

T. C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

YÜKSEK LİSANS TEZİ

**KİŞİSEL VERİLERİN TÜRK CEZA KANUNU
KAPSAMINDA KORUNMASI**

HAZIRLAYAN
ELİF MENDOS KUŞKONMAZ
2501110288

TEZ DANIŞMANI
PROF. DR. ADEM SÖZÜER

İSTANBUL
2013



YÜKSEK LİSANS

TEZ ONAYI

ÖĞRENCİNİN

Adı ve Soyadı : ELİF MENDOS KUŞKONMAZ

Numarası : 2501110288

Anabilim/Bilim Dalı : KAMU HUKUKU

Danışman : PROF.DR. ADEM SÖZÜER

Tez Savunma Tarihi : 13.08.2013

Tez Savunma Saati : 15:30

Tez Başlığı : KİŞİSEL VERİLERİN TÜRK CEZA KANUNU KAPSAMINDA KORUNMASI

TEZ SAVUNMA SINAVI, Lisansüstü Öğretim Yönetmeliği'nin 36. Maddesi uyarınca yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin KABULÜ'NE OYBİRLİĞİ / OYÇOKLUĞUYLA karar verilmiştir.

JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1. PROF.DR. ADEM SÖZÜER		KABUL
2. PROF.DR.CEMİL KAYA		KABUL
3. YRD.DOÇ.DR. SAADET YÜKSEL		KABUL
4. YRD.DOÇ.DR.TUBA TOPÇUOĞLU		KABUL
5. YRD.DOÇ.DR.ALİ EMRAH BOZBAYINDIR		KABUL

YEDEK JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1- DOÇ.DR. CANER YENİDÜNYA		
2- DOÇ.DR. MELİKŞAH YASİN		KABUL

Başlık: Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması

Yazar: Elif Mendos Kuşkonmaz

ÖZ

Bu çalışmada Türk hukukunda önemi yeni anlaşılmaya başlanan kişisel verilerin korunması ve Türk Ceza Kanunu'nda kişisel verilerin korunması alanında değerlendirilen suçlar ele alınmıştır.

Bilgi ve iletişim teknolojilerindeki artış bilgi akışını kolaylaştırmış ve artık kişisel verilerin korunması her geçen gün daha çok önem kazanmıştır. Öyle ki, kişisel verilerin hukuka uygun olarak işlenmesi ve kötüye kullanımlarının engellenmesi için dünyada kişisel verilerin korunmasını güvence altına alan bir mevzuat geliştirilmiştir.

Kişisel verilerin korunmasının temel hak ve özgürlüklerin kapsamında yer aldığı kabulü, günümüz toplumlarında bireylerin karşılaşılabileceği önemli ihlallere karşı bir güvence sistemini gerekli kılmaktadır. Nitekim Türk Ceza Kanunu'nda kişisel veriler bağlamında kişinin bireysel özerkliğine, özel hayatına ve insan onuruna yönelik zarar verici eylemler suç tipleri olarak öngörülmüştür.

Çalışma üç ana bölümden oluşmaktadır. İlk bölüm kişisel veri kavramına giriş yapmak amacıyla kavramın tanımı ve ilgili uluslararası düzenlemelere ayrılmıştır. Çalışmanın ikinci bölümünde ise kişisel verilerin etkili bir biçimde korunmasının sağlanabilmesi için kişisel verilerin korunması hakkına özgü kriterlere yer verilmiştir. Çalışmanın üçüncü ve son bölümünde ise kişisel verilerin korunmasına dair alan daraltılıp tez konusuyla bağlantılı olarak Türk Ceza Kanunu'nda düzenlenen kişisel verilerin korunmasına dair suçlar incelenmiştir.

Anahtar Kelimeler: Kişisel Veri, Özel Hayatın Gizliliğinin Korunması Hakkı, Ceza Hukuku, Türk Ceza Kanunu.

Title: Protection of Personal Data Pursuant to Turkish Criminal Code

Author: Elif Mendos Kuşkonmaz

ABSTRACT

This research deals with the protection of personal data as a relatively new issue in Turkish Law and Turkish Criminal Code in the field of protection of personal data.

The progress made in information and communication technologies has made the information flow considerably easier, therefore protection of personal data has emerged. It is for this reason that data protection regulations have been adopted worldwide to function the lawful processing of personal data and prohibit the misuse as such.

The acknowledgement of protection of personal data as a fundamental right makes an assurance system essential to protect individuals from the misuse of their personal data. Hence, unlawful acts against an individual's self-determination, right to privacy and human dignity have been adopted as criminal sanctions under Turkish Criminal Code.

Based on three main chapters thesis begins with a general introduction of the personal data and related legal arrangements in the first chapter. In the second chapter the main principles of personal data are explained in order to provide an effective personal data protection. The main aim of the third and the last chapter is the detailed analysis of criminal sanctions provided in Turkish Criminal Code.

Keywords: Personal Data, Right to Privacy, Criminal Law, Turkish Criminal Code.

ÖNSÖZ

Çalışmamızda zamanımıza damgasını vuran ve yeni bir üretim, iletişim biçiminin kilit noktasını oluşturan kişisel veri kavramı irdelenerek kişisel verilerin korunması hakkının temel hak ve özgürlükler içindeki yeri, Türk Ceza Kanunu'ndaki kişisel verilerin korunmasına ilişkin düzenlemesi ve uygulamadaki aksaklıkları, uluslararası mevzuat göz önünde bulundurarak ortaya koyulmaya çalışılmıştır.

Bu vesileyle, öncelikle danışmanım olmayı kabul eden ve tezin yazılış süreci aşamalarında yardımlarını ve desteğini esirgemeyen Sayın Prof. Dr. Adem Sözüer'e teşekkür ederim.

Ayrıca, öğrenci değişim programı kapsamında çalışmama dair araştırmaların bir kısmını yapma fırsatını edindiğim Porto Üniversitesi'nde bulunduğum süre boyunca yardımlarını esirgemeyen Sayın Doç. Dr. André Lamas Leite'ye teşekkürlerimi sunuyorum. Son olarak tüm bu süreç boyunca bana yardımlarını esirgemeyen, en büyük sabrı ve desteği gösteren anneme, babama ve kardeşime ne kadar teşekkür etsem azdır.

İÇİNDEKİLER

ÖZ	i
ABSTRACT	ii
ÖNSÖZ	iii
İÇİNDEKİLER	iv
KISALTMALAR	viii
GİRİŞ	1

BİRİNCİ BÖLÜM KİŞİSEL VERİ KAVRAMI VE İLGİLİ DÜZENLEMELER

I. KİŞİSEL VERİ KAVRAMININ AÇIKLANMASI	4
A. HER TÜR VERİ.....	5
B. KİMLİĞİ BELİRLİ VEYA BELİRLENEBİLİR GERÇEK KİŞİ	7
C. KİŞİYE İLİŞKİN VERİ	11
II. KİŞİSEL VERİLERİN KORUNMASI GEREKLİLİĞİ	13
III. KİŞİSEL VERİLERİN KORUNMASI HAKKININ HUKUKİ NİTELİĞİ	18
A. Mülkiyet Hakkı Görüşü	18
B. Fikri Mülkiyet Hakkı Görüşü	22
C. Özel Hayatın Gizliliği Hakkı ve Kişisel Verilerin Korunması	24
IV. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL DÜZENLEMELER	32
A. Tarihsel Gelişim	32
B. Uluslararası Belgelerde Kişisel Verilerin Korunmasına İlişkin Temel Kaynaklar	37
1. OECD ve Kişisel Verilerin Korunması	38
2. Birleşmiş Milletler Örgütü ve Kişisel Verilerin Korunması	42
3. Avrupa Konseyi ve Kişisel Verilerin Korunması	45
a.Genel Olarak	45
b. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme	47
c. Avrupa İnsan Hakları Sözleşmesi ve Kişisel Verilerin Korunması	53
(1) AİHS 8. Madde Kapsamında Kişisel Verilerin Korunması	53
(2) Kişisel Verilerin Korunmasına İlişkin AİHM Kararları	54
4. Avrupa Birliği'nde Kişisel Verilerin Korunması	65
a. Genel Olarak	65

b. Avrupa Birliği Temel Haklar Şartı	67
c. 95/46/AT Sayılı Kişisel Verilerin Korunması Direktifi	70
(1) Amaç	70
(2) Uygulama Alanı ve Kapsamı	73
(3) Üçüncü Ülkelere Veri Aktarımı Rejimi	78

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HAKKINA ÖZGÜ KRİTERLER

I. GENEL OLARAK	87
II. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN İLKELER	88
A. Hukuka ve Dürüstlük Kurallarına Uygun İşleme	88
B. Amaçla Bağlılık İlkesi	89
C. Kişisel Verilerin Doğru ve Eğer Gerekli İse Güncel Olarak Tutulma İlkesi	92
D. Amacın Gerektirdiğinden Daha Uzun Süre Tutulmama İlkesi	93
III. VERİLERİ İŞLENEN KİŞİLERİN HAKLARI	94
A. Kişisel Verilerin İşlenmesi Sırasında İlgilinin Bilgilendirilmesi	94
B. İlgilinin Bilgilerine Erişim Hakkı	96
C. İlgilinin Verilerini Düzeltme Hakkı	98
D. İlgilinin İtiraz Hakkı	99
E. İlgilinin Otomatik Kararların Konusu Olmama Hakkı	100
IV. VERİLERİN İŞLENMESİNE İLGİLİNİN RIZASI	101
A. Rıza Beyanının Önemi	101
B. Rıza Beyanının Niteliği	102
V. HASSAS VERİLERİN ÖZEL OLARAK KORUNMASI	105
A. Hassas Veri Türleri	106
B. Hassas Verilerde Kesin İşlem Yasağı ve İstisnaları	111
VI. VERİ GÜVENLİĞİ İLKESİ	116
A. Veri Güvenliğinin Sağlanabilmesinin Önemi	116
B. Kişisel Verilerin Korunmasına Dair Düzenlemelerde Veri Güvenliği İlkesi	118
VII. DENETİM VE YAPTIRIM SİSTEMLERİ	120
A. Verilerin İşlenmesinde Bildirim ve Ön Kontrol Uygulaması	120
B. Yargı Yolları ve Yaptırımlara İlişkin Düzenlemelerin Gerekliliği	121
C. Kişisel Verilerin İşlenmesinin Bağımsız Organlarca Denetimi	122

ÜÇÜNCÜ BÖLÜM
KİŞİSEL VERİLERİN TÜRK CEZA KANUNU KAPSAMINDA
KORUNMASI

I. GENEL OLARAK	126
II. KİŞİSEL VERİLERİN KAYDEDİLMESİ SUÇU	128
A. Suçla Korunan Hukuksal Değer	129
B. Maddi Unsur	133
1. Suçun Konusu	133
2. Fail ve Mağdur	138
3. Hareket	139
4. Netice	141
C. Manevi Unsur	142
D. Hukuka Aykırılık	142
E. Suçun Özel Görünüş Biçimleri	147
1. Teşebbüs	147
2. İştirak	148
3. İçtima	148
F. Suça Etki Eden Sebepler	149
1. Suçun Kamu Görevlisi Tarafından ve Görevinin Sağladığı Yetki Kötüye Kullanılmak Suretiyle İşlenmesi	150
2. Suçun Belli Bir Meslek ve Sanatın Sağladığı Kolaylıktan Yararlanmak Suretiyle İşlenmesi	151
G. Yaptırım ve Usul	152
II. VERİLERİ HUKUKA AYKIRI OLARAK VERME, YAYMA VEYA ELE GEÇİRME	152
A. Suçla Korunan Hukuksal Değer	153
B. Maddi Unsur	153
1. Suçun Konusu	153
2. Fail ve Mağdur	153
3. Hareket	154
4. Netice	155
C. Manevi Unsur	156
D. Hukuka Aykırılık	156
E. Suçun Özel Görünüş Biçimleri	157
1. Teşebbüs	157
2. İştirak	157
3. İçtima	158
F. Suça Etki Eden Sebepler	159
G. Yaptırım ve Usul	159
III. VERİLERİN YOK EDİLMEMESİ SUÇU	160
A. Suçla Korunan Hukuksal Değer	161
B. Maddi Unsur	162
1. Suçun Konusu	162

2. Fail ve Mağdur	163
3. Hareket	163
4. Netice	164
C. Manevi Unsur	165
D. Hukuka Aykırılık	166
E. Suçun Özel Görünüş Biçimleri	166
1. Teşebbüs	166
2. İştirak	166
3. İçtima.....	167
F. Suça Etki Eden Sebepler	167
G. Yaptırım ve Usul	167
SONUÇ	168
KAYNAKÇA	172

KISALTMALAR

a.g.e.	: Adı geçen eser
a.g.m.	: Adı geçen makale
AAD	: Avrupa Adalet Divanı
AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AK	: Avrupa Konseyi
AYMK	: Anayasa Mahkemesi Kararı
b.n.	: Başvuru no
C.	: Cilt
CMK	: Ceza Muhakemesi Kanunu
çev.	: Çeviren
d.n.	: Dipnot
E.	: Esas sayısı
EİHB	: Evrensel İnsan Hakları Beyannamesi
f.	: fıkra
haz.	: Hazırlayan
İÜHFİM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
İSS	: İnternet Servis Sağlayıcı
K.	: Karar sayısı
k.t.	: Karar tarihi
m.	: Madde
MERNİS	: Merkezi Nüfus İdaresi Sistemi
OECD	: Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)
para.	: Paragraf
paras.	: paragraflar
R.G.	: Resmi Gazete

s. : Sayfa
S. : Sayı
t. : tarih
TCK : Türk Ceza Kanunu
vd. : ve devamı
Yay. : Yayınları ya da Yayınevi

GİRİŞ

Bilgi teknolojilerini merkez alan teknoloji devrimi, ivme kazanan bir hızla toplumun maddi temelini yeniden şekillendirmeye başlamıştır. Bilgi artık yeni bir üretim, yönetim ve yaşama biçimi olarak tanımlanmaya başlanmıştır. Gelişen teknoloji ile birlikte bu bilgilerin paylaşımı, toplanması, yönetilmesi ve işlenmesi hiç olmadığı kadar kolay hale gelmiştir. Bu noktada bireyin isminden adresine, telefon numarasından beğenilerine kadar çok büyük bir alanı kapsayan kişisel verilerinin korunmasının önemi tartışılmaya başlanmıştır. Kişisel verilerin işlenmesinin artık sıradanlaştığı günümüzde bu veri işlem faaliyetlerinin hukuka aykırı olması veya bu türden verileri kötüye kullanma ihtimallerine karşı küresel anlamda hukuksal düzenlemeler yapılması ihtiyacı doğmuştur. Bu düzenlemeler nispeten yenidir ve daha çok 1970'li yıllarda elektronik bilgi bankalarında işlenen veriler dolayısıyla, bunların bireylerin özel yaşamlarına yönelik taşıdığı tehditlere cevaben kabul edilmişlerdir. Nitekim dile getirilen en büyük tehdit kişinin bir bütün ve sürekli olarak izleyen, kayıt altına alan devlet yapısı nedeniyle kişiye ilişkin verilerin artık kişisel olmaktan çıkartılarak şeffaf bir insan tipinin yaratılmasına ilişkindir. Kişisel verilerin korunması bireysel özerklik, kişinin özel hayatı ve insan onuru ile ilişkilidir. Bir yanda bilişim ve iletişim teknolojileri ile bilgi akışının getirdikleri diğer yanda ise kişinin kendisine ilişkin bilgileri üzerindeki denetimi çatışma halindedir. Şüphesiz ki bu türden verilere yönelik denetimimizi kaybetmemiz, bireysel özerkliğimizi kaybetmemiz demektir. Kişisel verilerin korunması, bilgi akışının karşısında bu süreçte denetimini kaybeden bireye, yeniden kendisine ilişkin veriler üzerinde denetim hakkı vermeyi hedefler. Bilgi akışının önünü kesmeden ve bireyi de bu süreçte aktif hale getirmeyi amaçlayan koruma, teknolojinin sağladığı olanaklar ile bireyin temel hak ve özgürlükleri arasında bir denge aracıdır.

