesi, m. 19/1. Buna göre bildirimde en azından şu hususlar yer almalıdır: (i) denetçinin ve, eğer varsa, temsilcisinin adı ve adresi; (ii) veri işlemenin amaçları; (iii) ilgili kişinin kategorileri; (iv) verinin iletileceği alıcıların kategorileri; (v) üçüncü ülkelere önerilen ver transferleri; (vi) işlemenin güvenliğini sağlayan önlemlerin genel tanımı.

²⁵⁸ Veri Koruma Yönergesi'nin 20/1 hükmü şu ifadeyi içermektedir: "*Üye Devletler, ilgili kişilerin hak ve özgürlüklerine yönelik özel riskler oluşturabilecek işleme etkinliklerini belirleyecek ve bunların işleme başlamadan önce kontrol edilip edilmediğini inceleyecektir*". Pek çok devlette bu işlem, Veri Koruma Otoritelerince yapılmaktadır. Ancak örneğin Almanya'da bu denetimi veri koruma görevlisi adlı bir kurum gerçekleştirmektedir. Christopher KUNER, s. 250. Federal Almanya Veri Koruma Yasası'nın 4d/5,6 hükümleri uyarınca otomatik işleme etkinlikleri ilgili kişinin hak ve özgürlükleri açısından risk taşıdığı için ön denetime tabi tutulmalıdır. Ön denetim özellikle özel kategorideki (hassas) kişisel verilerin işlenmesinde veya ilgili kişinin kişiliğine ilişkin bir değerlendirme yapma niyetiyle yapılan işlemlerde söz konusu olacaktır. Bu durumun istisnaları, yasal bir zorunluluk bulunması, ilgili kişinin rızasının alınması, toplama, işleme ve kullanmanın ilgili kişiyle yapılan bir sözleşmeden kaynaklanması durumlarıdır.

²⁵⁹ Christopher KUNER, s. 250.

²⁶⁰ Nitekim bu duruma Yönerge'de de işaret edilmiştir. Yönerge'nin başlangıç bölümü 53. paragrafına göre; belirli bazı işleme etkinlikleri özleri, kapsamı veya amaçları nedeniyle ilgili kişilerin hak ve özgürlükleri açısından özel riskler taşıyabilirler. Bu risk, kişinin yönelik bir haktan, çıkardan veya sözleşmeden mahrum bırakılmasından kaynaklanabileceği gibi, yeni bir teknolojinin kullanımı nedeniyle de ortaya çıkabilir. Bu durumda Üye Devletler, kendi tercihlerine göre ulusal hukuk sistemlerinde bu riskleri belirleyebilirler. Yönerge'nin başlangıç bölümü 54. paragrafında ise bu gibi özel risk yaratan işlemlerin oldukça sınırlı olduğuna işaret edilmiştir.

C. YARGI YOLLARI VE YAPTIRIM

Avrupa’da veri koruma yasalarının tamamında, ilgili hükümlerin ihlali durumunda başvurulacak hukuksal yollar ve uygulanacak yaptırımlar düzenlenmiştir. Bu düzenlemeler, genellikle para ve hapis cezaları, tazminat, lisansın ya da tescil kaydının iptali gibi hükümler içerir²⁶¹.

Yargı yolları ve yaptırım konusuna, AK Sözleşmesi, OECD ve BM Rehber İlkeleri ile APEC Çerçeve Belgesi’nde oldukça sınırlı bir şekilde değinilmiştir. Veri Koruma Yönergesi’nde ise çeşitli hükümler altında özel ve ayrıntılı olarak düzenlendiği görülür. Buna göre Üye Devletler, Yönerge hükümlerinin etkin bir şekilde uygulamasını sağlamak için gerekli önlemleri almalıdır²⁶².

İlk olarak Yönerge’nin 22. maddesi uyarınca ilgili kişilerin veri koruma otoritesine başvurmadan doğrudan mahkemeye erişimlerine izin verme üye devletlerin takdirine bırakılmıştır. Ayrıca Veri Koruma Yönergesi’nde hukuka aykırı işlemler sonucunda ortaya çıkan zararın giderilmesine yönelik çeşitli yollar öngörülmüştür. İlk olarak Yönerge uyarınca, ilgili kişilerin zarardan sorumlu olan veri denetçisinden tazminat alma hakkı bulunur²⁶³. Ancak denetçi, zarara neden olan olaydan sorumlu olmadığını kanıtlarsa sorumluluktan kısmen ya da tamamen muaf tutulabilir²⁶⁴. Buradaki “zarar” kavramının hem maddi hem de manevi kayıpları

²⁶¹ Lee A. BYGRAVE, **Data Protection Law**, s. 77; Fleeming MOOS, s. 176.

²⁶² Veri Koruma Yönergesi, m. 24.

²⁶³ Veri Koruma Yönergesi, m. 23/1. Bu noktada Üye Devletlerin farklı uygulamalarının dikkat çektiğini hatırlatmak gerekir. Farklılık çeşitli açılardan kendini göstermektedir. Örneğin Avusturya veri koruma mevzuatı uyarınca veri denetçisinin sorumluluğu ancak kusurlu olduğu durumlarda söz konusudur. Oysa Almanya uygulamasında veri denetçisi kamusal bir organsa tazminat, onun adına yapılan herhangi bir hatada söz konusu olacaktır. Alfred BÜLLESBACH ve diğ., s. 99. Alman veri koruma mevzuatı uyarınca tazminat talebinin şartı kasti ya da ihmali hareketi dolayısıyla zararın doğumuna bizzat o makamın sebep olmasıdır. Eğer veri denetçisi somut olayın özel koşulları uyarınca gereken ihtimamı göstermişse tazminat sorumluluğundan kurtulabilir. Bkz. Federal Almanya Veri Koruma Yasası, m. 7. Yasanın 7. madde hükmü yalnızca maddi zararlara ilişkindir. Ancak bunun yanında Almanya’da verilerin korunması ilkelerinin ihlal edilmesi dolayısıyla kişilerin uğradıkları zararlar başka bazı hükümler uyarınca tazminat konusu olabilir. Alman Medeni Kanununun ilgili hükümleri buradaki temel dayanaktır. Ancak bu noktada ihmalin ciddi olması ve zararın başka türlü giderilemiyor olması gerekir. Bkz. Fleeming MOOS, s. 176. Bu noktada Federal Almanya Veri Koruma Yasasının 8. maddesinde ise kamu makamlarının tazminat sorumluluğuna ilişkin tamamlayıcı hükümleri içerdiği belirtilmelidir. Burada kişisel verilerin otomatik yöntemlerle hukuka aykırı şekilde toplanması, işlenmesi ve kullanılması durumunda söz konusu olacak tazminat sorumluluğuna ilişkin ilkeler ayrıca belirlenmiştir.

²⁶⁴ Veri Koruma Yönergesi, m. 23/2. Kimi ülkeler ulusal hukuk sistemlerinde bu istisnayı Yönerge’den daha geniş bir şekilde yorumlamışlardır. Örneğin Birleşik Krallık’ta eğer veri

karşılıyıp karşılamadığı açık değildir. Ancak metnin başlangıç bölümü de dikkate alındığında buradaki bu deyim geniş yorumlanması gerektiği söylenebilir²⁶⁵.

Uygulamada veri koruma ilkelerinin ihlali durumunda para veya hapis cezalarındansa daha hafif yöntemlerle sorunların çözülmeye çalışıldığı, kamusal tartışmaya açıldığı ve karşılıklı diyalog sağlanmaya gayret gösterildiği görülmektedir²⁶⁶. Ancak hukuka aykırı veri işlemeye ilişkin çeşitli davalarda büyük şirketlere karşı ciddi meblağlarda cezaya hükmedildiği bilinmektedir²⁶⁷. Davalının kişiler olduğu durumlarda ise daha makul cezalar dikkat çekmektedir²⁶⁸.

denetçisi hukuka aykırı işlemeyi önlemek için gereken özeni göstermişse sorumluluktan kurtulabilmektedir. Peter CAREY, **Data Protection**, s. 45.

²⁶⁵ Lee A. BYGRAVE, **Data Protection Law**, s. 78-79. Nitekim Yönerge'nin başlangıç bölümünde, metnin ulusal hukuklardaki koruma sistemini ya da AİHS'nin 8. maddesindeki güvence sistemini zayıflatmasının düşünülemeyeceğine dikkat çekilmiştir(par. 10). Ayrıca yine başlangıç bölümünde, ilgili kişinin yakındığı "herhangi bir" zarardan söz edilmektedir(par. 55). Ancak Bygrave, "herhangi" deyiminin yalnızca Yönerge'nin İngilizce metninde yer aldığına, Fransızca, Almanca, Danimarkaca ve İsveççe metinlerinin hiçbirinde bu sıfatın bulunmadığına dikkat çekmektedir. Bkz. **a.g.e.** s. 79, d.n. 305.

²⁶⁶ Lee A. BYGRAVE, **Data Protection Law**, s. 79. AB üyesi çeşitli devletlerin uygulamalarından örnekler için bkz. Article 29 Data Protection Working Party, Recent examples of enforcement actions caried out by data Protection authorities, Ocak 2005, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp101a_en.pdf.

²⁶⁷ Örneğin İspanyol telefon şirketi Telefónica 2000 yılında, aynı grup içerisindeki bir başka şirkete (Telefónica Data) kişisel verileri aktarması dolayısıyla yapılan şikâyet üzerine, verilerin toplanma amacıyla uyumşayan şekilde işlenmesi, bunun ilgililerin rızası alınmaksızın gerçekleştirilmesi ve yine ilgililerin rızası olmaksızın üçüncü bir kişiye aktarılması dolayısıyla 420.708.47 Euro para cezasına çarptırılmıştır. Bkz. Alfred BÜLLESBACH ve diğ., s. 99. Bir başka örnek olarak ise Danimarka ticaret mahkemesinin bir kararı gösterilebilir. Mart 2005'te Danimarka Ticaret Mahkemesi, bir cep telefonu operatörü aleyhine, rakip firmanın müşterilerine çok sayıda kısa mesaj (SMS) ve e-posta göndermesi nedeniyle, iki milyon Danimarka Kromu(yaklaşık 270.000 Euro) para cezasına hükmetmiştir. Bkz. Christopher KUNER, s. 56.

²⁶⁸ Bireye karşı hükmedilen para cezalarının en bilinen örneği Bodil Lindqvist kararıdır. ATAD önüne de gelen bu davada İsveç Mahkemeleri, işleme için veri koruma otoritesinden uygun izni almaması ve aynı eksikliğin bulunmasına karşın hassas kişisel verileri işlemesi dolayısıyla Bodil Lindqvist'i 4,000 SEK para cezasına ve suç mağdurlarına yardım fonuna da 300 SEK ödemeye mahkûm edilmiştir. Alfred BÜLLESBACH ve diğ., s. 99. Bir başka örnek, Fransa'dan verilebilir. 2004 yılında Fransa Ticaret Mahkemesi, tahminen bir milyonun üzerinde istenmeyen ticari ileti gönderen Fransız iş adamı aleyhine 22.000 Euro para cezasına hükmetmiştir. Bkz. christopher KUNER, s. 490.

DÖRDÜNCÜ BÖLÜM

TÜRKİYE’DE KİŞİSEL VERİLERİN KORUNMASI

I. GENEL OLARAK

Çalışmamızın önceki bölümlerinde kişisel verilerin, temel hak ve özgürlükler içerisindeki yeri, uluslararası kaynakları ve korunmasının gerekliliğini, ayrıca bu alandaki temel ilkeleri genel olarak tanıtmaya çalıştık. Görüldüğü gibi hızla gelişen teknoloji ve bilginin küresel akışı insan haklarına saygılı yönetimlerde kişisel verilerin korunmasına kayıtsız kalınmasını gittikçe güçleştirmektedir. Nitekim günümüz dünyasında bir yandan kişisel verilere daha yüksek oranda gereksinim duyulurken, diğer yandan kişilerin özel yaşamlarına yönelik saldırılar da hızla artmaktadır. Bu, konuya ilişkin hukuksal düzenlemeler yapılması zorunluluğunu beraberinde getirir. Nitekim OECD, AK, BM, APEC gibi amaç, hedef ve etkileri birbirlerinden farklı uluslararası kuruluşların ve uluslarüstü bir kuruluş olan AB’nin verilerin korunmasına yönelik asgari ilkeler ile sınırötesi veri aktarımına ilişkin kuralların belirlendiği metinleri benimsemesi bunun en açık göstergesidir. Başta Avrupalı devletler olmak üzere Kanada, Avustralya, Japonya, İsrail gibi dünyanın çeşitli bölgelerinden demokratik devletler de kişisel verilerin korunmasını ulusal hukuk düzenlerinin bir parçası haline getirmiştir.

Kişisel verilerin korunmasına ilişkin ulusal hukuk sistemimizdeki düzenlemelerin incelenmesine geçmeden önce Türkiye’nin bu genel tablo içerisindeki yerine değinmek yararlı olabilir. Her şeyden önce Türkiye’de, teknolojiye ilişkin gelişmeler yakından izlenmektedir. Teknoloji ürünleri günlük yaşamın bir parçası haline gelmiştir. Türkiye’de İnternet kullanımı hızla artmakta ve bu ortamdaki Türkçe içerikler her geçen gün biraz daha çeşitlenmektedir¹. Pek çok kişi

¹ Türkiye İstatistik Kurumu’nun hane halkı bilişim teknolojileri kullanım araştırması sonuçlarına göre İnternet’e erişimi olan hane oranı 2007’de %19,7 iken, 2009’da %30’dur. Araştırma sonuçlarına göre 2009 yılında 16-74 yaş grubundaki bireylerde bilgisayar ve İnternet kullanım oranları sırasıyla erkeklerde % 50,5 ve % 48,6, kadınlarda % 30,0 ve % 28,0’dır. Bkz. <http://www.tuik.gov.tr> .

araştırmak, sosyal iletişim ağlarına bağlanmak, ekonomik etkinliklerde bulunmak ya da yalnızca eğlenmek için İnternet'i kullanmaktadır. Cep telefonları, kapalı devre televizyon sistemleri, RFID gibi ürünlerin, sosyal paylaşım ağlarının yaygın kullanımı dikkat çekmektedir. Bu eylemlerin her biri veri üretmekte, dolayısıyla kişisel veriler kimi zaman ilgili kişiler farkında bile olmadan, kimi zaman ise kendi istekleri ile bir yerlerde kayıt altında tutulmaktadır. Pek çok özel kuruluş bilişim teknolojilerini etkin bir şekilde kullanmaktadır. Özel teşebbüsler, bankalar, kütüphaneler bu alanda verilebilecek bir kaç örnektir. Bunun yanında kamu kurumları da pek çok işlemi elektronik ortamda gerçekleştirmekte, güvenlik güçleri görevlerini yerine getirebilmek için artan oranda teknoloji ürünlerinden yararlanmaktadır. Aşağıda incelenecek Merkezi Nüfus İdaresi Sistemi gibi kapsamlı veri tabanları kurulmakta ve kullanımları hızla yaygınlaşmaktadır.

O halde Türkiye'de hızla gelişen teknolojinin yakından izlendiği söylenebilir. Ne yazık ki aynı şeyi kişisel verilerin korunmasına ilişkin hukuksal düzenlemeler açısından söyleyebilmek olanaklı değildir. Kişilerin bu konuda hukuksal güvencelere kavuşturulmasında Türkiye, gelişmiş devletlerin oldukça gerisinde kalmıştır. Ülkemizde kapsayıcı bir kişisel verilerin korunması yasası bulunmamaktadır. Aşağıda incelenecek Kişisel Verilerin Korunması Kanun Tasarısı halen ilgili komisyondadır. AK Veri Koruma Sözleşmesi, Türkiye tarafından 28 Ocak 1981 tarihinde imzalanmış olmasına karşın konuya ilişkin yasal düzenleme halen yapılmadığından onaylama işlemi tamamlanamamaktadır. Ancak bu durum Türkiye'de kişisel verilerin tamamen korumasız olduğu anlamına gelmez. Aşağıda inceleneceği üzere kişisel verilerin korunmasının Anayasada oldukça sağlam dayanakları bulunmaktadır. Türk Medeni Kanunu, Türk Ceza Kanunu gibi temel metinlerde bazı güvencelerin tanındığı görülmektedir. Bunun yanında mevzuatımızda dağınık bir şekilde yer alan konuya ilişkin çeşitli hükümlerin bulunduğu görülmektedir. Aslında bu durum, pek de şaşırtıcı değildir. Nitekim kişisel verilerin toplanması, kullanılması, işlenmesi ile ilgili olmayan bir alan neredeyse bulunmamaktadır. Dolayısıyla hem özel, hem kamu hukuku kapsamında çok çeşitli alanlarda konuya ilişkin düzenlemeler bulmak olanaklıdır. Burada özellikle son dönemde kabul edilen metinlerde kişisel verilerin korunmasının artık göz ardı edilememesinin de etkisi olduğu söylenebilir.

Aşağıda yalnızca Türkiye’de konuya ilişkin hukuksal durumun ne olduğunu ortaya koymak için öne çıkan bazı alanlardaki düzenlemelere değinilecektir. Kişisel verilerin korunmasının anayasal temelleri değerlendirildikten sonra incelenecek düzenlemeler kuşkusuz yalnızca örnekleme niteliğindedir. Nitekim kişisel verilerin korunması ile ilişkili olan hukuksal metinlerin tam listesi bu çalışmanın amacını aşacak niteliktedir. Dolayısıyla öncelikle temel bazı yasal düzenlemeler bu çerçevede değerlendirilecek, ardından da öne çıkan bazı tartışma noktaları dikkate alınarak belirli konular üzerinde durulacaktır. Örneğin özel hukuk açısından işçilerin kişisel verilerinin korunması, iş ilişkisinin özel niteliği dolayısıyla konuya ilişkin tartışmalarda özel olarak yer verilen bir alanı oluşturmaktadır. Kamu hukuku alanında ise merkezi veri tabanlarına ilişkin çeşitli tartışmalar vergi mahremiyetinin ve sağlık verilerinin korunması bu kapsamda sayılabilir².

II. KİŞİSEL VERİLERİN KORUNMASININ ANAYASAL TEMELLERİ

A. GENEL OLARAK

Türkiye Cumhuriyeti Anayasasında kişisel verilerin korunmasına temel hak ve özgürlükler içerisinde ayrı bir yer verilmemiştir. Ancak bu durum konunun anayasal temelden yoksun olduğu anlamına gelmez. Anayasa’da kişisel verilerin korunmasına dayanak oluşturan önemli hak ve özgürlükler hüküm altına alınmıştır. Nitekim kişisel verilerin korunması alanında kapsayıcı hukuksal düzenlemeleri benimsemiş ülkelerin büyük bir bölümünde de durum böyledir. Pek çok ulusal hukuk sisteminde bu önemli alan, anayasal kaynağını özel yaşamın gizliliği hakkında bulur³. Bunun yanında örneğin Fransa’da kişisel verilerin korunması hakkı

² Son dönemde öne çıkan alanlar arasından mali veriler, sağlık verileri ve küçüklere ilişkin veriler bulunduğuna ilişkin bir değerlendirme için bkz. Jeffrey H. MATSUURA, **A Manager’s Guide to the Law and Economics of Data Networks**, Artech House, ABD 2000, s. 74.

³ Günümüzde pek çok devletin anayasasında, en azında konut dokunulmazlığını ve haberleşmenin gizliliğini koruyacak şekilde, özel yaşamın gizliliği hakkı temel bir hak alanı olarak tanınmıştır. Bunun yanında ABD, Kanada gibi kimi ülkelerin anayasalarında doğrudan ve açık bir şekilde bu hak alanı düzenlenmemiş olsa da mevcut hükümler çerçevesinde ilerleyen dönemlerde başta yüksek mahkeme kararları olmak üzere çeşitli yorum biçimleri ile özel yaşamın gizliliğinin yurttaşların temel bir hak olarak belirlendiği görülür. ABD’de özel yaşamın gizliliği hakkının gelişimi Warren ve Brandeis’in makalesinin yayınlanmasının ardından peşi sıra verilen Supreme

anayasada yer alan “özgürlük” hakkına dayandırılmıştır⁴. Almanya’da ise, daha önce belirttiğimiz gibi, bilgilerin geleceğini belirleme hakkı anayasal temelini “*genel kişilik hakkı*”nda bulmaktadır. O halde kişisel verilerin korunmasının anayasal temelini başta özel yaşamın gizliliği hakkı olmak üzere çağdaş, demokratik anayasalarda korunan çeşitli hak ve özgürlüklerde bulduğunu söyleyebiliriz. Bu durum ulusal ve uluslararası metinlere de yansımakta, bu bakımdan özel yaşamın gizliliği hakkı baskın olmakla birlikte, düzenlemelerin hedeflerinde çeşitlilik dikkat çekmektedir⁵.

Court kararları ile olmuştur. Bir başka Kuzey Amerika ülkesi olan Kanada’nın ise kişisel verilerin korunmasına yaklaşımı ABD’dekinden oldukça farklıdır. Aslında Kanada’da ABD’deki uygulamaya benzer şekilde özel yaşamın gizliliği anayasal bir hak değildir. Ancak Kanada Mahkemeleri özel yaşamın gizliliği hakkını Anayasa’ya 1982 yılında eklenen Kanada Haklar ve Özgürlükler Şartı’nın 8. maddesi kapsamında değerlendirmiştir. Kanada Yüksek Mahkemesi’ne göre, yetkisiz arama ve el koymalara karşı bireysel güvenliği sağlayan bu hükümde amaç, devletin özel yaşama yetkisiz müdahalelerine karşı mekânları değil insanları korumaktır. Şartın 8. maddesi kapsamında özel yaşamın korunmasının düzeyi, olayın somut koşullarına göre ilgilinin makul beklentisine bağlıdır. Bunun yanında bazı mahkemeler, özel yaşamın gizliliği hakkının Şartın “*Kişinin yaşamı, özgürlüğü ve güvenliği*”ni düzenleyen 7. maddesi ile temellendirilebileceğini ileri sürmüştür. Nitekim Kanada Yüksek Mahkemesi de tıbbi kayıtlar, kişinin fiziksel bütünlüğü, yoğun olarak kişisel kararları ilgilendiren konularda 7. maddeden kaynaklanan bir özel yaşamın gizliliği hakkının bulunabileceğini belirtmiştir. Bkz. Jason M. YOUNG, “Condtitutional Rights and New Technologies in Canada”, **Constitutonal Rights and New Technologies, A comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States**, haz. Bert-Jaap KOOPS, Ronald LEENES, Paul De HERT, Tilburg University, Hollanda 2007, s. 43-44; **Privacy and Human Rights 2006**, s. 308. Özel yaşamın gizliliğinin doğrudan anayasal güvence altında olmadığı Japonya’da ise 1963 yılında Japonya Yüksek Mahkemesi özel yaşamın gizliliği hakkını, 1946 Anayasasının yaşam, özgürlük ve mutluluğu arama haklarını düzenleyen 13. maddesinin kapsamında yorumlamıştır. **Privacy and Human Rights 2006**, s. 593.

⁴ **International Encyclopedia of Laws**, haz. R. BLANPAIN, **Constitutional Law**, C.3, haz. A. ALEN, Fransa Bölümü (Bu bölüm Michel FROMONT ve diğ. Tarafından hazırlanmıştır), Kluwer Law International, Hollanda 1999, s. 256-259. Fransız Anayasasında özel yaşamın gizliliği hakkının kaynaklarına ilişkin ayrıca bkz. John BELL, **French Constitutional Law**, Clarendon Press, Birleşik Krallık 1998, s. 147-148.

⁵ AB Yönergeleri, AK Sözleşmesi yanında pek çok ulusal düzenlemede özel yaşamın korunması hedefine atıf yapıldığı görülmektedir. Örneğin Federal Almanya Veri Koruma Yasası m.1/f.1’de yasanın amacı şöyle belirtilmiştir: “*Bireyin özel yaşamının gizliliği hakkının kişisel verilerinin kullanılması yoluyla ihlal edilmesini önlemektir*”. Bunun yanında kişisel verilerin korunmasında AB sisteminden ayrılan ABD, Kanada, Avusturalya gibi ülkelerde konuya ilişkin yasaların genelde Özel Yaşamın Gizliliği Yasası (privacy act) olarak adlandırılması da buna işaret etmektedir. Ancak Avrupa’da bazı veri koruma yasalarında özel yaşamın gizliliğinin korunmasına açıkça atıfta bulunulmadığı görülmektedir. İsviçre Veri Koruma Yasasında “*kişilik*”e, İsveç’te ise “*kişisel bütünlük*”e atıf yapılması örnek olarak gösterilebilir. Bygrave’e göre, “*hedeflerin böylesine geniş bir şekilde düzenlenmesi, yalnızca veri koruma yasalarının resmi mantığından çok daha fazla değere dayandırılabilmesini sağlamakla kalmaz, ayrıca insan hakları külliyatı ile normatif bağlarının güçlenmesine de hizmet eder. Ancak bir şekilde paradoksal olarak, böylesine geniş bir düzenleme veri koruma yasalarının özel yaşamın gizliliği hakkından başka, tam olarak hangi menfaatleri koruduğunun belirsizliğini de maskeleyebilir*”. Lee A. BYGRAVE, **Data Protection Law**, s. 38.

Bu Anayasaların büyük bir bölümü, henüz kişisel verilerin korunması bir hak alanı olarak tartışılmaya başlamadan önce kabul edilmiştir. Bu nedenle kişisel verilerin korunmasına özel olarak yer verilmemesi anayasal temelden yoksun olduğu anlamına gelmez. Bununla birlikte daha yeni kaleme alınmış çeşitli anayasalarda özel olarak bir kişinin kişisel verilerine ulaşma ve onu denetleme hakkının düzenlendiği de görülmektedir⁶. Portekiz, Hollanda ve İspanya Anayasaları burada verilebilecek bir kaç örnektir⁷. AB Temel Haklar Şartında da kişisel verilerin korunması ayrı bir hüküm ile güvence altına alınmıştır⁸.

Kişisel verilerin korunmasının başta özel yaşamın gizliliği hakkı ve kişinin maddi ve manevi bütünlüğü olmak üzere çeşitli temel hak ve özgürlüklerle yakından ilişkilidir. Dolayısıyla kişisel verilerin korunması, anayasal temelini bu hükümlerde bulabilmektedir. Ancak bunun yanında tam ve etkin koruma sağlayabilmek için konuya ilişkin özel bir düzenlemeye de gereksinim duyulmaktadır. Bu, kaynağını yine özel yaşamın gizliliği hakkında bulan haberleşme özgürlüğüne ya da temel felsefesi düşüncüyü açıklama özgürlüğüne dayanan basın özgürlüğüne benzetilerek açıklanabilir. Belirtilen temel hak ve özgürlüklerde olduğu gibi kişisel verilerin korunması da felsefi temelini bir başka hakta bulmakta ancak zaman içerisinde adeta o hak alanının sınırlarına sığmayacak şekilde geliştiğinden ayrı bir hak kategorisi olarak tanınmaya başlamıştır.

B. ANAYASA TASLAK VE ÖNERİLERİNDE KİŞİSEL VERİLERİN KORUNMASI HAKKI

Her ne kadar 1982 Anayasasında kişisel verilerin korunması hakkının sağlam dayanakları bulunsa da bu hakkın Anayasada özel olarak düzenlenmesinin bazı yararları olacağı da açıktır. Bu, her şeyden önce Anayasa koyucunun konuya verdiği özel önemin bir göstergesi olacak ve uygulayıcıları bu konuda daha duyarlı olmaya yönlendirecektir. Türkiye’de özellikle son dönemdeki Anayasa önerilerinde kişisel

⁶ **Privacy and Human Rights 2006, An International Survey of Privacy Laws and Developments**, Electronic Privacy Information Center and Privacy International, ABD 2007, s. 45.

⁷ Hollanda Anayasasında konunun düzenlenişine ilişkin genel bilgi için bkz. **International Encyclopedia of Laws**, haz. R. BLANPAIN, **Constitutional Law**, C.5, haz. A. ALLEN, Hollanda Bölümü (Bu bölüm Constantijn A.J.M. KORTMANN, Paul P.T. BOVEND’EERT tarafından hazırlanmıştır), Kluwer Law International, Hollanda 2000, s. 156.

⁸ ABTHŞ, m. 8.

verilerin korunmasına bağımsız bir hak olarak yer verildiği görülmektedir⁹. Olasılıkla bu yeni eğilimde 2000 yılında kabul edilen AB Temel Haklar Şartında kişisel verilerin korunmasının ayrı bir hüküm altında düzenlenmesi etkili olmuştur.¹⁰.

Burada değerlendirilebilecek ilk metin, Türkiye Barolar Birliği'nin bünyesinde hazırlanan Anayasa Önerisidir. Önerinin 33. maddesi “*Kişisel bilgi ve verilerin korunması*” kenar başlığını taşır¹¹ ve burada şu hüküm düzenlenir:

“(1)Herkes kendi yaşamına ve varlığına ilişkin özel bilgi ve verilerin gizli tutulmasını ve korunmasını isteme hakkına sahiptir. Bu bilgiler, ancak kişinin iznine veya kanunda öngörülen hukukun geçerli sayacağı başka bir nedene dayalı olarak kullanılabilir. (2) Herkes, kendisi hakkında toplanmış olan veya bilişim kayıtlarında yer alan bilgilere erişme, bunlarda düzeltme yaptırma ve bu bilgilerin amaçları doğrultusunda kullanılıp kullanılmadığını bilme hakkına sahiptir. (3) Bu kuralların uygulanması, kanunla kurulmuş bağımsız bir makam tarafından sağlanır ve denetlenir”.

Önerinin gerekçesinde de konunun artan önemine ve bağımsız bir organın gerekliliğine dikkat çekildiği görülmektedir. Nitekim gerekçede şu ifadeler yer alır:

“Herkesin kendi yaşamına ait duyarlı bilgi ve verilerin gizli tutulmasını ve korunmasını isteme hakkının güvence altına alınması, çağdaş iletişim araçlarındaki gelişimin doğurduğu bir gereksinim olarak düşünülmüştür. Bilişim sektöründe ortaya çıkan karmaşık sorunları düzenlemek ve insan hakları ihlallerinin önüne geçmek amacıyla uzman ve özerk bir birimin oluşturulması öngörülmektedir”.

⁹ Anayasa taslak ve önerilerine ilişkin genel bir değerlendirme için bkz. Serap YAZICI, **Yeni Bir Anayasa Hazırlığı ve Türkiye, Seçkincilikten Toplum Sözleşmesine**, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2009.

¹⁰ Nitekim bu tarihten önce açıklanan çeşitli önerilerde böylesine bir tercih görülmemektedir. Örneğin **Türkiye Odalar ve Borsalar Birliği TC Anayasa Önerisi** Anayasa 2000, Ankara 2000; **TBMM’de Temsil Edilen Siyasi Partilerin Anayasa Değişikliği Tekliflerinin Karşılaştırmalı Metinleri**, TBMM Başkanlığı, Ankara Mart 1993; Zafer ÜSKÜL, **Geniş Tabanlı Bir Uzlaşma Anlayışı için Karşılaştırmalı Anayasa Taslağı ve Anayasa Anketi**, Yayın no. 1, Toplumda Diyalog Forumu, Nisan 1992.

¹¹ Bkz. **Türkiye Cumhuriyeti Anayasa Önerisi**, Türkiye Barolar Birliği, Geliştirilmiş Gerekçeli Yeni Metin, 4. Baskı, Kasım 2007 Ankara. Bu metin, Prof. Dr. Rona AYBAY, Prof. Dr. Fazıl SAĞLAM, Prof. Dr. Süheyl BATUM, Prof. Dr. Oktay UYGUN, Doç. Dr. Korkut KANADOĞLU, Yard. Doç. Dr. Ece GÖZTEPE, Yard. Doç. Dr. Faruk BİLİR ve Koordinatör üye Av. Teoman ERGÜL tarafından hazırlanmış ve Türkiye Barolar Birliği Yönetim Kurulunun incelemesinin ardından Yasama Meclisinin ve kamuoyunun değerlendirmesine sunulmuştur.

Bu gerekçeden hareketle ilgili hükümde, kişisel verilerin korunması hakkı tanındığı gibi, bazı temel ilkelere vurgu da yapılmış ve ayrıca bağımsız bir denetim organının kurulması öngörülmüştür. Bu yaklaşım, ABTHŞ’na da uygundur.

Bunun yanında temel hak ve özgürlükler içerisinde kişisel verilerin korunmasının bağımsız olarak düzenlendiği tek Anayasa önerisi TBB tarafından sunulmamıştır. Eylül 2007 tarihinde Adalet ve Kalkınma Partisi’nin Prof. Dr. Ergun Özbudun başkanlığında bir bilim kuruluna hazırlattığı¹² anayasa taslağında da kişisel verilerin korunmasına ayrı bir hüküm içinde yer verildiği görülmektedir. Taslağın “*Kişisel bilgilerin korunması*” kenar başlıklı 20. maddesi şu hükmü içerir:

“(1) Herkes, kendisiyle ilgili kişisel bilgi ve verilerin korunması hakkına sahiptir. (2) Bu bilgiler, ancak kişinin açık rızasına veya kanunla öngörülen meşru bir sebebe dayalı olarak kullanılabilir. Herkes, kendisi hakkında toplanmış olan veya kayıtlarda yer alan bilgilere erişme, bunlarda düzeltme yaptırma ve bu bilgilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme hakkına sahiptir”.

Burada da kişisel verilerin korunması temel bir hak olarak düzenlenmiş ve konuya ilişkin bazı ilkelere anayasal güvence tanınmıştır. Ancak ilginç olan AB Temel Haklar Şartı ve TBB’nin Anayasa Önerisinin aksine burada kişisel verilerin işlenmesini denetleyecek bağımsız bir organının kurulmasına yer verilmemiş olmasıdır¹³. Oysa çalışmamızın üçüncü bölümünde de belirttiğimiz üzere etkin ve tam bir koruma için bağımsız bir denetim organı önemli bir gerekliliktir.

Bu ve benzeri taslak ve öneriler kabul edilip yürürlüğe girinceye kadar kişisel verilerin korunmasının anayasal dayanağını mevcut hükümler incelenerek belirlemek

¹² Kurulun diğer üyeleri, Prof. Dr. Zühtü ARSLAN, Prof. Dr. Yavuz ATAR, Prof. Dr. Fazıl Hüsnü ERDEM, Prof. Dr. Levent KÖKER ve Doç. Dr. Serap YAZICI’dır. Anayasa taslağının tam metni için bkz. <http://arsiv.ntvmsnbc.com/news/419856.asp>.

¹³ UYGUN bu eksikliği, belirtilen taslağın genel yapısını da dikkate alarak eleştirmiştir. Yazara göre belirtilen Anayasa taslağında böyle bir kuruma yer verilmemesi şaşırtıcı değildir: “*Getirdiği düzenlemelerle Hakimler ve Savcılar Yüksek Kurulu, Anayasa Mahkemesi, Danıştay ve Yüksek Öğretim Kurulu’nu Mecliste oluşan çoğunluk iradesine göre biçimlendirmeyi amaçlayan bir taslakta, bu konuda hükümetin hiyerarşik yönetimine tabi olmayan bağımsız bir kurula yer verilmesi beklenemezdi. Bağımsız, tarafsız kurullar çoğulcu demokrasi anlayışının ürünüdür. Özbudun metni ise, 1924 Anayasası’ndan esinlenen çoğunlukçu demokrasi anlayışını temel almıştır. O nedenle, yargı dahil tüm kamusal kurum ve organları Mecliste oluşan çoğunluk iradesi ve o iradenin desteğindeki hükümete tabi kılmak istemektedir*”. Bkz. Oktay UYGUN, “İnsan Hakları Açısından Yeni Anayasa Çalışmaları”, Maltepe Üniversitesi Hukuk Fakültesi’nde 28 Nisan 2008 tarihinde düzenlenen “Güncel Anayasa Sorunları” başlıklı sempozyumda sunulan bildiri metni, s. 12.

gerekecektir. Anayasada doğrudan düzenlenmesinin önemli yararları bulunmakla birlikte, bu gerçekleşinceye kadar Türkiye’de kişisel verilerin korunması hakkı anayasal temelden yoksun olmadığı gibi, oldukça güçlü dayanaklarının bulunduğu söylenebilir.

C. ANAYASANIN İLGİLİ HÜKÜMLERİ

1. İnsan Onuru ve Kişinin Maddi ve Manevi Varlığını Geliştirme Hakkı

Türkiye Cumhuriyeti Anayasasında kişisel verilerin korunmasının normatif temelini oluşturacak çeşitli hükümler bulunmaktadır. Öncelikle kişinin maddi ve manevi varlığını geliştirme hakkını dikkate almak gerekir¹⁴. Anayasanın Başlangıç 6. paragrafında ve 17/1 hükmünde kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı hüküm altına alınmıştır. Ayrıca 5. maddede “Devletin temel amaç ve görevleri” arasında “insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak” yer alır.

İnsanın maddi ve manevi varlığını geliştirme hakkı kaynağını hak ve özgürlüklerin ortak temeli olan insan onurunda bulur¹⁵. Ancak insan onuru tanımlanması oldukça güç bir kavramdır. Türk Anayasa Mahkemesine göre insan onuru kavramı “insanın ne durumda, hangi şartlar altında bulunursa bulunsun sırf insan oluşunun kazandırdığı değer tanınmasını ve sayılmasını anlatır. Bu öyle bir davranış çizgisidir ki ondan aşağı düşünce, muamele ona muhatap olan insanı insan olmaktan çıkarır”¹⁶.

Federal Almanya Anayasa Mahkemesi ise insan onurunun ihlal edilip edilmediğine ilişkin değerlendirmelerinde “obje formülü”nden yararlanmaktadır. Buna göre eğer insan, kamu erkinin etkinlikleri karşısında basit bir obje veya araç haline indirgeniyorsa insan onurunun ihlalinden söz edilir¹⁷. Obje formülü kişisel

¹⁴ Nitekim Federal Almanya Anayasa Mahkemesinin Nüfus kararında da benzer bir hareket noktası olduğu söylenebilir. Yukarıda da belirtildiği gibi bu kararda Mahkeme, “bilgilerin geleceğini belirleme hakkı”nın anayasal temelini kişiliğin serbestçe geliştirilmesi hakkı ile insan onurunda bulmuştur. Bkz. BVerfGE 65, 1.

¹⁵ İbrahim Ö. KABOĞLU, **Özgürlükler Hukuku**, s. 25. Kimi yazarlara göre ise “(b)ütün temel haklar, Anayasa madde 17’den çıkarılan “insanın maddi ve manevi varlığını geliştirme hakkı” olan temel özgürlük hakkının sonuçları olarak kabul edilmekte ve bu olgu Anayasadaki temel haklar içinde hiyerarşi olarak yorumlanmaktadır”. Zafer GÖREN, **Anayasa Hukukuna Giriş**, İzmir 1999, s. 412.

¹⁶ AYMK, E. 1963/132, K. 1966/29, t. 28 Haziran 1966; Ömer İZGİ, Zafer GÖREN, **Türkiye Cumhuriyeti Anayasası Yorumu**, Ankara 2002, s. 216.

¹⁷ BVerfGE 9, 89, 95; 27, 250, 275’den aktaran Oğuz ŞİMŞEK, s. 130.

verilerin korunmasının anayasal temeli ve ayrıca önemi konusunda ipuçları vermektedir. Nitekim bu çalışmanın birinci bölümünde incelendiği üzere gelişen teknoloji ve kişilerin farklı kaynaklardan sürekli olarak gözetimi, bireysel özerkliğin kaybına neden olabileceği gibi, otomatik karar alma süreçleri ile yaşamına yön verilen kişi bir öznenen nesneye doğru evrilebilir. Oysa kendisine ilişkin bilgileri, ne zaman, nasıl, ne oranda ve kimlere açıklayacağına öncelikle kişinin kendisi karar vermelidir. Bu konuda karar verme gücünü kaybeden birey öznenen nesneye dönüşeceği gibi, maddi ve manevi varlığını geliştirme hakkını da kaybedecektir. Çalışmamızın başından beri tekrar tekrar üzerinde durulduğu gibi, kişisel verilerin korunması hakkı, mutlak bir hak değildir, belirli durumlarda sınırlandırılabilir. Ancak burada kilit kavram bu durumların “*belirli*” olmasıdır. Kişinin hangi durumlarda hakkının sınırlandırılacağını bilmesi, bu sınırların da meşru temellere dayanması gerekir. Böylece kişi, kişisel verileri konusunda karar verme gücünü elinde tutmaya devam edebilir.

2. Özel Yaşamın Gizliliği Hakkı

İkinci olarak kişisel verilerin korunması hakkının anayasal temellerini özel yaşamın gizliliği hakkında bulmak olanaklıdır. Yukarıda da belirtildiği gibi konuya ilişkin pek çok ulusal ve uluslararası düzenlemede hedef olarak özel yaşamın gizliliği hakkı gösterilmektedir. Çalışmamızın birinci bölümünde açıklandığı üzere kişisel verilerin korunması kaynağını öncelikle özel yaşamın gizliliği hakkında bulmaktadır. Bu nedenle Türkiye’de kişisel verilerin korunmasının anayasal temelleri araştırılırken özel yaşamın gizliliği hakkına ilişkin düzenlemeyi de dikkate almak gerekir.

Türkiye’de 1982 Anayasası’nın 20. maddesinde özel yaşamın gizliliği hakkı güvence altına alınmıştır¹⁸. Belirtilen hükmün 1. fıkrasına göre “*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz*”. 2001 yılında bu cümleden sonra gelen adli soruşturma ve kovuşturmanın gerektirdiği istisnalar dışında bunların gizliliğine

¹⁸ Bu hak ülkemizde anayasal düzeyde ilk kez 1961 Anayasasının 15. maddesi ile tanınmıştır. 1961 Anayasasının 15. maddesinin 1971 yılında değiştirilmiş şekli şu hükmü içermekteydi: “(1)Özel hayatın gizliliğine dokunulamaz. (2)Adli kovuşturmanın gerektirdiği istisnalar saklıdır. Kanunun açıkça gösterdiği hallerde, usulüne göre verilmiş hâkim kararı olmadıkça; millî güvenlik veya kamu düzeni bakımından gecikmede sakınca bulunan hallerde de kanunla yetkili kılınan merciin emri bulunmadıkça kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz”.

dokunulamayacağı hükmü ilga edilmiştir. Dolayısıyla hakkın özel sınırlama sebepleri için artık yalnızca 20. maddenin 2. fıkrası dikkate alınmalıdır. Anayasanın 20/2 hükmünde kişilerin üstünün, özel kâğıtlarının ve eşyasının aranması ve bunlara el konulmasının hangi koşullar altında gerçekleşebileceği belirlenmiştir. Bir başka anlatımla hakkın özel bir görünümüne ilişkin sınırlar çizilmiştir. Ayrıca Anayasada herkesin haberleşme özgürlüğüne sahip olduğu, kural olarak haberleşmenin gizliliği ve ancak belirli durumlarda sınırlandırılabilmesi hükmü altına alınmıştır¹⁹.

Bu durumda özel yaşamın gizliliği hakkının sınırlarını kişisel verilerin korunması açısından değerlendirmek gerekir. Bu değerlendirmede öncelikle 2001 yılında gerçekleştirilen Anayasa değişikliklerinin temel hak ve özgürlükleri sınırlamanın sınırlarını belirleyen 13. maddedeki düzenleme dikkatten kaçmamalıdır. Buna göre:

“Temel hak ve özgürlükler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz”.

Anayasada yapılan bu değişiklik ile yasa koyucunun bir genel sınırlama nedenine dayanarak temel hak ve özgürlükleri sınırlaması önlenmek istenmiştir²⁰. Bu hüküm kişisel verilerin korunması konusunda birkaç açıdan önemlidir:

¹⁹ Anayasanın 22. maddesi şu hükmü içerir: “(1) Herkes haberleşme hürriyetine sahiptir. (2) Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya bir kaçına bağlı olarak usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakim onayına sunulur. Hakim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. (3) İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir”.

²⁰ Nitekim 2001 yılı öncesinde Anayasanın 13. maddesinde temel hak ve özgürlüklerin genel sınırlamaları belirlenmekteydi. Buna göre hükmün ilk şekli şöyleydi: “(1) Temel hak ve hürriyetler, Devletin ülkesi ve milletiyle bölünmez bütünlüğünün, milli egemenliğin, Cumhuriyetin, milli güvenliğin, kamu düzeninin, genel asayişin, kamu yararının, genel ahlakın ve genel sağlığın korunması amacı ile ve ayrıca Anayasanın ilgili maddelerinde öngörülen özel sebeplerle, Anayasanın sözüne ve ruhuna uygun olarak kanunla sınırlanabilir. (2) Temel hak ve hürriyetlerle ilgili genel ve özel sınırlamalar demokratik toplum düzeninin gereklerine aykırı olamaz ve öngörüldükleri amaç dışında kullanılamaz. (3) Bu maddede yer alan genel sınırlama sebepleri temel hak ve hürriyetlerin tümü için geçerlidir”. 2001 yılı değişiklikleri kapsamında madde AİHS’nde yer alan ilkeler doğrultusunda yeniden düzenlenmiştir. Bkz. 3 Kasım 2001 tarihli 4709 sayılı yasanın gerekçesi; Ömer İZGİ, Zafer GÖREN, s. 183.

Öncelikle Anayasanın özel yaşamın gizliliği ve haberleşme özgürlüğüne ilişkin hükümleri ile temel hak ve özgürlüklerin sınırlandırılmasının sınırlarını belirleyen 13. madde hükmünün birlikte okunması gerekir. 13. madde hükmünde açıkça temel hak ve özgürlüklerin “*yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak*” sınırlandırılabilmesi ifade edilmektedir. 20. maddenin 2. fıkrasındaki sınırlama ise yalnızca kişilerin üstünün, özel kâğıtlarının ve eşyasının aranması ve bunlara el konulmasına ilişkindir. Belirli açılardan kişisel verilerin korunması kapsamında değerlendirilebilecek konut dokunulmazlığı ve haberleşme özgürlüğüne getirilebilecek sınırlamaların kuralları ise 21. ve 22. maddelerde düzenlenmiştir. O halde özel yaşamın gizliliği hakkının, belirtilen özel görünümüleri dışında Anayasa’da mutlak olarak korunduğu söylenebilir. Bu, kişisel verilerin korunmasına ilişkin anayasal temelin ne kadar güçlü olduğunun bir göstergesidir. İkinci olarak Anayasanın belirtilen hükümleri kapsamında sınırlandırılma getirilecek olsa bile bunun mutlaka 13. maddede belirlenen kurallara uygun olarak gerçekleştirilmesi gerekir.

3. Düşünce Özgürlüğü

Anayasanın 25. maddesinde “*düşünce ve kanaat hürriyeti*”, 26. maddesinde ise “*Düşünceyi açıklama ve yayma hürriyeti*” düzenlenmiştir. Düşünceyi açıklama özgürlüğüne ilişkin hükümde ve bu alanla yakından ilişkili izleyen hükümlerde hak ve özgürlüklerin hangi durumlarda sınırlandırılabilmesi belirtilmiştir. 25. maddede yer alan düşünce ve kanaat özgürlüğünün ise mutlak olarak korunduğu görülmektedir. Buna göre “*Herkes, düşünce ve kanaat hürriyetine sahiptir. Her ne sebep ve amaçla olursa olsun kimse, düşünce ve kanaatlerini açıklamaya zorlanamaz; düşünce ve kanaatleri sebebiyle kınanamaz ve suçlanamaz*”. Anayasanın 15/2 hükmü uyarınca savaş, seferberlik, sıkıyönetim ve olağanüstü hallerde dahi “*kimse din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanamaz*”.

Bu alanın mutlak olarak korunması doğaldır. Nitekim herhangi bir anlatım aracıyla dış dünyaya yansımamış, insanların yalnızca zihinlerinde kurguladıkları düşüncelere sınırlama getirilmesi söz konusu olamaz. Hatta bu saptamadan hareketle düşünce özgürlüğünün ayrı bir koruma alanına gereksinim göstermediği de

düşünülebilir²¹. Oysa kişisel veriler açısından, özellikle İnternet kullanımı dikkate alındığında, korumanın mutlak niteliği oldukça önemli bir sonucu beraberinde getirmektedir.

Bu çalışmanın birinci bölümünde de işaret edildiği üzere İnternet üzerindeki her hareketimiz bir iz bırakmaktadır. Sanal ortamda alışveriş yapan, forumları ziyaret eden, çeşitli kuruluşların yayınladığı haberleri okuyan bir kişinin bu hareketlerine ilişkin bilgilerin toplanıp ayrıntılı bir profilinin oluşturulması kimi durumlarda özel yaşamın gizliliği hakkı yanında düşünce özgürlüğünün de ihlali anlamına gelebilir.

²¹ Öğretide düşünce özgürlüğü ile düşünceyi açıklama özgürlüğünün 1982 Anayasasında ayrı düzenlemelerin konusu olması önemli tartışmalara neden olmuştur. Her iki alan arasında ayırım yapılmasına gerek bulunup bulunmadığına ilişkin tartışmalar özellikle 1961 Anayasasındaki düzenleme şeklindeki farklılıktan kaynaklanır. 1961 Anayasasında düşünce özgürlüğü ve düşünceyi açıklama özgürlüğü bir arada düzenlenmiştir. 1961 Anayasasının “Düşünce hürriyeti” kenar başlıklı 20. maddesi uyarınca “*Herkes, düşünce ve kanaat hürriyetine sahiptir; düşünce ve kanaatlerini söz, yazı, resim ile veya başka yollarla, tek başına veya toplu olarak açıklayabilir ve yayabilir*”. 1982 Anayasasındaki düzenleme şekli ise iki açıdan tartışma konusu olmuştur. Birincisi Anayasadaki temel hak ve özgürlükler yaklaşımına ilişkindir. Yukarıda da işaret edildiği üzere, 2001 değişiklikleri öncesinde Anayasanın 13. maddesi genel sınırlama hükmü niteliğindeydi. Bu durumda 25. maddede düzenlenen ve insanın iç dünyası ile ilişkili düşünce özgürlüğüne bile sınırlama getirilmesi söz konusuydu. 13. maddenin yeni şekliyle bu sorunun ortadan kalktığı söylenebilir. İkincisi ise düşünce özgürlüğünün ayrı bir düzenleme alanına gereksinin gösterip göstermediğine ilişkindir. Öğretide konuya ilişkin değerlendirmelerin çeşitlendiği görülmektedir. Örneğin GÖLCÜKLÜ, düşünce özgürlüğünün statik, yani insanın iç dünyasında kalan durağan bir nitelikte iken, düşünceyi açıklama özgürlüğünün dinamik niteliğine dikkat çekmekte ve iki özgürlük alanının birbirinden ayrılması gerektiğini savunmaktadır. Bkz. Feyyaz GÖLCÜKLÜ, **Haberleşme Hukuku**, AÜSBFY no. 292, Ankara 1970, s. 4-6. ÖKÇESİZ ise konuyu farklı bir açıdan değerlendirmiştir. Yazara göre açıklama ve bilgilenme özgürlükleri düşünce özgürlüğünün gerçekleşmesine hizmet eden temel özgürlüklerdir. Ancak açıklama ve bilgilenme özgürlüklerinin “*kullanılmasında içerik olarak her zaman bir düşüncenin yer alması zorunlu değildir. Bu durum, düşünce içerikli açıklama ve bilgilenme özgürlüğü ile, düşünce içermeyen açıklama ve bilgilenme özgürlüğünün sınırları bakımından, daha ayrıntılı bir çalışmayı gerekli kılmaktadır*”. Bkz. Hayrettin ÖKÇESİZ, “Düşünce Özgürlüğü Üzerine Düşünceler”, **Hukuk Felsefesi ve Sosyolojisi Arkivi**, Haz. Hayrettin ÖKÇESİZ, 6. Kitap, İstanbul Barosu Yayınları, İstanbul 2003, s. 30. Buna karşın kimi yazarlar bu ayırımın sakıncalarına işaret etmektedir. Örneğin TANÖR’e göre “*düşünce özgürlüğü*”nü düşünceleri ifade etmekten ayırarak korumak, onu “*düşünme özgürlüğü*”ne indirmek olur. Bkz. Bülent TANÖR, Türkiye’nin İnsan Hakları Sorunu, s. 59. ÖZEK ise düşünce özgürlüğünün niteliği gereği düşüncenin açıklanabilmesi hakkını ve olanağını içinde barındırdığına, düşünce özgürlüğü ile düşüncenin açıklanması özgürlüğünü ayırmanın bu özgürlüğün sınırlanması olanaklarını yaratacağına işaret etmektedir. Bkz. Mithat SANCAR, “Düşünce Özgürlüğü: Neden?”, **Çağdaş Hukuk**, Mayıs-Haziran 1994, s. 8-13. Çetin ÖZEK, **Türk Basın Hukuku**, İÜY no. 2381, İstanbul 1978, s.10. Aynı yönde bkz. Yılmaz ALİFENDİOĞLU, “Bir Temel İnsan Hakkı: Düşünce Özgürlüğü”, **Yeni Türkiye**, Y. 1998, S. 22, s. 805. Ayrıca bkz. Nevzat TOROSLU, “Medya ve Hukuk: Basın Özgürlüğü ve Sınırları”, **Medya Gücü ve Demokratik Kurumlar**, haz. Korkmaz ALEMDAR, Afa, İstanbul 1999, s. 56; İbrahim Ö. KABOĞLU, **Özgürlükler Hukuku**, s. 334-335; Sulhi DÖNMEZER, **Basın ve Hukuku**, İÜY no. 2213, 4. Baskı, İstanbul 1976; Reyhan SUNAY, **İfade Özgürlüğünün Muhtevası ve Sınırları**, Liberal Düşünce Topluluğu, Ankara 2001, s. 6-8; Mümtaz SOYSAL, **100 Soruda Anayasanın Anlamı**, Gerçek Yayınevi, 6. Baskı, İstanbul 1986, s. 212-213; Hayrettin ÖKÇESİZ, “Düşünce Özgürlüğü”, **İstanbul Barosu Dergisi**, Mart 1998, s. 23-26. Bu konuda genel bir değerlendirme için ayrıca bkz. Elif KÜZECİ, **Basın Özgürlüğü ve İnternet**, (Yayınlanmamış yüksek lisans tezi), s. 16-18.

Nitekim burada kişinin, düşüncesini açıklamak gibi bir iradesi bulunmamasına karşın, çeşitli ipuçlarından hareketle böylesine sonuçlar çıkarılması söz konusudur.

4. Diğer Bazı Temel Hak ve Özgürlükler

Yukarıdaki açıklamalar ışığında kişisel verilerin korunmasının anayasal temellerini öncelikle “*maddi ve manevi varlığını geliştirme hakkı*” ile “*özel yaşamın gizliliği hakkı*”nda ve bazı durumlarda “*düşünce özgürlüğü*”nde bulunduğunu söyleyebiliriz. Ancak bunun yanında Anayasada konuyla yakından ilişkili başka bazı hükümler de bulunmaktadır. Haberleşme özgürlüğü, din ve vicdan özgürlüğü, basın özgürlüğü, kanun önünde eşitlik ilkesi, suçsuzluk karinesi bu kapsamda sayılabilir. Ancak daha önce de işaret ettiğimiz gibi bu gibi hükümlerin getirdiği koruma oldukça sınırlıdır.

Örneğin kanun önünde eşitlik ilkesi, kişilerin, din, ırk, siyasal düşünce gibi bilgilerinin kayıt edilemeyeceğini değil, bunlara dayalı olarak kanun önünde herhangi bir ayırım gözetilemeyeceğini güvence altına almaktadır. Benzer şekilde din ve vicdan özgürlüğü de düşünce özgürlüğünde olduğu gibi kişilerin dini inanç ve kanaatlerini açıklamaya zorlanamayacağını, bunlardan dolayı kınanamayacağını ve suçlanamayacağını hüküm altına almaktadır. Bu ise kişisel verilerin korunması açısından ancak sınırlı bir güvence oluşturabilir. Haberleşme özgürlüğü, kişilerin özel iletişimlerinin korunması açısından önem ifade ederken, suçsuzluk karinesini özellikle suçluluğun önlenmesi için herkesin kayıt altına alınmasını öngören uygulamalar açısından değerlendirmek gerekir. Düşünceyi açıklama ve basın özgürlüğünün ise kimi durumlarda özel yaşamın gizliliği hakkı ile dengelenmesi gerekir. 1982 Anayasasına baktığımızda bu konudaki ilkenin oldukça açık bir şekilde belirlendiğini ve düşünceyi açıklama ve basın özgürlüklerinin “*başkalarının şöhret veya haklarının, özel ve aile hayatlarının*” korunması amacıyla sınırlanabileceği hüküm altına alındığı görülür²².

Bütün bu açıklamalar ışığında bireylerin kişisel verilerinin meşru bir temele dayanmadan işlendiği durumlarda gerekli güvencelere sahip olmasının Anayasanın

²² AY.’nın 28/3 hükmü uyarınca “*Basın hürriyetinin sınırlanmasında, Anayasanın 26 ve 27 nci maddeleri hükümleri uygulanır*”. “*Düşünceyi açıklama ve yayma hürriyeti*” kenar başlıklı 26. maddenin 2. fıkrasında ise “*Bu hürriyetlerin kullanılması, ... başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması ... amaçlarıyla sınırlanabilir*” hükmü yer almaktadır.

40. maddesinin de bir gereği olduğu belirtilmelidir. Nitekim 40. maddenin 1. fıkrası uyarınca *“Anayasa ile tanınmış hak ve hürriyetleri ihlal edilen herkes, yetkili makama geciktirilmeden başvurma imkânının sağlanmasını isteme hakkına sahiptir”*. Ayrıca *“(d)evlet, işlemlerinde, ilgili kişilerin hangi kanun yolları ve mercilere başvuracağını ve sürelerini belirtmek zorundadır”*²³. Kişisel verilerin korunmasının anayasal hak ve özgürlükler ile temellendirildiğini kabul ettiğimizde doğal olarak bu hakkı ihlal edilen kişilerin hukuksal koruma mekanizmalarından yararlanabilmesi gerekecektir.

Son olarak: kişisel verilerin korunması ile ilişkili bir diğer önemli Anayasa hükmü ise 90. maddede yer alır. 90. maddenin son fıkrası uyarınca usulüne göre yürürlüğe konulmuş andlaşmalar yasa hükmündedir ve bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz. Belirtilen hükme 2004 yılında şu kural eklenmiştir²⁴: *“Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma hükümleri esas alınır”*.

Yukarıdaki açıklamalarımızda da belirtildiği üzere AİHM, kişisel verilerin korunmasında temel ilkelerin büyük bir bölümünü Türkiye’nin de taraf olduğu AİHS’nin 8. maddesi kapsamında tanımaktadır. Sözleşme hükümlerinin sınır ve kapsamlarını belirleyebilmek için AİHM’nin yorumlarının önemi açıktır. O halde hem Anayasanın 90. madde hükmünün bir gereği olarak, hem de bu konuda geliştirilen içtihatlarla aykırı uygulamaların AİHM önünde ihlal kararı ile sonuçlandırılacağını dikkate alarak gereken düzenlemeler yapılmalı, konuya ilişkin temel ilkeler belirlenmelidir.

5. Anayasa Mahkemesi Kararları

Görüldüğü gibi kişisel verilerin korunması anayasal temelden yoksun değildir. Aksine oldukça sağlam normatif temellerini Türkiye Cumhuriyeti Anayasasında bulmak olanaklıdır. Daha önce de belirtildiği üzere kişisel verilerin korunmasını anayasalarında ayrı bir hak alanı olarak yer vermemiş çeşitli devletlerin yargı organları, geliştirdikleri içtihatlar ile bu normatif temeli belirlemiştir. AİHM de

²³ AY. m.40/2.

²⁴ 7 Mayıs 2004 tarihli, 5170 sayılı Yasa, m. 7.

kişisel verilerin korunmasında hâkim olan pek çok temel ilkeyi Sözleşme'nin özel yaşamın gizliliği hakkını düzenleyen 8. maddesinin kapsamında görmüştür.

Türkiye'de Anayasa Mahkemesinin de benzer bir anlayışı benimsediği söylenebilir. Mahkeme, her ne kadar geçmişte verdiği bazı kararlarda konuya ilişkin temel ilkeleri Anayasanın 20. maddesi çerçevesinde yorumlamada biraz isteksiz görünse de²⁵ yakın zamanda verdiği bir karar kişisel verilerin korunmasını özel yaşamın gizliliği hakkı ve düşünce özgürlüğü çerçevesinde değerlendirdiğini açıkça ortaya koymaktadır. Mahkeme 2008 yılında, 5429 sayılı Türkiye İstatistik Kanunu'nun istatistiksel birimlerin (yani haklarında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşların yetkilerinin) kendilerinden istenen veri veya bilgileri, vermekle yükümlü olduklarına ve bu yükümlülüğe uymayanların para cezası ile cezalandırılacaklarına ilişkin hükmün iptaline ona karşı bir oyla karar vermiştir²⁶.

Mahkeme kararında, öncelikle istatistikten söz edebilmek için verilere gereksinim duyulduğuna ve verilerin de en çok anketlere dayanılarak toplandığına işaret etmiştir. Mahkemeye göre:

“Maddede açıklayıcı bir düzenleme bulunmadığı için, “kişisel veri” veya “isteme bağlı veri” olarak adlandırılan, belirli veya belirlenebilir kişilerle

²⁵ Anayasa Mahkemesinin kişisel verilerin korunmasına ilişkin verdiği üç önemli karar bulunmaktadır. Bunlardan ilk ikisi nüfus cüzdanlarında din hanesinin bulunmasına ilişkindir. AYM, E. 1979/9, K.1979/44, t. 27 Kasım 1979; AYM, E. 1995/17, K.1995/16, t. 21 Haziran 1995. Kanımızca bu düzenleme din özgürlüğünden sonra özel yaşamın gizliliği hakkı ile de ilişkilidir. Yukarıda da işaret ettiğimiz gibi belirtilen olayda olduğu gibi kimi durumlarda din özgürlüğü de kişisel verilerin korunmasının anayasal dayanağı olabilir. Ancak Anayasa Mahkemesi yaptığı her iki incelemede de aile kütüklerinde ve nüfus cüzdanlarında din hanesinin bulunma zorunluluğunun Anayasaya aykırı olmadığına karar vermiştir. Anayasa Mahkemesinin konuya ilişkin bir diğer önemli kararı ise 1774 sayılı Kimlik Bildirme Kanununa eklenen bir hüküm ile genel kolluk kuvvetlerinin bilgisayarlarında kişisel bilgilerin toplanması yetkisini, bu yetki kullanılırken hangi kurallara uyulması gerektiği belirlenmeden, tanıyan hükmüne ilişkindir. Anayasa Mahkemesinin kararda kullandığı ifadeden kişisel verilerin korunmasının Anayasanın 20. maddesi kapsamında değerlendirildiği anlaşılmaktadır. Ancak Mahkeme, Anayasaya aykırılık iddiasının reddine karar vermiştir. Bu karara aşağıda tekrar değinilecektir. AYMK, E. 1996/68; K. 1999/1; t. 6 Ocak 1999.

²⁶ AYMK, E. 2006/167;K. 2008/86; t. 20.3.2008. Bu noktada Anayasa Mahkemesinin belirtilen kararının çalışmamızın çeşitli yerlerinde daha önce de belirtilen Federal Almanya Anayasa Mahkemesinin Nüfus Kararı ile konu bakımından bir benzerlik taşıdığını da belirtmek gerekir. Hatırlanacağı gibi bu karara konu olan olayda 1983 yılında yapılacak nüfus sayımında yurttaşlara yaptırma bağlı olarak istatistiksel amaçlarla kişisel bilgileri açıklama yükümlülüğü getiren Nüfus Sayımı Kanununun ilgili hükmü değerlendirilmişti. Federal Almanya Anayasa Mahkemesi kararında bu düzenlemenin bireyin “bilgilerin geleceğini belirleme hakkı”nı ihlal ettiğine karar vermiş ve bu karar, yalnızca Almanya’da değil, neredeyse bütün dünyada kişisel verilerin korunması yasalarının gelişimini etkilemiştir. Bkz. BVerfGE, 65, 1; Marie TINNEFELD ve diğ., s. 143 vd.; Oğuz ŞİMŞEK, s. 114 vd.

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 bilgilerin 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, istatistiki 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 kanaat özgürlüğüne 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. AIHM kararlarında da belirtildiği gibi, özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililer hakkında rızası olmaksızın bilgi toplamasının her zaman söz konusu kişinin özel hayatını ilgilendireceği 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 toplamının sınırlarına yasal düzenlemede yer verilmemiştir. Açıklanan nedenlerle itiraz konusu kuralların Anayasa'nın 20. ve 25. maddelerine aykırı olduğundan iptali gerekir”.

Görüldüğü gibi Anayasa Mahkemesi bu kararında kişisel verilerin korunması ile özel yaşamın gizliliği hakkı ve düşünceyi açıklama özgürlüğü arasındaki ilişkiyi

açıkça ortaya koyduğu gibi, yönetimin kişisel verileri işleme gücü karşısında bireyin korunmasının önemine de işaret etmiştir.

III. ÖZEL HUKUKTA KİŞİSEL VERİLERİN KORUNMASI

A. MEDENİ HUKUKTA KİŞİSEL VERİLERİN KORUNMASI

Kişisel verileri koruyucu bazı hükümleri, medeni hukuk kapsamında bulabilmek olanaklıdır. Nitekim kişilik hakkı kişisel değerlerin bütünü üzerinde geçerlidir²⁷. Kişilik hakkının genel nitelikli olduğu ve sınırlı sayımla belirlenmediği görüşü kabul edildiğinde teknik gelişme ve günlük yaşam gereklerinden doğacak değerlerin de bu kapsamda kabul edilmesi gerekir²⁸. O halde kişisel verilerin, kişilik hakkının bir parçası olduğu²⁹ ve bu kapsamda korunacağı söylenebilir. Hatırlanacağı üzere çalışmamızın çeşitli yerlerinde üzerinde durduğumuz Alman Anayasa Mahkemesi'nin Nüfus Sayımı Kararında da kişisel verilerin korunmasının genel kişilik hakkı kapsamında anayasal korumadan yararlanacağına hükmedilmiştir³⁰. Bu karar ile kişiliğin korunmasının insan hakları çerçevesinde yeniden değerlendirildiği görülmektedir. Aralarındaki yakın ilişki dolayısıyla kişisel verilerin korunması

²⁷ Kişilik ile kişisel değerlerden oluşan bir bütün anlaşılmaktadır. Kişinin maddi bedensel değerleri (beden bütünlüğü ve sağlığı gibi), manevi değerleri (onuru, saygınlığı, sır alanı, inancı, adı ve resmi üzerindeki hakkı gibi) ve bazı mesleki-ticari değerleri (mesleki ve ticari sırları, mesleki itibarı gibi) bu bütünün parçalarıdır. Bkz. Aydın ZEVLİLİLER, **Medeni Hukuk (Giriş, Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku)**, haz. Aydın ZEVLİLİLER, Beşir ACABEY, Emre GÖKYAYLA, 6. Baskı, Seçkin, Ankara 1999, s. 441; Jale AKİPEK, Turgut AKINTÜRK, **Türk Medeni Hukuku (Yeni Medeni Kanuna Uyarlanmış Başlangıç Hükümleri, Kişiler Hukuku)**, C. I, 4. Baskı, Beta, İstanbul 2002, s. 358

²⁸ Kişinin genel bir kişilik hakkına mı (allegemeines Persönlichkeitsrecht) yoksa kişisel değerlerinin her biri üzerinde ayrı ayrı kişilik haklarının mı bulunduğu ilişkin öğretilerdeki tartışma hakkında genel bir bilgi için bkz. Aydın ZEVLİLİLER, s. 442-444; Jale AKİPEK, Turgut AKINTÜRK, s. 361-365.

²⁹ Almanya, Fransa, İngiltere'de medeni hukuk düzenlemelerinde özel alanının korunmasının tarihsel gelişimi ve bugünkü durumuna ilişkin olarak bkz. Stephan BALTHASAR, **Der Schutz der Privatsphäre im Zivilrecht (Eine historisch-vergleichende Untersuchung zum deutschen, französischen und englischen Recht vom ius commune bis heute)**, Mohr Siebeck, Almanya 2006; James GORDLEY, **Foundations of Private Law (Property, Tort, Contract, Unjust Enrichment)**, Oxford University Press, Birleşik Krallık 2007, s. 217-262. Özel hukuk kapsamında onura özel yaşamın gizliliğine yönelik saldırılara karşı korunmaya ilişkin karşılaştırmalı bir değerlendirme için ayrıca bkz. James GORDLEY, Arthur Taylor Von MEHREN, **An Introduction to the Comparative Study of Private Law (Readings, Cases, Materials)**, Cambridge University Press, Birleşik Krallık 2006, s. 246-305.

³⁰ BVerfGE 65, 1.

yasalarının, özel hukuk anlamında kişiliğin korunmasının bir bölümünü somutlaştırdığı söylenebilir³¹.

Her biri kişisel veriler ile doğrudan ilişkili bulunan kişinin onur ve saygınlığı, adı ve resmi üzerindeki hakkı, sır alanı kişilik hakkının konusu içerisinde değerlendirilmektedir. Bu bağlamda özel yaşamın çeşitli görünümüne ilişkin yapılan ayırım hatırlanmalıdır. Hukuksal sonuçları da belirlemek amacıyla özel yaşam alanı genel olarak üçe ayrılarak incelenir³²:

- (i) kişinin öteki kişilerin bilgisinden uzak tuttuğu gizli yaşam alanı,
- (ii) kişinin kendisine yakın kişilerle paylaştığı ancak bunlar dışındakilerden gizli kalması gereken özel yaşam alanı ve
- (iii) toplumsal ilişkilere karışarak diğer bireylerle paylaştığı ortak yaşam alanı.

Kişinin, gizli ve özel yaşam alanına yönelen saldırılara karşı Türk Medeni Kanunu (MK) kapsamında belirli oranda korunduğu görülmektedir. Kişinin gizli alanına sızarak sırlarını öğrenme, teknik aygıt ve araçlarla kaydetme, resmini ve filmini çekme, ayrıca bunları yayma ve aktarma bu kapsamda kişiye yönelebilecek saldırıların türlerini oluşturmaktadır ve bunlara karşı MK m. 24, 25 ve Borçlar Kanunu (BK) m. 49 kapsamında koruma getirilmektedir³³. Çalışmamızın üçüncü

³¹ İsviçre Medeni Kanunun ilgili hükmü bakımından yapılan aynı yönde değerlendirme için bkz. Peter TUOR, Bernhard SCHNYDER, Jörg SCHMID, Alexandra RUMO-JUNGO, **Das Schweizerische Zivilgesetzbuch**, 13. Baskı, Schulthess, İsviçre 2009, s. 76-77, 100-101.

³² Aydın ZEVLİLER, s. 465-468; Bilge ÖZTAN, **Medeni Hukuk'un Temel Kavramları**, 8. Baskı, Turhan Kitabevi, Ankara 2002, s. 255.

³³ 24. maddesinde kişiliğe yönelik saldırılara karşı temel ilke, 25. maddede ise başvurabilecek hukuksal yollar belirlenmiştir. Yasanın 24/1 hükmü uyarınca “*Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hakimden saldırıda bulunanlara karşı korunmasını isteyebilir*”. MK’nın 23. maddesinde ise kişiliğin korunmasından vazgeçme ve aşırı sınırlamaya karşı ilke şu şekilde düzenlenmiştir: “(1) Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez. (2) Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlaka aykırı olarak sınırlayamaz. (3) Yazılı rıza üzerine insan kökenli biyolojik maddelerin alınması ve nakli mümkündür. Ancak, biyolojik madde verme borcu altına girmiş olandan edimini yerine getirmesi istenemez; maddi ve manevi tazminat isteminde bulunulamaz”. MK’nın belirtilen hükümleri mehz kanun İsviçre Medeni Kanununda 27 vd. maddelere karşılık gelmektedir. İsviçre Medeni Kanununun ilgili hükümlerinin yorumu için bkz. Peter TUOR ve diğ., s.99-124. Ayrıca milletlerarası özel hukukta İnternet de dahil kitle iletişim araçları ile “*kişisel verilerin işlenmesi veya kişisel veriler hakkında bilgi alma hakkının sınırlandırılması yolu ile kişiliğin ihlal edilmesinden doğan talepler*”de uygulanacak hukuk belirlenmiştir. Milletlerarası Özel Hukuk Ve Usul Hukuku Hakkında Kanunun (Kanun no. 5718; t. 27 Kasım 2007, RG. t. 12 Aralık 2007, S. 26728) 35. maddesi şu hükmü içermektedir: “(1) Kişilik haklarının, basın, radyo, televizyon gibi medya yoluyla, internet veya diğer kitle iletişim araçları ile ihlalinden doğan taleplere, zarar görenin seçimine göre; a) Zarar veren, zararın bu ülkede meydana geleceğini bilecek durumda ise zarar görenin

bölümünde incelenen temel ilkelerin bazılarının koruma kapsamında olduğu söylenebilir. Yine bu alana yönelen saldırıların meşru görüldüğü durumlar da konuya ilişkin ulusal ve uluslar arası düzenlemeler ile büyük oranda uyumludur. Sır ve özel yaşam alanı ihlal edilen kişinin rızasının bulunması, müdahalenin kamu yararının gerekliliklerinden kaynaklanması, tarihsel araştırmalar için kullanılması ya da başkalarının haklı çıkarları bu kapsamda sayılabilir³⁴.

O halde MK ve ilgili düzenlemelerin kişisel verilerin korunmasını belirli oranda sağladığı söylenebilir. Ancak birkaç açıdan bu koruma eksik kalmaktadır. Kişisel verilerin korunmasına ilişkin bu konudaki temel ilkelerin hüküm altına alındığı kapsayıcı bir yasanın gerekliliği hissedilmektedir. Nitekim örneğin İsviçre Medeni Kanununda hemen hemen aynı düzenlemeye yer verilmiş olmasına karşın, ayrıca bir kişisel verilerin korunması yasasının kabul edilmesinin nedeni de budur. İsviçre, Almanya gibi medeni hukuk sistemimizi yakından etkileyen ülkelerde kişilik haklarına ilişkin açıklamalarda kişisel verilerin korunmasına sıklıkla atıfta bulunulması da bunun bir göstergesidir. Kişisel verilerin korunması yasaları burada MK ile karşılanamayan bir korumayı getirmekte, bir anlamda onu tamamlamaktadır³⁵.

mutad meskeni hukuku,b) Zarar verenin işyeri veya mutad meskeninin bulunduğu ülke hukuku veya c) Zarar veren, zararın bu ülkede meydana geleceğini bilecek durumda ise zararın meydana geldiği ülke hukuku, uygulanır. (2) Kişilik haklarının ihlalinde cevap hakkı, süreli yayınlarda, münhasıran baskının yapıldığı ya da programın yayınlandığı ülke hukukuna tabidir.(3) Maddenin birinci fıkrası, kişisel verilerin işlenmesi veya kişisel veriler hakkında bilgi alma hakkının sınırlandırılması yolu ile kişiliğin ihlal edilmesinden doğan taleplere de uygulanır”.

³⁴ Aydın ZEVLİLER, s. 470-472. Nitekim MK’nın 24/2 hükmü şu şekildedir: “*Kişilik hakkı zedelenen kişinin 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*”. Bu istisnalardan kişinin rızasının geçerli kabul edilebilmesi için, rızayı verenin ayırt etme gücü bulunması ve rızanın hukuka, ahlaka, kamu düzenine aykırı olmaması gerekir. Rıza beyanı kural olarak açık ya da örtülü olarak verilebilir. Ancak ilgili yasada rızanın örneğin yazılı biçimde verilmesi emredilmişse buna uyulması gerekecektir. Bkz. Ömer Uğur GENÇCAN, **Türk Medeni Kanunu (Bilimsel Açıklama-İçtihatlar-İlgili Mevzuat, Madde 1-184)**, 2. Baskı, Yetkin, Ankara 2007, s. 246-249.