Kişisel verilerin korunması Türkiye'de nispeten yeni tartışılmaya ve anlaşılmaya başlanan bir konudur. Nitekim korumanın temel hak ve özgürlüklerin

kapsamında deęerlendirilmesi ve Trkiye'nin Avrupa Birlięi'ne aday lke konumunun Avrupa Birlięi mkteseabatına uyum alıřmalarını gerektirmesi bu konuda Trk hukukunda da acilen yeterli gvencelerin saęlanmasını gerekli kılmıřtır. zellikle bilgi akıřının kresel olduęu bir dnyada ve bilginin artık toplumun merkezi haline geldięi gnmzde kiřisel verilere yklenen anlamın farklı bir boyut kazanmasıyla birlikte bunlara ynelik zarar verici yeni eylemler ortaya ıkmaktadır. İřte bu nedenledir ki kiřileri ve toplumu etkin biimde koruyabilmek adına kiřisel verilerin korunmasına dair yeni su tiplerinin yaratılması gerekmiřtir. Ayrıca gerek bir bilgi toplumuna dnřm ancak uygun hukuksal ortamın saęlanması ile mmkn olabilecektir. Bu baęlamda 1 Haziran 2005 tarihinde yrrlęe giren 5237 sayılı Trk Ceza Kanunu ile 765 sayılı mlga TCK'dan farklı olarak kiřisel verilerin korunmasına iliřkin sulara yer verilmiřtir¹.

alıřmamızda ilk nce kiřisel verileri kavramına genel bir giriř yapılacaktır. ncelikle kiřisel veri tanımlanarak bilgi ve kiři arasındaki baęın zerinde durulacak, ardından kiřisel verilerin korunması hakkının hukuki nitelięine dair grřler ortaya konulacaktır. Kiřisel verilerin korunması hakkını mlkiyet hakkı, fikri mlkiyet hakkı ve zel hayatın gizlilięi hakkı ile aıklayan grřler ele alınacaktır. Bu erevede mlkiyet hakkı ve fikri mlkiyet hakkının kiřisel veri kavramıyla eřitli aılardan rtřmedięi ve kiřisel verilerin korunması hakkı ile zel hayatın gizlilięi hakkının yakın iliřkisi aıklıęa kavuřturulmaya alıřılacaktır. Bu blmde son olarak kiřisel verilerin korunmasına iliřkin gemiřten gnmze kadar yapılan temel uluslararası dzenlemelere yer verilecektir. řphesiz ki alıřmamızda yer verdięimiz kiřisel verilerin korunması ihtiyacının ortaya ıkıřı ve bu konuda geliřmelerin takip edilebilmesi aısından nemlidir.

alıřmamızın ikinci blmnde ise kiřisel verilerin korunmasına iliřkin dzenlemelerde konuya zg kabul edilen bazı ortak ilkelere deęinilecektir. Nitekim kiřisel verilerin hukuka uygun bir řekilde iřlendięinden bahsetmek iin ngrlen bu

¹ R.G., t. 12.10.2004, S. 25611.

usul ve esaslara ya da ilkelere uygun davranılması gerekmektedir. Bu nedenle kişisel verilerin korunmasına özgü kriterlerin öğrenilmesi aynı zamanda ceza hukuku alanında hangi hallerde hukuka uygunluğun sağlandığının tespiti açısından da önemlidir.

Çalışmamızın üçüncü ve son bölümünde Türk Ceza Kanunu'nda düzenlenen kişisel verilerin korunmasına ilişkin suç tipleri incelenecektir. Bu bölümde anılan suç tiplerinin yasallık ilkesi gereği sınırlarının çizilmesi ve uygulama alanının belirlenmesine çalışılmıştır.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI VE İLGİLİ DÜZENLEMELER

I. KİŞİSEL VERİ KAVRAMININ AÇIKLANMASI

Kişisel veri kavramı, kişisel verilerin korunması ihtiyacı ve bu doğrultuda kabul edilen kişisel verilerin korunmasına ilişkin hukuki düzenlemelerin merkezini oluşturmaktadır. Özellikle teknolojik ilerlemeler ile önemi eskisine nazaran daha çok fark edilen kişisel veri kavramı, ulusal ve uluslararası pek çok hukuksal düzenlemede tanımlanmıştır. Bu anlamda konunun derinine inmeden önce ne tür verilerin kişisel veri olarak değerlendirildiğini açıklamamız gerekmektedir. Kişisel verilerin korunmasına ilişkin ilk uluslararası belge olan ve OECD tarafından 1980 yılında kabul edilen “Kişisel Verilerin Sınıraşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri”nde kişisel veri, *“belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgiler”* olarak tanımlanmıştır². Kişisel verilerin korunmasına ilişkin kabul edilmiş ilk bağlayıcı uluslararası hukuk belgesi olan 28 Ocak 1981 tarih ve 108 Sayılı “Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşmesi” ise kişisel veriyi, *“kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgiler”* şeklinde tanımlamaktadır³. Küresel anlamda önemli bir yere sahip “Kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması hakkındaki 95/46/AT sayı ve 24 Ekim 1995 tarihli Avrupa Birliği Konseyi ve Avrupa Parlamentosu Direktifi” ise kişisel veriyi, *“belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgiler”* olarak tanımlamaktadır⁴. Maddenin devamında kimliği belirlenebilir kişi, *“doğrudan veya*

² Bundan böyle OECD Rehber İlkeleri olarak anılacaktır. Bkz., OECD Rehber İlkeleri, m. 1

³ Bundan böyle 108 sayılı Sözleşme olarak anılacaktır. Bkz., 108 Sayılı Sözleşme, m. 2/a.

⁴ Bundan böyle AB Direktifi olarak anılacaktır. AB Direktifi, m. 2/a. Aynı doğrultuda Adalet Bakanlığınca 15.09.2011 tarihinde Başbakanlığa yazılan yazıyla yenilenmesinin uygun olacağı bildirilen ve halen daha Başbakanlıkta bulunan Kişisel Verilerin Korunması Kanun Tasarısı'nda kişisel veri, *“belirli veya belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler”* olarak tanımlanmaktadır. Bkz., Kişisel Verilerin Korunması Kanunu Tasarısı, m. 3/ç. Ayrıca Başbakanlıkta bulunan Tasarı'nın metni için bkz., (Çevrimiçi)

<http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Kanuntas/kisiselveriler.pdf>, 01.05.2013

dolaylı olarak özellikle bir kimlik numarasının veya kişinin fiziksel, fizyolojik, akli, ekonomik, kültürel veya sosyal kimliğine ait bir veya birden fazla spesifik faktörün referansına dayanılarak teşhis edilebilir olan kişi” olarak tanımlanmaktadır. Bütün bu tanımlamalardan yola çıkarak kişisel veriyi en yalın haliyle, belirli veya belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi olarak tanımlayabiliriz⁵. Bununla birlikte, hem ulusal hem de uluslararası düzenlemelerdeki tanımlamalarda kişisel veri çeşitli şekillerde tanımlanmıştır. Bu bağlamda kişisel verinin kapsamının sınırlarının çizilmesi gerekmektedir. Nitekim kapsamın belirlenmesi kimlerin kişisel verilerin korunmasına dair hukuki düzenlemelerin sağladığı güvencelerden faydalanabileceğinin tespit edilmesi bakımından önemlidir. Kişisel veriye dair üzerinde görüş birliği bulunan tanımı ele aldığımızda kavramın unsurları olarak (i) her tür veri (ii) kimliği belirli veya belirlenebilir bir kişi ve (iii) kişiye ilişkin veriden söz edebiliriz⁶.

A. HER TÜR VERİ

Kişisel veri tanımlamalarında Direktifi temel aldığımızda kavramın oldukça geniş tutulduğunu görürüz⁷. Her türlü verinin, diğer şartları da taşıması şartıyla,

⁵ Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin Yay., 2004, s.33. Bu dipnot bağlamında bilgi (information) ve veri (data) kavramlarına değinmemiz gerekmektedir. Anılan iki kavrama dair çeşitli tanımlamalar yapılmakta ve bu bağlamda farklı anlamlar taşıdıkları kabul edilmektedir. Nitekim Kurt, “*her iki tanım birlikte irdelendiğinde anlaşılacağı üzere bilgi ve veri birbirinden farklı kavramlar olup, en basit anlamda bilgi bizim algıladığımız temel ve her türlü malumat, bu malumatın bilgisayarın anlayıp işleyebileceği haline de veri denilmektedir.*” diyerek bu farklılığı kabul etmektedir. Güncel Türkçe Sözlük’te bilgi, “(bilişim açısından) kurallardan yararlanarak kişinin veriye yönelttiği anlamı” ve veri de “(bilişim açısından) olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi” olarak tanımlanmıştır. Bkz., TDK “Bilim ve Sanat Terimleri Sözlüğü”, (Çevrimiçi) <http://www.tdkterim.gov.tr/>, 01.05.2013. Genele baktığımızda bilişim teknolojileri açısından veri nitelik itibariyle bilginin yapı taşı olarak kabul edilmektedir. Ancak bizim çalışmamızda bilgi ve veri kavramları arasında farklılıkların bulunduğunu kabul etmekle birlikte çalışmamızın konusunu oluşturan kişisel verilerin korunması hususuna ilişkin olan iki kavramın bir diğerinin yerine kullanıldığı yaklaşımdan hareket edilmiştir.

⁶ Kişisel verinin kapsamının sınırlarının çizilmesi açısından Direktifin 29. maddesine göre kurulan ve kişisel verilerin korunması dahilinde faaliyet gösteren bağımsız bir tavsiye organı olan 29. Madde Veri Çalışma Grubunun konu hakkındaki raporu önemlidir. Çalışmamızda da kavramın unsurlarının incelenmesi açısından ilgili rapor temel alınmıştır. Rapor için bkz., Article 29 Working Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 20.06.2007, 01248/07/EN, WP 136.

⁷ Bununla birlikte Direktifte kişisel veri kavramının geniş tutulması bazı çevrelerce eleştirilmiştir. Direktifte yer alan geniş kapsamlı kişisel veri tanımlamasının ticari faaliyetlerde zorluklara yol

kişisel veri olarak kabul edilmesi söz konusu verinin gizli olmasını gerekli kılmamaktadır⁸.

Bir verinin niteliğinin objektif veya subjektif olması, bu verinin kişisel veri olarak kabul edilip edilmemesi bakımından önem taşımamaktadır. Bu anlamda kişinin kanında belirli bir maddenin bulunduğu gibi objektif veya bir kişinin değer yargıları, güvenilirliği gibi subjektif bilgiler de kişisel veri kapsamında değerlendirilecektir. Kaldı ki, örnek olarak verdiğimiz subjektif bilgiler, bankacılık, sigorta, istihdam sektöründe önemli ölçüde kullanılmaktadır. Kişisel veri ile ilgili diğer bir konu bu verinin, gerçek veya doğruluğunun kanıtlanmış olmasının gerekmemesidir⁹. Bu bağlamda kişisel verilerin korunmasına ilişkin düzenlemeler, verilerin yanlış olma ihtimalini öngörerek hakkında kişisel veri işlenen kişilere bu verilere erişim ve hataların düzeltilmesini talep etme hakkını tanımaktadır¹⁰.

Kişisel veri, verinin tutulduğu ortam veya tutulma şeklinden bağımsızdır. Eski zamanlara nazaran bilgi artık ağlar, ses veya görüntü kaydı üzerinden yayılması sağlanabilmektedir. Buna karşılık Direktif, öngördüğü Avrupa veri koruma rejiminin teknolojinin gerisinde kalmasını engellemek amacıyla ses ve görüntü verilerini de kişisel veri kapsamında değerlendirmektedir¹¹. Diyebiliriz ki, kişinin kamera ile kayıt

açabileceği öne sürülmüştür. Bkz., Andrew Charlesworth, “*Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?*”, **Hastings Law Journal**, C.54, 2002-2003, s. 941. Eleştiriler bir kenara bırakılacak olursa, özellikle teknolojik gelişmeler ile birlikte konunun statik bir yapıya sahip olmaması, ulusal düzenlemelerde kişisel veri kavramına dair yaklaşımların -hem anlam hem de uygulamada- çeşitlilik göstermesi açısından Direktifte kişisel veri tanımının kapsamının geniş tutulmasını yerinde bulmaktayız. Özellikle Direktif’in ilgili maddesinde yer alan “her tür veri” kavramı bu yaklaşımın bir yansımasıdır. Bkz., Article 29 Working Data Protection Working Party, **Opinion4/2007 on the Concept of Personal Data**, 20.06.2007, 01248/07/EN, WP 136, s. 6.

⁸Jerry Kang, “*Information Privacy in Cyberspace Transactions*”, **Stanford Law Review**, C.50, 1998, s. 1206. Ayrıca bkz., Çalışmamızın “*Kişisel Veri Kavramı ve İlgili Düzenlemeler*” adlı Birinci Bölümü, III numaralı “*Kişisel Verilerin Korunması Hakkının Hukuki Niteliği*” başlığı, “*Özel Hayatın Gizliliği Hakkı ve Kişisel Verilerin Korunması*” adlı altbaşlığı.

⁹Article 29 Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 20.06.2007, 01248/07/EN, WP 136, s. 6.

¹⁰Konu ile ilgili ayrıntılı bilgi için bkz., çalışmamızın “*Kişisel Verilerin Korunması Hakkında Özgü Kriterler*” adlı İkinci Bölümü, II numaralı “*Verileri İşlenen Kişilerin Hakları Kavramının Açıklanması*” başlığı.

¹¹Rupert Battcock, “*Data Protection: Where Next?*”, **International Journal of Law and Informational Technology**, C.3, 1995, s. 166. Ayrıca bkz., AB Direktifi, 14 numaralı gerekçe; AB Direktifi, m. 33/f.2. İlgili madde hükmü şöyledir: “*Komisyon, Direktif’in, özellikle gerçek kişilerin ses*

altına alınan görüntüleri ile telefon bankacılığı işlemleri sırasında müşterinin banda kaydedilen sesi kişisel veri kapsamına dahildir¹².

B. KİMLİĞİ BELİRLİ VEYA BELİRLENEBİLİR GERÇEK KİŞİ

Kişisel verinin diğer bir unsuru ise kimliği belirli veya belirlenebilir bir kişinin bulunmasıdır. Burada özellikle üzerinde durmak istediğimiz durumlar kişi kavramının kapsamına kimlerin gireceği ile söz konusu kişinin kimliğinin hangi hallerde belirli veya belirlenebilir olduğudur. Nitekim bu noktaların açıklığa kavuşturulması kimlerin kişisel verilerin korunmasına dair hukuki düzenlemelerin sağladığı güvencelerden faydalanabileceğinin tespit edilmesi açısından önemlidir.

Kişi kavramının kapsamına kimlerin gireceğine dair uluslararası doktrin ve mevzuatta farklı görüşler mevcuttur. Görüş ayrılığı sadece gerçek kişilere ilişkin bilgilerin mi kişisel veri niteliği taşıdığı yoksa tüzel kişilere ilişkin bilgilerin de mi bu kapsamda değerlendirilebilmesine ilişkindir.