³⁵ **Münchener Kommentar zum Bürgerlichen Gesetzbuch**, C.1 (m.1-240), haz. Kurt REBMANN, Franz Jürgen SÄCKER, Roland RIXECKER, 4. Baskı, Beck, Almanya 2001, s. 267-268. AMSTUTZ ve diğ.ne göre İsviçre Medeni Kanununda konuya yönelik korumanın sınırlı kalmasının nedenlerinden biri de özel yaşamı yukarıda da işaret edilen alanlara ayırarak açıklama eğilimidir. Yazarlara göre çok basit ve zararsız gibi görülen bilgilerin toplamından ilgili olduğu kişiye yönelik ayrıntılı profillerin çıkarılması olanaklıdır. Bu nedenle üç alan teorisi ile sınırlanan koruma veri koruma yasaları ile tamamlanmaktadır. Bu anlamda Veri Koruma Yasasındaki düzenlemenin İsviçre Medeni Kanunun 28. madde hükmünü somutlaştırdığı söylenebilir. Ancak bu noktadaki bir sorun hangi durumlarda Medeni Kanuna hangi durumlarda Veri Korunma Kanununa dayanılacağının her zaman açık olmamasıdır. Marc AMSTUTZ ve diğ.,

MK'daki düzenlemelere karşın bu gereksinim birkaç nedenden kaynaklanır. Öncelikle kişisel verilerin korunmasında hakim olan temel ilkeler büyük oranda önleyici koruma sağlamaktır. Kişisel verilerin ancak toplandıkları amaç için kullanılabilecek olmaları, özel nitelikteki bazı veri kategorilerinin işlenmesinin kural olarak yasak olması ya da veri bankası oluşturan kişi ya da kurumların bir sicile kayıt olması gibi ilkeler bir zararın ortaya çıkmasını, kişisel verilerin korunması hakkının ihlal edilmesini önleyici niteliktedir. Oysa MK ve BK kapsamında getirilen koruma büyük oranda saldırının gerçekleşmesinden sonra işleyebilecek bir sistemi öngörür. Her ne kadar MK m.25/1 uyarınca “(d)avacı hakimden saldırı tehlikesinin önlenmesini” isteyebilse de bunun oldukça sınırlı bir uygulama alanı olacağı açıktır³⁶. Her şeyden önce böylesine bir istem ancak “halen mevcut olmamakla beraber, bir takım eylem ve belirtilerden çok yakın bir gelecekte kişilik haklarına karşı gerçekleşmesi pek mümkün ve olası görülen hukuka aykırı saldırılara karşı” söz konusu olabilir³⁷. Gelişen teknoloji, buna bağlı olarak kişisel verileri toplama kaynaklarının çeşitliliği, işleme ve kullanma alanlarının genişliği, bunlara yönelik usullerin hızı ve yaygınlığı dikkate alındığında böylesine yakın bir tehlikenin saptanmasının ancak çok sınırlı konularda söz konusu olabileceği açıkça görülür. İkinci olarak kişisel verilere yönelen saldırılar özel hukuk konusu olduğu gibi kamu hukuku konusu da olabilmektedir. Bu nedenle kişisel verilerin korunması yasası ile konuya ilkin temel ilkelerin belirlenmesi oldukça önemlidir. Nitekim kişisel

Handkommenter zum Schweizer Privatrecht, Schulthess 2007, s. 47. Ayrıca bkz. Dieter MEDKUS, **Allgemeiner Teil des BGB**, 9. Baskı, C.F.Müller, Almanya, 421-422.

³⁶ MK'nın 25. maddesi şu hükmü içermektedir: “(1) Davacı, hakimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespiti isteyebilir. (2) Davacı, bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir. (3) Davacının, maddi ve manevi tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekaletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır. (4) Manevi tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; miras bırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez. (5) Davacı, kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yeri mahkemesinde dava açabilir”. Kişiliğe hukuka aykırı saldırıların durdurulmasını sağlayan davalara ilişkin olarak ayrıca bkz. Jale AKİPEK, Turgut AKINTÜRK, s. 414-435. BK m. 49 hükmü ise şu şekildedir: “(1) Şahsiyet hakkı, hukuka aykırı bir şekilde tecavüze uğrayan kişi, uğradığı manevi zarara karşılık manevi tazminat namıyla bir miktar para ödenmesini dava edebilir. (2) Hakim, manevi tazminatın miktarını tayin ederken, tarafların sıfatını, işgal ettikleri makamı ve diğer sosyal ve ekonomik durumlarını da dikkate alır. (3) Hakim, bu tazminatın ödenmesi yerine, diğer bir tazmin sureti ikame veya ilave edebileceği gibi tecavüzü kınayan bir karar vermekle yetinebilir ve bu kararın basın yoluyla ilanına da hükmedebilir”.

³⁷ Jale AKİPEK, Turgut AKINTÜRK, s. 417.

verilerin korunması yasalarının büyük bir bölümünde hem kamu hukuku, hem de özel hukuka ilişkin bazı alanların kapsandığı görülmektedir³⁸.

B. İŞ HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

Kişisel öncelikler belirlenirken iş, sağlık ve aile yaşamı sonrasında belki de en önde gelen konudur. İş bulmak, işsiz kalmamak, huzurlu bir iş yaşamı sürdürmek bireysel tatmin açısından oldukça önemlidir. Ayrıca sosyal bir varlık olan insan, başkalarıyla ilişki kurmada önemli bir fırsata iş yaşamında kavuşmaktadır³⁹. Bunlar iş ile ilgili konuların bir kimsenin yaşamındaki yerine işaret eder. Bu derece önemli bir alanda kişinin korumasız bırakılması ise düşünülemez. Nitekim konuya ilişkin çalışmalar incelendiğinde işyerinde kişisel verilerin korunmasının üzerinde özel olarak durulduğu görülmektedir. Bunun bir nedeni, yukarıda işaret edildiği gibi işte geçirilen zamanın ve kurulan ilişkilerin insan yaşamı açısından önemidir. Ayrıca konu, iş ilişkisinin kendine özgü yapısı dolayısıyla da özellik arz etmektedir.

Nitekim bu ilişkinin kilit kavramlarından birini işçinin işverene bağımlılığı oluşturur. Elbette burada söz konusu edilen işçinin hukuksal bağımlılığıdır⁴⁰. Ancak öte yandan, işçi niteliğinin belirlenmesinde kullanılacak bir ölçüt olmasa da işçinin ekonomik bağımlılığının bulunduğunu kabul etmek gerekir⁴¹. Bütün bu özellikler işçinin kişisel verilerinin hukuksal olarak korunmasının gerekliliğine işaret eder. Ayrıca gelişen bilişim ürünlerinin işyerinde artan oranda kullanımı bu gerekliliği daha da arttırmaktadır. Bütün bunlar, işçinin kişisel verilerinin korunmasının yakından incelenmesine ve kimi yerlerde özel düzenlemeler ile korunmasına neden olmuştur⁴². Uluslararası düzenlemelere bakıldığında ise Uluslararası Çalışma

³⁸ Bu konuya ilişkin olarak ayrıca bkz. Hans Michael RIEMER, **Personenrecht des ZGB: Studienbuch und Bundesgerichtspraxis**, 2. Baskı, İsviçre 2002, s. 13-14.

³⁹ Nitekim AİHM de bu duruma işaret etmektedir. Mahkemeye göre “... insanların büyük bir bölümü, dış dünyayla ilişkilerini geliştirme konusunda, en önemli değilse bile, önemli bir olanağa iş yaşamları sırasında kavuşmaktadır”. Malone, Birleşik Krallık’a karşı, bn. 8691/79, kt. 2 Ağustos 1984, par. 29.

⁴⁰ İş sözleşmesinde bağımlılık unsurunun varlığı konusunda öğretide görüş birliği bulunmaktadır. Bkz. Sarper SÜZEK, **İş Hukuku**, 4. baskı, Beta, İstanbul 2008, s. 213.

⁴¹ K. Ahmet SEVİMLİ, **İşçinin Özel Yaşamına Müdahalenin Sınırları**, Legal, İstanbul 2006, s. 81.

⁴² Kimi ülkelerde işçinin özel yaşamının gizliliği, kişisel verilerin korunması yasaları yanında başka bazı hukuksal metinler ile de koruma altına alınmaktadır. Örneğin Belçika’da 2002 yılında işçilerin kişisel verilerini korumaya yönelik bir ulusal toplu iş sözleşmesi (Belgium’s National Collective Agreement No. 81 of 26 April 2002 on the protection of employees’ personal privacy with respect to the monitoring of electronic on-line communications data) kabul edilmiştir.

Örgütünün (International Labour Organization-ILO) konuya ilişkin bir Sözleşme kabul etmediği ancak işçinin kişisel verilerinin korunmasına ilişkin uygulama ilkelerini belirlediği görülmektedir⁴³.

Türkiye’de iş hukuku mevzuatı incelendiğinde bu konuda yeterli bir korumanın bulunmadığı görülür. İşçinin kişisel bilgilerinin kişilik haklarına zarar verecek şekilde kullanılması halinde, İş Kanunundaki bazı hükümlere başvurmak ve sorunu bu yolla çözmek olanaklıdır. Ancak bu düzenlemeler kişi için oldukça önemli olan iş yaşamında kişisel verilerinin korunması açısından yetersiz kalmaktadır. Belirtmek gerekir: işçinin kişisel verilerinin korunmasına ilişkin sorunlar, henüz iş ilişkisi kurulmadan başlamakta ve bu ilişkinin sona ermesinin ardından da devam etmektedir. Bu nedenle incelemeyi her bir aşamada ortaya çıkabilecek sorunları dikkate alarak yapmak gerekir.

Öncelikle işveren, iş sözleşmesi yapmayı düşündüğü kişinin işe uygun olup olmadığına karar verme aşamasında ondan bazı bilgiler isteyebilir. İşe başvuran kişinin, adı, soyadı, ikametgâh adresi, eğitim durumu, daha önce çalıştığı yerler ve buralardan aldığı referanslar bu kapsamda sayılabilir. Daha sonra başka sorunlar yaşanmaması için kişinin sabıka kaydının istenmesi de kimi durumlarda makul görülebilir. Burada önemli bir husus, işverenin başvuruda bulunan kişiye ilişkin bilgileri gizli tutması, bunları üçüncü kişilerle paylaşmaması gerekliliğidir.

Ayrıca işverenin bu bilgilere dayanarak yapacağı değerlendirmeyi ayrımcılık yasağını da dikkate alarak incelemek gerekir. Örneğin bir işverenin koruma görevlisi olarak çalışmak üzere yapılan başvuruları değerlendirirken, çeşitli darp olaylarına

İngilizce tam metni için bkz. Roger BLANPAIN, Marc Van GESTEL, **Use and Monitoring of E-mail, Intranet and Internet Facilities at Work**, Kluwer Law International, Hollanda 2004, s. 247-263. Ayrıca Fransa, Almanya, Birleşik Krallık, İtalya, Japonya ve ABD’nin ulusal hukuk sistemlerinde işçinin kişisel verilerinin korunmasına yönelik düzenlemelere ilişkin olarak bkz. Michele COLUCCI, **The Impact of the Internet and New Technologies on the Workplace, A Legal Analysis from a Comparative Point of View**, Kluwer Law International, Hollanda 2002, s. 71-166. Birleşik Krallık’a ilişkin olarak ayrıca bkz. Simon DEAKIN, Gilliam S. MORRIS, **Labour Law**, 4. Baskı, Hart Publishing, ABD 2006. ABD’de konuya ilişkin hukuksal düzenlemeler ve yargı kararları için bkz. David P. TWOMEY, **Labour and Employment Law, Text and Cases**, 11. Baskı, West, ABD 2001, s. 607-652.

⁴³ Uygulama ilkeleri, Sözleşmeler gibi bağlayıcı nitelikte olmasa da konuya ilişkin ulusal düzenlemelerde ya da toplu iş sözleşmelerinde yararlanılabilecek kaynakları oluştururlar. Nitekim işçilerin kendi beklentileri ve gereksinimleri yönünde bu metine şekil vermeleri olanaklıdır. ILO İşçinin Kişisel Verilerinin Korunmasına İlişkin Uygulama İlkeleri için bkz. Roger BLANPAIN, Marc Van GESTEL, s. 31-39. İşçinin çevrimiçi kişisel verilerinin korunmasına ilişkin olarak bkz. “Online Rights at Work-A UNI Code of Practice”, <http://onlinerights.wordpress.com/2009/03/06/online-rights-at-work-a-uni-code-of-practice/>.

karışmış bir kişiyi işe almak istememesi makul görülebilir⁴⁴. Ancak bu noktada bir başka soru ile karşılaşılır: geçmişte bir hata yapmış kişilerin bunun cezasını yaşam boyu çekmesi doğru bulunabilir mi? Böylesine bir düşünce, infaz sisteminin temel mantığına aykırı olmaz mı? Bu noktada sabıka sicil kayıtlarının belirli bir süre sonrasında silinmesinin kişilerin yaşam boyu cezalandırılmamaları için kabul edildiğini hatırlatmak gerekir. Nitekim yine bu nedenle işin niteliği ile ilgili olsa bile sabıkanın sicil kaydından silinmesi durumunda aday kendisini sabıkasız olarak tanıtabilir⁴⁵.

Bir diğer önemli husus, işe alımlarda başvurana yöneltilen soruların işin niteliği açısından bilinmesinde yarar bulunması gerekliliğidir. Bir başka anlatımla işverenin yalnızca merak duygusunu gidermek için işçiye soru yöneltilmesi uygun olmayacaktır. Bu bağlamda işin niteliği ile bağlantılı olmayan sorulara işçinin bilerek yanlış cevap vermesinin sonuçlarının ne olacağı düşünülebilir. Hatırlanacağı gibi çalışmamızın üçüncü bölümünde kimi yazarların savunduğu işçinin “*yalan söyleme hakkı*”ndan söz etmiştik⁴⁶. Buradaki temel düşünce, işçinin işin niteliği ile bağlantılı olmayan bir konuda kendisine yöneltilen bir soruyu yanıtsız bırakması durumunda potansiyel iş olanağını kaçırmamasının önüne geçmektir.

Türk hukuk mevzuatı açısından düşünüldüğünde yine işin niteliği açısından gereklilik koşuluna bakmak gerekecektir. Nitekim İş Kanununun⁴⁷ 25/II-a hükmü uyarınca “*İş sözleşmesi yapıldığı sırada bu sözleşmenin esaslı noktalarından biri için gerekli vasıflar ve şartlar kendisinde bulunmadığı halde bunların kendisinde bulunduğunu ileri sürerek yahut gerçeğe uygun olmayan bilgiler veya sözler söyleyerek işçinin işvereni yanıltması*” iş sözleşmesinin feshedilmesinde haklı sebep olarak düzenlenmiştir.

Görüldüğü gibi işçinin gerçeğe uygun olmayan bilgiler veya sözler söyleyerek işvereni yanıltmasının haklı sebep sayılabilmesi için bunun sözleşmenin esaslı noktalarından birine ilişkin olması gerekir. O halde esaslı noktaların dışındaki

⁴⁴ Harry HENDERSON, s. 30.

⁴⁵ Ahmet SEVİMLİ, s. 156-157. Ancak Yargıtay kararlarına göre görülecek işle ilgili bulunmasa bile işçinin var olan sabıkasını gizlemesi sözleşmenin feshi için haklı sebep oluşturur. Yargıtay’a göre “*İşçinin, işe girmeden önce müessir fiil suçundan hüküm giymiş olduğu halde, giriş formuna hiçbir sabıkası yani mahkumiyeti bulunmadığı şeklinde cevap vermesi ve daha sonra durumun ortaya çıkması, işverene işi fesih hakkı verir*”. Bkz. Yarg. 9. HD, 6 Haziran 2000, E. 2000/4727, K. 2000/7993.

⁴⁶ Marie-Theres TINNEFELD ve diğ., s. 68.

⁴⁷ Kanun no. 4857, t. 22 Mayıs 2003; RG. t. 10 Haziran 2003, S. 25134.

konularda yanıltıcı ifadelerin kullanılmasının haklı sebep oluşturmayacağını kabul etmek gerekir. Ayrıca işveren, adayın işe uygunluğunu değerlendirirken sendika üyeliğine ilişkin soru da yöneltemez. Nitekim Anayasa ve ilgili yasalarda⁴⁸ güvence altına alınan sendika özgürlüğü uyarınca işveren, sendikalı-sendikasız ayrımı yapamaz.

İş sözleşmesi, işçi ile işveren arasında kişisel bağ kuran ve güven ilişkisine dayanan bir sözleşmedir. Dolayısıyla işçinin işverenin ve iş yerinin çıkarlarını koruması gerektiği gibi, işveren de işçiye korumalı ve gözetmelidir⁴⁹. İşçinin kişisel verilerinin korunması da bu bağlamda değerlendirilebilir. İş sözleşmesi sürerken çeşitli nedenlerden ötürü işçinin kişisel verileri, toplanabilir, kayıt edilebilir ve kullanılabilir. Örneğin işverenin iş görme ediminin ifası karşılığında ücret ödeme borcunu yerine getirebilmesi için, işçinin vergi kimlik numarası, sigorta numarası gibi çeşitli bilgilerine gereksinim duyması doğaldır⁵⁰. Bunun yanında işverenin, işçi özlük dosyası gibi tutmak zorunda olduğu belgeler de bulunur. Kimi durumlarda

⁴⁸ Anayasanın 51/1 hükmü şöyledir: “Çalışanlar ve işverenler, üyelerinin çalışma ilişkilerinde, ekonomik ve sosyal hak ve menfaatlerini korumak ve geliştirmek için önceden izin almaksızın sendikalar ve üst kuruluşlar kurma, bunlara serbestçe üye olma ve üyelikten serbestçe çekilme haklarına sahiptir. Hiç kimse bir sendikaya üye olmaya ya da üyelikten ayrılmaya zorlanamaz”. Sendikalar Kanununun (S. 2821 t. 5 Mayıs 1983; RG. t. 7 Mayıs 1983, S. 18040) 31. maddesi ise şu hükmü içerir: “(1) İşçilerin işe alınmaları, belli bir sendikaya girmeleri veya girmemeleri veya belli bir sendikadaki üyeliği muhafaza veya üyelikten istifa etmeleri veya sendikaya girmeleri veya girmemeleri şartına bağlı tutulamaz. (2) Toplu iş sözleşmelerine ve hizmet akitlerine bu hükme aykırı kayıtlar konulamaz. (3) İşveren, bir sendikaya üye olan işçilerle sendika üyesi olmayan işçiler veya ayrı sendikalara üye olan işçiler arasında, işin sevk ve dağıtımında, işçinin mesleki ilerlemesinde, işçinin ücret, ikramiye ve primlerinde, sosyal yardım ve disiplin hükümlerinde ve diğer hususlara ilişkin hükümlerin uygulanması veya çalıştırmaya son verilmesi bakımından herhangi bir ayırım yapamaz. (4) Ücret, ikramiye, prim ve paraya ilişkin sosyal yardım konularında toplu iş sözleşmesi hükümleri saklıdır. (5) İşçiler, sendikaya üye olmaları veya olmamaları, iş saatleri dışında veya işverenin rızası ile iş saatleri içinde, işçi sendika veya konfederasyonlarının faaliyetlerine katılmalarından dolayı işten çıkarılamaz veya herhangi bir nedenle farklı muameleye tabi tutulamazlar. (6) İşverenin, hizmet akdinin feshi dışında, üçüncü ve beşinci fıkra hükümlerine aykırı hareket etmesi halinde, işçinin bir yıllık ücret tutarından az olmamak üzere tazminata hükmedilir. Sendika üyeliği veya sendikal faaliyetlerden dolayı hizmet akdinin feshi halinde ise, İş Kanununun 18, 19, 20 ve 21 inci madde hükümleri uygulanır. Ancak, İş Kanununun 21 inci maddesinin birinci fıkrası uyarınca ödenecek tazminat işçinin bir yıllık ücret tutarından az olamaz. (7) 854 sayılı Deniz İş Kanunu, 5953 sayılı Basın Mesleğinde Çalışanlarla Çalıştıranlar Arasındaki Münasebetlerin Tanzimi Hakkında Kanun ile 818 sayılı Borçlar Kanununa tâbi olan işçiler ve tarımdan sayılan işlerde çalışanlar ile İş Kanununun 18 inci maddesinin birinci fıkrası uyarınca, aynı Kanunun 13/A, 13/B, 13/C, 13/D ve 13/E maddelerinin uygulanma alanı dışında kalan işçinin sendika üyeliği veya sendikal faaliyetlerden dolayı hizmet akdinin feshi iddiası ile açacağı davada, ispat yükümlülüğü işverende olmak üzere 5521 sayılı İş Mahkemeleri Kanununun genel hükümleri uygulanır. (8) İşçiye ödenecek tazminat miktarı için, altıncı fıkra hükmü esas alınır. (9) İşçinin iş kanunları ve diğer kanunlara göre haiz olduğu bütün hakları saklıdır”.

⁴⁹ Sarper SÜZEK, **İş Hukuku**, 4. Baskı, İstanbul 2008, s. 346.

⁵⁰ Ahmet SEVİMLİ, s. 146.

işveren bu belgeleri yetkili kişilere göstermek zorundadır. Ancak yasal bir dayanak ya da işçinin rızası olmaksızın üçüncü kişilerle bu bilgileri paylaşmaması gerekir⁵¹.

İşçi, iş görme borcunu işverenin yönetim, gözetim ve denetimi altında gerçekleştirir⁵². Son dönemlerde işverenlerin, maliyetleri düşürmek, verimliliği arttırmak gibi nedenlerle işçilerini gözetim altında tutan uygulamalara artan oranda başvurdukları görülmektedir. İşe giriş çıkışlarda parmak ya da el izi kaydı gibi biyometrik yöntemlerle kayıt alınması; işyerinin kapalı devre televizyon sistemleri ile izlenmesi; işçinin telefon görüşmelerinin dinlenmesi, e-posta iletilerinin okunması, İnternet iletişiminin izlenmesi bu kapsamda sayılabilecek birkaç örnektir⁵³. Bu noktada işverenin işçinin gözetlenmesi dolayısıyla sağlayacağı yararın derecesi belirlenmelidir. Pek çok durumda işçinin gözetimi meşru bir temele dayanmaktadır. Hırsızlığın, zimmete para geçirmenin önlenmesi, daha verimli çalışılması, daha kaliteli hizmet sunulması bu kapsamda sayılabilir. Ancak her durumda işverenin objektif ve haklı bir menfaati olması⁵⁴ ile işçinin rızasının alınması koşulu aranmalıdır.

Teknolojideki gelişmeler, iletişim kurma şekillerimizi de önemli oranda değiştirmektedir. Daha önce de değindiğimiz gibi e-posta, geleneksel mektupların büyük bir rakibi haline gelirken, İnternet sunduğu sınırsız olanaklarla her geçen gün biraz daha cazip hale gelmektedir. Öte yandan işyerinde bu araçların özel amaçlı kullanımı özellikle performans kaybı açısından işverenleri önemli oranda telaşlandırmaktadır. Türkiye’de de yüksek yargı kararlarına yansıyan kimi olaylarda bu durumun tartışıldığı görülür.

⁵¹ İş Kanununun “İşçi özlük dosyası” kenar başlıklı 75. maddesi şu ifadeyi içerir: “ (1) 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. (2) İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür”.

⁵² Sarper SÜZEK, s. 214.

⁵³ Özellikle personel devam kontrol sistemi olarak adlandırılan ve personelin işe giriş-çıkış zamanını gözlemek amacıyla kullanılan teknikler, kartlı geçiş ve parmak izi tanıma sisteminden, damar, iris, yüz tanıma sistemlerine kadar çeşitli teknolojilerin kullanıldığı görülmektedir. Bkz. “İşyerinde Her An İzleniyoruz”, **Hürriyet İnsan Kaynakları** (kapak konusu), 28 Aralık 2008.

⁵⁴ Günter SCHAUB, Ulrich KOCH, Rüdiger LINCK, Hinrich VOGELSANG, **Arbeitsrecht-Handbuch**, Münih 2007, (Linck), s. 1553.

Yargıtay’a göre işçinin özel amaçlı İnternet kullanımı, kimi durumlarda sözleşmenin feshi için geçerli ya da haklı neden oluşturabilir⁵⁵. Ancak bu noktada işçinin işyerindeki bilgisayarı özel amaçları için kullanabilip kullanamayacağını, eğer kullanabiliyorsa bunu sınırlarının kendisine bildirilmiş olması gerekir. İşyerinde kendi kullanımına yönelik bir bilgisayara ve kendi belirlediği şifresini kullandığı e-posta adresine sahip bir işçinin özel yaşamının gizliliği konusunda makul beklenti içinde olması doğaldır. İşçi herhangi bir şekilde uyarılmadan ve yasal bir dayanak bulunmaksızın e-posta iletişiminin içeriğinin ya da trafik verilerinin izlenmesi temel haklarının ihlali anlamına gelecektir. Nitekim AİHM de, yukarıda da değinildiği üzere, bu gibi durumlarda özel yaşamın gizliliği hakkının ihlal edildiğine hükmetmiştir⁵⁶.

Benzer bir saptama işçinin telefon görüşmelerinin dinlenmesi açısından da yapılabilir. İşçinin müşterilerle yaptığı görüşmeler çoğu zaman “*daha kaliteli hizmet sunma*” gerekçesi ile kayıt altına alınmaktadır. Bu durumda hem işçi, hem de görüştüğü kişi içeriğin kayıt altına alındığı konusunda bilgilendirilmektedir. Ancak bazı durumlarda işçilerin özel görüşmelerinin de üstleri tarafından dinlendiği görülebilmektedir. İşçinin herhangi bir şekilde uyarılmadan özel görüşmelerinin dinlenmesi ya da izlenmesi Anayasada güvence altına alınan özel yaşamın ve

⁵⁵ Örneğin Yargıtay bir kararında şu saptamada bulunmuştur: “*Somut olayda, davacının kendi adına web siteleri oluşturduğu ve mesai saati içerisinde çok sayıda mail aldığı veya gönderdiği, web sayfasında şirketin faksını bildirdiği anlaşılmaktadır. Dosya içeriğine göre davacının eylemi iş sözleşmesinin haklı nedenle feshini gerektirecek ağırlıkta değilse de, işin yürütümünü olumsuz yönde etkilemesi nedeni ile fesih için geçerli neden teşkil ettiği kabul edilmelidir.*” Yarg. 9. HD., 3.11.2008, E. 2008/5836, K.2008/29779. (kişisel arşiv).

⁵⁶ Halford’un Birleşik Krallık’a karşı yaptığı başvuruya (b.n. 20605/92, k.t. 25 Haziran 1997) konu olan olayda bir kadın polisin ev ve işyeri telefonunun dinlenmesi söz konusudur⁵⁶. Hükümet, başvuranın işyerinde yaptığı telefon görüşmelerinin 8. maddenin kapsamı dışında kaldığını iddia etmiş ve bunu başvuranın, belirtilen türdeki görüşmelerinin gizliliğine yönelik “*makul beklenti*” içinde olamayacağına dayandırmıştır. Oysa Mahkeme bu görüşü yerinde bulmamıştır, önceki kararlarında da belirttiği üzere, evden olduğu gibi, işyerinden yapılan görüşmeler de Sözleşme’nin 8/1 hükmünde yer alan “*özel yaşam*” ve “*haberleşme*” kavramlarının kapsamında yer alır(par.43-44). Ayrıca Mahkeme, başvuranın işyerinde telefonunun dinlenebileceğine ilişkin herhangi bir uyarı almadığına ve görüşmelerinin gizliliğine ilişkin “*makul beklenti*” içinde olmasının nedenleri bulunduğuna işaret etmiştir: Halford’un işyerinde yalnız kendi kullanımına tahsis edilmiş bir odası vardır ve bu odada iki telefonu bulunmaktadır. Telefonlardan biri başvuranın şahsi kullanımına yöneliktir. Üstelik başvurana, taraf olduğu cinsiyet ayrımcılığı davasına ilişkin olarak işyeri telefonlarını kullanabileceği konusunda garanti verilmiştir(par.45). Bu yaklaşım, somut olayda hükümetin de ileri sürdüğü, işverenin kendisinin sağladığı bir telefonda yapılan görüşmeleri, işçinin önceden haberi olmaksızın izleyebileceği yaklaşımını çürütmektedir.

haberleşmenin gizliliği haklarının ihlali olduğu gibi, TCK hükümleri uyarınca da suçtur. Nitekim Yargıtay da çeşitli kararlarında konunun önemine işaret etmiştir⁵⁷.

İşçilerin biyometrik yöntemlerle ve kapalı devre televizyon sistemleri ile izlenmesi ve kişisel verilerinin kaydının tutulması da ciddi sorunlar yaratabilir. Örneğin kişinin parmak izi onu diğer bütün bireylerden ayıran benzersiz bir nitelik taşır. Bir bireyin kişiliği ile sıkı sıkıya bağlı böylesine bir bilginin kayıt altında tutulması ve üçüncü kişilere aktarılması ciddi sorunların yaşanmasına neden olabilir. Bu nedenle işe giriş-çıkış saatleri gibi konuların kayıt altına alınması için bu ve benzeri yöntemler kullanılıyorsa uygulanacak ilkelerin belirlenmesi büyük önem taşır. Uygulamanın hukuka uygun olarak yürütüldüğü durumlarda bile veri güvenliğine ilişkin eksiklikler işçinin kişisel verilerinin korunması hakkının zarar görmesine neden olabilir.

İkinci olarak işçinin performans değerlendirmesi, iş güvenliği kurallarına uyup uymadığının saptanması ve izlenmesi için kapalı devre televizyon sistemleri ile gözlenmesi söz konusu olabilir. Ancak işçinin işyerindeki her hareketinin izlenmesi özel yaşamına müdahale oluşturur. Bunun önüne geçilmesi uygulamanın amacın gereklerini aşmaması ve işçinin bu konuda bilgilendirilmesi ile olanaklıdır⁵⁸. Unutmamak gerekir: işçi, her gün işyerinin kapısından içeri girdiğinde özel yaşamlarını bir elbise gibi çıkarıp dışarıda bırakmamaktadır. İşçilerin iş yaşamında da belirli bir düzeyde özel yaşamın gizliliği hakkına sahip olduklarının kabulü insan olmanın da bir gereğidir. Akvaryumun içerisindeki balıklar gibi her hareketinin izlendiğini düşünen işçinin psikolojisinin de olumsuz yönde etkileneceği ve bunun sonucunda verimliliğinin düşebileceği de bir gerçektir.

İş sözleşmesi sona erdikten sonra da işveren, iş ilişkisi dolayısıyla işçiye ilişkin olarak edindiği bilgileri saklamak, üçüncü kişilerle paylaşmamak yükümlülüğündedir. Ayrıca işçinin rızasının bulunmadığı durumlarda yeni işverenin

⁵⁷ Örneğin Yargıtay'ın bir kararına göre: *"Telefon konuşmasında yer alan sözler iki kişi arasında gizli kalması ve o kişilerin özel yaşam alanı ile ilgili bulunan sözler olduğu görülmektedir. Sözle bu içerikte olmasa dahi bir kişinin telefonunun dinlenmesi veya dinlenen görüşmelerin yayınlanması, başlı başına özel yaşama ve hatta son derece gizli kalması gereken yaşamın gizliliğine saldırı teşkil eder. ... Hatta hiç kimsenin telefonu da dinlenemez"*. Yarg. 4. HD, 31 Kasım 2000, E. 2000/6487, K. 2000/9467.

⁵⁸ İşçilerin işyerinde kapalı devre televizyon sistemleriyle izlenmesine ilişkin çeşitli ülkelerden hukuksal düzenlemeler için bkz. **Reasonable Expectations of Privacy, Eleven Country Reports on Camera Surveillance and Workplace Privacy**, haz. Sjaak NOUWT, Berend R. De VRIES, Corien PRINS, Asser Press, Hollanda 2005.

eski işverenden bilgi alamaması gerekir. Ancak eğer işçi, yeni işe başvururken eski işvereni referans olarak göstermişse kendi hakkında bilgi verilmesi konusunda rızasının bulunduğu kabul edilmelidir.

İş Kanunu kapsamında işçinin kişisel verilerinin korunmasına güvenceler oldukça sınırlıdır. Yukarıdaki değerlendirmelerin büyük bölümü İş hukukunun esasları ve ayrıca AİHM'nin konuya ilişkin yorumları dikkate alınarak yapılmıştır. İş Kanunu incelendiğinde ise 75. maddede yalnızca “işçi özlük dosyası”na yönelik bir korumanın öngörüldüğü görülür⁵⁹. Yürürlükteki BK'nın hizmet sözleşmesine ilişkin hükümlerinde de işçinin kişisel verilerinin korunmasına ilişkin herhangi bir hüküm bulunmamaktadır⁶⁰. Koruma ancak İş Kanunu, TCK, MK ve BK'da yer alan genel hükümlerin yorumlanması ile gerçekleştirilebilmektedir. Ancak daha önce de işaret edildiği üzere kişisel verilerin korunmasına ilişkin temel ilkeler belirlenmeden bu düzenlemeler sınırlı kalmaya mahkumdur. Bu durumda işçinin temel hak ve özgürlüklerinin korunması açısından oldukça önemli olan bu konuda, hukukumuzda bir boşluk olduğu söylenebilir. İş Kanununda konuya ilişkin özel bir düzenleme yapılması önemli bir gerekliliktir. Ancak bunun yanında yukarıdaki açıklamalar Kişisel Verilerin Korunması Yasasının gerekliliğini de bir kez daha ortaya koymaktadır.

IV. CEZA HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

A. GENEL OLARAK

Türk Ceza Kanununda⁶¹ (TCK) kişisel verilerin korunması alanında değerlendirilen bazı eylemlerin suç olarak düzenlendiği görülmektedir. Bu bakımdan özellikle yasanın dokuzuncu bölümünde yer alan “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” değerlendirilmelidir. Burada yer alan suçların bir bölümü eski

⁵⁹ İşçi özlük dosyasına ilişkin değerlendirmeler için bkz. Ufuk AYDIN, İşverenin İşçi Özlük Dosyası Tutma Yükümü, **İş Hukuku ve Sosyal Güvenlik Hukuku Türk Milli Komitesi 30. Yıl Armağanı**, Ankara 2006, s. 491-505.

⁶⁰ Nitekim bu durum yasa koyucu tarafından da fark edilmiş olacak ki BK Tasarısına konuya ilişkin bir hüküm eklenmiştir. Tasarının 418. maddesi uyarınca “(1)İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. (2)Özel kanun hükümleri saklıdır”.

⁶¹ Türk Ceza Kanunu, Kanun no. 5237, t. 26 Eylül 2004.

ceza kanununda da düzenlenirken kişisel verilerin korunması açısından oldukça önemli olan 135 vd. maddelerde yer alan suçlar ceza hukuku mevzuatımıza yeni yasa ile girmiştir⁶².

Kişisel verilerin korunmasını ulusal hukuklarının bir parçası haline getirmiş ülkelerdeki düzenlemeler incelendiğinde, ceza hukuku açısından iki yaklaşımdan birinin tercih edildiği görülür. Kişisel verilerin korunmasına ilişkin suçlar Almanya, İtalya gibi kimi ülkelerde konuya ilişkin özel düzenlemeler kapsamında yer alırken⁶³, Fransa gibi başka ülkelerde ise ceza kanunları kapsamında düzenlendiği görülmektedir. 5237 sayılı Türk Ceza Kanunu hazırlanırken Fransa’da benimsenen yöntemin izlendiği görülmektedir⁶⁴. Bu bağlamda TCK’nın 135 vd. maddelerinde kişisel verilerin korunmasının temel ilkelerinin bazılarının konu edildiği görülür. Ancak aşağıda tekrar değerlendirileceği üzere bu noktada eksiklik kişisel verilerin korunmasına yönelik bütüncül bir yasal düzenlemenin halen yürürlüğe girmemiş olmasıdır. Nitekim ceza kanununda konuya ilişkin bazı suçlar belirlenmiş ve bunlara yaptırımlar öngörülmüş olsa da burada sözü edilen etkinliklerin tanımlandığı ve kişisel verilerin korunmasının temel ilkelerinin belirlendiği bir düzenlemenin bulunmaması önemli bir eksikliktir. Ayrıca TCK’da aşağıda incelenecek hükümlerin varlığına karşın kişisel verilerin tanımlanmamış olması, özellikle konuya ilişkin özel yasanın halen kabul edilmediği dikkate alındığında, bir başka önemli sorun olarak karşımıza çıkmaktadır⁶⁵. Bu durumda aşağıdaki hükümler yorumlanırken kişisel veriyi, uluslararası sözleşmeler ve Kişisel Verilerin Korunması Kanun Tasarısında benimsenen “*belirli ya da belirlenebilir bir kişiye ilişkin her türlü bilgi*” olarak kabul etmek gerekir⁶⁶.

⁶² Bu kapsamda yer alan suçların bir bölümü 765 sayılı TCK’da da hüküm altına alınmıştır. Bu bağlamda “*haberleşmenin gizliliğini ihlal*”(m. 132), “*kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması*”(m.133) ve “*Özel hayatın gizliliğini ihlal*”(m.134) suçları ceza hukuku sisteminde daha önce de var olan suçlardır. Buna karşılık yine TCK’nın dokuzuncu bölümünde eski Ceza Yasasında yer almayan ve fakat kişisel verilerin korunmasıyla yakından ilgili başka bazı suçlara da yer verilmiştir. Bunlar; “*Kişisel verilerin kaydedilmesi*”(m.135), “*Verileri hukuka aykırı olarak verme veya ele geçirme*”(m. 136) ve “*Verileri yok etme*”(m.138) suçlarıdır.

⁶³ Bkz. Federal Almanya Veri Koruma Yasası (BDSG), m.43-44; İtalyan Veri Koruma Yasası, m. 167-172.

⁶⁴ Muammer KETİZMEN, **Türk Ceza Hukukunda Bilişim Suçları, Adalet, Ankara 2008**, s. 217.

⁶⁵ Bahri ÖZTÜRK, Mustafa Ruhan ERDEM, **Uygulamalı Ceza Muhakemesi Hukuku**, 11. Baskı, Seçkin, Ankara 2007, s. 623.

⁶⁶ TCK’da yer alan kişisel verilerin korunmasına yönelik suçları yorumlarken başta 108 sayılı AK Sözleşmesi olmak üzere uluslar arası düzenlemeler hep göz önünde tutulmalıdır. Nitekim yasa

B. KİŞİSEL VERİLERİN KAYDEDİLMESİ

TCK'nın 135. maddesinde “*kişisel verilerin kaydedilmesi*” suç olarak düzenlenmiştir⁶⁷. Burada kişisel verilerin hukuka aykırı olarak kayıt eden kimseye altı aydan üç yıla kadar hapis cezası verileceği öngörülmüştür⁶⁸. Kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri hukuka aykırı olarak kaydeden kimse de aynı hüküm uyarınca cezalandırılacaktır⁶⁹.

Burada dikkat çekilmesi gereken bir husus, yasa koyucunun hükmün birinci fıkrasında ve ikinci fıkranın belirtilen bölümünde suçun oluşabilmesi için kaydın “*hukuka aykırı*” olarak yapılmasını ararken “*(k)işilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine*” ilişkin bilgilerin kayıt edilmesi açısından bu ibareye yer vermemiş olmasıdır. O halde belirtilen türdeki bilgilerin kaydının her durumda hukuka aykırı olacağı söylenebilir⁷⁰. Burada bazı veri türleri özel nitelikte görülmüş

koyucunun belirtilen düzenlemeleri benimserken özellikle AK Sözleşmesini dikkate aldığını 135. maddenin gerekçesi ortaya koymaktadır. 135. maddenin gerekçesinde bu hüküm ile 108 sayılı AK Sözleşmesinin ilgili hükümlerine geçerlilik tanındığı belirtilmektedir. Nitekim örneğin ÖZBEK'e göre gerekçede yer alan bu ifade dolayısıyla maddenin açıklanması bakımından AK Sözleşmesi hükümlerinden yararlanmak olanaklıdır. Bkz. Veli Özer ÖZBEK, **Yeni Türk Ceza Kanununun Anlamı (Açıklamalı, Gerekçeli, İctihath)**, C. 2 (Özel Hükümler), Seçkin, Ankara 2008, s. 947. Kanımızca her ne kadar bu ifade yalnızca 135. maddenin gerekçesinde yer alsada da konuya ilişkin hükümlerin genelinde Sözleşmenin dikkate alındığının da bir işaretidir.

⁶⁷ Burada yalnızca “*kişisel verileri kaydeden kimse*”den söz edilmesi nedeniyle kayıt işinin suçun tamamlanması için bir koşul olduğunu belirtmek gerekir. O halde bundan önceki evrenin suça teşebbüs olduğunu, ancak kayıt için yalnızca hazırlık yapmanın hazırlık hareketleri olması dolayısıyla cezalandıramayacağını belirtmek gerekir. Zeki HAFIZOĞULLARI, s. 139.

⁶⁸ TCK'nın 135/1 hükmü şöyledir: “*Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir*”. Ancak 137. madde uyarınca bu suçun “*a. Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b. Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde verilecek ceza yarı oranında arttırılır*”. Buna göre suçun örneğin posta ve diğer görevli memurlar tarafından işlenmesi suçun nitelikli halini oluşturacaktır. İkinci olarak görev veya mesleği dolayısıyla kamunun güvenini sağlamış kişilerin bu güveni korumaları düşüncesi üzerine kurulmuş meslek sırrından hareketle, duçun din adamları, avukatlar, noterler, hekimler gibi kişilerce işlenmesi yine nitelikli bir hali oluşturmaktadır. Son olarak özel kargo şirketlerinde çalışanlar, video, kamera görüntüsü alan ve izleyenlerin suçu meslek ve sanatın sağladığı kolaylıktan yararlanarak işlemeleri halinde yine ceza yarı oranında arttırılacaktır. Bkz. Haydar EROL, **Gerekçeli, Açıklamalı, İctihath Yeni Türk Ceza Kanunu**, Ankara 2005, s. 692-693.

⁶⁹ TCK'nın 135/2 hükmü şöyledir: “*Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır*”.

⁷⁰ HAFIZOĞULLARI bu konuyu şu şekilde değerlendirmiştir: “*Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin bilgilerin kişisel veri olarak kayıt edilmesi söz konusu olduğunda, Kanunun “hukuka aykırı olarak” hükmüne yer vermediği gözlenmektedir. İfadeden,*

ve farklı bir düzenlemeye tabi tutulmuştur. Çalışmamız kapsamında daha önce de belirttiğimiz üzere, özellikle devlet kurum ve kuruluşlarının kamu hizmeti yerine getirirken bu türdeki bilgileri kişisel veri olarak tutmalarından herhangi bir yarar beklemek güçtür. Nitekim bir hukuk devletinde, yönetimin bu bilgiler karşısında gözlerinin bağlı olması gerekir.

Buna karşın bir kişi, kendi iradesi ile siyasi, felsefi veya dini görüşünü, ırksal kökeni açıklayabilir, hatta bunu çeşitli iletişim araçları ile duyurabilir. O zaman açıklanan bu bilgilerin kayıt altına alınması her durumda suç mu oluşturacaktır? Örneğin kişinin kendi özgür iradesi ile açıkladığı bu bilgilerin yazılı, görsel basında yer alması ve bunların doğal olarak arşivlerde korunması durumunda ne olacaktır? Bir kilisenin binlerce yıldır süre gelen geleneklerine uygun olarak cemaatine ilişkin tuttuğu kayıtlar TCK'nın belirtilen hükmü karşısında nasıl değerlendirilecektir?

135. maddenin gerekçesinde “(k)işinin kendi rızası ile, kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı muhakkaktır” ifadesi yer almaktadır⁷¹. Ancak madde gerekçesinin genelinden burada hükmün birinci fıkrasının kastedildiği yönünde bir anlam çıkmaktadır. Bu genel yorum, göz ardı edilerek gerekçede yer alan ifadeler uyarınca kişinin rızasının bir meşruluk nedeni olarak görülmesi olanaklıdır. Buna karşın kanımızca bu hükümde, belirtilen koşulun açıkça yer alması daha uygun olurdu⁷². Nitekim ilgili kişinin özgür iradesinin bir yansıması olan rızası ile bu bilgilerin kayıt altına alınmasının her hangi bir sakıncası olmamalı hatta o kişinin düşünciyi açıklama özgürlüğü çerçevesinde kabul görmelidir. Bu nedenle TCK'nın 24 vd. maddelerinde düzenlenen genel hukuka

bu bilgilerin kişisel veri olarak kaydedilmesinin, her zaman, mutlak olarak, hukuka aykırı olduğu sonucu çıkmaktadır. Kanunun, hem maddenin birinci fıkrası hükmünde, hem ikinci fıkrasında diğer durumlar için hukuka aykırı olmak hükmüne yer vermişken, bu hali, onlardan niçin ayırık tuttuğu anlaşılamamaktadır. Kanunun hazırlık çalışmalarında ve gerekçede bu konuya ilişkin bir açıklamaya rastlanmamıştır”. Zeki HAFIZOĞULLARI, Ceza Özel Hukuku, s. 139.

⁷¹ Burada ve aşağı TCK'nın ilgili hükümlerinin gerekçesi için şu kaynaktan yararlanılmıştır: İzzet ÖZGENÇ, **Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler)**, 2. Baskı, Seçkin, Ankara 2005.

⁷² Nitekim Fransız Ceza Kanunun ilgili hükmünde bilgisayar hafızalarında saklanan bu türdeki verilere ilişkin olarak ilgili kişinin mutabık olduğuna ilişkin beyanı hukuka uygunluk nedeni olarak görülmüştür. Bkz. Fransız Ceza Kanunu, m. 226-19. Başka sorunlu yanlarına karşın TCK Tasarısında rıza koşuluna yer verildiği görülmektedir. TCK Tasarısının 197. maddesinde yer alan ilgili hüküm şu şekildeydi: “Rızaları olmaksızın veya kanunların öngördüğü şekil ve usullere uyulmaksızın kişisel verileri bilişim sistemlerine yerleştiren veya işleyen kimseye altı aydan üç yıla kadar hapis cezası verilir. ... Kanunun öngördüğü haller dışında, kişilerin ahlaki niteliklerini, siyasal, felsefi veya dinsel görüşleri veya ırki kökenlerini veya sendikal bağlantılarını veya cinsel yaşamlarını veya sağlık durumlarını kişisel veri olarak sisteme yerleştiren veya işleyen kimseye bir yıldan iki yıla kadar hapis cezası verilir”. Muammer KETİZMEN, s. 230-231, d.n. 104.

uygunluk nedenlerine başvurmak ve “Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez” hükmünün⁷³ burada da geçerli olduğunu kabul etmek gerekir.

Kişilerin siyasal, felsefî, dini görüşleri ve ırksal kökenlerine ilişkin olmayan kişisel veriler açısından “hukuka aykırı” ibaresinin konumuz açısından içeriğini belirlemek gerekir⁷⁴. Yasada hukuka aykırılığın ayrıca belirtildiği durumlar öğretide kimi yazarlarca “hukuka özel aykırılık” olarak adlandırılmaktadır. Hukuka özel aykırılığın söz konusu olduğu durumlarda ise manevi unsurun arandığı belirtilmektedir.

Bunun yanında 135. maddenin gerekçesinde belirtildiği üzere “(s)öz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayrım gözetilmemiştir”⁷⁵. Her ne kadar kişisel verilerin korunmasına ilişkin hukuksal düzenlemelerin kabulünde bilgisayar ve diğer bilişim sistemlerindeki gelişmeler etki etmişse de hukuksal açıdan kâğıt üzerindeki veriler ile elektronik ortamda yer alan veriler arasında bir ayrım bulunmamaktadır. Bu nedenle yasada bu konuda bir ayrım yapılmaması yerindedir. Buna göre suçun oluşabilmesi için verilerin sistemli olarak kayıt edilmesi, bu kayıtların bilişim sistemlerinde tutulması gibi koşullar aranmamaktadır. Suçun kişisel verilerin herhangi bir şekilde kayıt edilmesi ile gerçekleşmesi olanaklıdır⁷⁶. Ayrıca suçun oluşması için kişisel verilerin yayınlanması, başkasının kullanımına açılması ya da

⁷³ TCK m. 26/2.

⁷⁴ KETİZMEN sorunu şu şekilde değerlendirmektedir: “Aslında burada sorun, maddenin kaynağını oluşturan Fransız Ceza Kanununda yer alan kişisel verilerin korunmasına ilişkin suçların eksik norm olarak düzenlenmesi ve özellikle kişisel verilerin korunmasına ilişkin kanunun varlığı karşısında, söz konusu kanunda gösterilen usul ve esaslara uyulmasının müeyyide altına alınmasından dolayı ortaya çıkmıştır. TCK’nin 135. maddesinde düzenlenen suç bakımından ise, Fransız hukukunda olduğu şekliyle, eksik norm olarak bağlantı kurulabilecek kişisel verilerin korunmasına ilişkin genel bir düzenleme bulunmamaktadır. Bu nedenle, maddede yer alan hukuka aykırı olarak kaydetmenin yorumlanması gerekmektedir”. Muammer KETİZMEN, s. 235.

⁷⁵ TCK Öntasarısı ve Tasarısında bilişim sistemine yerleştirme ve işleme “otomatik fişye ve işleme”, otomatik olmayan kişisel veri kayıtları ise “fişlik” olarak ifade edilmiştir. Daha sonra bu düzenleme şekli TBMM Adalet Komisyonunda değiştirilmiştir. Değişikliğin gerekçesinde suç tanımında her iki kayıt türü arasında bir ayrım bulunmadığı belirtilmiştir. Bkz. Muammer KETİZMEN, s. 233.

⁷⁶ Muammer KETİZMEN, s. 233; Murat Volkan DÜLGER, **Bilişim Suçları**, Seçkin, Ankara 2004, s. 269.

bir zararın oluşması gerekmez. Suçun gerçekleşmesi için kayıt etme işleminin gerçekleşmesi yeterlidir⁷⁷.

Dikkat çekilmesi gereken bir diğer nokta, TCK'nın 135. maddesinde yalnızca verilerin işlenmesinin bir türü olan kayıt etmenin suç olarak belirlenmesidir. Oysa çalışmamızın ikinci ve üçüncü bölümlerinde ilgili bahislerde belirtildiği üzere, kişisel verilerin işlenmesi yalnızca kayıt etmeyi değil, toplanma, kullanılma, aktarılma gibi çeşitli eylemleri içeren bir süreçtir. TCK'nın aşağıda incelenecek izleyen hükümlerinde bu eylemlerin bir kısmına ilişkin düzenlemeler bulunmaktadır. Ancak özellikle kişisel verilerin hukuka aykırı olarak kullanılmasına ilişkin düzenlemeye yasada yer verilmediği görülmektedir. Bu durumda hukuka uygun şekilde toplanan ve kayıt altına alınan kişisel verilerin sonraki kullanımlarında oluşabilecek aykırılıkların yaptırımsız kaldığı sonucu çıkmaktadır. Bu durum, amaçla bağlılık ilkesi ile uyumlu değildir. Nitekim bu ilkenin meşru olmayan ikincil ve daha sonraki işlemleri sınırlandırmaya yönelik işlevi TCK'nın 135. maddesinde dikkate alınmamıştır⁷⁸.

C. VERİLERİ HUKUKA AYKIRI OLARAK VERME, YAYMA VEYA ELE GEÇİRME

TCK'nın 136. maddesinde kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak ve ele geçirmek suçu düzenlenmiştir. Buna göre; *“Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır”*⁷⁹.

⁷⁷ Murat Volkan DÜLGER, s. 272.

⁷⁸ Muammer KETİZMEN, s. 238. Oysaki maddenin gerekçesinde *“Bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler”* yönünde bir saptama yer almaktadır. Ancak madde metninde oldukça önemli olan bu tehlikeyle örtüşen bir düzenleme getirilmemiştir. DÜLGER'e göre ise *“Kayıt etme eylemi, bir bilişim sisteminde ya da yazılı olarak bulunmayan bir bilginin sisteme girilmesi ya da yazılı hale getirilmesi şeklinde olabileceği gibi aslında başka bir kaynakta hukuka uygun olarak bulunan bir bilginin bir bilişim sistemine ya da kişisel dosyaya hukuka aykırı şekilde girilmesi şeklinde de gerçekleştirilebilecektir”*. Bkz. Murat Volkan DÜLGER, s. 271.

⁷⁹ 135. madde için söz konusu olduğu gibi bu hüküm açısından da 137. madde, suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ya da belirli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi hallerini ağırlaştırıcı neden olarak öngörmüştür.

136. maddede verme, yayma ve ele geçirme seçimlik hareketler olarak belirlenmiştir. Kişisel verilerin hukuka aykırı olarak verme ve yayma hareketlerinin yaptırıma bağlanmasındaki amaç yetkisiz üçüncü kişilere aktarılmasını önlemektir. Çalışmamızın üçüncü bölümünde de incelendiği üzere kişisel verilerin yalnızca ilk aşamada korunması yeterli değildir. Bu bağlamda bilgiler ilk olarak hukuka uygun olarak toplanmış ve kullanılmış olabilir. Daha sonraki aşamalar korumasız bırakıldığında ise bu kural da anlamını yitirir.

Bunun yanında verilerin yetkisiz üçüncü kişilerce ele geçirilmesi de önlenmek istenmiştir. Bu durumda kişisel verileri daha önceden kaydedilmiş olsun ya da olmasın hukuka aykırı olarak ele geçiren kişi 136. madde hükmünce cezalandırılacaktır⁸⁰. Daha önceden verinin kaydedilmesinin hukuka uygun olup olmamasının suçun oluşması açısından bir önemi bulunmamaktadır⁸¹. 136. maddede yer alan düzenleme kişisel verilerin korunmasını sağlayıcı bir niteliktedir. Bu noktada önlenmek istenen eylemler arasında başka bazı suçlara da neden olabilecek kimlik hırsızlığı vb. de bulunur.

D. VERİLERİ YOK ETMEME

TCK'nın 138. maddesinde verileri yok etmeme suçu düzenlenmiştir. Buna göre “(k)anunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir”. Burada kişisel verilerin korunmasında temel ilkeler arasında bulunan süre sınırı karşılanmıştır. Buna göre kişisel veriler, amaç için gerekli olandan daha uzun süre tutulmamalıdır. Kişisel verilerin süresiz olarak tutulmaması gerekliliği, amaçla bağlantılık ilkesi açısından da oldukça önemlidir. Artık gereksinim duyulmayan verilerin silinmesi veya anonimleştirilerek kişisel niteliğinin ortadan kaldırılması keyfi uygulamaların önüne geçilmesi için gereklidir.

⁸⁰ KETİZMEN ise şu görüştedir: “135. maddede genel olarak kişisel verilerin toplanmasından bahsedilmesi karşısında, bu maddede düzenlenen kişisel verinin ele geçirilmesi, kaydedilmiş olan kişisel verinin hukuka aykırı olarak elde edilmesi anlamına gelmektedir”. Muammer KETİZMEN, s. 240.

⁸¹ Nitekim 136. maddenin gerekçesinde şu ifade yer almaktadır: “Bu madde hükmü ile, hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır”.

138. madde hükmü açısından iki hususa işaret etmek gerekir. Birincisi, belirtilen hükümde suçun oluşabilmesi için “*kanunların belirlediği sürelerin geçmiş olması*” ölçütü esas alınmıştır. Bu bağlamda verinin toplanma amacı ile bir bağlantı kurulmadığı görülmektedir⁸². Bir başka anlatımla verileri toplanma amacı ortadan kalkmış ya da gerçekleşmiş olsa bile bunlar yasada belirtilen süreler boyunca saklanabilecektir. Bu durum amaca bağlılık ilkesi ile uyumlu değildir.⁸³

İkinci olarak şu noktaya dikkat çekmek gerekir: burada “*verileri sistem için yok etmek*”ten söz edilmektedir. Bu ifade belirtilen suçun otomatik yollarla işlenen verilere ilişkin olduğu izlenimini yaratmaktadır. Nitekim yukarıda incelenen verilerin kaydedilmesi ve hukuka aykırı olarak verme, yayma ve ele geçirme suçlarında böyle bir ifade yer almamaktadır. Bu farklılık, verileri yok etmeme suçunun diğerlerinin tersine yalnızca otomatik yolla işlenen verilere ilişkin olduğu yönünde şüphe yaratmaktadır. Bu şüphenin giderilmesi için verilerin yok edilmesi açısından sistemde bulunmaya ilişkin ifade madde metninden çıkartılmalıdır⁸⁴.

Son olarak verileri yok etmeme suçunun yalnızca ihmal yoluyla işlenebileceği belirtilmelidir. Yasal yükümlülük altında bulunanlar ihmalen bunu yerine getirmediklerinde suç gerçekleşmiş olur⁸⁵. Bu bağlamda süre aşıldıktan sonra verilerin yok edilmesi, eylemi suç olmaktan çıkarmayacağı gibi, mağdurun rızası da fiili hukuka uygun yapmaz⁸⁶. Ayrıca burada sözü geçen sürenin mutlaka 3 ay, 1 yıl gibi kesin bir zaman dilimi olarak düşünülmemesi gerekir. Örneğin CMK’nın 81/2 hükmü, şüpheli veya sanığın fizik kimliğinin saptanması için tutulan fotoğrafı, parmak izi gibi kayıtları; itirazın reddi, beraat gibi bazı durumlarda Cumhuriyet savcısının huzurunda derhal yok edilmesini emretmektedir. Bu kurala uygun hareket etmeyen memur, TCK m. 138’de belirtilen suçu işlemiş olacaktır.

⁸² Muammer KETİZMEN, s. 241; Doğan SOYASLAN, **Ceza Hukuku Özel Hükümler**, s. 275.

⁸³ “*Kişisel veriler, nerede ve ne maksatla bulunursa bulunsunlar, kişinin özel hayatına dâhildirler, dolayısıyla cezai himayenin konusunu oluşturmaktadırlar. Bazı kişisel veriler, ör., T.C. vatandaşlık numarası, tartışmalı olmakla birlikte, süresiz olarak başkalarının bilgisine açıktır. Buna karşılık, bazı kişisel veriler, kullanılma amaçları yönünden, kanunla, saklanmaları, bir süre ile sınırlandırılabilir. Bu süre sonunda, özel hayatın gizliliğinin korunmasının zorunlu sonucu olarak kişisel verilerin bulundukları yerde yok edilmeleri gerekmektedir*”. Zeki HAFIZOĞULLARI, s. 141.

⁸⁴ Bkz. aynı yönde Muammer KETİZMEN, s. 242.

⁸⁵ Muammer KETİZMEN, s. 241; Doğan SOYASLAN, s. 275; Zeki HAFIZOĞULLARI, s. 141-142.

⁸⁶ Zeki HAFIZOĞULLARI, s. 141-142.

E. TCK'DA KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK DİĞER HÜKÜMLER

Belirtilen hükümler yanında TCK'nın çeşitli hükümlerinin kişisel verilerin korunması açısından sonuç doğuracağı söylenebilir. Burada ilk akla gelen TCK'nın *"haberleşmenin gizliliğini ihlal"*, *"kişiler arası konuşmaların dinlenmesi ve kayda alınması"* ve *"özel hayatın gizliliğini ihlal"*e ilişkin hükümleridir⁸⁷. Türkiye'de ceza hukuku mevzuatında uzun süreden beri yer alan bu hükümler kaynağını Anayasa'nın özel yaşamın ve haberleşmenin gizliliğine ilişkin hükümlerinde bulunur. Çalışmamızın çeşitli yerlerinde daha önce de belirttiğimiz üzere kişisel verilerin korunması hakkı her iki alanla da yakından ilişkilidir. Bu nedenle ilgili durumlarda belirtilen hükümlerin de koruma getireceği söylenebilir.

Bunun yanında sırrın açıklanması ile ilgili suçları da dikkate almak gerekir⁸⁸. Şu hususu belirtmek gerekir: mevzuatımızda meslek sırrı içerisinde değerlendirilebilecek çeşitli konulara ilişkin düzenlemeler TCK ile sınırlı değildir. Mevzuatımızda sağlık personelinin, vergi memurlarının ya da benzeri görev gören diğer kişilerin meslekleri dolayısıyla edindikleri bilgileri açıklamama

⁸⁷ TCK'nın 132. maddesi şu hükmü içermektedir: *"(1) Kişiler arasındaki haberleşmenin gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu gizlilik ihlâli haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur. (2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. (3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. (4) Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması hâlinde, ceza yarı oranında artırılır"*. 133. madde ise şöyledir: *"(1) Kişiler arasındaki alenî olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki aydan altı aya kadar hapis cezası ile cezalandırılır. (2) Katıldığı alenî olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aya kadar hapis veya adli para cezası ile cezalandırılır. (3) Yukarıdaki fıkralarda yazılı fiillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişi, altı aydan iki yıla kadar hapis ve bin güne kadar adli para cezası ile cezalandırılır. Bu konuşmaların basın ve yayın yoluyla yayınlanması hâlinde de, aynı cezaya hükmolunur"*. 134. madde ise şu şekilde düzenlenmiştir: *"(1) Kişilerin özel hayatının gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlâl edilmesi hâlinde, cezanın alt sınırı bir yıldan az olamaz. (2) Kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Fiilin basın ve yayın yoluyla işlenmesi hâlinde, ceza yarı oranında artırılır"*.

⁸⁸ Bu suç tipine ilişkin ayrıntılı bilgi için bkz. Süheyl DONAY, **Meslek Sırrının Açıklanması Suçu**, İstanbul Üniversitesi Yayını, İstanbul 1978.

yükümlülüğünü doğuran çeşitli hükümler bulunmaktadır⁸⁹. Nitekim bunların bir kısmına aşağıda değinilecektir. TCK açısından ise özellikle 239. ve 258. maddeler üzerinde durulmalıdır.

TCK'nın 239. maddesinde *“ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi ve belgelerin açıklanması”* düzenlenmiştir. Hükümde bu türdeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi için şikayete bağlı cezai yaptırım öngörülmüştür. Bilgi veya belgeleri açıklayan kişinin bunları hukuka uygun ya da aykırı elde etmesi arasında da bir ayırım öngörülmemiştir. Bunların ticari sır, bankacılık veya müşteri sırrı niteliğinde olup olmadığı ise ilgili yasalarda belirlenen ölçütler göz önünde tutularak yargıç tarafından belirlenecektir⁹⁰. TCK'nın 239. maddesi konumuz açısından özellikle müşteri sırrını koruması açısından önemlidir. Nitekim ticari sır ve bankacılık sırrı aşağıda tekrar inceleneceği üzere gerçek kişilerin değil, tüzel kişilerin korunmasına yönelmiştir⁹¹. Kişisel verilerin korunması insan

⁸⁹ EKEN'e göre; *“Mesleki gizlilik yükümlülüğü, kişisel tıbbi bilgileri korumak amacıyla doktor, eczacı, ebe gibi sağlık alanında hizmet yürütenleri ve özel işletmelerin ekonomik menfaatini korumak için vergi, gümrük, borsa komisyon memurlarını, iş müfettişlerini, işletmelerde staj yapanları, sosyal güvenlik memurlarını vb. kapsamaktadır. ... Bu yükümlülüğün amaç, özel kişilerin çıkarları ve yaşamları ile ilgili bilgileri korumak olduğu gibi, yönetimin gizliliklerini de korumaktır. Örneğin posta hizmetlerinde çalışankişilerin yükümlülüğü, diploması ve ordu görevlilerinin bazı bilgileri ve sırları saklama ödevi, kamu düzeni ve ülke güvenliğini korumaya yöneliktir”*“Sadece kamu yönetime özgü olan bu yükümlülük, idarede çalışan memurlar içindir. ... Mesleki gizlilik, kişilerin ve onların bireysel hak ve mahremiyetlerinin korunmasına yönelikken, memurun sır saklama yükümlülüğü yönetimi korumaya yöneliktir. Söz konusu yükümlülük, tanımlanmış bir gizliliğin varlığını gerektirmemektedir. Bazı olayları ve belgeleri idarenin kendi çıkarlarına göre gizli değerlendirmesi yeterlidir” Bkz. Musa EKEN, s.35-36.

⁹⁰ Bkz. TCK m. 239, Gerekece. Ayrıca Vergi Usul Kanununun 362. maddesi uyarınca vergi mahremiyetini ihlal edenler de TCK'nın 239. maddesi uyarınca cezalandırılacaktır.

⁹¹ Ticari Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısında bu deyimlerin tanımları yer almaktadır. Tasarının 2. maddesi uyarınca “Bu kanunda geçen a) Ticarî sır: Bir ticarî işletme veya şirketin faaliyet alanı ile ilgili yalnızca belirli sayıdaki mensupları ve diğer görevlileri tarafından bilinen, elde edilebilen, özellikle rakipleri tarafından öğrenilmesi halinde zarar görme ihtimali bulunan ve üçüncü kişilere ve kamuya açıklanmaması gereken, işletme ve şirketin ekonomik hayattaki başarı ve verimliliği için büyük önemi bulunan; iç kuruluş yapısı ve organizasyonu, malî, iktisadî, kredi ve nakit durumu, araştırma ve geliştirme çalışmaları, faaliyet stratejisi, hammadde kaynakları, imalatının teknik özellikleri, fiyatlandırma politikaları, pazarlama taktikleri ve masrafları, pazar payları, toptancı ve perakendeci müşteri potansiyeli ve ağırları, izne tâbi veya tâbi olmayan sözleşme bağlantılarına ilişkin veya bu gibi bilgi ve belgeleri, b) Banka sırrı: Bankanın yönetim ve denetim organlarının üyeleri, mensupları ve diğer görevlileri tarafından bilinen malî, iktisadî, kredi ve nakit durumu ile ilgili bilgilerle, bankanın müşteri potansiyeli, kredi verme, mevduat toplama, yönetim esasları, diğer bankacılık hizmet ve faaliyetleri, risk pozisyonlarına ilişkin her türlü bilgi ve belgeleri, c) Müşteri sırrı: Ticarî işletme ve şirketlerin, bankaların, sigorta şirketlerinin, sermaye piyasasında ve malî piyasalarda faaliyet gösteren aracı kurumların, kendi faaliyet alanlarıyla ilgili olarak müşteriyle ilişkilerinde, müşterinin şahsî, iktisadî, malî, nakit ve kredi durumuna ilişkin doğrudan veya dolayısıyla edindikleri tüm bilgi ve belgeleri, ifade eder”. Bkz. http://www.alomaliye.com/2008/ticari_sir_tasarisi.doc.

hakları kapsamında değerlendirildiğine göre, ancak gerçek kişilere ilişkin bilgiler söz konusu olduğunda devreye girebilir. Öyleyse tüzel kişilere ilişkin bilgiler ancak bir gerçek kişiyle ilişkili olduğu ölçüde bu korumadan yararlanacaktır. Bu bakımdan ticari sır ve banka sırrı kimi zaman kişisel veri niteliğindeki bilgileri içerebilir. Müşteri sırrının ise çoğu zaman bu nitelikte olacağı belirtilmelidir. Nitekim müşteri sırrı ile “işletmelerin ticari faaliyetleri esnasında müşterilerine ilişkin olarak öğrendikleri ve gizli tutmak durumunda oldukları bilgiler” ifade edilir⁹².

TCK’nın 258. maddesinde ise kamu görevlileri açısından “göreve ilişkin sırrın açıklanması” düzenlenmiştir⁹³. Buna göre “(g)örevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği ve gizli kalması gereken belgeleri, kararları ve emirleri ve diğer tebligatı açıklayan ve yayınlayan veya ne suretle olursa olsun başkalarının bilgi edinmesini kolaylaştıran kamu görevlisine, bir yıldan dört yıla kadar hapis cezası verilir”⁹⁴. Bu hüküm kişisel veriler açısından dolaylı da olsa bir koruma getirmektedir. Nitekim belirtilen nitelikteki belgeler, kişisel veriler de içerebilir. 239. maddenin aksine burada belirlenen suç şikayete bağlı değildir.

Kamu görevlilerinin üzerine düşen bu yükümlük yönetime duyulan güvenin de bir gereğidir⁹⁵. Nitekim bu hüküm, TCK’nın “Kamu İdaresinin Güvenilirliğine ve İşleyişine Karşı Suçlar” başlıklı dördüncü kısmın birinci bölümünde düzenlenmiştir. Bu bağlamda yukarıda incelenen kişisel verilerin kaydedilmesi ve verileri hukuka aykırı olarak verme veya ele geçirme suçlarının kamu görevlisi ve görevinin verdiği yetki kötüye kullanılarak işlenmesinin ağırlaştırıcı neden olarak belirlenmesinin de aynı nedenden kaynaklandığı söylenebilir⁹⁶.

Son olarak TCK’nın “Bilişim Suçları” başlıklı üçüncü kısım, onuncu bölümünde yer alan suçların da kimi durumlarda dolaylı olarak kişisel verilerin

⁹² Mehmet Emin BİLGE, **Ticari Sırların Korunması**, Asil Yayın, 2. Baskı, Ankara 2005, s. 34-35.

⁹³ Kamu görevlisi, TCK’nın 6/c hükmünde “kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi” olarak tanımlanmıştır. Kamu görevlisi kavramına ilişkin geniş açıklama için bkz. Hasan Tahsin GÖKCAN, Mustafa ARTUÇ, **Ceza ve Ceza Usul Hukukunda Kamu Görevlisi Kavramı ve Özel Soruşturma Usulleri**, Seçkin, Ankara 2007.

⁹⁴ TCK m. 258/1.

⁹⁵ Geniş anlamda kamu görevlisi “hukuki durumlarına ve yaptıkları görevin niteliğine bakılmaksızın, kamu kesiminde ve de Devletin bütün organlarında görev yapan herkesi ifade etmektedir”. Bkz. Metin GÜNDAY, **İdare Hukuku**, 9. Baskı, İmaj, Ankara 2004, s. 516

⁹⁶ TCK m. 137.

korunmasına yardımcı olabileceği belirtilmelidir⁹⁷. Özellikle “*bilişim sistemine girme*”(m. 243) ve “*sistemi engelleme, bozma, verileri yok etme veya değiştirme*” (m. 244), çalışmamızın üçüncü bölümünde ayrıntılı olarak üzerinde durduğumuz veri güvenliğinin sağlanmasına yardımcı olacaktır.

Görüldüğü gibi TCK kapsamında kişisel verilerin hukuka aykırı olarak kaydedilmesi, ele geçirilmesi, verilmesi, yayılması ve yok edilmemesi konularında belirli oranda bir koruma getirilmiştir. Kişisel verilere hukuka aykırı müdahalelerde cezai yaptırımının uygulanabilmesi için öncelikle bu işlem ve eylemlerde uyulacak esasların belirlenmesi gerekir⁹⁸. Ancak halen bu alanda uygulanacak ilkeleri belirleyen bir kişisel verilerin korunması yasası mevzuatımızda bulunmadığı için bu işlem ve eylemlere ilişkin uyulacak esaslar belirsizliğini korumaktadır.

V. KOLLUK FAALİYETLERİNDE KİŞİSEL VERİLERİN KORUNMASI

A. GENEL OLARAK

Kolluk etkinliklerini idari kolluk ve adli kolluk olarak ikiye ayırmak gerekir. Ülkemizde idari kolluk ve adli kolluk, görevleri ve amaçları yönünden birbirinden farklıdır. Ancak teşkilatı ve görevlileri açısından birbirine karışmış durumdadır⁹⁹. Bu, kimi zaman her iki tür kolluğun birbirinden ayrılmasını güçleştirmektedir¹⁰⁰. Konuya ilişkin açıklamalara geçmeden önce bu farklılık üzerinde kısaca durmak gerekir. Nitekim idari kolluk ve adli kolluk etkinlikleri kişisel verilerin korunması açısından farklı sonuçları beraberinde getirebilmektedir.

⁹⁷ Ayrıntılı bilgi için bkz. Muammer KETİZMEN, s. 57-188; Levent KURT, **Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Seçkin, Ankara 2005, s. 139-278.

⁹⁸ Oğuz ŞİMŞEK, s. 191.

⁹⁹ Metin GÜNDAY, s. 250.

¹⁰⁰ Örneğin CENTEL ve ZAFER böyle bir soruna işaret etmişlerdir. Yazarlara göre “(s)uçlardan adli kolluğun ve cumhuriyet savcılığının haberdar olduğu hallerde, önleme ve adli amaçlı tedbirlerin hangisine başvurulacağı sorun yaratacak niteliktedir. Bu durum yetki çatışmalarına neden olabilir”. Nur CENTEL, Hamide ZAFER, **Ceza Muhakemesi Hukuku**, 6. Baskı, Beta, İstanbul 2008, s. 397.

Her insan topluluğu ortak yaşamı rahat ve huzurlu sürdürebilmek için düzene gereksinim duyar. Bunun kaçınılmaz bir sonucu olarak idarenin en başta gelen görevi kamu düzenini korumak ve insanların güvenlik ve huzur içinde yaşamalarını sağlamaktır. İdarenin bu amaçla yürüttüğü etkinliklere kolluk faaliyetleri denilmektedir¹⁰¹. Bu anlamda idari kolluk kamu düzeninin bozulmasını önlemekle görevlidir ve etkinliklerini bu amaç doğrultusunda yürütür. Bir başka anlatımla, idari kolluk yasaların suç saydığı bir eylem henüz işlenmeden, kamu düzenini tehdit eden bir durum ortaya çıktığında görevini yürütür.

Adli kolluk ise kamu düzenini bozan ve suç sayılan eylemlerin işlenmesi halinde harekete geçer. Amacı, suç faillerini ve delillerini araştırıp bulmak ve bunları adli mercilere teslim etmektir. O halde idari kolluğun aksine adli kolluğun, yasaların suç saydığı eylemlerin işlenmesinden sonra harekete geçtiğini ve adli kovuşturma amacıyla yürütülen bir etkinlik olduğunu söyleyebiliriz. Bunun sonucunda adli kolluğun bastırıcı niteliği öne çıkarken, idari kolluğun etkinlikleri daha çok önleyici ve durdurucu niteliktedir¹⁰².

Adli kolluk ve idari kolluk etkinlikleri kişisel verilerin korunması açısından değerlendirildiğinde farklı sonuçları beraberinde getirir. Çünkü yasaların suç saydığı bir eylemin gerçekleştirilmesinin ardından parmak izi, DNA profili gibi kişisel verilerin toplanması ve değerlendirilmesi, şüpheli veya sanığın telefon görüşmelerinin dinlenmesi ya da görüntülerinin kayıt altına alınması ile genel asayişin sağlanması, suçluluğun önlenmesi gibi gerekçelerle belirsiz sayıda kişiye ilişkin bu bilgilerin toplanması ve değerlendirilmesi birbirinden farklıdır. Nitekim

¹⁰¹ Metin GÜNDAY, s. 245. Yukarıda ilgili bölümde açıklandığı üzere neden ve sonuçlarındaki farklılık dolayısıyla çalışmamızda idari ve adli kolluk faaliyetlerinin kişisel verilerin korunması ile ilişkili olarak değerlendirilmesi ayrı ayrı yapılmıştır. Dolayısıyla bu alt başlık kapsamında yalnızca idari kolluk faaliyetleri değerlendirilecektir.

¹⁰² Metin GÜNDAY, s. 250. Ayrıca bkz. Kemal GÖZLER, **İdare Hukuku Dersleri**, 5. Baskı, Ekin, Bursa 2007, s. 561-564; İsmet GİRİTLİ, Pertev BİLGİN, Tayfun AKGÜNER, **İdare Hukuku**, 3. Baskı, Der, İstanbul 2008, s. 919-924. Adli kolluğa ilişkin olarak bkz. Nurullah KUNTER, Feridun YENİSEY, Ayşe NUHOĞLU, **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku**, Beta, 15. Baskı, s. 380-431. Adli kolluğun tanımı ve görevleri CMK'nın 164. maddesinde şöyle belirlenmiştir: "(1) Adli kolluk; 4.6.1937 tarihli ve 3201 sayılı Emniyet Teşkilatı Kanununun 8, 9 ve 12 nci Maddeleri, 10.3.1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun 7 nci Maddesi, 2.7.1993 tarihli ve 485 sayılı Gümrük Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 8 inci Maddesi ve 9.7.1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanununun 4 üncü Maddesinde belirtilen soruşturma işlemleri yapan güvenlik görevlilerini ifade eder. (2) Soruşturma işlemleri, Cumhuriyet savcısının emir ve talimatları doğrultusunda öncelikle adli kolluğa yaptırılır. Adli kolluk görevlileri, Cumhuriyet savcısının adli görevlere ilişkin emirlerini yerine getirir. (3) Adli kolluk, adli görevlerin haricindeki hizmetlerde, üstlerinin emrindedir".

burada her iki etkinliğin bir arada incelenmesinin bir nedeni de bu farkın önemli sonuçları bulunduğunu açıkça ortaya koyabilmektir. Türkiye’de bu konu yakın zamanda özellikle yaygın telefon dinlemeler dolayısıyla tartışılmıştır. Ancak sorun bununla sınırlı değildir.

Özellikle teknolojideki gelişmeler sorunun boyutlarının artmasına neden olmaktadır. Teknoloji geniş kitlelere ilişkin bilgilerin toplanmasını, değerlendirilmesini ve kullanılmasını olanaklı kılmaktadır. Bu ise, daha önce de değindiğimiz üzere, temel hak ve özgürlükler ile ilgili pek çok soruyu beraberinde getirir. Çeşitli idari ve adli kolluk etkinliklerinin kişisel verilerin korunması açısından değerlendirilmesine geçmeden önce bu sorun, Anayasa Mahkemesinin de önüne gelen bir örnek üzerinden incelenebilir.

1996 yılında 1774 sayılı Kimlik Bildirme Kanununa eklenen bir hüküm Anayasa Mahkemesinin önüne gelmiştir¹⁰³. Davacılar iptali istenen hüküm ile genel kolluk kuvvetlerinin bilgisayarlarında kişisel bilgilerin toplanması yetkisinin tanındığını ve yetkinin hangi koşullarda verileceğinin ve yetki kullanılırken hangi ilkelere uyulması gerektiğinin belirtilmemesi nedeniyle kuralın demokratik toplum düzeninin gerekleri, Anayasanın 2., 13. ve 20. maddelerine aykırı olduğunu ileri sürmüştür. Oysa Anayasa Mahkemesince *“1774 sayılı Yasa’nın 2. maddesinde sayılan özel veya resmî her türlü konaklama tesislerinden Bakanlar Kurulu’nca belirlenenlerde tutulacak kayıtların genel kolluk kuvvetlerinin bilgisayar terminallerine bağlanması zorunluluğunu getiren dava konusu kuralın, kamu düzeni, genel asayiş ve kamu yararını sağlama amacına yönelik olması ve demokratik toplum düzeninin gereklerine de aykırı bir yönü bulunmaması nedeniyle, Anayasa’nın 2. 13. ve 20. maddelerine aykırı olmadığı sonucuna varılmıştır. İptal isteminin reddi gerekir”*.

¹⁰³ AYMK, E. 1996/68; K. 1999/1; t. 6 Ocak 1999. İptali istenen hüküm şöyledir: *“(1) Bu Kanunun uygulanması sırasında genel kolluk kuvvetlerine ait karakollara, il merkezlerinden de sorgulanabilen bilgisayar terminalleri konulur. Bunun için gerekli giderler İçişleri Bakanlığı bütçesine konulacak ödenekten karşılanır. (2)İdarenin bilgisayar sistemi kurması ve gerekli teknik altyapıyı hazırlamasıyla birlikte, bu Kanunun 2 nci maddesinde sayılan özel veya resmi, her türlü konaklama tesislerinden, Bakanlar Kurulunca belirlenecek olanlar, tespit ve ilan tarihinden itibaren 3 yıl içerisinde tüm kayıtlarını bilgisayarda tutmak ve bilgisayar terminallerini genel kolluk kuvvetlerinin bilgisayar terminallerine bağlamak zorundadırlar. Bu şartı yerine getirmeyen kuruluşlara 50 milyon lira para cezası verilir. Tekrarı halinde işletme ruhsatları iptal edilir.”*

Burada Anayasa Mahkemesinin dayandığı 13. ve 20. maddeler yukarıda da işaret edildiği üzere 2001 yılında yapılan Anayasa değişiklikleri kapsamında yeniden düzenlendiğini belirtmek gerekir. Buna göre artık Anayasanın 13. maddesi temel hak ve özgürlükleri genel sınırlama hükmü olmaktan çıkmış ve sınırlamaların sınırını belirleyen bir kural haline gelmiştir. Bu nedenle özel yaşamın gizliliği hakkının sınırlarını saptamak için ilgili hükme bakmak gerekecektir. Yine aynı değişiklik kapsamında 20. maddenin birinci fıkrasında yer alan “*Adli soruşturma ve kovuşturmaların getirdiği istisnalar saklıdır*” hükmü madde metninden çıkarılmış ve ikinci fıkrada ise yalnızca kişilerin üstü, özel kâğıtları ve eşyasının aranması ve bunlara el konulmasına ilişkin koşullar belirlenmiştir.

O halde Anayasa Mahkemesinin önüne bugün benzer nitelikte bir olay gelmesi durumunda kararının değişeceği söylenebilir. Ancak kanımızca kararın verildiği tarihte yürürlükte olan hükümler çerçevesinde de uygulama Anayasaya aykırıdır. Belirtilen uygulama idari kolluk görevlilerinin hizmetine önemli kişisel verileri sunmakta, ancak bunların hangi amaçlar için, nasıl kullanılabileceğine ilişkin herhangi bir sınır öngörmemektedir. Bu temel hak ve özgürlüklere ciddi bir müdahaledir¹⁰⁴.

İdarenin elinde bugün on yıl öncesinden çok daha geniş bilgi kaynakları bulunmaktadır. Bu kanallardan akan bilgiler geniş veri tabanlarında saklanmakta ve kullanılmaktadır. Bu noktada ülkemizde kişisel verilerin korunmasına ilişkin kapsayıcı bir hukuksal düzenlemenin eksikliği hemen hemen her alanda hissedilmektedir. Kolluk etkinlikleri kapsamında gerçekleştirilen çeşitli etkinliklerde de bu boşluk temel hak ve özgürlüklerin ciddi oranda zarar görmesine neden olmaktadır. Aşağıda adli ve idari kolluk etkinliklerinde kişisel verilerin işlenmesine yönelik düzenlemelere ilişkin genel bir çerçeve çizilmeye çalışılacaktır. Birbirinden ayırmanın güçlüğüne karşın etkinliklerinin sonuçların bakımından ortaya çıkan önemli farkı açıkça ortaya koymak amacıyla adli ve idari kolluğun aynı başlık altında değerlendirilmesi tercih edilmiştir.

¹⁰⁴ Nitekim itiraz gerekçesinde de şu ifade yer almaktadır: “*iptali istenen hüküm, genel kolluk kuvvetlerinin bilgisayarlarında kişisel bilgilerin toplanması yetkisini tanımış, fakat bu yetkinin Anayasal haklara getireceği sınırlamayı sınırlamamıştır. Söz konusu yetkinin hangi koşullarla verilebileceği ve yetki kullanılırken hangi ilkelere uyulması gerektiği Avrupa hukuku çerçevesinde ayrıntılı bir şekilde belirlenmiştir. Avrupa ile bütünleşmeyi amaçladığını her fırsatta dile getiren bir ülkede, bu esaslara uyulmadan yapılan düzenleme, demokratik toplum düzeninin gerekleriyle bağdaşamaz*”.

B. ÖZEL İLETİŞİME MÜDAHALE

Telefon, posta gibi araçlarla yapılan özel iletişime müdahale, yasalarımızda belirli koşullara bağlanmıştır. Yukarıda da işaret edildiği gibi temel bir hak olan haberleşme özgürlüğüne müdahalenin sınırları öncelikle Anayasanın ilgili hükmünde çizilmiştir¹⁰⁵. Başta Ceza Muhakemesi Kanunu¹⁰⁶ (CMK) olmak üzere ilgili yasalarda ise usul ve esasları belirlenmiştir. Daha önce de açıklandığı üzere haberleşme özgürlüğü ile kişisel verilerin korunması hakkı yakından ilişkilidir. Kişilerin özel haberleşmeleri önemli oranda kişisel veri içerdiğinden hem haberleşme özgürlüğü, hem de kişisel verilerin korunması hakkının kapsamında değerlendirilebilir. AİHM de özel haberleşmeye yapılan müdahaleyi Sözleşmede özel yaşamın gizliliği hakkının düzenlendiği 8. maddesi kapsamında değerlendirmektedir. Bu noktada Mahkemenin özel haberleşme şekilleri arasında da bir ayrım öngörmediğini belirtmek gerekir. Her ne kadar AİHS’de modern iletişim şekillerine ilişkin bir ifade yer almasa da Mahkeme, birbirini izleyen kararlarında, telefon görüşmelerini¹⁰⁷, görüşülen kişilerin numaralarını¹⁰⁸, ses kaydını¹⁰⁹, e-posta ve İnternet aracılığıyla yapılan iletişimi¹¹⁰ 8. madde kapsamında görmüştür¹¹¹.

Türkiye’de CMK’nın 135 vd. maddelerinde “*telekomünikasyon yoluyla yapılan iletişimin denetlenmesi*” düzenlenmiştir¹¹². 135. madde uyarınca bazı

¹⁰⁵ Bkz. AY. m. 22.

¹⁰⁶ Ceza Muhakemesi Kanunu, Kanun no. 5271, t. 04 Aralık 2004, RG. t. 17 Aralık 2004, S. 25673.

¹⁰⁷ *Klass ve diğ. kararı*.

¹⁰⁸ *Malone, Birleşik Krallık’a karşı*, b.n. 8691/79, k.t. 2 Ağustos 1984.

¹⁰⁹ *P.G. ve J.H., Birleşik Krallık’a karşı*, b.n. 44797/98, k.t., 25 Eylül 2001.

¹¹⁰ *Copland, Birleşik Krallık’a karşı*, b.n. 62617/00, k.t. 3 Nisan 2007.

¹¹¹ Paul J. A. De HERT, s. 46.

¹¹² CMK’nın 135-138 madde hükümleri Genel Hükümler içerisinde I. Kısım, 5. bölümde düzenlenmiştir. 5. Bölümün başlığı “*telekomünikasyon yoluyla yapılan iletişimin denetlenmesi*”dir. Burada yer alan hükümler eski CMUK’da bulunmadığından hukuk düzenimiz açısından yeni oldukları söylenebilir. CMK’nın yürürlüğe girmesinden önce telekomünikasyon yoluyla iletişimin denetimine ilişkin hükümleri 2005 yılında ilga edilen 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanununda bulmak olanaklıydı. Fransızca kökenli bir kelime olan telekomünikasyon TDK Büyük Türkçe Sözlük’e göre “*Haber, yazı, resim, sembol veya her çeşit bilginin tel, radyo, optik vb. elektromanyetik sistemlerle iletilmesi, bunların yayımı veya alınması, uz iletişim*”dir. Bkz. <http://www.tdk.gov.tr> .Telekomünikasyon etkinliklerinin amacı “*nerede, nasıl üretilmiş, işlenmiş ya da nerede depolanmış olursa olsun, her türlü işaret, ses, sembol, görüntü ve diğer elektriksinyallere dönüştürülebilen her türlü verinin muhataplara iletilmesi, gönderilmesi, alınması suretiyle kişiler, kurumlar, bilgisayarlar ve sistemler arasında iletişiminin hızlı, etkin, kesintisiz ve kaliteli bir şekilde sağlanmasıdır*”. Şerafettin EKİCİ, **Özel Sektöre Açıldıktan Sonra Türk Telekomünikasyon Hukuku (Elektronik İletişim)**, Vedat, İstanbul 2006, s. 4. Aşağıda incelenecek Elektronik Haberleşme Kanununda ise

suçlarla ilgili olarak, yapılan soruşturma ve kovuşturmada, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Bu yola başvurulabilmesi için suç işlendiğine ilişkin kuvvetli şüphe bulunması ve başka şekilde delil elde edilememesi gerekir¹¹³. Ancak şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle yaptığı görüşmeler kayıt altına alınamaz¹¹⁴. Görüldüğü gibi özel iletişimin denetimi burada delillerin elde edilmesine yönelmiştir. Bunun gibi kimi durumlarda şüpheli ve sanığın yakalanması için de benzer tedbirlere başvurulabilir. Kişinin mobil telefonunun yerinin saptanması bu kapsamdadır¹¹⁵.

Her iki durumda da kişinin haberleşme özgürlüğüne ve kişisel verilerinin korunması hakkına müdahale söz konusudur. Ancak burada somut bir suçla yakın ilişkisi dikkatten kaçmamalıdır. Nitekim şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da hâkim onayının alınmaması halinde, uygulamaya son verilir ve saptama veya dinlemeye ilişkin kayıtlar Cumhuriyet

“telekomünikasyon” ifadesi yerine “elektronik haberleşme”nin tercih edildiği görülmektedir. Görüldüğü gibi telekomünikasyon radyo, televizyon ve benzeri araçlarla gerçekleştirilen kitlesel iletişimi de kapsamına alan bir deyimdir. Oysa CMK’nın 135 vd. hükümleri özel iletişimin denetimine ilişkin kuralları belirlemektedir. Bu nedenle örneğin KAYMAZ, bölümün başlığının “telekomünikasyon yoluyla yapılan özel iletişimin denetlenmesi” olması gerektiğine işaret etmektedir. Bkz. Seydi KAYMAZ, **Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi**, Seçkin, Ankara 2009, s. 47.

¹¹³ CMK m. 135. İletişimin dinlenmesi, kayda alınması tespiti ile sinyal bilgileri deyimleri ilgili yönetmeliklerde tanımlanmıştır. Buna göre iletişimin dinlenmesi ve kayda alınması, “Telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmalar ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemleri”, iletişimin tespiti ise “İletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri” anlamına gelir. Sinyal bilgileri ise “Bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi” ifade eder. Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi Ve Kayda Alınmasına Dair Usul Ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev Ve Yetkileri Hakkında Yönetmelik (RG. t. 10 Kasım 2005, S.25989), m.3/h, 1, p; Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik (RG. t. 14 Şubat 2007, S. 26434), m.4/e,f,h. Ayrıca bkz. Cumhur ŞAHİN, **Ceza Muhakemesi Kanunu Gazi Şerhi**, Seçkin, Ankara 2005, s. 380-381.

¹¹⁴ CMK m. 135/2.

¹¹⁵ CMK m. 135/4 uyarınca “Şüpheli veya sanığın yakalanabilmesi için, ... mobil telefonun yeri, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararına istinaden tespit edilebilir. Bu hususa ilişkin olarak verilen kararda, ... mobil telefon numarası ve tespit işleminin süresi belirtilir. Tespit işlemi en çok üç ay için yapılabilir; bu süre, bir defa daha uzatılabilir”.

savcısının denetimi altında en geç on gün içinde yok edilir¹¹⁶. Bu durumda soruşturma evresinin bitiminden başlayarak, en geç onbeş gün içinde, Cumhuriyet Başsavcılığı, tedbirin nedeni, kapsamı, süresi ve sonucu hakkında ilgisine yazılı olarak bilgi verir¹¹⁷.

Yazılı haberleşmeye müdahalenin koşulları ise CMK'nın 129. maddesinde belirlenmiştir. Buna göre *“(s)uçun delillerini oluşturduğundan şüphe edilen ve gerçeğin ortaya çıkarılması için soruşturma ve kovuşturmada adliyenin eli altında olması zorunlu sayılıp, posta hizmeti veren her türlü resmî veya özel kuruluştaki bulunan gönderilere, hâkimin veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararı ile el konulabilir”*¹¹⁸. Ayrıca bir suç dolayısıyla yapılan soruşturmada, başka şekilde delil elde etme olanağı bulunmuyorsa, savcının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verebilir¹¹⁹.

Görüldüğü gibi burada hedef, suç delillerinin elde edilmesi veya suçluların yakalanmasıdır¹²⁰. Bu niteliğiyle adli kolluk etkinliklerinin kapsamındadır¹²¹. Buna karşın iletişimin denetimi kimi durumlarda idari kolluk tarafından da gerçekleştirilebilir. Nitekim suç işlenmesinin önlenmesi veya istihbarat amacıyla iletişimin denetimi idari bir etkinliktir. Polis Vazife ve Salahiyet Kanununda (PVSK), Jandarma Teşkilat, Görev ve Yetkileri Kanununda, Devlet İstihbarat

¹¹⁶ CMK, m. 137/3.

¹¹⁷ CMK, m. 137/4. Türkiye’de telefon dinleme etkinliklerinin yaygınlığını ortaya koyan bir örnek Telekomünikasyon İletişim Başkanlığının 2009 yılında yaptığı bir açıklama ile bir kez daha görülmüştür. Çeşitli kitle iletişim araçlarına yansıyan habere göre üç yıl içinde on binlerce kişiye telefonlarının dinlendiği ancak herhangi bir suç unsuru bulunmadığı için kayıtlarının imha edildiği bildirilmiştir. Bkz. “12 bin 988 kişiye 'sizi dinledik' mektubu: Telekomünikasyon İletişim Başkanlığı son üç yıl içinde dinleyip hiçbir şüpheli bulgu ya da suç unsuruna rastlamadığı kişilere mektup göndererek dinleme kayıtlarının imha edildiğini bildirdi”, <http://www.ntvmsnbc.com/id/25022778/>.

¹¹⁸ CMK, m. 129/1.

¹¹⁹ CMK, m. 134/1.

¹²⁰ Ceza muhakemesinde karar verme yetkisi bulunanlarca başvuru ve hükümden önce temel hak ve özgürlüklere müdahaleyi gerektiren geçici yasal çareler koruma tedbiri olarak adlandırılmaktadır. Bkz. Seydi KAYMAZ, s. 51; Nur CENTEL, Hamide ZAFER, s. 302.

¹²¹ CMK’da öngörülen telekomünikasyon yoluyla iletişim denetlenmesine telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, gizli soruşturmacı ve teknik araçlarla izleme tedbirlerine ilişkin talepte bulunulması, kararların alınması ve uygulanmasında uyulacak usul ve esasları belirlemek üzere 2007 yılında bir yönetmelik kabul edilmiştir. Bkz. Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik (Adalet Bakanlığından), RG. t. 14 Ocak 2007, S. 26434.

Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda bu amaçlar doğrultusunda izleme yapılmasına ilişkin hükümler bulunmaktadır¹²². İletişime bu türdeki müdahalenin sınırlarının kesin olarak belirlenmesi temel hak ve özgürlüklerin korunması açısından oldukça önemlidir. Belirtilen yasal düzenlemeler ile yetkilendirilen Polis, Jandarma ya da MİT mensupları somut ve haklı gerekçeler olmaksızın yalnızca soyut olasılıklardan hareketle iletişime müdahale edemezler¹²³. Nitekim kişinin iletişiminin dinlenmesi ve izlenmesi özel yaşamın gizliliği hakkına ciddi bir müdahaledir.

Türkiye’de telefon dinleme etkinlikleri, özellikle bunların hukuksallığı açısından, ciddi tartışmalara neden olmuştur. 2000’li yıllara kadar Türkiye’de pek çok telefonun hukuksal dayanak bulunmaksızın yaygın şekilde dinlendiği bilinmektedir¹²⁴. Ancak tartışmalar geçen on yıl içerisinde azalmamış, aksine gündemde kalmaya devam etmiştir. İletişim teknolojilerindeki gelişmeler, bu kapsamda mobil telefonların ve e-postaların kullanımının yaygınlaşması sorunun daha ciddi boyutlara ulaşmasına neden olmuştur¹²⁵.

Teknolojideki gelişmeler, iletişimin izlenmesini daha kolay hale getirmektedir. Bu yalnızca devlet tarafından gerçekleştirilen keyfi izleme ve dinlemeler için söz konusu değildir. Artık kişilerin birbirini dinlemeleri de kolaylaşmıştır¹²⁶. Hatırlanacağı üzere yukarıda işverenlerin işçiler üzerindeki gözetiminin yaratabileceği sorunlar üzerinde kısaca durmuştuk.

¹²² Bkz. Polis Vazife Ve Selahiyet Kanunu (Kanun no. 2559, t. 4 Temmuz 1934; RG.t. 14 Temmuz 1934, S. 2751) Ek m. 7; Jandarma Teşkilat, Görev Ve Yetkileri Kanunu (Kanun no. 2803, t. 10 Mart 1983; RG t. 12 Mart 1983, S. 17985) Ek m. 5; Devlet İstihbarat Hizmetleri Ve Milli İstihbarat Teşkilatı Kanunu (Kanun no.2937, t. 1 Kasım 1983; RG. t. 3 Kasım 1983, S. 18210) m. 6. Ayrıca bkz. Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi Ve Kayda Alınmasına Dair Usul Ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev Ve Yetkileri Hakkında Yönetmelik (Başbakanlıktan), RG. t. 10 Kasım 2005; S. 25989.

¹²³ Ersan ŞEN, **Türk Hukukunda Telefon Dinleme, Gizli Soruşturmacı, X Muhbir**, 3. Baskı, Seçkin, Ankara 2009, s. 44-45.

¹²⁴ Faruk BİLDİRİCİ, **Gizli Kulaklar Ülkesi**, İletişim, Ankara 2001, s. 348; Kerem ALTIPARMAK, “Büyük Biraderin Gözetiminden Çıkış: Telefonların İzlenmesinde Devletin Sorumluluğu”, **Türkiye Barolar Birliği Dergisi**, S. 63, Mart-Nisan 2006, (29-66), <http://80.251.40.59/politics.ankara.edu.tr/altipar/Yayinlar/Buyuk%20Birader.pdf>, s. 2.

¹²⁵ 2009 yılı Eylül ayı sonu itibarıyla Türkiye’de 16,8 milyon sabit telefon hattı abonesi bulunurken, 63,7 milyon mobil abone bulunmaktadır. Bkz. Türkiye Elektronik Haberleşme Sektörü, Üç Aylık Pazar Verileri Raporu, 2009 Yıllı Üçüncü Çeyrek, Temmuz-Ağustos-Eylül, Sektörel Araştırma ve Stratejiler Dairesi Başkanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Kasım 2009, Ankara, http://www.tk.gov.tr/Yayin/pv/ucaylik09_3.pdf . Aynı rapora göre Türkiye’de 6, 4 milyon İnternet abonesi bulunmaktadır.

¹²⁶ Nitekim bu soruna Ulaştırma Bakanının da dikkat çektiği, dinleme cihazlarının denetimi hususunda yaşanan sıkıntılardan yakındığı görülmektedir. Bkz. “Dinleme cihazlarını denetleyemiyoruz: Ulaştırma Bakanı Yıldırım, dinleme cihazlarının denetimi konusunda zayıf

Bunun yanında iletişim hizmetlerinin bir bölümünü özel kuruluşların sunması da bu şirketlerin ihlallerine karşı korumanın gerekliliğini ortaya koymaktadır. Nitekim telekomünikasyon sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunmasının güvence altına alınmasına ilişkin usul ve esasları düzenlemek üzere Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik 2004 yılında kabul edilmiştir¹²⁷. Bu Yönetmelik ile güvenlik, trafik verilerinin işlenmesi, kullanım risklerini bildirme yükümlülüğü, iletişim gizliliği, istek dışı haberleşmeler (spam) gibi konularda hemen hemen AB düzenlemelerine denk hükümler getirilmiştir¹²⁸. Yönetmelik'in 8. maddesi uyarınca *“(1)Yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının izni olmaksızın, telekomünikasyonun üçüncü şahıs tarafından dinlenmesi, kaydedilmesi, saklanması, kesilmesi veya gözetimi yasaktır.*

olduklarını itiraf etti”, 7 Ocak 2010, <http://www.ntvmsnbc.com/id/25041522>. Alman kriptoloji uzmanı Karsten NOHL'un bir grup arkadaşıyla beraber 2010 başında GSM şifrelemesinde kullanılan algoritmayı kırması ve izlediği yöntemi, kullandığı araçları ve gerekli dosyaları dünya ile paylaşması cep telefonlarından yapılan görüşmelerin güvenliğini bir kez daha tartışma konusu haline getirmiştir. Bkz. Evren ÖNDER, “GSM Şifresi Kırıldı: Artık Herkes Dinleyebilir”, **NTV Bilim**, Şubat 2010, S. 12, s. 48-53.

¹²⁷ RG. t. 6 Şubat 2004, S. 25365.

¹²⁸ Yönetmelik uyarınca *“İşletmeciler verdikleri hizmetlerin güvenliğini sağlamak amacıyla, hizmetin gerektirdiği hallerde şebekenin güvenliğine ilişkin alacakları tüm gerekli teknik ve yapısal önlemleri Kurumun onayına sunar”(m.6). Ayrıca “İşletmecinin verdiği hizmetlerle ilgili olarak şebeke güvenliğinin ihlaline ilişkin, işletmeci tarafından alınan önlemlerin dışında olağanüstü bir risk söz konusu olduğunda işletmeci, riskler ve riskin giderilme yolları konusunda derhal abonelerini uyarır”. Yönetmelikte trafik verilerinin işlenmesine ilişkin esaslar da belirlenmiştir: “Telekomünikasyon hizmetlerini pazarlamak ya da katma değerli hizmetleri sağlamak amacıyla; abone veya kullanıcı kişisel bilgilerinin kullanılmasına izin verirse, işletmeci bu tür hizmetler ve pazarlama için gerekli kapsam ve sürede veriyi işleyebilir. Kullanıcı ve aboneler, kişisel bilgilerinin işlenmesi için verdikleri izinleri her zaman geri alabilirler” (m.9/1). Bunun yanında “Abone ve kullanıcılarla ilgili yer verileri sadece abone ve kullanıcıların isimsizleştirildiği veya katma değerli bir hizmetin sağlanması için gereken kapsam ve sürede abonelerin aksi başvuruları olmadığı hallerde işlenebilir. İşletmeciler, işlenecek yer verisi tipini, işlemenin amaç ve süresi ile bu bilgilerin üçüncü şahıslara katma değerli hizmet sağlama amacıyla gönderilip gönderilmeyeceği hususlarında, aboneleri bilgilendirir. Aboneler, yer verilerinin işlenmemesi için her zaman başvuru yapabilirler”(m. 15). Son olarak Yönetmelikte istek dışı haberleşmeleri reddetme hakkının tanındığı da belirtilmelidir. Yönetmelik'in 20. maddesi uyarınca *“(1)İşletmeciler kişi müdahalesi olmadan çalışan fakslar, elektronik posta, kısa mesaj gibi otomatik arama sistemlerini, abonenin önceden izni olmadan siyasi propaganda amacıyla kullanamazlar. Söz konusu otomatik arama sistemlerinin doğrudan pazarlama amacıyla kullanılması halinde kullanıcılara gelen her bir mesajı bundan sonrası için almayı reddetme hakkı ücretsiz ve kolay bir yolla sağlanır. (2)Doğrudan pazarlama amacıyla gönderilen ve kimin adına haberleşme yapıldığı hususunda göndericinin kimliğini saklayan veya alıcının bu iletişimin sonlandırılması konusunda talepte bulunacağı bir adres bulunmayan elektronik mektupların gönderilmesi abonenin bu yöndeki talebi halinde engellenir”.**

(2)İlgili trafik verilerinin ise işletmeci tarafından hizmet amaçları dışında kaydedilmesi, saklanması ve gözetimi yasaktır”.

Çalışmamızın birinci bölümünde de belirttiğimiz gibi günümüzde hızla gelişen gözetim toplumunun izleyicileri artık yalnızca “büyük birader” değil, “küçük kardeşler” de olmaktadır. Öte yandan devlet de gözetim pratiklerini yeni araçlara da yaygınlaştırmaktadır. Bu durum, gözetimin, izlemenin, denetimin istisna olmaktan çıkıp kural haline gelmesine neden olabilir. Bu tehlikeyi önleyebilmek için etkili hukuksal düzenlemeleri kabul etmek bir zorunluluktur.

Son on yılda iletişimin denetimi, bir bölümüne yukarıda işaret edilen, yasal düzenlemelerin konusu edilmişse de keyfiliğin önüne geçildiğini söylemek zordur. Yazılı ve görsel basına da yansıyan belirsiz sayıda kişiye yönelik izleme ve dinleme etkinliklerini hukuk devleti ilkesiyle bağdaştırabilmek olanaklı değildir¹²⁹. Kişilerin izlenmesine ve dinlenmesine olanak veren geniş kapsamlı hukuksal düzenlemeler ancak polis devletinde olabilir.

Özel iletişime bu şekilde müdahale edilmesi niteliği gereği gizli yürütülen bir etkinlik olması dolayısıyla kişiler izlendiklerini bilememekte, hukuk aykırı bir durum olması halinde haklarını savunamamaktadır¹³⁰. Ayrıca kamuoyunun gündemine gelen ancak kimi zaman kanıtlanamayan bu türdeki iddialar, toplumda sürekli bir

¹²⁹ Örneğin bkz. “Yargıtay üç ay dinlenmiş: Yargıtay Birinci Başkanlığı’nın usulsüz dinlendiği, hem teknik raporda hem de mahkeme kararları ile ortaya konuldu. Raporda, dinleme kayıtlarının da imha edilmeden, başka bir veri taşıyıcısına kopyalandığı belirtildi”, 19 Aralık 2009, <http://www.ntvmsnbc.com/id/25033832/> . “Kızılay üç saat çıplak: Ankara’nın merkezinde 27 Ocak 2009’da 3 saat boyunca o bölgede kimin kiminle konuştuğu belirlenip savcılığa bildirildi”, **Hürriyet** (manşet haber), 4 Haziran 2009, “Telefon dinlemeye aynen devam! Yargıtay kararına rağmen dinlemeler devam ediyor”, 18 Temmuz 2008, <http://www.gazetevatan.com>; “Dinlemeye İptal: Yargıtay, skandal yetkiye son noktayı koydu: tüm yurttaşlar şüpheli görülemez”, Cumhuriyet, 5 Haziran 2008.

¹³⁰ AİHK ve AİHM kararlarında da bu soruna işaret edildiği görülmektedir. AİHK’ye göre “ ... sadece bir ihlalin mağduru olduğunu iddia eden kişi başvuruda bulunabilir. Bununla beraber başvuru, örneğin izlemeye tabi tutulan müvekkillerinin hukuki temsili sırasında kendilerinin de gizli izlemeye tabi tutulabileceklerini veya tutulmuş olabileceklerini ve ayrıca gizli izlemeye tabi tutulan bu kişilerin daha sonra kendileri hakkında alınan önlemlerden her zaman haberdar edilmediklerini ifade etmektedirler. Davanın bu özel tarafı nedeniyle, başvuru, 25. madde anlamında mağdur olduklarının düşünülmesi gerekir”. A.g.k., par. 26. Çeviri için bkz. Osman DOĞRU, **İnsan Hakları Avrupa Mahkemesi İçtihatları**, Cilt I, Legal, İstanbul 2004, s. 252. Mahkemeye göre; “(a)çıktır ki, gizli önlem alma yetkilerinden biri bir kişiye bir kez uygulandığında, bireyin özel ve aile yaşamına ve haberleşmesine saygı hakkını kullanmasına kamu makamları tarafından yapılacak bir müdahale meydana getirecektir. Ayrıca yasanın sadece kendi başına varlığı, yasanın uygulanabileceği bütün kişileri izlenme tehdidi altına sokmaktadır. Bu tehdit, posta ve telekomünikasyon hizmetlerini kullananların haberleşme özgürlüklerini doğallıkla etkiler; bu suretle başvuranların özel ve aile yaşamı ve haberleşme haklarını kullanmalarına ‘kamu makamlarının müdahalesi’ni oluşturur”. Copland, *Birleşik Krallık’a karşı*, par. 41; çeviri için bkz. Osman DOĞRU, Cilt I, s. 257- 258.

güvensizlik ortamının oluşmasına, kişilerin sürekli izlendikleri korkusuna kapılmalarına neden olmaktadır.

Genel olarak suçlulukla mücadele gibi gerekçelerle nesnel ölçütlere bağlanmadan keyfi olarak herkesin telefonlarının dinlenmesi, e-postalarının okunması gibi etkinlikler her şeyden önce hukuk devleti ilkesine aykırı olacaktır. Hukuk devleti en genel şekliyle “*kişilere hukuk güvenliği sağlayan devlet düzenini*” ifade etmek için kullanılır¹³¹. Böylesine uygulamalar karşısında kişilerin hukuk güvenliğine sahip olduklarını söyleyebilmek olanaklı değildir. Ayrıca bu türdeki uygulamalar, haberleşme özgürlüğünü anlamsız kılar ve demokratik toplumun gerekleri ile bağdaşmaz. Çalışmamızın birinci bölümünde belirttiğimiz gibi, birey her hareketinin izlendiği, özel görüşmelerinin dinlendiği gibi bir düşünceye kapıldığında kişiliğini serbestçe geliştirmekten kaçınabilir ve bireysel özerkliğini kaybeder. Nitekim demokratik yönetimler altında yaşayanların bile hızla şeffaflaşması, adeta camdan insanlara dönüşmesi 21. yüzyılda en çok tartışılan konulardan biridir.

Bu noktada iletişimin içeriğine yönelik bir müdahalenin bulunmadığı, ancak iletişime ilişkin arama, yer bilgisi ve kimlik bilgilerinin kayıt edildiği izleme etkinliklerinin de temel haklar açısından ciddi sorunlar yarattığına işaret etmek gerekir. Nitekim AİHM içtihadı da telefon görüşmelerinin zamanı, tarihi, uzunluğu ve bu görüşmelerin kimlerle yapıldığına ilişkin bilginin “*telefonla yapılan iletişimin bir parçası*” olduğu yönündedir¹³². Belirtilen kararında Mahkeme, bu bilgiye meşru yollardan ulaşılmasının ihlalin bulunmasını engellemeyeceğine, nitekim bireyin özel yaşamına ilişkin kişisel verilerinin depolanmasının Sözleşme’nin 8/1 hükmü kapsamında değerlendirildiğine işaret etmiştir. Ayrıca Mahkeme, bu bilgilerin başkalarına açıklanmamış olmasının veya başvuranın aleyhine disiplin soruşturması veya başka işlemlerde kullanılmadığına ilişkin Hükümet’in itirazını da yersiz bulmuştur¹³³.

Daha önce de belirttiğimiz gibi iletişimin izlenmesi neredeyse içeriğinin dinlenmesi kadar ciddi sonuçlar yaratabildiği gibi, çok daha fazla sayıda kişiye

¹³¹ Şeref GÖZÜBÜYÜK, Turgut TAN, **İdare Hukuku (İdari Yargılama Hukuku)**, C. 2, Turhan, Ankara 2006, s. 3. Hukuk devleti düşüncesinin gelişimi için bkz. Kemal GÖZLER, **İdare Hukuku Dersleri**, s. 53-59; İsmet GİRİTLİ, Pertev BİLGİN, Tayfun AKGÜNER, **İdare Hukuku**, 3. Baskı, Der, İstanbul 2008, s. 56-68; İlhan ÖZAY, **Günışığında Yönetim**, Alfa, İstanbul 2002, s. 9-118.

¹³² *Halford, Birleşik Krallık’a karşı*, b.n. 20605/92, k.t. 25 Haziran 1997, par. 43.

¹³³ **A.g.k.**, par. 43.

ilişkin bu türdeki bilgilerin depo edilmesi olanaklı bulunduğundan haberleşmeye müdahalenin daha yaygın bir şekilde gerçekleşmesine de neden olabilir. Somut bir olayla bağlantı kurulmaksızın “*bir gün gerekli olursa*” düşüncesiyle kişisel verilerin kayıt altında tutulması, yaygın izleme etkinlikleri olarak karşımıza çıkmaktadır.

Burada sorun, ülkemizde de çeşitli dönemlerde tartışma konusu haline gelen “*fişleme*”lerdir. Nitekim kişilere ilişkin bilgilerin somut bir gereklilik olmaksızın toplanıp kayıt edilmesi bu sonucu beraberinde getirecektir. AİHM de kararlarında verilerin toplanması ve depolanmasının özel yaşamın gizliliğine yönelik ihlalin oluşması için yeterli olduğuna işaret etmiştir. Örneğin Amann kararına konu olan somut olayda, İsviçre vatandaşı olan ve ticaretle uğraşan başvuranın 1981 yılında eski SSCB Büyükelçiliğinde çalışan bir kişi tarafından bir sipariş için aranması, bu görüşmenin dinlenmesi ve bu görüşme dolayısıyla “*ulusal güvenlik kart fihristi*”nde kendisi hakkında bir fiş (veri kartı) düzenlenmesi söz konusudur. Başvuran, 1990 yılında bu fişlerden haberdar olması üzerine fişlerin içeriğini öğrenmek istemiş ve kendisine bazı paragrafları sansürlenmiş olmakla birlikte bu kartın bir fotokopisi verilmiştir¹³⁴.

Amann’ın AİHM’ne başvurusunun 8. madde boyutu iki iddia açısından değerlendirilmiştir: birincisi, 1981 yılında telefon görüşmelerine müdahale edilmesi, ikincisi ise kendisi hakkında bir fiş oluşturulup, bu fişin de Konfederasyon’un Kart Fihrist’inde yer almasına ilişkindir. İsviçre hükümeti, bu fişlerde başvuranın özel yaşamına ilişkin herhangi bir hassas verinin bulunmadığı ve ayrıca bu kartın oluşturulması ve tutulması neticesinde başvuran açısından mahsurlu her hangi bir sonuç doğmadığı gibi, bu konuda üçüncü bir kişi ile de görüşülmediği itirazında bulunmuştur. Bu itiraz dolayısıyla Mahkeme öncelikle kişinin özel yaşamına ilişkin bilginin kamusal bir otorite tarafından tutulmasının tek başına 8. maddenin 1. fıkrasına aykırılık oluşturduğuna, bu bilginin daha sonra kullanımının ise belirtilen saptama üzerinde bir etki yaratmayacağına dikkat çekmiştir¹³⁵. Mahkeme “*başvuran hakkında toplanmış bilgilerin hassas olup olmadığı veya başvuran için bir rahatsızlık yaratıp yaratmadığı*” ile ilgilenmemektedir: “*Bireyin özel yaşamını ilgilendiren verilerin kamusal bir otorite tarafından tutulması, somut olayda şüpheli*

¹³⁴ Amann, İsviçre’ye karşı, b.n. 27798/95; k.t. 16 Şubat 2000, par.7-16.

¹³⁵ A.g.k., par. 68- 69.

bir kartın yaratılması ve saklanması, 8. madde anlamında başvuranın özel yaşamının gizliliği hakkının ihlal edildiği sonucuna ulaşmak için yeterlidir”¹³⁶.

Türk hukuk mevzuatı açısından baktığımızda bu türdeki uygulamaların kimi zaman doğrudan yasadan kaynaklandığı da görülmektedir. Örneğin 5651 sayılı yasa uyarınca erişim sağlayıcı “(s)ağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla” yükümlüdür¹³⁷. Yönetmelik ile bu süre, daha açık bir şekilde bir yıl olarak belirlenmiştir¹³⁸. Çalışmamızın ikinci bölümünde İletişim Trafik Verilerinin Saklanması Yönergesine ilişkin yaptığımız açıklamalardan hatırlanacağı üzere benzer hükümler AB mevzuatında da bulunmamaktadır. Ancak daha önce de belirttiğimiz gibi bu hükümler ciddi tartışmalara neden olmuş ve kuvvetli eleştirilere maruz kalmıştır. Üstelik bu türdeki hükümlere ilişkin duyulan endişe, burada toplanan bilgilerin kullanım alanlarının sınırlı olmasına ve AB’de kişisel verilerin korunmasını sağlayan güçlü hukuksal metinlerin varlığına rağmen sürmektedir. Oysa Türkiye’de kişisel verilerin korunmasına ilişkin kapsayıcı yasal bir düzenleme bulunmadan, denetim organı oluşturulmadan bu verilerin saklanması öngörülmüştür. Bunun yaygın gözetime ilişkin var olan endişeleri güçlendireceğini gözden kaçırmamak gerekir¹³⁹.

C. GÖRÜNTÜ KAYDI

Son yıllarda artan oranda kullanılan görüntü kayıt cihazları ile kamusal ulaşılabilir alanların gözetimi kişisel verilerin korunması açısından değerlendirilmesi gereken bir başka önemli konudur. 1970’lerden günümüze hem kamu hem de özel sektörde başta kapalı devre televizyon sistemleri¹⁴⁰ olmak üzere çeşitli yöntemlerle

¹³⁶ A.g.k., par. 70.

¹³⁷ İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Kanun No. 5651, t. 4 Mayıs 2007; RG. t. 23 Mayıs 2007, S. 26530.

¹³⁸ İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik (Başbakanlıktan), RG. t. 30 Kasım 2007, S. 26716, m. 8/b.

¹³⁹ Aynı yönde bkz. Yaman Akdeniz, Kerem Altıparmak, **İnternet: Girilmesi Tehlikeli ve Yasaktır**, s. 130-132.

¹⁴⁰ “Kapalı devre televizyon”, İngilizce bir deyim olan “close circuit television”ın Türkçe karşılığıdır.

görüntülü gözetimin artarak sürdüğü görülmektedir¹⁴¹. Kayıt edilen görüntüler çoğu zaman bir kişinin doğrudan ya da dolaylı olarak belirlenmesine olanak tanımaktadır. Bu nedenle kişisel verilerin korunması ilkelerinin burada da geçerli olması gerekir. Nitekim bu türdeki görüntü kayıt eden araçların kişisel verilerin korunması açısından yaratabileceği sorunlara daha önce de değinmiştik.

Kapalı devre televizyon sistemlerinin gözlemleyici, müdahaleci ve/veya caydırıcı gözetim amacıyla kurulduğu görülmektedir. Bu sistemler, bina, cadde gibi belirli bir objenin güvenliğini sağlamak ya da trafik akışını izlemek gibi amaçlarla kullanılabilir gibi, şüpheli ya da sanık gibi belirli bir kişinin izlenmesine yönelik olabilir ya da suç işlenmesini önlemek amacıyla stadyumlar, otobüs terminalleri gibi kamusal alanların gözetimi için de kullanılabilir¹⁴². Konumuz açısından öncelikle bu kayıtların bir kişinin kimliğinin belirlenmesini sağlayıp sağlayamayacağı değerlendirilmelidir. Nitekim görüntüler, kişisel veriler ile ilişkili olmadığından konumuz açısından bir değerlendirme yapmak da gerekmeyecektir. Kapalı devre televizyon sisteminin trafik akışının izlenmesi için kullanıldığı çoğu durum böyledir. İkinci olarak alınan görüntülerin yalnızca o an izlenmesi ve kayıt edilip arşivlenmesi arasında da bir ayrım öngörmek gerekir.

AIHM de bir kararında kişilerin kamusal ulaşılabilir alanlarda görsel olarak izlenmesinin ancak bu görüntülerin kayıt edilmemesinin özel yaşama müdahale olmayacağına işaret etmiştir. Ancak görüntülerin kayıt edilmesi ve bu kaydın sistemli

¹⁴¹ Video ile kamusal alanların izlenmesine ilişkin 1950’li yıllarda bazı uygulamalara rastlanmaktadır. Örneğin ABD’de 1956 yılında bazı şehirlerde suçluluğun önlenmesinde polislere yardımcı olmak amacıyla kimi caddelerin video ile izlendiği bilinmektedir. Daha sonra 1960’lı yıllarda da çeşitli projeler geliştirilmişse de bu ilk girişimlerin pek de başarılı olmadığını belirtmek gerekir. Bkz. Robert D. BICKEL, Susan BRINKLEY, Wendy WHITE, “Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?”, *Stetson Law Review*, C. 33, Y. 2003-2004, s. 301-306 (299-367). 1970’lerden günümüze video kayıtları ile gözetimin gelişimine ilişkin genel bir bilgi için bkz. Giovanni BUTTARELLI, **Protection of personal data with regard to surveillance (2000) and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance**, s. 2-3. Günümüzde örneğin İngiltere’de 2005 yılındaki terör saldırılarının ardından devlet, 1,5 milyonun üzerinde kamerayı kullanıma sokmuştur. Londra’da yaşayan bir kişinin 300 kareden fazla resminin yalnızca bir günde kayıt edildiği tahmin edilmektedir. Bkz. “Video Surveillance”, Electronic Privacy Information Center, <http://epic.org/privacy/surveillance/> . Ayrıca bkz. Benjamin Jervis GOOLD, **CCTV and Policing: Public Area Surveillance and Police Practices in Britain**, Oxford University Press, Büyük Britanya 2004.

¹⁴² Oğuz ŞİMŞEK, s. 162-163.

ya da kalıcı yapılması bu durumu değiştirir¹⁴³. Bu, amaca bağlılık ilkesinin de bir gereğidir. Buna göre kişilerin neden izlendiği her zaman göz önünde tutulmalıdır. Meşru amaca ulaşmak için örneğin verilerin kayıt edilmesi mutlaka gerekmiyorsa bu yolla başvurulmamalıdır. Bunun gibi kayıtların kişilerin kimliğini belli edecek şekilde tutulması gerekmiyorsa kayıtlar anonim olarak tutulmalıdır¹⁴⁴.

Türkiye’de hem adli hem de idari kolluk etkinlikleri çerçevesinde video gözetimi yapılmaktadır. CMK’nın 140. maddesi, Jandarma Teşkilat Görev ve Yetkileri Kanununun ek 5. maddesi, Polis Vazife ve Selahiyet Kanunun ek 7. maddesinde kişilerin teknik araçlarla görüntü kaydının alınmasının ve bu şekilde izlenmelerinin hukuksal temelleri bulunmaktadır.

CMK’nın 140. maddesine göre hükümde belirtilen suçlardan birinin işlendiği konusunda kuvvetli şüphe bulunması ve başka şekilde delil elde edilememesi durumunda, şüpheli veya sanığın kamuya açık yerlerdeki etkinlikleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir¹⁴⁵. Teknik araçlarla izleme, “şüpheli veya sanığın kamuya açık yerlerdeki faaliyetlerinin ve işyerinin teknik araçlarla izlenmesi ses ve görüntü kaydının alınmasıdır”¹⁴⁶. Özel iletişime

¹⁴³ Peck, Birleşik Krallık’a karşı, b.n. 44647/98, k.t. 28 Nisan 2003, par. 59. (D)Rotaru ve Amann kararlarında kamusal otorite tarafından, gizli izleme teknikleri kullanılsa bile, verilerin toplanmasının başvuranın özel yaşamına müdahale oluşturacağı belirtilmiştir. *Rotaru, Romanya’ya karşı*, par. 43-44; *Amann, İsviçre’ye karşı*, par. 65- 67. *P.G. ve J.H. kararında* da, polis hücrelerinde polis tarafından dinlenirken sesleri kalıcı olarak kayıt edilen başvuruların seslerinin daha sonra değerlendirilmesi kişisel verilerinin işlenmesi olarak kabul edilmiş ve özel yaşama müdahale oluşturduğuna karar verilmiştir. *P.G. ve J.H., Birleşik Krallık’a karşı*, par. 59-60.

¹⁴⁴ Nitekim bu gerekliliklere AK bünyesinde hazırlanan konuya ilişkin bir raporda da işaret edildiği görülmektedir. Bkz. **Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance(2003)**, European Committee on Legal Co-operation, 20-23 Mayıs 2003.

¹⁴⁵ CMK 140/1 hükmü uyarınca bu suçlar şunlardır: “a) Türk Ceza Kanununda yer alan; 1. Göçmen kaçakçılığı ve insan ticareti (Madde 79, 80); 2. Kasten öldürme (Madde 81, 82, 83), 3. Uyuşturucu veya uyarıcı Madde imal ve ticareti (Madde 188), 4. Parada sahtecilik (Madde 197), 5. Suç işlemek amacıyla örgüt kurma (iki, yedi ve sekizinci fıkralar hariç, Madde 220), 6. (Ek alt bend: 25/05/2005-5353 S.K./19.mad) *1* Fuhuş (Madde 227, fıkra 3), 7. İhaleye fesat karıştırma (Madde 235), 8. Rüşvet (Madde 252), 9. Suçtan kaynaklanan malvarlığı değerlerini aklama (Madde 282), 10. Silahlı örgüt (Madde 314) veya bu örgütlere silah sağlama (Madde 315), 11. Devlet Sırlarına Karşı Suçlar ve Casusluk (Madde 328, 329, 330, 331, 333, 334, 335, 336, 337) suçları; b) Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (Madde 12) suçları; c) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar; d) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74 üncü Maddelerinde tanımlanan suçlar”.

¹⁴⁶ Süheyl DONAY, **Ceza Muhakemesi Kanunu Şerhi**, Beta, İstanbul 2009, s. 232. MALKOÇ ve YÜKSEKTEPE’ye göre ise burada geçen izlemeden maksat “belirli bir süre devam eden ve kişilerin hareket, ilişki veya başkalarıyla yaptıkları konuşmaların tespiti amacını güden

müdahalede olduğu gibi ses ve görüntü kaydeden teknik araçlarla izleme de bir koruma tedbiridir¹⁴⁷. Burada belirtilen koşullar gerçekleşmeden yapılan izleme, TCK'nın 134. maddesinde düzenlenen özel yaşamın gizliliğini ihlal suçunu oluşturabilir¹⁴⁸. Verilerin yok edilmemesi ise yine TCK'nın 138. maddesi uyarınca suç teşkil eder.

Adli kolluk etkinliklerinde kapalı devre televizyon sistemleri ile gözetim yapılması ile idari kolluk etkinliklerinde bunun yapılması arasında önemli bir farklılık bulunur. CMK'nın 140. maddesine dayanılarak yapılan izleme, adli kolluk faaliyetleri olmasından dolayı somut bir suç ile ilişkilidir. Ancak Polis, Jandarma ve MİT tarafından somut bir suç şüphesi bulunmadan istihbarat ya da suçların önlenmesi amacıyla kişilerin görüntülerinin izlenmesi ve kayda alınması olanaklıdır. Nitekim Türkiye'de bu konuda çeşitli uygulamaların yapıldığı bilinmektedir. Bunun belki de en bilinen örneği İstanbul valiliğinin desteği ile İstanbul Emniyet Müdürlüğü bünyesinde faaliyete geçirilen *“kent bilgi ve güvenlik sistemi”* MOBESE'dir¹⁴⁹. Sistem içerisinde yer alan çeşitli unsurların yanında *“bölge görüntüleme sistemi”* ile *“halkın yoğun olarak bulunduğu ve geçiş güzergahı olarak bilinen yerlere konulan kameralar ile, bu kameralardan alınan görüntülerin merkeze sürekli olarak aktarılıp kaydedilmesi”* söz konusudur. Asayiş, güvenlik gerekçeleriyle pek çok demokratik devlette benzer uygulamaların bulunduğu görülmektedir. Buradaki sorun ise sistemin

işlemlerdir”. İsmail MALKOÇ, Mert YÜKSEKTEPE, **Açıklamalar ve Yorumlarla 5271 sayılı Yeni Ceza Muhakemesi Kanunu**, C. I, Malkoç 2008, s. 707.

¹⁴⁷ CENTEL ve ZAFER'e göre: “teknik araçlarla izleme, koruma tedbiri niteliğinde olmayıp, delile ulaşmak için başvurulmuş bir araştırma vasıtasıdır. Ancak belirtelim ki bu işlemin bir araştırma vasıtası olarak kabulü, kişi hak ve özgürlüklerini güvence altına alacak şekilde koruma tedbirlerine paralel olarak düzenlenmesini engellememektedir. Yasallık ilkesinin, kişi hak ve özgürlüklerini kısıtlayan hükümler açısından ceza muhakemesi hukukunda da geçerli olduğu hatırlandığında, koruma tedbirleri için öngörülen bütün teminatların bu işlem açısından da kabul edilmesi zorunludur”. Nur CENTEL, Hamide ZAFER, s. 402.

¹⁴⁸ Nur CENTEL, Hamide ZAFER, s. 402.

¹⁴⁹ MOBESE'nin tam açılımı, *“Mobil Elektronik Sistem Entegrasyonu”*dur. Resmi İnternet sitesinde sistemin hedefleri şöyle belirlenmiştir: *“İstanbul halkına sunulmakta olan kamu hizmetlerinin iyileştirilmesi, yönetim işlevinin kolaylaştırılması, muhtarlık hizmetlerinin düzenlenmesi ve suç sayısının düşürülmesi hedeflenmektedir. Bu çerçevede 952 muhtarlık, 3500 polis aracı, İl ve İlçe Komuta Merkezleri ve İl Emniyet Müdürlüğü hizmetlerinin yürütülmesini sağlayan 10 ayrı sistem, yazılımlar ile entegre edilmiştir. Acil durum hizmetleri “emergency” (iftaiye, sağlık, vb.) başta olmak üzere, zamanla gerekli görülen diğer kurumların da sisteme entegre edilmesi planlanmaktadır. Böylelikle, söz konusu hizmetlerin yürütülmesiyle ilgili olarak, İstanbul ilinde görevli bulunan yöneticilerin, yönetim ile ilgili görevlerini daha etkin bir şekilde yerine getirebilmeleri mümkün olacaktır”*. <http://mobese.iem.gov.tr/>.

kurulması değil, bu konuya ilişkin herhangi bir yasal düzenlemenin bulunmamasıdır¹⁵⁰.

Oysa bu tür tedbirlerin temel hak ve özgürlüklere müdahale oluşturduğu unutulmamalıdır. Dolayısıyla bu müdahalenin meşru olabilmesi için, sınırlamanın yasayla belirlenmesi, ölçülü olması ve Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olması gerekir. Ayrıca görüntülerin bir kişinin kimliğini belirlenebilir kılması durumunda kişisel verilerin korunması ilkeleri dikkate alınmalıdır. Nitekim kişisel verilerin korunması hakkı, verinin toplanma ve işlenme şeklinden bağımsız olarak bütün kişisel verileri kapsar¹⁵¹.

Meşru bir sebebe dayanılarak yapılan müdahalelerde amaca bağlılık ilkesi hiçbir zaman göz ardı edilmemelidir. Buna göre kamera sistemleri ile gözetimde kişinin kimliği ile ilişkilendirme gerekli değilse kayıtlar anonim olarak tutulmalıdır. Yüz tanımlama sistemlerinin kullanımının yaygınlaşması bu konuya ilişkin tartışmaları arttırmaktadır. Bu gibi uygulamaların yaygınlaşması, kişilerin kendileri hakkındaki bilgileri kimlerin, hangi amaçla tuttuğunu bilme gerekliliğini bir kez daha ortaya koyar.

Kişilerin nerelerde kameralarla izlendiklerini de bilmeleri gerekir. Bunu sağlamanın belki de en kolay yolu, kapalı devre televizyon sistemleri izlenen havaalanları, tren istasyonları, meydanlar gibi kamusal ulaşılabilir alanlara bu uygulamanın varlığına ilişkin tabelalar koymaktır. Bu yaklaşım, sistemin amacına ulaşabilmesi için de gereklidir. Nitekim kameralar tek başlarına suçluluğu önleyemez ya da suçluları yakalayamaz. Ancak işlenen suçun tespit edilmesini sağlayabilir ya da

¹⁵⁰ 22 Şubat 2009 tarihinde, MOBESE sisteminin yasal dayanağı, MOBESE sistemi içerisinde elde edilen kamera görüntülerinin nerede, ne kadar süre için tutulacağını, hangi amaçlar için kullanılacağını belirleyen hukuksal bir düzenleme olup olmadığına ilişkin, bilgi edinme hakkı kapsamında İstanbul Emniyet Müdürlüğüne yaptığımız başvuru şöyle yanıtlanmıştır: MOBESE “bir sistemler bütünüdür tanımlaması olup bir çok bileşenden oluşmaktadır. İstanbul halkına sunulmakta olan kamu hizmetlerinin iyileştirilmesi, yönetim işlevinin kolaylaştırılması, diğer hizmetlerin düzenlenmesi ve suç sayısının düşürülmesi hedefinin gelişen teknolojiye ayak uydurarak yapılmasıdır. Bunun yapılmasında kanuni bir engel bulunmamakla beraber Polisin mevzuatla kendisine verilen yetki ve görevleri kapsamında teşkilatın kurulmasından beri yapılan hizmetin daha verimli olarak yapılabilmesi amacı ile Mobese kameraları kurularak faaliyete geçirilmiştir. Bu kameralara ait görüntüler hardisk içerisinde bulunduğu direk üzerindeki kamera sayısına da bağlı olarak ortalama sistem tarafından 10 gün süreyle saklanmakta, yine sistem tarafından otomatikman en eski kayıt silinerek kayda devam etmektedir. Görüntüler ilgili adli kurumun talebi üzerine ilgili mahkemelere verilmektedir”. 26 Şubat 2002 tarihli, B.05.1.EGM.4.34.00.77.14.2010/1065 sayılı bilgi edinme başvurusu.

¹⁵¹ Oğuz ŞİMŞEK, s. 169.

suçluluğun önlenmesi için bir caydırıcılık unsuru olabilir. Özellikle ikincisinin söz konusu olabilmesi için kameralar mutlaka görünür olmalıdır.

Bunun yanında görüntülerin yalnızca izlenmesi yeterli ise ayrıca bunları kayıt altına almamak gerekir. Nitekim kamusal alanda kayıt altına almadan yalnızca izleme, çevredeki başka kişilerden de yönelebilecek doğal bir durumdur. Nitekim P.G. ve J.H. Birleşik Krallık’a karşı kararında AİHM de benzer bir saptamada bulunmuştur. Mahkemeye göre (F) *“Bir kişinin evinin veya özel mülkünün dışında alınan önlemlerin, kişinin özel hayatına dahil olup olmadığının belirlenmesinde göz önünde bulundurulması gereken bir kaç unsur vardır. İnsanlar bazen kamuya açık bir biçimde kaydedilebilen veya rapor edilebilen faaliyetlere bilerek veya kasten dahil olabildikleri için, kişinin mahremiyet hakkındaki makul beklentileri, kararı belirleyen faktör olmasa da, önemli bir faktör olabilir. Sokakta yürüyen bir kişi, kaçınılmaz olarak orada bulunan diğer kişiler tarafından görünür olacaktır. Teknolojik yöntemlerle aynı kamusal mekanın izlenmesi de (örneğin kapalı devre televizyon ile güvenlik görevlilerinin izlemesi) benzer özelliktedir. Ancak kamu alanındaki bu tür bilgilerin sistematik veya kalıcı olarak kaydı söz konusu olunca, özel hayatla ilgili konular ortaya çıkmaktadır. İşte bu nedenle güvenlik görevlileri tarafından belirli bir birey hakkında toplanan dosyalar, söz konusu bilgi müdahaleci ve gizli bir yöntemle toplanmamış olsa bile, 8. madde kapsamına girer”*¹⁵².

Kamusal ulaşılabilir alanlarının sürekli olarak gözetlenmesi, güvenliğin arttırılmasından çok, kişilerin güvenlik duygularının arttırılmasına yaramaktadır. Bu güvenlik hissi için pek çok kişinin özel yaşamın gizliliği hakkından feragat ettiği bir gerçektir. Oysa koşulsuz bir vazgeçişin ağır sonuçları olacağı açıktır. Gözetim toplumuna dönüşmemek için bu türdeki müdahalelerin istisnai olmasının gerekliliği unutulmamalıdır.

D. PARMAK İZİ VE DNA ANALİZİ KAYDI

Kolluk kuvvetlerinin adli görevlerinden biri de olay yeri incelemesidir¹⁵³. Bu inceleme kapsamında kolluk kuvvetleri, olay yerinde bırakılan izleri değerlendirerek

¹⁵² P.G. ve J.H., Birleşik Krallık’a karşı, par. 57; çev. için bkz. Gilles DUETRTRE, s. 286-287.

¹⁵³ Ziyaettin KAYGUSUZ, “Olay Yeri İnceleme Çalışmalarında Bilimsellik ve Hukukilik”, **Polis Dergisi**, S.42,

suçluları saptamaya çalışır. Bu doğrultuda 20. yüzyılın başlarında en çok kullanılan yöntem parmak izi analizleri iken günümüzde bunun yanında DNA profillerine de artan oranda başvurulduğu görülmektedir¹⁵⁴.

CMK'nın 75 vd. maddelerinde bir suça ilişkin delil elde etmek amacıyla şüpheli veya sanığın ya da mağdurun beden muayenesi ve vücudundan örnek alınmasına ilişkin hükümler düzenlenmiştir¹⁵⁵. Bu hükümler uyarınca alınan örnekler üzerinde yapılan inceleme kişisel veri niteliğindedir¹⁵⁶. Bu nedenle kişisel verilerin korunmasında hâkim olan temel ilkelere tabi olmalıdır. Oldukça hassas nitelikte

http://www.egm.gov.tr/egitim/dergi/eskisayi/42/makale/Ziyaettin_KAYGUSUZ.htm#_ftn27 . Olay yeri incelemesine ilişkin olarak ayrıca bkz. Oğuz POLAT, **Klinik Adli Tıp, Adli Tıp Uygulamaları**, 2. Baskı, Seçkin, Ankara 2006, s. 375-404.

¹⁵⁴ Yusuf BÜYÜKAY, “Gen Analizleri ve Mukayeseli Hukuktaki Düzenlemeler”, **AÜEHFD**, C. 9, S. 3-4, Y. 2005, s. 358-362. (355-382)

¹⁵⁵ CMK'nın 75. maddesi şu hükmü içerir: “(1) 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. (2) İç beden muayenesi yapılabilmesi veya vücuttan kan veya benzeri biyolojik örnekler alınabilmesi için müdahalenin, kişinin sağlığına zarar verme tehlikesinin bulunmaması gerekir. (3) İç beden muayenesi veya vücuttan kan veya benzeri biyolojik örnekler alınması, ancak tabip veya sağlık mesleği mensubu diğer bir kişi tarafından yapılabilir. (4) Cinsel organlar veya anüs bölgesinde yapılan muayene de iç beden muayenesi sayılır. (5) Üst sınırı iki yıldan daha az hapis cezasını gerektiren suçlarda, kişi üzerinde iç beden muayenesi yapılamaz; kişiden kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınamaz. (6) Bu Madde gereğince alınacak hâkim veya mahkeme kararlarına itiraz edilebilir. (7) Özel kanunlardaki alkol muayenesine ve kan örneği alınmasına ilişkin hükümler saklıdır”. “Diğer Kişilerin Beden Muayenesi Ve Vücuttan Örnek Alınması” kenar başlıklı 76. madde hükmü ise şöyledir: “(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, yirmi dört saat içinde hâkim veya mahkemenin onayına sunulur. Hâkim veya mahkeme, yirmi dört 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. (4) Tanıklıktan çekinme sebepleri ile muayeneden veya vücuttan örnek alınmasından kaçınılabilir. Çocuk ve akıl hastasının çekinmesi konusunda kanunî temsilcisi karar verir. Çocuk veya akıl hastasının, tanıklığın hukukî anlam ve sonuçlarını algılayabilecek durumda olması hâlinde, görüşü de alınır. Kanunî temsilci de şüpheli veya sanık ise bu konuda hâkim tarafından karar verilir. Ancak, bu hâlde elde edilen deliller davanın ileri aşamalarında şüpheli veya sanık olmayan kanunî temsilcinin izni olmadıkça kullanılamaz. (5) Bu Madde gereğince verilen hâkim veya mahkeme kararlarına itiraz edilebilir”. 77. madde ise şu hükmü içerir: “(1) Kadının muayenesi, istemi halinde ve olanaklar elverdiğinde bir kadın hekim tarafından yapılır”.

¹⁵⁶ Bahri ÖZTÜRK, Mustafa Ruhan ERDEM, s. 623.

kişisel veriler içeren DNA analizi ise yeni CMK'nın 78. maddesi ile hukuk düzenimizde suçluların yakalanması açısından hukuksal temeline kavuşmuştur. CMK'nın 78. maddesi uyarınca bir suça ilişkin delil elde etmek amacıyla yukarıda belirtilen hükümler çerçevesinde elde edilen örnekler üzerinde “*soybağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için zorunlu olması halinde moleküler genetik incelemeler yapılabilir*”. DNA analizinin ceza muhakemesi hukukunda, bağımsız bir tedbir olarak düzenlenmediğini belirtmek gerekir. Bu yöntem, vücudun muayenesinin bir parçası, keşif veya olay yeri incelemenin bir uzantısı olarak değerlendirilebilir¹⁵⁷.

2005 yılında Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler Ve Fizik Kimliğin Tespiti Hakkında Yönetmelik yürürlüğe girmiştir¹⁵⁸. Belirtilen Yönetmelikte DNA analizinin CMK'ya paralel bir şekilde moleküler genetik inceleme olarak adlandırıldığı görülmektedir. Moleküler genetik inceleme ilgili Yönetmelikte, “(g)ereken tür ve miktardaki biyolojik materyali kullanarak, kişiyi diğer kişilerden ayıran ve kalıtım kurallarına uygun olarak aktarılan hastalık dışındaki özelliklerinin moleküler düzeyde araştırılması” şeklinde tanımlanmaktadır¹⁵⁹.

Yukarıda işaret edilen CMK'nın 75 vd. hükümleri uyarınca elde edilen bilgilerin tamamı kişisel veri niteliğinde¹⁶⁰ olmakla birlikte Yasada “*moleküler genetik inceleme*” olarak adlandırılan DNA verileri üzerinde özel olarak durmak gerekir. Nitekim AİHM de kişilerin hücre örnekleri ve DNA profilleri ile parmak izlerinin kayıt edilmesi arasında bir ayırım yapılması gerektiğine dikkat çekmektedir. Mahkeme'ye göre, kişinin hücre örnekleri sağlığına ilişkin veriler sunması nedeniyle oldukça hassas bilgiler içerir. Ayrıca bu örnekler kişinin benzersiz genetik kodunu

¹⁵⁷ Veli Özer ÖZBEK, “Ceza Muhakemesi Hukukunda DNA Analizi”,

¹⁵⁸ Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler Ve Fizik Kimliğin Tespiti Hakkında Yönetmelik, Adalet Bakanlığından: RG. T. 01 Haziran 2005, S. 25832. Yönetmeliğin amacı “*b)ir suça ilişkin iz, eser, emare ve delillerin elde edilmesi; ayrıca, maddi gerçeğin ortaya çıkartılması bakımından şüpheli, sanık, mağdur ve diğer kişilerin beden muayenelerinin yapılması, tıbbi incelemelerde bulunmak üzere vücuttan, kan veya benzeri biyolojik örneklerle, saç, tükürük, tırnak gibi örneklerin alınması, moleküler genetik incelemeler ile şüpheli ve sanığın kimliğinin tespiti için gerekli fiziki özelliklerin tespitine ilişkin usul ve esasları düzenlemek*”tir. Suçluların yakalanmasında moleküler genetik incelemenin şekli ve kullanımının tarihçesi için bkz. Hakan KIZILARSLAN, **Ceza Muhakemesi, Adli Tıp, Adli Bilimlerde Vücutun Muayenesi ve Örnek Alma**, Kızılarşlan Serisi I, Ankara 2007, s. 136-140.

¹⁵⁹ Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler Ve Fizik Kimliğin Tespiti Hakkında Yönetmelik, m. 3.

¹⁶⁰ CMK m. 80/1.

içerdiği için hem kendilerinin hem de yakınlarının kişiliği ile ilişkilidir. DNA profillerinin oluşturulması ise bireyler arasında belirlenebilir genetik ilişkileri ortaya koyması dolayısıyla özel yaşama ciddi bir müdahaledir. Bunun yanında DNA profilleri kişinin etnik kökenine ilişkin sonuçlar çıkarmayı olanaklı kılmaktadır¹⁶¹.

Dolayısıyla bu türdeki bilgilerin kaydı ve kullanımında azami dikkat gösterilmesi gerekir. Nitekim *“kimlik tespiti veya adli amaçlarla DNA örneklerinin alınması, analiz yapılması, verilerin saklanması, verilerden yararlanılması ile Türkiye Milli DNA Veri Bankasının kuruluş ve görevlerine ilişkin esas ve usullerini”* düzenlemek amacıyla DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı¹⁶² hazırlanmıştır. Belirtmek gerekir: *“tıbbi etik kuralları çerçevesinde bir hastalığın teşhis ve tedavisi ile bilimsel araştırma ve deney amacıyla yapılan DNA analizleri hakkında uygulanmaz”*¹⁶³. Eleştirilen kimi yönlerine karşın temel hak ve özgürlüklere ilişkin böylesine önemli bir konuda mevzuatımızdaki boşluğun doldurulması açısından böyle bir yasaya gereksinim duyulmaktadır. Bu türdeki uygulamaların her aşamasında uyulacak ilkeleri belirleyen Kişisel verilerin korunmasına yönelik kapsayıcı bir yasanın da mevzuatımızda bulunmadığı düşünüldüğünde bu eksiklik daha da açık bir şekilde görülebilir.

CMK’da konuya ilişkin güvenceler oldukça sınırlıdır. Buna göre, alınan örnekler üzerinde bu amaçlar dışında tespitler yapılmasına yönelik incelemeler yasaktır¹⁶⁴ ve moleküler genetik inceleme yapamaya yalnızca hâkim karar verebilir¹⁶⁵. Yasada 75-78. maddelerdeki düzenleme uyarınca alınan örnekler ile yapılan inceleme sonuçlarının başka bir amaçla kullanılamayacağı ve dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemeyeceği hüküm altına alınmıştır¹⁶⁶. Ayrıca bu bilgiler, *“kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı*

¹⁶¹ Mahkeme bu noktada AK Kişisel Verilerin Korunması Sözleşmesi’ne ve İngiltere’de geçerli olan Veri Koruma Yasası’na da atıf yapmıştır. Her iki metinde de hassas niteliği dolayısıyla kişilerin etnik kökenine ilişkin bilgiler özel veri kategorileri içerisinde sayılmıştır. Bkz. *S. ve Marper, Birleşik Krallık’a karşı*, par. 76.

¹⁶² Ülkü ÇINAR, “‘DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı’ Üzerine Bir Değerlendirme ve Öneriler”, **Terazi**, Y. 3, S. 21, Mayıs 2008, s. 147-156.

¹⁶³ DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı, m. 1/2

¹⁶⁴ CMK m. 78/1.

¹⁶⁵ CMK m. 79/1.

¹⁶⁶ CMK m. 80/1.

kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir”¹⁶⁷.

O halde bir suçtan dolayı şüpheli veya sanık durumunda olan ya da hakkında mahkûmiyet kararı verilen kişiye ilişkin kayıtların tutulması ile kovuşturma ya da soruşturmanın takipsizlik ile sonuçlanması ya da kişinin beraat kararının çıkmasının ardından bu kayıtların saklanmaya devam etmesi farklı iki durumdur. Nitekim AİHM de yakın zamanda verdiği bir kararında verilerin tutulma süresine bir sınırlama getirilmemesini ve aklanan kişinin bilgilerinin ulusal veri tabanından çıkarılmasını veya bu bilgilerin yok edilmesi için çok sınırlı bir olanak tanınmasını, diğer unsurlarla birlikte AİHS’nin 8. maddesine aykırı bulmuştur¹⁶⁸.

CMK’da fizik kimliğin tespiti ise 81. maddede düzenlenmiştir. Buna göre belirli bir ağırlıktaki suçtan dolayı şüpheli veya sanığın, kimliğinin tespiti için gerekli olduğu durumlarda Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konulur. Moleküler genetik incelemelere ilişkin yukarıda belirtilen kişinin suçla ilişkisinin kalmaması durumunda kayıtların yok edilmesine ilişkin ilke burada da kabul edilmiştir¹⁶⁹. Bu, oldukça önemlidir. Nitekim kişilerin genetik profilleri, parmak izleri ile karşılaştırıldığında daha hassas kişisel veriler olsa da¹⁷⁰ parmak izinin kişinin benzersiz bir niteliği olduğu unutulmamalıdır¹⁷¹. Bu

¹⁶⁷ CMK m. 80/2.

¹⁶⁸ *S. ve Marper, Birleşik Krallık’a karşı*, b.n. 30562/04, 30566/04, k.t. 4 Aralık 2008.

¹⁶⁹ CMK’nın 81. maddesi şu düzenlemeyi getirmektedir: (1) *Üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın, kimliğinin tespiti için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konulur.* (2) *Kovuşturmayla yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde söz konusu kayıtlar Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus tutanağa geçirilir”.*

¹⁷⁰ “Government Databases Have More Information than Needed to Solve Crimes”, haz. Electronic Privacy Information Center (EPIC), **DNA Databases**, Thomson & Gale, ABD 2007, s. 77-78.

¹⁷¹ AİHM de yukarıda söz edilen *S. ve Marper* kararında parmak izi kayıtları ile özel yaşamın gizliliği hakkı arasındaki ilişkiyi incelemiştir. Mahkeme, parmak izi kayıtlarının özel yaşama bir müdahale oluşturup oluşturmadığını değerlendirirken daha önce *Friedl* ile *P.G. ve J.H.* kararlarında fotoğraf ve ses örneklerine ilişkin yaptığı değerlendirmeyi izlemiştir. Bu bağlamda Mahkeme, parmak izinin bir kişi ile ilişkilendirilebilmesi için karşılaştırılacak bir parmak izi verisine ve bu işlemi gerçekleştirecek eğitilmiş bir kişiye gereksinim gösterdiğine işaret etmiştir. Bu açıdan fotoğraftan farklı bir nitelikte olduğu açıktır. Ancak bu, parmak izinin bir kişiye ilişkin benzersiz bir bilgi içerdiği gerçeğini değiştirmemektedir. Ayrıca pek çok durumda bu bilgi kişi

nedenle parmak izi kayıtlarının tutulması da özel yaşamın gizliliği hakkına müdahale oluşturacak, dolayısıyla temel hak ve özgürlüklerin sınırlandırılmasına yönelik ilkelere tabi olacaktır.

Adli kolluk etkinlikleri yanında 1990'lı yıllardan günümüze idari kolluk etkinlikleri de içerisinde kişisel verilerin toplanması, kayıt edilmesi ve kullanılmasına ilişkin uygulamaların hızla arttığı görülmektedir. Örneğin 2007 yılında Polis Vazife ve Salahiyet Kanununda (PVSK)¹⁷² yapılan bir değişiklikle parmak izi ve fotoğrafların kayda alınmasının uygulama alanı oldukça genişletilmiştir. PVSK'nın 2007 yılında değiştirilen 5. maddesi uyarınca polis tarafından, dört grup kişiden parmak izi kaydı ve ayrıca gönüllüler hariç diğerlerinden fotoğraflar kaydı alınacağı hükmü getirilmiştir. Buna göre belirtilen dört grup kişi şöyledir¹⁷³:

- (i) Bir suçtan dolayı şüpheli veya sanık durumunda olanlar;
- (ii) Devletten kimi taleplerde bulunanlar (silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda

ile ilişkilendirilebilmektedir. Bu nedenle Mahkeme, parmak izi kaydının kişinin özel yaşamını etkilediğine hükmetmiştir. Bkz. **A.g.k.** par. 84.

¹⁷² Polis Vazife ve Selahiyet Kanunu, Kanun no. 2559, t. 4 Temmuz 1934; RG. t. 14 Temmuz 1934; S. 2751.

¹⁷³ Madde hükmü şöyledir: “(1) Polis; a) Gönüllü, b) Her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan, c) Başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen, ç) Türk vatandaşlığına başvuruda bulunan, d) Sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı, e) Gözaltına alınan kişilerin parmak izini alır. (2) Birinci fıkraya göre alınan parmak izi, ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, bu amaca özgü sisteme kaydedilerek saklanır. Ancak, parmak izinin hangi sebeple alındığı sisteme kaydedilmez. (3) Olay yerinden elde edilen ve kime ait olduğu henüz tespit edilemeyen parmak izleri, kime ait olduğu tespit edilmeye kadar, ilgili soruşturma dosya numarası ile birlikte sisteme kaydedilir. (4) 5271 sayılı Ceza Muhakemesi Kanununun 81 inci maddesi ile 5275 sayılı Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanunun 21 inci maddesi hükümlerine göre alınan parmak izleri de bu sisteme kaydedilir. (5) bendi hariç birinci fıkra ile dördüncü fıkra kapsamına giren kişilerin ayrıca fotoğrafları alınarak, ikinci fıkra da belirlenen esaslara uygun olarak parmak izi ile birlikte sisteme kaydedilir. (6) Bu sistemde yer alan bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddi gerçeğin ortaya çıkarılması amacıyla mahkeme, hâkim, Cumhuriyet savcısı ve kolluk tarafından kullanılabilir. (7) Kolluk birimleri, kimlik tespiti yapmak ya da olay yerinden alınan parmak izini karşılaştırmak amacıyla doğrudan bu sistemle bağlantı kurabilir. (8) Sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi kurulur. (9) Sistemde yer alan kayıtlar gizlidir; altıncı ve yedinci fıkralarda belirlenen amaçlar dışında kullanılamaz. (10) Sisteme kayıtlı olan parmak izi ve fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinir. (11) Parmak izi ile fotoğrafların sistemde kaydedilmesi ve saklanması ile bu kayıtlardan yararlanmaya ilişkin diğer esas ve usûller, İçişleri Bakanlığı tarafından Adalet Bakanlığının görüşü alınarak çıkarılacak yönetmelikle düzenlenir”.

bulunanlar, Türk vatandaşlığına başvuranlar, sığınma talebinde bulunanlar ve ülkeye giriş yapan bazı yabancılar);

- (iii) Kimi görevlerde çalışanlar (başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilenler);
- (iv) Gönüllüler.