OECD Rehber İlkeleri ve 108 sayılı Sözleşme kişisel verilerin koruma alanını gerçek kişiler için öngörmüşlerdir¹³. Aynı şekilde Direktif de kural olarak tüzel kişiler hakkında tutulan verileri uygulama alanına almamaktadır¹⁴. Kişisel verilerin

ve görüntülerine ilişkin verileri bakımından uygulanmasını incelemeli ve bilgi toplumunun ilerlemesi ışığında, bilgi teknolojilerinin gelişimini dikkate alarak gerekli göreceği uygun önerileri sunmalıdır". Kişisel verilerin korunmasına ilişkin düzenlemelere ulusal mevzuatında yer veren birçok ülkede de ses ve görüntülerin kişisel veri niteliği taşıdıkları yer almaktadır. Örnek vermek gerekirse Fransız Veri Koruma Kanunu'nda dijital biçimde saklanması ve kimliği belirlenebilir bir kişi ile ilişkin olmaları şartıyla, ses ve görüntü verilerinin de kişisel veri niteliği taşıdıkları ifade edilmiştir. Bkz., Douwe Korff, **EC Study on Implementation of Data Protection Directive-Comparative Summary of National Laws**, Cambridge, 2002, s. 20. (Bundan böyle **EC Study on Implementation of Data Protection Directive-Comparative Summary of National Laws** olarak anılacaktır).

¹² Article 29 Working Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 20.06.2007, 01248/07/EN, WP 136, s. 8.

¹³ Çalışmamızın ilgili bölümünde de belirttiğimiz gibi OECD Rehber İlkeleri ve 108 sayılı Sözleşme kişisel verilerin korunmasına dair minimum standartları belirlemektedirler. Buna göre 108 sayılı Sözleşme'nin 3. maddesinin 2. fıkrasının b bendinde de belirtildiği gibi koruma kapsamına tüzel kişiler de dahil edilebilir. OECD Rehber İlkeleri'nde de bazı ülkelerde kişi gruplarına veya benzer kurumlara ilgili bilgilere korumanın sağlandığı belirtilmekle birlikte bunlara ilişkin bilgilerin korunması ile bireylerin kendilerine ilişkin bilgilerin korunmasının farklı ihtiyaçları yansıttığı vurgulanmıştır. Öyle ki bu farklı ihtiyaçlar, farklı düzenlemeleri gerektirmektedir. Bkz., OECD Rehber İlkeleri, m. 33.

¹⁴ AB Direktifi, 24 numaralı gerekçe. Ayrıca AB düzeyinde kişisel verilerin korunmasına yönelik diğer

koruma alanına dair Direktif'te yer alan genel kural belirttiğimiz gibi olmak ile birlikte üye devletler ulusal veri koruma yasalarında tüzel kişileri de kapsar şekilde düzenleme yapabilmektedirler¹⁵. Nitekim üye devletlerden Avusturya, Danimarka, İtalya ve Lüksemburg kişisel verilerin korunmasına ilişkin hukuksal düzenlemelerinde tüzel kişileri de koruma kapsamına almışlardır¹⁶. Ayrıca belirtmek isteriz ki tüzel kişilere ilişkin bilgilerin gerçek bir kişi ile ilişkilendirilmesi mümkün olduğu hallerde korumadan yararlanacaktır¹⁷.

Kişisel verilere ilişkin korumanın yalnızca gerçek kişileri kapsamı gerektiği, tüzel kişilere ait bilgilerin bu kapsamda değerlendirilmemesine dair yaklaşım kişisel veri kavramının niteliği ve korumanın ihtiyacı ile açıklanmaktadır. Kişisel verilerin korunması insan onuru ve temel özgürlüklerin sağlanmasını kapsamaktadır. Ayrıca, kişisel verilerin korunması ilk aşamada özel hayatın gizliliği çerçevesinde değerlendirilmiş, daha sonraki dönemlerde ise pek çok faktörün etkisi ile birlikte özel hayatın gizliliği hakkında bağımsız bir temel insan hakkı olarak kabul görmeye başlamıştır¹⁸. Kişisel verilerin korunması bir insan hakkıdır. Bu nedenle yalnızca gerçek kişilere ilişkin bilgilerin güvence kapsamında sayılmasının yerinde olduğunu söylemek yanlış olmaz¹⁹. Öte yandan kişisel verilerin işlenmesinin tüzel kişilerin

bir düzenleme olan “*Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin 2002/58/AT sayılı Avrupa Birliği Direktifi*” yalnızca elektronik haberleşme sektörüne ilişkin olarak hem gerçek hem de tüzel kişilerin veri sahibi kabul edileceğini ifade etmektedir. Ancak anılan Direktif ile üye devletlere 95/46/AT sayılı Direktifin uygulama alanını tüzel kişileri de kapsayacak şekilde genişletme yükümlülüğü getirilmediği açıkça belirtilmektedir. Bkz., 2002/58/AT sayılı Direktif 12 numaralı gerekçe

¹⁵ Üye devletlerin kişinin özel hayatının korunması ile serbest veri akışı arasındaki dengenin korunduğu sürece Direktif'i daha geniş yorumlayabilecekleri; ayrıca üye devletlerin ulusal düzenlemelerinde Direktif'in uygulama kapsamını, Topluluk hukukuna dair diğer hükümlerin engellemesi şartıyla genişletebileceğine dair bkz., Bodil Lindqvist, Case C-101/01, 06.11.2003, paras. 97, 98, 99.

¹⁶ Korff, **EC Study on Implementation of Data Protection Directive-Comparative Summary of National Laws**, s. 21.

¹⁷ Başalp, **a.g.e.**, s. 35.

¹⁸ Kişisel verilerin korunması hakkına dair yaklaşımlara ve kişisel verilerin özel hayatın gizliliği çerçevesinde değerlendirilmesine çalışmamızın ileriki bölümlerinde yer vereceğiz. Bkz., Çalışmamızın “*Kişisel Veri Kavramı ve İlgili Düzenlemeler*” adlı Birinci Bölümü, III numaralı “*Kişisel Verilerin Korunması Hakkının Hukuki Niteliği*” başlığı.

¹⁹ Kişisel veri kavramının niteliğinden dolayı tüzel kişilere ilişkin bilgilerin koruma kapsamı dışında bırakıldığı Almanya, Yunanistan ve diğerleri kadar olmasa da belirli bir ölçüde Fransa'da kişisel verilerin korunması kişilik hakkı veya insan kimliği ile temellendirilmiştir ve gerçek kişilerin özel hayatını korumayı amaçlamaktadır. Aynı şekilde İspanya ve Finlandiya gibi ülkelerde de kişisel

menfaatlerini de koruması gerektiği savunulmaktadır. *Korff*, dini, siyasi ve sendikal örgütler gibi tüzel kişileri bu kapsamda değerlendirmiştir. Bu tüzel kişiler ticari işletmeler veya büyük şirketler gibi tüzel kişilere kıyasla daha çok korunma ihtiyacı içindedirler²⁰. Uluslararası şirketler, özel girişimciler veya kâr amacı gütmeyen kuruluşlar gibi farklı tür ve nitelikteki tüzel kişilerin bu durumlarına uygun olarak farklı yasal düzenleme getirilmesi gerektiği de ileri sürülen diğer bir yaklaşımdır²¹. Karşıt görüşte olan *Tezcan* ise savında ticari işletmeleri temel almıştır. Yazara göre tüzel kişiler için ticari sırrın korunması söz konusu olacaktır. Ticari işletmeler bakımından geçerli olan şeffaflık ilkesi de bu tüzel kişilere ilişkin bilgilerin kişisel veri olarak değil, yalnızca ticari sır olarak kabul edilmesini öngörmektedir²². Diyebiliriz ki gerçek veya tüzel kişilerin koruma kapsamına alınmasına dair uluslararası mevzuatta ve öğretide görüş birliği bulunmamaktadır. Ancak, kişisel verilerin korunması ile bireysel özerkliğin gerektirdiği bireyin kendisi ile ilgili bilgilerin üzerinde denetim hakkının sağlanması amaçlanmaktadır. Kişisel verilerin korunması hakkı da bu bağlamda insan hakkı kapsamında değerlendirilmektedir. İşte bu nedenledir ki kişisel verinin tüzel kişileri de kapsadığı tanım örnekleri bir kenara bırakılırsa, yalnızca gerçek kişilere ilişkin bilgileri güvence altına alması yerindedir. Bununla birlikte tüzel kişilere ilişkin bazı verilerin içerisinde gerçek kişiye ilişkin bilgiler de bulunabilmektedir. Kişisel verilerin korunması esas olarak bireyin özerkliğini ve haklarını korumayı amaçladığından gerçek kişiye ilişkin bu veriler kişiyi belirli veya belirlenebilir kılıyorsa kişisel verilerin korunması kapsamına dahil

verilerin korunması mahremiyet, özel hayat, kişi veya aile onuru gibi geleneksel değerlerle ilişkilendirilmiştir. Bu anlamda tüzel kişilerin kişilik hakkı, insan kimliği veya özel hayatının olmadığından bahisle koruma kapsamına alınmaması gerektiği, aksine incelemeye açık olmaları gerektiği savunulmuştur. Bkz., Douwe Korff, **Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons**, Study Contract ETD/97/B5-9500/78, s. 41. (Bundan böyle **Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons** olarak anılacaktır).

²⁰ A.g.e., s. 42-43.

²¹ I.N. Walden ve R.N. Savage, "Data Protection and Privacy Laws: Should Organisations Be Protected?", **International and Comparative Law Quarterly**, C. 37. S. 22, 1988, s. 347.

²² Durmuş Tezcan, "Bilgisayar Karşısında Özel Hayatın Korunması", **Anayasa Yargısı Dergisi**, C.8, 1991, s. 389. Tüzel kişilere ait bilgiler, kişisel verilerin korunması kapsamında güvence altına alınmasa dahi marka, patent, telif hakkı, gizlilik sözleşmesi gibi alternatif hukuki güvenceler kapsamında bu bilgilerin denetimi sağlanabilmelidir. Ayrıca bkz., Kang, **a.g.m.**, s.20.

edilebilecektir.

Hangi hallerde kişinin kimliğinin belirli veya belirlenebilir olduğunun tespit edilmesi, o kişinin bir grup insan tarafından ayırt edilebilmesi veya henüz ayırt edilmemiş olmakla birlikte bu kişinin diğerlerinden ayırt edilmesinin mümkün olduğu anlamına gelmektedir. Konu ile ilgili Direktifin düzenlemesine tekrar baktığımızda kimliği belirlenebilir kişi, “*özellikle bir kimlik numarasına veya fiziksel, psikolojik, zihinsel, ekonomik, sosyal kimliğine dayanılarak, doğrudan veya dolaylı şekilde kimliği belirlenebilir olan kimse*” olarak tanımlanmaktadır²³. Buna göre kişinin ismi, dış görünüşü ile kimliğinin doğrudan belirlenebilir olması mümkün olduğu gibi telefon numarası, pasaport numarası, yaşı, mesleği gibi birden çok ölçütün değerlendirilmesi ile de dolaylı olarak belirlenmesi mümkündür²⁴. Hangi bilgilerin kişinin diğerlerinden ayırt edilmesi için yeterli olduğu her somut olayın özelliklerine göre değerlendirilmelidir²⁵. Bahsi geçen “belirleme” faaliyeti açısından bazı unsurların dikkate alınması gereklidir. Genel bir değerlendirme yapmak gerekirse kişisel verilerin korunması kapsamında bir kişinin kimliğinin belirlenebilir olup olmadığını tespit etmeye çalışan kişinin, bu amaçla “kullanılabilecek makul tüm araçları” göz önüne alınmalıdır²⁶. Bu anlamda somut olayın tüm özellikleri incelenirken kişinin kimliğinin belirlenebilmesi amacıyla kullanılabilecek resmi siciller, kayıtlar, gazetecinin haberi hazırlama sürecindeki yoğun çaba ile kişinin kimliğinin tespit edilmesi örneğinde olduğu gibi ilgili veriyi inceleyen kişinin özellikleri göz önünde tutulmalıdır. Ayrıca belirleme faaliyetinin finansal maliyetleri ile teknolojik gelişmeler de kişinin kimliğinin belirlenebilir olup olmadığında göz önünde tutulmalıdır.

Kişinin kimliğinin belirlenebilir olması unsurunun gerektirdiği diğer bir

²³ AB Direktifi, m. 2/a.

²⁴ Avrupa Adalet Divanı da kişisel veri kapsamının Direktifin 2. maddesinin a bendine göre, bir kimsenin ismi ile birlikte onun telefon numarası, çalışma şartları ve hobileri gibi bilgileri de kapsayacağını kabul etmiştir. Bkz., Bodil Lindqvist, C-101/01, 06.11.2003, para. 24.

²⁵ Article 29 Working Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 20.06.2007, 01248/07/EN, WP 136, s. 13.

²⁶ AB Direktifi, 26 numaralı gerekçe.

sonuç ise anonim verilerin kişisel veri kapsamında değerlendirilip değerlendirilmeyeceğine ilişkindir. Verilerin anonimleştirilmesi ile belirlenebilir bir birey ile verinin arasındaki bağ koparılmakta, bireyin kimliğinin tespiti olanaksız hale getirilmektedir. Bu bağlamda anonim veriler, kişisel veri sayılmadıklarından veri koruma ilkelerinin kapsamı dışında kalacaklardır²⁷.

C. KİŞİYE İLİŞKİN VERİ

Verinin kişiye ilişkin olması unsurunda aranan kriter, söz konusu verinin “içerik”, “amaç” veya “sonuç” yönünden kişi ile bağlantılı olmasıdır. Bilginin içerik bakımından kişiye ilişkin olması söz konusu bilginin kişi hakkında olmasını ifade eder. Çalışan hakkında işyerinde düzenlenen dosyalar, bir hastanın tıbbi kayıtları bu duruma örnek olarak verilebilir. Bazı hallerde ise bilgi, içerik itibarıyla kişiye ilişkin olmamasına rağmen bu bilginin kişisel veri olarak kabul edilmesi gerekebilmektedir. Örneğin, bir taşınmazın değeri genel olarak kişisel veri kapsamında değerlendirilmeyecektir. Ancak bu taşınmazın değeri malikinin vergi yükümlülüğünün kapsamını belirlemek için kullanılabilmektedir. Bu bağlamda taşınmazın değeri, kişisel veri kapsamında değerlendirilecektir²⁸.

²⁷ Aynı doğrultudaki düzenleme için bkz., AB Direktifi, 24 numaralı gerekçe. Takma ad kullanılan veriler ile şifreli veriler ise anonim verilerden farklı özelliktedirler. Söz konusu veriler özellikle istatistikî çalışmalar amacıyla kişilere kendilerini temsilen bir kod numarası ya da farklı isim verilmekte, kişilerin kimliklerini gizli tutmakta ise de gizli tutulan bu bilgilere ulaşıp söz konusu kişilerin kimlik bilgilerinin tespiti ihtimal dahilindedir. Tıbbi bir araştırmada kullanılmak üzere kişilerin sağlıklarına ilişkin verilerin bilgisayar tarafından rastgele olarak atanan kodlar dahilinde bir ilaç firmasına gönderilmesi örneğinde söz konusu verileri ilk elden toplayan doktor şifrelenmiş bu verileri ilgili kişiler ile ilişkilendirerek kişileri belirli kılacaktır. Nitekim bu gibi durumlarda şifrelenen bu türden veriler de kişisel veri olarak kabul edilecek ve kişisel verilerin korunmasına ilişkin düzenlemelere tabi kabul edilecektir. Bazı yazarlar kişisel veri kavramının şifreli verileri veya takma ad kullanılan verileri de kapsamına alacak şekilde geniş tutulmasının tıbbi araştırmalar gibi uzun vadeli araştırmalar açısından daha kârlı ve pahalı olacağını dile getirmişler, bir anlamda kişisel verilerin korunmasının mali yönüne ağırlık vermişlerdir. Bkz., 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, 2000, s. 74. Ayrıca anonimleştirme sürecinin Direktif kapsamında kişisel veri işlenmesi olduğuna dair bkz., Ian Walden, “Anonymising Personal Data”, **International Journal of Law and Information Technology**, C.10, S.2, 2002, s. 224-237.