Yukarıda adli kolluk faaliyetlerine ilişkin açıklamalarımızda da işaret ettiğimiz gibi ceza kovuşturması sırasında suçlulukla mücadele ya da kamu düzeninin sağlanması gibi amaçlarla parmak izi alınabilir. Nitekim birinci gruba girenler bu kapsamda yer almaktadır. Ancak yine yukarıda işaret ettiğimiz gibi adli kolluk ile idari kolluk etkinlikleri ayrı ayrı değerlendirilmelidir. Nitekim kişisel verilerin korunması hakkı açısından yaratacakları sonuçlar farklı olacaktır.

PVSK’nda getirilen düzenleme ile aklanma ile verilerin silinmesi arasında bir bağlantı kurulmadığı gibi, sistemde yer alan bilgilerin her halde seksen yıl geçtikten sonra silineceği kuralı benimsenmiştir. O halde bu hükmün AİHS’ne açıkça aykırılık taşıdığı söylenebilir. Ancak sorun bu noktada da bitmemektedir. Nitekim kişisel verilerin ceza kovuşturması ve bir suçun failinin yakalanması gibi amaçlarla toplanması ve kullanılması, verilerin kullanımını ve tutulma süresine ilişkin makul ilkeler benimsenmesi koşuluyla, meşru görülebilir. Ancak PVSK’nın 5. maddesi ile hemen hemen herkesin parmak izinin alınması ve kayıt edilmesi öngörülmektedir. O halde buradaki amacın ceza kovuşturması veya belirli bir suç türüyle mücadele değil, genel bir önlem alınması olduğu söylenebilir. Nitekim gönüllü parmak izi kaydının düzenlenmesi de bunun bir göstergesidir. Burada “*getirilen sistem, ulaşılmak istenen amaçla (kamu düzeni), feda edilen yarar(özel hayatın gizliliği hakkı) arasındaki dengeyi hiçbir şekilde gözetmemiştir*”¹⁷⁴. Çalışmamızın üçüncü bölümünde de ayrıntılı olarak üzerinde durduğumuz gibi amaçla bağlılık kişisel verilerin korunmasında hâkim olan en önemli ilkelerden biridir. Buna göre kişisel veriler

¹⁷⁴ Kerem ALTIPARMAK, Ahmet Murat AYTAÇ, Onur KARAHANOGULLARI, Türkan HANÇER, Devrim AYDIN, “Polis Vazife ve Selahiyet Kanununda Değişiklik: Durdurma-Kimlik Sorma-Arama-Parmak İzi Alınması-Silah Kullanma”, **Hukuk ve Adalet**, S. 11, Y. 2007, <http://80.251.40.59/politics.ankara.edu.tr/karahan/makale/pvsk.htm>. Yazarlar ayrıca CMK uyarınca kovuşturmaya yer olmadığı, beraat veya ceza verilmesine yer olmadığı kararları kesinleştğinde parmak izi kayıtları yok edilirken pasaport başvurusunda bulunan kişinin parmak izinin seksen sene muhafaza edileceğine dikkat çekmektedirler.

yalnızca belirli amaçlar için ve gerektiği kadar toplanmalı, amacın gerektirdiği yerlerde kullanılmalı ve amaç için gerekli olandan uzun süre tutulmamalıdır.

Bu durum yeni teknolojilerin devreye girmesiyle daha da önemli hale gelmektedir. Nitekim bilgisayarlarda veri tabanlarında saklanan ve uzaktan erişime açılan bu bilgiler pek çok tehlikeyi de beraberinde getirmektedir. AİHM'ne göre de eğer adalet sistemi içerisinde modern bilimsel teknikler, herhangi bir maliyette ve bunların potansiyel yararı ile özel yaşamdan kaynaklanan önemli çıkarlar dengelenmeden kullanılırsa 8. maddenin sağladığı koruma önemli oranda zayıflamış olacaktır¹⁷⁵. O halde DNA veri bankalarının yararları ile yarattıkları riskler tartışılmalıdır. Böyle bir değerlendirme sonrasında bu veri bankalarının yararlarının ağır basması ancak genetik örneklerin mümkün olduğunca anonim tutulması, kural olarak gönüllülük esasına dayalı olarak alınması ve bu verilerin etkin bir şekilde korunması ile olanaklıdır¹⁷⁶.

VI. İDARE HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

A. GENEL OLARAK

Yönetimin etkinlikleri doğası gereği kişisel verilere gereksinim gösterir. Çalışmamızın birinci bölümünde de üzerinde durduğumuz gibi planlama, sosyal devletin yaşama geçirilmesi, güvenliğin sağlanması, suçluluğun önlenmesi ve suçluların yakalanması gibi görevleri dolayısıyla modern devlet, kişisel bilgileri, toplar, işler ve kullanır. Doğumdan ölüme kadar topladığı ve kayıt ettiği veriler dolayısıyla idare, en büyük bilgi gücüne sahiptir. Hatta bunun bazı alanlarda bir bilgi tekeline dönüştüğü de görülmektedir. Çalışmamızın bir önceki bölümünde adli kolluk faaliyetleri yanında idari kolluk faaliyetlerinde de kişisel verilerin korunmasına değinildiği için burada güvenlikle ilişkili konulara girilmeyecektir.

¹⁷⁵ S. ve Marper, *Birleşik Krallık'a karşı*, par. 112.

¹⁷⁶ Bu konuya ilişkin olarak ayrıca bkz. Christine ROSEN, "What Are the Benefits and Burdens of DNA Databases?", *DNA Databases*, Thomson & Gale, ABD 2007, s. 10-21.

Aşağıda yalnızca bazı kamu hizmetlerinin görülmesi ile ilişkili olarak kişisel verilerin korunması üzerinde durulacaktır¹⁷⁷.

Bu noktada çalışmamız içerisinde pek çok kez belirttiğimiz bir konunun tekrar altını çizmekte yarar vardır: idarenin kişisel verilere gereksinim duyması işin niteliği gereği kaçınılmazdır. Ancak modern dünyada verilerin toplanması, işlenmesi ve aktarılmasına, işlenmesine ilişkin ilkelerin belirlenmesi de önemli bir gerekliliktir¹⁷⁸. İdarenin bu bilgileri hukuka uygun şekilde elde etmesi, kullanması ve yalnızca zorunlu olduğu durumlarda aktarması gerekir. Bütün bu süreç boyunca amaca bağlılık ilkesi uyarınca ulaşılmak istenen hedef için gerekli olandan fazla veriyi toplamamalı, işlememeli, kullanmamalıdır. Bu idarenin kanuniliği ilkesinin ve keyfilikten uzak olması koşulunun da bir gereğidir. Nitekim günümüzün idari usul (yönetmelik yöntemi) anlayışı “*yönetimin mükemmel ve tam işleyişinin, etkisinin sağlanması*” yanında “*bireyin korunması*”nı da amaç ve değer olarak kapsamına almaktadır. Bu bağlamda bireyin haklarını dışlayan etkinlik yanıltıcı olacaktır. Kişi ile ilişkili olarak yapılan idari işlemlerde bireysel hakların korunması gerekir¹⁷⁹. Günümüzde devlet ile birey arasındaki ilişkide bireyin konumu o devletin yönetim sistemini belirleyen en önemli ölçütlerden biri olarak kabul edilmektedir. Bu noktada birbirini tamamlayan iki alan kişisel verilerin korunması ve aşağıda incelenecek bilgi edinme hakkı öne çıkan iki konuyu oluşturur.

Türkiye Cumhuriyeti’nde devlet, üzerine düşen görevleri yerine getirebilmek için kişisel verileri toplamakta, kullanmakta, işlemekte ve kimi zaman üçüncü kişilere aktarmaktadır. Özellikle son yıllarda bu işlemler yapılırken artan oranda bilişim sistemlerinden yararlanıldığı görülmektedir. Kamu hizmetinin gelişkin ağı içerisinde yönetimin kişisel verileri kullanırken bağlı olduğu mevzuatın tamamına yalnızca değinmek bile bu çalışmanın sınırlarını aşacak niteliktedir. Bu nedenle aşağıda yalnızca öne çıkan bazı alanlarda çeşitli konu ve sorunlar genel olarak değerlendirilecektir. Bu açıklamalar kapsamında görüleceği üzere kişisel verilerin

¹⁷⁷ Kamu hizmeti en genel şekliyle “(s)iyasal organlar tarafından kamuya yararlı kabul edilen, bir kamu kuruluşunun ya kendisi ya da yakın denetimi ve gözetimi altında özel kesim tarafından yürütülen faaliyetler” olarak tanımlanabilir. Metin GÜNDAY, s. 269.

¹⁷⁸ William WADE, Christopher FORSYTH, **Administrative Law**, 8. Baskı, Oxford University Press, Büyük Britanya 2000, s. 61.

¹⁷⁹ Tekin AKILLIOĞLU, “İdari Usul ve Kişisel Verilerin Korunması”, 11 Ağustos 2004, www.idare.gen.tr/akillioglu-idariusul.htm . Ayrıca bkz. T. Akıllıoğlu, “Bireyin Yönetmelik İşlemleri Karşısında Korunması ve Yönetim Hukukumuz”, **AİD**, Cilt 14 sayı 3 1981, s. 37-56.

korunmasında hakim olan temel ilkeleri belirleyen bir yasanın eksikliği diğer alanlarda olduğu gibi idare hukuku alanında da fazlasıyla hissedilmektedir.

B. ELEKTRONİK DEVLET (E-DEVLET)

1. Türkiye’de Genel Olarak E-Devlet Uygulamaları

1990’lı yıllardan günümüze hızla artan kullanım oranı ile İnternet, ekonomik, toplumsal ve kültürel etkileriyle önemli bir değişim yaratmaktadır. Ticaretten eğitime pek çok konuda sanal ortamda da etkinlik gösterilmektedir. Kamu hizmetlerinin sunulmasında da İnternet ve benzeri teknolojilerden artan oranda yararlanıldığı belirtilmelidir. Bu kapsamda ilk olarak elektronik devlet projesinden söz etmek gerekir¹⁸⁰. Elektronik devlet(ya da yaygın kullanımıyla e-devlet), yurttaşlara devlet tarafından verilen hizmetlerin elektronik ortamda sunulması demektir¹⁸¹. E-devlet, *“kamu yönetiminde her türlü faaliyetin, vatandaşlar, işletmeler, kamu çalışanları ve devletin diğer fonksiyonlarıyla ilgili etkileşimlerin elektronik ortam üzerine taşınması, birebir ve aracasız olarak kullanılabilir hale gelmesidir”*¹⁸². Bu ortamda kamu kuruluşları, özel sektör ve yurttaşlardan oluşan üç unsurun buluşturulmaktadır. Amaç devlet hizmetlerinin yurttaşa kolay ve etkin yoldan, kaliteli, hızlı, kesintisiz ve güvenli bir şekilde ulaştırılmasıdır. Bürokratik ve geleneksel devlet kavramının yerini almaya başlayan e-devlet anlayışı ile kurum ve kişilerin bilgi ve iletişim

¹⁸⁰ Elektronik devlet aslında daha büyük bir projenin e-dönüşümün bir parçası olarak kabul edilebilir. E-dönüşüm en genel şekliyle “(b)ilgi ve iletişim teknolojilerini etkin kullanarak, mevcut kültürün, iş modelinin, iş süreçlerinin, ürün ve hizmetlerin; çalışan, vatandaş, iş ortakları ve diğer tüm paydaşlarının yararına, bir bütünlük içinde değiştirilmesi” olarak tanımlanabilir. Bkz. Ali ARİFOĞLU, **E-Dönüşüm: Yol Haritası, Dünya**, Türkiye, Sas Bilişim, Ankara 2004. Bu doğrultuda e-devlet 2000 yılında aniden ülke gündemine yerleşen e-Avrupa + ve e- Türkiye projesinin bir parçası olarak değerlendirilebilir. E- Avrupa+ girişimine 2001 yılında katılan Türkiye, Eylem Planında belirtilen çalışmaların tamamlanmasını taahhüt etmiştir. Bu bağlamda hedefler ana hatlarıyla şöyledir: (0) Bilgi toplumunun temel yapı taşlarının oluşumunun hızlandırılması; (1) Daha ucuz, daha hızlı, daha güvenli İnternet; (2) İnsan kaynaklarına yatırım; (3) İnternet kullanımının canlandırılması. E-devlet, bir başka anlatımla kamu hizmetlerine elektronik erişim, e-ticaretin hızlandırılması, çevrim içi sağlık, akıllı ulaşım sistemleri gibi diğer alanlarla birlikte İnternet kullanımının canlandırılması başlığı altında değerlendirilmektedir. Bkz. Seçkin GÜLTAN, **Bilgi Toplumu Sürecinde Avrupa Birliği ve Türkiye**, AÜATAUM Araştırma Dizisi no. 19, Ankara 2003, s. 199-204. E-devlet uygulamalarına ilişkin genel bilgi için ayrıca bkz. **Elektronik Devlet Paneli**, haz. Murat ERDAL, İÜSBF, 15 Ekim 2003.

¹⁸¹ E-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı’nda ise e-devlet şu şekilde tanımlanmıştır (m. 2/h): *“Bilgi ve iletişim teknolojilerini kullanarak; devletin iş ve işlemlerinin kolaylaştırılmasını, kamu hizmetlerinin sunulmasını ve gerçek ve tüzel kişilerin kamu yönetimine etkin katılımının sağlanmasını”* ifade eder.

¹⁸² Murat ERDAL, **Elektronik Devlet, E-Türkiye ve Kurumsal Dönüşüm**, Filiz, İstanbul 2004, s. 1.

teknolojilerini kullanan sistemler ile kamu kurumlarına ve kurumlarca sunulan hizmetlere kolayca erişmesi hedeflenmektedir¹⁸³.

Günümüzde kamusal işlemlerin tamamen ya da kısmen elektronik ortamda gerçekleştirilmesi yönünde çalışmalar bütün dünyada yürütülmektedir. Türkiye’de ise özellikle 2000’li yıllarda e-devlet hizmetlerini oluşturma ve geliştirme konusunda önemli çalışmaların yürütüldüğü görülmektedir¹⁸⁴. E-devlet uygulamalarının oldukça geniş bir alana yayıldığı söylenebilir. Merkezi Nüfus İdaresi Sistemi (MERNİS), Kimlik Paylaşım Sistemi, Vergi Daireleri Otomasyonu Projesi (VEDOP I-II), Ulusal Yargı Ağı Projesi (UYAP), Gümrük İdaresinin Modernizasyonu Projesi (GİMOP), Polis Bilgi Ağı (POLNET), Saymanlık Otomasyon Sistemi (Say2000i), e-Bildirge ve Başbakanlık Mevzuat Bilgi Sistemi yaygın olarak hizmet veren başlıca e-devlet uygulamalarıdır¹⁸⁵. Bu örnekler yanında İnternet üzerinden alınabilen kamu hizmetlerinin her geçen gün çeşitlendiğini belirtmek gerekir¹⁸⁶.

¹⁸³ Bkz. Sıkça Sorulan Sorular: <https://www.turkiye.gov.tr> . Ayrıca bkz. **E-Devlet Yolunda Türkiye**, TBD, Ankara 2002, s. 12. Türkiye’de 2003 yılında başlayan e-devlet projesinin önemli ayaklarından biri olan e-devlet kapısı ise 18 Aralık 2008 günü açılmıştır. E-Devlet Kapısı, bütün kamu hizmetlerine tek bir noktadan erişim olanağı sağlayan bir İnternet sitesidir. Siteye <http://www.turkiye.gov.tr> veya <http://www.turkiye.gov.tr> adreslerinden ulaşmak olanaklıdır. Kapı’nın amacı kamu hizmetlerini, vatandaşlara, işletmelere, kamu kurumlarına bilgi ve iletişim teknolojileriyle etkin ve verimli bir şekilde sunmak ve bürokrasinin hantal kolları arasından sıkışmış bireyi biraz olsun rahatlatmaktır. Nitekim e-devlet kapısının açılışını yorumlayan Ulaştırma Bakanı Binali Yıldırım bu ideali "Bu git-gel kapısı değil. Bu vatandaşın ayağına geliyor. Bu kapı, vatandaşın elinin altında" sözleriyle dile getirmiştir. Bkz. <http://www.bilisim2023.org> . Ayrıca bkz. Mehmet TAŞNİKLİ, "e-Devlet ve Bilgi Toplumu Kanunu için Görüşler Toplanıyor", 9 Eylül 2009, <http://www.turk.internet.com/haber/yazigoster.php3?yaziid=24942> .

¹⁸⁴ Belirtilen nitelikteki uygulamaları geliştirmek üzere Devlet Planlama Teşkilatı bünyesinde Bilgi Toplumu Dairesi kurulmuştur. Dünya’da ve Türkiye’de e-devlet projelerinin ortaya çıkışı ve gelişimine ilişkin olarak bkz. Ali ARİFOĞLU, **e-Dönüşüm: Yol Haritası, Türkiye, Dünya**, Sas Bilişim Yayınları, Ankara 2004.

¹⁸⁵ E-dönüşüm ve e-devlet projelerine ilişkin bkz. DPT Müsteşarlığı Bilgi Toplumu Dairesi resmi İnternet sitesi: <http://www.bilgitoplumu.gov.tr> .

¹⁸⁶ 2009 yılında kamuoyunun görüşüne açılan "E-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı" bu kapsamdaki önemli çalışmalardan biridir. Taslakta Yasanın amacı "*Bu kanunun amacı e-devlet hizmetlerinin yürütülmesine ilişkin usul ve esasları belirlemek, bilgi toplumuna dönüşüm sürecini planlamak ve koordine etmek üzere kurulan Bilgi Toplumu Ajansının teşkilat yapısını, görevlerini ve yetkilerini düzenlemek*" olarak belirlenmiştir(m.1). Görüldüğü gibi yasalaşması durumunda bu düzenleme Bilgi Toplumu Ajansı’nın kurulmasını öngörmektedir. Ancak Taslağın bütünü değerlendirildiğinde bu Ajansın orantısız yetkilerle donatıldığı görülmektedir. Nitekim E-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağında bilgi Toplumu Ajansı’nın "*kuralı koyan, uygulayan ve denetleyen*" bir birim olarak düzenlediği, kişisel verilerin korunmasına yönelik yasal düzenleme olmaksızın böylesine geniş yetkilerle donatılmış bir Ajansın endişe uyandırıcı olacağı gibi gerekçelerle eleştirildiği görülmektedir. Bkz. TBD E-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı Hakkındaki Görüşleri, 16 Eylül 2009, <http://www.tbd.org.tr> . Taslağın "*Hizmet sunumunda kişisel verilerin korunması*" kenarbaşlıklı 26. maddesi uyarınca "*(1) Hizmet sunanlar verdikleri hizmetlerle ilgili olarak, sözleşme çerçevesinde kişilerden temin ettikleri ve*

Bu türdeki uygulamaların yaygınlaşmasının pek çok yararı olduğu açıktır. Her şeyden önce maliyet ve zaman tasarrufu sağlamaktadır. Bilgisayar ve İnternet kullanımındaki artışla doğru orantılı olarak bu sistemlerin kullanımının da artacağı makul bir beklentidir. Nitekim ülkemizde e-devlet uygulamalarında yazılı ve görsel basına da yansıyan bazı yanlış uygulamalar görülmüştür. Bu aksaklıkların özellikle kişisel verilerin korunması ile ilişkili alanlarda yoğunlaştığı söylenebilir.

E-devlet projeleri çerçevesinde kişisel verilerin çeşitli kurumlarca işlenmesi ve bu bilgilerin İnternet ortamında yer alması özellikle veri güvenliğine ilişkin bazı sorunların görülmesine neden olmuştur. Kişisel verilere yalnızca ilgili kişilerin erişimini sağlamak için kurum ve kuruluşlar bazı önlemler almaya çalışmaktadır. Ancak her kurumun kendi başına belirlediği önlemler hedefin, yani kişisel verilerin korunmasının, gerçekleştirilebilmesi için yeterli değildir. Nitekim bir İnternet sitesinde yer alan bilgi, diğerinde verilere erişimin anahtarı olabilir¹⁸⁷. Bu sakıncanın giderilmesi için bütün kurum ve kuruluşların uyacakları ortak standartların belirlenmesi gerekir.

2. Merkezi Nüfus İdaresi Sistemi (MERNİS)

Kamu kurumlarınca kişisel verilerin kayıt edilmesi ve işlenmesi konusunda önemli etkinliklerden biri Merkezi Nüfus İdaresi Sistemi (MERNİS) Projesidir. Bu proje, *“tüm Ahvali Şahsiye bilgilerini elektronik ortama aktaran ve Ahval-i Şahsiye bilgilerinde meydana gelen her tür değişikliğin ülkenin her tarafına dağılmış 957 merkezden anlık güncellenmesini ve bir ağ üzerinden güvenle paylaşımını”*¹⁸⁸ sağlamak üzere geliştirilmiştir. E-devlet çalışmalarının en önemli ayağı sayılabilecek MERNİS projesi ile kurulan sistem üzerinde kısaca durmak gerekir. Nitekim bu

hizmet sunumunda kullandıkları tüm kişisel verilerin korunmasından sorumludur. Hizmet sunanlar kendisinin bilgisine sunulan kişisel verileri, kişisel veri sahibi ile aksine özel bir anlaşması olmadıkça münhasıran e-devlet hizmetleri sunumu maksadıyla kullanabilir. (2) Sözleşmede hizmet sunulması şartı, kişinin kendi kişisel verilerinin üçüncü tarafa verilmesi hükmüne bağlanamaz”.

¹⁸⁷ KETİZMEN ve ÜLKÜDERNER çarpıcı bir çalışmada sorunun ciddiyetini ortaya koymuştur. Yazarlar e-devlet hizmeti sunan kurum ve kuruluşların İnternet sitelerine girerek hangi bilgilere ulaşabileceğini araştırmışlardır. Sonuçta çıkan tablo, bir siteden alınan bilginin adeta diğer sitenin anahtarı olduğu ve sonuçta kişilere ilişkin oldukça önemli bilgilere ulaşılabilmiştir. Bkz. Muammer KETİZMEN, Çağlar ÜLKÜDERLER, “E-Devlet Uygulamalarında Kişisel Verilerin Korunma(ma)sı”, **XII. Türkiye’de İnternet Konferansı**, Bilkent Üniversitesi Güzel Sanatlar Fakültesi, 8-10 Kasım 2007, Ankara, haz. Mustafa AKGÜL, Ufuk ÇAĞLAYAN, Ethem DERMAN, Atilla ÖZGİT, Ankara 2007, s. 189-193.

¹⁸⁸ http://www.nvi.gov.tr/Hakkimizda/Projeler,Mernis_Genel.html .

türdeki merkezi bir nüfus sisteminde önemli kişisel verilerin bulunduğu açıktır. Ayrıca çalışmamızın önceki bölümlerinden de hatırlanacağı gibi ilk kişisel veri koruma yasalarının kabulünde benzeri merkezi nüfus sistemlerinin yaratabileceği olası tehlikeden korunma düşüncesi etkili olmuştur.

1972 yılından beri süren bir çalışmanın ürünü olan Mernis, nihayet 2006 yılında yeni Nüfus Hizmetleri Kanununun kabulü ile kurulmuştur¹⁸⁹. Yasa uyarınca MERNİS, “*Merkezî veri tabanı ve Kimlik Paylaşımı Sistemini de kapsayan Merkezî Nüfus İdaresi Sistemini*” ifade eder¹⁹⁰. O halde merkezi veri tabanı ve kimlik paylaşım sisteminin Mernis’in iki önemli bileşeni olduğu söylenebilir. Yasaya göre merkezi veri tabanı, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünde elektronik ortamda tutulan aile kütüğü kayıtlarını; kimlik paylaşım sistemi ise “*Genel Müdürlükçe merkezî veri tabanından ayrı olarak elektronik ortamda tutulan, Kimlik Paylaşımı Sisteminden yararlanacak kurumların istifadesine sunulan ve sınırlandırılmış bilgiler ihtiva eden aile kütüğü kayıtlarını*” ifade eder¹⁹¹.

MERNİS ile ağır ve aksak işleyen bürokrasiye ilişkin bazı sorunların giderilmesi hedeflenmektedir. Kişilerin nüfus kayıtlarına ilişkin yanlışlıklar, bunların yarattığı çeşitli sorunlar ve yanlışlıkların giderilmesinde tekrar yaşanan aksaklıklar pek çoklarının yakındığı bir gerçektir¹⁹². Nitekim MERNİS’in temel hedefleri arasında doğru, hızlı ve verimli hizmet sunmak yer alır. Ayrıca MERNİS kapsamında her yurttaşa on bir haneli T.C. kimlik numarası verilmesi ile isim benzerliğinden dolayı ortaya çıkan aksaklıkları gidermek ve kamu kuruluşları arasındaki bilgi alışverişini hızlandırmak da hedeflenmektedir¹⁹³. Yasanın Geçici 1. maddesi

¹⁸⁹ Nüfus Hizmetleri Kanunu, kanun no.5490, t. 25 Nisan 2006; RG. t. 29 Nisan 2006, S. 26153. Yasanın uygulamasını göstermek üzere ise yine 2006 yılında çıkarılan yönetmelik için bkz. Nüfus Hizmetleri Kanununun Uygulanmasına İlişkin Yönetmelik, Bakanlar Kurulu Karar t. 29 Eylül 2006, S. 2006/11081, RG. t. 23/11/2006, S. 26355. Mernis projesinin tarihsel gelişimi için bkz. http://www.nvi.gov.tr/Hakkimizda/Projeler,Mernis_Dundenbugune.html.

¹⁹⁰ Nüfus Hizmetleri Kanunu, m. 3/n.

¹⁹¹ Nüfus Hizmetleri Kanunu, m.3/k,m.

¹⁹² M. Gökhan AHI, “Mernis’in Hukuki İncelemesi”, <http://www.hukukcu.com/bilimsel/kitaplar/mernis.htm>. Gerçi hemen belirtelim: Mernis uygulamaya geçtikten sonra da bu ve benzeri sorunların tam anlamıyla çözüldüğünü söylemek olanaklı değildir. Hatta sistemin uygulamaya geçmesinden kısa bir süre sonra, MERNİS’te yurttaşların T.C. kimlik bilgilerinin yüzde yirmi beşinin hatalı olduğu belirlenmiştir. Bkz. “Mernis Skandalı”, Milliyet, 11 Aralık 2006.

¹⁹³ T.C. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü’nün resmi İnternet sitesinde yer alan bilgiye göre MERNİS projesinin hedefleri şunlardır: “(i) Nüfus kütükleri üzerinde tam bir denetim kurmak ve nüfus kütüklerini güvenilir belgeler haline getirerek hizmette sürat ve verimlilik sağlamak; (ii) Merkezde bir bilgi bankası oluşturmak ve bu yoldan nüfus

uyarınca “(k)urumlar ve tüzel kişiler bu Kanunun yayımı tarihinden itibaren iki yıl içinde mevzuatlarını bu Kanun hükümlerine uygun hale getirerek işlemlerinde kimlik numarasını kullanmak zorundadırlar”.

MERNİS öncesinde de Türkiye’de çeşitli veri tabanlarında kişilere ilişkin bilgiler tutulmaktaydı. Bu projeyi önemli kılan ise birbirinden farklı veri tabanlarındaki bilgilere tek yerden ulaşma olanağı sağlamasıdır. Ancak kişisel verilerin korunmasına yönelik ilkeler belirlenmeden böyle bir sistemin uygulamaya geçmesi ciddi tehlikelerin ortaya çıkmasına neden olabilir. Federal Almanya Anayasa Mahkemesinin yukarıda da işaret edilen Nüfus Sayımı kararında da belirtildiği gibi, veriler arasında ilişki kurabilme olanağından dolayı, ilk başta önemsiz gibi görülen verilerden hareketle ayrıntılı kişilik profilleri çıkarılabilir. Bu ise kişiliğin serbestçe geliştirilmesi önünde önemli bir engel oluşturacaktır¹⁹⁴. Bu nedenle MERNİS projesi kapsamında birleştirilen veri tabanlarında yer alan bilgilerin, yetkili olmayan kişilerce ve toplanma amacından ayrı kullanımlarının bir hayli ciddi sonuçları olabileceği dikkatten kaçmamalıdır.

Öncelikle MERNİS projesi kapsamında kurulan sistem içerisinde oldukça hassas nitelikte olanlar da dahil önemli kişisel verilerin yer aldığı belirtilmelidir. Örneğin Kimlik Paylaşım Sisteminde üç grup bilgi yer almaktadır¹⁹⁵:

- (i) Kişi bilgileri (Kimlik numarası, adı, soyadı, kızlık soyadı, cinsiyeti, baba adı, anne adı, doğum yeri, doğum ve kütüğe kayıt tarihleri gibi kişisel bilgiler; medeni hali, dini ve ölüm tarihi gibi durum bilgileri; İl, ilçe, cilt, mahalle veya köy, aile sıra numarası ve birey sıra numarası gibi nüfusa kayıtlı olduğu yer bilgileri.
- (ii) Nüfus Cüzdanı Bilgileri (nüfus cüzdanı üzerinde yer alan bilgiler, 1 Haziran 2000 tarihinden sonra düzenlenen cüzdanlarda seri ve numarası ile verildiği yer ve tarihi, 1 Haziran 2000 tarihinden önce

kütüklerindeki bilgileri kamu hizmetleri açısından değerlendirmek; (iii) Nüfus kütüklerindeki bilgileri istatistik verileri olarak değerlendirerek, nüfus ve aile istatistiklerini elde etmek; (iv) Her vatandaşa bir Türkiye Cumhuriyeti kimlik numarası vermek suretiyle isim benzerliğinden dolayı ortaya çıkan aksaklıkları gidermek ve kamu kuruluşları arasındaki bilgi alışverişini hızlandırmak; (v) Mevcut nüfus cüzdanlarını dünya standartlarına uygun şekilde kart şeklinde nüfus cüzdanlarına dönüştürmek”.

¹⁹⁴ BVerfGE 65, 1.

¹⁹⁵ Kimlik Paylaşımı Sistemi Uygulama Yönetmeliği, (İçişleri Bakanlığından, RG. t. 10 Temmuz 2005; S. 25871) m. 8.

düzenlenmiş cüzdanlarda cüzdan seri, no ve verildiği maliye saymanlığının adı).

- (iii) Nüfus Olay Bilgileri; (evlenme, boşanma, soybağının düzeltilmesi veya reddi, ölüm, vatandaşlığın kazanılması veya kaybedilmesi gibi kişilere ait nüfus olay bilgilerinin tarihi ve açıklamaları).
- (iv) İstatistik Bilgileri (Doğum, ölüm, evlenme, boşanma sayıları gibi bilgiler).

Görüldüğü gibi bunlar, kişilerin özel yaşamlarına ilişkin oldukça önemli bilgilerdir. Ayrıca bu kapsamda kişisel durum sicilleri ile istatistik verilerinin birleştirildiği de dikkat çekmektedir¹⁹⁶. Bu kapsamda kişinin dinine ilişkin bilgiler üzerinde özel olarak durulmalıdır. Aile kütüklerinde ve nüfus cüzdanlarında kişinin dininin yazılması zorunluluğu 1587 sayılı Nüfus Kanununda da yer almaktaydı. Bu kural din özgürlüğünü zedelediği gerekçesi ile yoğun olarak eleştirilmiş ve iki kez da Anayasa Mahkemesinin önüne götürülmüştür. Ancak AYM, 1587 sayılı Nüfus Kanunun nüfus cüzdanlarında din hanesi bulunma zorunluluğuna ilişkin hükmünü din özgürlüğüne ve Anayasaya aykırı bulmamıştır. Anayasaya aykırılığı iddia edilen 1587 sayılı Nüfus Kanununun 43. maddesinde “... aile kütükleri ailenin bütün fertlerinin... dinini... ihtiva eder” denilmektedir¹⁹⁷.

Anayasa Mahkemesine göre “Nüfusa kaydolunurken kişinin, Anayasa’nın kastettiği anlamda dinî inanç ve kanaatlerini de değil, sadece dininin ne olduğunu açıklamasına yol açabilecek bir durum yaratmaktadır ki, bu kuralın zorlayıcı bir niteliği ve zorlama ile ilişkisi yoktur”¹⁹⁸. 1995 yılında verdiği kararda ise Mahkeme şöyle demektedir:

¹⁹⁶ İstatistik açısından kişisel verilerin korunmasına ilişkin açıklamalar izleyen alt başlık altında yapılacaktır. Kişisel durum sicilleri ise devletçe atanan memurlar tarafından tutulan, kişinin doğumu, ölümü, evlenmesi, boşanması, evlat edinilmesi gibi durumları ve durumlarda meydana gelen değişiklikleri gösteren sicillerdir. Nitekim MK’nın 36/1 hükmüne göre “Kişisel durum, bu amaçla tutulan resmi sicille belirlenir”. Kişisel durum sicilinin tutulmasından doğan zararlar ise kusurlu memura rücu edilmek şartıyla devletçe karşılanacaktır(MK m. 38). Bkz. Serap HELVACI, 150-156; İsviçre Medeni Kanunundaki mehzaz düzenleme ve yorumuna ilişkin olarak bkz. Hans Michael RIEMER, **Personenrecht des ZGB (Studienbuch und Bundesgerichtspraxis)**, Stämpfli, 2. Baskı, İsviçre 2002, s. 125-127.

¹⁹⁷ AYMK, 1979 ve 1995 yıllarında verdiği kararlarda bu hükmün anayasaya aykırılık iddiasını reddetmiştir. Bkz. AYMK, E. 1979/9, K.1979/44, t. 27 Kasım 1979; AYMK, E. 1995/17, K.1995/16, t. 21 Haziran 1995.

¹⁹⁸ AYMK, E. 1979/9, K.1979/44, t. 27 Kasım 1979.

“Anayasa’nın “Kimse ... dinî inancı ve kanaatlerini açıklamaya zorlanamaz” kuralından, kişilerin hangi dine bağlı olduğunun bir bilgi olarak resmî kayıtlara geçirilemeyeceği anlamı çıkarılamaz. ... Anayasa’nın 24. maddesinde yasaklanan, kişinin dininin öğrenilmesi değil, dinî inanç ve kanaatlerinin zorla açıklattırılmasıdır. Ayrıca kişi, dinî inançlarından ve kanaatlerinden dolayı kınanamayacak ve suçlanamayacaktır. Bu iki husus birbirini tamamlamaktadır. Nüfus Yasası’nın 43. maddesinin, Yasa’nın tümüyle birlikte incelendiğinde, Anayasa’nın 24. maddesinde ifadesini bulan dinî inanç ve kanaatlerin zorla açıklanmaması ve dinî inanç ve kanaatlerinden dolayı kişinin kınanmaması ve suçlanmaması ile hiçbir ilgisinin bulunmadığı açıklıkla anlaşılmaktadır. Burada dinî inanç ve kanaatler yönünden herhangi bir zorlama olmadığı gibi, bir kınama ve suçlama da söz konusu değildir”¹⁹⁹.

Buna karşın Anayasa Mahkemesi kısa süre sonra verdiği bir başka kararında, 1412 Sayılı Ceza Muhakemeleri Usulü Kanunun tanığa yemininden önce diğer bilgilerin yanında dininin de sorulmasına ilişkin ifadeyi Anayasaya aykırı bularak iptal etmiştir²⁰⁰. Mahkemenin gerekçesinde şu ifade yer almaktadır:

“İtiraz konusu kuralda olduğu gibi, dininin sorulması, kişinin isteği dışında bu inancını açıklaması sonucunu doğuracağından Anayasa’nın 24. maddesinin üçüncü fıkrasına açık bir aykırılık oluşturacaktır. Kişilere dinleri ile ilgili olarak sorulan soruların yanıtlanmamasının bir yaptırıma bağlanıp bağlanmaması da bu sonucu değiştirecek nitelikte değildir. Çünkü yasa buyruklarına uyma zorunluluğu hukuk devleti ilkesinin doğal bir sonucudur. Bu durumda, itiraz konusu kuralın, tanıklık yapan kişileri dinlerini açıklamaya zorlayarak, din ve vicdan özgürlüğünü zedelediği açıktır”.

Mahkemenin burada geliştirdiği yorum elbette yerindedir. Ancak bu noktada kişinin dinine ilişkin bilginin nüfus cüzdanlarında yer alması ile tanığa dininin sorulması arasında bu kadar keskin bir ayrım yapmayı anlamak güçtür²⁰¹. Nitekim

¹⁹⁹ AYMK, E. 1995/17, K.1995/16, t. 21 Haziran 1995

²⁰⁰ AYMK, E. 1995/25, K. 1996/5, t. 2 Şubat 1996.

²⁰¹ Nitekim karara katılmayan dört üyenin karşı oy yazısında da her iki karar konusu hüküm arasında benzerlik kurulduğu görülmektedir. Karşı oy yazısını kaleme alan Anayasa Mahkemesi üyelerine göre “Anılan Anayasa Mahkemesi kararlarında da açıklıkla belirtildiği gibi, “dinî inanç ve kanaat” kavramı, bir kişinin şu ya da bu dinden veya inançtan olmasını kapsayan dar bir kavram

Anayasanın kimsenin dini inanç ve kanaatlerini açıklamaya zorlanamayacağı hükmü karşısında, dinin ne olduğunu açıklamanın yasal zorunluluğa bağlanması din özgürlüğünü zedeleyecektir. Bunun yanında yukarıda da işaret ettiğimiz gibi kişinin dinsel inancı oldukça hassas nitelikte bir kişisel bilgidir. Uluslar arası metinlerde bu türdeki bilgilerin kayıt altında tutulmasının şartları özel olarak düzenlenmiştir. Kanımızca kişinin dini inancına ilişkin bilgiler, sağlık verileri, adli ve cezai veriler gibi diğer hassas kişisel verilerden de ayrılmaktadır. Nitekim kişinin dini inancına ilişkin bilginin kayıt altında tutulmasının makul bir yararı olmadığı gibi, bunların kötüye kullanımı ciddi zararlara yol açabilir. Bu noktada Avrupa Parlamentosunun da 1993 yılında verdiği bir kararla nüfus kaydı zorunluluğunu din özgürlüğüne ve Avrupa ölçütlerine aykırı bulduğunu belirtmek gerekir²⁰².

Şimdi ise sorun daha ciddi boyuttadır. Artık bu bilgiler MERNİS projesi kapsamında Kimlik Paylaşım Sisteminde de yer almaktadır. Bu, daha fazla sayıda kişinin daha kolay bir şekilde bu bilgilere ulaşabilmesi ve başka bilgilerle ilişkilendirebilmesi sonucunu getirir. Ülkemizde geçmişte özellikle fişleme konusundaki yanlış uygulamalar düşünüldüğünde sorunun ciddiyetinin arttığını kabul etmek gerekecektir. Nüfus cüzdanlarından din hanesinin çıkarılması 2000 yılında MERNİS projesinin ve daha sonra 2006 yılında yürürlüğe giren yeni Nüfus Hizmetleri Kanununun hazırlanma sürecinde gündeme gelmiş, ancak kabul edilmemiştir²⁰³. Günümüz temel hak ve özgürlükler anlayışında bu uygulama, kabul edilemez bir nitelik taşır. Kaldı ki kişisel verilerin korunmasına ilişkin standartların henüz belirlenmediği bir ortamda ortaya çıkabilecek tehlikenin de boyutu artmaktadır.

C. İSTATİSTİK

Günümüzde devletler, sosyal ve ekonomik hedeflerini belirlemek, bu hedeflere planlı bir şekilde ulaşmak için istatistik biliminden sıklıkla

olmayıp, din ve inanç yönünden pek çok hususu bünyesinde barındıran geniş bir kavramdır. Dava konusu kuralda yer alan “din” sözcüğü de, yargıcın bilgilenmesine yönelik genel anlamda ve hiçbir ayırım gözetilmeksizin tanıklık yapacak herkes için geçerli bir konuyu kapsamaktadır”.

²⁰² İbrahim Ö. KABOĞLU, **Özgürlükler Hukuku**, s. 365.

²⁰³ Selin ESEN, Levent GÖNENÇ, “Religious Information on Identity Cards: a Turkish Debate”, **Journal of Law and Religion**, C. 23, S. 2, Y. 2007 - 2008, s. 584 - 587. (579 - 603)

yararlanmaktadır²⁰⁴. Sosyal devlet ilkesi kabul edildiğinde ise istatistiğin sunduğu sonuçlar daha da önemli hale gelir. Bu çerçevede yararlanılan bilgileri konumuz açısından anonim veriler ve kişisel veriler olmak üzere ikiye ayırarak değerlendirmek gerekir.

Daha önce de açıklandığı gibi anonim veriler, ilgili olduğu kişinin kimliğini belirleme olanağı tanımadan tutulan bilgilerdir ve istatistik çalışmalarında sıklıkla kullanılır. Bu türdeki veriler konumuzun kapsamı dışındadır. Bununla birlikte istatistiksel çalışmalar içerisinde toplanan verilerin bir bölümü belirli bir kişiyle ilgili olabilir ya da ilgili kişinin belirlenmesini sağlayabilir. Bu gibi durumlarda konuyu kişisel verilerin korunmasının temel ilkeleri açısından değerlendirmek gerekecektir.

Türkiye’de istatistik çalışmaları 1926 yılında “Merkezi İstatistik Dairesi”nin kurulmasıyla başlamış, konuya ilişkin ilk yasal düzenleme 1939 yılında yapılmıştır²⁰⁵. Şu anda resmi istatistiklerin oluşturulmasının koşul ve kurallarını belirleyen temel düzenleme, 5429 sayılı Türkiye İstatistik Kanunudur²⁰⁶. Bu yasanın uygulamasını sağlamak üzere, Başbakanlığa bağlı Türkiye İstatistik Kurumu (TÜİK) kurulmuştur²⁰⁷. Yasaya göre “*bireysel veri*” hakkında veri toplanan gerçek ve tüzel kişiler ile kamu kurum ve kuruluşlarının özellikleriyle birlikte tanımlayan veri anlamına gelmektedir²⁰⁸. Bunun yanında yasada “*gizli veri*” olarak nitelendirilen bir başka veri türü de belirlenmiştir. Yasaya göre gizli veri “*(i)statistikî birimin doğrudan veya dolaylı bir şekilde sahip olduğu özellikleri ile birlikte tanınabilmesine ve bu şekilde bireysel bilgilerin açığa çıkarılmasına imkân sağlayan bireysel veya tablo hâlinde saklı tutulan veriyi*” ifade eder²⁰⁹. Yasa uyarınca herkese açık

²⁰⁴ TDK İstatistik Terimleri Sözlüğüne göre istatistik: “*Verileri derleme, bölümlendirme, çizelgeler ve çizgelerle özetleme, olasılık kuramı yardımıyla deney tasarımı ve gözlem ilkelerini saptama, örneklem bilgilerinin anlamlılığını inceleme, yorumlama ve genelleme yöntemlerini veren bilim*”dir. Bkz. <http://www.tdk.gov.tr>.

²⁰⁵ Bkz. “Türkiye İstatistik Kurumu Ve İstatistiğin Tarihçesi” <http://www.tuik.gov.tr/UstMenu.do?metod=tarihce>.

²⁰⁶ Kanun no. 5429; t. 10 Kasım 2005; RG. t. 18 Kasım 2005, S. 25997. Yasanın 1. maddesi uyarınca amacı: “*resmî istatistiklerin üretimine ve organizasyonuna ilişkin temel ilkeleri ve standartları belirlemek; ülkenin ihtiyaç duyduğu alanlarda veri ve bilgilerin derlenmesini, değerlendirilmesini, gerekli istatistiklerin üretilmesini, yayımlanmasını, dağıtımını ve Resmî İstatistik Programında istatistik sürecine dâhil kurum ve kuruluşlar arasında koordinasyonu sağlamak üzere, Türkiye İstatistik Kurumunun kuruluş, görev ve yetkilerine ilişkin esasları düzenlemektir*”.

²⁰⁷ Kurum etkinlikleri ile ilgili bilgi için bkz. <http://tuik.gov.tr>.

²⁰⁸ Türkiye İstatistik Kanunu, m. 2/h,o.

²⁰⁹ Türkiye İstatistik Kanunu, m. 2/s.

kaynaklardan elde edilen bilgiler gizli kabul edilmez²¹⁰. Buna karşın veri tablosundan ilgili kişinin kimliğinin ortaya çıkabileceği bazı durumlarda da verilerin gizli kabul edildiği söylenebilir²¹¹.

Aşağıda görüleceği gibi Yasada bireysel veriler ve gizli verilere ilişkin ilkeler ayrı ayrı belirlenmiştir. Ancak bunlar incelendiğinde her iki kavram arasında sınır çizmenin güç olduğu fark edilir. Temel hareket noktası kişisel verilerin korunması olduğunda aslında böylesine ikili bir ayrım içerisinde değerlendirmenin gerekli olmadığı görülecektir. Kanımızca Yasada benimsenen bu ayrım, kavram kargaşası oluşması gibi bir sorunu beraberinde getirmektedir.

Yasanın esasları “(r)esmî istatistiklerin gerçekleri yansıtmalarının sağlanması, tüm kullanıcılara tarafsız ve eş zamanlı olarak sunulması, gizlilik ilkesine riayet edilmesi, kamuoyunun bilgi edinme hakkının gözetilmesi” olarak belirlenmiştir²¹². Türkiye İstatistik Kanununun 7-15. maddelerinde ise bilgilerin toplanması, dağıtımı ve gizliliğine ilişkin kurallar düzenlenmiştir. Bunun yanında veri gizliliği ve güvenliğine ilişkin usul ve esasları belirlemek üzere 2006 yılında Resmi İstatistiklerde Veri ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik kabul edilmiştir²¹³.

Yasanın ve Yönetmeliğin ilgili hükümlerinde kişisel verilerin korunmasına ilişkin olarak özellikle amaca bağlılık, veri güvenliği, bilgilere erişim hakkı ve verilerin üçüncü kişilere aktarımına ilişkin usul ve esasların belirlendiği görülür. Bu noktada gizli ve bireysel veriler arasında da bir ayrıma gidilmiştir. Buna göre gizli verilere yalnızca resmi istatistik üretiminde görev alanlar ve yalnızca görevlerini yerine getirmek için gereksinim duydukları ölçüde erişebilir²¹⁴. Bu kişilere Yasada ve Yönetmelikte belirtilen gizlilik ilkelerine ilişkin eğitim verilmesi ve bu kişilerden

²¹⁰ Türkiye İstatistik Kanunu, m. 13/5.

²¹¹ Türkiye İstatistik Kanunu, m.13/2 şöyledir: “Bireysel verinin toplulaştırılması ile oluşturulan veri tablosunun herhangi bir hücreindeki istatistikî birim sayısının üçten az olması veya birim sayısı üç ve daha fazla olduğu hâlde bir veya iki istatistikî birimin hakim durumda olması hâlinde ilgili hücredeki veri gizli kabul edilir”.

²¹² Türkiye İstatistik Kanunu, m. 4/2.

²¹³ RG. t. 20 Haziran 2006, S. 26204.

²¹⁴ Türkiye İstatistik Kanunu, m. 13/1. Resmî İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul Ve Esaslar Hakkında Yönetmelik’in 8/2 hükmü uyarınca: “Kurumlar/kuruluşlar, sorumlulukları altındaki veri derleme, işleme ve saklama çalışmalarını kimlerin yürüteceğini belirleyerek bu görevlilerin hangi ayrıntıdaki veriye ulaşabileceklerini, hangi tarihlerde yetkili olduklarını açık olarak tanımlar ve istatistik üretim sürecinin her aşamasındaki görev değişikliklerinin düzenli olarak kaydını tutar”.

bir “gizlilik taahhüt belgesi” alınması da öngörülmüştür²¹⁵. Gizli verilere üçüncü kişilerin erişimi ise yasaklanmıştır²¹⁶. Bunun istisnası ise ilgili kişinin verilerinin açıklanmasına yazılı onay vermesidir²¹⁷. Burada dikkat çekici bir husus, Yasadaki bu sınırın Yönetmelik ile genişletilmiş olmasıdır. Nitekim Yönetmelikte herkese açık kaynaklardan elde edilen veriler yanında “iş kayıtları sistemi kapsamında bulunan istatistikî birimlerin bu nitelikteki unvan, faaliyet ve adres bilgileri” gizli verinin istisnaları arasında sayılmıştır²¹⁸. Bu düzenleme şekli temel hak ve özgürlüklerin ancak yasa ile sınırlandırılabilceği hükmüne aykırılık oluşturmaktadır.

Gizli verilerin diğer bilgilerle birleştirilerek yayımlanmasının koşulu ise doğrudan veya dolaylı tanımlamaya yol açmayacak bir biçime sokulması, bir başka anlatımla anonimleştirilmesidir²¹⁹. Aynı şekilde bireysel veriler de anonimleştirildikten sonra münferit birimlere atıfta bulunmayan bilimsel amaçlı araştırmalarda kullanılması kaydı ve Başkanlığın yazılı izniyle üçüncü kişilere verilebilir. Ancak bu hakkı elde edenler verileri başkalarıyla paylaşamazlar²²⁰. Ayrıca yasada kendilerinden veri talep edilenlerin bilgi edinme ve gizli verinin açıklanması durumunda maddi ve manevi tazminat hakları bulunduğu hatırlatılmıştır²²¹. Resmî İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul Ve Esaslar Hakkında Yönetmelik uyarınca, veri gizliliği ve güvenliği konularındaki gelişmeleri takip etmek, kurumsal stratejileri belirlemek ve resmî istatistik çalışmaları kapsamında hangi verinin gizli veri olduğu hususunda gerektiğinde görüş oluşturmak amacıyla Veri Gizliliği İhtisas Komisyonu oluşturulmuştur²²².

²¹⁵ Resmî İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul Ve Esaslar Hakkında Yönetmelik, m. 11.

²¹⁶ Türkiye İstatistik Kanununun 13. maddesinin 3 ve 4. fıkraları şöyledir: “(3) Resmî istatistiklerin üretilmesi için toplanan, işlenen ve saklanan verilerden gizli olanları, idarî, adlî ve askerî hiçbir organ, makam, merci veya kişiye verilemez, istatistik amacı dışında kullanılamaz ve ispat aracı olamaz. Bu bilgileri derleyen ve değerlendiren memurlar ve diğer görevliler de bu yasağa uymak zorundadır. Bu yükümlülük, görevlilerin görevlerinden ayrılmalarından sonra da devam eder. (4) Resmî istatistik üreten kurum ve kuruluşların yetkilileri tarafından, gizli verilerin hukuka aykırı erişimine, açıklanmasına veya kullanımına karşı her türlü önlem alınır”.

²¹⁷ Türkiye İstatistik Kanunu, m. 13/6.

²¹⁸ Resmî İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul Ve Esaslar Hakkında Yönetmelik, m. 5.

²¹⁹ Türkiye İstatistik Kanunu, m. 13/7.

²²⁰ Türkiye İstatistik Kanunu, m. 14.

²²¹ Türkiye İstatistik Kanunu, m. 15.

²²² Resmî İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul Ve Esaslar Hakkında Yönetmelik, m. 14-15.

Görüldüğü gibi Resmi İstatistik Kanunu ve yukarıda belirtilen Yönetmeliğin ilgili hükümleri çerçevesinde kişisel verilerin belirli oranda korunduğu görülmektedir. Ancak yasanın bazı hükümleri ile bu koruma önemli ölçüde zayıflatılmıştır. Bu konuda en ciddi yarayı açan iki hüküm yukarıda da belirtildiği gibi Anayasa Mahkemesinin önüne gitmiştir. Türkiye İstatistik Kanununun gerçek kişilerin ve diğer istatistiki birimlerin kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz, doğru ve ücretsiz olarak vermekle yükümlü olduklarına ilişkin 8. madde ile buna uymayanların para cezası ile cezalandırılacaklarına ilişkin 54/2,b hükmü Anayasa Mahkemesi tarafından Anayasaya aykırı bulunarak iptal edilmiştir²²³. Yukarıda da değindiğimiz gibi bu karar, kişisel verilerin korunmasının anayasal dayanaklarının Türk Anayasa Mahkemesi tarafından bu kadar açık bir şekilde ortaya koyması dolayısıyla özellikle önemlidir. Ayrıca bu karar sayesinde istatistik çalışmaları sırasında toplanan verilerin geleceği açısından önemli bir yanlışlık giderilmiştir.

Anayasa Mahkemesinin kararının ardından Yasa koyucu oluşan boşluğu gidermek amacıyla Türkiye İstatistik Kanununun 8. maddesini yeniden düzenlemiştir. Hükmün yeni şekli şöyledir: *“İstatistikî birimler, ülkenin ekonomi, sosyal, demografi, kültür, çevre, bilim, teknoloji ve ihtiyaç duyulan diğer alanlardaki resmi istatistikleri üretmek üzere, Anayasa’da belirlenen temel haklar ve ödevler çerçevesinde, kendilerinden istenen veri veya bilgileri, Başkanlığın belirleyeceği şekil, süre ve standartlarda eksiksiz ve doğru olarak ücretsiz vermekle yükümlüdür”*. Her ne kadar düzenlemenin yeni şeklinde kapsam öncekine göre sınırlandırılmış gibi gözükse de, aslında uygulamada ciddi bir değişiklik getirmediği söylenebilir. Nitekim hükümde sözü edilen alanlar sınırlayıcı olmadığı gibi, eğer öyle olsaydı da neredeyse her türlü veriyi kapsayabilecek genişlikte kavramlardır. Bu nedenle istatistiki birimlerden hemen hemen her konuda bilgi istemek olanaklıdır. Ancak hükümde temel hak ve ödevlerin hatırlatılması kişilerin kendilerinden istenen özel bilgileri vermemekte direnmesine yardımcı olabileceği gibi, artık bilgileri vermemenin yaptırımını da yasanın kapsamından çıkmış bulunmaktadır.

Türkiye İstatistik Kurumu Başkanlığı, geniş bir bilgilere erişim ağına sahiptir. Başkanlık, kurumun görev alanına giren konularla ilgili sayım ve araştırmalarda

²²³ AYMK, E. 2006/167, K. 2008/86, t. 20 Mart 2008.

doğrudan isteme yetkisine sahip olduğu gibi, idari kurum ve kuruluşlar kendi ellerindeki verileri ve görev alanlarına giren ulusal kayıt sistemlerini Türkiye İstatistik Kurumu Başkanlığının kullanımına açmak zorundadırlar²²⁴. Doğru, tam ve güncel istatistiki bilgilere de ancak bu şekilde ulaşılabileceği açıktır. Ancak geniş veri kaynakları, toplanan verilerin çeşitliliği ve işlemenin büyük oranda elektronik ortamda yapıldığı²²⁵ düşünüldüğünde güvencelerin önemi tekrar anlaşılabilir. Ülkemizde kişisel verilerin korunmasına ilişkin ilkelere uygun hareket edilip edilmediğini denetleyen bir kurumun bulunmaması ise ayrı bir sorundur. Nitekim TCK, MK gibi temel yasalar çerçevesinde veri öznesinin bazı hakları bulunduğunu yukarıda belirtmiştik. Ancak önleyici koruma sağlayacak sistemlerin eksikliği hissedilmektedir.

D. ADLİ SİCİL KAYDI VE GÜVENLİK SORUŞTIRMALARI

Adli sicil kaydı, güvenlik soruşturmaları ve ilgili diğer uygulamalar kişisel verilerin korunması açısından değerlendirmeyi gerektirir. Nitekim meşru kullanımları bulunmakla beraber bu gibi etkinliklerin kullanım alanlarının genişletilmesi hukuk devleti ilkesinden uzaklaşılarak polis devletine yaklaşıması sonucunu getirebilir.

1. Adli Sicil Kaydı

Siciller, kimi konular veya kişilere ilişkin olarak tutulan, bunlarla ilgili bilgiler içeren kayıtlardır. Bu kayıtlardaki bilgilere erişim, belge ve örnek alabilme hakkı, hukukumuzda ilgili sicile ilişkin düzenlemelerde ayrı ayrı belirtilmiştir²²⁶. Bu kapsamda burada yalnızca adli sicil kaydına ilişkin düzenleme üzerinde durulacaktır. Türkiye’de kişilerin geçmişlerindeki suçluluk durumuna ilişkin belgelerin tutulduğu

²²⁴ Türkiye İstatistik Kanunu, m. 7/1, 9, 10.

²²⁵ Yasanın 7/3 hükmünde verilerin elektronik ortamda işlenebileceğine ilişkin temel ilke şu şekilde belirlenmiştir: “Başkanlığın veri ve bilgi derleme ve yayımlama işlemleri dâhil her türlü faaliyetleri elektronik ortamda yapılabilir, arşivlenebilir ve elektronik imza kullanılabilir”. 7. maddenin 4. fıkrasında ise elektronik ortamda yer alan bilgilere ilişkin daha yüksek bir koruma öngörüldüğü görülmektedir. Buna göre “Elektronik ortamda tutulan bilgilere ilişkin belgeler, bu veri ve bilgilerin kesinleşip kullanıma açık hâle gelmesine kadar saklanır ve bu sürenin sonunda imha edilir”.

²²⁶ Murat SEZGİNER, “İdari Belgelere Ulaşma Hakkı-Fransa Örneği”, SÜHFD, Prof. Dr. Süleyman Arslan’a Armağan, C.6, S.1-2, 1998, s. 322. (s.299-343)

tek yetkili organ Adli Sicil'dir²²⁷. İyi hal kağıdı, temiz kağıdı, sabıka kaydı gibi adlarla da anılan adli sicil kaydı “*adli sicil bürosunda her hükümlü için ayrı ayrı tutulan ve kişinin geçmiş mahkûmiyetleri ve cezasının infazı ile ilgili bilgileri içeren kayıtlardır*”²²⁸.

Adli Sicil ve arşiv kayıtlarının tutulmasına ve kullanımına ilişkin ilkeler Adli Sicil Kanunu ve ilgili yönetmelikte belirlenmiştir²²⁹. Yasanın 1. maddesine göre amaç ve kapsamı “*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*” belirlemektir. Kişilerin adli sicilleri oldukça hassas nitelikte kişisel veriler içerir. Nitekim çalışmamızın ikinci bölümünde incelenen konuya ilişkin uluslar arası metinlerin önemli bir bölümünde özel nitelikteki kişisel veriler arasında sayılmış ve bunlar için daha nitelikli bir koruma öngörülmüştür.

Adli Sicil Kanunu ve ilgili yönetmelik incelendiğinde kişisel verilerin korunmasına yönelik bazı ilkelerin belirlendiği görülür. Yasada adli sicil ve arşiv bilgilerinin kimlere verilebileceği düzenlenmiştir. Buna göre adli sicil bilgileri; kullanılış amacı belirtilmek şartıyla, (i) ilgili kişiye veya vekaletinde açıkça belirtilmişse vekiline, (ii) kamu kurum ve kuruluşlarına, kamu kurum ve kuruluşu niteliğindeki meslek kuruluşlarına verilebilir²³⁰. Adli sicildeki bilgiler (i) cezanın veya güvenlik tedbirinin tamamlanması; (ii) ceza mahkûmiyetini bütün sonuçlarıyla ortadan kaldıran şikayetten vazgeçme veya etkin pişmanlık; (iii) ceza zamanaşımının dolması, (iv) Genel af halinde adli sicilden silinerek arşiv kaydına alınır²³¹.

²²⁷ Adli Sicil Kanununun 2. maddesi uyarınca “*Hakkında Türk mahkemeleri veya yabancı ülke mahkemeleri tarafından kesinleşmiş ve Türk Hukukuna göre tanınan mahkûmiyet kararı bulunan Türk vatandaşları ile Türkiye’de suç işlemiş olan yabancıların kayıtları da dahil tüm adli sicil bilgileri; mahallinde bilgisayar ortamına aktarılmasını takiben, Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğündeki Merkezî Adli Sicilde tutulur*”.

²²⁸ Onur KARAHANOĞULLARI, “Güvenlik Soruşturması”, **AÜSBFD**, C. 53, S. 1-4, Y. 1998, s. 159-185.

²²⁹ Adli Sicil Kanunu, Kanun No. 5352 t. 25 Mayıs 2005; R.G. t. 1 Haziran 2005, S. 25832; Adli Sicil Yönetmeliği, R.G. t. 7 Eylül 2005, S. 25929.

²³⁰ Adli Sicil Kanunu, m. 7.

²³¹ Adli Sicil Kanunu, m. 9/1. Hükmün 2. ve 3. fıkrası ise şu şekildedir: “(2) *Adli sicil bilgileri, ilgilinin ölümü üzerine tamamen silinir.*(3) *Türk vatandaşları hakkında yabancı mahkemelerce verilmiş olup 4 üncü Maddenin birinci fıkrasının (f) bendine göre adli sicile kaydedilen hürriyeti bağlayıcı cezaya mahkûmiyet hükümleri, kesinleştiği tarihten itibaren mahkûmiyet kararında*

Arşiv bilgilerini isteyebilecek kişi ve kurumlar açısından yasada daha ayrıntılı bir düzenleme getirildiği görülmektedir²³². Aynı koşullara bağlı olarak kişinin kendisi ya da vekili yanında arşiv bilgileri, bir soruşturma veya kovuşturma kapsamında Cumhuriyet başsavcılıkları, yargıç veya mahkemeler, yetkili seçim kurulları, özel yasalarda gösterilen hallerde ilgili kamu kurum ve kuruluşları tarafından istenebilir²³³. Bunun yanında arşiv bilgilerine ilişkin olarak yasada açıkça belirtilmediği durumlarda kişi hakkında alınacak bir karar veya yapılacak bir işlemle ilgili olarak, bir yakınının adlî sicil ve arşiv kayıtlarının istenemeyeceği ve bu bilgilerin kişiyi herhangi bir haktan yoksun bırakmak için dayanak olarak kullanılamayacağı ilkesi benimsenmiştir²³⁴. Bunun yanında onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları yalnızca soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, yargıç veya mahkemelerce istenebilir²³⁵.

Yasanın 11. maddesi ise “*Adli sicil ve arşiv bilgilerinin gizliliği*” kenar başlığı ile şu hükmü içermektedir: “*Adlî sicil ve arşiv bilgileri gizlidir. Bu bilgiler, görevlilerce açıklanamaz ve bu Kanun hükümlerine göre verilen kişi, kurum ve kuruluşlarca veriliş amacı dışında kullanılamaz*”. Yukarıda belirtilen ilkeler kişilerin adli sicil kayıtlarını koruyucu niteliktedir. Buna karşın adli sicil kaydının istenmesini öngören yasalarda da amaçla sıkı sıkıya bağlılık kurulmaması halinde korumanın sınırlı kalacağı belirtilmelidir. Aynı durum adli sicil ve arşiv kayıtlarında sorgulama yetkisi olanlar için de geçerlidir. Adli Sicil Kanunu uyarınca mahkeme, yargıç, askerî yargıç, Cumhuriyet Başsavcılığı ve askerî savcılık doğrudan doğruya; kolluk ve diğer kamu kurum ve kuruluşları Adalet Bakanının onayı ile bir suça ilişkin soruşturma ve kovuşturma kapsamında adlî sicil ve arşiv kayıtlarında sorgulama yapabilirler²³⁶.

belirtilen sürenin geçmesiyle, Adlî Sicil ve İstatistik Genel Müdürlüğünce adlî sicil kayıtlarından çıkartılarak arşiv kaydına alınır. Adlî para cezasına mahkûmiyet hükümleri ile cezanın ertelenmesine ilişkin hükümler, adlî sicil kaydına alınmadan doğrudan arşive kaydedilir”.

²³² Arşiv, “*belli bir yönetim dairesine ait işlemi bitmiş resmi evrakın, düzenli bir şekilde bir araya toplanması ve bu yazılı belgelerin saklanıp korunduğu yer anlamlarında kullanılmıştır*”. İsmet Binark, Arşiv ve Arşivcilik Bilgileri, Başbakanlık Basımevi, no. 3, Ankara 1980, s. 3’den aktaran; Cemil KAYA, s. 107. Genel olarak arşiv araştırmalarının kişisel verilerin korunması ile yakından ilişkisi bulunmasına karşın burada yalnızca adli siciller ile ilgili arşiv kayıtlarından söz edilmektedir.

²³³ Adli Sicil Kanunu, m. 10/1.

²³⁴ Adli Sicil Kanunu, m. 10/2.

²³⁵ Adli Sicil Kanunu m. 10/3.

²³⁶ Adli Sicil Kanunu m. 11.

Bir kişinin sabıka ve arşiv kaydının gizliliği, bu bağlamda bu bilgilere ulaşabileceklerin sınırlandırılması, kişilerin yaşamlarına devam edebilmeleri açısından oldukça önemlidir. Geçmişte yapılan bir hatanın yaşamın tamamına etki eder şekilde tekrar tekrar kişinin önüne gelmesi her defasında bir kez daha cezalandırılmasına neden olur. Bu ise cezalandırma sisteminin temel mantığı ile uyumsuz. Nitekim adli sicil kayıtlarının yasa ile belirlenen süreler sonunda silinmesi de kaynağını burada buluyor olmalıdır. Yeni bir sayfa açabilmek ve yaşamını sürdürebilmek için kişilerin buna gereksinim duyacakları açıktır.

2. Güvenlik Soruşturması

Ülkemizde pek çok soruna ve tartışmaya neden olmuş güvenlik soruşturmaları ve fişleme üzerinde de kısaca durmak gerekir²³⁷. Güvenlik soruşturması ve buna bağlı olan “fişleme” sabıka kaydı istenmesinden ayrı bir uygulamadır. Fişleme, “güvenlik ve istihbaratla görevli kuruluşların, kendiliğinden bilgi toplayıp depolamaları” iken, güvenlik soruşturması “bir kişi hakkında, bir kurum veya makamın talebi üzerine, güvenlik ya da haber alma kuruluşunca, belli bir amaçla kullanılmak üzere rapor düzenlenip ilgili makama iletilmesidir”²³⁸.

²³⁷ “Fişleme”nin uygulanmasının oldukça geçmişe dayandığı bilinmektedir. “Ülkemizde kamu görevlileri için bilinen en eski ve yasal fişleme, “gizli tezkiye varakaları”dır. Osmanlı Devleti’nden kalan bu yöntem, soyuttan somuta yönelen bir içerikle, Cumhuriyet döneminde de sürdürülmüştür. Demokrat Parti’nin ilk iktidar yıllarında çıkardığı “... ahlak ve yetersizlik sebeplerinden dolayı ...” olumsuz sicil alan memurların doğrudan emekli edilmelerine olanak veren Tüzük, getirdiği belirsiz ölçütler nedeniyle o günlerde çok eleştirilmişti”. Bkz. Güney DİNÇ, s. 112. Ancak fişlemeye ilişkin tartışmalar, bugün de oldukça hararetli bir şekilde sürmektedir. Çeşitli tarihlerde, birbirinden oldukça farklı düşünce akımlarını temsil eden gazetelerde yer alan haberler bunun en açık göstergesidir. Örneğin bkz. “Fişleme, Özel Kuvvetlerin Rutin Görevlerinden Biri İmiş”, Yeni Asya, 8 Ağustos 2008; “Öğrencilerden Fişleme Tepkisi”, <http://www.haberler.com>, 23 Aralık 2009; Son dönemde konuya yazılı sınavı kazandığı halde mülakatta sürekli olarak elenen hâkim adayı M.D.’nin “öğrenciliği sırasında örgütsel eylemlere katılmış olabilir” ifadesini içeren fiş kaydının bulunduğu ortaya çıkması konuya ilişkin tartışmaları bir kez daha gündeme taşımıştır. Bkz. 17 Ağustos 2009, Hürriyet Manşet Haber: “Meğer Devlet Fişleri Silmemiş”; “Ben Emniyetim, Fişlerim”, **Radikal**, 17 Ağustos 2009.

²³⁸ Onur KARAHANOGULLARI, “Güvenlik Soruşturması”. TANÖR belirtilen kavramlar arasındaki farklılığı ve sabıka kaydı istemine ilişkin Türkiye’de yakın tarihteki bazı uygulamaları şu şekilde özetlemektedir: “Güvenlik soruşturması ve buna bağlı olarak fişe ya da arşive başvurma, “sabıka kaydı istenmesi”nden de ayrı uygulamalardır. Gerçi, 12 Mart rejiminden sonra Sıkıyönetim komutanlarının emirleri, yasalara aykırı bir takım genelgeler ve bazı bürokratların kendilerini sağlama alma çabaları yüzünden “sabıka kaydı getirme” işlemleri yaygınlaşmış, gece ortaokulu ve lisesine kaydolmak isteyenlerden üniversite giriş sınavını kazananlara, resmi ve hatta özel kuruluşlara işçi olarak girmek isteyenlere ya da pasaport talebinde bulunanlara kadar genişlemiştir. Ama “sabıka kaydı”nın hammaddesi ve ölçüsü, mahkemelerce verilmiş hükümlülük kararının bulunup bulunmadığının araştırılmasından ibarettir. Bu inceleme, normalde adliye sicillerine bakılarak yapılır. Fişleme ve güvenlik

Güvenlik soruşturmasında kullanılan fişlerin hukuksal ve nesnel ölçütlere bağlı olması gerekir²³⁹. Ancak uygulamada bu ölçütlerden uzaklaşılabilirdiği görülmektedir. Ayrıca bu raporlar özelliği gereği gizli olarak hazırlanmakta ve kullanılmaktadır²⁴⁰. Bu ise diğer sorunların yanında fişlerde kişinin kendisi hakkında yanlış bilgiler bulunması halinde ciddi sorunlara yol açabilir. Nitekim “*gelişigüzel fişlemek ve ‘sakıncalı’ sayılmak son derece kolay, bunları değiştirebilmek ise hemen hemen imkânsızdır*”²⁴¹. Kayda geçirilirken yapılacak basit hatalar ciddi sonuçlara neden olabilir²⁴². Bu kayıtlara ulaşabilmek ve yanlışları düzeltmek ise oldukça zordur. Bu

soruşturması ise, bunları içeren ama aynı zamanda çok aşan, esas olarak adli kayıtları dışındaki alana yayılan işlemlerdir”. Bülent TANÖR, **Türkiye’nin İnsan Hakları Sorunu**, s. 32-33. Güvenlik soruşturması ve arşiv araştırması ilgili yönetmelikte tanımlanmıştır. Buna göre arşiv araştırması “*Kişinin kolluk kuvvetleri tarafından halen aranıp aranmadığının, kolluk kuvvetleri ve istihbarat ünitelerinde ilişkisi ile adli sicil kaydının ve hakkında herhangi bir tahdit olup olmadığının mevcut kayıtlardan saptanmasını*”, güvenlik soruşturması ise “*kişinin kolluk kuvvetleri tarafından halen aranıp aranmadığının, kolluk kuvvetleri ve istihbarat ünitelerinde ilişkisi ile adli sicil kaydının ve hakkında herhangi bir tahdit olup olmadığının, yıkıcı ve bölücü faaliyetlerde bulunup bulunmadığının, ahlaki durumunun, yabancılar ile ilgisinin ve sır saklama yeteneğinin mevcut kayıtlardan ve yerinden araştırılmak suretiyle saptanması ve değerlendirilmesini*” ifade eder. Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği,

Bakanlar Kurulu Karar t. 14 Şubat 2000, S. 2000/284; Dayandığı Kanun t. 26 Ekim 1994, S. 4045; RG. t. 12 Nisan 2000, S. 24018, m. 4/f,g.

²³⁹ Çeşitli örnekler devletlerin her zaman hukuksal ve nesnel ölçütlere başvurmayabileceğini ortaya koymaktadır. Bu, daha çok otoriter rejimlerde görülen bir uygulama olsa da demokratik sistemlerde de kimi zaman yurttaşların fişlenmesi yoluna gidildiği bilinmektedir. İngiltere’de bir dönem İşçi Partisinin ileri gelenlerinin fişlenmesi, ABD’de McCarthy’nin uygulamaları örnek olarak gösterilebilir. Bkz. Reg WHITAKER, s. 19-23. Ancak gözetim ve fişleme konusunda belki de en ileri gitmiş uygulamanın eski Doğu Almanya’nın güvenlik birimi STASI tarafından gerçekleştirildiğini belirtmek gerekir. Stasi 16 milyon nüfuslu Doğu Almanya’nın yurttaşlarının neredeyse üçte biri fişlenmiş, iki yüz kişiden biri muhbirlik yapmış ve kişilerin özel yaşamlarına acımasız şekilde müdahale etmiştir. Stasi’nin tuttuğu fişlerin akıbeti, Doğu Almanya’nın yıkılıp Federal Almanya ile birleşmesinden sonra önemli tartışmalara neden olmuş ve bu tartışmaların sonunda kişilerin kendilerine ilişkin fişlere ulaşmasını sağlayacak bir düzenleme yapılmasına karar verilmiştir. Bu konuya ilişkin olarak bkz. Hansjürgen GARTSKA, “Freedom of Information and Data Protection: The Data Collections of the Former East Germany State Security Service”, **Law, Justice and the State III: Problems in law**, haz. Arend SOETEMAN, Mikael M. KARLSSON, , Franz Steiner Verlag, Almanya 1995, s. 184-190. Günümüzde gelişen teknoloji ile artan gözetim etkinliklerinin özellikle Almanya’da Stasi’nin uygulamaları hatırlatılarak protesto edildiği görülmektedir. Örneğin Almanya’da konuya ilişkin yürütülen önemli bir kampanyanın sloganı, web 2.0 teknolojisine atıfla “Stasi 2.0”dır. Bkz. “Stasi 2.0: Widerstand mit Schäublone gegen den Bundesinnenminister”, jetzt.de, 26 Nisan 2007, <http://jetzt.sueddeutsche.de/texte/anzeigen/378419>. İngiltere’de artan oranda kullanılan gözetim teknolojilerinin de yine Stasi uygulamaları hatırlatılarak eleştirildiği görülmektedir. Bkz. Timothy Garton ASH, “Our state collects more data than the Stasi ever did. We need to fight back”, **The Guardian**, 31 Ocak 2008, <http://www.guardian.co.uk/commentisfree/2008/jan/31/immigrationpolicy.politics>.

²⁴⁰ Onur KARAHANOGULLARI, “Güvenlik Soruşturması”.

²⁴¹ Bülent TANÖR, **Türkiye’nin İnsan Hakları Sorunu**, s. 36.

²⁴² Çarpıcı örnekler için bkz. Muammer AKSOY, “Güvenlik Soruşturması Denilen Hukuksal Sapıklığın, MİT Raporlarındaki Korkunç Yanlış ve Yalanlar Işığında Değerlendirilmesi”, **Bahri Savcı’ya Armağan**, Mülkiyeliler Birliği Yayınları 7. (BAK)

nedenle demokratik bir hukuk devletinde bu türdeki sistemlere bazı istisnalar dışında başvurulmaması ve yurttaşların kendilerini ilgilendiren konularda bilgi edinebilmesi gerekir. Aşağıda incelenecek Bilgi Edinme Kanunu bu açıdan oldukça önemlidir.

Özellikle 1994 yılına kadar yasal dayanak olmaksızın yürütülen güvenlik soruşturmaları ciddi oranda eleştirilmiştir. Nitekim yönetmelik ile belirlenen güvenlik soruşturması uygulaması keyfiliğe açık belirsiz bir nitelik taşımaktaydı²⁴³. 1994 yılında kabul edilen ve halen yürürlükte olan 4045 sayılı yasa ile hakkında güvenlik soruşturması yapılabilecek kişiler belirlenmiştir. Buna göre güvenlik soruşturması ve arşiv araştırması; *“kamu kurum ve kuruluşlarında, yetkili olmayan kişilerin bilgi sahibi olmaları halinde devlet güvenliğinin, ulusal varlığın ve bütünlüğün, iç ve dış menfaatlerin zarar görebileceği veya tehlikeye düşebileceği bilgi ve belgelerin bulunduğu gizlilik dereceli birimler ile askeri, emniyet ve istihbarat teşkilatlarında çalıştırılacak kamu personeli ve ceza infaz kurumları ve tutukevlerinde çalışacak personel hakkında yapılır”*²⁴⁴.