²⁸ Article 29 Working Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 20.06.2007, 01248/07/EN, WP 136, s.9.

Bilginin amaç yönünden kişiye ilişkin kabul edilebilmesi bu kişinin durumunu veya davranışlarını değerlendirmek, kişiyi etki altında bırakmak amacıyla bilginin kullanılması halinde mümkündür²⁹. Bununla birlikte, somut olayın özelliklerine göre bir bilginin kullanılması kişinin bazı hak ve menfaatlerini etkileyebildiği takdirde bu bilginin sonuç itibarıyla söz konusu kişiye ilişkin olduğu kabul edilir. Burada önemli olan bilginin kullanılmasının kişi hak ve menfaatleri üzerindeki etkisinin boyutu değil, yalnızca kişinin başkalarından farklı bir muameleye maruz kalıp kalmadığıdır. Örneğin, bir taksi durağının müşterilerine daha iyi hizmet sunmak ve yakıt tasarrufu sağlamak amacıyla uydu üzerinden taksilerini izleyen bir sistemi kullanması taksi sürücüsü hakkında bilgi toplamak amacı taşımamaktadır. Ancak bu sistem sürücünün hız limitine uyup uymadığı, seyir halinde olup olmadığı gibi verimliliğine ilişkin bilgilerin de elde edilmesine olanak tanımaktadır. O halde bu sistemden alınan bilgiler, sürücülerin menfaatlerini ilgilendirdiğinden kişisel veri olarak kabul edilmelidir³⁰.

Buraya kadar çalışma konumuzun merkezini oluşturan kişisel veri kavramını açıklamaya çalıştık. Birçok farklı tanımlamaya karşın kişisel verinin üzerinde görüş birliği olan tanımı, *“belirli veya kimliği belirlenebilir bir kişiye ilişkin bütün bilgiler”*dir. Buna göre kişinin adı, doğum tarihi, ulusal kimlik numarası, fotoğrafı, parmak izi, sağlık raporları kişisel verilere örnek olarak verilebilir. Yalnızca gerçek kişilere ilişkin verilerin mi kişisel veri olarak değerlendirileceği yoksa tüzel kişilere ilişkin verilerin de bu kapsamda değerlendirilip değerlendirilemeyeceğine dair farklı yaklaşımlar mevcuttur. Ancak çalışmamızın ileriki bölümlerinde de vurgulayacağımız üzere kişisel verilerin korunması bir insan hakkıdır. İşte bu nedenledir ki kişisel verilerin kapsamına gerçek kişilere ilişkin bilgiler girmektedir. Son olarak kişisel veri kavramı ve bunun korunmasının ihtiyacı birey ve onun temel özgürlüklerinin sağlanması ile ilgilidir. Konunun daha iyi anlaşılması için korumanın

²⁹ Article 29 Working Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 20.06.2007, 01248/07/EN, WP 136, s.10.

³⁰ Article 29 Working Data Protection Working Party, **Opinion 4/2007 on the Concept of Personal Data**, 20.06.2007, 01248/07/EN, WP 136, s.11.

gerekliliğine değinmemiz gereklidir.

II. KİŞİSEL VERİLERİN KORUNMASI GEREKLİLİĞİ

Kişisel verilerin korunması gerekliliğinin fark edilmesi nispeten yenidir. Konu ile ilgili hukuksal düzenlemeler teknolojik gelişmeler ve küreselleşme ile eş zamanlı olarak gelişme göstermiştir. Bilgi, içinde bulunduğumuz yeniçağın temel üretim ve güç faktörünü oluşturmaktadır. Kamu organları düzenin sağlanması, kamu hizmetlerini sunma, vergi toplama gibi nedenlerle; özel teşebbüsler ise verimliliğin ve kârlılığın geliştirilmesi için bilgiye gereksinim duymaktadır. Bu anlamda özellikle son yirmi yıldan beri bilişim teknolojisinde gerçekleşen olağanüstü gelişmeler birey ile ilgili bilgiye yönelik açlığı daha da görünür hale getirmiştir. Bir zamanlar yalnızca kağıt üzerindeki ya da loş hafızalarımızdaki bilgiler artık gelişen teknolojik altyapı ile birlikte bilgisayarların dijital hafızalarında veya geniş veri tabanlarında depolanabilmektedir³¹. Kişisel verilerin daha ucuz, kolay ve hızlı depolanabilmesi, internetin de yaygınlaşmasıyla birlikte artık bunların paylaşılabilmesi ve eşleştirilebilmesi sağlanmıştır. Elbette ki kişisel veri artışının tek sebebi teknik alanda yaşanan ilerlemeler değildir. Kişisel veri miktarı çevrimiçi sosyal paylaşım ağları ve kullanıcı tabanlı sistemlerin ortaya çıkması ile de önemli ölçüde artmıştır. Böylesi bir dijital ortamda kişilerin temel hak ve özgürlüklerine yönelik çeşitli risklerin ortaya çıkması adeta kaçınılmaz olmuştur.

İsteklerimiz, tüketim tercihlerimiz, ilgi alanlarımız, siyasal düşüncelerimiz ve hatta bize rutin gelen gündelik eylemlerimize dair bıraktığımız izler takip edilmekte; bizim bilgimiz dahilinde veya haricinde hakkımızda sürekli veriler toplanmakta, işlenmekte ve depolanmaktadır³². Öyle ki artık belli bir amaca hizmet eden izleme, etiketleme, dinleme, seyretme, kaydetme ya da kimlik belirleme aracına yakalanmamamız olanaksızdır³³. İşte bu durum bireyin sürekli izlendiği duygusunu

³¹ Daniel J. Solove, **The Digital Person Technology and Privacy in the Information Age**, New York University Press, ABD, 2004, s. 1.

³² A.g.e., s. 19.

³³ David Lyon, **Günlük Hayatı Kontrol Etmek, Gözetlenen Toplum**, çev. Gözde Soykan, İstanbul,

taşımasına neden olmaktadır. Bu anlamda kamu organları ve özel kurumlar tarafından bireylere yönelik gözetim isteğine dair endişelerin arttığını söylemek yanlış olmaz. Nitekim içinde bulunduğumuz evre bu bağlamda gözetim toplumu olarak adlandırılmaktadır³⁴.

Kişisel verilerin korunmasının gereksinimini daha iyi anlayabilmemiz için bu iki kavramın tanımlamalarına kısaca bakmamız gerekir. Gözetim en yalın şekliyle, bir veya daha çok kişinin iletişim veya eyleminin sistematik olarak araştırılması ve izlenmesidir³⁵. *Westin* kişiye yönelik gözetimi üç farklı boyutta incelemektedir. Bunlar; kişinin bulunduğu yerin, hareketlerinin, konuşmalarının ya da özel yazışmalarının kişinin bilgisi dışında optik veya akustik araçlarla gözetlenmesi olan “fiziksel gözetim”; yazılı veya sözlü testlerin ya da araçların veya maddelerin kullanılması ile kişiden isteyerek vermediği bilgileri elde etme veya kişinin özel hayatı ve kişiliği bakımından önemli olabilecek hususları farkında olmadan açığa çıkarma olan “psikolojik gözetim”; son olarak da veri işleme faaliyetleri aracılığıyla kişi veya gruplar hakkında bilginin toplanması, değişimi ve kullanımı olan “veri gözetimi”dir³⁶. *Lyon* gözetimi kişisel veri kapsamında değerlendirmiştir. Bu bağlamda gözetim, hakkında veri toplananları etkileme veya idare etme amacıyla tanımlanmış ya da tanımlanmamış herhangi bir kişisel veri toplanması ve işlenmesi olarak tanımlanmaktadır³⁷. Gözetimin geçmişi çok eski dönemlere dayansa bile son

Kalkedon Yay., 2006, s. 11.

³⁴ Garry T. Marx, “Privacy and Technology”, January 1996, (Çevrimiçi) <http://web.mit.edu/gtmarx/www/privantt.html>, 01.05.2013. Ayrıca bkz., **A Report on the Surveillance Society, For the Informational Commisioner by the Surveillance Society Network**, Eylül, 2006, haz. David Murakami Wodd, s. 1.

³⁵ Roger Clarke, “Dataveillance: Delivering '1984'”, February 1993, (Çevrimiçi) <http://www.rogerclarke.com/DV/PaperPopular.html>, 01.05.2013.

³⁶ Alan Westin, **Privacy and Freedom**, New York, 1970, s. 52 vd.'den aktaran Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, 2008, Turhan Kitabevi, s. 193 vd.

³⁷ Lyon, **a.g.e.**, s. 13. Ayrıca burada konu ile ilgili başka bir kavramın da tanımlamasını yapmamız gerekmektedir. Gelişmiş teknolojik altyapıya sahip veri tabanlarında kişisel verilerin toplanması ve saklanması kolaylık sağlandığı gibi bu veriler arasında eşleştirmelerin yapıp bireyler hakkında profillerin oluşturulması mümkün hale gelmiştir. Bu durum, farklı bir gözetim çeşidi olarak “veriizleme”nin (dataveillance) tartışılmasına neden olmuştur. Veriizleme ilk olarak Roger Clarke tarafından 1980'li yılların ortalarında dile getirilmiştir. Bu anlamda fiziksel veya elektronik gözetimden farklı olarak “veriizleme”, bir veya birden çok kişinin hareketlerinin veya iletişiminin “veri sistemleri aracılığıyla” sistemli olarak araştırılması ya da izlemesi olarak tanımlanmıştır. Veriizleme iki şekilde karşımıza çıkabilir. İlki, özel olarak belirli kişilerin izlenmesidir. Diğerisi ise

zamanlarda bilişim teknolojilerinin gelişimine paralel olarak asıl ağırlığını hissettirmeye başlamıştır. Yukarıda yer verdiğimiz tanımlamalara da baktığımızda günümüzde bireyin gözetimine ilişkin en etkili ve en kolay yolun veri gözetimi yani kişisel veriler aracılığıyla gözetim şeklinde gerçekleştiğini söyleyebiliriz. Gözetim araçları sayesinde toplanan kişisel bilginin miktarı sürekli artmıştır. Bilişim teknolojileri potansiyel olarak olağanüstü kalabalık bir kitleyi görünmeksizin ve bilinmeksizin izlenebilir hale getirmiştir³⁸. Genel itibariyle sosyal kontrolün gerçekleştirilmesi amacıyla yönelik olarak bireylerin ve grupların kimliklerinin saptanması ve durumlarının takip edilmesinin rutinleşmesi gözetim toplumu kavramının tartışılmasına neden olmuştur. Buna göre gözetim toplumu, gözetime elverişli teknikler kullanılarak örgütlenmiş ve yapılanmış toplumdur³⁹. Lyon ise yönetilme ve kontrol işlevleri için iletişim ve bilgilendirme teknolojilerine bağımlı olan bütün toplumları gözetim toplumu olarak tanımlamıştır⁴⁰. Peki, gözetimin ve gözetim toplumunun bireylere yönelik taşıdığı potansiyel tehlike nedir? Gözetim araçları vasıtasıyla bir bütün olarak ve sınırsız bir şekilde izlenen ve kayıt altına alınan ve egemen güçlerin karşısında şeffaflaşan bireyin özgürlüğünden söz edilebilmesi olanaksızdır. Böyle bir durumda birey yalnızca özgürlüklerinden yoksun bırakılmakla kalmaz, davranışlarını özgür iradelerine göre yönlendiremeyecekleri ve hayatlarını yönetemeyecekleri bir durum ortaya çıkar. Ayrıca rutin gözetime tabi birey, demokrasinin işlemesi için esas olan bağımsız düşünceyi gerçekleştiremeyecektir⁴¹. Bireyin davranışlarının izlenildiğini ve kaydedildiğini

kitlesel veriizleme olarak adlandırabileceğimiz bir grubun ya da daha geniş bir topluluğun izlenmesidir. Konu ile ilgili ayrıntılı bilgi için bkz., Clarke, "Dataveillance: Delivering '1984'". Herkes için elektronik profillerin oluşturulması ve sistemli olarak kişilerin kendileri ile ilgili bu bilgisayar verileri üzerinden sistematik olarak izlenmesi herhangi bir şüphe olmaksızın yapılan keyfi soruşturmaya eşdeğerdir. Bu yöntemin temel mantığı herkesin potansiyel suçlu olduğuna dayanmaktadır. Bu durum ise suçluluk karinesine aykırıdır. Bkz., Elif Küzeci, **Kişisel Verilerin Korunması**, Ankara, 2010, s. 58.

³⁸Veysel Bozkurt, "Gözetim ve İnternet: Özel Yaşamın Sonu Mu?", **Birikim Dergisi**, S.136, 2000, s. 70.

³⁹**A Report on the Surveillance Society**, For the Informational Commisioner by the Surveillance Society Network, haz. David Murakami Wodd, Eylül 2006, s. 3.

⁴⁰Lyon, **a.g.e.**, s. 11.

⁴¹Deborah G. Johnson, **Computer Ethics**, Prentice- Hall, Inc 2001, s. 120'den aktaran Gözde Dedeoğlu, "Gözetleme, Mahremiyet ve İnsan Onuru", **TBD Bilişim Dergisi**, 2004, (Çevrimiçi) <http://dergi.tbd.org.tr>, 01.05.2013, s. 3.

bilmesi otosansüre neden olur ve yalnızca bu durum dahi insan onurunu zedeleyicidir⁴².

Bireyin izlenmesi ve dolayısıyla davranışlarını sınırlandırma sorunun yalnızca bir parçasıdır. Konunun diğer bir boyutu ise verinin herhangi bir belirli amaçtan yoksun olarak daha sonra kullanılmak üzere depolanmasıdır⁴³. Bu durum bireyin kendisi ile ilişkin bilgileri üzerindeki denetim hakkını ortadan kaldırır. Oysaki bireysel özerkliğin sağlanması ancak bireye kişisel verileri üzerinde denetim hakkının güvence altına alınması ile mümkündür. Ayrıca belirtmemiz gerekir ki bireylerin kişisel verilerin korunmasına dair talepleri kendileri hakkındaki bilgilerin yalnızca vermiş oldukları onay kapsamında kullanılacağına dair güvencelerin sağlanmasına yöneliktir⁴⁴.

Kişisel verilerin korunması gerekliliği ile ilgili diğer bir husus ise demokrasi ekseninde açıklanmaktadır. Kendisi hakkındaki bilgi üzerinde denetimini kaybeden birey, güçsüzleşir. Bu durum bireyin temel hak ve özgürlüklerinin, bireysel çıkarlarının tehlikeye girmesine neden olur. Oysaki demokratik bir devletin gerekliliği bireysel hakların anayasal düzeyde korunmasıdır. İşte kişisel verilerin korunması ile bireylerin kendileri ile ilgili kişisel verileri üzerinde denetim hakkı sağlanmakta, temel hak ve özgürlükleri güvence altına alınmaktadır.

Tarihsel sürece baktığımızda kişisel veri sayısındaki artış ile bu verilerin kaydı konusundaki gelişmeler insan hak ve özgürlükleri, insan onuru ve demokratik topluma yönelik haklı tedirginliklerin çoğalmasına neden olmuştur. Nitekim kamusal tepkinin yansıması olarak 1970'li yıllardan itibaren Avrupa'da konu ile ilgili hukuksal düzenlemeler kabul edilmeye başlanmıştır. Bu bağlamda Almanya'nın Hessen eyaletinde ilk veri koruma yasası kabul edilmiş ve bunu takiben 1973 yılında İsveç'te ilk ulusal veri koruma yasası kabul edilmiştir. Kişisel verilerin korunması ile insan

⁴²Kang, **a.g.m.**, s. 1269. Aynı doğrultuda görüş için bkz., Solove, **a.g.e.**, s. 35.