Gizlilik dereceli birimler ve benzeri ifadelerin kapsamı, güvenlik soruşturmasının nasıl yürütüleceği gibi hususlar ise belirtilen yasanın 1. maddesine dayanılarak çıkartılan Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği ile düzenlenmiştir. 2000 yılında Bakanlar Kurulunca kabul edilen bu Yönetmelikte önceki uygulama ile karşılaştırıldığında haklarında güvenlik soruşturması yapılacak kişilerin kapsamının daraltıldığı görülür²⁴⁵. Buna karşın kişisel verilerin korunmasına ilişkin uyulması gereken yasal ölçütler belirlenmeden ve bunların uygulamasını denetleyecek bağımsız bir organ oluşturulmadan uygulama, insan hakları açısından çeşitli sorunlar yaratmaya devam edecektir²⁴⁶. Bunun yanında mevcut hukuksal düzenlemenin uygulanmasına ilişkin bazı sorunlar da dikkat çekmektedir. Nitekim

²⁴³ Tekin AKILLIOĞLU, “İdari Usul ve Kişisel Verilerin Korunması”.

²⁴⁴ Güvenlik Soruşturması, Bazı Nedenlerle Görevlerine Son Verilen Kamu Personeli İle Kamu Görevine Alınmayanların Haklarının Geri Verilmesine Ve 1402 Numaralı Sıkıyönetim Kanununda Değişiklik Yapılmasına İlişkin Kanun, (kanun no. 4045, t. 26 Ekim 1994; RG. t. 03/11/1994, S. 22100) m.1.

²⁴⁵ Kimler hakkında güvenlik soruşturması ve arşiv araştırması yapılacağı belirlenmiş olmasına karşın uygulamada *“tütün eksperleri, öğretmen, öğretim üyesi”* atamalarında bile güvenlik soruşturması yapıldığına işaret edilmektedir. Emin MEMİŞ, “Mevzuatımızda ve Uygulamada Kamu Hizmetlerine Girme, Çekilme Hakları, Arşiv Araştırması ve Güvenlik Soruşturması Analizleri”, Kamu Personeli Sempozyumunda sunulan bildiri, 4-5 Nisan 2003, Anadolu Üniversitesi Hukuk Fakültesi, Eskişehir 2003, s. 28’den aktaran Müslüm AKINCI, s. 43, d.n. 36.

²⁴⁶ AKILLIOĞLU, bu eksiklikler giderilmediği sürece Yönetmelik AİHS’ne ve Avrupa Sosyal Şartı’na aykırı olmaya devam edeceğini belirtmektedir. Tekin AKILLIOĞLU, “İdari Usul ve Kişisel Verilerin Korunması”.

kimi örnekler göstermektedir ki burada belirlenen ilkelere karşın fiş kayıtları kalıcılığını ve etkisini sürdürmektedir.

Güvenlik soruşturmasında yaygın uygulama, kamu hizmetine giriş ve atanmadadır. Güvenlikle ya da istihbaratla ilgili kamu hizmetlerinde ya da diplomasi gibi özel gizlilik gerektiren görevlerde çalışacak kişilerin özel bir inceleme ve değerlendirmeden geçirilmesi doğaldır²⁴⁷. Nitekim dünyadaki uygulama da bu yöndedir. Ancak bu türdeki uygulamanın alanının genişletilmesi çok önemli sakıncalara neden olabilir. Bütün kamu hizmetlerini ve hatta özel sektörü kapsayacak şekildeki, üstelik de gizlilik içerisinde yürütülen uygulamalar başta insanın maddi ve manevi varlığını geliştirme hakkı olmak üzere insan onurunun korunmasına yönelik temel haklara müdahaledir. Nitekim kendisine ilişkin yanlış ve yanıltıcı bilgileri düzeltemeyen kişi, haberi bile olmaksızın bu yanlışlığın mağduru olabilir. Ayrıca nesnel ölçütlere dayanmayan bir inceleme, Anayasanın 70. maddesinden kaynaklanan “*serbestlik*” ve “*eşitlik*” ilkelerine de aykırılık oluşturur. Nitekim Anayasanın 70. maddesinde her Türk vatandaşının kamu hizmetine girme hakkı olduğu belirtildikten sonra, hizmetin gerektirdiğinden başka hiçbir ayırım gözetilemeyeceği hüküm altına alınmıştır²⁴⁸.

Devletin kişiler hakkında yürüttüğü gizli araştırmaların geniş uygulama alanı bulması hukuk devletinden polis devletine doğru bir kaymaya neden olabilir. Nitekim yurttaşların nesnel ölçütler olmaksızın keyfi ve gizli kayıtlarla izlenmesi demokratik hukuk devleti ile bağdaşmaz. Bu türdeki uygulamalara özellikle otoriter rejimlerde sıklıkla başvurulduğu ve “*sakıncalı*” grupların hukukun genel ilkeleri ile bağdaşmayacak uygulamalara maruz bırakıldığı bilinmektedir. Kişisel verilerin korunması hakkının gelişmesinde de bu gibi tehditlere karşı bireyin korunması düşüncesinin etkili olduğu unutulmamalıdır. Çalışmamızın birinci bölümünde de incelendiği üzere bu hakkın Avrupa’da doğması bir tesadüf sonucu olmamıştır. II. Dünya Savaşı sırasında ve öncesinde başta Almanya olmak üzere pek çok Avrupa ülkesi yurttaşların bu şekilde fişlenmesinin yaratabileceği yıkıcı sonuçlara tanık

²⁴⁷ Bülent TANÖR, **Türkiye’nin İnsan Hakları Sorunu**, s. 33.

²⁴⁸ Yakın dönemde çeşitli basın organlarına yansıyan bir olay, hakimlik sınavlarına giren ancak mülakatları kaybeden M.D.nin Adalet Bakanlığına yaptığı başvuru üzerine “öğrenciliği sırasında örgütsel eylemlere katılmış olabilir” diye fişlendiğini öğrenmesine ilişkindir. Oysa yukarıda değinilen 2000 yılında çıkarılan Yönetmelik uyarınca bu türdeki fişlerin silinmesi gerekmektedir. Bkz. “Meğer Devlet Fişleri Silmemiş”, **Hürriyet**, 18 Ağustos 2009.

olmuştur. İlgili kanunlarda sabıka kaydı istemi, güvenlik soruşturması ve fişleme gibi uygulamaların sınırlandırılması gerekliliği yanında, Türkiye’de kişilerin bilgilerini koruyan bir sistemin kurulması önemli bir gerekliliktir.

E. SAĞLIK HİZMETİ

Bir zamanlar hasta kayıtları hekimlerin odalarındaki dosyalarda, aldıkları kişisel notlarda ve hastanenin tozlu arşiv raflarında yer alıyordu. Diğer sağlık personelinin ve hasta yakınlarının bu bilgilere ulaşması ise gerekli olduğu durumlarda hekimin uygun görmesi ile olanaklıydı. Gelişen teknoloji ile bu durum büyük oranda değişti. Günümüzde kişilerin sağlık durumlarına ilişkin bilgiler artan oranda elektronik ortama aktarılmaktadır. Pek çok sağlık kuruluşunda hastaların randevuları, sağlık geçmişlerine ilişkin bilgiler, tahlil sonuçları, kendilerine konulan tanılar, tedavileri ve bunların süresi dijital ortamda yer almaktadır. Artık kişilerin sağlık bilgileri doktorların kişisel notlarından bilgisayar ortamına, hastanenin arşiv katından siber uzayın sanal koridorlarına taşınmıştır. Çalışmamızın çeşitli yerlerinde daha önce de belirtildiği üzere bu durumun bazı yararları olduğu gibi, önemli sakıncaları da bulunur.

Hastaların geçmişteki tanı ve tedavilerine hekimlerin ulaşabilmesi yeni tanıların doğru bir şekilde konulmasını, müdahalenin daha çabuk ve daha az riskli gerçekleştirilmesini sağlayabilir. Sağlık alanında yapılan araştırmalarda da hasta bilgilerinin ulaşılabilir olmasının önemli yararlar sağlayacağı kuşkusuzdur. Ancak diğer taraftan bir kişinin sağlık durumuna ilişkin bilgiler kişiseldir ve yanlış kullanımı ilgili kişiye ciddi zararlar verebilir. Nitekim daha önce de belirtildiği üzere hassas niteliğinden dolayı bu türdeki veriler için konuya ilişkin hukuksal metinlerde çoğu zaman daha yüksek düzeyde bir koruma öngörülmüştür. İnsanların bu konudaki bilgilerin gizli tutulmasını istemelerinin makul nedenleri bulunur. Yeni dönemde tehlikenin boyutunun artması öncelikle bu bilgilere ulaşabilecek kişi sayısındaki artış ile ilişkilidir.

Bu bilgiler dolayısıyla kişilerin tehlide maruz kalabilecekleri, eşleri tarafından terk edilebilecekleri, işlerinden kovulabilecekleri düşünüldüğünde bunların başkalarının eline geçmesinin yarattığı tehlikenin boyutu kolaylıkla fark

edilebilir²⁴⁹. Pek çok kişi, sağlık bilgilerinin kolaylıkla aktarılması sonucunda sosyal ayrımcılığa uğrama, sigorta hizmetine erişimde sorun yaşama gibi korkular içerisinde. Böylesine bir korku içerisinde olan kişinin, karşılaştığı tehlike yalnızca özel yaşamının gizliliğinin ihlal edilmesi ile ilişkili değildir. Kişinin sağlık hizmeti almaktan kaçınması durumunda beden bütünlüğüne ve yaşamına yönelik bir tehlike de söz konusu olacaktır. AİHM'in daha önce belirtilen Z. Finlandiya'ya karşı kararında da ifade edildiği üzere özellikle salgın hastalıklar söz konusu olduğunda böylesine bir durum, toplum sağlığını da tehdit eder bir niteliğe bürünebilir. Bunlar ancak hukuksal güvencelerin etkili bir şekilde sağlanması ile giderilebilir.

Türkiye'de sağlık bilgilerinin saklanmasına ve gizliliğine ilişkin çeşitli düzeylerde pek çok önemli düzenleme yürürlüktedir. Sağlık Hizmetleri Temel Kanunu'nun 3/f hükmü uyarınca *"Herkesin sağlık durumunu takip edebilmek için gerekli kayıt ve bildirim sistemi kurulur"*²⁵⁰. Bu hüküm, konumuz açısından oldukça önemli bazı uygulamalara hukuksal dayanak oluşturmaktadır. Sağlık Bakanlığı'nın Sağlık.Net uygulaması ve elektronik sağlık kaydı sistemleri bu kapsamdadır²⁵¹. Bununla birlikte Sağlık Hizmetleri Temel Kanunu'nda hekimlerin ve diğer sağlık personelinin sorumluluğuna ilişkin bir hüküm yer almamaktadır. Bu konuya ilişkin düzenlemeleri daha çok ilgili yönetmeliklerde ve etik kuralların düzenlendiği belgelerde bulmak olanaklıdır.

Sağlık bilgilerinin gizliliği konusunda hekimlerin sorumluluğu çeşitli düzenlemelerde hüküm altına alınmıştır²⁵². Burada öncelikle yukarıda incelenen Türkiye Cumhuriyeti Anayasasında belirlenen temel ilkelerin hiçbir zaman dikkatten kaçmaması gerekir. Bunun yanında Türk Medeni Kanunu, Türk Ceza Kanunu gibi yasalarda yer alan genel hükümlerin bu alanda da geçerli olduğu unutulmamalıdır. Nitekim hekimlerin ve diğer sağlık personelinin sır saklama yükümlülüğünü ihlal etmesi ceza kanunları çerçevesinde suç olarak düzenlendiği gibi, tazminat

²⁴⁹ Bruce SCHNEIER, *Secrets & Lies (Digital Security in a Networked World)*, Wiley, ABD 2004, s.66.

²⁵⁰ Sağlık Hizmetleri Temel Kanunu, K.n.: 3359; R.G. t: 15 Mayıs 1987; S. 19461.

²⁵¹ İlginç olan bu hükmün sağlık verilerinin korunmasına ilişkin bazı düzenlemelere de kaynak olmasıdır. Örneğin aşağıda değinilecek Hasta Hakları Yönetmeliği, 3359 Sayılı Sağlık Hizmetleri Temel Kanunu'nun 9. maddesinin (c) bendine ve 181 sayılı Sağlık Bakanlığı'nın Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 43. maddesine dayanılarak hazırlanmıştır. Bkz. Hasta Hakları Yönetmeliği., m. 3.

²⁵² Konuya ilişkin genel bir değerlendirme için bkz. **Türk Hukukunda Hekimin Hukuki ve Cezai Sorumluluğu**, Mukayeseli Hukuk Araştırma ve Uygulama Merkezi, Sorumluluk Hukukunda Yeni Gelişmeler V. Sempozyumu, Ankara 12-13 Mart 1982, Fakülteler Matbaası, İstanbul 1983.

sorumluluğunu da getirmektedir²⁵³. Doğrudan sağlık hizmetine ilişkin düzenlemeler getiren yasa, tüzük ve yönetmeliklerde ise daha çok arşiv, kayıt ve bilgi sistemlerinin kurulmasına ilişkin düzenlemelerin yer aldığı görülmektedir. Bunlar içerisinde kişilerin sağlık verilerinin gizli tutulmasına ilişkin hükümlere oldukça sınırlı bir şekilde yer verildiği görülmektedir²⁵⁴.

Sağlık verilerinin gizliliğine ilişkin hukuksal düzenlemeler incelenirken Türkiye'nin onaylayıp taraf olduğu kimi uluslar arası sözleşmeler de dikkate alınmalıdır. Yukarıda da işaret edildiği üzere Anayasanın 90. maddesi uyarınca temel hak ve özgürlüklere ilişkin uluslararası andlaşmalar yasa hükmünde olduğu ve bunlarla yasaların çatışması durumunda andlaşma hükümlerine öncelik verileceği

²⁵³ Örneğin Yargıtay bir kararında “İstanbul Üniversitesi Tıp Fakültesi Çapa Psikiyatri Bölümü’nde tedavi gördüğü sırada, tedavi amacıyla sorulan sorulara verilen cevapların yayınlanması dolayısıyla idari yargıda tazminat davası açılabilmesine karar vermiştir”, Yargıtay 4. HD, 28. 03.1977. Ayrıca bkz. TCK m. 136, 280; CMK m. 46/1-b, Çocuk Koruma Kanunu, m.6. Bkz. Hakan HAKERİ, **Tıp Hukuku**, Seçkin, Ankara 2007, s. 473-474.

²⁵⁴ Örneğin sağlık hizmetlerinin düzenlenmesi açısından önemli yasalardan biri olan Tababet ve Şuabatı Sanatlarının Tarzı İcrasına Dair Kanun’da (Kanun no. 1219, t. 11 Nisan 1928; R.G. t. 14 Nisan 1928, S. 863) hasta bilgilerinin gizliliğine ilişkin herhangi bir hüküm yer almamakta, yalnızca 70. maddede hekimin yapacağı tıbbi müdahaleye ilişkin olarak hastanın rızasını alması gerektiği düzenlenmektedir. Aile Hekimliği Pilot Uygulaması Hakkında Kanun’da (Kanun no. 5258, t. 24 Kasım 2004; R.G. t. 9 Aralık 2004, S. 25665) ise Sağlık Bakanlığının pilot olarak belirleyeceği illerde “*kişisel sağlık kayıtlarının tutulması*” yasanın amaçları içerisinde yer almaktadır (m.1). Buna karşılık kayıtların gizliliğine ilişkin hükümlere sınırlı bir şekilde yer verilmiştir. Yasanın 5/3 hükmü uyarınca “Aile hekimlerinin şahsi kayıtları ilgili il ve ilçe sağlık idare birimlerinde tutulur. Aile hekimlerinin kullandığı basılı veya elektronik ortamda tutulan kayıtlar, kişilerin sağlık dosyaları ile raporlar, sevk belgesi ve reçete gibi belgeler resmi kayıt ve evrak niteliğindedir. Bu kayıt ve belgeler, hekimin ayrılması veya kişinin hekim değiştirmesi halinde eksiksiz olarak devredilir”. Aile Hekimliği Pilot Uygulaması Hakkında Yönetmelikte ise (t. 6 Temmuz 2005, R. G. S. 25867) kayıtların güvenliği ve mahremiyetinden aile hekiminin sorumlu olacağı (m. 28/1), aile hekiminin denetimlerde kendisine kayıtlı kişilerin dosyalarını, hasta haklarına riayet etmek suretiyle göstermek zorunda olduğu (m.28/2) ve kişinin kendisine ilişkin kayıtların bir örneğini talep edebileceği (m.28/3) düzenlenmiştir. Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun (Kanun no. 5510, t. 31 Mayıs 2006, R.G. t. 16 Haziran 2006, S. 26200) 100/1 hükmü ise şu düzenlemeyi getirmektedir: “5411 sayılı Bankacılık Kanunu kapsamındaki kuruluşlar, döner sermayeli kuruluşlar ile diğer gerçek ve tüzel kişiler doğrudan, münferit olarak bilgi ve belge istemesi hariç olmak üzere kamu idareleri ile kanunla kurulan kurum ve kuruluşlar ise Kurumla yapılacak protokoller çerçevesinde, Devletin güvenliği ve temel dış yararlarına karşı ağır sonuçlar doğuracak haller ile özel hayat ve aile hayatının gizliliği ve savunma hakkına ilişkin hükümler saklı kalmak kaydıyla özel kanunlardaki yasaklayıcı ve sınırlayıcı hükümler dikkate alınmaksızın gizli dahi olsa Kurum tarafından kişilerin sosyal güvenliğinin sağlanması, 6183 sayılı Kanuna göre Kurum alacaklarının takip ve tahsili ile bu Kanun kapsamında verilen diğer görevler ile sınırlı olmak üzere istenecek her türlü bilgi ve belgeyi sürekli ve/veya belli aralıklarla vermeye, bilgilerin elektronik ortamda görüntülenmesini sağlamaya, görüntülenen bu bilgilerin güvenliğini sağlamaya, muhafaza etmek zorunda oldukları her türlü belge ile vermek zorunda oldukları bilgilere ilişkin mikrofiş, mikrofilm, manyetik teyp, disket ve benzeri ortamlardaki kayıtlarını ve bu kayıtlara erişim veya kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifreleri incelemek için ibraz etmeye mecburdurlar”. İlgili mevzuata ilişkin olarak ayrıca bkz. Leyla KESER BERBER, Mahir M. ÜLGÜ, Cüneyd ER, **Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği**, İstanbul 2009, s. 257-334.

için bu hükümler oldukça önemlidir. Burada öncelikle AİHS gibi temel insan hakları metinleri akla gelmektedir. Ancak bunun yanında doğrudan sağlık verileri ile ilişkili konularda da Türkiye'nin taraf olduğu çeşitli metinler bulunmaktadır. İnsan Hakları ve Biyotıp Sözleşmesi²⁵⁵ burada örnek olarak gösterilebilir. Sözleşmede ilgili kişinin özel yaşamın gizliliği hakkına atıf yapılmış olmakla birlikte²⁵⁶ çalışmamızın ikinci bölümünde belirtildiği üzere koruma sınırlı çerçevesi dolayısıyla eleştirilmektedir.

Türkiye'de sağlık verilerinin gizliliğine ilişkin temel kaynak Hasta Hakları Yönetmeliği'dir²⁵⁷. Hasta hakları, Yönetmelikte de belirtildiği üzere *“temel insan haklarının sağlık sahasındaki yansıması”*dır²⁵⁸. Bu kapsamda diğer haklar yanında kişilerin sağlık verilerinin korunması üzerinde de durulmuştur. Nitekim yasa ile izin verilen durumlar ve tıbbi zorunluluk dışında hastanın özel ve aile yaşamının gizliliğine dokunulamayacağı hasta haklarına ilişkin ilkeler kapsamında yer alır²⁵⁹.

Yönetmeliğin ilgili hükümleri ile kişisel verilerin korunmasının temel ilkelerine büyük oranda karşılanmaktadır. Hastanın kişisel verilerine erişim hakkı bulunmaktadır. Buna göre, *“Hasta, sağlık durumu ile ilgili bilgiler bulunan dosyayı ve kayıtları, doğrudan veya vekili veya kanuni temsilcisi vasıtası ile inceleyebilir ve bir suretini alabilir”*²⁶⁰. Hastanın mahremiyetine saygı gösterilmesi esastır²⁶¹. Bu

²⁵⁵ Biyoloji ve tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, Kanun no. 5013, R.G. t. 11 Aralık 2003; S. 25311.

²⁵⁶ Sözleşmenin 1. maddesi uyarınca *“Bu Sözleşmenin Tarafları, tüm insanların haysiyetini ve kimliğini koruyacak ve biyoloji ve tıbbın uygulanmasında, ayırım yapmadan herkesin, bütünlüğüne ve diğer hak ve özgürlüklerine saygı gösterilmesini güvence altına alacaklardır”*. Sözleşmenin *“özel yaşam ve bilgilendirme hakkı”* kenar başlıklı 10. maddesi ise şu hükmü içerir: *“(1) Herkes, kendi sağlığıyla ilgili bilgiler bakımından, özel yaşamına saygı gösterilmesini isteme hakkına sahiptir. (2) Herkes, kendi sağlığı hakkında toplanmış herhangi bir bilgiyi öğrenme hakkına sahiptir. Bununla beraber, bireylerin, bilgilendirilmeme istekleri de gözetilecektir. (3) İstisnai durumlarda, 2nci paragrafta belirtilen hakların kullanılmasında hastanın yararları bakımından kanun tarafından kısıtlamalar öngörülebilir”*.

²⁵⁷ Hasta Hakları Yönetmeliği, R.G. t. 1 Ağustos 1998; S. 23420.

²⁵⁸ Yönetmeliğin 1. maddesinde amaç şu şekilde belirlenmiştir: *“Bu Yönetmelik; temel insan haklarının sağlık sahasındaki yansıması olan ve başta Türkiye Cumhuriyeti Anayasası'nda, diğer mevzuatta ve milletler arası hukuki metinlerde kabul edilen “hasta hakları”nı somut olarak göstermek ve sağlık hizmeti verilen bütün kurum ve kuruluşlarda ve sağlık kurum ve kuruluşları dışında sağlık hizmeti verilen hallerde, insan haysiyetine yakışır şekilde herkesin “hasta hakları”ndan faydalanabilmesine, hak ihlallerinden korunabilmesine ve gerektiğinde hukuki korunma yollarını fiilen kullanabilmesine dair usul ve esasları düzenlemek amacı ile hazırlanmıştır”*.

²⁵⁹ Hasta Hakları Yönetmeliği, m. 5/f.

²⁶⁰ Hasta Hakları Yönetmeliği, m. 16.

²⁶¹ Hasta Hakları Yönetmeliği'nin 21. maddesi bu esası şu şekilde belirlemektedir: *“(1) Hastanın, mahremiyetine saygı gösterilmesi esastır. Hasta mahremiyetinin korunmasını açıkça talep de edebilir. Her türlü tıbbi müdahale, hastanın mahremiyetine saygı gösterilmek suretiyle icra*

kayıtlar yalnızca hastanın tedavisi ile doğrudan ilgili olanlarca görülebilir²⁶². “İlgili mevzuat hükümlerine ve hastalığın mahiyetine göre, yetkili mercilerce alınacak tedbirlerin gerektirdiği haller dışında; hasta, sağlık durumu hakkında kendisine veya ailesine veya yakınlarına bilgi verilmemesini isteyebilir”²⁶³. Ayrıca hastaya ilişkin olarak sağlık hizmetinin verilmesiyle edinilen bilgiler hiçbir şekilde açıklanamaz. Bunun tek istisnası yasa ile müsaade edilen hallerdir²⁶⁴.

Sağlık bilgilerin açıklanması, hukuksal boyutu yanında, bir tıp etiği sorunudur ve Hipokrat yemininde de yer alır²⁶⁵. Nitekim hekimlerin mesleklerinin uygulanması sırasında edindikleri bilgileri gizli tutacakları kuralı, Tıbbi Deontoloji Nizamnamesi’nde²⁶⁶ ve Türk Tabipler Birliği Hekimlik Meslek Etiği Kuralları²⁶⁷ kapsamındadır²⁶⁸.

edilir. Mahremiyete saygı gösterilmesi ve bunu istemek hakkı; a) Hastanın, sağlık durumu ile ilgili tıbbi değerlendirmelerin gizlilik içerisinde yürütülmesini, b) Muayenenin, teşhisin, tedavinin ve hasta ile doğrudan teması gerektiren diğer işlemlerin makul bir gizlilik ortamında gerçekleştirilmesini, c) Tıbben sakınca olmayan hallerde yanında bir yakınının bulunmasına izin verilmesini, d) Tedavisi ile doğrudan ilgili olmayan kimselerin, tıbbi müdahale sırasında bulunmamasını, e) Hastalığın mahiyeti gerektirmedikçe hastanın şahsi ve ailevi hayatına müdahale edilmemesini, f) Sağlık harcamalarının kaynağının gizli tutulmasını, kapsar. (2) Ölüm olayı, mahremiyetin bozulması hakkını vermez. (3) Eğitim verilen sağlık kurum ve kuruluşlarında, hastanın tedavisi ile doğrudan ilgili olmayanların tıbbi müdahale sırasında bulunması gerekli ise; önceden veya tedavi sırasında bunun için hastanın ayrıca rızası alınır”.

²⁶² Hasta Hakları Yönetmeliği, m. 16.

²⁶³ Hasta Hakları Yönetmeliği, m. 20.

²⁶⁴ Hasta Hakları Yönetmeliği m. 23/1. Belirtilen hükmün izleyen fıkraları ise şu şekildedir: “(2) Kişinin rızasına dayansa bile, kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlandırılması neticesini doğuran hallerde bilginin açıklanması, bunları açıklayanın hukuki sorumluluğunu kaldırmaz. (3) Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektirir. (4) Araştırma ve eğitim amacıyla yapılan faaliyetlerde de hastanın kimlik bilgileri, rızası olmaksızın açıklanamaz”.

²⁶⁵ Sultan ÜZELTÜRK, s.112.

²⁶⁶ Tıbbi Deontoloji Nizamnamesi, Bakanlar Kurulu Kararı t. 13 Ocak 1960; S. 4112578; R.G. t. 19 Şubat 1960, S. 10436.

²⁶⁷ Türk Tabipler Birliği Hekimlik Meslek Etiği Kuralları, TTB 47. Büyük Kongresi’nde (10-11 Ekim 1998) kabul edilmiştir.

²⁶⁸ Tıbbi Deontoloji Nizamnamesi’nin 4. maddesi uyarınca: “(1) Tabip ve dış tabibi, meslek ve sanatının icrası vesilesiyle muttali olduğu sırları, kanuni mecburiyet olmadıkça, ifşa edemez. (2) Tıbbi toplantılarda takdim edilen veya yayınlarda bahis konusu olan vakalarda, hastanın hüviyeti açıklanamaz”. Türk Tabipler Birliği Hekimlik Meslek Etiği Kuralları’nın 9. maddesi ise şu şekildedir: “(1) Hekim hastasından mesleğini uygularken öğrendiği sırları açıklayamaz. Hastanın ölmesi ya da o hekimle ilişkisinin sona ermesi bu yükümlülüğünü ortadan kaldırmaz. (2) Hastanın onam vermesi ya da sırrın saklanması hasta ya da öteki insanların yaşamını tehlikeye sokması durumunda, hastanın kişilik haklarının zedelenmemesi koşuluyla, hekim bu sırrı saklamakla yükümlü değildir. (3) Yasal zorunluluk durumlarından hekimin rapor düzenlemesi de meslek sırrının açıklanması anlamına gelmez. (4) Hekim, tanık ya da bilirkişi olarak mahkemeye çağrıldığında olayın meslek sırrı olduğunu ileri sürerek bu görevden çekilebilir”. Konuya ilişkin pek çok uluslararası metinde de benzer kurallar benimsenmiştir. Örneğin bkz. 1981 yılında Dünya Tabipler Birliği’nce yayınlanan Lizbon Bildirgesi m.4; 1995

Hasta-hekim ilişkisinin özel niteliği ve hekimin sır saklama yükümlülüğünün Hipokrat Yemini'ne kadar uzanan geleneği mevzuatta konuya ilişkin çeşitli düzenlemelerin yapılmasını sağlamıştır. Bu bakımdan kişisel verilerin korunmasına ilişkin Türkiye'de en geniş kapsamlı düzenlemelerin sağlık hizmetlerine ilişkin olarak yapıldığı söylenebilir. Ancak her düzenlemede konunun tekrar belirtilmesi gerekliliği ve hasta haklarına ilişkin kuralların bir yönetmelik ile belirlenmiş olması kişisel verilerin korunması yasasının gerekliliğini bir kez daha ortaya koymaktadır. Genel nitelikli böylesine bir yasa kabul edildikten sonra da sağlık verilerine ilişkin özel düzenlemelere gereksinim duyulacaktır. Ancak kişisel verilerin etkin bir şekilde korunmasını sağlayacak sistemi kuran ve temel ilkeleri belirleyen bir yasa hassas ve önemli olan bu konuda oluşabilecek boşlukların giderilmesi için gereklidir.

Hekimler işlerinin gereği bilişim teknolojileri konusunda uzman olmak zorunda değillerdir. Bu nedenle belirtilen teknolojiler kullanıldığında oluşabilecek zararlar hakkında bilgilendirilmeleri de oldukça önemlidir. Bu şekilde konunun uzmanlarından teknik yardım alabilecekleri gibi, veri güvenliği konusunda basit ama oldukça etkili önlemleri kendileri de alabilirler.

F. VERGİ MAHREMİYETİ

Çalışmanın birinci bölümünde de belirtildiği üzere modern devlet üzerine düşen görevleri yerine getirebilmek için yurttaşlarının çeşitli bilgilerine gereksinim duyar. Bu durumun açıkça görüldüğü alanlardan biri de vergilendirme ve mali araştırmalardır. Vergilendirmeyi ilgilendiren konularda yönetim, özellikle iki nedenle kişisel bilgilere gereksinim duyar: (i) vergi verecek kişilerin yani yükümlülerin (mükellefin) saptanabilmesi; (ii) mevcut yükümlülerin doğru bir şekilde vergilendirilmesi. Her iki amacın da gerçekleştirilebilmesi için pek çok ülkede vergi idaresine yükümlülerden ve onlarla bağlantılı kişilerden, kamu kurum ve kuruluşlarından, uluslararası anlaşmalar çerçevesinde yabancı ülkelerin ilgili birimlerinden bilgi alınmasını ve araştırma yapılmasını sağlayıcı düzenlemeler benimsenmiştir²⁶⁹. Bu gibi etkinlikler dolayısıyla devlet organlarının bilgileri

yılında Dünya Tabipler Birliği'nce yayınlanan Bali Bildirgesi m.7, 8, 10; 28-30 Mart 1994 Avrupa Hasta Haklarının Geliştirilmesi Bildirgesi(Amsterdam Bildirgesi).

²⁶⁹ Selda AYDIN, "Mükellefin Gizlilik Alanına (Sır Çevresine) İlişkin Hakları", **Vergi Sorunları**, S. 213, Haziran 2006, s. 26. (25-37)

toplama, kullanma, üçüncü kişilere aktarma gibi konularda uyacakları esasların belirlenmesi oldukça önemlidir.

Türkiye’de konuya ilişkin düzenlemeler incelenirken ilk olarak vergi mahremiyeti üzerinde durulmalıdır. Vergi Usul Kanunun (VUK)²⁷⁰ 5. maddesinde düzenlenen vergi mahremiyeti, anayasal koruma altındaki özel yaşamın gizliliği hakkının yasal düzeydeki yansımalarından biridir²⁷¹. Kişilerin vergi bilgilerinin açıklanmayacağına güven duymaları özel yaşam alanlarına koruyabilmeleri açısından önemli olduğu gibi, doğru beyanda bulunmalarını sağlaması açısından vergilendirmenin sağlıklı bir şekilde yapılması için de bir gerekliliktir. Nitekim vergi mahremiyetine ilişkin düzenleme yapılmasının temel nedenlerinden biri de budur²⁷². VUK’un 5. maddesi uyarınca vergi idaresine, yükümlülerin kişisel, mali ve ticari sırlarını açıklama yasağı getirilmektedir²⁷³. Ancak 5. maddenin ikinci fıkrası ile

²⁷⁰ Kanun no. 213, t. 4 Ocak 1961; R.G. t. 10 Ocak 1961, S. 10703-10705.

²⁷¹ Billur YALTI, **Vergi Yükümlüsünün Hakları**, Beta, İstanbul 2006, s. 175.

²⁷² SONSUZOĞLU’na göre; “*Vergi mahremiyeti kurumu, beyan esasına dayanan Türk Vergi Sisteminde, mükelleflerin vercekleri vergi bilgilerinin açıklanmayacağına güven duymaları ve bu sayede doğru beyanda bulunmalarını sağlamak için getirilmiş bir düzenlemedir. ... Her ne kadar vergi idaresi mükellefleri denetlese de beyan esaslı mükelleflerin verdikleri bilgilerin gizli tutulacağına inançları sayesinde, onları doğru beyanda bulunmaya özendirecek ve bu sayede beyan sistemi etkinlik kazanacaktır. ... Vergi mahremiyeti kurumu, kamusal olanı bireysel olana üstün tutam vergi hukukunda, devlet karşısında bireyin Anayasal haklarını koruyan bir kurum olarak düzenlenmiştir. Bu düzenleme aynı zamanda vergiye karşı tepkiyi azaltıcı nitelik de taşımaktadır*”. Elif SONSUZOĞLU, “Çeşitli Yasalar Açısından Vergi Mahremiyetine İlişkin Düzenlemelerin Değerlendirilmesi”, **Vergi Sorunları**, Haziran 2000, S. 141, s. 116. (116-134)

²⁷³ VUK’un pek çok kez değişikliğe uğrayan ve kimi hükümleri ilga edilen 5. maddesi şu düzenlemeyi içermektedir: “(1)*Aşağıda yazılı kimseler görevleri dolayısıyla, mükellefin ve mükellefle ilgili kimselerin şahıslarına, muamele ve hesap durumlarına, işlerine, işletmelerine, servetlerine veya mesleklerine mütaallik olmak üzere öğrendikleri sırları veya gizli kalması lazımgelen diğer hususları ifşa edemezler ve kendilerinin veya üçüncü şahısların nefine kullanamazlar; 1. Vergi muameleleri ve incelemeleri ile uğraşan memurlar; 2. Vergi mahkemeleri, bölge idare mahkemeleri ve Danıştayda görevli olanlar; 3. Vergi kanunlarına göre kurulan komisyonlara iştirak edenler; 4. Vergi işlerinde kullanılan bilirkişiler. (2)Bu yasa, yukarıda yazılı kimseler, bu görevlerinden ayrılırlar dahi devam eder. (3) Ancak, vergi güvenliğini sağlamak amacıyla Gelir Vergisi mükelleflerinin yıllık Gelir Vergisi, sermaye şirketlerinin Kurumlar Vergisi beyannamelerinde gösterdikleri matrahları (zarar dahil) ve beyanları üzerinden tarh olunan Gelir ve Kurumlar Vergileri ile mükelleflerin ad ve unvanları, bağlı oldukları vergi dairelerince beyannamelerin verildiği yıl içinde dairenin münasip yerlerine asılacak cetvellerle ilan olunur. Mükellefin bağlı bulunduğu teşekkül varsa, bu ilan orada da yapılır. (4) Mükelleflerin vergi tarhına esas olan beyanları, kesinleşen vergi ve cezaları ile vadesi geçtiği halde ödenmemiş bulunan vergi ve ceza miktarları Maliye Bakanlığınca açıklanabilir. Maliye Bakanlığı bu yetkisini mahalline devredebilir. Ayrıca, kamu görevlilerince yapılan adli ve idari soruşturmalar ile ilgili olarak talep edilen bilgi ve belgeler ile bankalara, yapacakları vergi tahsiline yönelik bilgiler verilebilir. Bu bilgilerin verilmesine ilişkin usul ve esaslar Maliye Bakanlığınca belirlenir. Sahte veya muhteviyatı itibariyle yanıltıcı belge düzeledikleri veya kullandıkları vergi inceleme raporuyla tespit olunanların, kanunla kurulmuş mesleki kuruluşlarına ve 3568 sayılı Kanunla kurulan birlik ve meslek odalarına bildirilmesi vergi mahremiyetini ihlal sayılmaz. Bu takdirde kendilerine bilgi verilen kişi ve kurumlar da bu madde*

getirilen istisnalar ile her türlü açıklamanın vergi mahremiyeti kapsamında değerlendirilemeyeceği de belirlenmiştir.

Vergi mahremiyetine ilişkin temel ilke ile oluşturulan koruma alanı, burada belirlenen ilkenin ihlali durumunda söz konusu olacak yaptırıma ilişkin hükümler ile de tamamlanmıştır²⁷⁴. VUK'un ilgili hükümleri uyarınca, "(a)çıklanan bu bilgiler ele alınarak, mükelleflerin haysiyet, şeref ve haklarına" tecavüz edilmesi ya da vergi mahremiyetine uymaya yükümlü olanların, yükümlülüklerini yerine getirmemeleri durumunda ceza kanununda yer alan yaptırımların belirli oranda ağırlaştırılarak uygulanacağı hüküm altına alınmıştır²⁷⁵.

Yükümlünün vergisel bilgilerinin üçüncü kişilere aktarılması çeşitli sorunları beraberinde getirecektir. Kişilerin mali durumuna ilişkin bu türdeki bilgilerin yetkisiz kişilerin eline geçmesi yaşamını derinden etkileyebilir. Nitekim pek çok ülkede benimsenen konuya ilişkin bildirgelerde özel yaşamın gizliliğinin korunması; sır ve bilgilerin gizliliği vergi yükümlüsünün temel hakları arasında sayılmıştır²⁷⁶.

Özellikle kişinin mali bilgilerini meslekleri dolayısıyla öğrenenlerin gizliliği korumaları gerekir. Nitekim yukarıda da işaret edildiği üzere meslek sırrının açıklanması ceza kanunlarında suç olarak öngörülmüştür. Burada vergi memurları yanında, serbest muhasebe, mali müşavirlik meslek mensuplarının, yanında çalışanların, oda ve birlik personelinin de sır saklama yükümlülüğü bulunduğu belirtilmelidir. Serbest Muhasebeci, Mali Müşavirlik ve Yeminli Mali Müşavirlik

yazılı yasalara uymak zorundadırlar. Maliye Bakanlığı bilgilerin açıklanmasıyla ilgili usulleri belirlemeye yetkilidir. (5) Gelir Vergisi mükellefleri (Kazancı basit usulde tespit edilenler dahil) (...) ile sermaye şirketleri her yıl Mayıs ayının son gününe kadar vergi tarhına esas olan kazanç tutarları ile bunlara isabet eden vergi miktarlarını gösteren levhayı merkezlerine, şubelerine, satış mağazalarına iş sahipleri ile mükellefler tarafından kolayca okunup görünecek şekilde asmak zorundadırlar. İlan ve levhalara ilişkin diğer hususlar Maliye Bakanlığınca belli edilir. (6) (Ek fıkra: 26/06/1964 - 485/1 md.;Değişik fıkra: 23/01/2008-5728 S.K./272.mad) Açıklanan bu bilgiler ele alınarak mükelleflerin haysiyet, şeref ve haklarına tecavüz edilemez".

²⁷⁴ Gülşen GEDİK, "Vergi Mahremiyeti Kapsamındaki Bilgilerin Basında Yer Alması", **Vergi Dünyası**, S. 317, Ocak 2008, s. 126.

²⁷⁵ Bkz. VUK m. 5/5, 362. VUK m. 362 uyarınca vergi mahremiyetini ihlal edenler, TCK'nın 239. maddesi uyarınca cezalandırılacaktır. Burada suçun failinin yalnızca mükellefe ait sırları görevleri nedeniyle öğrenenlerin olabileceğini söyleyebiliriz. Dolayısıyla görevleri dışında örneğin tesadüfen bir yerde duyarak bu sırları öğrenenler suçun faili olamazlar. Vergi mahremiyetinin ihlali suçu için ayrıca bkz. Süheyl DONAY, **Ceza Mahkemesinde Yargılanan Vergi Suçları**, Beta, İstanbul 2008, s. 165-172.

²⁷⁶ **Tax Payers' Rights and Obligations-Practice Note**, haz. OECD Committee of Fiscal Affairs Forum on Tax Administration, 2003. Ayrıca OECD ülkelerinde yükümlü hakları uygulamalarına ilişkin olarak bkz. bkz. Selda AYDIN, s. 32-33.

Kanununun²⁷⁷ 43/1 hükmünde bu husus açıkça düzenlenmiştir²⁷⁸. Ancak aynı hükmün ikinci fıkrasında suç teşkil eden her türlü durumun ihbarının zorunlu olarak getirilmesi önemli bir sınırlamadır. Nitekim Anayasa'nın 20. maddesinden “adli soruşturma ve kovuşturmanın gerektirdiği haller”de özel ve aile yaşamının gizliliği hakkına sınırlama getirilebileceğine ilişkin hüküm çıkarılmıştır. TCK'da ise yalnızca devletin varlığını ortadan kaldırmaya ilişkin suçların ihbarı yükümlülüğü getirilmektedir²⁷⁹. Bu durumda her ne kadar Serbest Muhasebeci, Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanununun 43. maddesi özel yaşamın gizliliğini koruyucu bir hüküm olarak tasarlansa da sınırlamalarda aşırıya kaçıldığı görülmektedir.

Kişinin vergi ile ilişkili bilgilerinin basın yoluyla açıklanması durumunda da önemli zararlar doğabilir. Böyle bir durumda elbette yukarıda değinilen hukuk ve ceza dava yollarına gitmek olanaklıdır. Her durumda gizliliği sağlamakla yükümlü olanların sorumluluğu bulunacaktır. Ancak burada bu bilgileri açıklayan basın görevlilerinin sorumluluğu ne olacağı sorusu akla gelebilir. Bu noktada, daha önce de değinildiği gibi iki alan arasında tartma ve dengeleme gerekir. Özellikle siyasal figürler üstlenmiş kişiler söz konusu olduğunda düşünciyi açıklama ve bu kapsamda basın özgürlüğüne ağırlık verildiği görülmektedir²⁸⁰.

²⁷⁷ Kanun no. 3568, t. 1 Haziran 1989, R.G. t. 13 Haziran 1989, S. 20194.

²⁷⁸ Belirtilen kanunun 43.madde hükmü şöyledir: “(1)Meslek mensupları ve bunların yanlarında çalışanlar, işleri dolayısıyla öğrendikleri bilgi ve sırları ifşa edemezler, çeşitli kanunlarla muhbirlerle tanınan hak ve menfaatlerden faydalanamazlar. (2)Ancak, suç teşkil eden hallerin yetkili mercilere duyurulması mecburidir. (3)Adli veya idari her türlü inceleme veya soruşturma birinci fıkra hükmünün dışındadır. (4) Tanıklık, sırrın ifşası sayılmaz. (5) Yukarıdaki hükümler oda ve birlik personeli hakkında da uygulanır”.

²⁷⁹ Bu konuya ilişkin olarak ayrıca bkz. Leyla ATEŞ, “Meslek Mensuplarının Sır Saklama Yükümlülüğünü Özel Yaşamın Gizliliği ile Okumak”. **E-Yaklaşım**, Kasım 2003, S. 4, <http://www.yaklasim.com>.

²⁸⁰ YALTI'ya göre bu soru yanıtlanırken “özel yaşam-siyasi sorumluluk kavramları üzerinden yapılacak bir okuma, ölçünün demokratik toplum gerekleri ve bu bağlamda şeffaflık olarak ortaya konabileceğini göstermektedir. (AİHM) (bir) kararında siyasi organlarda görev alan kişilerin özel yaşam haklarının sıradan vergi yükümlülerine nazaran daha sınırlandırılabilir olduğunu ve böyle olduğu takdirde bunun demokratik toplumun gereklerine aykırı olmadığını/olamayacağını ortaya koymuştur”. Billur YALTI, s. 175. Yükümlülerin vergisel işlerine ilişkin bilgilerin basında yer alması AİHM önünde de değerlendirilmiştir. Örneğin Verlagsgruppe News GmbH'nin Avusturya'ya karşı yaptığı başvuru (No.2, b.n. 10520/02, k.t. 14 Mart 2007) vergi kaçakçılığına ilişkin hukuksal süreç devam ederken yükümlünün fotoğraflarının yayınlanması nedeniyle gazete kuruluşunun sorumlu bulunmasına ilişkindir. Mahkeme burada özel yaşamın gizliliği hakkı ile düşünciyi açıklama özgürlüğünün karşı karşıya geldiği durumlarda basında yer alan fotoğraf ya da metnin kamuoyu yaratmasına olan katkısının dikkate alınması gerektiğini vurgulamıştır (par. 40). Somut olayda da AİHM fotoğrafın yayınlanmasının mutlak surette yasaklanmasının izlenilen meşru amaçla orantılı olmadığına, dolayısıyla AİHS'in düşünciyi açıklama özgürlüğünü düzenleyen 10. maddesinin ihlaline karar vermiştir. Bu noktada siyasal figürler söz konusu olduğunda bu bilgilerden kaynaklı kamusal yararın daha yüksek

Her alanda olduğu gibi mali konularda da bilişim teknolojileri artan oranda kullanılmaktadır. Bu bağlamda her gerçek ve tüzel kişinin bir vergi numarası olması uygulaması yürürlüğe girmiştir. VUK'un 8/5 hükmü uyarınca “*Türkiye Cumhuriyeti tabiyetinde bulunan her gerçek kişi ile tüzel kişilere bir vergi numarası verilir*”²⁸¹. Kişi hak ve özgürlüklerinin korunabilmesi için belirtilen hükümde vergi numarası ile yükümlüye ilişkin bilgilere üçüncü kişilerce ulaşılmayacağının açıkça belirtilmesi gerekirken böylesine bir düzenleme yapılmamıştır²⁸².

Vergi İstihbarat Arşivi'nin kurulması ise vergilendirme alanında bilişim teknolojilerinin kullanılmasının bir diğer örneğidir. Yasal dayanağını VUK'nun 152. maddesinde bulan İstihbarat Arşivi²⁸³, “mükellefler hakkında yapılan inceleme ve değerlendirmelerde esas alınmasında fayda görülen bilgileri toplamak, toplanan bilgilerin bilgisayar kayıtlarına geçirilmesini sağlamak, bilgisayardan alınan bilgilerle sistemli bir istihbarat arşivi oluşturmak ve arşivden oluşan bilgileri denetim birimlerine periyodik olarak göndermek üzere kurulmuştur”²⁸⁴.

Vergi idaresinin yükümlülere ilişkin bilgileri toplamada çeşitli kaynakları olduğu belirtilmelidir. Nitekim VUK'un ilgili hükümlerinde bu konuya ilişkin genel kurallar saptanmıştır. Buna göre kendisinden bilgi istenen kişi ve kurumlar kendilerinden istenen bilgileri vermeye zorunludurlar²⁸⁵. Kimi zaman bu zorunluluk

olacağı dikkatten kaçmamalıdır. Ancak tekrar işaret etmek gerekir ki buradaki değerlendirme gazetecilerin sorumluluğuna ilişkindir, bilgilerin üçüncü kişilere aktarılmasını sağlamakla yükümlü olanların sorumluluğu devam edecektir. Nitekim Fressoz ve Roire, Fransa'ya karşı kararında (b.n. 29183, k.t. 21 Ocak 1999) AİHM de bu konuya işaret etmiştir. Başvuruya konu olan olayda bir vergi memurundan elde ettikleri vergi beyannamelerinin ellerinde bulunması nedeniyle gazeteciler mahkum edilmiştir. AİHM yaptığı değerlendirmede de yalnızca vergi memurlarının gizlilikle ilgili yükümlülüğü bulunduğuna, gazetecilerin kendilerine anonim olarak gönderilmiş olan beyannamelerin güvenin ihlali yoluyla elde edilmiş olduğunu bilemeyeceklerine işaret etmiştir(par. 46).

²⁸¹ VUK m. 8/5 şu hükmü içermektedir: “*Türkiye Cumhuriyeti tabiyetinde bulunan her gerçek kişi ile tüzel kişilere bir vergi numarası verilir. Bu hükmün uygulanmasına ilişkin usul ve esasları tespit etmeye ve vergi numarasının kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerce yapılacak işlemlerle ilgili kayıtlarda ve düzenlenecek belgelerde kullanılması mecburiyetini getirmeye Maliye Bakanlığı yetkilidir*”.

²⁸² Nitekim GÜNEŞ ve ŞİRİN'e göre “*verilen vergi numarası ile mükellefe ilişkin bilgilere başka şahıslarca veya kurumlarca ulaşılamayacağının, ulaşılsa cezai müeyyide uygulanacağının yasada açıkça belirtilmesi gerekmektedir*”. Bkz. Gülşen GÜNEŞ, Ertunç ŞİRİN, “Vergi Ödevlisinin Hakları”, **Vergi Sorunları**, S. 197, Şubat 2005, s. 139.

²⁸³ Vergi mevzuatı açısından İstihbarat Arşivine ilişkin düzenlemelerin tarihsel gelişimi için bkz. Fazıl AYDIN, “Vergi İstihbarat Arşivi”, **Vergi Sorunları**, S. 167, Ağustos 2002, s. 219-220.

²⁸⁴ Ali DAYIOĞLU, “Vergi İstihbarat Arşivi”, **Vergi Sorunları Dergisi**, S. 6, Ekim-Kasım 1987, s. 27'den aktaran; Fazıl AYDIN, s. 218.

²⁸⁵ VUK'un “*bilgi verme*” kenar başlıklı 148. maddesi uyarınca “*(1) Kamu idare ve müesseseleri, mükellefler veya mükelleflerle muamelede bulunan diğer gerçek ve tüzel kişiler, Maliye*

belirli aralıklarla düzenli ve devamlı bilgi vermeyi de kapsayabilir²⁸⁶. Bazı istisnaları olmakla birlikte “(k)endilerinden bilgi istenilen gerçek ve tüzel kişiler, özel kanunlarda yazılı mahremiyet hükümlerini ileri sürerek, bilgi vermekten imtina edemezler”²⁸⁷. Böylesi bir durumda kendisinden bilgi istenen kişi veya kurumun özel yaşamın gizliliği hakkını ihlal etmesinden kaynaklı sorumluluğu ile vergi idaresine karşı olan yükümlülüğünün karşı karşıya geleceği düşünüldüğünde, hangi durumlarda bilgi verileceğinin sınırlarının belirlenmesinin önemi bir kez daha anlaşılacaktır²⁸⁸.

Devletin vergilendirmenin etkin ve doğru bir şekilde gerçekleştirilebilmesi için kişisel bilgilere gereksinim duyduğu açıktır. Kişisel bilgilerin orantılılık ilkesini uygun bir şekilde bu nedenle toplanması meşrudur. Öte yandan yukarıda verilen birkaç örnekte de görüldüğü üzere, sorun daha çok edinilen bilgilerin gizli olarak tutulması ve üçüncü kişilere hangi durumlarda aktarılabilmesine ya da yükümlü ve

Bakanlığının veya vergi incelemesi yapmaya yetkili olanların istiyebilecekleri bilgileri vermeye mecburdurlar. (2) Bilgiler yazı veya sözle istenilir. Sözle istenen bilgileri vermeyenlere keyfiyet yazı ile tekit ve cevap vermeleri için kendilerine münasip bir mühlet tayin olunur. Bilgi istenmek üzere ilgililer vergi dairesine zorla getirilemez. (3) Memleket dışı imtiyazlarından faydalanan yabancı Devlet memurları bilgi verme mecburiyetine tabi olamazlar”.

²⁸⁶ VUK’un “devamlı bilgi verme” kenar başlıklı 149. maddesi uyarınca “Kamu idare ve müesseseleri (Kamu hizmeti ifa eden kurum ve kuruluşlar dahil) ile gerçek ve tüzel kişiler vergilendirmeye ilişkin olaylarla ilgili olarak Maliye ve Gümrük Bakanlığı ve vergi dairesince kendilerinden yazı ile istenecek bilgileri belli fasıllarla ve devamlı olarak yazı ile vermeye mecburdurlar”.

²⁸⁷ VUK’un 151. maddesinde bu kural ve istisnaları belirlenmiştir. Buna göre “Kendilerinden bilgi istenilen gerçek ve tüzel kişiler, özel kanunlarda yazılı mahremiyet hükümlerini ileri sürerek, bilgi vermekten imtina edemezler. Ancak: 1. Posta, Telgraf ve Telefon İdaresinin muhabere haklarında tutmaya mecbur olduğu mahremiyet saklıdır; 2. Hekimlerden, diş hekimlerinden, dişçilerden, ebelerden ve sağlık memurlarından hastaların hastalıklarının nevi’ne mütaallik bilgiler istenemez. 3. Avukatlardan ve dava vekillerinden kendilerine tevdi olunan işler veya görevleri dolayısıyla muttali oldukları ahval ve hususların bildirilmesi istenemez; şu kadar ki, bu yasak müvekkil adlariyle vekalet ücretlerine ve giderlerine şamil değildir; 4. Ceza Muhakemeleri Usulü Kanununun 88 inci Maddesi gereğince gösterilmesi veya teslimi caiz olmıyan evrakın muhteviyatı hakkında bilgi istenemez. Şu kadar ki, doğrudan doğruya vergi ile ilgili olmak üzere, bu gibi evraka müsteniden doğan borçların miktarlarına ve alacaklıların adlarına bilgiler istenebilir”.

²⁸⁸ Bankaların bilgi verme yükümlülüğünün sınırlarını değerlendirdiği makalesinde BAŞARAN şu saptamada bulunmuştur: “İdarenin ne zaman yetkisini aşarak anayasa ve kanunlara aykırı davranmış olacağına gelince, ne yazık ki VUK’da bu konuda yeterli düzenleme getirilmemiştir. Oysa, bankanın bilgi verme yükümlünün sınırlarını, idarenin bilgi talep edebilme yetkisinin sınırları oluşturmaktadır. Hukuka aykırı bilgi talebini reddetmeyen banka, bu davranışından ötürü müşterisine karşı hukuken ve cezaen sorumlu olacak; hukuka uygun bilgi talebini yerine getiremeyen banka ise, özel usulsüzlük cezası ile cezalandırılacaktır. Vergi idaresinin bilgi talep edebilme yetkisinin sınırlarını ya da tespit ve geliştirme görevi, kanundaki düzenlemelerin yetersizliği karşısında içtihatlar ve doktrine aittir”. Funda BAŞARAN, “Bankaların Bilgi Verme Yükümlülüğünün Sınırları ve Bilgi Vermekten Çekinmeye Bağlı Özel Usulsüzlük Suçu-Müşteri Sırrını Saklama Yükümlülüğü ile Özel Usulsüzlük Suçu Arasında Bir Gri Bölge”, **Vergi Sorunları**, S. 143, Ağustos 2000, s. 194.

üçüncü kişilerden bu bilgilerin ne zaman istenebileceğine ilişkindir. Edinilen bilgilerin yalnızca amaçları doğrultusunda kullanılması ve üçüncü kişilere aktarılmaması yükümlünün temel hak ve özgürlüklerinin korunması açısından oldukça önemlidir. Konuya ilişkin her bir düzenlemede bu hususlara özellikle dikkat edilmelidir. Oluşabilecek boşluklara ilişkin temel düzenleme ise ancak genel bir kişisel verilerin korunması yasının kabulü ile olanaklıdır. Nitekim bu yasa ile vergi yükümlüsü bilgilerinin ancak hangi amaçlar için ve kimlerce kullanılacağını öngörebileceği gibi, kendisinden bilgi istenen kişi ve kurumların da hangi bilgileri paylaşabileceğinin sınırları belirlenmiş olacaktır.

G. BİLGİ EDİNME HAKKI

Çalışmamızın birinci bölümünde de belirtildiği üzere bilgi edinme hakkı ve kişisel verilerin korunması birbirleriyle yakından ilişkili alanlardır. Hatta bu nedenle kimi çalışmalarda bilgi toplumunun iki önemli sütunu olarak nitelendirildikleri görülmektedir. Her iki hak alanı kimi açılardan birbirlerini tamamlarken kimi durumlarda da diğerinin sınırlarını oluşturur. İşte bu nedenle pek çok ülkede kişisel verilerin korunması ve bilgi edinme hakkı yasaları eş zamanlı olarak yürürlüğe girmiştir. Türkiye’de ise “*İdari Usul ve Bilgi Edinme Kanunu*” hazırlığı yapılmış ancak bir sonuca varılamamıştır. Oysa idari usul, bilgi edinme hakkı ve kişisel verilerin korunmasına ilişkin yasaların eş zamanlı kabulü ve ortak bir dille hazırlanması aralarındaki yakınlık dolayısıyla oldukça önemlidir²⁸⁹.

Türkiye’de Bilgi Edinme Hakkı Kanunu, 24 Nisan 2004’te yürürlüğe girerken Kişisel Verilerin Korunması Kanun Tasarısı halen ilgili komisyonun önündedir. Uygulamada etkin sonuç alınamaması gibi eleştirilere maruz kalan Bilgi Edinme Hakkı Kanununun (BEHK), şeffaf yönetim özleminin de bir ürünü olduğunu belirtmek gerekir. BEHK’nın düzenleme alanı dar ve sınırlı olmasına karşın bir ilerleme sayılabilir²⁹⁰.

Nitekim bilgi edinme hakkının öznesi bireydir. Birey, bu hakkını kullanarak kamu gücü karşısındaki “*edilgen*” yapısından kurtulup, “*etken*” olmuş, “*soran*”, “*sorgulayabilen*”, “*soruşturabilen*” bir varlık haline gelmiştir. Bu, hukuk düzeni

²⁸⁹ Tekin AKILLIOĞLU, “İdari Usul ve Kişisel Verilerin Korunması”.

²⁹⁰ İbrahim Ö. KABOĞLU, *Anayasa Hukuku Dersleri*, 2. Baskı, Legal, İstanbul 2005, s. 281.

içinde daha güçlü bir konuma kavuşmasını sağlamaktadır²⁹¹. Bu bağlamda BEHK, bireye idarenin elinde bulunan kişisel verilerini öğrenme hakkını vermektedir. Bu anlamda bilgi edinme hakkının bir yönüyle kişisel verilerin korunmasının temel ilkelerinden bilgilere erişim hakkını sağladığı söylenebilir.

Bilgi edinme hakkı ile kişisel verilerin korunmasının kaynağını bulduğu özel yaşamın gizliliği hakkı arasındaki yakın ilişkiyi AİHM kararları da ortaya koymaktadır. AİHM ilk kez Gaskin kararında²⁹² bilgilere erişim hakkının Sözleşmenin özel yaşamın gizliliğinin düzenlendiği 8. maddesi kapsamında değerlendirilebileceğine hükmetmiştir. Bu yaklaşım, daha sonraki başka kararlarda da tekrarlanmış ve devlet tarafından tutulan kişisel verilere erişim talepleri 8. maddenin kapsamında görülmüştür²⁹³. Ancak konuya ilişkin kararlar incelendiğinde bu hakkın her durumda tanınmadığı görülür. Örneğin Gaskin kararında başvuranın talep ettiği bilgilere ulaşmasının kişisel gelişimi açısından önemine dikkat çekilmiştir. Bu nedenle kararın her türdeki kişisel veriye erişim hakkının tanınması gerektiği şeklinde yorumlanması yanlış olacaktır²⁹⁴. Ayrıca Mahkeme, kişisel verilere erişim hakkına ilişkin kararlarında denge testini uygulamış ve bilginin toplanıp saklanması ile bireye açıklanması arasındaki dengenin adil olarak sağlanması gerektiğine işaret etmiştir. Ayrıca kamusal yararın ağır bastığını saptadığı *M.G., Birleşik Krallık'a karşı* ve *Roche, Birleşik Krallık'a karşı* gibi kararlarında, çıkar çatışmasını önlemek üzere iç hukukta bağımsız bir organın bulunması

²⁹¹ Müslüm AKINCI, “ ‘Güvenlik Kayıtları’ ya da ‘Bilgi Fişleri’nin İdare Hukuku Bakımından Değerlendirilmesi”, **Bülent Tanör Armağanı**, Legal, İstanbul 2004, s. 31.

²⁹² *Gaskin, Birleşik Krallık'a karşı*, b.n. 10454/83, k.t. 7 Temmuz 1989. Kişisel verilere erişime ilişkin olarak Gaskin ve Leander kararlarının farklı sonuçlanmasını Mahkeme’nin bu konuda bir içtihat değişikliğine gittiği şeklinde yorumlamamak gerekir. Nitekim her iki karar nitelikleri bakımından oldukça farklıdır. Örneğin Gaskin davasında kayıtlar bir gencin vesayet altındaki durumuna ilişkinken, Leander davasında ulusal güvenlik ile ilişkilidir. Bu konuya ilişkin kısa bir değerlendirme için bkz. Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s. 278, d.n. 128.

²⁹³ Örneğin bkz. *Guerra ve diğ. İtalya'ya karşı, Rotaru, Romanya'ya karşı, Amann, İsviçre'ye karşı, McGinley ve Egan Birleşik Krallık'a karşı*, b.n. 21825/93, 9 Haziran 1998. Gaskin kararına konu olan olay, başvuranın ergenlik döneminde vesayeti altında bulunduğu yerel merci tarafından bu dönem boyunca kendisi hakkında tutulan gizli belgelere erişim isteğinin reddine ilişkindir. Taraf Devletin iç hukuku uyarınca bu karara karşı gidilebilecek bir üst makam da bulunmamaktadır. Sonuçta Mahkeme Gaskin kararında Birleşik Krallık’ın Sözleşme’nin 8. maddesini ihlal ettiğine karar vermiştir. Mahkemeye göre, bir kişinin çocukluğu ve gelişimi konusunda bilgi alması yaşamsal bir çıkara karşılık gelmektedir. Buna karşılık kamu organları tutulan kayıtların gizliliğinin de bazı çıkarlara hizmet ettiği akılda tutulmalıdır. Bu durum kendini özellikle, objektif ve güvenilir bilgiler edinilmesi ve üçüncü kişilerin haklarının korunması açısından gösterir. *Gaskin kararı*, par. 49.

²⁹⁴ Lee A. BYGRAVE, “Data Protection Pursuant to the Right to Privacy”, s. 278.

gerektiğine işaret etmiştir²⁹⁵. Dolayısıyla bilgi edinme hakkının kişisel verilerin korunması için sınırlı da olsa bir katkı sağladığı ancak yeterli olmadığı söylenebilir.

Öte yandan kimi durumlarda kişisel verilerin korunması hakkı bilgi edinme hakkının sınırını da oluşturabilmektedir. Nitekim BEHK’da da bu konuya ilişkin bir hüküm bulunmaktadır. Yasanın “*özel hayatın gizliliği*” kenar başlıklı 21. maddesi uyarınca kişinin sağlık bilgileri, özel ve aile yaşamına ilişkin bilgiler, şeref ve haysiyetine haksız müdahale sayılabilecek bilgiler ve mesleki ve ekonomik değerlerine haksız müdahale sayılabilecek bilgiler bilgi edinme hakkının kapsamı dışında tutulmuştur²⁹⁶. Ancak kamu yararının gerektirdiği hallerde kişisel nitelikteki bilgi ve belgeler ilgiliye en az yedi gün önceden haber verilerek yazılı rızası alınmak suretiyle açıklanabilir²⁹⁷.

VII. KİŞİSEL VERİLERİN KORUNMASI KANUN TASARISI

A. KİŞİSEL VERİLERİN KORUNMASI YASASI GEREKLİ Mİ?

Kişisel Verilerin Korunması Kanun Tasarısında yer alan hükümlerin incelenmesine geçmeden önce kanımızca konuya ilişkin daha genel bir sorunun cevaplanması gerekir: Türkiye’de bir kişisel verilerin korunması yasası gerekli midir?

²⁹⁵ Cavidan SOYKAN, s. 69-70. Bkz. *M.G., Birleşik Krallık’a karşı*, b.n. 39393/98, 24 Eylül 2002; *Roche, Birleşik Krallık’a karşı*, b.n. 32555/96, k.t. 23 Mayıs 2002.

²⁹⁶ BEHK’nın hükümet teklifinde 21/1 hükmünde yalnızca aile yaşamına yer verilmiştir. TBMM’de yasalaşma sürecinde ise Avrupa Birliği Uyum Komisyonunun Raporuna uygun olarak “*özel ve aile yaşamı*” şeklinde kanımızca oldukça yerinde olan bir değişiklik yapılmıştır. BEHK’nın yasalaşma sürecine ilişkin olarak bkz. Haşmet Sırrı AKŞENER, Ramazan ÇAKMAKÇI, **Açıklamalı, Gerekçeli Bilgi Edinme Hakkı Kanunu**, Legal, İstanbul 2004.

²⁹⁷ Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas Ve Usuller Hakkında Yönetmelik’in (27 Nisan 2004 Tarihli Resmi Gazete, Sayı: 25445, Karar S. 2004/7189), 32. maddesi şöyleydi: “(1) Kişinin izin verdiği haller saklı kalmak üzere, *özel hayatın gizliliği* kapsamında, açıklanması halinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, mesleki ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. (2) Kamu yararının gerektirdiği hallerde, kurum ve kuruluşların kayıtlarında bulunan kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir”.

Türkiye, insan haklarına saygılı demokratik bir hukuk devleti olma idealini Anayasasında açıklamış bir devlettir. AK, BM, OECD gibi örgütlerin üyesi olan Türkiye, uluslararası alanda da bu niteliğiyle varlığını sürdürmektedir. Ancak ne yazık ki kişisel verilerin korunması alanında bu kuruluşlar bünyesinde benimsenen ilkeleri iç hukukunun bir parçası haline getirmemiş ve çalışmamızın ikinci bölümünde incelenen önemli gelişmelerin gerisinde kalmıştır.

AK Kişisel Verilerin Korunması Sözleşmesi Türkiye tarafından 1981 yılında imzalanmış olmasına karşın, iç hukukta gereken düzenlemeler yapılmadığı için onaylama işlemi halen gerçekleşmemiştir²⁹⁸. Türkiye’de kapsayıcı bir kişisel verilerin korunması yasasının yürürlüğe girmemesi BM ve OECD’nin yukarıda incelenen rehber ilkelerine uygun bir düzenlemenin de yapılamadığını gösterir. Nitekim yukarıda işaret edildiği üzere mevzuatımızda konuya ilişkin dağınık hükümlerin bulunmasına karşın temel ilkelerin belirlendiği özel ve kapsayıcı bir yasanın yokluğu önemli bir eksiklik olarak karşımıza çıkmaktadır.

Daha önce de belirtildiği üzere Avrupalı devletlerin bir çoğunda kişisel verilerin korunması, yaklaşık kırk yıldır hukuksal düzenin bir parçasıdır. Bu bakımdan en köklü düzenlemelerin Avrupa’da bulunduğunu söylemek yanlış olmayacaktır. ABD bir yana bırakılacak olursa çağdaş demokratik devletlerin hemen hemen tamamı bu konuda düzenlemeler benimsemiştir²⁹⁹. Henüz bu konuda

²⁹⁸ Şubat 2009 itibarıyla AK üyesi devletlerden yalnızca altısı Sözleşmeyi onaylamamıştır. Bunlar, Azerbaycan, Ermenistan, Rusya, San Marino, Türkiye ve Ukrayna’dır. Bkz. <http://conventions.coe.int>.

²⁹⁹ Örneğin Kanada’da, hem federal hem de federe düzeyde AB’nin benimsediği ölçütlere uygun yasal düzenlemeler yürürlüktedir. Michael ERBSCHLOE, John VACCA, **Net Privacy (A Guide to Developing and Implementing an Ironclad Ebusiness Privacy Plan)**, Mc Graw-Hill, ABD 2001, s. 37. Federal düzeyde kabul edilmiş iki önemli yasadandır, kamu sektörüne yönelik Özel Yaşamın Gizliliği Yasası (Privacy Act), diğeri ise özel sektöre yönelik Kişisel Bilgilerin Korunması ve Elektronik Belgeler Yasasıdır (The Personal Information Protection and Electronic Documents Act-PIPEDA). Bunun yanında çalışmamızın ikinci bölümünde işaret edildiği üzere Orta ve Kuzey Amerika’da konuya ilişkin farklı bir yaklaşım benimsenmiş ve bölgedeki çeşitli ülkelerde kişisel verilerin “*habeas data*” bireysel şikayeti ile korunması tercih edilmiştir. Dünyanın farklı bir coğrafyasından verilebilecek bir diğer örnek ise Hong Kong’dur. Hong Kong’da da kişisel verilerin korunması kapsayıcı bir yasal düzenlemenin konusudur. Hong Kong’da kişisel verilerin korunmasının çerçevesini oluşturan yasal düzenleme, 1996 yılında yürürlüğe giren Kişisel Veriler (Özel Yaşamın Gizliliği) Talimatnamesi’dir (Personal Data (Privacy) Ordinance- PDPO). Metnin birinci ekinde, kişisel verilerin toplanma amacı ve usulü, doğruluğu, saklanma süresi, kullanımı, güvenliği de dahil olmak üzere konuya ilişkin temel ilkeler belirlenmiştir. Metin genel olarak mücadeleci değil, uzlaştırıcı bir yaklaşımı yansıtmaktadır. Ji Lian YAP, s. 321-322. Avustralya ve Yeni Zelanda da kişisel verilerin korunmasını ulusal hukuk sistemlerinde yaptıkları düzenlemeler ile güvence altına almışlardır. Bkz. **Privacy and Human Rights 2006**, s. 229-248; 711-725.

düzenleme yapmamış devletlerin üzerinde ise artan oranda bir baskı olduğu söylenebilir³⁰⁰.

Bu doğrultuda kişisel verilerin ulusal hukuk sistemlerinde genel yasalar ile korunması yönünde bir eğilimin güçlendiğini belirtmek gerekir. Bunun temelde üç nedenden kaynaklandığı söylenebilir³⁰¹. İlk olarak özellikle daha önce otoriter siyasal sistemlerin hüküm sürdüğü, Orta Avrupa, Güney Amerika ve Güney Afrika gibi bölgelerde bu acıların tekrar yaşanmaması için alınan önlemler kapsamında kişisel verilerin korunmasına yönelik hukuksal düzenlemeler kabul edilmiştir.

İkinci olarak ekonomik etkenler dikkate alınmalıdır. Burada en başta gelen konu elektronik ticaret (e-ticaret) tir. İleride karşılaşılabilecekleri sorunların farkında olan pek çok İnternet kullanıcısının, kişisel verilerini sanal ortamda paylaşmak konusunda isteksiz olduğu görülmektedir³⁰². E-ticaretin önündeki bu engeli fark eden pek çok ülke, kişisel verilerin korunması yönünde düzenlemeler yapmayı tercih etmiştir. En bilinen örnekler olarak bazı Asya devletleri ve yine Kanada verilebilir. Üçüncü olarak AB düzenlemeleri ile uyumu sağlamak da kişisel verilerin korunması

³⁰⁰ Örneğin Çin’de kişisel verilerin korunmasına ilişkin bir yasa bulunmamaktadır. Ancak konuya yönelik artan ilgi ve kamudan yükselen talepler dolayısıyla kişisel verilerin korunmasına ilişkin bir tasarı hazırlanmış ve Devlet Konseyine sunulmuştur. Çin’de kişilik haklarının korunmasına ilişkin hükümler çerçevesinde oldukça sınırlı da olsa bazı güvenceler bulunmaktadır. Bunun yanında Çin Ceza Kanun’da yapılacak değişiklik tasarısında hükümet organlarında ya da telekomünikasyon, finans, taşımacılık, eğitim ve tıp sektörlerinde görev yapan kişilerin kişisel verileri satmaları ve açıklamaları durumunda cezai yaptırım öngörülmektedir. Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 63. Orta Doğu ve Afrika’da ise özel yaşamın gizliliğinin oldukça sınırlı bir biçimde korunduğu belirtilmelidir. Bölgedeki pek çok ülkede gözetimin kural, kişisel verilerin korunmasının ise istisna olduğu söylenebilir. Orta Doğu’da yalnızca İsrail, Afrika kıtasının genelinde ise yalnızca Güney Afrika kişisel verilerin korunmasına yönelik yasalara sahiptir. David BANISAR, “Privacy and Data Protection Around the World”, s. 4. Kişisel verilerin korunmasına ilişkin İsrail hukuk düzeninin getirdiği hükümleri AB Yönergesi’ndeki gereklilikler çerçevesinde inceleyen eleştirel bir değerlendirme için bkz. Omer TENE, “Is Israel Data Protection Law ‘Adequate’ Under Article 25”, **Privacy and Data Protection**, C.8, S.5, Y. 2008, s. 9-13. Ancak AB Veri Koruma Yönergesi’nin zorlayıcılığı bu bölgede de hissedilmektedir. Bir yanda hızla gelişen uluslararası ticaret ve bu kapsamda dünyanın en önemli güçlerinden AB ile ticari ilişkilerin sürdürülmesi gerekliliği, diğer yanda farklı bir kültür ile beslenen ve batılı ülkelerin kendi kültürlerini dayattıkları düşüncesi, özellikle bölgedeki İslam devletleriinn konuya çekimser yaklaşılmasına neden olmaktadır.

³⁰¹ David BANISAR, “Privacy and Data Protection Around the World”, s. 2; **Privacy and Human Rights 2006**, s. 9.

³⁰² Hatta kişisel verilerin korunmasına ilişkin ilkelerin benimsenmesi, e-ticaretin gelişmesi ve çevrim içi tüketicilerin bu yeni ortama güvenlerinin sağlanması için bir önkoşul olarak bile kabul edilebilir. Yaman AKDENİZ, **Beyaz Kitap**, Papatya, İstanbul 2003, s. 29. Bu noktada şuna da işaret etmek gerekir: kişisel verilerin korunmasında itici güç olan ekonomik faktörü yalnızca doğrudan ticari çıkarlar üzerinden düşünmemek gerekir. Ekonomik kalkınma sağlandıkça bireyler özel yaşamın gizliliği ve kişisel verilerin korunmasının da içinde bulunduğu temel hak ve özgürlüklerine ilişkin daha bilinçli hale gelmesi de önemli bir etkidir. Gabriela KENNEDY, Sarah DOYLE, Brenda LUI ve diğ., s. 60.

yasalarının benimsenmesinde itici güç olabilmektedir³⁰³. AK üyesi ve AB'ye üyelik sürecindeki devletler yanında, Güney Amerika'daki bazı devletler ve Kanada'da AB Yönergesindeki gereklilikler dolayısıyla ticaretin etkilenmemesi hedefiyle kişisel verilerin korunması yasalarını kabul edilmiştir³⁰⁴.

Türkiye açısından baktığımızda kişisel verilerin korunması yasasının kabulü açısından her üç nedenin de etkili olması gerektiğini söyleyebiliriz. Birincisi, 20. yüzyılda Türkiye'de II. Dünya Savaşı döneminde Almanya, İtalya gibi Avrupa ülkelerinde, daha sonraki dönemde ise Güney Amerika ve Doğu Avrupa ülkelerinde görülen sistemli baskıcı bir yönetim hüküm sürmemişse de geçmişteki bazı kötü uygulamalar, kişisel verilerin korunmadığı bir ortamda oluşabilecek zararlara ilişkin ipucu vermektedir. Nitekim yukarıda da işaret edildiği üzere Türkiye'de çeşitli dönemlerde güvenlik soruşturmalarına, bunların sonuçlarına ve özellikle fişleme uygulamasına ilişkin pek çok tartışmanın alevlendiği bir gerçektir³⁰⁵. Kamusal organların bireyleri kayıt altına alma yönündeki eğilimleri teknolojiye gelişmelerle birleştiğinde temel hak ve özgürlüklere yönelik ciddi bir tehdidin ortaya çıkabileceği ise açıktır.