⁴³Solove, **a.g.e.**, s. 41.

⁴⁴**A.g.e.**, s. 43.

onurunun ve kişilik hakkının güvence altına alınacağını vurgulayan bir diğer önemli gelişme ise 1983 yılında Alman Anayasa Mahkemesinin verdiği “Nüfus Sayım Kararı”dır⁴⁵. Mahkeme bu kararında bireysel başvuru yolu ile önüne getirilen Nüfus Sayım Yasası'nı anayasaya aykırı bulmuştur. Yaptığı inceleme sırasında Mahkeme, devletin kişisel veriler ile ilişkisini Federal Almanya Cumhuriyeti Anayasası 1. maddesinin 2. fıkrasında düzenlenen insan onuru ve 2. maddesinin ilk fıkrasında düzenlenen kişiliğin korunması hakkına dair hükümleri değerlendirerek “bilgilerin geleceğini belirleme hakkı”nı kabul etmiştir. Bu hak ile bireye verilerinin kullanılması üzerinde denetim hakkı sağlanmış; sürekli izlenen ve kayıt altına alınan bireyin kişiliğini serbestçe geliştiremeyeceği ve özgürlükçü demokratik toplumun sağlanamayacağına vurgulanmıştır.

Buraya kadar gelişen teknoloji ile eş zamanlı olarak kişisel verilerin bireyler açısından teşkil ettiği öneme değinmeye çalıştık. Elbette ki kişisel verilerin eskisine nazaran daha fazla ve rutin biçimde sunulduğu, bilişim teknolojilerinin saklama ve dağıtma olanakları açısından bu denli güçlü olduğu günümüzde, teknolojik bir arıza veya zayıflık nedeniyle bu verilerin bozulması veya bu verilere izinsiz erişim içinde söz konusu olabilmektedir. Belirli bir amaç doğrultusunda verilen kişisel bilgilerin bozulmadan korunacağı, sadece belirlenen amaç doğrultusunda kullanılacağı, üçüncü şahıslara dağıtılmayacağı veya veri öznesinin bilgi ve rızası olmadan verilmeyeceği, veri öznesinin kişisel bilgisini gözden geçirmesine ve gerekiyorsa bu bilgilerde düzeltme yapabilmesine, geçerliliği kalmayan bilginin iptal edilmesine dair hukuksal güvencelere gereksinim duyulması doğaldır⁴⁶. İşte bu anlamda kişisel verilerin korunması, bireye verilerinin kullanılması üzerinde denetim hakkı sağlanarak temel hak ve özgürlükleri güvence altına alınması açısından bir gerekliliktir. Öyle ki hukuki çare olarak kişisel verilerin işlenmesi sürecindeki herhangi bir aşamada etki olanağını kaybetmiş bireye kişiliğine bağlı her türlü veri üzerinde tasarrufta bulunma hakkı sağlanması amacıyla kişisel verilerin korunması hakkı kabul edilmeye

⁴⁵BverfGE, 65, 1-Volkszählung.

⁴⁶Dedeoğlu, **a.g.m.**, s.2.

başlanmıştır.

III. KİŞİSEL VERİLERİN KORUNMASI HAKKININ HUKUKİ NİTELİĞİ

Bilgi merkezli modern yaşamın temeli olan kişisel verilerin özünde hangi hukuki varlık ve menfaatin yattığına yönelik farklı teorik tartışmalar mevcuttur. Tartışmalar kişisel verilere yönelik korumanın hangi hak temeline dayanması gerektiği yönündedir. Genele baktığımızda bu teorik tartışmalar verilerin, üzerinde tasarrufta bulunabilen bir mal olarak mı kabul edildiği yoksa bireylerin sahip olduğu temel haklardan mı olduğu üzerinde yoğunlaşmıştır. Burada konu ile ilgili esas itibariyle iki yaklaşım dikkat çeker. Bunlardan biri, kişisel verilerin özünü ve bu verilerin korunmasını ekonomik bir hak olarak değerlendiren yaklaşımdır. Diğer yaklaşım ise konunun insan hakları kapsamında değerlendirilmesidir⁴⁷. Temelde ikiye ayırdığımız yaklaşımların alt başlıkları çeşitli olsa da bu alt başlıkları da üç temel başlık altında inceleyebiliriz. Bu başlıklar (i) mülkiyet hakkı görüşü, (ii) fıkri mülkiyet hakkı görüşü ve (iii) özel hayatın gizliliği hakkı kapsamında kişisel verilerin korunmasıdır⁴⁸.

A. Mülkiyet Hakkı Görüşü

Kişisel verilerin mülkiyet hakkı ile açıklanması esasında kişisel verilerin üzerindeki denetimin kime ait olduğuna dayanır. Bu denetim tartışmasından yola

⁴⁷Roger Clarke, “Beyond OECD Rules: Privacy Protection for the 21st Century”, (Çevrimiçi), <http://www.rogerclarke.com/DV/PP21C.html>, 01.05.2013.

⁴⁸Bu temel başlıklar dışında kişisel verilerin korunmasına dair ekonomik hak yaklaşımına ayrıca kişisel verilerin ticari sır olarak değerlendirilmesi ve buna ilişkin bazı hükümler ile korunabileceğini de savunan yazarlar mevcuttur. Bkz. Pamela Samuelson, “*Privacy as Intellectual Property*”, **Stanford Law Review**, C.52, 2000, s. 1152. Bunun gibi konu, diğer insan hak alanları ile de ilişkilidir. Kişisel verilerin korunması hakkı bu bağlamda insan onuru, bireysel özerklik ve bilgilerin geleceğini belirleme hakkı, düşünceyi açıklama özgürlüğü, anonimlik hakkı, bilgi edinme hakkı, özel haberleşmenin gizliliği, bilim özgürlüğü gibi çok geniş bir alan ile ilişkilidir. Ayrıntılı bilgi için bkz., Küzeci, **a.g.e.**, s. 85 vd.; Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, İstanbul, 2008, Beta Yay., s. 137 vd. Çalışmamızın konusunu oluşturan suçlar Türk Ceza Kanunu’nun “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlığı altında düzenlenmiştir. Bu nedenle çalışmamızda bir insan hakkı olarak kabul ettiğimiz kişisel verilerin korunması hakkının özel hayatın gizliliği hakkı ile değerlendirilmesine yer verilmiştir.

çıkan bazı yazarlar kişisel verileri mülkiyet hak alanı ile açıklamaya çalışmışlardır⁴⁹. Kişisel verilerin bir mülkiyet türü olduğu ve anlamda kişisel verilerin hukuki niteliğinin mülkiyet hakkı ile açıklandığı görüş özellikle Amerikan hukukunda ileri sürülmüştür. Kıta Avrupası ve Amerikan yaklaşımı arasındaki bu görüş farklılığı kişisel verilerin korunmasına hangi açıdan yaklaşıldığını ortaya koymaktadır. Kıta Avrupası'nda kişisel veriler “sosyal değer” merkezli olarak açıklanırken ABD'de “ekonomik-teknolojik” yaklaşım merkez alınmıştır⁵⁰. Amerikan hukukunda kişisel verilerin korunması hakkını da içeren özel hayatın gizliliği hakkı anayasal bir hak değildir. Özel yaşamın gizliliği hakkı içtihatlarla kabul görmüştür. Son zamanlarda kişisel verilerin korunması gerekliliğine dair tartışmalarda artış görülmesine rağmen diyebiliriz ki ABD'de kişisel verilerin korunması son derece düşük düzeydedir. ABD'de konu ile ilgili katı ve kapsayıcı bir düzenleme yerine sektörel çözümler tercih edilmiştir⁵¹. Bu nedenledir ki Kıta Avrupası'nda kişisel verilerin niteliği insan hakları dahilinde açıklanırken, ABD'de veri pazarının etkinliğine yönelik kaygılar ve kişilerin verileri üzerinde mülkiyet hakkına sahip olduğu görüşü öne çıkmaktadır.

Kişisel verilerin hukuki niteliğinin mülkiyet hakkı ile açıklandığı yaklaşıma göre herkes kendisine ilişkin kişisel verilerin sahibidir ve herkes mülkiyetindeki bu verilerin hangi şartlar altında kullanılabileceğini kontrol edebilmelidir. Bilginin güç ile eşdeğer tutulduğu günümüzde, kişisel veriler ticari değer kazanmıştır⁵². Özellikle serbest piyasa ekonomisinde şirketler, kişisel verileri şirket malvarlığı olarak saymakta ve tüketici bilgilerini işlemek amacıyla yazılım sistemlerine yatırım

⁴⁹ Solove, **a.g.e.**, s. 76. Burada önemle belirtmek isteriz ki, aşağıda insan hakları yaklaşımında da açıklayacağımız gibi, her iki yaklaşım esasen kişisel verilerine ilişkin bireyin denetimini açıklamak ile birlikte temel aldıkları görüşler açısından farklı sonuçlara ulaşmaktadırlar.

⁵⁰ Clarke, “Beyond OECD Rules: Privacy Protection for the 21st Century”.

⁵¹ Küzeci, **a.g.e.**, s. 61. Bunun gibi kişisel verilerin korunmasının mülkiyet gibi bir hak alanı kapsamında değerlendirilmesi, Amerikan hukukunun aksine, Kıta Avrupası'nın bilgilerin gizliliğinin tarihçesine, teorisine ve buna dair teamüllerine aykırı olacaktır. En basit örnek, AB üyesi birçok devlet kişisel verilerin korunmasını anayasal bir temel hak olarak kabul etmesidir. Viktor Mayer-Schönberger, “Beyond Privacy, Beyond Rights-Toward a 'Systems' Theory of Information Governance”, **California Law Review**, S. 98, s. 1862.

⁵² Corien Prins, “When Personal Data, Behavior and Virtual Identities Become A Commodity: Would A Property Rights Approach Matter?”, **SCRIPT-ed A Journal of Law, Technology and Society**, C.3, S.4, 2006, s. 274.

yapmaktadırlar. Şirketler topladıkları tüketici bilgileri ile sundukları hizmetin kalitesini arttırmakta, iç pazar stratejilerini belirlemekte, bu bilgileri üçüncü kişilere devrederek ticari kazanç sağlamaktadırlar⁵³. Verilerin artan ticari değerine karşılık olarak veri pazarı da hareketlenmiştir. Ancak bu noktada veri sahiplerinin oynadıkları rol azalmaktadır. Kişi, belirli bir amaç için kendisine ait verilerin kullanımına dair bir şirket ile kişisel verilerini paylaşabilmektedir. Daha sonra bu şirket tarafından paylaştığı kişisel verilerinin amacı dışında kullanıldığını bilememekte, şirketin bu uygulamasının olumsuz sonuçları doğrudan kişi üzerinde doğmakta, ancak herhangi bir hak iddia edememektedir. Bu noktada mülkiyet hakkı görüşünü savunan yazarlara göre kişinin kendi kişisel verileri üzerinde mülkiyet hakkına sahip olduğu kabul edildiği takdirde kişi, sahip olduğu verilerin hangi işletmeler ile hangi bedel üzerinden paylaşabileceği konusunda pazarlık edebilecektir⁵⁴. Diyebiliriz ki mülkiyet hakkı görüşü prensipte iki menfaat üzerine kurulmuştur. Bunlardan ilki, kişinin kendisine ilişkin kişisel verilerini adil bir bedel karşılığında satabilmesidir. Ayrıca, mülkiyet hakkı modelinin kabulü ile şirketler verilerin toplanmasının ve üçüncü kişiler tarafından kullanılmasının sosyal maliyetini benimsemeye zorlanacak ve bu sayede özel yaşamın gizliliğinin korunması daha güçlü sağlanabilecektir⁵⁵. Ayrıca mülkiyet hakkı görüşünün kabulü ile veri sahibi, mülkiyet sahibine tanınan geniş yasal korumalardan yararlanabilecektir. Kişi, paylaştığı verilerin kötüye kullanılması durumunda dava açma veya zararın giderilmesi için talepte bulunabilecektir⁵⁶.

Kişiyne mülkiyet hakkı ile kendisine ilişkin veri üzerinde denetim olanağının sağlanması ve bu hakkını mahkeme önünde savunma imkanının verilmesi kişisel verilerin korunması açısından yeterli değildir. Mülkiyet hakkı görüşü, kavramın

⁵³ Samuelson, **a.g.m.**, s. 1126. Ayrıca son yıllarda birçok şirket e-ticaretin yaygınlaşması ile nakit para akışını sağlamak için tüketici bilgilerini satma eğilimi içerisindeyler. Kişisel veriler şirket birleşmeleri, yeniden yapılanma ve diğer şirket stratejileri nedeniyle el değiştirmektedir. Örneğin, 2011 yılında internet üzerinden perakende satış yapan Toysmart.com şirketi iflasını açıklamasının ardından yaklaşık 200,000 müşterisinin bilgilerini açık arttırma ile satışa çıkartmıştır. Prins, **a.g.m.**, s. 275.

⁵⁴ Samuelson, **a.g.m.**, s. 1127; Prins, **a.g.m.**, s. 279.

⁵⁵ Samuelson, **a.g.m.**, s. 1132; Prins, **a.g.m.**, s. 279.

⁵⁶ Küzeci, **a.g.e.**, s. 62.

niteliği itibariyle kişisel verilerin korunması açısından kabul edilemez. Öncelikle diyebiliriz ki, kişisel verileri açısından kişiye denetim ve pazarlık yapma olanağı sağlansa dahi pazarlıkta taraflar eşit değildir. Bu durum pazarlığın diğer tarafında hem devletin hem de özel sektör şirketlerinin bulunmasında ortaya çıkmaktadır. İlk olarak kişi, bir devlet kurumunda çalışmak için başvuruda bulunduğu verileri üzerindeki mülkiyet hakkından vazgeçecektir. Ayrıca çoğu zaman özel sektördeki şirketler korumaya ilişkin kuralların belirlenmesinde daha güçlü konumda yer almakta, sektörü şekillendirmekte ve bireyin kararlarını etkilemektedirler. Buna göre özel sektörde durum daha az varlıklı olan kesimin aleyhine olacaktır⁵⁷.

Mülkiyet hakkının temel niteliklerinden biri malikin malı sattıktan sonra artık rızası aranmaksızın malı satın alanın malı, üçüncü kişilere rahatlıkla devredebilmesidir. Mülkiyet hakkının malike sağladığı yetki olan bu tasarruf yetkisini kişisel veriler açısından kabul etmek güçtür. Kişisel verilerin korunması, kişinin kendisine ait verilerin kimler tarafından kullanıldığını bilmesini kapsamaktadır. Ancak tasarruf yetkisinin kişisel veriler açısından kabulü ile birlikte kişiye ait veriler kendisinden soyutlanmaktadır. Örnek vermek gerekirse birey, bir şirket ile kendisine ait verileri belirli bir amaç için kullanılması için anlaşmış olabilir. Ancak bu demek değildir ki bu anlaşma ile birey bu şirkete başka bir şirkete verileri satabilme yetkisi vermiştir ya da verilerin başka amaçlarla kullanılmasına onay vermiştir. Tasarruf yetkisi arabalara veya gayrimenkullere ilişkin olarak işleyebilirken aynı durum kişisel veriler açısından kabulü mümkün değildir⁵⁸. Kişisel verilerin üçüncü kişiye devrinin geçersizliği, kişisel verilerin korunması hakkının ve bilgilerin gizliliğinin her bir kişiye özgü ve bağlı olduğu insan hakkı yaklaşımı ile savunulmaktadır. Buna göre, bireyin kişiliğinin bir uzantısı olarak kabul edilen kişisel veriler ticari veya herhangi bir amaç ile devredilemez⁵⁹. Ayrıca mülkiyet hakkı,

⁵⁷ Paul M. Schwartz, “*Property, Privacy and Personal Data*”, **Harvard Law Review**, S.117, 2003-2004, s. 2082 (Bundan böyle **Property, Privacy and Personal Data** olarak anılacaktır); Prins, **a.g.m.**, s. 292.

⁵⁸ Samuelson, **a.g.m.**, 1138.

⁵⁹ Prins, **a.g.m.**, s. 280.

sınırlı kaynakların dağılımını sağlamaktadır. Bunun ise kişisel verilere uygulanabilmesi olanaklı değildir. Kişisel veriler bakımından herhangi bir kıtlık söz konusu değildir. Kişisel veriler açısından kıtlık bilgilerin gizliliğidir ve korumanın işlevi bunun sağlanmasıdır⁶⁰.

Kişisel verilerin korunmasının bir temel hak olarak kabulü gerekmektedir. Buna göre korunan menfaatler bireyin sosyo-ekonomik durumuna göre değişmemelidir. Kişisel verilerin korunması, bireyin kendi geleceğini belirleme hakkı ve demokratik bir toplum için gereklidir⁶¹.

B. Fikri Mülkiyet Hakkı Görüşü

Fikri mülkiyet hakkı görüşünü savunan yazarlar hem fikri mülkiyet hakları hem de kişisel verilerin korunmasının amacının bilgi ekonomisi olduğu, bilginin korunması ve kontrolünün sağlanmasının temel alındığından hareket etmektedirler⁶². Ayrıca hem fikri mülkiyet hakkında hem de kişisel verilerin korunmasında bireye ait ancak denetimini kaybedebileceği bir veri vardır. Her ikisinde de internet, denetimin kaybında etkilidir. Telif hakkıyla korunan ürün açısından internet bedava kopyalar çıkartmaya yardımcı olurken, kişisel verilerin korunmasın açısından ise davranışlarımızın sürekli ve uzun denetimini sağlamaktadır⁶³. Buna göre teknolojik gelişmeler karşısında fikri mülkiyet hakkı örneğinde olduğu gibi bir mülkiyet kavramının kişisel veriler açısından da sağlanabileceği savunulmuştur⁶⁴.

Kişisel verilerin fikri mülkiyet hakkı görüşü ile açıklanması kişisel veri sahibinin kendisine ilişkin veriler üzerindeki hakları ile fikri mülkiyet hukukundaki eser sahibinin meydana getirdiği eser üzerindeki manevi hakları arasındaki benzerlik açısından değerlendirilmektedir⁶⁵. Eser sahibinin manevi haklarından yola çıkılarak

⁶⁰ **Ibid**, s. 1138.

⁶¹ Schwartz, “**Property, Privacy and Personal Data**”, s. 2087.

⁶² Samuelson, **a.g.m.**, s. 1134; Prins, **a.g.m.**, s. 279.

⁶³ Küzeci, **a.g.e.**, s. 64.

⁶⁴ Prins, **a.g.m.**, s. 279.

⁶⁵ Ayrıca Bartow, fikri mülkiyet hakkı görüşüne dair değerlendirmesinde işletmelerin ünvanlarında ve

kişilerin verileri açısından da manevi hakların varlığının kabulü ile kişisel menfaatlerinin korunmasından bahsedilebilecektir⁶⁶. Eser sahibinin fikri mülkiyet hukukundan doğan manevi haklardan “*eseri umuma arz etme yetkisi*”, “*eserde değişiklik yapılmasını yasaklama yetkisi*” ile kişisel verilerin veri sahibine sağladığı haklar arasında bağlantı kurulabilir. Fikri mülkiyet hakkı dahilindeki bu haklara benzer şekilde kişisel veri sahibinin de kendisine ait verilerin bütünlüğünün ve doğruluğunun korunmasını isteme yetkisi, bu verilerin kimler ile hangi şartlar altında paylaşacağını tespit etme yetkisi bulunmaktadır⁶⁷.

Benzerlikler yukarıda değindiğimiz gibi olmak ile birlikte fikri mülkiyet hakkı ve kişisel verilerin korunması hakkı arasında önemli farklılıklar bulunmaktadır. Bu farklılıklar nedeniyledir ki fikri mülkiyet gibi bir hak alanı ile kişisel verileri korumak mümkün değildir. Öncelikle fikri mülkiyete konu olan değerler kişinin sarf ettiği güç ve çabanın ürünleridir. Kişisel veriler ise fikir ürünü olarak nitelendirilemezler. Bunlar, kişinin tabii varlığından doğmaktadır⁶⁸.

Fikri mülkiyet hakkı görüşünün olanaklı olmamasının diğer bir nedeni ise amaçsal farklılıktır. Fikri mülkiyet hakkının amacı gelişimin teşvik edilmesi, fikri ve sınai alanda kalkınmanın sağlanmasıdır. Bu hak ile eser sahibine fikri çabası sonucu meydana getirdiği eserlerinin ticari semerelerinden faydalanma imkanı sağlanmaktadır. Bu sayede yeni buluş ve eserlerdeki üretimin korunması teşvik edilmeye çalışılmaktadır. Bu anlamda eser sahiplerine eserleri üzerinde belirli bazı haklar tanınarak kamusal yararın sağlanması hedeflenmektedir. Ancak kişisel verilerin işlenmesi teşvik edici bir değer taşımamaktadır. Kişisel verilerin korunması ile amaçlanan verilerin izinsiz kullanılıp kullanılmadığı değil, bu verilerin kimler

verilerinde olduğu gibi bir mülkiyet hakkının kişisel veriler açısından kabul edilmesi gerektiği görüşündedir. Bkz., Ann Bartow, “*Our Data, Ourselves: Privacy, Propertization and Gender*”, **University of San Francisco Law Review**, C. 34, 2000, s. 685.

⁶⁶ Samuelson, **a.g.m.**, s. 1146.

⁶⁷ **A.g.m.**, s. 1148.

⁶⁸ **A.g.m.**, s. 1140; Prins, **a.g.m.**, s. 296.

tarafından, hangi şartlar altında ve ne tür amaçlarla kullanıldığıdır⁶⁹.

C. Özel Hayatın Gizliliği Hakkı ve Kişisel Verilerin Korunması

Günümüzde kişisel veriler, serbest piyasa ekonomisinde iç piyasa stratejilerinde kullanılmaktadır. Bu bağlamda kişisel verilerin ekonomik değer kazandığı yadsınamaz bir gerçektir. Ancak bireylerin başka çıkarlarının yanında ekonomik çıkarlarının da korunması gereklidir. Yukarıda değindiğimiz mülkiyet hakkı ve fikri mülkiyet hakkı görüşleri kişisel verilerin ticaret konusu yapılarak metalaştırılmasını teşvik etmektedir. Bu anlamda iki görüş de belirli açılardan veri sahiplerinin çıkarlarını korumakla birlikte, esas olarak menfaat dengesini veri işleyenlerin lehine bozmaktadır. Böylece kişisel verilerin sosyal değeri dikkate alınmamakta ve kişiliğe sıkı sıkıya bağlı bilgilerin korunması uluslararası ticaret ve serbest piyasa ekonomisinin işlemesi uğruna göz ardı edilmektedir. Açıktır ki bu durum insan olma ve insan onuruna uygun davranmayı temel alan insan hakları temelli yaklaşım ile çelişmektedir. Ayrıca kişisel verilerin korunmasının hukuki niteliğinin mülkiyet hak alanı ile açıklayan görüş seçme hakkı, düşünceyi açıklama özgürlüğünün de metalaştırılmasından farksızdır. Bu görüş, etik açıdan da yanlıştır⁷⁰.

Bireylerin ekonomik çıkarları dışında başka çıkarları da bulunmaktadır. Kişisel bilgileri teknolojik gelişmelere paralel olarak sınırsız bir şekilde toplanan, kullanılan, devredilen birey ile bu bireyin insan onuru ve temel hak ve özgürlüklerinin korunması gerekmektedir. Nitekim baskın görüş de kişisel verilerin korunmasının temel bir insan hakkı olduğu yönündedir⁷¹.

⁶⁹J. E. J. Prins, “*The Propertization of Personal Data and Identities*”, **Electronic Journal of Comparative Law**, C. 8, S. 3, s. 6'dan aktaran Hüseyin Can Aksoy, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Ankara, Çakmak Yay., 2010, s. 65.

⁷⁰ Paul M. Schwartz, “**Property, Privacy and Personal Data**”, s. 2086.

⁷¹ Clarke, “Beyond OECD Guidelines”. Kişisel verilerin korunmasının temel bir insan hakkı olarak kabul edildiği görüşü özellikle Kıta Avrupası'nda öne çıkmaktadır. Nitekim kişisel verilerin korunmasına ilişkin AB rejimi olarak ifade edilen 95/46/AT sayılı AB Veri Koruma Direktifi'nin 1. maddesinde de Direktif'in amacı, bireylerin temel hak ve özgürlüklerinin ve özellikle de özel hayatın gizliliğinin korunması olarak ifade edilmiştir. Bununla birlikte Amerikan hukukunda da özel hayat ile kişisel veri ilişkisine dair yargı kararları mevcuttur. San Francisco Federal Mahkemesi 2003 yılında

Kişisel verilerin korunması bir özgürlük sorunu olarak ilk aşamada özel hayat ve özel hayatın gizliliğine müdahale kapsamında ele alınmıştır. Ancak gelişen teknoloji ile birlikte özel hayatın gizliliği hakkına genel yaklaşım ve bu alanda benimsenen ilkeler kişisel verilerin korunmasında yetersiz kalmıştır. Öyle ki, tarihsel süreç içerisinde kişisel verilerin korunması özel hayatın gizliliği hakkından ayrılmaya başlamıştır. Yine de kişisel verilerin korunması ve özel hayatın gizliliği hakkı arasındaki yakın ilişki yadsınamaz. Bu nedenle kişisel verilerin korunması gereksinimine cevap ararken öncelikle özel hayat kavramı ile özel hayatın gizliliği hakkına değinmemiz gerekir⁷².

Özel hayat, son derece geniş ve bir o kadar da karmaşık yapısıyla tanımlanması güç bir kavramdır⁷³. Kavramın hukuki uygulamaya kesinlik kazandıracak kadar belirgin bir içerik ve belli sınırlara sahip olmamasının nedeni, özel hayat ile ilgili temel hakların iç içe geçmesinden ve özel hayatın gizliliği hakkı ile korunmak istenen değerlerin belirginleştirilememesinden kaynaklanmaktadır⁷⁴. Bununla birlikte insan hakları hukukundaki ve teknolojideki gelişmeler ile bu kavramın içinin doldurulmasına yönelik pek çok düşünce ortaya atılmıştır. Kavramın daha net açıklanması için Türk hukukunda da kabul gören “Üç Alan” teorisi kullanılmaktadır⁷⁵. Buna göre hayat, üç farklı alan olarak düşünülmüştür. Birinci

verdiği bir karar ile federal mahkumlar ve koşullu salıverilen kişilerin, Federal Soruşturma Bürosu veri tabanında saklanmak üzere DNA örneklerinin alınmasını öngören kanunu, işlemin hiçbir şüphe olmadan yapılmasından ötürü özel hayatın gizliliğini ihlal ettiği gerekçesiyle anayasaya aykırı bulmuştur. Bkz., Güçlü Akyürek, **Özel Hayatın Gizliliğini İhlal Suçu**, Ankara, Seçkin Yay., 2011, s. 50. Kişisel verilere ve özel hayatın gizliliği hakkına Amerikan yaklaşımının Kıta Avrupası yaklaşımından farklı olduğunu tekrar belirtmek ile birlikte anılan karar özel hayatın gizliliği ve kişisel verilerin korunması arasındaki yakın ilişkiye açısından önemlidir.

⁷² Küzeci, **a.g.e.**, s. 70 vd.

⁷³ Kavramın tanımlanmasının güçlüğü Avrupa İnsan Hakları Mahkemesi kararlarında da belirtilmiştir. Özel hayat kavramının hukuki uygulamaya kesinlik kazandıracak kadar belirgin bir içerik ve belirli sınırlara sahip bulunmadığının kabulü gerekmektedir. AIHM de bu anlamda kazuistik bir yol izleyerek her somut olayı kendisine özgü koşulları içinde değerlendirmiş ve özel hayat kavramına dahil olup olmadığını saptamıştır. Konu ile ilgili ayrıntılı bilgi için bkz., A. Şeref Gözübüyük ve Feyyaz Gölcüklü, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, Ankara, Truhan Kitabevi, 2009, s. 334. Konu ile ilgili örnek Mahkeme kararları için bkz., *Niemitz/Almanya*, b.n. 13710/88, k.t. 16.12.1992, para. 29; *Rotaru/Romanya*, b.n. 28341/954, k.t. 04.05 Mayıs 2000, para. 43, *P.G ve J.H/Birleşik Krallık*, b.n. 44787/98, k.t. 25.07.2001, para. 56.

⁷⁴ Benjamin J. Goold ve Liora Lazarus, **Security and Human Rights**, Portland, 2007, s. 61

⁷⁵ Akyürek, **a.g.e.**, s. 44.

olarak kişinin gizli hayatı diğer bir adıyla sır alanı yer almaktadır. Bu alan kişinin sırlarını kapsar ve ancak ilgili kişinin istemi halinde başka kişilere açılabilir. Kişinin sır alanı genel kişilik hakkının özüdür. Bu alan özel hayatın gizliliği hakkının çekirdek kısmını oluşturur. İkinci olarak “kişinin özel hayat alanı” gelir ve kişinin yakın çevresince bilinebilen hayatını ifade eder. Son olarak “kişinin genel yaşam alanı” yer almaktadır ve kişinin herkesle paylaşabileceği, kamuya açık alanlarını içermektedir⁷⁶.

Yukarıdaki gibi alanlara ayrıldığı kabul edilen özel hayata dair koruma kişinin kendisini geliştirebileceği, ifade edebileceği ve diğer kişiler ile ilişki kurabileceği bir alana duyduğu ihtiyaçtan doğar. Ayrıca özel hayatını kiminle paylaşacağını, neyi açıklayacağını veya saklı tutacağını kendisinin karar vermesi ile kişi, hayatına istediği şekilde yön verebilmektedir. Ancak izlenildiğini hissetmek, kişiye yönelik daha sonraki haksız eylemlere temel sağlanacağını düşünmek ile kişi baskı altında kalmaktadır. İşte, özel hayatın gizliliği hakkı sayesinde ise bireye kişinin kendisini geliştirmesi ve güvence altında olması sağlanmaktadır⁷⁷.

Özel hayatın gizliliği hakkı, gerek uluslararası hukukta gerekse ulusal hukukta garanti altına alınan temel bir haktır. Bu hak, İnsan Hakları Evrensel Beyannamesi’nin 12.maddesinde, Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesi’nin 17. maddesinde, Avrupa İnsan Hakları Sözleşmesi’nin 8.maddesinde ve 1982 Anayasasının 20. maddesinde temel bir hak olarak düzenlenmiş ve garanti edilmiştir. Özel hayatın gizliliği hakkının hem özel hayat kavramının görece karakteri hem de özel hayata yönelen saldırıların çeşitliliğinden ötürü mutlak bir tanımının yapılması güçtür⁷⁸.

⁷⁶ Oya Araslı, **Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi**, Yayınlanmamış Yüksek Lisans Tezi, s. 4 vd., Volkan Sırabaşı, **İnternet ve Radyo-Televizyon Aracılığıyla kişilik Haklarına Tecavüz (İnternet Rejimi)**, Ankara, Adalet Yayınevi, 2003, s.34-39.

⁷⁷ Ergun Özbudun, “*Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği*”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi 50.Yıl Armağanı**, C.1, Ankara, 1977, s. 266-268.