³⁰³ Örneğin Birleşik Krallıkta ilgili yasanın çıkarılma nedenlerini tartışan bir çalışmada iki temel nedenin ileri sürüldüğü görülmektedir. Birincisi, Avrupa Konseyi bünyesinde hazırlanan Veri Koruma Anlaşmasını (Data Protection Convention) onaylama zorunluluğudur. Bu anlaşmanın onaylanmaması durumunda Birleşik Krallıkta etkinlik gösteren şirketler, veri koruma yasalarını kabul etmiş ülkelerde çalışanlarla rekabette ciddi sıkıntılar yaşayacaklardır. Çünkü anlaşma, taraf devletlere, veri korumaya ilişkin olarak yeterli düzeyde koruma sağlamayan devletlere kişisel bilgilerin transferini reddetme hakkı tanımaktadır. İkinci neden ise, yüksek hızlı bilgisayarların kişisel bilgileri işleme ve birbirleriyle ilişkilendirme becerileriyle birlikte hızla yayılmasının mahremiyete karşı ciddi bir tehdit oluşturmasıdır. Chris EDWARDS, Nigel SAVAGE, **Information Technology and the Law**, Macmillan Publishers, Birleşik Krallık 1986, s. 75.

³⁰⁴ David BANISAR, "Privacy and Data Protection Around the World", s. 2; **Privacy and Human Rights 2006**, s. 9.

³⁰⁵ Bu türdeki uygulamaların ciddiyetine örnek olarak 11-12 Nisan 1987'de Ankara'da toplanan TBB'nin 8. Olağanüstü Genel Kurul Kararı'nın 3. madde hükmü aktarılabilir: "*Kamu personelinin, hatta yargıç ve savcılarının atama, yükseltme, yer değiştirme işlemleri anayasal ve yasal dayanağı bulunmayan güvenlik soruşturması sonuçlarına bağlanmıştır. Yurttaşlar öğrencilik yıllarından başlayarak yetkisiz kişi ve kurumlarca fişlenmektedirler. Olağanüstü dönemlerde bile benimsenmeyecek yöntemler, Resmi Gazete'de yayınlanmayan kararname ve genelgelerle olağan dönemin süreklilik taşıyan uygulamaları arasına girmiştir. Türkiye'de kişilerin geçmişteki suçluluk durumlarını belgeleyecek tek yetkili kaynak Adli sicil kayıtlarıdır. Devlet memurlarının yasada belirlenen genel nitelikleri yalnız bu kuruluştan sağlanabilir. Hukuk devleti ilkeleri ile bağdaşmayan, kamu hizmetinin işleyişini olumsuz yönde etkileyen, kamu personelini siyasal iktidara daha da bağımlı kılan ve yasa önünde eşitlik kuralını işlemez duruma getiren: -Güvenlik soruşturması uygulamasına, -Yurttaşların fişlenmesine son verilmelidir. Öte yandan bilgisayarların kullanılmaya başlanmasıyla, özel bilgi işlem odakları yaygınlaşmaktadır. Özel kuruluşlar da kendi uğraş alanlarında kişisel bilgiler derlemekte, böylece özel yaşamın gizliliği ilkesi yara almaktadır. Denetimsiz birimlerin özellikle gelecekte yaratacağı sakıncalar gözetilerek bu gelişmeler kişi hak ve özgürlüklerini güvence altına alan yasal kurallara bağlanmalıdır". Alıntı için bkz. Güney DİNÇ, s. 197-198*

Böylesine uygulamaların yalnızca otoriter yönetimlerde görülmediği, demokratik yönetimlerde de gerekli önlemler alınmadığı takdirde temel hak ve özgürlüklere zarar verebilecek yaygın gözetim uygulamalarına başvurulabilir. Çalışmamızın birinci bölümünde de belirtildiği üzere “*kadife eldiven demir yumruğu saklayabilir*” ve kişiler farkında bile olmadan kayıt altına alınan, manipüle edilen camdan nesnelere dönüşebilir. Bu yalnızca Türkiye açısından söz konusu olan bir tehdit değildir. Ancak yukarıda işaret edildiği üzere demokratik devletlerin hemen hemen tamamı bu konuda hukuksal önlemler almıştır ve uygulamadaki sorunları tartışarak daha etkin bir koruma geliştirmeye çalışmaktadır. Oysa Türkiye’de yalnızca bu konuya hasredilmiş bir düzenleme bulunmamaktadır.

Türkiye’de Kişisel Verilerin Korunması Yasası her şeyden önce temel bir insan hakkı olduğu için korunmalıdır. Ancak ne yazık ki Tasarının Türkiye’deki serüvenine bakıldığında haklarına yönelebilecek tehditler dolayısıyla yurttaşların duyduğu kaygıdan değil, uluslararası alanda hissedilen baskı dolayısıyla hazırlıklara başlandığı görülür. Dolayısıyla yalnızca konuya ilişkin bir yasanın kabulü değil, bunun yanında kişisel verilerin korunmasına ilişkin yurttaşların bilinçlendirilmesi de önemli bir gerekliliktir.

İkinci olarak gelişmekte olan elektronik ticaret ve benzeri ekonomik etkinliklerde Türkiye’nin diğer devletlerin gerisinde kalmaması için kişisel verilerin korunmasına yönelik önlemlerin alınması gerekir. Ülkemizde e-ticaret, e-bankacılık gibi etkinliklerin yaygınlaşması isteniyorsa, kullanıcılara hukuksal bir güven ortamı yaratılmalıdır. Bu ortamın iki önemli ayağını ise veri güvenliği ve kişisel verilerin korunması oluşturur. Ayrıca 95/46/AT sayılı Veri Koruma Yönergesinin 25 ve 26. maddeleri uyarınca yeterli düzeyde koruma sağlamayan ülkelere veri aktarımı yasaklandığı için Avrupa pazarında etkinlik gösterebilmek açısından da bu yöndeki bir düzenleme oldukça önemlidir. Nitekim şu anda belirtilen hükümler dolayısıyla çeşitli sorunlar yaşanmaktadır.

Örneğin AK üyesi devletlerden, adli yardım anlaşmalarının uygulanması çerçevesinde, Türk mahkemelerinin adres tespiti, istinabe gibi istemleri Türkiye’nin konuya ilişkin yeterli koruma sağlayan mevzuatı bulunmaması gerekçesiyle reddedilmektedir. Kişisel verilerin korunmasındaki eksiklik ayrıca Türkiye ile AB

üyesi devletlerin gümrük idareleri arasındaki bilgi akışını da olumsuz yönde etkilemektedir³⁰⁶.

Üçüncü olarak bu konudaki bir düzenleme Türkiye'nin AB adaylık süreci açısından da bir gerekliliktir. Türkiye, AB'ye aday adayı³⁰⁷ bir ülke olması nedeniyle mevzuatı uyumlaştırma çalışmalarını uzun süredir gerçekleştirmektedir. Bu doğrultuda her yıl açıklanan ilerleme raporlarında AB'nin kişisel verilerin korunması yasasının eksikliğine işaret ettiği görülmektedir³⁰⁸. 2009 İlerleme Raporunda ise yine kişisel verilerin hukuksal düzenlemeler kapsamında korunması gerekliliğine işaret edilmiştir.

Bütün bu nedenler ve en önemlisi insan haklarına saygılı, çağdaş, demokratik bir devlet olma idealinin gereği olarak, Türkiye'de kişisel verilerin korunması gerekir. Kişisel verilerin korumasız bırakıldığı her geçen gün tehlikenin boyutları artmaktadır. Nitekim teknolojiye hızlı gelişim tehdidin artmasına ve düzenleme yapılması gereksiniminin aciliyet kazanmasına neden olmaktadır³⁰⁹.

³⁰⁶ KVKKT, Genel Gerekeçe.

³⁰⁷ “Avrupa Birliği Müktesebatının Üstlenilmesine İlişkin Türkiye Ulusal Programı” ile “Avrupa Birliği Müktesebatının Üstlenilmesine İlişkin Türkiye Ulusal Programının Uygulanması, Koordinasyonu ve İzlenmesine Dair Karar” Bakanlar Kurulu tarafından kabul edilerek, Resmi Gazete’de yayınlanmıştır. R.G. S. 5. Mükerrer 27097, t. 31 Aralık 2008.

³⁰⁸ Metinde şu ifade yer almaktadır: “*Özel hayata ve aile hayatına saygı ile özellikle kişisel verilerin korunması hakkına ilişkin olarak, Türkiye’nin mevzuatını, başta 95/46/AT sayılı Direktif olmak üzere verilerin korunmasına dair AB müktesebatı ile uyumlaştırması ve bu kapsamda tam bağımsız bir veri koruma denetleme birimi kurması gerekmektedir. Türkiye’nin ayrıca hem Elektronik Ortamda İşlenmesi Bağlamında Bireylerin Korunması Hakkında Avrupa Konseyi Sözleşmesini (CETS No: 108), hem de bu sözleşmenin Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Ek Protokolünü (CETS No: 181) onaylaması gerekmektedir. Telefon görüşmelerinin yaygın olarak dinlendiği belirtilmektedir ve bunların kayıtları basında yer almaktadır*”. Avrupa Toplulukları Komisyonu, Komisyon Tarafından Konseye ve Avrupa Parlamentosuna Sunulan Bildirim, Genişleme Stratejisi ve Başlıca Zorluklar 2009-2010, (COM (2009) 533 final) ekindeki Komisyon Çalışma Belgesi 2009 Yılı Türkiye İlerleme Raporu, Brüksel 14 Kasım 2009, s. 71. Metne ulaşmak için bkz. http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/IlerlemeRaporlari/turkiye_ilerleme_rap_2009.pdf. Nitekim KVKKT’nin Genel Gerekeçesinde de bu yükümlülüğe işaret edildiği, ayrıca OECD ve AK’nin konuya ilişkin düzenlemelerine atıf yapıldığı görülmektedir.

³⁰⁹ Ancak bu konuda bazı karşı görüşlerin de bulunduğu belirtilmelidir. Kimi yazarlara göre teknolojinin doğası gereği bu sorunlar yeni olsa da hepsi yeni yasal düzenlemelerin konusunu oluşturmamaktadır. Bir başka anlatımla, yeni sorunlarla karşılaşmamız mutlaka yeni düzenlemeler yapmamızı gerektirmez. KLEVE ve MULDER bilişim teknolojileri ve hukuk ekseninde konuyu değerlendirmiştir. Yazarlara göre dengeli bir bakış öncelikle yeni sorunun çözümüne hangi alanın uygun olduğunu saptamalıdır. Bundan sonra var olan kurallar değerlendirilebilir. Ardından öğretilerdeki yorumlar dikkate alınarak bu kuralların uygulanabilirliği araştırılır. Ancak bundan sonra eğer sorunun çözümü için mevcut kuralların uygulama olanağının bulunmadığı anlaşılırsa yeni düzenlemelere gidilmesi söz konusu olabilir. Bu noktada ise başka bir sorunun cevaplanması gerekir: Yeni yasal düzenlemelerin yapılması isteği, mevcut yasal düzenlemelerdeki kuralların ve kavramların yeni durumla uyumlamasından mı kaynaklanmaktadır; sosyal gelişimin kendisi ve değişim dolayısıyla mı buna ihtiyaç

Bu açıklamalar ışığında kişisel verilerin korunmasına yönelik kapsayıcı yasal düzenlemelerin yapılmasının bir gereklilik olduğu söylenebilir. O halde ikinci olarak Türkiye’de mevcut düzenlemelerin kişisel verilerin korunması açısından yeterli olup olmadığı değerlendirilmelidir. Yukarıda çizmeye çalıştığımız genel hukuksal tablo dikkate alınarak, yeri geldikçe belirtilen bazı hususlar şu şekilde özetlenebilir:

1. Gelişen teknolojinin ülkemizde yakından izleniyor ve uygulanıyor oluşu son dönemde kişisel verilerin korunmasının daha önemli bir hale gelmesine neden olmuştur. Nitekim gelişen teknoloji temel hak ve özgürlükler açısından pek çok fırsatı sunması yanında kimi durumlarda bunlara yönelik önemli saldırıların kaynağı da olabilmektedir. Teknolojinin bu görünmez yan etkilerini en aza indirebilmek için etkin hukuksal güvenceler tanınmalıdır.
2. Ülkemizde geçmişte ve günümüzde görülen bazı kötü uygulamalar kişisel verilerin hukuksal korumasının ne kadar önemli ve gerekli olduğunun altını çizmektedir.
3. Kişisel verilerin korunmasının Anayasa’da, başta kişinin maddi ve manevi varlığını geliştirme hakkı ile özel yaşamın gizliliği hakkı olmak üzere oldukça sağlam temelleri bulunmaktadır. Son dönemde gündeme gelen anayasa taslak ve önerilerinde bağımsız bir hak olarak yer verilmesi ise geleceğe yönelik umut verici bir işaret olarak değerlendirilebilir. Nitekim böylesine bir düzenleme, Anayasa Mahkemesinin ve diğer yargı organlarının

duyulmaktadır yoksa bunun nedeni bu ilke ve kavramların gerisinde normlar ve değerlerde dönüşüm yaşanması mıdır? Günümüzde içinde bulunduğumuz durumun da bu sonucunu olduğu söylenebilir. Yasama girişimlerinde eğer bu yaklaşım dikkate alınmışsa son yıllarda bilgi teknolojilerinin bir sonucu olarak pek çok yeni yasanın yürürlüğe girmesi biraz şaşırtıcıdır. Bu yeni yasalar, varolan yasaların uygulanması ile sağlanamayacak hiçbir yeni sonuca ulaşamamışlardır. Örneğin elektronik imzayı ele alacak olursak, ıslak imzaya ilişkin düzenlemeler yorumlanarak bunu da kapsam dahiline almak olanaklı olabilirdi. Elektronik imzanın da sonuçta bir imza olduğunu düşündüğümüzde bu yeni düzenlemenin tamamen gereksiz olduğu sonucuna varabiliriz. Örnekler, yazılım ve veri tabanına ilişkin düzenlemeler ve ya da dosya paylaşımı ve spamlere ilişkin olarak da genişletilebilir. KLEVE ve MULDER ayrıca teknoloji, toplumsal gelişmeler ve hukuk arasındaki ilişkiyi şöyle bir sıralamayla açıklamaktadırlar: Teknoloji bazı şeyleri “*yapabilir*”, bunu iş yönetiminin (REMP/business administration) “*istemleri*” izler ve sonuçta yasal düzenlemelere ulaşılır: insanların “*istemleri*” ve “*yapılabilirlikler*”le sınırlanmış bir alan olarak. Pieter KLEVE, Richard De MULDER, “Privacy Protection and The Right to Information: In Search of a New Symbiosis in the Information Age”, **Cyberlaw Security & Privacy**, haz. Sylvia Mercado KIERKEGAARD, The Second International Conference on Legal, Security and Privacy Issues in Information Technology (LSPI) 2007, Beijing, Çin, Ankara Barosu Yayınları, 2. Baskı, Ankara 2007, s. 335-337.

yorumlarını kişisel verilerin korunması yönünde daha açık bir şekilde gelişmesini sağlayacaktır.

4. Kişisel verilerin korunmasına ilişkin mevzuatımızda çeşitli hükümler bulunmaktadır. Son dönemde kabul edilen yeni TCK, CMK gibi temel yasalarda kişisel verilerin korunmasına yönelik ilkelerin benimsendiği görülmektedir. Bunlar, konuya ilişkin sınırlı da olsa bir koruma sağlamaktadır. Ancak mevzuatın çok çeşitli alanlarına dağılmış bu kurallar ülkemizde kişisel verilerin bütüncül korumasında yetersiz kalmaktadır. Ayrıca yürürlükteki düzenlemeler kapsamında getirilen korumanın büyük oranda zararın ortaya çıkmasından sonra uygulanabilir niteliği dikkat çekmektedir. Oysa zarar henüz ortaya çıkmadan kişilerin bu alandaki haklarını güvence altına alacak önleyici korumaya gereksinim duyulmaktadır. Bunun yanında konuya ilişkin temel ilkeler belirlenmeden çeşitli düzenlemelerde tanınan güvencelerin tam anlamıyla uygulanamaması söz konusu olabilir.
5. Çalışmamızın ikinci bölümünde yapılan açıklamalar çerçevesinde görüldüğü üzere uluslararası ve uluslararası örgütler kişisel verilerin korunmasına ilişkin oldukça ayrıntılı sistemler geliştirmektedir. Çağdaş, demokratik bir hukuk devleti olma idealini Anayasasında açıklamış olan Türkiye Cumhuriyeti'nin kişisel verilerin korunması alanındaki boşluğu doldurması gerekir.

İşte bütün bu nedenlerden ötürü kanımızca Türkiye'de kişisel verilerin toplanması, kullanılması ve aktarılmasına ilişkin ilkeleri düzenleyen kapsayıcı bir yasaya gereksinim duyulmaktadır³¹⁰. Nitekim ilgili komisyonun önünde halen beklemekte olan Kişisel Verilerin Korunması Kanun Tasarısının (KVKK) gerekçesinde bu nedenlerin büyük bir bölümüne işaret edildiği görülmektedir³¹¹.

³¹⁰ Konunun önemine yasa koyucu tarafından da işaret edildiği görülmektedir. Nitekim TCK'nın hukuka aykırı olarak "kişisel verilerin kaydedilmesi"nin yaptırımını belirleyen 135. maddenin gerekçesinde şu ifade yer almaktadır: "Çağımızda kişilerle ilgili kayıtların bilgisayar ortamına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alışveriş yapılan mağazaların müşterilerine ilişkin kayıtlar, böylece tutulmaktadır. Bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişi büyük zararlara uğrayabilmektedir".

³¹¹ KVKK Genel Gerekçesinde şu ifadelerin yer aldığı görülmektedir: "Kişisel verilerin korunması, çağımızda, insan hakları kavramı ve korunması bilincinin gittikçe gelişmesine paralel olarak önemini arttırmaktadır. Bu nedenle bir ülkenin mevzuatında değişik düzenlemeler içinde

Ülkemizde kişisel verilerin korunmasına ilişkin bir yasa tasarısı hazırlamak üzere ilk komisyon 13 Eylül 1995'te kurulmuştur. Ancak bu komisyon çalışmalarını tamamlayamamıştır. Daha sonra 2000 yılında oluşturulan ikinci komisyon üç yıllık bir çalışmanın ardından Kişisel Verilerin Korunması Kanun Tasarısını hazırlamıştır. Adalet Bakanlığı tarafından 7 Eylül 2003 tarihinde açıklanan bu Tasarı, AB raporlarında ve e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planlarında konuya ilişkin ifadelerin yer almasına karşın yasalaşmamıştır³¹². Adalet Bakanlığı 2003 yılında hazırlanan bu ilk tasarı üzerindeki çalışmalarını 2008 yılında tamamlamış ve Başbakanlığa iletmıştır³¹³. Aşağıda incelenecek metin Kişisel Verilerin Korunması Kanun Tasarısının 22 Nisan 2008 tarihinde Başbakanlıktan TBMM'ye iletilen son halidir³¹⁴. 2008 yılı Ekim ayından beri Tasarı TBMM Adalet Alt Komisyonunda incelenmektedir³¹⁵.

B. KVKKT'DE BENİMSENEN SİSTEM

Kişisel verilerin korunmasına yönelik ulusal hukuk sistemlerindeki düzenlemeler incelendiğinde bazı farklılıklar bulunduğu görülmektedir. Farklılık

yer alan farklı hükümlerin, bu konuya özgü felsefeden yoksun olması halinde kişisel verilerin korunması konusunda artan ihtiyaca cevap vermesi mümkün olmamaktadır. Bunun öncelikli sebebi, söz konusu hükümlerin başlı başına yetersiz olmalarından ziyade; bu hükümlerin hukuk sisteminde yer almasının, kişisel verilerin korunması amacı ile değil, ancak her bir hükmün ilgili olduğu sahalarda zamanının ihtiyaçlarına cevap vermesi amacı ile düzenlenmiş olmasıdır. Bundan dolayı hemen tüm modern hukuk sistemlerinde olduğu gibi, ülkemizde de kişisel verilerin korunması amacına yönelik münhasır bir kanunun yürürlüğe girmesi kaçınılmaz hale gelmiştir. Tasarı, kişisel verilerin korunması bakımından gerekli olan tüm hususlarda çerçeve niteliğinde ilkeleri belirlemekte ve öngördüğü bağımsız Kurul ile de bu ilkelerin uygulanmasının izlenmesini temin etmektedir”.

³¹² Nilgün BAŞALP, **Kişisel Verilerin Korunması ve Saklanması**, s. 107-108. Kişisel Verilerin Korunması Kanun Tasarısının 2003 yılında kabul edilen ilk şekline ilişkin genel bir değerlendirme için bkz. Ceylin BEYLİ, “Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Üzerine Eleştiriler”, **Bilişim Hukuku**, der. Mete TEVETOĞLU, Kadir Has Üniversitesi Yayınları, İstanbul 2006, s. 70-79.

³¹³ “Kişisel Verilerin Korunması Projesi”, 17 Haziran 2008, http://www.bilgiedinmehakki.org/tr/index.php?option=com_content&task=view&id=83&Itemid=24. Ayrıca belirtmek gerekir: kişisel verilerin korunması yasasını hazırlama görevi Bilgi Toplumu Stratejisi Raporu Eylem Planında (RG. T. 28 Temmuz 2006, S. 26242) yer alan 87 numaralı eylemle Adalet bakanlığına verilmiştir. Belirtilen Planda 2006 yılından başlamak üzere Bakanlığa 9 aylık süre verilmiş olmasına karşın Tasarı halen yasalaşmamıştır. Bkz. aynı yer.

³¹⁴ Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü'nün, B.02.0.KKG.0.10/101-902/1812 sayılı, 22 Nisan 2008 tarihli yazısı ile TBMM'ne iletilmiştir. Bkz. <http://www.tbmm.gov.tr/d23/1/1-0576.pdf>.

³¹⁵ Fikret İLKİZ, “Kişisel Verilerin Korunması ve Kanun Tasarısı”, **Güncel Hukuk**, Y. 2009, S.7-67, s. 12. (12-23)

kimi zaman sistemin bütününden, kimi zaman ise kapsamından kaynaklanır. Kişisel verilerin korunmasına yönelik hukuksal bir düzenleme yapılmasına karar verildiğinde ilk aşamada şu soruların yanıtlanması gerekecektir³¹⁶:

- (i) Kişisel verilerin korunması nasıl olmalıdır? Yalnızca belirli konulara yönelik bir korumaya mı gidilmelidir, yoksa kapsayıcı bir yasal düzenleme mi benimsenmelidir?
- (ii) Korumanın kapsamına hangi veriler girmelidir?
- (iii) Gerçek kişiler yanında tüzel kişiler de korumadan yararlanmalı mıdır?
- (iv) Hangi kesimin elinde bulunan veriler koruma kapsamına alınmalıdır?
- (v) Kişisel verilerin işlenmesinde hangi ilkeler benimsenmelidir?
- (vi) Bağımsız bir denetim organına gereksinim var mıdır?

KVKKT hazırlanırken bu sorulara yanıt aranmış ve verilen cevaplara göre bazı tercihlerde bulunulmuştur. İdeal bir düzenlemeye kavuşabilmek için bu soruları dikkate almak ve Tasarıdaki tercihleri, alternatifleri ile birlikte, değerlendirmek gerekir.

Çeşitli düzenlemeler incelendiğinde şu an için AB sisteminin etkisiyle ağırlığın konuya ilişkin temel ilkeleri belirleyen çerçeve niteliğindeki düzenlemelerde olduğu söylenebilir. Bunun yanında sektörel yaklaşım, kendiliğinden düzenleme ve teknoloji tabanlı düzenlemeler dikkat çeken güvencelerdir. Ancak hemen belirtelim: bir ulusal hukuk sisteminde bu yaklaşımlardan mutlaka yalnızca birinin tercih edilmesi gerekmez. Kişisel verilerin korunması hedefini

³¹⁶ Bu sorular belirlenirken TEZCAN'ın Türkiye'de kişisel verilerin korunmasına yönelik tartışmaların henüz yeni yeni başladığı bir dönemde kaleme alınmış makalesinden yararlanılmıştır. Nitekim TEZCAN 1991 yılında yayınladığı makalesinde bu soruları yedi temel başlık altında toplamıştır. Yazara göre özel yaşamın yeni teknolojiler karşısında korunmasını sağlamak amacıyla bir yasal düzenleme yapıldığında yasa koyucunun özellikle şu sorulara yanıt bulması gerekir: "1. Özel hayatın bilgisayar karşısında korunması nasıl olmalıdır? Sadece belli konularda mı korumaya gidilmelidir (ABD modeli) yoksa topyekün bir düzenlemeye mi gidilmelidir (Fr.F.Alm. modeli)? 2. Denetimin kapsamına hangi veriler girmelidir? 3. Hangi kesim denetim kapsamına alınmalıdır? 4. Gerçek kişiler yanında tüzel kişiler de bu korumadan yararlanmalı mıdır? 5. Hangi verilerin toplanmasına izin verilmelidir? 6. Kişisel nitelikli verilerin denetimi hangi yolla sağlanmalıdır? 7. Denetimin kapsamı ve sınırları ne olmalıdır?" Durmuş TEZCAN, "Bilgisayar Karşısında Özel Hayatın Korunması", **Anayasa Yargısı Dergisi**, Y.1991, C.8, s.387.

gerçekleştirmek üzere, birden fazla yaklaşım birbirini destekler şekilde bir arada bulunabilir.

Nitekim KVKKT’de AB ile uyumlu bir sistemin benimsendiği görülür. Aşağıda kapsamı genel olarak değerlendirilecek Tasarı, çerçeve niteliğinde ilkeler belirlemektedir. Ancak Tasarının Genel Gerekçesinde de belirtildiği üzere burada yer alan ilkeler doğrultusunda çeşitli kuruluşların kendi alanlarındaki gereksinimleri saptayıp bu konuda mevzuatta gereken düzenlemeleri yapıp mesleki davranış kurallarını da bunlara uyarlamaları gerekmektedir. Bir başka anlatımla burada çerçeve bir yasa ile kuralların belirlenmesi, ancak sektörlerin kendi gereksinimlerine uygun özel düzenlemelerle bu güvence sisteminin tamamlanması yaklaşımı kabul edilmiştir³¹⁷. Kanımızca Tasarıda benimsenen bu yaklaşım yerindedir. Nitekim kişisel verilerin korunması ilkelerinin düzenlendiği çerçeve yasa, etkin bir güvence sistemi için ilk adımdır. Böylelikle kişisel verilerin işlendiği her durum için geçerli ilkeler belirlenmiş olacaktır. Bunun yanında konuyu özel sektör açısından değerlendiren çeşitli çalışmalarda böylesine bir yaklaşımın faydaları içerisinde sınır ötesi veri akışını kolaylaştıracağına ve bu nedenle ticari ilişkileri güçlendireceğine de işaret edildiği görülmektedir. Bu yaklaşımın en önemli sakıncası ise oldukça külfetli ve maliyetli olmasıdır³¹⁸.

³¹⁷ Yukarıda da açıklandığı üzere sektörel yaklaşımı benimseyen ülkelerden en bilineni ABD’dir. ABD’de kişisel verilerin korunmasına ilişkin federal düzeyde genel bir yasa bulunmamaktadır. Yukarıda ABD’de AB’nin getirdiği standartları sağlayan bir veri koruma sisteminin bulunmamasının yarattığı sorunlardan ve bunun sonucunda Bağışıklık Sözleşmelerinin kabul edilmesi ile soruna bir çözüm bulunduğu söz etmiştik. Ancak bunun yanında ABD’de kişisel verilerin korunmasına ilişkin çeşitli sektörlere özel düzenlemeler bulunmaktadır. Örneğin video kiralama kayıtlarının gizliliğini ya da mali bilgilerin gizliliğini sağlayan yasalar bulunmaktadır. Bu, devletin soruna minimum müdahalesinin ya da daha olumlu bir ifade şekliyle gerektiği kadar müdahalesinin bir örneği olarak değerlendirilebilir. Ancak bu şekilde yalnızca belirli sektörler ya da belirli teknolojilere ilişkin yasal düzenlemelerin bulunması birkaç açıdan korumanın tam anlamıyla gerçekleşmemesine neden olmaktadır. Bunlarda biri, böylesine bir yaklaşımın her yeni teknoloji için yeni bir yasanın gerekmesinden kaynaklanır. Ayrıca çeşitli sektörler açısından belirlenen farklı kurallar bireylerin hakları konusunda bilinçlenmesini de zorlaştıracaktır. Bunun yanında, yasaların uygulamasını denetleyecek bir organının bulunmaması ise bir başka sorundur. David BANISAR, “Privacy and Data Protection Around the World”, s. 2; **Privacy and Human Rights**, s. 4. Telekomünikasyon, sağlık, finans, sigortacılık, bankacılık gibi sektörler kişisel verilerin korunmasının oldukça önemli olduğu alanları oluşturmaktadır ve kendi nitelikleri dolayısıyla birbirinden çeşitli açılardan farklılaşan gereklilikleri de beraberinde getirirler. Öyleyse sektörel düzenlemeler tek başına kişisel verilerin korunması için yetersiz kalsa da, etkin bir güvence sisteminin kurulması için önemli bir bileşendir. Kapsayıcı çerçeve yasalar, konuya ilişkin genel ilkeleri belirlerken, gerekli alanlarda yapılan sektörel düzenlemeler onun tamamlayıcısı olacaktır.

³¹⁸ Örneğin bkz. **Report on a Model Data Protection Code for the Private Sector**, s. 46.

Kişisel verilerin etkin korunması için genel ve özel yasalarda teknolojiye yeni gelişmelere de uygulanabilecek güvencelere de yer verilmesi gerekir. Nitekim teknoloji son derece dinamik bir alanken, hukuk oldukça statiktir. Hukuksal düzenlemelerin teknolojiye gelişmelerle aynı hızda benimsenmesi beklenemez³¹⁹. O halde temel hak ve özgürlüklerin korunması açısından bir boşluk oluşmaması için ilgili hükümlerin yeni gelişen teknolojiye de uyarlanabilmesi gerekir. “*Teknoloji geçirmez*” ya da “*teknoloji nötr*” olarak adlandırılan bu düzenleme şekli AB veri korunma sisteminin belki de en güçlü yönünü oluşturmaktadır. Tasarıda bu koşulun büyük oranda karşılandığı söylenebilir. Nitekim kişisel verilerin işlenmesi oldukça geniş kapsamlı olarak tanımlanmaktadır. KVKKT uyarınca kişisel verilerin işlenmesi “(k)işisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi veya tasniflenmesi

³¹⁹ Önce yeni bir teknolojinin gelişip buna ilişkin düzenlemelerin sonradan benimsenmesi olayın doğası gereği normaldir. Ancak nadiren de olsa farklı örneklerin görüldüğü belirtilmelidir. Türkiye açısından yakın dönemden verilebilecek bir örnek elektronik imzaya ilişkin hukuksal düzenlemenin, henüz bu teknoloji uygulamaya geçmeden önce yapılmış olmasıdır. Türkiye’de elektronik imzanın hukuksal yapısı ve kullanımı ile elektronik sertifika hizmet sağlayıcıların etkinliklerini düzenleyen 5070 sayılı E-İmza Kanunu 2004 yılında yürürlüğe girmiştir. E-imza, veriyi gönderenin ve alanın kimliğinin kanıtlanmasına olanak tanımaktadır. Bunun sonucunda e-imzalanmış bir belgeyi gönderen, gönderdiğini; alan ise aldığını inkar edemez. Bu niteliğiyle elle atılan, geleneksel, ıslak imzanın sanal ortamdaki karşılığı olduğu söylenebilir. Veri güvenliği açısından oldukça güvenli olan e-imzanın dolaylı da olsa kişisel verilerin korunmasına katkı sağladığı söylenebilir. E-imzanın kapsamı oldukça geniştir. Şöyle ki “*kişilerin elle atmış olduğu imzaların tarayıcıdan geçirilmiş hali olan sayısallaştırılmış imzaları, kişilerin göz retinası, parmak izi ya da ses gibi biyolojik özelliklerinin kaydedilerek kullanıldığı biyometrik yöntemleri içeren elektronik imzaları veya bilginin bütünlüğünü ve tarafların kimliklerinin doğruluğunu sağlayan sayısal imzaları da içermektedir*”. Mesut ORTA, **Elektronik İmza ve Uygulaması**, Seçkin, Ankara 2005, s. 36. Elektronik imzaya ilişkin olarak ayrıca bkz. Leyla KESER BERBER, **İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza**, Yetkin, Ankara 2002; M. H. M. SCHELLEKENS, **Electronic Signature, Authentication Technology from a Legal Perspective**, Asser Press, Hollanda 2004; Volker GRUHN, Vincent WOLFF-MARTING, André KÖHLER, Christian HAASE, Torsten KRESSE, **Elektronische Signaturen in modernen Geschäftsprozessen**, Vieweg, Almanya 2007; Michael CHISSICK, Alistair KELMAN, **Electronic Commerce, Law and Practice**, 3. Baskı, Sweet and Maxwell, Büyük Britanya 2002, s. 167-188; Horst SPEICHERT, **Praxis des It-Rechts, Praktische Rechtsfragen der It-Sicherheit und Internetnutzung**, 2. Baskı, Vieweg + Teuber, Almanya 2008, s. 19-30; Johann BIEZER, Anja MIEDBRANDT, “Die digitale Signatur im elektronischen Rechtsverkehr-Deutsches Signaturgesetz und Entwurf der ‘Europäischen Richtlinie’”, **Handbuch zum Internet-Recht, Electronic Commerce, Informations-, Kommunikations- und Mediendienste**, haz. Detlef KRÖGEL, Marc A. GIMMY, Springer, Almanya 2000, s. 135-166.

*veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen bir işlem veya işlemler bütünü” ifade eder*³²⁰.

Görüldüğü gibi burada sınırlı sayımla bir ifade yer almamaktadır. Dolayısıyla AB veri koruma sistemine uygun şekilde verilerin toplanmasından üçüncü kişilere aktarılmasına kadar her türlü işlem aşağıda incelenecek hükümler çerçevesinde değerlendirilecektir. Burada belirtilen işlemler gerçekleştirilirken kullanılan araca ilişkin bir sınırlandırılma getirilmediğine göre Tasarıda düzenlenen “işleme” etkinliği açısından ilkesel olarak verilerin RFID ya da kapalı devre televizyon sistemleri (CCTV) aracılığıyla toplanması, İnternet ya da başka bir ağ üzerinden aktarılması arasında herhangi bir farklılık bulunmamaktadır. Bu gibi araçlar, kendine özgü yapıları dolayısıyla ayrı düzenlemelere gereksinim gösterse de temel ilkelerin varlığı bu düzenlemeler yapılıncaya kadar bir boşluk oluşmasını önleyecektir.

C. KVKKT’NİN AMACI VE KAPSAMI

KVKKT’nin 1. maddesi uyarınca amacı “*kişisel verilerin işlenmesinde kişinin dokunulmazlığı, maddi ve manevi varlığı ile temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemektir*”. Görüldüğü gibi Tasarının temel hedefi hak ve özgürlüklerin korunmasıdır. Daha önce de işaret edildiği üzere kişisel verilerin korunması yasaları incelendiğinde hedefleri açısından bir çeşitlilik dikkat çeker.

Pek çok ülkede özel yaşamın gizliliği hakkına atıf yapılırken, bazılarında kişilik hakkının korunmasının öne çıkarıldığı görülmektedir. KVKKT’de ise bunlar yerine kişinin dokunulmazlığı, maddi ve manevi varlığı ile temel hak ve özgürlüklerini korumak hedef olarak belirlenmiştir. Kanımızca bu genel çerçeve, kişisel verilerin korunmasının insan hakları ile yakın ilişkisini ortaya koymakta yeterli olduğundan, özel yaşamın gizliliği gibi diğer bazı hakların burada sayılamaması herhangi bir eksiklik yaratmamaktadır. Aksine bu bakış açısı temel bir hak olarak kişisel verilerin korunmasının gelişimine olanak tanıyıcı niteliktedir.

³²⁰ KVKKT m. 3/e.

Bununla birlikte Tasarının 1. maddesinde ya da izleyen diğer hükümlerinde kişisel verilerin korunması “*hakkı*”ndan söz edilmediğini belirtmek gerekir. Oysa kişisel verilerin korunmasının temel bir hak olarak güvence altına alınması, bu bilgilerin keyfi, sınırsız ve hukuka aykırı olarak toplanması ve işlenmesi karşısında bireyi daha sağlam bir koruma altına alacak ve bunun temel bir hak olduğunun anlaşılmasını kolaylaştıracaktır³²¹.

Tasarının amacının temel hak ve özgürlükler olarak belirlenmesi diğer hükümlerin değerlendirilmesi sırasında her zaman göz önünde tutulmalıdır. Bu, ilk olarak yasanın kapsamı açısından önemlidir. Tasarının 2/1 hükmü uyarınca “*(b)u Kanun hükümleri, kişisel verileri işlenen gerçek ve tüzel kişiler ile bu verileri tamamen veya kısmen, otomatik olan veya olmayan yollarla herhangi bir veri kütüğüne dahil olacak şekilde işleyen gerçek ve tüzel kişiler hakkında uygulanır*”. Bunun hükümde belirlenen bir istisnası “*kişisel verilerin gerçek kişiler tarafından sadece kişisel veya birlikte oturanlarla ilgili faaliyetlerine*” ilişkin olarak işlenmesidir³²². Görüldüğü gibi 2. maddede Tasarının uygulama alanı oldukça geniş bir şekilde belirlenmiştir.

Kişisel verilerin korunması yasaları temel olarak kişisel veri ya da bilgilere odaklanmıştır. En genel şekliyle kişisel veri, belirli ya da belirlenebilir bir kişiye ilişkin her türlü bilgiyi ifade eder³²³. Burada ilk olarak tanımda geçen “*kişi*”nin

³²¹ Oğuz ŞİMŞEK, s. 207. Nitekim bu konuda çeşitli sivil toplum kuruluşlarından eleştiri ve önerilerin geldiği görülmektedir. Aralık 2009’da açıklanan bir raporda da “*(k)işisel verilere daha sağlam bir güvence sağlanabilmesi için Tasarının 1. maddesinde kişisel verilerin korunması kavramını temel bir hak olarak açıkça*” düzenleme gerekliliğine işaret edildiği görülmektedir. Sözü geçen rapor, yasa yapma sürecine sivil toplumun katılımını sağlamak amacıyla Başbakanlık, Parlamenter Danışmanları Derneği ve Yasama Derneği, BM Kalkınma Fonunun desteğiyle yürütülen bir proje kapsamında dört pilot ilde (Çorum, Mersin, Bursa ve Mardin) KVKKT müzakere edilmesi sonucunda hazırlanmıştır. Bkz. **Türkiye’de Yasa Yapma Süreçlerine Etkin Sivil Katılım Projesi**, Müzakereci Demokrasiye Doğru, Parlamenter Danışmanları Derneği, Aralık 2009, http://www.tbmmdanismanlari.org/images/proje_raporu_2.pdf, s. 14.

³²² Bu istisna hükmü, 95/46/AT sayılı Veri Koruma Yönergesi ile uyumludur. Bkz. AB Veri Koruma Yönergesi, m. 3/2.

³²³ Ancak bu durumun bazı sorunlar yaratabileceği de kimi yazarlarca dile getirilmektedir. Örneğin AB Veri Koruma Yönerge’sinde kişisel veri içeren profillerin yaratabileceği sorunlara karşı bir koruma bulunmaktadır. Ancak grup profilleri her zaman kişisel veri taşımazlar. Bu durumda AB Yönerge’sinin uygulama alanı dışında kalacaklardır. Bir grup profili, belirli bir gruba ilişkin özelliği ya da özellikler toplamını yansıtır. Bunların bir kısmı, sigara içenlerin ortalama yaşam sürelerinin içmeyenlere göre daha kısa olması gibi, herkesin bildiği bilgileri içerebileceği gibi, bir kısmı da, şehrin belirli bir bölgesinde yaşayanların terörist olma olasılığının daha yüksek olması gibi, tamamen yeni bilgiler de içerebilir. Her ne kadar doğrudan bir kişiyle bağlantı kurulmadan oluşturulan bilgiler olsa da, özellikle hassas veriler olarak adlandırılan etnik köken, dinsel tercihler gibi temellerden hareketle bir ölçüt oluşturulup grup profili çıkartıldığında ayrımcılığa

kapsamında gerçek kişilerin yanında, tüzel kişilerin de yer alıp almadığı incelenmelidir³²⁴. Hemen belirtelim KVKKT’de “*tüzel kişilere ilişkin bütün bilgiler*”in kişisel veri kapsamında değerlendirileceği açıkça belirtilmiştir³²⁵. Oysa Tasarı hazırlanırken örnek alınan 95/46/AT sayılı Veri Koruma Yönergesi yalnızca gerçek kişilerin verilerini koruyan bir düzenlemedir. Konuya ilişkin ulusal ve uluslararası düzenlemelerin büyük bir bölümünde de benzer bir yaklaşım benimsendiği görülmektedir³²⁶.

Peki neden Tasarıda tüzel kişilerin de kapsam dahiline alınması tercih edilmiştir? 2. maddenin gerekçesinde bunun nedeni olarak 95/46/AT sayılı Veri Koruma Yönergesinde yalnızca gerçek kişiler koruma kapsamına alınmışsa da 2002/58 sayılı Yönerge ile tüzel kişilerin de koruma kapsamına alınması ve 2003 yılında yürürlüğe giren İtalyan Veri Koruma Kanununda da benzer bir yaklaşımın benimsenmesi gösterilmiştir. Kanımızca bu tercih birkaç açıdan yanlıştır ve Tasarının bu şekliyle yürürlüğe girmesi durumunda bazı sorulara neden olacaktır.

İlk olarak 2002/58/ AT sayılı Yönergenin çalışmamızın ikinci bölümünde de belirttiğimiz üzere özel bir alanda: telekomünikasyon sektöründe kişisel verilerin korunmasına ilişkin ilkeleri belirleyen bir metin olduğu hatırlanmalıdır. Bu niteliğiyle 95/46/AT sayılı Veri Koruma Yönergesinde belirlenen korumayı güçlendirir ve tamamlar. Ayrıca bu Yönerge açısından söz konusu olan “*tüzel kişiliği haiz abonelerin yasal çıkarlarının korunması*”dır³²⁷. Dolayısıyla kapsamın bu şekilde genişletilmesindeki amaç, abonenin tüzel kişi olması durumunda yasal çıkarlarına zarar gelmesini önlemektir. Kanımızca bu, AB veri koruma sisteminin

ilişkin bazı kaygılar haklı olarak ileri sürülebilir. Ayrıca bu profillerin kamuya açık olması durumunda bazı grupların damgalanması da söz konusu olabilecektir. Bunun yanında grup profillerinin her zaman bir gerçekliği yansıtmayabileceği de unutulmamalıdır. Bart CUSTER, s. 294-297.

³²⁴ Günümüzde çağdaş hukuk sistemlerinin tamamı insanları “*gerçek kişi*” olarak kabul eder. Ayrıntılı bilgi için bkz. Serap HELVACI, **Gerçek Kişiler**, 2. Baskı, Arıkan, İstanbul 2007. “*Tüzel kişi*”ler ise hukuk düzenince kendilerine kişilik tanınmış bazı özellikleri taşıyan ve belirli bir amaca yönelmiş insan ya da mal topluluklarıdır. MK’nın 47. maddesi uyarınca “(1) Başlıbaşına bir varlık olmak üzere örgütlenmiş kişi toplulukları ve belli bir amaca özgülenmiş olan mal toplulukları, kendileri ile ilgili özel hükümler uyarınca tüzel kişilik kazanırlar. (2) Amacı hukuka ve ahlaka aykırı olan kişi ve mal toplulukları tüzel kişilik kazanamaz”. Ayrıca bkz. Rona SEROZAN, **Medeni Hukuk (Genel Bölüm)**, 2. Baskı, Vedat, İstanbul 2008, s. 170-208.

³²⁵ KVKKT’nin 3/ç hükmü uyarınca kişisel veri “(b) *elirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgileri*” ifade eder.

³²⁶ Ulusal düzenlemelere ilişkin olarak bkz. Tablo 4.1.

³²⁷ Özel Yaşamın ve Elektronik İletişimin Korunması Yönergesi, m. 1/2.

bütününde tüzel kişilerin de kapsam dahiline alındığı anlamına gelmez. O halde tüzel kişilerin de koruma kapsamında görülmesinin konuya ilişkin genel eğilime aykırı olduğu söylenebilir.

İkinci ve kanımızca daha önemli olan husus, tüzel kişilerin de Tasarının kapsamına alınmasının kişisel verilerin korunmasının temel felsefesi ile çelişmesidir. Tasarının 1. maddesinde de işaret edildiği üzere amaç insan haklarının korunmasıdır. Nitekim çalışmamızın başından beri tekrar tekrar işaret ettiğimiz üzere kişisel verilerin korunması başta özel yaşamın gizliliği hakkı olmak üzere temel hak ve özgürlüklerde kaynağını bulmaktadır ve bağımsız bir hak alanı olma yolunda gelişmektedir. Bu kapsama tüzel kişilerin de alınması kişisel verilerin korunmasının temel felsefesine aykırı olacağı gibi, korumanın zayıflaması tehlikesini de beraberinde getirecektir. Nitekim korunan alanın bu kadar genişlemesi, hedeften uzaklaşılmasına neden olabilir. Ayrıca tüzel kişilerin belirli bir hedef için kuruldukları ve bu hedefleri doğrultusunda etkinlik gösterdikleri unutulmamalıdır. Dolayısıyla temel kaygıları bu hedefle ilişkilidir. Oysa insan hakları yalnızca insan olmakla kazanılan ve doğuştan geldiği kabul edilen haklar olmaları dolayısıyla farklı bir niteliktedir. Bu noktada Tasarının amacının temel hak ve özgürlüklerin korunması olduğu bir kez daha hatırlanmalıdır.

Son olarak şunu da belirtmek gerekir: tüzel kişilerin verilerinin korunması hukukumuzda başka bir alanın, ticari sırların konusunu oluşturur³²⁸. İlgili düzenlemelerde tüzel kişilere ilişkin korunan bilgiler “gizli” olanlardır. Nitekim ticari sır kavramı da gizlilik unsurunu içerir³²⁹. Bunun öncelikli nedeni tüzel kişilerde esas olanın şeffaflık olmasıdır. Ancak bazı durumlarda gizlilik gerekebileceği için çeşitli düzenlemelerde “sır” niteliğindeki bilgilerin korunması öngörülmüştür. Oysa gerçek kişilere ilişkin bilgiler açısından tamamen aksi bir durum söz konusudur. Daha önce de açıkladığımız üzere özel yaşamın kapsamı, kişilerin giz alanından çok daha geniştir. Dolayısıyla gerçek kişilere ilişkin bilgiler tüzel kişilere ilişkin olandan çok daha geniş bir alanda koruma gerektirir.

³²⁸ Yukarıda da işaret edildiği gibi konuya ilişkin çeşitli düzenlemeler bulunmakla birlikte, özel olarak bu konuya hasredilmiş “*Ticari Sır, Banka Sırrı, Müşteri Sırrı Hakkında Kanun Tasarısı*” da ilgili komisyonda görüşülmektedir.

³²⁹ Ticari sır genel olarak “*bağımsız bir değeri olan veya iktisadi faaliyetlerde sahibi lehine bir rekabet avantajı sağlayan, aleni olmayan (sadece sınırlı bir çevrede bilinen) ve sahibinin gizli kalmasını istediği her türlü bilgi*” olarak tanımlanabilir. Mehmet Emin BİLGE, s. 5.

Unutulmamalıdır: kişisel veri, bir (gerçek) kişiyi belirlenebilir kılan her türlü bilgidir. Eğer tüzel kişilere ilişkin veriler içerisinde böyle bir bilgi yer alıyorsa elbette kişisel verilerin korunması kapsamında değerlendirilecektir. Ancak eğer bir kişiyle ilişki kurulmaksızın yalnızca tüzel kişilikle ilgiliyse kişisel verilerin korunması kapsamında olmamalıdır³³⁰. Nitekim bu türdeki bilgiler ticaret kanunları ve ilgili diğer metinlerde korunmaktadır. O halde Kişisel Verilerin Korunması Kanun Tasarısının kapsamında tüzel kişilerin de alınmasının yerinde olmadığını belirtmek gerekir. Nitekim öğretilerdeki baskın görüş de bu yöndedir³³¹.

Buna karşın, Tasarıda veri işleme türü ve hükümlerin uygulanacağı alan bakımından herhangi bir ayırım öngörülmemesi olumludur. Nitekim otomatik yolla işlenen veriler yanında elle işlenen kişisel veriler Tasarıdaki güvenceler kapsamında olduğu gibi bu işlemin kamu sektörü ya da özel sektör tarafından yapılması arasında da bir ayırım öngörülmemiştir. Bu yaklaşım, konuya ilişkin dünyadaki genel eğilime de uygundur(Örneğin bkz. Tablo 4.1.'de yer alan düzenlemeler).

Kişisel verilerin korunmasına ilişkin ulusal ve uluslar arası düzenlemeler incelendiğinde otomatik yolla devlet kurum ve kuruluşları tarafından işlenen verilerin neredeyse her zaman koruma kapsamında olduğu görülür. Örneğin AK Sözleşmesinde korumanın geçerli olması için verilerin, en azından kısmen, otomatik yollarla işlenmesi koşulunu aramıştır. Bu, birinci bölümde incelendiği üzere kişisel verilerin korunması gerekliliğinin teknolojiye gelişmeyle artmasından kaynaklanır. Ancak sınırlı bazı konular dışında her iki tür işlemeden kaynaklı sorunlar aynıdır. Dijital ortamda veriler daha hızlı, daha kolay ilişkilendirilebilir ve aktarılabilir, ancak bu, tozlu raflardaki dosyalarda yer alan bilgilerin kullanımının kişisel verilerin korunması hakkının ihlali olmayacağı anlamına gelemez. Bunun yanında yine çalışmamızın birinci bölümünde açıklandığı üzere kişisel verilerin korunması ilk

³³⁰ Benzer bir değerlendirmeyi BİLGE, ticari sır ve kişilik hakkı ekseninde yapmıştır. Yazara göre: “ticari sırların, işletmeyle ilgili olup da başkalarınca bilinmeyen her türlü bilgiyi kapsayan oldukça geniş kapsamı nedeniyle, tüm ticari sır bilgilerinin bir şahsiyet hakkı olduğu ve tüm ticari sırlara yapılacak saldırıların kişilik haklarına yapılmış bir saldırı anlamı taşıdığı ileri sürülemez. Bununla birlikte, ticari sırlar arasında kişinin iktisadi yaşamına ve özgürlüğüne müdahale anlamına gelecek sırların ihlali, kişilik hakkının da ihlali olacaktır. Dolayısıyla, bazı durumlarda ticari sırların açıklanması kişilik haklarının da ihlali anlamına gelebilir”. Mehmet Emin BİLGE, s. 41-42.

³³¹ Aynı yönde bkz. Oğuz ŞİMŞEK, s. 207. Aslı E. GÜRBÜZ USLU, **Türk Özel Hukukunda Özellikle Anonim Şirketlerde Ticari Sırrın Korunması**, Vedat, İstanbul 2009, s. 48-49, d.n. 160; Durmuş TEZCAN, “Bilgisayar Karşısında Özel Hayatın Korunması”, **Anayasa Yargısı**, 1991, s. 389. Karşı görüş için bkz. Nilgün BAŞALP, s. 109.

ařamada doęal olarak devlete karřı gelişmektedir. Ancak kamu kurum ve kuruluşları yanında özel sektörden yönelen tehditler de her geçen gün biraz daha artmaktadır. Dolayısıyla Tasarıda kamu sektörü yanında özel sektör tarafından işlenen verilerin de koruma kapsamında görülmesinin olumlu bir yaklaşım olduğunu belirtmek gerekir. Nitekim pek çok ulusal hukuk sisteminde de verilerin kimin tarafından işlendięi konusunda ya da hangi yöntemle işlendięine ilişkin bir ayırım öngörülmeden bütüncül bir korumanın benimsendięi görülmektedir (Bkz. Tablo 4.1.)

Tablo 4.1. Mevzuatında Kişisel Verilerin Korunmasına Yönelik Özel Düzenleme Bulunan Bazı Devletlerde Bu Düzenlemelerin Kapsamı

DEVLET	ELLE İŞLEME	TÜZEL KİŞİLER	ÖZEL SEKTÖR
Almanya	x		x
Arjantin	x		x
Avustralya	x		x
Avusturya	x	x	x
Belçika	x		x
Birleşik Krallık	x		x
Bosna-Hersek			x
Bulgaristan	x	x	x
Çek Cumhuriyeti	x		x
Danimarka	x	bazı	x
Finlandiya	x		x
Fransa	x	x (3 Temmuz 1984 tarihli CNIL'in idari kararı ile)	x
Güney Kore			
Hırvatistan	x		x
Hong Kong			x
İrlanda			x
İspanya	x		x
İsveç	x		x
İsviçre	x	x	x
İtalya	x	x	x
Japonya			
Kanada	x		
Maceristan	x		x
Norveç	x		x
Peru	x		x
Portekiz	x		x
Şili	x	x	x
Yunanistan	x		x

Kaynak: http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents.

Aşağıda yer alan devletlerin tamamının iç hukukunda kişisel verilerin korunmasına yönelik bir ya da birden fazla özel düzenleme bulunmaktadır. Bu düzenlemelerin hepsinde otomatik yolla işlenen veriler, gerçek kişilere ilişkin veriler ve kamu sektöründe işlenen veriler düzenleme kapsamındadır. Farklılık aşağıdaki tabloda görüldüğü üzere elle işleme, tüzel kişiler ve özel sektörün koruma kapsamında olup olmamasında görülmektedir.

D. KVKK'TE BENİMSENEN TEMEL İLKELER

KVKK'Te temel ilkelerin bütün alanları kapsayacak şekilde belirlendiği görülür. İlgili hükümler incelendiğinde burada yer alan ilkelerin saptanmasında büyük oranda 95/46/AT sayılı Veri Koruma Yönergesinden yararlanıldığı görülmektedir. Nitekim Tasarının Gerekçesinde de bu düzenlemenin AB ile mevzuat uyum çalışmalarında önemli bir gereksinimi karşılayacağına işaret edilmiştir. Tasarıda çalışmaların üçüncü bölümünde incelenen kişisel verilerin korunmasında temel ilkelerin büyük bölümüne yer verildiği söylenebilir. Ancak Tasarı yasalaşmadan düzeltilmesi gereken bazı önemli sorunların bulunduğu da belirtilmelidir.

1. Kişisel Verilerin Niteliğine İlişkin İlkeler

Daha önce de işaret edildiği üzere, hukuka ve dürüstlük kurallarına uygun işleme, belirli, açık ve meşru amaçlar için toplanma, doğru ve güncel olma gibi verilerin işlenmesinin bazı nitelikleri karşılaması gerekir. Pek çok metinde kabul edilen bu ilke, kişisel verilerin korunması açısından merkezi öneme sahiptir³³². “*Verilerin kaliteli olması gerekliliği*” olarak da ifade edilebilecek bu ilke, KVKK açısından 4 vd. maddeleri çerçevesinde değerlendirilmelidir.

Tasarının 4. maddesi uyarınca kişisel verilerin işlenebilmesi için yasal bir dayanağının olması zorunludur³³³. Hemen belirtelim: kişisel verilerin korunması temel haklar kapsamında kabul edildiğine göre, Anayasanın 13. maddesinin hükmü uyarınca bu alandaki sınırlamalar zaten yalnızca yasa ile belirlenebilir. Ancak henüz Anayasamızda kişisel verilerin korunmasının bağımsız bir hak alanı olarak düzenlenmediği ve Tasarıda da “*kişisel verilerin korunması hakkı*” ifadesine yer verilmediği düşünüldüğünde 4. maddede ancak yasa ile işlenebilme koşuluna vurgu yapılmasının gerekli ve yerinde olduğu söylenebilir.

³³² AB Veri Koruma Yönergesi, m. 6, AK Veri Koruma Sözleşmesi m. 5, BM Rehber İlkeleri 1. İlke, OECD Rehber İlkeleri par. 7, APEC Çerçeve Belge par. 18.

³³³ KVKK 4. maddesi şöyledir: “*Kişisel veriler, ancak, bu Kanunda ve diğer kanunlarda öngörülen hallerde işlenebilir*”. İlginç olan bir nokta Tasarının kapsamında ya da belirtilen 4. madde hükmünde kamu ile özel sektör arasında bir ayrım öngörülmemiş olmasına karşın 4. maddenin gerekçesinde yalnızca kamu kurum ve kuruluşlarının kişisel verileri işleyebilmesinin yasayla öngörülen hallerle sınırlandırılmasından söz edilmiş olmasıdır.

Tasarının 5. maddesinde “*kişisel verilerin işlenmesine ilişkin ilkeler*”, 6. maddesinde ise “*hukuka uygunluk sebepleri*” düzenlenmiştir. KVKKKT’nin 5/1 hükmü ile çalışmamızın üçüncü bölümünde incelenen temel ilkelerin büyük oranda karşılandığı söylenebilir³³⁴. Burada belirlenen ilkeler bütün veri işleme etkinliklerinde dikkate alınacaktır. Bu nedenle Tasarının diğer hükümleri yorumlanırken de bunların göz ardı edilmemesi gerekir. Ayrıca kişisel verilerin, kamunun yararlanmasına açık olduğu veya ilgili kişinin veri işlenmesine itirazının bulunmadığı durumlarda bile bu fıkra da belirlenen koşulların varlığının aranacağı dikkatten kaçmamalıdır³³⁵.

Daha önce yukarıda Türk hukuk mevzuatında kişisel verilerin korunmasına ilişkin hükümleri değerlendirirken kişisel verilerin işlenmesinde geçerli olacak temel ilkelerin belirlenmemesinin önemli bir eksiklik olacağından söz etmiştik. Bu eksiklik, Tasarı yasalaşırsa büyük oranda giderilmiş olacaktır. Örneğin TCK’nın 135 vd. hükümlerinde yer alan suçlara ilişkin bazı belirsizlikler bu şekilde önemli oranda giderilmiş olacaktır. Belirli, somut bir amaç olmaksızın “*bir gün gerekli olursa*” düşüncesi ile kişisel verilerin toplanması da bu hüküm ile yasaklandığından fişleme ve benzeri etkinliklerin engellenmesi açısından da bu hükmün yararlı sonuçlar vereceği söylenebilir³³⁶.

³³⁴ KVKKKT’nin 5. maddesi uyarınca “(1)Kişisel verilerin; (a) Hukuka ve dürüstlük kurallarına uygun işlenmesi, (b) Belirli, açık ve meşru amaçlar için toplanması ve bu amaçlara aykırı olarak yeniden işlenmemesi, (c) Toplandıkları amaçla bağlantılı, yeterli, orantılı olması, (ç) Doğru olması ve gerektiğinde güncellenmesi, (d) İlgili kişilerin kimliklerini belirtecek biçimde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar muhafaza edilmesi zorunludur. (2) Kişisel veriler, ilgili mevzuatta yeniden işleme amacına yönelik yeterli koruma tedbirleri getiren düzenlemenin bulunması veya kişisel verileri kontrol eden tarafından bu yönde gerekli tedbirlerin alınması şartıyla tarihi, istatistiki veya bilimsel amaçlarla yeniden işlenebilir veya birinci fıkranın (d) bendinde öngörülenden daha uzun bir süre saklanabilir”. Tasarının 5/1,a hükmünde yer alan kişisel verilerin “hukuka ve dürüstlük kurallarına uygun olarak işlenmesi” ifadesinin, yalnızca “işlenmeyi” kapsadığı oysa “elde edilmesi” açısından da bu korumanın gerekli olduğu yönünde eleştirildiği görülmektedir. Örneğin bkz. Fikret İLKİZ, s. 15; **Türkiye’de Yasa Yapma Süreçlerine Etkin Sivil Katılım Projesi**, s. 11. Oysa konuya ilişkin uluslararası düzenlemelere uygun olarak Tasarının tanımlara ilişkin 3/a hükmünde de belirtildiği gibi “işleme” “kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi”ni de kapsayan işlem ya da işlemler bütünü ifade eder. Dolayısıyla işleminin hukuka ve dürüstlük kurallarına uygun olması zorunluluğu, elde edilmesi de dahil veri üzerindeki bütün işlemleri kapsamaktadır.

³³⁵ KVKKKT 5. madde, Gerekeçe.

³³⁶ Nitekim Tasarının 5/c hükmünde yer alan kişisel verilerin “(b)elirli, açık ve meşru amaçlar için toplanması ve bu amaçlara aykırı olarak yeniden işlenmemesi” hükmü nün gerekçesinde bu ilke ile “olası kullanıma olanak yaratılması için verilerin toplanması”nın yasaklandığı açıkça belirtilmektedir.

Tasarının 6/1 hükmü uyarınca kişisel veriler, yalnızca ilgili kişinin açık rızasının bulunması halinde işlenebilir. Bu hüküm, kişilerin kendilerine ilişkin “bilgilerin geleceğini belirleme hakkı”nın açık bir yansımasıdır³³⁷. Buna karşın yasayla öngörülen yükümlülüklerin yerine getirilmesi dışında ilgili kişinin itirazda bulunması durumunda veriler işlenemez³³⁸. Ancak kişisel verilerin korunmasının insan hakları kapsamında değerlendirildiği dikkatten kaçmamalıdır. Bu nedenle kişisel verilerin işlenmemesinin kural, işlenmesinin ise istisna olması gerekir³³⁹. Hükümde yer alan ilkenin “(y)asayla öngörülen yükümlülüklerin yerine getirilmesi dışında, ilgili kişinin rıza göstermemesi halinde veri işlenemez” şeklinde düzenlenmesi bu sorunun giderilmesini sağlayacaktır.

Tasarının 6/3 hükmünde yer alan hukuka uygunluk sebeplerinin büyük oranda 95/46/AT sayılı Veri Koruma Yönergesi ile uyumlu olduğu görülmektedir³⁴⁰. Ancak diğer bütün insan hak ve özgürlükleri açısından söz konusu olduğu gibi burada da sınırlamaların dar yorumlanması gerektiği unutulmamalıdır. Bu temel kurala uyulmadığı takdirde Anayasanın 13. maddesine aykırı olarak hakkın özüne dokunacak, onun tanınmasını anlamsız kılacak ölçüde geniş sınırlamalara gidilebilir.

Bunun yanında kişisel verilerin korunmasının anayasal temelleri düşünüldüğünde kimi durumlarda yapılacak herhangi bir sınırlama ciddi sorunlara neden olabilir. Yukarıda işaret edildiği üzere, arama, el koyma, konut dokunulmazlığı ve haberleşmenin gizliliği dışında özel yaşamın gizliliği hakkı Anayasamızda mutlak olarak korunmaktadır. Yine kişisel verilerin korunmasının anayasal temellerini oluşturan kişinin maddi ve manevi varlığını geliştirme hakkı, kimi durumlarda düşünce özgürlüğü, mutlak olarak korunan alanları oluşturur. Bu,

³³⁷ Hükümün gerekçesinde rızaya ilişkin olarak 95/46/AT sayılı Veri Koruma Yönergesine atıf yapılmıştır. Bu nedenle hükmün yorumunda Yönergenin ilgili hükmünün dikkate alınması gerekecektir.

³³⁸ KVKK m. 6/2.

³³⁹ Aynı yönde bkz. Fikret İLKİZ, “Kişisel Verilerin Korunması ve Kanun Tasarısı”, s. 16; Oğuz ŞİMŞEK, s. 208.

³⁴⁰ KVKK’nın 6/3 hükmü şöyledir: “Aşağıdaki hallerde de hukuka uygunluk sebeplerinin bulunduğu kabul edilir: (a) Kanunun öngördüğü bir zorunluluk dolayısıyla, kamu yararına veya resmi olarak verilmiş bir görevin yerine getirilmesi amacıyla veri işlenmesi, (b) Kişisel verilerin, ilgili kişinin rızasını açıklayamayacak durumda olması halinde kendisinin veya başkasının hayatını veya beden dokunulmazlığını korumak amacıyla işlenmesi, (c) Bir sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesi, (ç) İlgili kişiler tarafından açıklanmış olması veya açık sicillerde mevcut bilgiler olması sebebiyle herkesçe bilinen kişisel verilerin işlenmesi, (d) Veri kütüğü sahibinin kendi haklı çıkarları için, ilgili kişinin temel hak ve özgürlükleri ile meşru çıkarlarına zarar vermediği sürece, veri işleminin zorunlu olması”.

kişisel verilerin korunması kapsamında değerlendirilen pek çok konunun Anayasada mutlak olarak korunduğu sonucunu getirir. O halde kişisel verilerin işlendiği kimi durumlarda belirtilen koşullara uygun hareket edilse bile Anayasaya aykırılık sorunu ile karşılaşılması söz konusu olabilir. Yine yukarıda da belirtildiği gibi çeşitli Anayasa taslak ve önerilerinde yer aldığı kişisel verilerin korunmasının Anayasada ayrı bir hüküm altında düzenlenmesi bu ve benzeri sorunların giderilmesini sağlayacaktır.

Kişisel verilerin bazı alanlarda kullanımına ilişkin de özel istisnalar getirildiği görülmektedir. Tasarının 5/2 hükmü uyarınca yeterli korumanın sağlanması şartıyla kişisel veriler tarihsel, istatistiksel ya da bilimsel amaçlarla yeniden işlenebileceği gibi, kaydedildikleri amaçtan daha uzun süre muhafaza edilebilirler. Bu noktada verilerin yeniden işlendikleri durumlarda da temel ilkelere uyulacağı ve verilerin tutulma sürelerinin bu kez de belirtilen istisna kapsamındaki amaçların gerçekleşmesi ile sınırlı olacağı unutulmamalıdır. Tarihsel, istatistiksel ya da bilimsel araştırmaların gerçekleştirilebilmesi için verilerin mutlaka bir kişiyle ilişkili olarak tutulması gerekmiyor ise anonimleştirilmeleri gerekir. Nitekim KVKKT’de de artık gereksinim duyulmayan verilerin anonim hale getirileceği veya yok edileceği düzenlenmiştir³⁴¹.

Burada ilginç olan Tasarının 10. maddesinde kişisel verilerin “*araştırma, planlama ve istatistik gibi amaçlarla*” anonim hale getirilmeleri şartıyla işlenebileceklerinin düzenlenmiş olmasıdır. Aynı alana ilişkin iki hüküm arasında verilerin belirtilen amaçlarla işlenmesinde uyulacak esaslar açısından çatışma doğabilir³⁴². Bu nedenle kanımızca Tasarının 5/2 hükmü ile 10. maddesi bir arada tek

³⁴¹ KVKKT’nin 9. maddesi şu hükmü içerir: “(1) İhtiyaç duyulmayan kişisel veriler, koruma tedbiri veya ispat amacıyla muhafazasının gerekli olmadığı durumlarda, anonim hale getirilir veya yok edilir. (2) Verilerin anonim hale getirilmesi veya yok edilmesine ilişkin usul ve esaslar Kurulca, ilgili kamu kurum ve kuruluşları ile diğer özel hukuk tüzel kişilerinin görüşleri alınarak hazırlanan yönetmelikte gösterilir”.

³⁴² KVKKT’nin 5/2 hükmü şöyledir: “Kişisel veriler, ilgili mevzuatta yeniden işleme amacına yönelik yeterli koruma tedbirleri getiren düzenlemenin bulunması veya kişisel verileri kontrol eden tarafından bu yönde gerekli tedbirlerin alınması şartıyla tarihi, istatistiki veya bilimsel amaçlarla yeniden işlenebilir veya birinci fıkranın (d) bendinde öngörülenden daha uzun bir süre saklanabilir”. Tasarının 10. maddesi ise şu hükmü içermektedir: “Kişisel veriler, araştırma, planlama ve istatistik gibi amaçlarla anonim hale getirilmesi kaydıyla işlenebilir. Bu suretle elde edilen veriler ve sonuçlar üçüncü kişilere aktarılabilir veya yayımlanabilir”. Bu noktada dikkat çekilmesi gereken bir diğer husus, maddenin gerekçesinde bu hükmün hukuka uygunluk sebeplerinden biri olduğunun belirtilmesidir. Daha önce de belirtildiği üzere anonim veriler belirli ya da belirlenebilir bir kişiyle ilişki kurulmasına izin vermediği için zaten kişisel verilerin korunması kapsamında değildir. O halde önemli olan bu verilerin tam anlamıyla anonim şekle dönüştürülmesidir. Nitekim yine daha önce belirttiğimiz gibi takma adlaştırma ile anonimleştirme

bir hüküm altında yeniden düzenlenmelidir. Bunun yanında ilgili kişinin aşağıda incelenecek bilgilere erişim, sildirme, düzeltme, engelleme gibi Tasarının 12. maddesinde düzenlenen hakları ise “*kişisel verilerin özellikle belirli bir kişiye ilişkin tedbir veya karar alınmasına yönelik kullanılmadığı ve ilgili kişinin özel yaşamının gizliliğinin ihlal edilmesi riskinin bulunmadığı hallerde, ilgili mevzuatta yeterli koruma tedbiri bulunması kaydıyla, bilimsel araştırma veya istatistik oluşturma amaçları ile sınırlanabilir*”³⁴³.

2. Özel Nitelikteki Kişisel Verilerin Nitelikli Korunması İlkesi

Kişisel verilerin korunmasında Avrupa sistemine uygun olarak Tasarının 7. maddesinde “*özel niteliği olan kişisel veriler*” açısından ayrı bir düzenleme öngörülmüştür. Buna göre “*(k)işilerin ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkûmiyetleri ile ilgili kişisel verileri işlenemez*”³⁴⁴. Üçüncü bölümde yaptığımız açıklamalardan hatırlanacağı üzere konuya ilişkin pek çok düzenlemede bazı bilgi türleri, diğerlerine göre daha hassas nitelikte olmaları dolayısıyla daha güçlü bir şekilde korunmaktadır³⁴⁵. Başta 95/46/AT sayılı Veri Koruma Yönergesi olmak üzere bu yaklaşımı benimseyen düzenlemelerden hareketle Tasarıda da bazı bilgi türlerinin ayrı bir koruma rejimine tabi olması tercih edilmiştir. Ancak önemli bazı farklılıklar bulunduğu dikkatten kaçmamalıdır (Bkz. Tablo 4.2).

Öncelikle 95/46/AT sayılı Veri Koruma Yönergesinde kişilerin cinsel yaşamları da özel nitelikte kişisel veriler arasında sayılırken Tasarı kapsamına alınmaması dikkat çekicidir. Nitekim bir kişinin cinsel yaşamı özel alanın çekirdeğinde yer alır. Cinsel yaşama ilişkin bilgilerin, hükümde yer alan “*özel yaşamları ... ile ilgili kişisel veriler*” kapsamında korunacağı düşünülebilir³⁴⁶. Ancak bu ifade bazı sorunlara neden olabilir. Nitekim özel yaşam, yalnızca mahrem alanı değil, kişisel verileri ve hatta kimi zaman ilgili kişinin kamusal alandaki

farklı kavramlardır. Veriler anonimleştirildikten sonra ayrık hukuka uygunluk nedenine gereksinim göstermeksizin aktarılabilecektir.

³⁴³ KVKKT m. 22/2.

³⁴⁴ KVKKT m. 7/1.

³⁴⁵ Tasarının 7/1 hükmünün gerekçesinde de şu ifade yer alır: “*Bu veriler, başkalarının öğrenilmeleri halinde özellikleri gereği ilgili kişinin mağduriyetine yol açabilecek ve ayrımcılık tehlikesini oluşturacak nitelikte hassas verilerdir. Özel nitelikteki verilere dolaylı da olsa erişim imkanı veren veriler de madde kapsamında yerini almalıdır*”.

³⁴⁶ Oğuz ŞİMŞEK, s. 209.

etkinliklerini de kapsayan oldukça geniş bir kavramdır. Bu nedenle özel nitelikteki kişisel veriler arasında sayılması doğru değildir³⁴⁷. Her şeyden önce böylesine bir yaklaşım istisnaların sınırlarının genişletilmesine neden olacaktır. Nitekim “*özel yaşam*” kavramı, kişisel verilerin hemen hemen tamamını kapsadığından bazı veri türlerinin daha sağlam güvencelerle korunmasını olanaksız kılacaktır³⁴⁸. Bu nedenle hükümden “*özel yaşam*” ifadesinin çıkartılıp bunun “*cinsel yaşam*” ile değiştirilmesi daha uygun olacaktır³⁴⁹.

³⁴⁷ Aynı yönde bkz. **Kişisel Verilerin Korunması**, Türkiye Bilişim Derneği Kamu-BİB, 2. Çalışma Grubu, Nisan 2008, http://www.tbd.org.tr/resimler/ekler/8f0b864598a1291_ek.pdf, s. 76.

³⁴⁸ Bu noktada bazı veri türlerinin özel olarak korunması yaklaşımının çeşitli açılardan tartışıldığını hatırlatmak gerekir. Bu konuya ilişkin görüş ve değerlendirmelerimiz için bkz. Üçüncü bölüm, “Özel Kategorideki (Hassas) Kişisel Verilerin Nitelikli Korunması” başlığı.

³⁴⁹ Belirtilen hükme “*genetik bilgiler*” ve “*cinsiyete ait veriler*”in eklenmesi yönünde önerilerin bulunduğu da görülmektedir. Bkz. **Türkiye’de Yasa Yapma Süreçlerine Etkin Sivil Katılım Projesi**, s. 12. Kanımızca “*genetik bilgiler*”in ayrıca belirtilmesinin önünde bir sakınca bulunmamakla beraber, bu vurgu mutlaka gerekli değildir. Nitekim genetik bilgilerin sağlık verileri içerisinde evleviyetle korunacağı kabul edilmelidir. Buna karşın “*cinsiyete ait veriler*”in hassas veriler kapsamında yer alması bazı sorunlara neden olabilir. Nitekim cinsiyete ait veriler ile ne kastedildiği tam olarak açık değildir. Eğer burada kişinin cinsiyetinin ne olduğu bilgisi kastediliyorsa bu, kişinin adı, adresi, telefon numarası gibi diğer bilgilerle beraber korunabilir. Ayrıca özel nitelikte kişisel veriler kapsamına alınmasına gerek bulunmamaktadır. Eğer bunun yanında cinsiyet değişikliği ya da cinsel tercihlere ilişkin bilgiler de kastediliyorsa, kanımızca bu türdeki bilgilerin kişilerin “cinsel yaşamları” kapsamında korunması daha doğru olacaktır.

Tablo 4.2. Çeşitli düzenlemelerde hassas kişisel verilerin kapsamı

KVKKT (m. 7)	TCK (m. 135)	Belçika Veri Koruma Yasası (m. 6)	Fransa Veri Koruma Yasası (m. 8)	Almanya Veri Koruma Yasası (m.3/9, 4d/5, 28/6)	95/46/AT sayılı Veri Koruma Yönergesi (m. 8)	108 sayılı AK Sözleşmesi (m. 6)
İrk	İrki köken	İrksal ya da etnik köken	İrksal ya da etnik köken	İrksal ya da etnik köken	İrksal veya etnik köken	İrksal köken
Siyasal düşünce	Siyasal görüş	Siyasal görüş	Siyasal görüş	Siyasal görüş	Siyasal görüş	Siyasal görüş
Felsefi inanç	Felsefi görüş	Felsefi inanç	Felsefi görüş	Felsefi inanç	Felsefi inanç	
Din, mezhep veya diğer inançlar	Dini görüş	Dinsel inanç	Dinsel görüş	Dinsel inanç	Dinsel inanç	Dinsel ya da diğer inançlar
Dernek, vakıf ve sendika üyeliği	Sendikal Bağlantılar	Sendika üyeliği	Sendika üyeliği	Sendika üyeliği	Sendika üyeliği	
Sağlık	Sağlık durumları	Sağlık	Sağlık	Sağlık	Sağlık	Sağlık
Özel yaşam						
Her türlü mahkumiyet					Ceza mahkumiyeti	Ceza mahkumiyeti
	Cinsel yaşam	Cinsel yaşam	Cinsel yaşam	Cinsel yaşam	Cinsel yaşam	Cinsel yaşam
	Ahlaki eğilim					

Aşağıdaki tablo özel nitelikteki (hassas) kişisel verilere ilişkin çeşitli hukuksal metinlerdeki tanımların kapsamına ilişkin bir karşılaştırma sunmaktadır. Belçika, Almanya ve Fransa Veri Koruma Yasalarına ilişkin bilgilerde AK'nin resmi İnternet sitesinde bağlantı verilen İngilizce metinlerinden yararlanılmıştır. Bkz. http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/national%20laws/1NATIONALLAWS_en.asp#TopOfPage.