⁷⁸ Özel hayatın gizliliğinin tanımı ve kapsamının tartışmalı olmasının yanında konuyu açıklamak için pek çok kavram birbirlerinin yerine veya eş anlamlı olarak kullanılmaktadır. Türk Hukukunda özellikle özel hayatın gizliliği ile ilgili olarak “mahremiyet” kavramı da kullanılmaktadır.

Tıpkı özel hayat kavramı gibi özel hayatın gizliliği hakkına dair de pek çok tanımlama yapılmıştır. *Warren ve Brandeis*, ünlü makalelerinde gelişen toplum ve yaşam koşulları ile birlikte kişinin tinsel doğası, duyguları ve aklının tanınmış olduğunu dile getirmişlerdir. Uygarlığın gelişmesi ile zihinsel yoğunluk arttığı gibi kişinin yalnızlık gereksinimi de artmıştır. Bu anlamda yazarlar kişilerin özel hayatları ile ilgili bilgilerin yayınlanmasına karşı hukuki bir talep ya da bir hak olarak “yalnız bırakılma hakkı”nı ifade etmişlerdir⁷⁹. Gözetim potansiyeli yüksek bilişim sistemlerinin özel hayatın gizliliğinin korunması açısından barındırdığı potansiyel tehlikelere farkındalığın arttığı döneme kadar özel hayatın gizliliği, genel olarak bireyin toplum içerisinde konumu sınırlı erişim merkezinde ele alınmıştır. Bu dönem sonrasında ise özel hayatın gizliliğine ilişkin olarak, kişisel verileri de kapsayacak şekilde tanımlar yapılmıştır. Bu bağlamda *Westin* özel hayatın gizliliği hakkını, “*bireylerin, toplulukların ve kurumların kendileri hakkındaki bilgilerin ne zaman, nasıl ve hangi kapsamda başkaları ile ilişki içinde bulunacağına kendilerinin karar verme hakkı*” olarak tanımlamıştır⁸⁰. Özel hayatın gizliliği hakkına kişisel verilerin korunmasını temel alan bir tanım da *Rodotà* tarafından yapılmıştır. Yazara göre özel hayatın gizliliği hakkı, “*her türlü kamusal denetim ve sosyal damgalamaya karşı yaşam tercihlerimizin korunması*”dır⁸¹. Aynı doğrultuda Avrupa Konseyi Parlamenterler Meclisi'nin 1998 tarihli kararında Meclisin 1970 tarihli ve 428 sayılı kararında “*kişinin kendi hayatını en az müdahaleyle yaşaması hakkı*” olarak tanımlanmış olan özel hayatın gizliliği hakkına, yeni iletişim teknolojilerinin kişisel

“Mahremiyet” Osmanlıca bir sözcük olup “mahrem olan” anlamına gelmektedir. “Mahrem” ise “gizli” ve “herkese söylenmez, herkesçe bilinmez” anlamındadır. Bkz., Mustafa Nihat Özön, **Osmanlıca-Türkçe Sözlük**, İstanbul, İnkılap ve Aka Yay., 1979. Bu anlamda özel hayatın gizliliği ve mahremiyet kavramları eş anlamlı değildir. Özel hayatın gizliliği bireyin yalnızca mahrem alanlarını değil, açık alanlarını da korumakta ve bu anlamda da mahremiyet özel hayatın gizliliği kavramının sadece bir boyutunu kapsamaktadır. Bkz., Sultan Üzeltürk, **1982 Anayasası ve İnsan Hakları Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı**, İstanbul, Beta Yay., 2004, s.7.

⁷⁹ Samuel D. Warren ve Louis D. Brandeis, “*The Right to Privacy*”, **Harvard Law Review**, S. 5, 15.11.1890, s. 193-220. Bu makalenin Türkçe çevirisi için bkz., Samuel D. Warren, Louis D. Brandeis, “*Mahremiyet Hakkı*”, çev., Gülay Arslan, **Özel Yaşam, Medya ve Ceza Hukuku, Karşılaştırmalı Güncel Ceza Hukuku Serisi 7**, Ankara, 2007, s.19-42.

⁸⁰ Alan Westin, **Privacy and Freedom**, ABD, 1970, s.7'den aktaran Küzeci, a.g.e., s. 73.

⁸¹ Stefano Rodotà, “*Data Protection as Fundamental Right*”, **Reinventing Data Protection**, haz. Serge Gutwirth, Yves Poullet, Cécile de Terwangne, Sjaak Nouwt, 2009, s. 78'den aktaran Küzeci, a.g.e., s. 74.

verilerin saklanması ve kullanılmasını olanaklı kılması sonucu “*kişinin kendisi hakkındaki verileri kontrol hakkı*”nın eklenmesi gerektiği belirtilmiştir⁸².

Özel hayatın gizliliği hakkının mutlak bir tanımı olmaması ile birlikte AİHM de söz konusu hakkı oldukça geniş yorumlamıştır. Mahkemeye göre özel hayat kavramının tüketici biçimde tanımlamaya çalışmak ne olasıdır ne de gereklidir. Ayrıca Mahkeme, bireyin kendi özel hayatını istediği gibi yaşayabileceği bir “iç alanla” kısıtlamanın ve bu alanın dışında kalan dış dünyayı bu alandan tamamen hariç tutmanın aşırı sınırlayıcı bir yaklaşım olduğunu, özel hayata saygının başka insanlarla ilişki kurmak ve söz konusu ilişkileri geliştirmek hakkını da bir dereceye kadar içermesi gerektiğini vurgulamıştır⁸³. *Rotaru/Romanya* kararında da aynı görüşü vurgulamakla birlikte mesleki nitelikteki ilişki ve faaliyetlerin de özel hayat kapsamında değerlendirilmesi gerektiğini belirtmiştir⁸⁴. *P.G. ve J.H./Birleşik Krallık* kararında AİHS’in 8. maddesinin kişinin kendi kimliğini belirleme, kişisel gelişim ve diğer insanlarla ve dış dünyayla ilişki kurma ve geliştirme hakkını da koruduğunu belirten Mahkeme, bu nedenle, bir kişinin kamuyla paylaştığı, kamuya açık alanlarda geçen yaşantısının da özel hayat kapsamında değerlendirilebileceğini vurgulamıştır. Mahkemenin bu değerlendirmesine göre kamuya açık alanların ve kamusal mekanların düzenli olarak izlenmesi, görüntü kaydının yapılması gibi uygulamaların özel hayata müdahale oluşturmaktadır⁸⁵.

Yukarıdaki açıklamalarımıza paralel olarak özel hayatın gizliliği hakkının tanımlaması Anayasa Mahkemesi tarafından yapılmıştır. Mahkemenin 1987 tarihli kararına göre, “*özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Orada cereyan edenlerin yalnız kendisi veya kendisinin bilmesini istediği kimseler tarafından bilinmesini*

⁸² Parliamentary Assembly of the Council of Europe, **Right to Privacy**, Resolution No. 1165(1998), paras. 4-5.

⁸³ *Niemitz/Almanya*, b.n. 13710/88, k.t. 16.11.1992, para. 29.

⁸⁴ *Rotaru/Romanya*, b.n. 28341/954, k.t. 04.05.2000, para. 43.

⁸⁵ *P.G. ve J.H./Birleşik Krallık*, b.n. 44787/98, k.t. 25.07.2001, para. 56.

istemek hakkı, kişinin temel haklarından biridir”⁸⁶.

Bütün bu tanımlardan sonra diyebiliriz ki, özel hayata müdahale teşkil eden bir davranış kişisel verilerin korunmasına da müdahale niteliği taşıyabilmektedir. Kişinin rızası haricinde özel hayatının sır alanına girmek ve kişisel verilere ulaşmak ihlal teşkil edecektir. Kişinin esasen özel hayatının sır alanına girdiği kabul edilen dini tercihler, ırksal köken, cinsel yaşam gibi konulara ilişkin veriler hassas veri olarak kabul edilmekte ve özel olarak korunmaktadırlar. Kişinin özel hayat alanına müdahale hukuk devleti ilkesi çerçevesinde ve ancak ağırlıklı bir kamu yararının varlığı halinde söz konusu olabilir. Ayrıca birey, “genel hayat alanı” içerisinde de korumasız değildir. Bu alanın kişinin sosyal ve kamusal alanını kapsadığı, bu anlamda özel hayatın gizliliği hakkının tamamen ortadan kalkmasından ötürü kişisel verilerin korunmayacağı ileri sürülemez. Genel hayat alanında dahi kişisel verilerin korunmasına ilişkin ilkelere uyulması gerekmektedir. Kamusal alanda örneğin, kişinin rızası dışında ses veya video kaydının alınması kişisel verilerin elde edilmesini teşkil eder. Bu eylemler de kişisel verilerin korunması hakkının ihlali anlamına gelebilir⁸⁷.

Gördüğümüz gibi özel hayatın gizliliği hakkı, kişisel verilerin korunmasından çok daha geniş bir alanı kapsamaktadır. Ancak günümüzde kazandığı önem dolayısıyla kişisel verilerin korunması, özel hayatın gizliliği hakkına ilişkin temel ilkelere beslense de ayrı bir hak alanı olarak kabul görmeye başlamıştır⁸⁸. Nitekim özel hayatın gizliliği hakkı bireyin kendisine ilişkin kişisel verilere ulaşma hakkı, kişisel verilerin işlenmesine ilişkin temel ilkeler gibi konuya ilişkin bazı konularda sınırlı kalmaktadır. Temel haklar kataloğunda ayrı bir hak olarak tanınmasıyla kişisel

⁸⁶AYMK, E. 1986/24, K. 1987/8, t. 31.03.1987.

⁸⁷Şimşek, **a.g.e.**, s. 142.

⁸⁸*Küzeci* kişisel verilerin korunmasının özel hayatın gizliliği hakkı ile bağlantısının yanında konunun öneminden dolayı ayrı bir hak alanı olarak görülmeye başlamasını haberleşme özgürlüğü ile örneklendirmiştir. Haberleşme özgürlüğü de kişisel verilerin korunması gibi özel hayatın gizliliği hakkı kapsamındadır. Ayrıca tıpkı kişisel verilerin korunması hakkı gibi konunun özel önemi ve gereklilikleri dolayısıyla pek çok metinde ayrı olarak düzenlenmiştir. Düşünceyi açıklama özgürlüğü ve basın özgürlüğü de örnek olarak verilebilir. Konu ile ilgili ayrıntılı bilgi için bkz., *Küzeci*, **a.g.e.**, s. 74.

veriler, kişinin hangi yaşam alanına girdiğine ve gizliliğine bakılmaksızın korunabilecektir⁸⁹. Bununla birlikte kişisel verilerin korunmasına özgü temel ilkelerden kabul edilen kişinin kendisi ile ilgili verilerin işlenmesi sırasında bilgilendirilmesi hakkı, ilgilinin bilgilerine erişim hakkı, ilgilinin verilerini düzeltme hakkı, ilgilinin itiraz hakkı, ilgilinin otomatik kararların konusu olmama hakkı sağlanarak özel hayatın gizliliği hakkı ile ancak sınırlı düzeyde sağlanabilen kişinin kişisel verilerin işlenmesi sırasında aktif katılım imkanı ön plana çıkarılmıştır⁹⁰.

Kişisel verilerin korumasının ayrı bir hak alanı olarak düzenlenmesine uluslararası alanda en somut örnek Avrupa Birliği Temel Haklar Şartı'dır. Bu önemli metinde özel yaşamın gizliliği hakkı ile kişisel verilerin korunması farklı maddelerde düzenlenmiştir. Kişisel verilerin korunması, anayasal temelde de bağımsız bir hak olarak tanımlanmaya başlanmıştır⁹¹.

Kişisel verilerin korunması açısından Türk hukukunda anayasallaştırma süreci burada önem taşımaktadır. Türkiye Büyük Millet Meclisi tarafından 7 Mayıs 2010 tarihinde kabul edilen 5982 sayılı Türkiye Cumhuriyeti Anayasasının Çeşitli Maddelerinde Değişiklik Yapılması Hakkında Kanun, 12 Eylül 2010 yılında halkoylaması ile onaylanmıştır. İlgili kanunun 2. maddesi ile Anayasanın “Özel Hayatın Gizliliği” başlıklı 20. maddesine kişisel veriler ile ilgili hüküm eklenmiştir. Eklenen hükme göre; *“herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir”*.

⁸⁹ Konuya ilişkin bir örnek de Belçika'dan verilebilir. Buna göre Belçika'da kişisel veriler özel hayatın ötesinde bir anlam taşımakta ve özel hayata haksız bir müdahale olmasa bile koruma kuralları geçerli olmaktadır. Bkz., Akyürek, **a.g.e.**, s. 49.

⁹⁰ Ayrıntılı bilgi için bkz., Çalışmamızın İkinci Bölümü, “*Kişisel Verilerin Korunması Hakkına Özgür Kriterler*” başlığı.

⁹¹ Hollanda Anayasası m. 10/2,3; Portekiz Anayasası m. 35; İspanya Anayasası m. 18/4.

Değişiklik öncesinde kişisel verilerin korunmasını anayasalarında ayrı bir hak alanı olarak yer vermemiş çeşitli devletler gibi mevzuatımızda da bu korumanın normatif temeli yargı organlarınca geliştirilen içtihatlar ile belirlenmekteydi. Bu doğrultuda Türkiye'de de Anayasa Mahkemesi kişisel verilerin korunmasını özel hayatın gizliliği hakkı çerçevesinde değerlendirmiştir⁹². Ancak, yukarıda belirtmiş olduğumuz düzenleme ile kişisel verilerin korunması hakkı artık özel hayatın gizliliği hakkından ayrı anayasal bir temele kavuşturulmaktadır. Kuşkusuz ki bu durum korumanın sağlanabilmesi açısından önemli bir adımdır. Öte yandan hükümde öngörülen ve kişisel verilerin yasal usullere göre işlenebilmesine dair ayrıntıları içeren kanun halen tasarı olarak beklemektedir⁹³.

Diyebiliriz ki, kişisel verilerin korunması her durumda bireylerin özel hayatlarının korunması anlamına gelecektir. Kişisel verilerin korunması en genel şekliyle bireye kişiliğine dair her türlü veri üzerinde tasarrufta bulunma hakkı vermektedir. Özellikle teknolojik gelişmeler nedeniyle ortaya çıkabilecek tehlikeler karşısında kişisel verilerin kullanımı ve devri konusunda bireye belirleme yetkisi tanınarak kendi iradesi ile hayatını şekillendirme ve karar verme özgürlüğü de tanınmaktadır. Her iki hak alanının koruduğu temel değer açısından ortaklıkları mevcuttur⁹⁴. Yine de özel hayatın gizliliği hakkı bağlamında kişisel verilerin

⁹² AYMK, E: 1996/68, K. 1999/1, t. 06.06.1999; AYMK, E. 2006/167, K. 2008/86, t. 20.03.2008. Bu kararlara aşağıda tekrar değinilecektir.