Özel nitelikteki kişisel verilerin işlenme yasağına Tasarının 7/2 hükmü ile *“özel hayatın ve aile hayatının gizliliğinin korunmasını sağlayacak yeterli önlemlerin alınması şartıyla”* bazı istisnalar getirilmiştir. Bu hükümdeki istisnalar, oldukça geniş kapsamlı olmakla birlikte büyük oranda AT Veri Koruma Yönergesi ile uyumludur³⁵⁰. Ancak belirtmek gerekir: Tasarının özellikle 7/3 hükmünün dikkatle yorumlanmalıdır. Belirtilen hüküm uyarınca *“(ö)zel hayatın ve aile hayatının gizliliğine dokunmamak şartıyla, temel kamu yararlarının gerektirmesi halinde, ilgili mevzuatta yeterli koruma bulunması kaydıyla, (Kişisel Verilerin Korunması)Kurul(u), özel niteliği olan kişisel verilerin işlenmesine karar verebilir”*.

Özel ve aile yaşamının korunması, kamu yararının gerektirmesi, ilgili mevzuatta yeterli korumanın bulunması koşulları getirilmiş olmakla birlikte Kurula verilen bu yetkinin geniş tutulması özel nitelikteki kişisel verilerin korunma alanını neredeyse yok etmek anlamına gelir. Bu noktada *“kamu yararı”* kavramının belirsizliği, neyin *“yeterli koruma”* sağlayacağını da açık olmadığı düşünüldüğünde bu hüküm ile hassas kişisel verilerin keyfi işlenmesinin önüne geçildiğini söyleyebilmek hayli güç olacaktır. Bu noktada özel niteliği olan kişisel verilerin işlenmesine karar verecek Kurulun niteliği de dikkate alınmalıdır. Aşağıda tekrar değerlendirileceği üzere Kişisel Verilerin Korunması Kurulu oluşum şekli dolayısıyla yürütmeye bağımlı görülmektedir.

Din, etnik köken gibi bilgiler kişilerin kendi istekleri bu yönde olmadığı sürece hiçbir zaman kayıt altında tutulmaması gereken verilerdir. Kişinin sendika üyeliğine, sağlık durumuna ilişkin bilgiler ise kimi zaman kayıt altına alınabilen ancak herhangi bir bilgidен daha üst bir korumayı gerektiren en hassas bilgileri oluşturur. Bu nedenle pek çok ulusal ve uluslararası metinde bunlar gibi bazı bilgiler için diğer verilere göre daha nitelikli bir koruma öngörülmüştür. Hatırlanacağı üzere bu konudaki tartışmaları çalışmamızın üçüncü bölümünde değerlendirmiştik³⁵¹. KVKKT’nin 7/3 hükmü ise adeta özel nitelikteki kişisel verilerin diğerlerine göre daha düşük bir seviyede korunmasına neden olmaktadır. Nitekim hükümdeki koşullar yeterli güvence sağlamadığı gibi, burada yer alan türde bir istisna kişisel verilerin işlenmesinde genel hukuka uygunluk sebepleri arasında da yer

³⁵⁰ Bkz. 95/46/AT sayılı Veri Koruma Yönergesi m. 8.

³⁵¹ Bu konuya ilişkin değerlendirmelerimiz için ayrıca bkz. üçüncü bölüm, “Özel Kategorideki (Hassas) Kişisel Verilerin Nitelikli Korunması” başlığı.

almamaktadır. Bütün bu nedenlerden ötürü Tasarının 7/3 hükmünün metinden çıkarılması en doğru yaklaşım olacaktır.

Son olarak 7. maddede TC kimlik numarasına ilişkin bir düzenlemeye de yer verildiğini belirtmek gerekir. Maddenin son fıkrası uyarınca“(v)atandaşlık kimlik numarası veya benzeri karakteristik işaretlerin işleme usul ve esaslarını belirlemek amacıyla yapılacak yönetmeliklerde kurulun görüşü alınır”. AT Veri Koruma Yönergesi, ulusal kimlik numaraları kullanımını devletlerin takdirine bırakmıştır³⁵². Daha önce de işaret edildiği gibi, ulusal kimlik numaraları kişisel verilerin korunmasına ilişkin önemli tartışmalara neden olmaktadır. Hatta kişisel verilerin korunması hukukunun gelişiminde bile devletlerin bu ve benzer uygulamalara ilişkin planlarının etkili olduğu söylenebilir. Ülkemizde yeteri kadar tartışılmadan kullanılmaya başlanan bu numaralar, bilgi edinme hakkı başvurusundan, faturalara, banka işlemlerinden, hastane kayıtlarına kadar hemen hemen her türlü hareketimizin kolaylıkla ilişkilendirilmesini ve bunlar sonucunda ayrıntılı profillerin oluşturulmasını sağlayabilir. Özel yaşam açısından ciddi sonuçları olabilecek bu numaraların işlenmesine ilişkin usul ve esasların yönetmelik ile belirlenmesi yeterli değildir. Bu derece hassas bir konuda gereken güvencelerin KVKKT kapsamına alınması daha yerinde olur.

3. Kişisel Verilerin Üçüncü Ülkelere Aktarımı

KVKKT’nin 8. maddesinde ise kişisel verilerin üçüncü kişilere aktarımına ilişkin kurallar düzenlenmiştir. Daha önce de belirtildiği gibi kişisel verilerin etkin korumasının sağlanabilmesi için verilerin yalnızca toplanmalarının hukuka uygun olması yeterli değildir. Eğer verilerin aktarımı meşru koşullara bağlanmazsa ilk aşamadaki hukuka uygun hareket büyük oranda anlamını yitirir.

Tasarının 8. maddesinde kişisel verilerin üçüncü kişilere aktarımı kural olarak yasaklanmış gibi görülse de geniş istisna ve sınırlamalar dolayısıyla uygulamada sonucun farklı olacağı açıktır. Çalışmamızın çeşitli yerlerinde daha önce de belirtildiği üzere 21. yüzyıl dünyasında ekonomik, sosyal ve siyasal yapının bir gereği olarak bilgi, hızla ve sürekli olarak sınır tanımaz bir şekilde akmaktadır. Kişisel verilerin korunması hukukunun amacı, bu akışın önüne set çekmek değildir.

³⁵² AB Veri Koruma Yönergesi, m. 8/7.

Buradaki hedef, bilgi akışının temel hak ve özgürlüklere saygılı bir şekilde gerçekleşmesini sağlamaktır. O halde Tasarıda kişisel verilerin üçüncü ülkelere aktarımının mutlak olarak yasaklanması zaten söz konusu olmamalıdır. Ancak bu alanda hiçbir koruma getirmemiş ülkelere yurttaşların kişisel bilgilerini göndermek, koruma alanını önemli oranda daraltacağı gibi, AB ile uyum sürecinde de ciddi sorunlara neden olabilir.

KVKKT'nin konuya ilişkin hükümleri değerlendirildiğinde bazı ifadelerin sorun yaratabilecek nitelikte olduğu söylenebilir. Nitekim istisnalar içerisinde yer alan “*milli güvenlik*”, “*suçun önlenmesi*”, “*istihbari faaliyetler*” gibi ifadelerin sınırlarının belirsiz olmasından dolayı, geniş yorumlanmaları durumunda hükmün anlamsız kalacağı dikkatten kaçmamalıdır. Bunun gibi “*kanundan doğan bir görevin yerine getirmesi*” ifadesi üzerinde de durulmalıdır: yasadan doğan görev ile kişisel verilerin işlenmesi gerekliliği arasında doğrudan ve açık bir bağlantının bulunmadığı durumlarda aktarım gerçekleştirilmemelidir³⁵³.

Kişisel verilerin yurtdışına aktarımına ilişkin olarak ise Tasarının 14. maddesi ile AB sistemine benzer bir düzenleme getirilmiştir. Kural olarak kişisel veriler ancak hedef ülkede “*eşdeğer ve etkin*” bir koruma mevcutsa aktarılabilir. Kişisel verilerin talep edildiği sorumlular, ilgili ülkede yeterli korumanın bulunup bulunmadığını incelemek zorundadır.

4. Veri Güvenliği

KVKKT uyarınca “*kişisel verilerin işlenmesinin amaç ve metodlarını tek başına veya başkaları ile birlikte belirleyen gerçek ve tüzel kişiler*” veri kütüğü sahibi olarak nitelendirilmektedir³⁵⁴. Veri kütüğü sahibi, kişisel verilerin işlenmesine ilişkin teknik ve idari tedbirler almalıdır³⁵⁵. Buna göre verileri işleyenler, teknolojideki gelişmeleri, işlemeden kaynaklanan riskleri, verinin niteliğini dikkate

³⁵³ “*Kanundan doğan bir görevin yerine getirilmesi*” ölçütünün tek başına kabulü doğru değildir. Buradan kaynaklanabilecek sıkıntıların giderilebilmesi için “*görevler*” ile “*kişisel veri*” arasında sıkı bir bağlantının aranması gerekir. Bkz. **Türkiye’de Yasa Yapma Süreçlerine Etkin Sivil Katılım Projesi**, s. 16.

³⁵⁴ Tasarıda veri kütüğü sahibi ifadesinin kullanımının da eleştirildiği görülmektedir. Veri kütüğü sahibi yerine, veri işlem sorumlusu ya da veri kütüğü sorumlusu gibi bir ifadenin kullanımı kişilerin sorumlu kişiyi daha net bir şekilde saptamalarını sağlayabilir. Bkz. Oğuz ŞİMŞEK, s. 210. Fikret İLKİZ, s. 18.

³⁵⁵ KVKKT m. 15.

olarak uygun teknik önlemleri almalı ve gerekli idari personeli istihdam etmelidir. Böylece veri güvenliği ilkesinin Tasarı kapsamında yer aldığı görülmektedir.

5. İlgili Kişinin Katılımı ve Denetimi

Tasarının 11. maddesi uyarınca veri kütüğü sahibinin kişisel verilerin elde edilmesi halinde ilgili kişiyi aydınlatma yükümlülüğü bulunmaktadır. Bilgilerin geleceğini belirleme hakkının bir uzantısı olan ve Avrupa veri koruma sistemine uygun bir şekilde düzenlenen bu hüküm uyarınca kişisel verileri elde eden kendi kimliği, verilerin işleme amacı, kimlere aktarılabileceği gibi konularda bilgi vermekle yükümlüdür. Daha önce de belirtildiği gibi bu, verileri elinde tutan kişinin bilgilendirme yükümlülüğüdür. Buna karşın bir de ilgili kişinin bilgilere erişim hakkı bulunur. Bu hakkın Tasarının 12. maddesi kapsamında düzenlendiği görülmektedir.

KVKKT'nin 12. maddesi uyarınca ilgili kişinin bilgiler erişim, yanlış bilgileri düzeltme, hukuka aykırı olanları sildirme, aktarılmasını engelleme hakları düzenlenmiştir³⁵⁶. Ancak Tasarının genelinde görülen bir sorunun burada da geçerli olduğunu belirtmek gerekir: geniş kapsamlı istisnalar hükmün uygulamasını ciddi oranda sınırlamaktadır. Tasarının 12/3 hükmü uyarınca bu maddede sayılan haklar şu durumlarda sınırlandırılabilir: *“(a) Milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi, suçun önlenmesi veya istihbarat amacıyla yapılan faaliyetlerle ilgili olarak kanundan doğan bir görevin yerine getirilmesi, (b) Ceza soruşturması veya kovuşturmasına zarar verilmesinin engellenmesi”*.

Burada yer alan ifadelerin kapsamının son derece geniş olması bir yana belirtilen hükümde yer alan hakların bir bölümü açısından dar sınırlamaların bile kabul edilebilir bir yanı bulunmamaktadır. Örneğin hukuka aykırı verinin silinmesinin engellenmesi meşru kabul edilebilir mi? Bunun gibi yanlış bir bilginin düzeltilmesine sınırlama getirilmesi haklı görülebilir mi? Eğer bir bilgi yanlışsa ona dayanılarak varılacak sonuç da yanlış olacaktır. Böylesine bir durumun yalnızca ilgili kişiye değil, veriyi işleyene de zarar vereceği açıktır. Dolayısıyla yanlış bilginin düzeltilmesini engellenmenin makul bir nedeni bulunmamaktadır.

³⁵⁶ Bu maddeye göre yapılacak başvuruların usulü ise Tasarının 13. maddesinde düzenlenmiştir.

Son olarak Tasarıda düzenlenen, kişinin katılımı ve denetimine yönelik ilkelerin kapsamına 95/46/AT sayılı Veri Koruma Yönergesinde yer alan “*ilgilinin otomatik kararların konusu olmama hakkı*”nın alınmadığını belirtmek gerekir³⁵⁷. Çalışmamızın üçüncü bölümünde de belirtildiği üzere uygulamasına nadiren rastlansa da bu hüküm, verilerin korunmasında ileride gelişeceği düşünülen bir ilkenin temelini oluşturur. Nitekim belirtilen ilke, kişinin karakterinin tamamen otomatik yollardan değerlendirilmesinin, onun çıkarlarını önemli ölçüde etkileyecek kararların temelini oluşturmaması düşüncesine dayanır.

6. İstisna ve Sınırlamalar

Tasarının madde hükümlerinde yer alan çeşitli istisnalar yanında 22. maddede hukuka uygunluk sebepleri (m.6), aydınlatma yükümlülüğü (m.11), veri kütüğüne kayıt(m.16, 17) ve aşağıda değinilecek ön inceleme (m.19) açısından geçerli olacak bazı genel sınırlama sebepleri de öngörülmüştür. Buna göre belirtilen madde hükümleri, milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbarat faaliyetlerinin yürütülmesi durumunda uygulanmaz. Bunun yanında kamu düzeninin korunması, suçun önlenmesi için gerekli olması, suç veya meslek ahlak kurallarını ihlal eden eylemlerin soruşturulması veya kovuşturulması, bütçe, vergi ve mali konulara ilişkin devletin önemli ekonomik çıkarlarının, ayrıca belirtilen konularda resmi mercilerin izleme, denetleme veya düzenleme görevlerinin gerektirmesi halinde yine uygulanmayacaktır.

Ayrıca bu durumların varlığı 25. madde uyarınca “*kanunda yer alan genel ilkeleri taşımayan*” kişisel verilerin silinmesi ve yok edilmesinin de istisnası olarak görülmüştür. 25. maddenin gerekçesinde bu hükümle “*artık ihtiyaç duyulmayan kişisel verilerin silinmesi veya yok edilmesi*” konusunun düzenlendiği belirtilmektedir. Oysa “*kanunda yer alan genel ilkeleri taşımama*” ile “*artık ihtiyaç duyulmama*” birbirinden farklı kavramlardır. Belirtilen sınırlama nedenlerinin söz konusu olduğu durumlarda yasada yer alan genel ilkeleri taşımayan verilerin silinememesi ve yok edilememesi kişisel verilerin korunması hakkının özüne zarar verici bir nitelik taşır.

³⁵⁷ AB Veri Koruma Yönergesi, m. 15/1.

Tasarı, ilgili hükümlerde yer alan istisnalar yanında belirtilen daha genel istisnalar ile birlikte artık kişisel verilerin korunması işlevini büyük oranda kaybetmiş, adeta istisna kural haline gelmiştir³⁵⁸. Bu sorunun giderilebilmesi için öncelikle istisnaların sınırları belirlenmelidir. Örneğin milli güvenliğin korunması istisnasının uygulanabilmesi için yakın tehdit ve tehlikenin varlığı koşulu aranabilir³⁵⁹.

Bunun yanında kişisel verilerin korunması temel insan hakları içerisinde değerlendirilen bir konu olduğuna göre sınırlamalarda Anayasanın 13. maddesinde belirlenen kurallara uyulmalıdır. Buna göre hakkın özüne dokunulmaksızın, yalnızca Anayasada belirtilen sebeplere bağlı olarak yasayla sınırlanması, ayrıca Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.

Sınırlamanın sınırlarına ilişkin olarak dikkate alınması gereken bir diğer önemli metin AİHS'dir. Özellikle Sözleşmenin 8. maddesi ve bu hüküm çerçevesinde AİHM'in geliştirdiği yorum bu noktada mutlaka dikkate alınmalıdır. Buna göre kişisel verilerin korunmasına getirilecek sınırlamanın yasayla öngörülmesi ve belirlenen meşru amaçlara yönelmesi yanında ancak *“demokratik bir toplum için gerekli olması”* koşulunu karşılaması gerekir. Bu hususların uygulayıcılar tarafından daha açık bir şekilde görülmesi için yasa metnine de alınması yararlı olabilir. Ancak daha önemlisi kişisel verilerin korunması *“hakkı”*na Tasarıda açıkça yer verilmesidir.

KVKKT'de öngörülen denetim ve yaptırım sistemlerine ilişkin açıklamalara geçmeden önce gazetecilik amacıyla kişisel verilerin işlenmesinin de Tasarıda ayrıca düzenlendiği belirtilmelidir. Buna göre kişisel verilerin yalnızca gazetecilik amaçlarıyla işlenmesi halinde kişisel verilerin işlenmesine ilişkin ilkeler ve tedbirlere ilişkin hükümler uygulanacağı gibi, kişisel verilerin işlenmesi bakımından belirlenen meslek davranış kurallarına da uyulacaktır. Kişisel verilerin gazetecilik amacıyla işlenmesi *“ancak düşünceyi açıklama ve yayma hürriyeti sınırları çerçevesinde, yayın sahipleri veya temsilcileri ve bunların çalışanlarının enformasyon ihtiyaçlarının karşılanması için gerekli olması halinde hukuka uygun sayılır”*³⁶⁰.

³⁵⁸ Kişisel Verilerin Korunması, TBD Kamu-BİB, s. 79.

³⁵⁹ **Türkiye’de Yasa Yapma Süreçlerine Etkin Sivil Katılım Projesi**, s. 18.

³⁶⁰ KVKKT m. 23/2.

Tasarı uyarınca faaliyet gösterdikleri sektörün özelliklerine uygun olarak meslek birlikleri tarafından hazırlanan davranış kurallarının Yasaya uygunluğunun denetimi için aşağıda incelenecek Kişisel Verilerin Korunması Kurulunun görüşü alınacaktır. Bu noktada Kurul'un bir onay makamı olmadığını belirtmek gerekir. Aksi düşünce meslek kuruluşlarının özerkliğinin ihlali anlamına gelir³⁶¹.

E. KVKK'TA ÖNGÖRÜLEN DENETİM VE YAPTIRIM SİSTEMİ

KVKK'Ta kişisel verilerin belirlenen ilkelere uygun bir şekilde işlenip işlenmediğini izlemek, denetlemek ve hukuka aykırı uygulamaları yaptırıma bağlamak üzere çeşitli hükümler yer almaktadır. Çalışmamızın üçüncü bölümünde yaptığımız açıklamalardan hatırlanacağı üzere kişisel verilerin korunmasını ulusal hukuk sistemlerinin bir parçası haline getiren pek çok ülkede de benzer ilkeler kabul edilmiştir (Bkz. Tablo 4.3.).

Öncelikle Tasarı uyarınca kişisel verileri işleyen gerçek kişiler ile kamu ve özel hukuk tüzel kişilerinin veri kütüğü kurmadan önce tescil edilecekleri bir sicilin oluşturulması öngörülmektedir³⁶². Sicile kayıt başvuru yapılırken veri kütüğü sahibinin kimliği, kişisel verilerin işleme amacı gibi konuları içeren bir bildirimin yapılması zorunludur³⁶³. Bu bildirimler kişisel verilerin Tasarıda belirlenen ilkelere

³⁶¹ Fikret İLKİZ, s. 20.

³⁶² KVKK m. 16. Tasarı uyarınca veri kütüğü ile “Gerçek ve tüzel kişilere ilişkin belirli bir ölçüte göre kişisel verilere ulaşımı kolaylaştıracak şekilde yapılandırılmış herhangi bir kişisel veri grubu” ifade edilmektedir. KVKK m. 3/1, h. KVKK Gereğesinde kişisel veri kütüklerinin önemi üzerinde özel olarak durulduğu görülmektedir. Gereğesinde şu ifade yer alır: “Kişisel veri kütüğü sistemleri iki grup açısından önem arz etmektedir: Bunlardan birincisini kişisel veri sicillerini kullananlar oluşturmaktadır. Yukarıda da belirtildiği gibi, mal ve hizmetlerin ihtiyaca uygun bir şekilde üretimi ve dağıtımı için bu tür sicillerden yararlanılması zorunlu hale gelmiştir. Bu sicillerden yararlananların, ihtiyaçları olan kişisel verileri işlemeleri engellenmemeli, aksine kolaylaştırılmalı, ancak ilkelere bağlanmalıdır. Diğer grubu ise, hakkında kişisel veri işlenen gerçek ve tüzel kişiler oluşturmaktadır. Elektronik bilgi işlem sistemlerinde zorunlu olarak kişiler hakkında kişisel veriler işlenmektedir. Kişisel veriler sınırsız olarak gelişigüzel toplandığı, denetimsiz olarak açıklandığı, yetkisiz kişilerin eline geçtiği takdirde kötüye kullanılarak kişilik hakları ihlal edilebilecektir. Bu nedenle kişisel veri sicillerinin bu tür sakıncaları giderecek şekilde kurulması, faaliyet göstermesi ve denetim altına alınması zorunlu hale gelmiştir. Tasarı, bu iki grubun çıkarlarını koruyarak dengelemek ve kişilik hakları ile temel hak ve hürriyetleri korumak amacıyla hazırlanmıştır”.

³⁶³ KVKK m. 17. Bildirimin istisnaları ise 18. maddede düzenlenmiştir.

uygun bir şekilde işlenmesi açısından oldukça önemlidir³⁶⁴. Nitekim Kişisel Verilerin Korunması Kurulu, veri konusu kişilerin, kişiliklerine, temel hak ve özgürlüklerine yönelik risk taşıma olasılığı bulunan ve Tasarıda belirlenen koşulları taşımayan veri işlemleri belirlemek için işlem başlamadan önce bir ön inceleme yapar³⁶⁵.

Tablo 4.3. Bazı Devletlerde Kayıt, Bildirim Zorunluluğu ve Bağımsız Organlarca Denetim Usulü

DEVLET	KAYIT veya BİLDİRİM	VERİ KORUMA ORGANI
Almanya	Bazı veriler	Federal Veri Koruma Komiserliği [http://www.bfdi.bund.de/]
Arjantin	Bütün veriler	Adalet Bakanlığı bünyesinde bağımsız bir kurul
Avusturya	Bütün veriler (önemli istisnalarla)	Veri Koruma Kurulu [http://www.dsk.gv.at/]
Belçika	Bütün veriler	Özel Yaşamın Gizliliğini Koruma Kurulu [http://www.privacycommission.be/]
Birleşik Krallık	Bütün veriler	Enformasyon Komiserliği Ofisi [http://www.ico.gov.uk/]
Fransa	Bazı veriler	Özgürlük ve Bilgisayarlaşma Ulusal Kurulu [http://www.cnil.fr/]
Hırvatistan	Bütün veriler (önemli istisnalarla)	Kişisel Verilerin Korunması Kurulu [http://www.azop.hr/default.asp]
Hong Kong		Kişisel Veriler için Özel Yaşamın Gizliliği Görevlisi Ofisi [http://www.pcpd.org.hk/]
İrlanda	Bazı veriler	Veri Koruma Kurulu [http://www.dataprotection.ie/docs/Home/4.htm]
İspanya	Bütün veriler	Veri Koruma Dairesi [https://www.agpd.es/]
İsviçre	Bazı veriler	Federal Veri Koruma ve Enformasyon Komiserliği [http://www.edoeb.admin.ch/index.html?lang=en]
İtalya	Bazı veriler	Kişisel Verilerin Korunması Denetmeni [http://www.garanteprivacy.it/]
Norveç	Bütün veriler	Veri Teftiş Heyeti [http://www.datatilsynet.no/]
Portekiz	Bazı veriler	Ulusal Veri Koruma Kurulu [http://www.cnpd.pt/]
Yunanistan	Bütün veriler	Kişisel Verilerin Korunması Kurulu [http://www.dpa.gr/]

Kaynak: http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents.

Aşağıda örnekleme yoluyla seçilen bazı devletlerde kişisel verilerin korunması kapsamında bağımsız bir denetim organı ile kayıt ve bildirim zorunluluğunun kabul edilip edilmediğine ilişkin karşılaştırmalı bir tablo sunulmaktadır. Veri koruma organına ilişkin daha ayrıntılı bilgi parantez içinde verilen resmi İnternet sitelerinden edinilebilir.

³⁶⁴ Veri kütüğü sahiplerinin Tasarıda belirlenen hükümlerin uygulanmasını sağlamak üzere bağımsız bir denetim kuruluşunu görevlendirmeleri de olanaklıdır. Bkz. KVKKT m. 20, 21.

³⁶⁵ KVKKT m. 19.

Tasarının Dördüncü Kısımında düzenlenen Kişisel Verileri Koruma Kurulu, Bakanlar Kurulunun seçtiği yedi üyeden oluşur³⁶⁶. Kurulun başkanı yine Bakanlar Kurulunca, başkan vekili ise Kurul tarafından kendi üyeleri arasından seçilir³⁶⁷. Her ne kadar kurulun yetkilerini bağımsız olarak kullanacağı belirtilmişse de³⁶⁸ üyelerin ve başkanın Bakanlar Kurulu tarafından seçilmesi bu ilkeye ciddi oranda zarar vermektedir³⁶⁹.

Kişisel Verileri Koruma Kurulunun oluşumuna ilişkin 26. maddenin gerekçesinde AK Sözleşmesine ve AT Veri Koruma Yönergesine atıfta bulunulduğu görülmektedir. Her iki düzenleme de bağımsız bir denetim organının kurulmasını öngörmektedir. Ancak bu bağımsızlığı yalnızca kağıt üzerinde kalan bir ifade olarak anlamamak gerekir. KVKKT’de Veri Koruma Kurulunun yetkilerini bağımsız olarak kullanacağı hiçbir organ, makam, merci ve kişinin Kurulun kararını etkilemek için emir ve talimat veremeyeceği belirtilmiştir. Ancak Kurulun üyelerin belirlenme usulü dikkate alındığında bunun yalnızca temenni düzeyinde kalma olasılığı açıkça görülebilir. Nitekim Kişisel Verilerin Korunması Kurulunun oluşum şekli Tasarının en çok eleştirilen hükümlerinden birini oluşturmaktadır³⁷⁰.

Tasarı uyarınca Kurul üyelerinin görev süresi altı yıldır ve süreyi dolduranlar bir daha seçilemez. Tasarıda Kurul üyelerinin tarafsızlığını ve ilgili kişilerin bilgilerini koruyacak bazı hükümlerin yer aldığı görülür³⁷¹. Bunun yanında Kurulun

³⁶⁶ KVKKT m. 27/1.

³⁶⁷ KVKKT m. 27/4.

³⁶⁸ KVKKT m. 26/2.

³⁶⁹ Oysa Tasarının 2003 yılında Adalet Bakanlığı tarafından kabul edilen şeklinde Kurulun oluşumunun daha özerk olduğu görülmektedir. Tasarının önceki şeklinde Kurulun “*üç üyesi bakanlıkların gösterecekleri birer; bir üyesi Türkiye Odalar ve Borsalar Birliğince, bir üyesi Türkiye Bilimsel ve Teknik Araştırma Kurumunca, bir üyesi Yükseköğretim Kurumunca, bir üyesi de Adalet Bakanlığınca bu Bakanlıkta idarî görevlerde çalışan birinci sınıfa ayrılmış hâkimler arasından gösterilen üçer aday arasından Bakanlar Kurulunca*” seçilip atanacağı düzenlenmişti. Bu üyelerin belirlenme sisteminde değişikliğe gidilmesinin nedeni ilgili maddenin gerekçesinde de açıklanmamıştır.

³⁷⁰ Kurulun yeni oluşumuna ilişkin eleştirilerin basına da yansıdığı görülmektedir: “Adalet Komisyonu’nda bulunan tasarılarından biri hükümete zırh, diğeri yurttaş ‘fişleme’ getirecek-İktidar ‘sır’la korunacak”, *Cumhuriyet*, 24 Mayıs 2008. “**Jandarma Talebi Değil, Kişisel Verilerin Korunması Kanun Tasarısı Sorunlu**”, <http://www.bianet.org>, 18 Haziran 2008. Kurulun bu oluşum şeklinin değiştirilmesi yönünde çeşitli öneriler bulunduğu da görülmektedir. Kurul üyeleri arasında akademisyenlerin, sivil toplum ve baro temsilcilerinin yer alması, başkan ve üyelerin bağlı oldukları kurumları ilgilendiren kararlara ilişkin kararlara ilgili toplantı ve oylamalara katılamayacaklarına ilişkin bir kuralın eklenmesi bu kapsamda sayılabilir. Bkz. **Türkiye’de Yasa Yapma Süreçlerine Etkin Sivil Katılım Projesi**, s. 22.

³⁷¹ KVKKT 30/2 hükmü şöyledir: “*Başkan ve üyeler kendilerini, üçüncü dereceye kadar kan ve ikinci dereceye kadar kayın hısımlarını, evlatlıklarını ve aralarındaki evlilik bağı kalkmış olsa bile eşlerini ilgilendiren kararlara ilgili toplantı ve oylamaya katılamaz*”. Tasarının 30/3 hükmü

görev ve yetkilerinin oldukça geniş bir şekilde belirlendiğini de belirtmek gerekir³⁷². Bu yetkiler Kurulun Türkiye’de kişisel verilerin korunması açısından kilit bir konumda olacağını ortaya koymaktadır. Bu nedenle etkin ve yeterli korumanın sağlanabilmesi için Tasarı yasalaşmadan Kurulun oluşum şeklinde değişiklik yapılması ve özerk bir kuruluş haline getirilmesinin önemine tekrar işaret edilmelidir.

Son olarak KVKKT’de bazı cezai ve idari yaptırımların da öngörüldüğünü belirtilmelidir. Buna göre cezai yaptırımlar konusunda yukarıda incelenen TCK’nın 135 vd. maddelerine atıf yapılmıştır. Ayrıca aydınlatma yükümlülüğü (m.11), ilgili kişinin hakları (m.12), kişisel verilerin işlenmesine ilişkin tedbirler (m.15), ön inceleme (m. 19), Kişisel Verilerin Korunması Kurulunun bilgi ve belge istemleri (m.26/3) ve Kurulun inceleme usul ve esasları (m.33) ile ilişkili belirtilen madde hükümlerinin ihlali halinde beş bin Türk Lirası idari para cezası öngörülmüştür³⁷³.

Veri kütüğü siciline kaydolma yükümlülüğü (m.16), bağımsız denetim kuruluşunun Kurula bildirilme zorunluluğu(m.21) ve kişisel verilerin işlenmesi bakımından meslek davranış kurallarına (m.24) aykırı hareket edilmesi halinde ise Kurul tarafından onbin Türk Lirası idari para cezası verileceğine hükmedilmiştir³⁷⁴. Belirtilen hükümlerle suçta kanunilik ilkesinin korunması hedeflenmiş ve ihlalin ağırlık derecesine göre giderek artan para cezaları öngörülmüştür³⁷⁵. Kanımızca bunun yanında hukuka aykırı veri işlemlere kişilerin tazminat hakkı bulunduğu ilişkili bir hükmün bulunması yerinde olur.

ise şöyledir: “Kurul üyeleri çalışmaları ve denetlemeleri sırasında ilgililere ve üçüncü kişilere ait öğrendikleri sırları bu konuda kanunen yetkili kılınan mercilerden başkasına açıklayamazlar ve kendi yararlarına kullanamazlar. Bu yükümlülük görevlerinden ayrılmalarından sonra da devam eder”.

³⁷² KVKKT’nin 31. maddesi uyarınca Kurulun görev ve yetkileri şunlardır: “(a) Kişilik hakları ihlal edilenlerin başvuruları hakkında karar vermek, (b) İlgili kişi bakımından telifisi güç veya imkansız bir zararın doğması ihtimalinin bulunması halinde geçici önlemler almak, (c) Kişisel verilerin işlenmesine ilişkin konularda düzenleyici işlemleri hazırlamak, (ç) Yabancı ülkelere veri aktarımı konusunda tereddüt bulunması halinde karar vermek, (d) Başkanın sunduğu önerileri karara bağlamak, (e) Kurul faaliyetleri hakkında yıllık rapor hazırlamak, (f) Sicilin tutulmasını sağlamak, (g) Yurtiçi ve yurtdışında verilerin korunması makamları ile işbirliği yapmak, (ğ) Veri koruma hukuku alanındaki gelişmeleri takip etmek ve bunların uygulanması için gerekli önlemleri almak, (h) İhtiyaç duyulan alanlarda ulusal ve uluslar arası kurum ve kuruluşlarla işbirliği içinde araştırma ve teknik yardım projeleri hazırlamak, geliştirmek ve yürütmek, (ı) Kanunlarda verilen diğer görevleri yerine getirmek”.

³⁷³ KVKKT m. 37/1, a.

³⁷⁴ KVKKT m. 37/1,b; 2.

³⁷⁵ KVKKT 37. madde, Gerekçe.

SONUÇ

Kişisel verilerin korunması, ilk bakışta yeni gelişen ve hukuksal koruma gerektiren her hangi bir konu gibi görülebilir. Oysa biraz daha dikkatli bir bakış, kişisel verilerin korunmasının çözüm bulunması gereken basit bir konudan çok daha öte bir anlamı olduğunu gösterecektir. Nitekim verileri kimin, nasıl kullanacağı sorusu, bireylerin, kurumların ve devletlerin gücüyle ilgili yanıtlar sunar.

Bireyin modern devletin ve kapitalist işletmelerin çarkları arasında kaybolmadan, kişiliğini korumaya ve geliştirmeye devam edebilmesi için, bilgilerin geleceğini belirleme hakkına gereksinim bulunur. Nitekim kişisel verilerin korunması doğrudan insanın kendisiyle ve kendisine ilişkin olanla ilgilidir. Bu nedenle insan hak ve özgürlüklerinin kapsamında değerlendirilir. Kişisel verilerin korunması, temelde bireyin kişiliğinin korumasına, kendine ilişkin bilgilerin geleceğine karar verebilmesine hizmet eder. Yalnızca rakamlardan oluşmadığının bir göstergesidir. Yalnızca kendisine ait olan bir alana gereksinim duyduğunun işaretidir.

Bu temel konuların hiçbiri aslında doğrudan teknoloji ile ilişkili değildir. Ancak teknoloji tehlikenin çok daha ciddi boyutlara taşınmasında etkili olmuştur. Kişisel veriler, her geçen gün biraz daha fazla üretilmekte, toplanmakta, kullanılmakta, ilişkilendirilmekte ve başkalarına aktarılmaktadır. Üstelik bu teknolojiler hızla ucuzlamakta ve bunları kullanan kişi ve kurumların sayısı da hızla artmaktadır. Bunlar elbette öncelikle teknolojinin sunduğu olanaklardır. Ancak bu olanakların ilk başta görülmeyen bazı yan etkileri bulunur. Teknolojide gelişimin gözetim olanaklarını arttırması bunun açık bir örneğidir.

İşte bu nedenle kişisel verilerin korunmasına yönelik ilk hukuksal düzenlemeler, merkezi veri bankalarının kullanımına ilişkin çeşitli projelerin geliştirildiği 1970'li yıllarda ortaya çıkmıştır. Burada hedef yalnızca devlete karşı bireyi korumak iken, zaman içerisinde özel teşebbüslere karşı koruma geliştirmenin de önemli ve gerekli olduğu anlaşılmıştır. Nitekim günümüzde özel teşebbüsler, en az devletler kadar (hatta belki onlardan daha fazla) kişisel verilere gereksinim duymakta, onları çeşitli kaynaklardan toplamakta, işlemekte ve değerlendirmektedir.

Günümüzde bir yandan İnternet ile saniyeler içinde kıtalar arası bilgi akışı gerçekleştirilirken, diğer yandan RFID, kapalı devre televizyon sistemleri (CCTV)

gibi araçlarla yeni ve daha ayrıntılı bilgiler hızla toplanmaktadır. Bu, daha fazla sayıda verinin ulaşılabilir olmasını sağladığı gibi, daha önce kayıt altına alınması olanaklı bulunmayan bazı bilgileri de depo edilebilir kılmaktadır. Artık kişilerin görüntüleri, sesleri, bulundukları yerler kayıt edilebilir durumdadır. DNA profilleri aracılığıyla kişilere ve hatta yakınlarına ilişkin daha önce kendilerinin bile bilmesi olanaklı olmayan bilgilere ulaşılabilir.

Bütün bunlar, özel yaşama yönelen tehdidin daha önemli bir boyuta gelmesine neden olur. Ancak sorun bununla da sınırlı kalmaz. Yukarıda açıklamaya çalıştığımız gibi bu bilgiler kolaylıkla ilişkilendirilebilmekte ve anlamlı sonuçlar çıkarılabilmektedir. Üstelik bu işlem, çoğu zaman insan müdahalesi olmaksızın otomatik yollarla gerçekleştirilebilir. Bu ise bireyin özerkliğine ve “insan” olmasından kaynaklı değerine karşı ciddi bir tehdit oluşturur. Nitekim kişinin yaşamına yönelik kararların sayısal verileri değerlendiren makinelerle bırakılması öznenen nesneye dönüşmesine neden olabilir.

Günlük yaşamı çeşitli gözetleme araçlarıyla kuşatılmış “camdan bireylere” doğru evrilmemek için teknolojinin önüne bariyerler koymadan, onun gelişimini durdurmaya gayret göstermeden bireyin özel alanını korumaya çalışmak gerekir. Amaç, bilgi akışını engellemek değildir. Bilgi üretimi, kullanımı ve aktarımı 21. yüzyılın en önemli unsurlarından biridir. Ancak bu süreç içerisinde birey özerkliğini kaybetmemeli, özgürlüğünü koruyabilmeli ve kişisel verileri üzerinde karar verebilmelidir. Bu ise ancak çatışan çıkarların dengelenmesi ile söz konusu olabilir.

Nitekim bilginin düzenin en önemli bileşeni olduğu günümüzde kişisel verilerin korunması çok boyutludur: siyasal, sosyal, ekonomik yansımaları bulunur. Hukuksal açıdan ise hemen hemen her alanla ilişkilidir: idare hukukundan ticaret hukukuna, medeni hukuktan ceza hukukuna kişisel verilerin korunmasına ilişkin çeşitli ilkelere yer verilmesi gerekmeyen alan hemen hemen yok gibidir. 21. yüzyılda artık e-ticaret ekonomik yaşamın önemli bir parçası, e-devlet projeleri siyasal düzenin bir gerekliliği, İnternet ortamındaki onlarca iletişim şekli sosyal yaşamın yeni şekilleridir.

İşte kişisel verilerin korunması hukuku bu düşüncenin ürünüdür. Teknolojideki hızlı gelişim, kişi, kurum ve devletlerin bilgi gereksinimi ile bireylerin özel yaşamları arasındaki dengeyi birinciler lehine bozmuştur. Kişisel verilerin

korunması hukuku dengeyi tekrar kurmayı, kişisel verileri işlenen bireye tekrar söz hakkı tanımayı hedefler. Aksi durum bireyin öznenen nesneye doğru evrilmesine neden olur. Bu ise insan haklarının temel değeri olan insan onurunun kaybı anlamına gelir.

Bu düşüncelerden hareketle yaklaşık 40 yıldır dünyanın pek çok yerinde bu konuyu düzenleyen kurallar ve ilkeler geliştirilmiştir. Yukarıda açıklamaya çalıştığımız üzere en köklü düzenlemeler Avrupa'da olsa da, Kanada'dan Avustralya'ya demokratik devletlerin hemen hemen tamamı konuyu ulusal hukuk sistemlerinde titizlikle düzenlemektedir. OECD, BM, AK ve AB gibi önemli uluslararası ve uluslararası kuruluşlar konuya ilişkin yol gösterici temel ilkeleri belirlemekte, daha etkin bir koruma için araştırma ve çalışmaları sürdürmektedir.

Bu metinler incelendiğinde ortak bir özellik kolaylıkla fark edilebilir: kişisel verilerin korunmasında hâkim olan temel ilkeler büyük oranda önleyici niteliktedir. Bir başka anlatımla henüz bir zarar oluşmadan kişisel verilerin korunması hedeflenmektedir. Kişisel verilerin hangi amaçla işleneceğinin belirli olması gerekliliği, ilgilinin rıza beyanının önemi, hassas nitelikli bazı veri türlerinin işlenmesinin kural olarak yasak olması bu düşünceden kaynaklanır. Nitekim kişisel verilerin korunması hukukunun en önemli işlevi de budur.

Ne yazık ki Türk hukuk sisteminde bu konuda önemli bir eksiklik bulunmaktadır. Ülkemizde yukarıda söz edilen teknolojik gelişmelerin yakından izlenmesine karşın halen kişisel verilerin korunması yeterli bir hukuksal güvence altına alınmamıştır. Türkiye'de hukuk mevzuatı incelendiğinde düzenlemelerin daha çok zarar oluştuğundan sonra bunun giderimine yönelik olduğu görülür. İdarenin haksız işlemlerine karşı yargı yoluna gidilebilir ya da kişilik haklarının ihlali dolayısıyla tazminat ve benzeri istemlerde bulunulabilir. Kişisel verilerin hukuka aykırı olarak ele geçirilmesi gibi durumlarda TCK uyarınca çeşitli yaptırımlar öngörülmüştür.

Ancak kişisel verilerin korunmasında hâkim olan temel ilkelerin uygulanmadığı bir ortamda bunlar, zararın oluşmasını önlemeye yetmemektedir. Oysa kişisel verilerin korunması hukuku zararın oluşmasını engellemek için oldukça yararlı araçlar sunmaktadır. Bilgilere erişim hakkı, ilgili kişiyi bilgilendirme gerekliliği bu araçlara örnek olarak verilebilir. Bu ve benzeri ilkelerin kabul edilmediği bir ortamda birey kendisine ilişkin bilgiler üzerinde denetimini kaybeder.

Oysa “*bilgilerin geleceğini belirleme hakkı*” kişiliğin önemli bir parçasıdır. Öte yandan şu husus da dikkatten kaçmamalıdır: kişisel verilerin toplanması ve çeşitli amaçlarla kullanılmasının olumsuz sonuçları, hukuksal açıdan her zaman “*zarar*” kavramını karşılar bir nitelikte olmayabilir.

Çalışmamızın birinci bölümünde işaret ettiğimiz üzere, teknolojideki gelişmelerle hız kazanan oranda, bireyin özel yaşamına yönelen ciddi tehditler bulunmaktadır. Bu tehditlerin gerçek ve yakın olduğu açıktır. Kişisel verilerin korunmasına ilişkin temel ilkelerin belirlenmesi, bunların uygulanabilmesi ve etkinliği ilk olarak tehditlerin önlenmesine hizmet edecektir. Ayrıca bunun yanında bireyin üzerindeki sürekli izlenme psikolojisinin ortadan kaldırılmasını sağlayacağı da dikkatten kaçmamalıdır.

Birey, ancak kendini özgür hissettiği oranda özgürleşebilir. Sürekli gözetlendiğini düşünen kişi, temel hak ve özgürlüklerini kullanırken çekingen davranabilir, bireysel özerkliğini kaybedebilir. Bu ise insanın insan olmasında kaynağını bulan çok önemli değerlerin yıkımı olur. Zarar büyüktür ancak hukuksal alanda saptanması da bir o kadar güçtür. O halde kişisel verilerin korunmasının bireysel özerkliğin korunması açısından önemli işlevini bir kez daha anımsamak gerekir.

Çalışmamızın başından beri işaret ettiğimiz üzere kişisel verilerin korunması yaklaşık kırk yıldır Batılı hukuk sistemlerinde çeşitli şekillerde düzenlenen ve güvence altına alınan son derece önemli bir alanı oluşturmaktadır. Türkiye’de AK Veri Koruma Sözleşmesi yaklaşık otuz yıl önce imzalanmasına karşın halen bu konuda kapsayıcı bir çerçeve düzenleme yapılmaması ise önemli bir eksikliktir. Bu nedenle kanımızca ülkemizde kişisel verilerin korunmasını sağlayacak, bu konuda temel ilkeleri ve denetim usulünü belirleyecek bir yasal düzenlemenin yapılması zorunludur.

Kişisel verilerin korunmasına yönelik çerçeve bir yasanın konuya ilişkin ilkeleri belirlemesi birkaç açıdan önemlidir. İlk olarak kişisel verileri işleyenlerin uyacakları usul ve esasların belirlenmesi ve ilgili kişilerin haklarının güvence altına alınması şu anda eksikliği hissedilen önleyici koruma gereksinimini giderecektir. Bunun yanında çeşitli hukuksal düzenlemelerde dağınık bir şekilde bulunan konuya ilişkin hükümlerin uygulamasına da açıklık getirecektir.

Bunun yanında AB Veri Koruma Yönergesinin yeterli oranda veri koruma sağlamayan ülkelere veri aktarımını yasaklayan hükümleri dolayısıyla, Avrupa devletleri ile ticari ilişkilerde, adli işbirliğinde sorun yaşanmaması için de böylesine bir yasaya gereksinim duyulmaktadır. AB'ye adaylık sürecinde ise bu gereksinim adeta bir zorunluluğa dönüşmektedir.

Bu ve benzeri nedenlerle bir KVKKT hazırlanmıştır. Ancak KVKKT'nin yukarıda işaret edilen şekli bu gereksinimi karşılamaktan uzaktır. Oldukça geniş kapsamlı istisnalarla uygulama alanı daraltılmış ilkeler ve yürütme organına adeta bağımlı kılınmış bir denetim organıyla tasarı ancak görüntüde kişisel verilerin korunmasını sağlayabilecek niteliktedir. Hatta Tasarının kişisel verilerin korunmasının değil, korunmamasının yasal dayanağının oluşturacağını bile söylemek olanaklıdır. Bu haliyle Tasarı, istisnanın kural haline geldiği düzenlemeleri içermektedir. Tasarıda düzenlenen “bağımsız” denetim organının tamamen idareye bağımlı olarak oluşturulması zaten geniş istisnaların uygulamada daha da ciddi sorunlar yaratabileceğine işaret etmektedir.

Türkiye’de her geçen gün önemi artan, kişisel verilerin korunmasına yönelik etkili bir yasal düzenlemenin kabulü gerekmektedir. Çerçeve niteliğinde bir yasal düzenlemede kişisel verilerin korunması ilkelerinin tanınması ve bu ilkelerin uygulamasını denetleyecek gerçek anlamda bağımsız bir organın oluşturulması, insan haklarına saygılı, demokratik bir hukuk devletinin gereğidir. İkinci olarak ABTHŞ’de yer aldığı ve Türkiye’de çeşitli Anayasa Taslaklarında önerildiği üzere kişisel verilerin korunmasının doğrudan anayasal güvenceye kavuşturulması oldukça önemlidir. Buna karşın, böylesine bir düzenleme kabul edilinceye kadar, kişinin maddi ve manevi varlığını geliştirme hakkı, özel yaşamın gizliliği hakkı ve düşünce özgürlüğü gibi güçlü anayasal dayanakların bulunduğu unutulmamalıdır. Son olarak her an kişisel verileri toplanan, değerlendirilen, kullanılan ve aktarılan bireylerin karşı karşıya oldukları tehdidin bilincinde olması ve “*verilerine*” ya da daha doğru bir ifadeyle “*öz benliklerine*” sahip çıkmaları, bilinçlenmeleri ve bu yönde talepte bulunmaları en az yasal düzenlemeler kadar önemlidir.

KAYNAKÇA

* Çalışmamız içerisinde yararlanılan kaynaklar arasında, parantez içerisinde son yararlanma tarihi gösterilmemiş bütün İnternet adresleri 1 Mart 2010 tarihinde ziyaret edilmiş ve bu tarih itibariyle atıf yapılan adresteki varlıkları teyit edilmiştir.

I. KİTAP VE MAKALELER

“Balancing Security and Liberty Within the European Human Rights Framework, A critical reading of the Court’s case law in the light of surveillance and criminal law enforcement strategies after 9/11”, **Security and Civil Liberties**, haz. Antonie M. HOL, John A. E. VERVAELE, Intersentia, İngiltere 2005, s. 37-77.

“Foucault and Panopticism Revisited”, **Surveillance & Society**, C.1, S.3, <http://www.surveillance-and-society.org/journalv1i3.htm> (s.y. 23 Kasım 2008).

“Government Databases Have More Information than Needed to Solve Crimes”, haz. Electronic Privacy Information Center (EPIC), **DNA Databases**, Thomson & Gale, ABD 2007, s. 76-82.

A Report on the Surveillance Society, For the Informational Commisioner by the Surveillance Society Network, , haz. David Murakami WOOD, Eylül 2006.

AAS, Katja Franco, **Globalisation and Crime**, Sage, Birleşik Krallık 2007.

ABD, Terör ve İslam, 11 Eylül Üzerine, der. Ahmet DEMİRHAN, Vadi, Ankara 2001.

Access Denied: The Practice and Policy of Global Internet Filtering (Information Revolution and Global Politics), haz. DEIBERT, Ronald J., PALFREY, John G., ROHOZINSKI, Rafal, ZITTRAIN, Jonathan, The MIT Press, ABD 2008.

AHİ, M. Gökhan, “Mernis’in Hukuki İncelemesi”, <http://www.hukukcu.com/bilimsel/kitaplar/mernis.htm> .

- AKDENİZ, Yaman, “Anonymous Now”, **Index on Censorship**, Privacy Issue, S.3, Y.2000, s. 57-62.
- AKDENİZ, Yaman, **Beyaz Kitap**, Papatya, İstanbul 2003.
- AKDENİZ, Yaman; ALTIPARMAK, Kerem, **İnternet: Girilmesi Tehlikeli ve Yasaktır**, İmaj, Ankara 2008.
- AKILLIOĞLU, Tekin, "Bireyin Yönetmel İşlemler Karşısında Korunması ve Yönetim Hukukumuz", **Amme İdaresi Dergisi**, C. 14, S. 3 1981, s. 37-56.
- AKILLIOĞLU, Tekin, “İdari Usul ve Kişisel Verilerin Korunması”, 11 Ağustos 2004, www.idare.gen.tr/akkillioglu-idariusul.htm .
- AKILLIOĞLU, Tekin, “Yönetimde Açıklık-Gizlilik ve Bilgi Alma Hakkı”, **AÜSBFD**, C.46, S.3-4, Haziran-Aralık 1991, s.1-12.
- AKINCI, Müslüm, “ ‘Güvenlik Kayıtları’ ya da ‘Bilgi Fişleri’nin İdare Hukuku Bakımından Değerlendirilmesi”, **Bülent Tanör Armağanı**, Legal, İstanbul 2004, s. 31-51.
- AKİPEK, Jale; AKINTÜRK, Turgut, **Türk Medeni Hukuku (Yeni Medeni Kanuna Uyarlanmış Başlangıç Hükümleri, Kişiler Hukuku)**, C. I, 4. Baskı, Beta, İstanbul 2002.
- AKSOY, Muammer, “Güvenlik Soruşturması Denilen Hukuksal Sapıklığın, MİT Raporlarındaki Korkunç Yanlış ve Yalanlar Işığında Değerlendirilmesi”, **Bahri Savcı’ya Armağan**, Mülkiyeliler Birliği Yayınları no: 7, Ankara 1988.
- AKŞENER, Haşmet Sırrı; ÇAKMAKÇI, Ramazan, **Açıklamalı, Gerekçeli Bilgi Edinme Hakkı Kanunu**, Legal, İstanbul 2004.
- ALBRECHT, Katherine, McINTYRE, Liz, **Spychips, How Major Corporations and Government Plan to Track your Every Purchase and Watch Your Every Move**, A Plume Book, ABD 2006.
- ALIEFENDİOĞLU, Yılmaz, “Bir Temel İnsan Hakkı: Düşünce Özgürlüğü”, **Yeni Türkiye**, Y. 1998, S. 22, s. 804-813.
- Al-MIDANI, Mohammed Amin, CABANETTES, Matilde, AKRAM, Susan M., “Arab Charter on Human Rights 2004”, **Boston University International Law Journal**, C.24, Y. 2006, s. 147-164, http://www.acihl.org/res/Arab_Charter_on_Human_Rights_2004.pdf)

- ALTIPARMAK, Kerem, “Büyük Biraderin Gözetiminden Çıkış: Telefonların İzlenmesinde Devletin Sorumluluğu”, **Türkiye Barolar Birliği Dergisi**, S. 63, Mart-Nisan 2006, s. 29-66.
- ALTIPARMAK, Kerem; AYTAÇ, Ahmet Murat; KARAHANOGULLARI, Onur; HANÇER, Türkan; AYDIN, Devrim, “Polis Vazife ve Selahiyet Kanununda Değişiklik: Durdurma-Kimlik Sorma-Arama-Parmak İzi Alınması-Silah Kullanma”, **Hukuk ve Adalet**, S. 11, Y. 2007.
- AMSTUTZ, Marc, ve diğ., **Handkommenter zum Schweizer Privatrecht**, Schulthess 2007.
- ANDENAS, Mads; ZLEPTNIG, Stefan, “Surveillance and Data Protection: Regulatory Approaches in the EU and Member States”, **European Business Law Review**, Y. 2003, s. 765-813.
- ANNAS, George J., “Protecting Privacy and the Public-Limits on Police Use of Bioidentifiers in Europe”, **The New England Journal of Medicine**, 361;2, 9 Temmuz 2009, s. 196-201.
- ARAI-TAKAHASHI, Yutaka, **The Magrin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR**, Intersentia, Birleşik Krallık 2001.
- ARASLI, Oya, **Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi**, Ankara 1979 (yayımlanmamış doçentlik tezi).
- ARİFOĞLU, Ali, **E-Dönüşüm: Yol Haritası, Dünya**, Türkiye, Sas Bilişim, Ankara 2004.
- Arthur R. MILLER, **The Assault on Privacy, Computers, Data Banks, and Dossiers**, The University of Michigan Press, ABD 1971.
- ATEŞ, Leyla, “Meslek Mensuplarının Sır Saklama Yükümlülüğünü Özel Yaşamın Gizliliği ile Okumak”. **E-Yaklaşım**, Kasım 2003, S. 4, <http://www.yaklasim.com>.
- ATEŞ, Mustafa, **Fikir ve Sanat Eserleri Üzerindeki Hakların Kapsamı ve Sınırlandırılması**, Seçkin, Ankara 2003.
- AYDIN, Fazıl, “Vergi İstihbarat Arşivi”, **Vergi Sorunları**, S. 167, Ağustos 2002, s. 217-234.

- AYDIN, Selda, “Mükellefin Gizlilik Alanına (Sır Çevresine) İlişkin Hakları”, **Vergi Sorunları**, S. 213, Haziran 2006, s. 25-37.
- AYDIN, Ufuk, “İşverenin İşçi Özlük Dosyası Tutma Yükümü, **İş Hukuku ve Sosyal Güvenlik Hukuku Türk Milli Komitesi 30. Yıl Armağanı**, Ankara 2006, s. 491-505.
- BAINBRIDGE, David I., **EC Data Protection Directive**, Butterworths, Birleşik Krallık 1996.
- BALTHASAR, Stephan, **Der Schutz der Privatsphäre im Zivilrecht (Eine historisch-vergleichende Untersuchung zum deutschen, französischen und englischen Recht vom ius commune bis heute)**, Mohr Siebeck, Almanya 2006.
- BANISAR, David, “Freedom of Information and Access to Government Record Laws Around the World”, **The Freedominfo.org Global Survey**, s.6, http://www.freedominfo.org/documents/global_survey2004.pdf (s.y. 25 Şubat 2009).
- BANISAR, David, “Privacy and Data Protection Around the World”, s. 3, <http://www.pcpd.org.hk/english/infocentre/files/banisar-paper.doc> (s.y. 3 Nisan 2009).
- BANISAR, David, **Freedom of Information Around the World 2006, A Global Survey of Access to Government Information Laws**, Privacy International, ABD 2006.
- BARTOW, Ann, “Our Data, Ourselves: Privacy, Propertization and Gender”, **University of San Fransisco Law Review**, Y.2000, C.34, s. 633-704.
- BASHO, Kalindo, “The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?”, **California Law Review**, C. 88, Y. 2000.
- BAŞARAN, Funda, “Bankaların Bilgi Verme Yükümlülüğünün Sınırları ve Bilgi Vermekten Çekinmeye Bağlı Özel Usulsüzlük Suçu-Müşteri Sırrını Saklama Yükümlülüğü ile Özel Usulsüzlük Suçu Arasında Bir Gri Bölge”, **Vergi Sorunları**, S. 143, Ağustos 2000, s. 178-195.
- BAUMAN, Zygmunt, **Küreselleşme,(Toplumsal Sonuçları)**, Ayrıntı, 2. Baskı, İstanbul 2006.
- BELL, Daniel, **The Coming of Post-Industrial Society**, Basic Books, ABD 1973.

- BELL, John, **French Constitutional Law**, Clarendon Press, Birleşik Krallık 1998.
- BELLIA, Patricia L., BERMAN, Paul Schiff, POST, David G, **Cyberlaw, Problems of Policy and Jurisprudence in the Information Age**, Thomson-West, 2. Baskı, ABD 2003.
- BENIGER, James R., **The Control Revolution, Technolical and Economic Origins of the Information Society**, Harvard University Press, ABD 1989.
- BENNETT, Colin J., **Regulating Privacy, Data Protection and Public Policy in Europe and the United States**, Cornell University Press, ABD 1992.
- BERGKAMP, Lucas; DHONT, Jan, “Data Protection in Europe and the Internet: An Analysis of the European Community’s Privacy Legislation in the Context of the World Wide Web”, **The EDI Law Review**, s.7, Y. 2000, s. 71-114.
- BERMAN, Marshall, **Katı Olan Herşey Buharlaşıyor**, İletişim, 4. Baskı, İstanbul 2001.
- BERMANN, Sol, “Privacy and Access to Public Records in the Information Age”, **bepress Legal Series**, Y. 2006, <http://law.bepress.com/expresson/eps/1303> (s.y. 2 Mart 2008), s. 1-24.
- BEYLEVELD, Deryck, “The Duty to Provide Information to the Data Subject: Articles 10 and 11 of Directive 95/46/EC”, **The Data Protection Directive and Medical Research Across Europe**, Ashgate, İngiltere 2004, s. 69-88.
- BEYLİ, Ceylin, “Bilgi Toplumunda Kişisel Veriler- Kişisel Verilerin Korunması Kanun Tasarısı Üzerine Eleştiriler”, **Bilişim Hukuku**, Der. Mete Tevetoğlu, Kadir Has Üniversitesi Yayınları, İstanbul 2006, s.70-79.
- BIBAS, Steven A., “A Contractual Approach to Data Privacy”, **Harvard Journal of Law & Public Policy**, C.17, Y. 1994.
- BICKEL, Robert D.; BRINKLEY, Susan; WHITE, Wendy, “Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?”, **Stetson Law Review**, C. 33, Y. 2003-2004, s. 299-367.
- BIDGOLI, Hossein, **The Internet Encyclopedia** (Cilt II), John Wiley and Sons Inc., ABD 2003.

- BIEZER, Johann; MIEDBRANDT, Anja, “Die digitale Signatur im elektronischen Rechtsverkehr-Deutsches Signaturgesetz und Entwurf der; Europäischen Richtlinie”, **Handbuch zum Internet-Recht, Electronic Commerce, Informations-, Kommunikations- und Mediendienste**, haz. Detlef KRÖGEL, Marc A. GIMMY, Springer, Almanya 2000, s. 135-166.
- BİLDİRİCİ, Faruk, **Gizli Kulaklar Ülkesi**, İletişim, Ankara 2001.
- BİLGE, Mehmet Emin, **Ticari Sırların Korunması**, Asil Yayın, 2. Baskı, Ankara 2005.
- BİNARK, İsmet, **Arşiv ve Arşivcilik Bilgileri**, Başbakanlık Basımevi, no. 3, Ankara 1980.
- Blackwell’in Siyaset Bilimi Ansiklopedisi**, C.II, haz. Vernon BOGDANOR, Türkçe yayıma haz. Erhan YÜKSELCİ, çev. Erhan YÜKSELCİ, Sema YÜKSELCİ, Bülent PEKER, Ümit Yayıncılık, Ankara 2003.
- BLANPAIN, Roger; GESTEL, Marc Van, **Use and Monitoring of E-mail, Intranet and Internet Facilities at Work**, **Kluwer Law International**, Hollanda 2004.
- BLOUSTEIN, Edward J., “Privacy as an Aspect of Human Dignity”, New York University Law Review, Y.1964, C.39, S.5, s. 962-1007.
- BOND, Robert, **New Economy Equity (Navigating Security and Legal Issues in Digital Business)**, John Wiley & Sons, LTD, İngiltere 2002.
- BOYLE, James, “Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwire Censors”, **University of Cincinnati Law Review**, C.66, Y.1997, s.177-205.
- BOZKURT, Enver; ÖZCAN, Mehmet; KÖKTAŞ, Arif, **Avrupa Birliği Hukuku**, 3. Baskı, Asil Yayın, Ankara 2002.
- BREYER, Patrick, “Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with ECHR”, **European Law Journal**, C. 11, S. 3, Y. 2005, s. 365-375.
- BRIN, David, “Some Notes About Calamity and Opportunity”, (Bu yazı ilk kez 2001 yılında 11 Eylül saldırılarından kısa bir süre sonra yayınlanmıştır), <http://www.futurist.com/archives/society-and-culture/calamity-and-opportunity/> (s.y.: 12 Şubat 2009).

- BRIN, David, **The Transparent Society (Will Technology Force Us to Choose Between Privacy and Freedom)**, Addison-Wesley, ABD 1998.
- BROEDERS, Dennis, "The New Digital Borders of Europe", **International Sociology**, C. 22, S. 1, Y. 2007, s. 71-92.
- BURKERT, Herbert, "Freedom of Information and Electronic Government", **Governance and Information Technology, From Electronic Government to Information Government**, haz. Victor MAYER-SCHÖNBERGER, David LAZER, The MIT Press, İngiltere 2007, s. 125-143.
- BURNS FLOREY, Kitty, **Script and Scribble: the Rise and Fall of Handwriting**, Melville House, ABD 2009.
- BÜLLESBACH, Alfred; POULLET, Yves; Corien PRINS, **Concise European IT Law**, Kluwer Law International, Hollanda 2006, s. 122-123.
- BÜYÜKAY, Yusuf, "Gen Analizleri ve Mukayeseli Hukuktaki Düzenlemeler", **AÜEHFD**, C. 9, S. 3-4, Y. 2005, s. 355-382.
- BYGRAVE, Lee A., "Data Protection Law-Sweden: Balancing Data Protection and Freedom of Expression in the Context of Website Publishing-Recent Swedish Case Law", **Computer Law and Security Report**, C.18, S.1, s. 56-58. (Balancing Data Protection and Freedom of Expression)
- BYGRAVE, Lee A., "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", **International Journal of Law and Information Technology**, C.6, S.3, s. 247-284.
- BYGRAVE, Lee A., "Germany's Teleservices Data Protection Act", **Privacy Law and Policy Reporter**, C. 5, Y. 1998.
- BYGRAVE, Lee A., "International Agreements to Protect Personal Data", **Global Privacy Protection: The First Generation**, haz. James B. RULE, Graham GREENLEAF, Edward Elgar Publishing, Büyük Britanya 2008, s. 15-49.
- BYGRAVE, Lee A., "Privacy Protection in a Global Context-A Comparative Overview" , **Scandinavian Studies in Law**, Y. 2004, C. 47, s. 319-348, <http://folk.uio.no/lee/publications/Privacy%20in%20global%20context.pdf> (s.y. 20 Nisan 2009).

- BYGRAVE, Lee A., "Where have all the judges gone? Reflections on judicial involvement in developing data Protection law", **Privacy Law and Policy Reporter**, Y.2000,C.7,s.11-14, 33- 36.
- BYGRAVE, Lee A., **Data Protection Law, (Approaching Its Rationale, Logic and Limits)**, Kluwer Law International, Hollanda 2002.
- CADAUX, Louise, "Privacy: Our Future Under Close Surveillance", **Freedom of Expression (And New Communication Technologies)**, Haz. Mich  l   PAR  , Peter DESBARATAS, IQ Collectif, Kanada 1998.
- CAREY, Peter, **Data Protection, A Practical Guide to UK and EU Law**, Oxford University Press, 2. Baskı, B  y  k Britanya 2004.
- CASTELLS, Manuel, **Enformasyon   ađı: Enformasyon   ađı, Ekonomi, Toplum ve K  lt  r**, I. ve II. Cilt,   ev. Ebru KILI  , 2. Baskı, İstanbul Bilgi   niversitesi Yayınları, İstanbul 2004.
- CATE, Fred H., **Privacy in the Information Age**, Brookings Institution Press, ABD 1997.
- CAVOUKIAN, Ann, TAPSCOTT, Don, **Who Knows, Safeguarding Privacy in a Networked World**, McGraw-Hill, ABD 1997.
- CENTEL, Nur; ZAFER, Hamide, **Ceza Muhakemesi Hukuku**, 6. Baskı, Beta, İstanbul 2008.
- CERRAH, İbrahim, "Biliřim Teknolojileri ve Etik: Biliřim Teknolojilerinin G  venlik Hizmetinde Kullanımının 'Etik Boyutu' ve 'Sosyal' Sonu  ları", **Uluslararası Polislik ve İ   G  venlik**, Haz. T  lin G  nřen İ  Lİ, Fatih KARAOSMANOđLU, Nobel, Ankara 2003, s. 449-468.
- CHALMERS, Damien; TOMKINS, Adam, **European Union Public Law**, Cambridge University Press, Birleřik Krallık 2007.
- CHARLESWORTH, Andrew, "Clash of the Data Titans? US and EU Data Privacy Regulation", **European Public Law**, C. 6, S.2, Y. 2000, s. 253-274.
- CHARLESWORTH, Andrew, "The Governance of the Internet in Europe", **The Internet, Law and Society**, haz. Yaman AKDENİZ, Clive WALKER, David WALL, Pearson Education Limited, İngiltere 2000.
- CHECKLAND, Peter, SCHOLÉS, Jim, **Soft Systems in Action**, New York, John Wiley & Sons, 1990, s.330.

- CHISSICK, Michael; KELMAN, Alistair, **Electronic Commerce, Law and Practice**, 3. Baskı, Sweet and Maxwell, Büyük Britanya 2002.
- CHOMSKY, Noam, **11 Eylül**, çev. Dost KÖRPE, OM Şimdi, İstanbul 2002.
- CLAPHAM, Andrew, **Human Rights in Private Sphere**, Oxford University Press, ABD 1996.
- CLARKE, Roger, “Beyond the OECD Guidelines: Privacy Protection for the 21st Century,” 4 Ocak 2000, <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html> (s.y. 2 Şubat 2009).
- CLARKE, Roger, “Dataveillance: Delivering ‘1984’”, 9 Şubat 1993 <http://www.anu.edu.au/people/Roger.Clarke/DV/PaperPopular.html>, (s.y. 1 Şubat 2009).
- CLARKE, Roger, “Identified, Anonymous, Psedonymous Transactions: The Spectrum of Choise”, 30 Nisan 1999, <http://www.rogerclarke.com/DV/UIPP99.html> (s.y.: 6 Mart 2009).
- CLARKE, Roger, “Person Location and Person Tracking-Technologies, Risks and Policy Implications”, **Information Technology and People**, Y. 2001, C. 14, S. 2, s. 206-231.
- CLARKE, Roger, “Privacy and ‘Public Registers’”, **Adres to the IIR Conference on Data Protection and Privacy**, Mayıs 1997, <http://www.rogerclarke.com/DV/PublicRegisters.html> (s.y. 13 Mart 2008).
- COHEN, Julie E., “Examined Lives: Informational Privacy and the Subject as Object”, **Stanford Law Review**, C.52, Y.1999-2000, s. 1373-1438.
- COLUCCI, Michele, **The Impact of the Internet and New Technologies on the Workplace, A Legal Analysis from a Comparative Point of View**, Kluwer Law International, Hollanda 2002.
- Constitutional Rights and New Technologies**, A Comparative Study Covering Belgium, France, Germany, Sweden, and the United States, haz. Bert-Jaap KOOPS, Ronald LEENES, Paul de HERT, Tilburg, Şubat 2007, <http://www.voxinternet.fr/IMG/crant-report-2007def-1.pdf> (s.y. 20 Şubat 2009).

- Construction Project Data Exchange and Management Module,
<http://cig.bre.co.uk/dataexchange/subjectIntro/dataOrInformation.jsp>
(son yararlanma: 20.09.2007).
- CRAIG, Paul; BÚRCA, Gráinne de, **EU Law, Text, Cases, and Material**, 4. Baskı, Oxford University Press, ABD 2008.
- CREIFELDS, Carl, ve diğ., **Rechtswörterbuch**, Becks, Almanya 1997.
- CUSTER, Bart, “Tapping and Data Retention in Ultrafast Communication Networks”, **Cyberlaw Security & Privacy**, haz. Sylvia Mercado KIERKEGAARD, The Second International Conference on Legal, Security and Privacy Issues in Information Technology (LSPI) 2007 Çin, Ankara Barosu Yayınları, 2. Baskı, Ankara 2007, s. 289-300.
- ÇANKAYA, Hürol, **Biyoteknoloji ve İnsan Hakları**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Genel Kamu Hukuku Anabilim Dalı, yayınlanmamış doktora tezi, Ankara 2008.
- ÇAVUŞOĞLU, Naz, “Avrupa Konseyi: İnsan Hakları Avrupa Sözleşmesi’nin Denetim Sistemi”, **İnsan Hakları**, YKY, İstanbul 2000, s. 458-477.
- ÇINAR, Ülkü, “ ‘DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu Tasarısı’ Üzerine Bir Değerlendirme ve Öneriler”, **Terazi**, Y. 3, S. 21, Mayıs 2008, s. 147-156.
- ÇUBUKÇU, Faruk, **Bilgisayar Terimleri Sözlüğü**, V Yayınları, Ankara 1987.
- DALLMANN, Hans-Ulrich, “Niklas Luhmann’s System Theory as a Challenge for Ethics”, **Ethical Theory and Moral Practice**, C.1, S.1, Y.1998, s.85-102.
- DANDEKER, Christopher, **Surveillance, Power and Modernity, Bureucracy and Disipline from 1700 to the Present Day**, St. Martin’s Press, ABD 1990.
- DANZIGER, James D., DUTTON, William H., KLING, Rob, KRAEMER, Kenneth L., **Computers and Politics, High Technology in American Local Governments**, Columbia University Press, ABD 1982.
- DAVIES, Simon, **Big Brother, Britain’s Web of Surveillance and the New Technological Order**, Pan Books, İngiltere 1996.
- DAVIS, Gordon B, OLSON, Margrethe H., **Management Information Systems: Conceptual Foundations, Structure and Development**, 2. Baskı, Mc Graw-Hill, ABD 1985.

- DEAKIN, Simon; MORRIS, Gilliam S., **Labour Law**, 4. Baskı, Hart Publishing, ABD 2006.
- Dictionary of Computer and Internet Words**, Houghton Miffling Company, ABD 2001.
- DİJK, P. Van, HOOFF, G.J.H. Van, **Theory and Practice of the European Convention on Human Rights**, Kluwer Law International, Hollanda 1998.
- DİNÇ, Güney, **Güvensizlik Üçgeni (1402'likler, Fişleme, Güvenlik Soruşturması)**, Say, İstanbul 1987.
- DOĞRU, Osman, **İnsan Hakları Avrupa Mahkemesi İçtihatları**, Cilt I, Legal, İstanbul 2004.
- DONAY, Süheyl, **Ceza Mahkemesinde Yargılanan Vergi Suçları**, Beta, İstanbul 2008.
- DONAY, Süheyl, **Ceza Muhakemesi Kanunu Şerhi**, Beta, İstanbul 2009.
- DONAY, Süheyl, **Meslek Sırrının Açıklanması Suçu**, İstanbul Üniversitesi Yayını, İstanbul 1978. s. 25-54.
- DONOS, Pelopidas K., **Datenschutz, Prinzipien und Ziele, Unter Besonderer Berücksichtigung der Entwicklung der Kommunikations-und Systemtheorie**, Nomos, Almanya 1998.
- DOWINING, Douglas A., COVINGTON, Michael A., Melody Mauldin COVINGTON, **Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü**, çev. ve haz.: Boğaç ERKAN, Murat SONGÜR, 5. Baskı, Hacettepe-Taş, Ankara 1999.
- DÖNMEZER, Sulhi, **Basın ve Hukuku**, İÜY no. 2213, 4. Baskı, İstanbul 1976.
- DREIER, Horst ve diğ., **Grundgesetz Kommentar**, C.1 (Giriş, Madde 1-19), Mohr Siebeck, 2. Baskı, Almanya 2004.
- DUTERTRE, Gilles, **Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler**, Avrupa Konseyi Yayınları, Ankara 2007.
- DÜLGER, Murat Volkan, **Bilişim Suçları**, Seçkin, Ankara, 2004.
- EARLY, Lawrence, "Science, Technology and Human Rights: The Role of Data Protection", **Human Rights in the Twenty-first Century, A Global Challenge**, C.2, haz. Katleen E. MAHONEY, Paul MAHONEY, Maritus Nijhoff Publishers, Hollanda 1993, s.801-815.

E-Devlet Yolunda Türkiye, TBD, Ankara 2002.

EDWARDS, Chris; SAVAGE, Nigel, **Information Technology and the Law**, Macmillan Publishers, Birleşik Krallık 1986.

EDWARDS, Lilian, “Reconstructing Consumer Privacy Protection On-line: A Modest Proposal”, **International Review of Law, Computers and Technology**, Y.2004, C. 18, S. 3, s. 313-344.

EKEN, Musa, “Kamu Yönetiminde Gizlilik Geleneği ve Açıklık İhtiyacı”, **AİD**, C.27, S.2, Haziran 1994, s. 25-54.

EKİCİ, Şerafettin, **Özel Sektöre Açıldıktan Sonra Türk Telekomünikasyon Hukuku (Elektronik İletişim)**, Vedat, İstanbul 2006.

Elektronik Devlet Paneli, haz. Murat ERDAL, İÜSBF, 15 Ekim 2003.

Entscheidungen des Bundesverfassungsgerichts, C.65, Y. 1984, J.C.B.MOHR, Almanyada 1984, s.1-71.
http://www.datenschutz.rlp.de/downloads/bverfge_65_1_-_volkszaehlung.pdf.

ERBSCHLOE, Michael, VACCA, John, **Net Privacy (A Guide To Developing and Implementing an Ironclad Ebusiness Privacy Plan)**, McGraw-Hill, ABD 2001.

ERDAL, Murat, **Elektronik Devlet, E-Türkiye ve Kurumsal Dönüşüm**, Filiz, İstanbul 2004.

EROL, Haydar, **Gerekçeli, Açıklamalı, İçtihatlı Yeni Türk Ceza Kanunu**, Ankara 2005.

ESEN, Selin; GÖNENÇ, Levent, “Religious Information on Identity Cards: a Turkish Debate”, **Journal of Law and Religion**, C. 23, S. 2, Y. 2007 - 2008, s. 579-603.

ETZIONI, Amitai, “Identification Cards in America”, **Society**, C.36, S.5, Temmuz 1999, s.70-76.

ETZIONI, Amitai, “Introduction: Rights and Responsibilities Post 9/11”, **Rights vs. Public Safety After 9/11, America in the Age of Terrorism**, haz. Amitai ETZIONI, Jason H. MARSH, Rowmann & Littlefield, İngiltere 2003.

ETZIONI, Amitai, **The Limits of Privacy**, Basic Books, ABD 1999.

- FERRETTI, Federico, **The Law and Consumer Credit Information in the European Community, The Regulation of Credit Information Systems**, Routledge-Cavendish, ABD-Kanada 2008.
- FISCHER-HÜBNER, Simone, **IT Security and Privacy-Enhancing Security Mechanisms**, Springer 2001.
- FLAHERTY, David H., "On the Utility of Constitutional Rights to Privacy and Data Protection", **Case Western Reserve Law Review**, Y.1990, C.41, s.831-857.
- FLAHERTY, David H., **Privacy and Data Protection, An International Bibliography**, Mansell, Birleşik Krallık 1984.
- FLAHERTY, David H., **Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States**, The University of North Carolina Press, ABD 1992.
- FLENDROVSKY, Alexander, "The Scope of the Right to Access Under the Fundamental Right of Data Protection, Austrian Constitutional Court Judgement of October 2nd, 2007, (B227/05)", **International Constitutional Law Journal**, C. 2, S. 3, Y. 2008, s.213-217, <http://www.icl-journal.com>.
- FLORIDI, Luciano, "Information", **The Blackwell Guide to the Philosophy of Computing and Information**, haz. Luciano Floridi, Wiley-Blackwell, ABD 2003, s. 40-62.
- FLORIDI, Luciano, "Is Information Meaningful Data?" <http://citeseer.ist.psu.edu/cache/papers/cs/18292/http:zSzzSzwww.wolfson.ox.ac.ukzSz~floridizSzfi.pdf/is-information-meaningful-data.pdf>.
- FOUCAULT, Michel, **Hapishanenin Doğuşu, Gözetim Altında Tutmak ve Cezalandırmak**, çev. Mehmet Ali KILIÇBAY, 3. Baskı, İmge, Ankara 2006.
- FOWLER, James H., **Connected: The Suprising Power of Our Social Networks and How They Shape Our Lives**, ABD 2009.
- Francesca E. BIGNAMI, "Privacy and Law Enforcement in the European Union: The Data Retention Directive", **Chicago Journal of International Law**, C.8, S. 1, Y. 2007, s. 233-255.
- FRIEDRICH, Christian, "Fundamentals of Privacy", **Datenschutzaspekte im Umfeld des Pervasive Computing**, Prof. H.-U. HEISS, Prof. B. LUTTERBECK, Yaz 2004, <http://ig.cs.tu->

berlin.de/lehre/s2004/pvc/ablauf/01/Friedrich-PrivacyBackgroundtext-2004-07-21.pdf .

FUSTER, Gloria Gonzalez; PAEPA, Pieter, “Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects”, **Security versus Justice?**, haz. Elspeth GUILD, Florian GEYER, Ashgate, İngiltere 2008, s. 129-152.

GANDY, Jr.,Oscar H., **The Panoptic Sort, a Political Economy of Personal Information**, Westview Press, ABD 1993.

GARFINKEL, Simson, “Privacy and the New Technology”, **The Nation**, C. 8, S. 270, s.11.

GARFINKEL, Simson, **Database Nation, The Death of Privacy in the 21st Century**, O'Reilly, ABD 2000.

GARRIE, Daniel B., WONG, Rebecca, “The Future of Consumer Web Data: A European/US Perspective”, **International Journal of Law and Information Technology**, Y. 2006, C.15, S.2, s. 129-152.

GARTSKA, Hansjürgen, “Freedom of Information and Data Protection: The Data Collections of the Former East Germany State Security Service”, **Law, Justice and the State III: Problems in law**, haz. Arend SOETEMAN, Mikael M. KARLSSON, , Franz Steiner Verlag, Almanya 1995, s. 184-190.

GEDİK, Gülşen, “Vergi Mahremiyeti Kapsamındaki Bilgilerin Basında Yer Alması”, **Vergi Dünyası**, S. 317, Ocak 2008, s. 125-138.

GELLMAN, Robert, “Public Records: Access, Privacy, and Public Policy”, Center for Democracy and Technology, 21 Nisan 1995, <http://www.cdt.org/privacy/pubrecs/pubrec.html> (s.y.: 20 Şubat 2009).

GEMALMAZ, Mehmet Semih, **Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş**, 6. Baskı, Legal 2007.

GENÇCAN, Ömer Uğur, **Türk Medeni Kanunu (Bilimsel Açıklama-İçtihatlar-İlgili Mevzuat, Madde 1-184)**, 2. Baskı, Yetkin, Ankara 2007.

GENZ, Alexendar, **Datenschutz in Europa und den USA, Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung**, Deutscher Universitäts-Verlag, Almanya 2004.

- George ORWELL, **Bin dokuz yüz seksen dört**, çev. N. AKGÖREN, Can, İstanbul 1989.
- George ORWELL, **Nineteen eighty-four**, Penguin, Büyük Britanya 2000.
- Gerd WORFLAM, Birgit GAMPL, Peter GABRIEL, **The RFID Roadmap: The Next Steps for Europe**, Springer, Almanya 2008.
- GIDDENS, Anthony, **Siyaset, Sosyoloji ve Toplumsal Teori**, Metis, İstanbul 2000.
- GIDDENS, Anthony, **Sociology**, Polity Pres, 2. Baskı, Birleşik Krallık 1994.
- GIDDENS, Anthony, **The Nation-State and Violence (Volume Two of a Contemporary Critique of Historical Materialism)**, Polity Press, Birleşik Krallık 1996.
- GILLIOM, John, **Surveillance, Privacy and the Law, (Employee Drug Testing and the Politics of Social Control)**, The University of Michigan Press, ABD 1994.
- GILMORE, John, "Privacy, Technology and the Open Society", Conference on Computers, Freedom and Privacy, 28 Mart 1991, <http://www.toad.com/gnu/cfp.talk.txt> (s.y. 18 Şubat 2008).
- GİRİTLİ, İsmet; BİLGİN, Pertev; AKGÜNER, Tayfun, **İdare Hukuku**, 3. Baskı, Der, İstanbul 2008.
- GOLA, Peter, SCHOMERUS, Rudolf, **Bundesdatenschutzgesetz Kommentar**, Beck, Almanya 2007.
- GOOLD, Benjamin Jervis, **CCTV and Policing: Public Area Surveillance and Police Practices in Britain**, Oxford University Press, Büyük Britanya 2004.
- GORDLEY, James, **Foundations of Private Law (Property, Tort, Contract, Unjust Enrichment)**, Oxford University Press, Birleşik Krallık 2007.
- GORDLEY, James; MEHREN, Arthur Taylor Von, **An Introduction to the Comparative Study of Private Law (Readings, Cases, Materials)**, Cambridge University Press, Birleşik Krallık 2006.
- GÖKCAN, Hasan Tahsin; ARTUÇ, Mustafa, **Ceza ve Ceza Usul Hukukunda Kamu Görevlisi Kavramı ve Özel Soruşturma Usulleri**, Seçkin, Ankara 2007.
- GÖLCÜKLÜ, Feyyaz, GÖZÜBÜYÜK, Şeref, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, 3. Baskı, Turhan, Ankara 2002.

- GÖLCÜKLÜ, Feyyaz, **Haberleşme Hukuku, Basın-Radyo-TV**, AÜSBF Yayınları, No.292, Ankara 1970.
- GÖREN, Zafer, **Anayasa Hukukuna Giriş**, İzmir 1999.
- GÖZLER, Kemal, **İdare Hukuku Dersleri**, 5. Baskı, Ekin, Bursa 2007.
- GÖZÜBÜYÜK, Şeref; TAN, Turgut, **İdare Hukuku (İdari Yargılama Hukuku)**, C. 2, Turhan, Ankara 2006.
- GREENLEAF, Graham, “APEC Privacy Framework Completed: No Threat to Privacy Standards”, **Privacy Law and Policy Reporter**, S.5, Y. 2006, <http://www.worldlii.org/au/journals/PLPR/2006/5.html> .
- GROEBNER, Valentin, **Who Are You?, Identification, Deception, and Surveillance in Early Modern Europe**, Almanca’dan İngilizce’ye çev. Mark KYBURZ, John PECK, Zone Books, ABD 2007.
- GRUHN, Volker; WOLFF-MARTING, Vincent; KÖHLER, André; HAASE, Christian; KRESSE, Torsten; **Elektronische Signaturen in modernen Geschäftsprozessen**, Vieweg, Almanya 2007.
- GUADAMUZ, Andrés, “Habeas Data vs. European Data Protection Directive”, **Journal of Information Law and Technology**, Y. 2001, S.3, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/guadamuz (s.y. 20 Nisan 2009). (s.1-19)
- GUNTON, Tony, **Dictionary of Information Technology and Computer Science**, Penguin, Büyük Britanya 1992.
- GURAK, Laura J., **Persuasion and Privacy in cyberspace (The Online Protests over Lotus Market Place and the Clipper Chip)**, Yale University Press, ABD 1997.
- GÜLMEZ, Mesut, **Birleşmiş Milletler Sisteminde İnsan Haklarının Korunması**, Türkiye Barolar Birliği Yayınları, Ankara 2004.
- GÜLTAN, Seçkin, **Bilgi Toplumu Sürecinde Avrupa Birliği ve Türkiye**, AÜATAUM Araştırma Dizisi no. 19, Ankara 2003.
- GÜNDAY, Metin, **İdare Hukuku**, 9. Baskı, İmaj, Ankara 2004.
- GÜNEŞ, Gülşen; ŞİRİN, Ertunç, “Vergi Ödevlisinin Hakları”, **Vergi Sorunları**, S. 197, Şubat 2005, s. 135-145.

- GÜNUĞUR, Haluk, **Avrupa Birliği'nin Hukuk Düzeni**, Avrupa Ekonomik Danışma Merkezi, Ankara 2007.
- GÜNUĞUR, Haluk, **Avrupa Birliği'nin Kurucu Antlaşmaları**, Avrupa Ekonomik Danışma Merkezi, Ankara 2005.
- GÜRBÜZ USLUEL, Aslı E. **Türk Özel Hukukunda Özellikle Anonim Şirketlerde Ticari Sırrın Korunması**, Vedat, İstanbul 2009.
- HABERMAS, Jürgen, **İletişimsel Eylem Kuramı**, çev. Mustafa TÜZEL, Kabalcı, İstanbul 2001.
- HABERMAS, Jürgen, **Theorie des kommunikativen Handelns**, Cilt II, Schurkamp, 6. Baskı, Almanya 2006.
- HAFIZOĞULLARI, Zeki, **Ceza Özel Hukuku**, Yayına hazırlanıyor.
- HAFNER, Katie, LYON, Matthew, **İnternet Tarihi: Sihirbazların Gecelediği Yer**, çev. Sinem YAZICIOĞLU, Güncel, İstanbul 2000.
- HAGEL III, John, RAYPORT, Jeffrey F., "The Coming Battle for Customer Information", **Creating Value in the Network Economy**, Harvard Business Review Book Series, ABD 1999.
- HAKERİ, Hakan, **Tıp Hukuku**, Seçkin, Ankara 2007.
- HARRIS, David John, O'BOYLE, Michael, WARBRICK, Colin, **Law of the European Convention on Human Rights**, Butterworths, Birleşik Krallık 1995.
- HEISENBERG, Dorothee, **Negotiating Privacy, The European Union, The United States, and Personal Data Protection**, Lynne Rienner Publishers, Londra 2005.
- HELMS, Shawn C., "Translating Privacy Values with Technology", **Boston University Journal of Science and Technology Law**, C.7, Y.2001, s. 288-326.
- HELVACI, Serap **Gerçek Kişiler**, 2. Baskı, Arıkan, İstanbul 2007.
- HENDERSON, Harry, **Privacy in the Information Age**, Facts of File, ABD 2006.
- HERT, Paul De, GUTWIRTH, Serge, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", **Reinventing Data Protection**, haz. Serge GUTWIRTH, Yves POULLET, Cécile de TERWANGNE, Sjaak NOUWT, Springer 2009, s. 3-45.

- HERT, Paul de; GUTWIRTH, Serge, “Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power”, **Privacy and the Criminal Law**, haz. Erik CLAES, Anthony, DUFF, Serge GUTWIRTH, Intersentia, 2006, s. 61-109.
- HILL, David G., **Data Protection, Governance, Risk Management and Compliance**, CRC Press, ABD 2009.
- HIMMANEN, Pekka, **The Hacker Ethic and the Spirit of the Information Age**, Vintage, Büyük Britanya 2001.
- HIZ, Yüksel, YILMAZ, Zekeriya, **Bilgi Edinme ve Dilekçe Hakkı**, Seçkin, Ankara 2004.
- HOBBS, Thomas, **Leviathan, veya Bir Din ve Dünya Devletinin İçeriği, Biçimi ve Kudreti**, çev. Semih LİM, 4. Baskı, YKY, İstanbul 2004.
- HOFFMAN, Bruce, **Inside Terrorism**, Columbia University Press, 2. Baskı, ABD 2006.
- HOFSTADTER, Samuel H., HOROWITZ, George, **The Right of Privacy**, Central Book Company, ABD 1964.
- HOLLAND, Martin, **European Integration: From Community to Union**, Pinter Publishers, Birleşik Krallık 1993.
- HOLZNAGEL, Bonnekoh, “Radio Frequency Identification-Innovation vs. Datenschutz?”, **MMR**, 2006, Heft 1, s.17-24.
- HONDUS, Frits W., **Emerging Data Protection in Europe**, North-Holland Publishing Company, Hollanda 1975.
- HOOFNAGLE, Chris Jay, **Privacy Self-Regulation: A Decade of Disappointment**, 4 Mart 2005, <http://www.epic.org> , s. 7.
- HORNUNG, Gerrit; SCHNABEL, Christoph, “Data Protection in Germany I: The Population census decision and the right to informational self-determination”, **Computer Law and Security Report**, C. 25, S. 1, Y. 2009, s. 84-88.
- HOVEN, Jeroen Van Den, VERMAAS, Pieter E., “Nano-technology and Privacy: On Continuous Surveillance Outside the Panopticon”, **Journal of Medicine and Philosophy**, C.32, Y.2007, s. 283-297.
- HUGHES, Eric, “A Cypherpunk’s Manifesto”, 9 Mart 1993, <http://activism.net/cypherpunk/manifesto.html> , (s.y. 18 Şubat 2008).

- HUSTINX, Peter, “Data Protection in the Light of the Lisbon Treaty and the Consequences for Present Regulation”, **11th Conference on Data Protection and Data Security-DuD 2009**, Berlin 8 Haziran 2009, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2009/09-06-08_Berlin_DP_Lisbon_Treaty_EN.pdf , s. 1-10.
- HUSTINX, Peter, “The Role of Data Protection Authorities”, **Reinventing Data Protection**, haz. Serge GUTWIRTH, Yves POULLET, Paul de HERT, Cécile de Terwangne, Sjaak NOUWT, Springer, Almanya 2009.
- HUXLEY, Aldous, **Brave New World Revisited**, 1958, <http://www.huxley.net/bnw-revisited/index.html> (s.y. 30 Ocak 2009).
- HUXLEY, Aldous, **Brave New World**, Vintage Classics, Büyük Britanya 2004.
- HUXLEY, Aldous, **Cesur Yeni Dünya**, İthaki, İstanbul 2000.
- Implementation of the Data Protection Directive in Relation to Medical Research in Europe**, haz. Deryck BEYLEVELD, David TOWNEND, Ségolène ROUILLÉ-MIRZA, Jessica WRIGHT, Ashgate, İngiltere 2005.
- International Encyclopedia of Laws**, haz. R. BLANPAIN, **Constitutional Law**, C.3, haz. A. ALEN, Kluwer Law International, Hollanda 2000.
- İÇEL, Kayıhan, **Kitle Haberleşme Hukuku, Basın, Radyo-Televizyon, Sinema, İnternet**, 5. Baskı, Beta, İstanbul 2001.
- İLKİZ, Fikret, “Kişisel Verilerin Korunması ve Kanun Tasarsısı”, **Güncel Hukuk**, Y. 2009, S.7-67, s. 12-23.
- İnternet ve Hukuk**, der. Yeşim M. ATAMER, çev. İnternet ve Hukuk Platformu, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2004.
- İŞEVİ, A.Semih, ÇELME, Burçin, “Bilgi Çağında Yeni Hazine: Entelektüel Sermaye ile Rekabeti Yakalamak”, I. ÜNAK Genel Konferansı, **ÜNAK 2002**, 19 Mayıs Üniversitesi, Samsun, 10-12 Ekim 2002, Araştırma ve Teknoloji Genel Müdür Yardımcılığı, 2002 Ulusal ve Uluslar arası Bildiriler, Şişecam İstanbul 2002, (s.38-50), <http://eprints.rclis.org/archive/00005618/01/bilgidunyasiES.pdf> .
- İZGİ, Ömer; GÖREN, Zafer, **Türkiye Cumhuriyeti Anayasası Yorumu**, Ankara 2002.

- JACOBY, Nicole, “The Decision of the Bundesverfassungsgericht of April 12, 2005- Concerning Police Use of Global Position Systems as a Surveillance Tool”, **German Law Journal**, C. 6, S.7, Y. 2005.
- Jeremy Haris LIPSCHULTZ, **Free Expression in the Age of the Internet**, Social and Legal Boundaries, Westview Press, ABD 2000.
- JÓRI, András, “dataprotection.eu”, <http://www.dataprotection.eu/> .
- KABOĞLU, İbrahim Özden, “Bilim ve Sanat Özgürlüğü”, **İnsan Hakları**, YKY, İstanbul 2000, s. 121-134.
- KABOĞLU, İbrahim Özden, **Anayasa Hukuku Dersleri**, 2. Baskı, Legal, İstanbul 2005.
- KABOĞLU, İbrahim Özden, **Özgürlükler Hukuku, İnsan Haklarının Hukuksal Yapısı**, 6.Baskı, İmge, Ankara 2002.
- KAFKA, Franz, **Dava** (Oxford Metni), çev. Ahmet CEMAL, 5. Baskı, Can, İstanbul 2005.
- KAHN, Robert E., CERF, Vinton G., “What is the Internet (and What Makes it Work)”, Aralık 1999, <http://www.policyscience.net/cerf.pdf> .
- KANG, Jerry, “Information Privacy in Cyberspace Transactions”, **Stanford Law Review**, C. 50, Y. 1998, s. 1193-1294.
- KAPLAN, Yavuz, **İnternet Ortamında Fikri Hakların Korunmasında Uygulanacak Hukuk**, Seçkin, Ankara 2004.
- KARAHANOGULLARI, Onur, “Güvenlik Soruşturması”, **AÜSBFD**, C. 53, S. 1-4, Y. 1998, s. 159-185.
- KAYA, Cemil, **İdare Hukukunda Bilgi Edinme Hakkı**, Seçkin, Ankara 2005.
- KAYGUSUZ, Ziyaettin, “Olay Yeri İnceleme Çalışmalarında Bilimsellik ve Hukukilik”, **Polis Dergisi**, S.42, http://www.egm.gov.tr/egitim/dergi/eskisayi/42/makale/Ziyaettin_KAYGUSUZ.htm#_ftn27 .
- KAYMAZ, Seydi, **Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi**, Seçkin, Ankara 2009.
- KENNEDY, Gabriela, DOYLE, Sarah, LUI, Brenda ve diğ., “Data Protection in the Asia Pasific Region”, **Computer Law and Security Review**, Y. 2009, S. 25, s. 59-68.

- KERR, Orin S., “Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn’t”, **Northwestern University Law Review**, C. 97, Y. 2003, s. 607-637.
- KESER BERBER, Leyla, **İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza**, Yetkin, Ankara 2002.
- KESER BERBER, Leyla, Mahir M. ÜLGÜ, Cüneyd ER, **Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği**, İstanbul 2009.
- KESER BERBER, Leyla; LOSTAR, Murat, **Bilişimde Biyometrik Yöntemler**, Yetkin, Ankara 2006.
- KETİZMEN, Muammer, **Türk Ceza Hukukunda Bilişim Suçları**, Adalet, Ankara 2008.
- KETİZMEN, Muammer; ÜLKÜDERLER, Çağlar, “E-Devlet Uygulamalarında Kişisel Verilerin Korunma(ma)sı”, **XII. Türkiye’de İnternet Konferansı**, Bilkent Üniversitesi Güzel Sanatlar Fakültesi, 8-10 Kasım 2007, Ankara, haz. Mustafa AKGÜL, Ufuk ÇAĞLAYAN, Ethem DERMAN, Atilla ÖZGİT, Ankara 2007, s. 189-193.
- KHLERT, H., “Einheitliches Schutzniveau für personbezogene Daten in der Gemeinschaft”, **European Law Reporter**, 2003, s. 286-287.
- KILIÇOĞLU, Ahmet, **Borçlar Hukuku, Genel Hükümler**, Turhan, 7. Baskı, Ankara 2006.
- KING, Roger C., STANSFIELD, William D., **A Dictionary of Genetics**, Oxford University Press, 5. Baskı, Büyük Britanya 1997.
- KIZILARSLAN, Hakan, **Ceza Muhakemesi, Adli Tıp, Adli Bilimlerde Vücutun Muayenesi ve Örnek Alma**, Kızılarслан Serisi I, Ankara 2007.
- Kişisel Verilerin Korunması**, Türkiye Bilişim Derneği Kamu-BİB, 2. Çalışma Grubu, Nisan 2008, http://www.tbd.org.tr/resimler/ekler/8f0b864598a1291_ek.pdf.
- KLEVE, Pieter, MULDER, Richard De, “Privacy Protection and The Right to Information: In Search of a New Symbiosis in the Information Age”, **Cyberlaw Security & Privacy**, haz. Sylvia Mercado KIERKEGAARD, The Second International Conference on Legal, Security and Privacy Issues in

- Information Technology (LSPI) 2007, Beijing, Çin, Ankara Barosu Yayınları, 2. Baskı, Ankara 2007, s. 331-351.
- KLOSEK, Jaqueline, “European Court Establishes Broad Interpretation of Data Protection Law”, <http://library.findlaw.com/2004/Mar/19/133351.html> .
- KOOPS, Bert-Jaap, LEENES, Ronald, “ ‘Code’ and the Slow Erosion of Privacy”, <http://law.bepress.com/expresso/eps/625> (s.y. 2 Şubat 2009).
- KU, Raymond Shih Ray, “The Founders’ Privacy: The Fourth Amendment and the Power of Technological Surveillance”, **Minnesota Law Review**, C.86, Y.2001-2002, s. 1325-1378.
- KUMAR, Krishan, **From Post-Industrial to Post-Modern Society, New Theories of the Contemporary World**, Blackwell, Büyük Britanya 1997.
- KUNER, Christopher, **European Data Protection Law, Corporate Compliance and Regulation**, 2. Baskı, Oxford University Press, Büyük Britanya 2007.
- KUNTER, Nurullah; YENİSEY, Feridun; NUHOĞLU, Ayşe, **Muhakeme Hukuku Dahı Olarak Ceza Muhakemesi Hukuku**, 15. Baskı Beta, İstanbul.
- KURT, Levent, **Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Seçkin, Ankara 2005.
- KÜHLING, Jürgen, “Fundamental Rights”, **Principles of European Constitutional Law**, haz. Armin von BOGDANDY, Jürgen BAST, Hart Publishing, 2. Baskı, ABD 2007, s. 501-548.
- KÜHLING, Jürgen; SEIDEL, Christian; SIVRIDIS, Anastasios, **Datenschutzrecht**, Verlag Recht und Wirtschaft GmbH, Almanya 2008.
- KÜZECİ, Elif, **Basın Özgürlüğü ve İnternet**, (yayınlanmamış yüksek lisans tezi), Ankara 2004.
- LAUDON, Kenneth C., “Markets and Privacy, **Communication of the ACM**, C.39, S.9, Y.1996, s.92-104.
- LEATHERS, Daniel R., “Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement”, **Case Western Reserve Journal of International Law**, C. 41, S. 1, Y. 2009, s. 193-242.
- LEE, Laurie Thomas, “Privacy, Security, and Intellectual Property”, Understanding the Web, **Social, Political, and Economic Dimensions of the Internet**, haz.

- Alan B. ALBARRAN, David H. GOFF, Iowa State University Press, ABD 2000, s. 135-164.
- LEITH, Philip, "The Socio-legal context of Privacy", **International Journal of Law in Context**, C. 2, S. 2, Y. 2006, s. 105-136.
- LESSIG, Lawrence, "Privacy as Property", **Social Research: An International Quarterly of Social Sciences**, Y.2002, C.69, S.1, s. 247-269.
- LESSIG, Lawrence, **Code Version 0.2.**, Basic Books, ABD 2006.
- LEVI, Michael, WALL, David S., "Technologies, Security, and Privacy in the post-9/11 European Information Society", **Journal of Law and Society**, C.31, S.2, Y. 2004, s. 194-220.
- LIGERTWOOD, Julian; JACKSON, Margaret, "Transborder Data Protection and the Effects on Business and Government", **Usability and Internationalization, Global and Local User Interfaces**, haz. Nuray AYKIN, Springer, Almanya 2007, s. 140-149.
- LIPSCHULTZ, Jeremy Haris, **Free Expression in the Age of the Internet, Social and Legal Boundaries**, Westview Press 2000.
- LOO, Hans Van Der, Williem, REIJEN, Van, **Modernleşmenin Paradoksları**, İnsan Yayınları, İstanbul 2003.
- LYON, David, "9/11 Synopticon, and Scopophilia: Watching and Being Watched", **The New Politics of Surveillance and Visibility**, haz. Kevin D. HAGGERTY, Richard V. ERICSON, University of Toronto Press, Kanada 2006, s. 35-54.
- LYON, David, **Elektronik Göz, Gözetim Toplumunun Yükselişi**, çev. Dilek HATTATOĞLU, Sarmal, İstanbul 1997.
- LYON, David, **Günlük Hayatı Kontrol Etmek, Gözetlenen Toplum**, çev. Gözde SOYKAN, Kalkedon, İstanbul 2006.
- MAGEE, James, **Freedom of Expression**, Greenwood Press, ABD 2002.
- MALKOÇ, İsmail; YÜKSEKTEPE, Mert, **Açıklamalar ve Yorumlarla 5271 sayılı Yeni Ceza Muhakemesi Kanunu**, C. I, Malkoç 2008.
- MARTINO, Alessandra Di, **Datenschutz im europäischen Recht**, Nomos, Baden-Baden 2005.

- MARX, Gary T., “For Sale: Personal Information About You”, Washington Post, 11 Aralık 1989, bu makaleye ayrıca şu kaynaktan ulaşılabilir: <http://web.mit.edu/gtmarx/www/forsale.html> .
- MARX, Gary T., “The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures”, **The Social Fabric: Dimensions and Issues**, der. E., SHORT, Jr., ABD 1986.
- MARX, Gary T., **Undercover, Police Surveillance in America**, University of California Press, ABD 1988.
- MASUDA, Yoneji, **The Information Society as Post-Industrial Society**, 2. Baskı, World Future Society, ABD 1983.
- MATHIESEN, Thomas, “On the Globalisation of Control: Towards an Integrated Surveillance System in Europe”, **Criminal Policy in Transition**, haz. Penny GREEN, Andrew RUTHERFORD, Hart Publishing, Büyük Britanya 2000.
- MATHIESEN, Thomas, “The Viewer Society”, **Theoretical Criminology**, C.1, S.1, Y. 1997, s. 215-234.
- MATHIESEN, Thomas, **Silently Silenced, Essays on the Creation of Acquiescence in Modern State**, Waterside Press, Büyük Britanya 2004.
- MATSUURA, Jeffrey H., **A Manager’s Guide to the Law and Economics of Data Networks**, Artech House, ABD 2000.
- MAYER-SCHÖNBERGER, Viktor, “Generational Development of Data Protection in Europe”, **Technology and Privacy: The New Landscape**, haz. Philip E. AGRE, Marc ROTENBERG, MIT Press, ABD 1998.
- MAYER-SCHÖNBERGER, Viktor, BRANDL, Ernst O., **Datenschutzgesetz, Grundsätze und europarechtliche Rahmenbedingungen Gesetzestext mit Materialien, Datenschutz-Verordnungen und Richtlinien im Anhang**, 2. Baskı, Avusturya 2006.
- MEDKUS, Dieter, **Allgemeiner Teil des BGB**, 9. Baskı, C.F.Müller, Almanya.
- MEREDITH, Barbara, “Data Protection and Freedom of Information”, **BMJ**, Y.2005, S.330, s. 490-491, <http://www.bmj.com/cgi/reprint/330/7490/490.pdf> (s.y.: 22 Şubat 2009).
- MILLER, Arthur R., **The Assault on Privacy, Computers, Data Banks, and Dossiers**, The University of Michigan Press, ABD 1971.

- MOOS, Flemming, **Datenschutz-recht, Schnell Erfasst**, Springer, Almanya 2006.
- MOROZOVA, Darjia, “EU-US Passenger Name Record Data Transfer: Most Privacy Rights be a Casualty of the War on Terrorism”, **EuroJournal.org, Journal of Foreign Policy of Moldova**, S. 6, Y. 2004.
- MUMCU, Ahmet; KÜZECİ, Elif, **İnsan Hakları ve Kamu Özgürlükleri, Kavramlar, Evrensel ve Ulusal Gelişimleri, Bugünkü Durumları**, Turhan Kitabevi, 4. Baskı, Ankara 2007.
- MURPHY, Richard S., “Property Rights in Personal Information: An Economic Defence of Privacy”, **Georgetown Law Journal**, C.84,Y. 1995, s. 2381-2418.
- Münchener Kommentar zum Bürgerlichen Gesetzbuch**, C.1 (m.1-240), haz. Kurt REBMANN, Franz Jürgen SÄCKER, Roland RIXECKER, 4. Baskı, Beck, Almanya 2001.
- NAISBITT, John, ABURDENE, Patricia, **Megatrends 2000, Ten New Directions for the 1990's**, William Morrow and Company, Inc, ABD 1990.
- NAISBITT, John, **Megatrends, Ten New Directions Transforming Our Lives**, Warner Books, ABD 1988.
- NEISSER, Heinrich; VERSCHRAEGEN, Bea, **Die Europäische Union, Anspruch und Wirklichkeit**, Springer, Avusturya 2001.
- NELSON, Lisa S., “Constructing Policy: The Unsettled Question of Biometric Technology and Privacy”, **Privacy and Technologies of Identity, A Cross-Disciplinary Conversation**, haz. Katherine STRANBURG, Daniela Stan RAICU, Springer, ABD 2006.
- NICOL, Andrew, MILLAR, Gavin, SHARLAND, Andrew, **Media Law and Human Rights**, Oxford University Press, Birleşik Krallık 2001.
- NORRIS, Clive, ARMSTRONG, Gary, **The Maximum Surveillance Society: The Rise of CCTV**, Berg Publishers, ABD 1999.
- NTOUVAS, Ioannis, “Air Passenger Data Transfer to the USA: the Decision of the ECJ and Latest Developments”, **International Journal of Law and Information Technology**, C.16, S. 1, s. 72-95.
- OCCHIPINTI, John D., **The Politics of EU Police Cooperation, Toward a European FBI?**, Lynne Ryener Publishers, ABD 2003.

- ODER, Bertil Emrah, **Avrupa Birliği'nde Anayasa ve Anayasacılık**, Anahtar Kitaplar, İstanbul 2004.
- OĞUZMAN, Kemal, BARLAS, Nami, **Medeni Hukuk (Giriş, Kaynaklar, Temel Kavramlar)**, 15. Baskı, Vedat Kitapçılık, İstanbul 2008.
- ORTA, Mesut, **Elektronik İmza ve Uygulaması**, Seçkin, Ankara 2005.
- ORWELL, George, "Why I Write", 1946, <http://www.netcharles.com/orwell/essays/whyiwrite.htm> (s.y.: 6 Mart 2009).
- ÖKÇESİZ, Hayrettin, "Düşünce Özgürlüğü Üzerine Düşünceler", **Hukuk Felsefesi ve Sosyolojisi Arkivi**, Haz. Hayrettin ÖKÇESİZ, 6. Kitap, İstanbul Barosu Yayınları, İstanbul 2003, s. 28-36.
- ÖKÇESİZ, Hayrettin, "Düşünce Özgürlüğü", **İstanbul Barosu Dergisi**, Mart 1998, s. 23-26.
- ÖNDER, Evren, "GSM Şifresi Kırıldı: Artık Herkes Dinleyebilir", **NTV Bilim**, Şubat 2010, S. 12, s. 48-53.
- ÖZAY, İlhan, **Günışığında Yönetim**, Alfa, İstanbul 2002.
- ÖZBEK, Veli Özer, "Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, İstanbul, C.LIX, S.1-2,2001.
- ÖZBEK, Veli Özer, **Yeni Türk Ceza Kanunun Anlamı (Açıklamalı, Gerekçeli, İctihatlı)**, C. 2 (Özel Hükümler), Seçkin, Ankara 2008.
- ÖZDEMİR, Hayrunnisa, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin, Ankara 2009.
- ÖZDİLEK, Ali Osman, **İnternet ve Hukuk**, Papatya, İstanbul 2002.
- ÖZEK, Çetin, **Türk Basın Hukuku**, İÜY no. 2381, İstanbul 1978.
- ÖZGENÇ, İzzet, **Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler)**, 2. Baskı, Seçkin, Ankara 2005.
- ÖZTAN, Bilge, **Medeni Hukuk'un Temel Kavramları**, 8. Baskı, Turhan Kitabevi, Ankara 2002.
- ÖZTÜRK, Bahri; ERDEM, Mustafa Ruhan, **Uygulamalı Ceza Muhakemesi Hukuku**, 11. Baskı, Seçkin, Ankara 2007.

PEETERS, Maarten, “Identity Theft Scandals in the U.S. : Opportunity to Improve Data Protection”, **MMR**, Y. 2005 Heft 7, s. 415-420.

PIERSON, Christopher, **Modern Devlet**, çev. Dilek HATTATOĞLU, Çivi yazıları, İstanbul 2000.

Platform for Privacy Preferences (P3P) and the Open Profiling Standard(OPS), Working Party on the Protection of the Individuals with regard to the processing of Personal Data, Opinion 1/98, WP 11, 16 Haziran 1998.

POGGI, Gianfranco, **Modern Devletin Gelişimi, (Sosyolojik Bir Yaklaşım)**, çev. Şule KURT, Binnaz TOPRAK, İstanbul Bilgi Üniversitesi Yayınları, 2. Baskı, İstanbul 2002.

POLAT, Oğuz, **Klinik Adli Tıp, Adli Tıp Uygulamaları**, 2. Baskı, Seçkin, Ankara 2006.

Ponemon Institut and TRUSTe Announce Results of Annual Report Most Trusted Companies for Privacy Survey, http://www.truste.org/about/press_release/12_15_08.php (s.y. 6 Şubat 2009).

POSNER, Richard A., “Orwell versus Huxley: Economics, Technology, Privacy and Satire”, John M. OLIN Law and Economics Working Paper No.89, <http://www.law.uchicago.edu/Publications/Working/index.html> , s. 1-43.

POSNER, Richard A., “The Right of Privacy”, **Georgia Law Review**, C.12, Y. 1978 s.393-422.

POSTER, Mark, **The Second Media Age**, Polity Press, Büyük Britanya 1995.

POULLET, Yves, “EU data protection policy, The Directive 95/46/EC: Ten years after”, **Computer Law and Security Report**, 2006, s. 206-217.

POULLET, Yves; LOUVEAUX, Sophie; ASINARI, María Verónica Pérez, “Data Protection and Privacy in Global Networks: A European Approach”, Meda Conference, Atina, 25 Nisan 2001, **The EDI Law Review**, Y. 2001, S.8, s. 147-196.

POWER, Robert, “Changing Expectations of Privacy and Fourth Amendment”, **bepress Legal Series**, S. 1153, Y. 2006, <http://law.bepress.com/expresso/eps/1153> (s.y. 1 Mart 2008), s.1-28.

- Practices to Implement the OECD Privacy Guidelines on Global Networks**, OECD Working Papers, C. 6, S.97, Y.1998, s.6.
- PRINS J. E. J.; DELLEN, M. J. M. Van, **Digital Anonymity and the Law: Tensions and Dimensions**, Asser Press, ABD 2003.
- PRINS, Corien, "Property and Privacy: Perspectives and the Commodification of our Identity", **The Future of the Public Domain**, haz. L. GUIBAULT, P.B. HUGENHOLTZ, Kluwer Law International, Hollanda 2006, s.223-257.
- Privacy and Human Rights 2006, An International Survey of Privacy Laws and Developments**, Electronic Privacy Information Center and Privacy International, ABD 2007.
- PROSSER, William L., "Privacy", **California Law Review**, Y. 1960, C.48, S.3, s. 383-423.
- RACHELS, James, "Why Privacy Is Important?", **Philosophy and Public Affairs**, C.4, S. 4, Y. 1975, s. 323-333.
- RAUHOFER, Judith, "Intrusion in the Sphere of Personal Communications", **Socioeconomic and Legal Implications of Electronic Intrusion**, haz. Dionisios POLITIS, Phaedon KOZYRIS, Ionnis IGLEZAKIS, Information Science Reference, 2009, s. 25-46.
- REIDENBERG, Joel R., Paul M. SCHWARTZ, **Data Protection Law and On-line Services: Regulatory Responses**, http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/regul_en.pdf.
- Research Ethics Committees, Data Protection and Medical Research in European Countries**, haz. Deryck BEYLEVELD, David TOWNEND, Jessica WRIGHT, Ashgate, İngiltere 2005.
- RIEMER, Hans Michael, **Personenrecht des ZGB (Studienbuch und Bundesgerichtspraxis)**, Stämpfli, 2. Baskı, İsviçre 2002.
- ROBINS, Kevin, WEBSTER, Frank, **Times of the Technoculture, From the Information Society to the Virtual Life**, Routledge, Büyük Britanya 1999.
- ROSEN, Christine, "What Are the Benefits and Burdens of DNA Databases?", **DNA Databases**, Thomson & Gale, ABD 2007, s. 10-21.
- ROSEN, Jeffrey, **The Unwanted Gaze, The Destruction of Privacy in America**, Vintage Books, ABD 2001.

- ROTENBERG, Marc, "Privacy and Secrecy After September 11", **Minnesota Law Review**, Y. 2002, S.86, s.1115-1135.
- ROWLAND, Diane; MACDONALD, Elizabeth, **Information Technology Law**, 3. Baskı, Cavendish Publishing, ABD 2005.
- ROßNAGEL, Alexander, "Konflikte Zwischen Informationsfreiheit und Datenschutz?", **MMR**, 2007, Heft 1, s.16-21.
- ROßNAGEL, Alexander, SCHOLZ, Philip, "Datenschutz durch Anonymität und Pseudonimität-Rechtsfolgen der Verwendung anonymer und psedonymer Daten", **MMR** 2000, Heft 12, s. 721-731.
- ROßNAGEL, Alexander, ve diğ., **Handbuch Datenschutzrecht, Die Neuen Grundlagen für Wirtschaft und Verwaltung**, Verlag C.H. Beck, Almanya 2003.
- SAID, Edwar, "Şüphencilğin Zorunluluğu, Geri Tepki ve Geriye Dönüş", **ABD, Terör ve İslam, 11 Eylül Üzerine**, der. Ahmet DEMİRHAN, Vadi, Ankara 2001, s. 29-36.
- SALAVERRIA, Leila, "SC Drafting Writ of Habeas DataInvoking Right to Truth", 31 Ağustos 2007, Inquirer.net, http://newsinfo.inquirer.net/inquirerheadlines/nation/view/20070831-85704/SC_drafting_writ_of_habeas_data_invoking_right_to_truth (s.y. 23 Nisan 2009).
- SAMUELSON, Pamela, "Privacy as Intellectual Property?", **Stanford Law Review**, C.52, Mayıs 2000, s.1125-1173.
- SANCAR, Mithat, "Düşünce Özgürlüğü: Neden?", **Çağdaş Hukuk**, Mayıs-Haziran 1994, s. 8-13.
- SANCAR, Mithat, "Kalıcı Global Olağanüstü Hal", **Birikim**, Kasım 2001, S.151, s.12-21.
- SAYGILI, Abdurrahman, "Mikro-İktidarın Bir Fiziği: Hapishane", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C.53, S.2, Y.2004.
- Sayısal Haklar Yönetimi(DRM)**, İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi, İstanbul 2006, http://bthukuku.bilgi.edu.tr/documents/DRM%20rapor%20son_temiz%20versiyon.pdf

- SCHAAR, Peter, **Das Ende der Privatsphäre, Der Weg in die Überwachungsgesellschaft**, Goldmann, Almany 2009.
- SCHAAR, Peter, **Datenschutz im Internet, Die Grundlagen**, Verlag C.H. Beck, Almany 2002.
- SCHAUB, Günter; KOCH, Ulrich; LINCK, Rüdiger; VOGELSANG, Hinrich, **Arbeitsrecht-Handbuch**, Almany 2007.
- SHELLEKENS, M. H. M., **Electronic Signature, Authentication Technology from a Legal Perspective**, Asser Press, Hollanda 2004.
- SCHMITZ, Thomas, “Die EU-Grundrechtecharta aus grundrechtsdogmatischer und grundrechtstheoretischer Sicht”, **Juristenzeitung**, Y. 2001, s. 833-843.
- SCHNEIER, Bruce, **Secrets and Lies, Digital Security in a Networked World, (with new information about post-9/11 security)**, Wiley, ABD 2004.
- SCHOEMAN, Ferdinand, “Privacy: Philosophical Dimensions of the Literature”, **Philosophical Dimensions of Privacy**, haz. Ferdinand David SCHOEMAN, Cambridge University Press, ABD 1984.
- SCHREURS, Wim; HILDEBRANDT, Mireille; KINDT, Els; VANFLETEREN, Michaël, **Profiling the European Citizen, Cross-Disciplinary Perspectives**, haz. Mireille HILDEBRANDT, Serge GUTWIRTH, Springer, 2008, s. 241-270.
- SCHWARTZ, Paul M., “Internet Privacy and the State”, **Connecticut Law Review**, Y.2000, C. 32, s. s.815-859.
- SCHWARTZ, Paul M., “Property, Privacy and Personal Data”, **Harvard Law Review**, S.117, Y.2003-2004, s. 2055-2128.
- SCHWENKE, Matthias Christoph, **Individualisierung, Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung**, Deutscher Universitäts-Verlag, Almany 2006.
- SENCER, Muzaffer, **Belgelerle İnsan Hakları**, Beta, İstanbul 1988.
- SERRANO, Vanessa, “Comment: The European Court of Justice’s Decision to Anul the Aggrement Between the United States and European Community Regarding the Transfer of Personal Name Record Data, Its Effects, and Recommendations for a New Solution”, **ILSA Journal of International and Comparative Law**, S.13, Y. 2006-2007.

- SEVER, Hayri, TONTA, Yaşar, “Arama Motorları”, **Türkiye Bilişim Ansiklopedisi**, haz. Tuncer ÖREN, ÜNEY, Tuncer, ÇÖLKESEN, Rifat, Papatya, İstanbul 2006, s. 95-99.
- SEVİMLİ, K. Ahmet, **İşçinin Özel Yaşamına Müdahalenin Sınırları**, Legal, İstanbul 2006.
- SEZGİNER, Murat, “İdari Belgelere Ulaşma Hakkı-Fransa Örneği”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Prof. Dr. Süleyman Arslan’a Armağan, C.6, S.1-2, 1998, s.299-343.
- SHAW, Jo, **Law of the European Union**, 3. Baskı, Palgrave Macmillan, Büyük Britanya 2000.
- SIMITIS, Spiros, “Die informationelle Selbstbestimmung-Grundbedingung einer verfassungskonformen Informationsordnung”, **NJW**, Heft 8, Y. 1984, s. 398-405.
- SIMITIS, Spiros, “From the Market to the Polis: The EU Directive on Protection of Personal Data”, **Iowa Law Review**, C.80, Y. 1994.
- SIMITIS, Spiros, “Übermittlung der Daten von Flugpassagieren in die USA: Dispens vom Datenschutz?” **Neue Juristische Wochenschrift** 2006, Heft 28, s. 2011-2014.
- SIMITIS, Spiros, **Revisiting Sensitive Data**, 1999, http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/ , s. 1-11.
- SINAR, Hasan, **İnternet ve Ceza Hukuku**, Beta, İstanbul 2001.
- SMITH, David, “The Supervisory Authority: Ombudsman or Regulator”, Proceedings of the Council of Europe Conference on Data Protection, Varşova, 19-20 Kasım 2001, [http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/events/conferences/2DP\(2001\)Proceedings_Warsaw_EN.pdf](http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/events/conferences/2DP(2001)Proceedings_Warsaw_EN.pdf) .
- SOLOVE, Daniel J., “Access and Aggregation: Public Records, Privacy and the Constitution”, **Minnesota Law Review**, C. 86, Y. 2001-2002, s.1137-1218.
- SOLOVE, Daniel J., “Reconstruncting Electronic Surveillance Law”, **The George Washington Law Review**, C. 72, Y. 2004, s. 1264-1305.

- SOLOVE, Daniel J., **The Digital Person, Technology and Privacy in the Information Age**, New York University Press, ABD 2004.
- SONSUZOĞLU, Elif, “Çeşitli Yasalar Açısından Vergi Mahremiyetine İlişkin Düzenlemelerin Değerlendirilmesi”, **Vergi Sorunları**, Haziran 2000, S. 141, s. 116-134.
- SOYKAN, Cavidan, “Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı”, <http://auhf.ankara.edu.tr/dergiler/auhfd-arsiv/AUHF-2007-56-02/AUHF-2007-56-02-soykan.pdf> (s.y.: 26 Şubat 2009).
- SOYSAL, Mümtaz, **100 Soruda Anayasanın Anlamı**, Gerçek Yayınevi, 6. Baskı, İstanbul 1986.
- SPEICHERT, Horst, **Praxis des It-Rechts, Praktische Rechtsfragen der It-Sicherheit und Internetnutzung**, 2. Baskı, Vieweg + Teuber, Almanya 2008.
- SPIES, Axel, “USA: Datenschutz im Internet”, **Multimedia und Recht**, 2002, Heft 7, s. 12-13.
- SPYROPOULOS, Phillipos C.; FORTSAKIS, Theodore P., **Constitutional Law in Greece**, Kluwer Law International, Hollanda 2009.
- STAPLES, William G., **Encyclopedia of Privacy**, Greenwood Pres, ABD 2007.
- STEEVES, Valerie, “Privacy, Free Speech and Community: Applying Human Rights Law to Cyberspace”, **Human Rights and the Internet**, Macmillan Press, Birleşik Krallık 2000, s.187-199.
- STIGLER, George J., “An Introduction to Privacy in Economics and Politics”, **Journal of Legal Studies**, C.9, Y.1980, s.623-644.
- STROSS, Randall, **Planet Google: One Company’s Audacious Plan to Organize Everything We Know**, Simon and Schuster, 2009.
- STURCKE, James, “DNA Pioneer Alec Jeffreys: drop innocent from database”, **The Guardian**, 15 Nisan 2009. Hükümetin 7 Ağustos 2009’a kadar kamunun görüşüne açtığı konuya ilişkin raporu için bkz. Keeping the Right People on the DNA Database, Science and Public Protection, Homeoffice, Mayıs 2009, <http://www.homeoffice.gov.uk/documents/cons-2009-dna-database/dna-consultation?view=Binary>.
- SUNAY, Reyhan, **İfade Özgürlüğünün Muhtevası ve Sınırları**, Liberal Düşünce Topluluğu, Ankara 2001.
- SUN-TZU, **The Art of War**, Oxford University Press, Büyük Britanya 1971.

- SÜZEK, Sarper, **İş Hukuku**, 4. baskı, Beta, İstanbul 2008.
- SWIRE, Peter P.; LITAN, Robert E., **None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive**, the Brookings Institution Press, ABD 1998.
- Şafak N. EREL, **Türk Fikir ve Sanat Hukuku**, İmaj, 2. Baskı, Ankara 1998.
- ŞAHİN, Cumhur, **Ceza Muhakemesi Kanunu Gazi Şerhi**, Seçkin, Ankara 2005.
- ŞEN, Ersan, **Türk Hukukunda Telefon Dinleme, Gizli Soruşturmacı, X Muhbir**, 3. Baskı, Seçkin, Ankara 2009.
- ŞİMŞEK, Oğuz, **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta, İstanbul 2008.
- TANÖR, Bülent, **Türkiye'nin İnsan Hakları Sorunu**, BDS Yayınları, 3. Baskı, İstanbul 1994.
- TANSUĞ, Avniye, "AB'nin Yeni Ekonomi Silahı: "Veri Saklama Hukuku", **Bilişim Hukuku**, der. Mete TEVETOĞLU, Kadir Has Üniversitesi Yayınları, İstanbul 2006.
- TARHANLI, Turgut, "Birleşmiş Örgütü ve İnsan Haklarının Korunmasına İlişkin Başlıca Usuller", **İnsan Hakları**, YKY, İstanbul 2000, s. 407-436.
- TBMM'de Temsil Edilen Siyasi Partilerin Anayasa Değişikliği Tekliflerinin Karşılaştırmalı Metinleri**, TBMM Başkanlığı, Ankara Mart 1993.
- TEKİNALP, Ünal, **Fikri Mülkiyet Hukuku**, 2. Baskı, Beta, İstanbul 2002.
- TENE, Omer, "Is Israel Data Protection Law 'Adequate' Under Article 25", **Privacy and Data Protection**, C.8, S.5, Y. 2008, s. 9-13.
- TEZCAN, Durmuş, "Bilgisayar Karşısında Özel Hayatın Korunması", **Anayasa Yargısı Dergisi**, Y.1991, C.8, s. 385-392.
- TEZCAN, Ercüment, **Avrupa Birliği Hukukunda Birey**, İletişim, İstanbul 2002.
- The Age of Terror**, Amerika and the World After September 11, haz. Strobe TALBOTT, Nayan CHANDA, Basic Books, ABD 2001.
- The Internet of Things, First International Conference**, IOT 2008 Zurich, Switzerland, March 2008 Proceedings, haz. Christian FLOERKEMEIER, Marc LANGHEINRICH, Elgar FLEISCH, Friedemann MATTERN, Sanjay E. SARMA, Springer, Almany 2008.

- TINNEFELD, Marie-Theres, EHMANN, Eugen, GERLING, Rainer W., **Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht**, 4. Baskı, Oldenbourg Verlag, Münih 2005.
- TOFLER, Alvin, **Üçüncü Dalga**, çev. Ali SEDEN, Altın Kitaplar Yayınevi, İstanbul 1981.
- TOPALOĞLU, Mustafa, **Bilişim Hukuku**, Karahan, Adana 2005.
- TOROSLU, Nevzat, “Medya ve Hukuk: Basın Özgürlüğü ve Sınırları”, **Medya Gücü ve Demokratik Kurumlar**, haz. Korkmaz ALEMDAR, Afa, İstanbul 1999.
- TORTOP, Nuri, “İletişim ve Bilgi Edinme Hakkının Önemi”, **AİD**, C.37, S.1, Mart 2004, s.29-44.
- TOURAINÉ, Alain, **Return of the Actor, Social Theory in Postindustrial Society**, University of Minnesota Press, ABD 1988.
- TOWNEND, David, “Overriding Data Subjects’ Rights in the Public Interest”, **The Data Protection Directive and Medical Research Across Europe**, Ashgate, İngiltere 2004.
- TUOR, Peter; SCHNYDER, Berhard; SCHMID, Jörg; RUMO-JUNGO, Alexandra, **Das Schweizerische Zivilgesetzbuch**, 13. Baskı, Schulthess, İsviçre 2009.
- Türk Hukukunda Hekimin Hukuki ve Cezai Sorumluluğu**, Mukayeseli Hukuk Araştırma ve Uygulama Merkezi, Sorumluluk Hukukunda Yeni Gelişmeler V. Sempozyumu, Ankara 12-13 Mart 1982, Fakülteler Matbaası, İstanbul 1983.
- Türkiye Bilişim Ansiklopedisi**, haz. Tuncer ÖREN, Tuncer ÜNEY, Rıfat ÇÖLKESEN ve diğ., Papatya, İstanbul 2006.
- Türkiye Cumhuriyeti Anayasa Önerisi**, Türkiye Barolar Birliği, Geliştirilmiş Gerekçeli Yeni Metin, 4. Baskı, Kasım 2007 Ankara.
- Türkiye Odalar ve Borsalar Birliği TC Anayasa Önerisi** Anayasa 2000, Ankara 2000.
- TWOMEY, David P., **Labour and Employment Law, Text and Cases**, 11. Baskı, West, ABD 2001.
- TYSON, Peter, “The Hippocratic Oath Today”, <http://www.pbs.org/wgbh/nova/doctors/oath.htm> .

- UERPMMANN-WITZACK, Robert, “Personal Rights and Prohibition of Discrimination”, **European Fundamental Rights and Freedoms**, haz. Dirk EHLERS, Ulrich BECKER, De Gruyter Rechtswissenschaften Verlags-GmbH, Almanya 2008.
- ULUŞAHİN, Nur, “İnsan Onuru Kavramı Temelinde Mahremiyet, İfade Özgürlüğü ve Medya”, **II. Ulusal Uygulamalı Etik Kongresi Bildiriler Kitabı, 18-20 Ekim 2006**, Ankara 2007, s.675-682 .
- UYGUN, Oktay, “İnsan Hakları Açısından Yeni Anayasa Çalışmaları”, Maltepe Üniversitesi Hukuk Fakültesi’nde 28 Nisan 2008 tarihinde düzenlenen “Güncel Anayasa Sorunları” başlıklı sempozyumda sunulan bildiri metni.
- UYGUN, Oktay, “İnsan Hakları Kuramı”, **İnsan Hakları**, YKY, İstanbul 2000, s. 13-44.
- ÜSKÜL, Zafer, **Geniş Tabanlı Bir Uzlaşma Anlayışı için Karşılaştırmalı Anayasa Taslağı ve Anayasa Anketi**, Yayın no. 1, Toplumda Diyalog Forumu, Nisan 1992.
- ÜZELTÜRK, Sultan, **1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı**, Beta, İstanbul 2004.
- VIETHEN, Alexander, **Datenschutz als Aufgabe der EG-Bestandsaufnahme des datenschutzspezifischen Sekundärrechts und Analyse anhand der Kompetenzordnung des EG-Vertrages**, Kölner Schriften zum Internationalen und Europäischen Recht Band 5, LIT Verlag, Almanya 2003.
- WADE, William; FORSYTH, Christopher, **Administrative Law**, 8. Baskı, Oxford University Press, Büyük Britanya 2000.
- WALETZKO, Katja, **Der gläserne Passagier - Datenüberwachung im amerikanischen Flugverkehr**, GRIN Verlag, Almanya 2007.
- WALKER, Clive, AKDENİZ, Yaman, “Anti-Terrorism Laws and Data Retention: War is Over?”, **Northern Ireland Legal Quarterly**, C.54, S.2, Y. 2003, s. 159-182.
- WARREN, Samuel D., BRANDEIS, Louis D., “The Right to Privacy”, **Harvard Law Review**, C. 4, S.5, 15 Aralık 1890, s.194-221.
- WATERS, Nigel, “Can the Media and Privacy Ever Get On?”, **Privacy Law and policy Reporter**, Y. 2002, C.8, S.8,

<http://www.austlii.edu.au/au/journals/PLPR/2002/1.html> (s.y. 20 Şubat 2009).

- WEBSTER, Frank, **Theories of the Information Society**, Routledge, 1995.
- WELLS BRANSCOMB, Anne, **Who Owns Information? From Privacy to Public Access**, Basic Books, ABD 1994.
- WESTBY, Jody R., **International Guide to Privacy**, American Bar Association, ABD 2005.
- WESTIN, Alan F., **Privacy and Freedom**, Atheneum, ABD 1970.
- WHITAKER, Reg, **The End of Privacy, How Total Surveillance Is Becoming a Reality**, The New Press, ABD 1999, s. 40-41.
- WINKEL, Olaf, "The Democratic Potentials of Interactive Information Technologies under Discussion-Problems, Viewpointts, and Perspectives", **Elektronische Demokratie (Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis)**, haz. Bernd Holznagel, Andreas Grünwald, Anika Hanssmann.
- WINKLER, Roland, **Die Grundrechte der Europäischen Union**, Springer, Avusturya 2006.
- WINN, Jane K.; WRIGHT, Benjamin, **Law of Electronic Commerce**, 4. Baskı, Aspen Law & Business, ABD 2000.
- WITT, Bernhard C., **Datenschutz Kompakt und Verständlich, Eine praxisorientierte Einführung**, Vieweg, Almanya 2008.
- WOHLGEMUTH, Hans H., GERLOFF, Jürgen, **Datenschutzrecht, Eine Einführung mit praktischen Fällen**, 3. Baskı, Almanya 2005.
- WONG, Rebecca, "Data Protection Online: Alternative Approaches to Sensitive Data", **Journal of International Commercial Law and Technology**, C.2, S. 1, Y. 2007, <http://www.jiclt.com>.
- WRIGHT, Steve, "Political Control and the Internet", **Human Rights and the Internet**, haz. Steven HICK, HALPIN, Edward F., HOSKINS, Eric, Macmillan Press, Büyük Britanya 2000, s. 200-210.
- YALTI, Billur, **Vergi Yükümlüsünün Hakları**, Beta, İstanbul 2006.
- YAP, Ji Lian, "The Regulation of Data Privacy in Hong Kong", **Cyberlaw, Security and Privacy**, haz. Sylvia Mercado KIERKEGAARD, The Second Conference

- on Legal, Security and Privacy Issues in Information Technology (LSPI) 2007, China, 2. Baskı, Ankara Barosu Yayınları, Ankara 2007.
- YAZICI, Serap, **Yeni Bir Anayasa Hazırlığı ve Türkiye, Seçkincilikten Toplum Sözleşmesine**, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2009.
- YOUNG, Jason M., “Condtitutional Rights and New Technologies in Canada”, **Constitutonal Rights and New Technologies, A comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States**, haz. Bert-Jaap KOOPS, Ronald LEENES, Paul De HERT, Tilburg University, Hollanda 2007.
- YOUROW, Howard Charles, **The Magrin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence**, Martinus Nijhoff Publishers, Hollanda 1996.
- ZEVKLİLER, Aydın, ACARBAY, Beşir, GÖKYAYLA, Emre, **Medeni Hukuk**, 6. Baskı, Seçkin, Ankara 1999.
- ZEVKLİLER, Aydın, **Medeni Hukuk (Giriş, Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku)**, haz. Aydın ZEVKLİLER, Beşir ACABEY, Emre GÖKYAYLA, 6. Baskı, Seçkin, Ankara 1999.
- ZITTRAIN, Jonathan, “What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication”, **The Berkman Center for Internet & Society at Harvard Law School, Research Publication No. 2000-01**, <http://cyber.law.harvard.edu/publications> (s.y. 11.11.2007).

II. BELGE, GÖRÜŞ, ARAŞTIRMA VE RAPORLAR

- “FNC Resolution of ‘Internet’”, 24 Ekim 1995, http://www.itrd.gov/fnc/Internet_res.html .
- “From Cradle to Grave: Government Records and Privacy”, Privacy Rights Clearinghouse, <http://www.privacyrights.org/fs/fs11-pub.htm> (s.y.: 20 Şubat 2009).
- “Video Surveillance”, Electronic Privacy Information Center, <http://epic.org/privacy/surveillance/> .
- “Whole Body Imaging Technology and Body Scanners”; Electronic Privacy Information Center, <http://epic.org/privacy/airtravel/backscatter/>.

Almost half of all Internet users now use search engines on a typical day, haz. Deborah Fallows, 6 Ağustos 2008, http://www.pewinternet.org/~media/Files/Reports/2008/PIP_Search_Aug08.pdf.pdf.

Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union, Article 29 Data Protection Working Party, WP 106, 18 Ocak 2005.

Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı, İnternet ve Hukuk Platformu, Ankara Barosu, Ankara 2006.

Birleşmiş Milletlerde İnsan Hakları Yorumları, İnsan Hakları Komitesi ve Ekonomik, Sosyal ve Kültürel Haklar Komitesi, 1981-2006, der. ve çev. Lema UYAR, İnsan Hakları Hukuku Çalışmaları, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2006.

BUTTARELLI, Giovanni, **Protection of personal data with regard to surveillance (2000) and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance**, http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/.

Children's Privacy Online: The Role of Parental Consent, International Working Group on Data Protection in Telecommunications Working Paper, adopted at the 31st meeting, Auckland (New Zealand), 26-27 Mart 2002.

Common Position on data protection aspects in the Draft convention on cyber-crime of the Council of Europe, International Working Group on Data Protection in Telecommunications, 13-14 Eylül 2000, http://www.datenschutz-berlin.de/attachments/218/cy_en.pdf.

Common Position on Essentials for privacy-enhancing Technologies (e.g. P3P) on the World Wide Web, International Working Group on Data Protection in Telecommunications, adopted at the 23rd meeting in Hong Kong SAR, China, 15 Nisan 1998.

Common Statement on Cryptography, International Working Group On Data Protection in Telecommunications 12 Eylül 1997.

Cyrtography and Liberty 2000, An International Survey of Encryption Policy, Electronic Privacy Information Center, Washington DC, ABD 2000.

Declaration of Civil Society Organizations on the Role of Data Protection and Privacy Commissioners, Montréal, September 25, 2007, <http://thepublicvoice.org/events/montreal07/declaration.pdf> par. 8.

Declaration of the Article 29 Working Party on Enforcement, Article 29 Data Protection Working Party, WP 101, 25 Kasım 2004.

Dilemmas of Privacy and Surveillance, Challenges of Technological Change, The Royal Academy of Engineering, Mart 2007.

Guiding principles for the protection of personal data with regard to smart cards (2004), as adopted by CDCJ at its 79th Plenary, 11-14 Mayıs 2004.

How to Use Web 2.0 and Social Networking Sites Securely, IT Governance Research Team, IT Governance Publishing, Birleşik Krallık 2009.

Modal Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows, with Explanatory Memorandum, study made jointly by the Council of Europe, the Commission of European Communities and the International Chamber of Commerce, Strasburg 2 Kasım 1992.

New Technologies: a Challenge to Privacy Protection?, (Study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-Operation (CDCJ), Strasburg 1989.

OECD Guidelines for the Security of Information Systems and Networks, Towards a Culture of Security, (25 Temmuz 2002'de OECD Konsey'inin 1037. oturumunda tavsiye niteliğinde kabul edilmiştir), <http://www.oecd.org/dataoecd/16/22/15582260.pdf> (s.y. 20 Nisan 2009).

Opinion 1/2008 on Data rotection Issues Related to Search Engines, Article 29 Data Protection Working Party, ,4 Nisan 2008, 00737/EN, WP 148.

Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), WP 159, 10 Şubat 2009.

Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities, Article 29 Data Protection Working Party,kabul tarihi: 15 Şubat 2007, yeniden gözden geçirilme ve güncellenme tarihi: 24 Haziran 2008, 00345/07/EN WP 132, 00345-01/07/EN WP 151.

- Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)**, Article 29 Data Protection Working Party, WP 160, 11 Şubat 2009.
- Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)**, Article 29 Data Protection Working Party, WP 160, 11 Şubat 2009.
- Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)**, Article 29 Data Protection Working Party, WP 160, 11 Şubat 2009, s. 11.
- Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)**, Article 29 Data Protection Working Party, WP 160, 11 Şubat 2009.
- Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC**, Article 29 Data Protection Working Party, WP 119, 25 Mart 2006.
- Opinion 4/2001 On the Council of Europe's Draft Convention on Cybercrime**, Article 29 Data Protection Working Party, 22 Mart 2001, 5001/01/EN/Final WP 41,
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp41en.pdf.
- Opinion 4/2007 on the Concept of Personal Data**, 20 Haziran 2007, Article 29 Data Protection working Party 01248/07/EN, WP 136.
- Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC**, Article 29 Data Protection Working Party, WP 90, 27 Şubat 2004, s. 7.
- Opinion 5/2009 on online social networking**, Article 29 Data Protection Working Party, 01189/09/EN WP 163, 12 Haziran 2009.

- Opinion 6/2002 on transmission Passenger Manifest Information and other data from airlines to the United States**, Article 29 Data Protection Working Party, WP 66, 24 Ekim 2002.
- Opinion 7/2000 on the European Commission Proposal for a Directive of the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM(2000)385**, Article 29 Working Party, WP 36, 2 Kasım 2000.
- Opinion 8/2006, 26 Eylül 2006; Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)**, WP 150, 15 Mayıs 2008.
- Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision establishing the European Police Office(Europol), COM (2006)817 final (2007/C 255/02)**, 27 Ekim 2007; http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-02-16_Europol_EN.pdf.
- Opinion on the Processing of Personal Data in the Employment Context**, Article 29 Working Party, Opinion 8/2001, WP 48, 13 Eylül 2001.
- Personal Data for Public Good: using health information in medical research**, haz. The Academy of Medical Sciences, Ocak 2006.
- Privacy on the Internet: A Comprehensive EU Approach to Online Data Protection**, Article 29 Working Party, WP 37, 21 Kasım 2001.
- Privacy on the Internet: an Integrated EU Approach to On-line Data Protection**, Article 29 Data Protection Working Party, 21 Kasım 2000.
- Reasonable Expectations of Privacy, Eleven Country Reports on Camera Surveillance and Workplace Privacy**, haz. Sjaak NOUWT, Berend R. De VRIES, Corien PRINS, Asser Press, Hollanda 2005.
- Recent examples of enforcement actions carried out by data Protection authorities**, Article 29 Data Protection Working Party, Ocak 2005.

Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, Working Party on the Protection of Individuals with regard to the Processing of Personal data, WP 17, 23 Şubat 1999.

Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, Working Party on the Protection of Individuals with regard to the Processing of Personal data, WP 17, 23 Şubat 1999.

Recommendation on the Implementation and Application of the Council of Europe Convention No. 185 on Cybercrime (a.k.a. “Budapest Convention”), International Working Group on Data Protection in Telecommunications, 4 Mart 2008, http://www.datenschutz-berlin.de/attachements/218/cy_en.pdf.

Records, Computers and the Rights of Citizen, U.S. Department of Health, Education and Welfare (HEW), Report of Secretary’s Advisory Committee on Automated Personal Data Systems, Haziran 1973, <http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm>, (s.y. 2 Şubat 2009).

Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (2003), European Committee on Legal Co-operation, 20-23 Mayıs 2003.

Report From the Commission, First report on the implementation of the Data Protection Directive (95/46/EC), Commission of the European Communities, 15 Mayıs 2003 Brüksel, COM(2003) 265 final.

Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommendation Policies and Measures, 26 Nisan 2006, <http://www.oecd-antispam.org>.

Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, 26 Eylül 1973.

Review of the European Data Protection Directive, haz. Neil ROBINSON, Hans GRAUX, Maarten BOTERMAN, Lorenzo VALERI, (Rapor İngiliz Veri

Koruma Denetçiliği Kurumu'nun isteği ile RAND Europe tarafından hazırlanmıştır), <http://www.statewatch.org/news/2009/may/ico-dp-report.pdf>.

RFID, Radio Frequency Identification, OECD Policy Guidance, A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives, OECD Ministerial Meeting on the Future of the Internet Economy, Seul, Güney Kore, 17-18 Haziran 2008, <http://www.oecd.org/dataoecd/19/42/40892347.pdf> (s.y. 20 Nisan 2009).

Safeguarding Privacy in the Fight Against Terrorism, Report of the Technology and Privacy Advisory Committee, Mart 2004 ABD.

Self Regulation and Personal Data Protection, haz. Working Group Meeting at Santa Cruz de la Sierra, Bolivya, 3-5 Mayıs 2006, Red Iberoamericano de Proteccion de Datos.

Tax Payers' Rights and Obligations-Practice Note, haz. OECD Committee of Fiscal Affairs Forum on Tax Administration, 2003.

The Dimensions of Privacy, A National Opinion Research Survey of Attitudes Toward Privacy, (Araştırma Louis Harris and Associates Inc. ile Dr. Alan F. Westin yönetiminde yürütülmüştür), Garland Publishing, ABD 1981.

The Implementation of Directive 95/46/EC to the Processing of Sound and Image Data, British Institute of International and Comparative Law, Londra 2003, http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/biicl-study-soundimage_en.pdf.

The implementation of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, Commission Staff Working Document, Commission of the European Communities, 20 Ekim 2004, SEC(2004) 1323.

The OECD Ministerial Declaration on the Protection of Privacy on Global Networks, Privacy Online: Policy and Practica Guidance, Committee for Information Computer and Communications Policy, Working Group on Information Security and Practice, 21 Ocak 2003,

[http://www.oecd.org/olis/2002doc.nsf/LinkTo/NT000029C6/\\$FILE/JT00137976.PDF](http://www.oecd.org/olis/2002doc.nsf/LinkTo/NT000029C6/$FILE/JT00137976.PDF) (s.y. 20 Nisan 2009).

The Protectin of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities (“Montreaux Declaration”), International Conference of Data Protection and Privacy Commissioners, 16 Eylül 2005, s.3,

<http://www.unhcr.org/refworld/publisher,ICDPPC,,,435914f74,0.html> (s.y. 23 Nisan 2009).

Türkiye’de Yasa Yapma Süreçlerine Etkin Sivil Katılım Projesi, Müzakereci Demokrasiye Doğru, Parlamenter Danışmanları Derneği, Aralık 2009, http://www.tbmmdanismanlari.org/images/proje_raporu_2.pdf.

VOGEL, Hans-Heinrich, **Comments on Draft No.4735 on Protection of Processing of Personal Data, European Commision for Democracy Through Law** (Venice Commisison), Opinion No. 207/2002_lux, 17 Mayıs 2002, CDL(2002)67, [http://www.venice.coe.int/docs/2002/CDL\(2002\)067-e.pdf](http://www.venice.coe.int/docs/2002/CDL(2002)067-e.pdf) (s.y.: 18 Şubat 2009).

Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, Article 29 Working Party, 25 Kasım 2005, 2093/05/WP 114.

Working document on determining the international aplication of EU data protection law to personal data processing on the Internet by non-EU based websites, Article 29 Working Party, WP 56.

Working Document on the processing of personal data relating to health in electronic health records (EHR), Article 29 Working Party, WP 131, 15 Şubat 2007.

Working Document on the processing of personal data relating to health in electronic health records (EHR), Article 29 Working Party, WP 131, 15 Şubat 2007.

Working Document on the Surveillance of Electronic Communications in the Workplace, Article 29 Working Party, WP 55, 29 Mayıs 2002.

Working Document, Transfer of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, WP 12, 24 Temmuz 1998.

Working Document: Privacy on the Internet-An Integrated EU Approach to On-line Data Protection, Article 29 Data Protection Working Party, WP 37, 21 Kasım 2000.

Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Article 29 Working Party, WP 74, 3 Haziran 2003.

Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, Working Party on the Protection of Individuals with regard to the Processing of Personal Data, WP 12, 24 Temmuz 1998.

Working Party on Police and Justice, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, Article 29 Working Data Protection Working Party, WP 168, 1 Aralık 2009.

III. GAZETE VE DERGİ HABERLERİ

“Adalet Komisyonu’nda bulunan tasarılarından biri hükümete zırh, diğeri yurttaşla ‘fişleme’ getirecek-İktidar ‘sır’la korunacak”, **Cumhuriyet**, 24 Mayıs 2008.

“Ben Emniyetim, Fişlerim”, **Radikal**, 17 Ağustos 2009.

“Büyük Gözaltı: İzleniyoruz, Gözleniyoruz, Dinleniyoruz”, **NTV Bilim**, 2 Nisan 2009.

“Dauerlauf gegen in die Sucht”, **Der Spiegel**, S. 35, Y. 2009, s. 136-138.

“Dinlemeye İptal: Yargıtay, skandal yetkiye son noktayı koydu: tüm yurttaşlar şüpheli görülemez”, **Cumhuriyet**, 5 Haziran 2008.

“Fişleme, Özel Kuvvetlerin Rutin Görevlerinden Biri İmiş”, **Yeni Asya**, 8 Ağustos 2008.

“freiheit@unendlich.welt”, **Der Spiegel**, Y. 2009, S. 33, s. 68-79.

- “İşyerinde Her An İzleniyoruz”, **Hürriyet İnsan Kaynakları** (kapak konusu), 28 Aralık 2008.
- “**Jandarma Talebi Değil, Kişisel Verilerin Korunması Kanun Tasarısı Sorunlu**”, <http://www.bianet.org>, 18 Haziran 2008.
- “Kızılay üç saat çıplak: Ankara’nın merkezinde 27 Ocak 2009’da 3 saat boyunca o bölgede kimin kiminle konuştuğu belirlenip savcılığa bildirildi”, **Hürriyet** (manşet haber), 4 Haziran 2009.
- “Lauschangriff im Internet”, **Der Spiegel**, Y. 2008, S.26.
- “Meğer Devlet Fişleri Silmemiş”, **Hürriyet** (Manşet Haber), 17 Ağustos 2009.
- “Meğer Devlet Fişleri Silmemiş”, **Hürriyet**, 18 Ağustos 2009.
- “Mernis Skandalı”, **Milliyet**, 11 Aralık 2006.
- “Müslüman Yolcuya Ayrımcılık”, **Radikal**, 5 Ocak 2010.
- “Öğrencilerden Fişleme Tepkisi”, <http://www.haberler.com>, 23 Aralık 2009.
- “Telefon dinlemeye aynen devam! Yargıtay kararına rağmen dinlemeler devam ediyor”, **Vatan**, 18 Temmuz 2008, <http://www.gazetevatan.com>.
- “The Scary New World of Identity Theft”, **Newsweek**, 5 Eylül 2005.
- “Yargıtay üç ay dinlenmiş: Yargıtay Birinci Başkanlığı’nın usulsüz dinlendiği, hem teknik raporda hem de mahkeme kararları ile ortaya konuldu. Raporda, dinleme kayıtlarının da imha edilmeden, başka bir veri taşıyıcısına kopyalandığı belirtildi”, **NTVMSNBC** 19 Aralık 2009, <http://www.ntvmsnbc.com/id/25033832/>.
- ASH, Timothy Garton “Our state collects more data than the Stasi ever did. We need to fight back”, **The Guardian**, 31 Ocak 2008, <http://www.guardian.co.uk/commentisfree/2008/jan/31/immigrationpolicy.politics>.
- BABAOĞLU, Alparslan, “Kriptolojinin Geçmişi: Bir Şifre Algoritması Kullanmadan Önce Son Kullanma Tarihine Bakın!”, **Bilim ve Teknik**, Y. 42, S. 500, Temmuz 2009, s. 24-27.
- MACRONIN, Rebecca, “Electronic Data Recorders in Vehicles”, 17 Aralık 2008, <http://www.privacydigest.com/2008/12/17/electronic+data+recorders+vehicles>.

IV. YARARLANILAN BAŞLICA İNTERNET SİTELERİ

- **Ulusal Düzenlemeler**

- Genel olarak

<<http://www.mevzuat.gov.tr/>>

- Kişisel Verilerin Kanun Tasarısı

< <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf>>

- **Uluslararası Düzenlemeler**

- Avrupa Konseyi Sözleşmeleri

< <http://conventions.coe.int/>>

- 95/46/AT sayılı Veri Koruma Yönergesi

<<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>>

- 2002/58/AT sayılı Özel Yaşamın ve Elektronik İletişim Korunması Yönergesi

<<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>>

- 2006/24/AT sayılı İletişim Trafik Verilerinin Saklanması Yönergesi

<<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:en:NOT>>

- OECD Rehber İlkeleri

<http://www.oecd.org/document/53/0,3343,en_2649_34255_15589524_1_1_1_37441,00.html>

- BM Rehber İlkeleri

<http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm>

- APEC Çerçeve İlkeleri

<[http://www.ema.gov.au/www/agd/rwpattach.nsf/VAP/\(03995EABC73F94816C2AF4AA2645824B\)~APEC+Privacy+Framework.pdf/\\$file/APEC+Privacy+Framework.pdf](http://www.ema.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf)>

- **Mahkeme Kararları**

- T.C. Anayasa Mahkemesi Kararları
<http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=search&id=24>
- Avrupa İnsan Hakları Mahkemesi Kararları
<<http://www.echr.coe.int/echr/>>
- Avrupa Adalet Divanı Kararları
< http://curia.europa.eu/jcms/jcms/Jo1_6308/>
- ABD “Supreme Court” Kararları
<<http://www.law.cornell.edu/supct/>>
- Federal Almanya Anayasa Mahkemesi Kararları
< <http://www.bundesverfassungsgericht.de/>>

- **Diğer**

- Avrupa Veri Koruma Denetmeni (European Data Protection Supervisor)
<<http://www.edps.europa.eu/EDPSWEB/>>
- 29. Madde Veri Koruma Grubu
<http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/>
- Telekomünikasyonda Veri Koruması Uluslararası Çalışma Grubu
<<http://www.datenschutz.berlin.de>>
- Avrupa Konseyi Veri Koruma Sayfası
<http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/>
- Sanal Veri Koruma Ofisi
< <http://www.datenschutz.de/>>
- Konuyla İlgili Bazı Sivil Toplum Kuruluşları
Statewatch <<http://www.statewatch.org/>>
European Digital Rights <<http://www.edri.org/>>
Electronic Privacy Information Center <<http://epic.org/>>
Privacy International <<http://www.privacyinternational.org/>>
Electronic Frontier Foundation<<http://www.privacyinternational.org/>>