⁹³ Kişisel Verilerin Korunması Kanun Tasarısı ile ilgili ilk çalışmalar 1989 yılında başlamış ve 2000'li yıllara kadar çeşitli tasarılar hazırlanmış ancak çalışmalar sonuçlandırılmamıştır. 2000 yılında kurulan komisyonun da tasarı çalışmalarını tamamlayamaması üzerine 30.03.2004 tarihli Bakan Oluru ile Prof. Dr. Bahri Öztürk başkanlığında yeni bir Komisyon oluşturularak Tasarı hazırlık çalışmalarına devam edilmiştir. Bu Komisyon tarafından hazırlanan Tasarı, kamu kurumları, üniversiteler ve sivil toplum örgütleri de dahil olmak üzere toplam 53 kuruluşa görüşe gönderilmiş, Başbakanlık aşamasında da tekrar görüş alınmıştır. Tasarı, 28.07.2006 tarihinde Başbakanlığa gönderilmiştir. Tasarı, Başbakanlık tarafından 22.4.2008 tarihinde Türkiye Büyük Millet Meclisi'ne sevk edilmiştir. Tasarı, 02.05.2008 tarihinde esas komisyon olarak Adalet Komisyonuna gönderilmiştir. Tasarı, 07.05.2008 tarihinde Meclis Adalet Komisyonu tarafından Alt Komisyona havale edilmiştir. Alt Komisyon Tasarı ile ilgili birkaç toplantı yaptıktan sonra yoğun gündem nedeniyle çalışmalarına ara vermiş ve Adalet Alt Komisyonunda bulunan Tasarı, araya TBMM Seçimlerinin girmesi nedeniyle yasalaşamayınca İktüzüğünün 77. maddesi gereğince hükümsüz sayılmıştır. Bunun üzerine, Adalet Bakanlığınca 15.09.2011 tarihinde Başbakanlığa yazılan yazıyla Tasarının yenilenmesinin uygun olacağı bildirilmiştir. Tasarı halen Başbakanlıkta bulunmaktadır. Bu çalışmanın yazımı aşamasında Tasarı'nın Başbakanlıkta bulunan hali için bkz., (Çevrimiçi) <http://www.kgm.adalet.gov.tr/Tasariasamaları/Basbakanlik/Kanuntas/kisiselveriler.pdf>, 01.05.2013.

⁹⁴ Küzeci, a.g.e., s. 76.

korunması sınırlı kalmasından ötürü özünü özel hayatın gizliliği hakkının korunmasında bulsa da bağımsız bir hak olarak yeni bir temel değer oluşturmaya başlamıştır.

IV. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL DÜZENLEMELER

A. Tarihsel Gelişim

Tarih sürecinde insanın birey olarak kabulü ile özgün kişiliğinin sağlanmasına yönelik korumalara dair birçok düşünce ortaya çıkmıştır. En yaygın örnek olarak belirli meslek gruplarının sır saklama yükümlülüğü verilebilir. Örnek vermek gerekirse, M.Ö. 5. yüzyılda gelişen Hipokrat Yemini ile belirli meslek gurupları ve bireyler arasında güven ilişkisi sağlanmaya çalışılmıştır. Tabii ki sır saklama yükümlülüğü kişisel verilerin korunmasının günümüzde anlaşıldığı halini tam olarak sağlamasa da güven ilişkisi çerçevesinde bireyin hastalığının bilinmesi ile sosyal çevrede göreceği zarar önlenmeye çalışılarak bireyin kişiliğinin korunmasına örnek teşkil eder⁹⁵.

Kişisel verilerin korunması yeni ve bir o kadar da gelişmelere açık, dinamik bir alandır. Teknolojide atılan her bir adım ile kişisel verilerin korunmasına yönelik yeni düşünceler ortaya atılmakta, konuya ilişkin düzenlemelerde değişiklikler meydana gelmektedir. Teknolojinin ivme kazanmasından ve bilgisayar kullanımının yaygınlaşmasından önce kişisel veriler otomatik olmayan yollar ile işlenmekteydi. Bu dönemde kişisel verilerin işlenmesi ve gözetim yüksek iş gücü ve büyük meblağlarda yatırım demektir. Bunlar da kişisel verilerin işlenmesi sonucu özel hayatın ihlalinin bir nevi doğal sınırlarını oluşturmaktaydı. Otomatik veri işleme teknolojilerinin gelişmesi ile birlikte bugün anladığımız haliyle kişisel verilerin korunmasına yönelik hukuksal düzenlemeler tartışılmaya başlanmıştır.

⁹⁵ Şimşek, a.g.e., s.6.

1960'lı yıllar bilgisayarın ve merkezi veri tabanlarının gelişmesine sahne olmuştur. Bu yıllardan başlayarak sunduğu birçok olanaklar ve kolaylıklar ile bilgisayarların kullanımı yaygınlaşmaya başlamıştır. Zamanına göre bir hayli pahalı olan bilgisayar teknolojisi devlet organları ve çeşitli büyük işletmeler eliyle kullanılmaktaydı. Bürokrasi, yeni teknolojilerin sağladığı olanaklar ile öncesine nazaran hız kazanmaktaydı. Devlet organları, elde ettiği bilgileri yeni teknoloji yöntemleri kullanarak birbirleri ile ilişkilendirmekte ve bu bilgileri merkezi bir veri tabanında birleştirmeye dair hazırlıklar yapmaktaydılar. Bu durum, bireyin devlet karşısında daha da güçsüz duruma düşeceği endişesini haklı olarak destekledi. Bu anlamda devlet, iktidarın birey karşısında bilginin sağladığı güç ile üstünlük sağladı. Bilgisayarın ve veri tabanlarının kişisel bilgilerin kaydı amacıyla ilk olarak yalnızca devlet organlarında kullanılması, ilk tepkilerin de devletlere yönelmesine sebep olmuştur. Devletin bireylerin karşısında aşırı güçlenmesinin önüne geçilmesi, yeni teknolojilerin getirdiği olanakların denetlenebilmesi için yapılan hukuksal düzenlemeler kişisel verilerin korunmasına yönelik ilk düzenlemelerin genel endişesini oluşturmaktadır⁹⁶.

Verilerin korunmasına dair hukuksal düzenlemelere gidilmesindeki ilk aşama 1970'li yıllardır. Konuya dair ilk hukuki düzenleme 1970 yılında Almanya'nın Hessen eyaletinde çıkarılmıştır. "Hessen Planı" kapsamında federe düzeyde merkezi bir veri bankasının kurulma tasarısı bu hukuki düzenlemenin dinamliğini teşkil eder. Hessen eyaletinde yapılan düzenlemeler kişisel verilerin korunmasına ilişkin bir başka düzenlemeyi tetiklemiştir. Böylece federe düzeydeki hukuki düzenleme, Almanya'da federal düzeyde bir korumanın öngörülmesinde etkili olmuştur ve 1977 yılında Federal Almanya Veri Koruma Yasası kabul edilmiştir.

Kişisel verilerin korunmasına dair ilk ulusal düzenleme 1973 yılında İsveç'te yapılmıştır. Daha sonra 1974 yılında Amerika Birleşik Devletleri'nde özel alanın korunmasına ilişkin kanun (Privacy Act) kabul edilmiştir. Bunları 1977 tarihli

⁹⁶ Andreas Jori, "dataprotection.eu", (Çevrimiçi) <http://www.dataprotection.eu>. 01.05.2013.

Kanada İnsan Haklar Kanunu, 1978 tarihli Elektronik Veri İşlenmesi, Veriler ve Özgürlük Haklarına İlişkin Fransız Kanunu izlemiştir.

Kişisel verilerin korunmasına ilişkin ilk hukuki düzenlemelerin görüldüğü döneme ait olarak genel değerlendirme yapmak gerekirse bu dönemdeki sakıncaların yeni bilgisayar teknolojilerinin getirdiği olanakların etkilerine yönelik oldukları söylenebilir. Bu dönemde kabul edilen hukuki düzenlemelerin temel noktası kişisel verilerin korunmasına yönelik olmaktan öte daha çok devletlerdeki enformasyonel gücün artmasına karşı bir denge sağlamaya yöneliktir. Devletin elindeki merkezi ve geniş kapsamlı veri bankalarının şeffaflaştırılmasına dair tutumlar yoğunlaşmıştır. Günümüze nazaran daha az sayıda olan veri tabanlarının kayıt altına alınması kabul edilmiştir. Yine, günümüzde kişisel verilerin korunmasına özgü temel ilkelerden sayılan kişisel verilere ulaşma ve onları düzeltme hakkına yönelik düzenlemeler bu dönemde kabul edilmiştir.

Bilişim teknolojilerindeki yeni gelişmeler, kişisel verilerin korunmasına ilişkin ilk hukuki düzenlemelerin kısa sürede yetersiz kalmasına yol açmıştır. Aynı gelişmeler sürecinde bilgisayarların kullanımı yalnızca kamu merkezli olmaktan çıkarak özel sektöre de kaymıştır. İlk zamanlarda kişisel verilerin işlenmesi sonucu ortaya çıkabilecek tehlikeler kamu ve tek merkezli olarak yorumlanırken artık durum dağınık ve çok merkezli bir hal almıştır⁹⁷. İşte, tehlikenin boyutunun ve anlamının değişmesi ile birlikte kişisel verilerin korunmasına ilişkin hukuki düzenlemeler için yeni bir döneme girilmiştir. Artık konu, insan hakları boyutuna taşınmıştır. Bununla birlikte, teknik alandaki hızlı gelişmelere karşı bunları düzenleyici hukuki düzenlemelerin yetersiz kalması sonucu yasakoyucular teknoloji temelli hukuki düzenlemeler yerine bireyi temel alıp onu kişisel verilerin işlenmesi sürecine dahil ederek en azından teoride de olsa korumayı sağlamaya çalışmışlardır⁹⁸. Yine bu döneme ait bir başka kayda değer yaklaşım ise özellikle Kıta Avrupası'nda kişisel

⁹⁷ Küzeci, **a.g.e.**, s. 111.

⁹⁸ Jori, “dataprotection.eu”.

verilerin korunmasını anayasallaştırma eğilimlerinin yaygınlaşmasıdır⁹⁹.

Kişisel verilerin korunmasına ilişkin ikinci dönem, konunun insan hakları kapsamında değerlendirilmesi ve “*self-determinasyon*”un (bilgilerin geleceğini belirleme hakkı) kabulü ile nitelendirilebilir. 1983 yılında Alman Anayasası Mahkemesi'nin “Nüfus Sayım Kararı” bu bakımdan önemlidir. Bu karar, kişisel verilerin korunmasına ilişkin tartışmalarda yol gösterici niteliktedir. Kararda kişisel verilerin korunması kişilik hakkı kapsamında yorumlanmıştır. Buna göre;

“Eğer bir kimse kendisi hakkında belirli alanlarda hangi enformasyonun toplumsal çevresinde bilindiğini yeterli kesinlikle öngöremiyorsa ve iletilme ihtimali olan tarafları yeterince tahmin edemiyorsa, herhangi bir baskı ya da etki altında kalmadan hür bir şekilde planlama ya da karar verme hürriyetinden alıkonulmuş demektir. Enformasyona ilişkin self-determinasyon hakkı, vatandaşların bundan sonra kendileri hakkında kimlerin ne zaman ve hangi nedenle ne bildiklerini bilemeyecekleri bir duruma olanak veren toplumsal ve yasal düzeni engeller. Eğer bir kişinin, ayrıksı davranışlarının sistemli bir şekilde enformasyon olarak saklanıyor, bu husus uygulanıyor ya da intikal ettiriliyor yönünde şüphesi varsa, o kişi bu tür bir davranışla ilgiyi üzerine çekmemeye gayret edecektir. Sivil girişime ya a toplantıya katılımın kaydedildiği ve bu yüzden kişisel bir risk oluşabileceği gözüyle bakıyorsa, muhtemel olarak bu haklarının kullanımından vazgeçecektir. Bu durum sadece kendi gelişmesine zarar vermeyecek aynı zamanda toplumun menfaatlerine de zarar verecektir. Çünkü self-determinasyon vatandaşlarının hareket ve katılımına dayalı olan özgür demokratik toplumun temel işlevsel koşuludur”¹⁰⁰.

⁹⁹ Portekiz Anayasası'nın 35. maddesinde kişisel verilerin korunması hakkı düzenlenmiştir. İspanya Anayasası'nın 18. maddesinin 4. fıkrası ise kişisel verilerin işlenmesini yasa ile sınırlandırılması gerektiği hükmünü içermektedir. Avusturya, Macaristan ve İsveç gibi ülkelerde de benzer düzenlemeler yapılmıştır. Bkz., Küzeci, a.g.e., s. 111.

¹⁰⁰James Micheal, **Privacy and Human Rights: an International and Comparative Study with Special Reference to Development in Information Technology**, UNESCO, 1994'ten aktaran

İkinci dönem içerisindeki düzenlemelere bakıldığında verilerin korunması daha önceki düzenlemelerdeki gibi yalnızca teknolojinin olumsuz sonuçlarına karşı korunmak olarak algılanmamış, en iyi yolun bireyin bu konuda mücadele etmesi olduğu ifade edilmiştir¹⁰¹.

Kişisel verilerin korunmasının gelişimi yukarıda açıkladığımız gibi olmak ile birlikte, zaman içerisinde bireyler için yeterli güvenceler tanınmadan verilen hakların etkin bir şekilde korunmadığı görülmüştür¹⁰². Almanya Anayasa Mahkemesinin verdiği “bilgilerin geleceğini belirleme hakkı” kararı Almanya dışında diğer ülkelerdeki hukuki düzenlemeleri etkilemiş olsa da uygulamada beklenen etkiyi gösterememiştir. Kimi yazarlara göre söz konusu hakkın kabulü ile birey, ekonomik olarak üstün konumda olan ve verilerin kullanılmasına ilişkin pazarlıkta denge lehine olan kişisel verileri işleyenler karşısında güçsüz durumdadır. Bireyler, kişisel verileri işleyenler ile yaptıkları sözleşmeler ile haklarından vazgeçebilmektedirler. Bilgilerin geleceğini belirleme hakkı bu haliyle yalnızca ekonomik ve sosyal olarak haklarını kullanabilen azınlığa terk edilmektedir¹⁰³.

Bilgi, toplumumuz açısından hem hammadde hem de üründür. Özellikle küreselleşme olgusu ile verinin küresel boyutlardaki trafiği artık inkar edilemez bir boyuta ulaşmıştır. Peki, ekonomik ve sosyal açıdan önemi gün geçtikçe artan bilgi/veri trafiğine engel olmadan kişisel verilerin uluslararası düzeyde korunması nasıl sağlanmalıdır? Günümüzde bu alanda düzenlenen birçok belgeye, ülkeler arasında akdedilen antlaşmalara rağmen tam bir etkin sonuç getirilememiştir. Kişisel

Ketizmen, **a.g.e.**, s. 199.

¹⁰¹ Şimşek, **a.g.e.**, s. 9. Ayrıca, bu döneme ait hukuki düzenlemeler daha önceki düzenlemelere nazaran teknik terimlerden arındırılmıştır. Böylece vatandaşlar için daha anlaşılabilir bir dil sağlanmıştır. Bkz., Jori, “dataprotection.eu”. Düzenlemelere dair getirilen bu değişikliklerin, veri işleme faaliyetleri karşısında bireyin katılımının sağlanması ve kendi haklarını talep edebilmesi için getirildiği söylenebilir.

¹⁰² Küzeci, **a.g.e.**, s. 115.

¹⁰³ *Mayer-Schönberger*, veri işleme sektörünün etkisi ile ortaya çıkan bu durumu anlatmak için veri koruma kurallarını dışsız kağıttan kaplanlara benzetmiştir. Viktor Mayer-Shönberger, **Generational Development of Data Protection in Europe, Technology and Privacy: The New Landscape**, haz. Philip E. Agre, Marc Rotenberg, MIT Press, ABD 1998'den aktaran Jori, “dataprotection.eu”.

verilerin korunmasında etkin sonuçların elde edilmesi gerekliliği çözüm arayışı ve yaklaşımların çeşitlenmesine neden olmaktadır.

Kişisel verilerin korunmasının tarihsel gelişiminin genel tablosu yukarıda açıkladığımız gibidir. Bununla birlikte özellikle veri aktarımının sınır ötesi bir anlam kazandığını belirtmemiz gerekir. Bu durum konunun küresel düzeyde tartışılmasını zorunlu kılmıştır. Kişisel verilerin korunmasına dair temel uluslararası kaynaklar aşağıda ayrıntılı olarak değerlendirilecektir.

B. Uluslararası Belgelerde Kişisel Verilerin Korunmasına İlişkin Temel Kaynaklar

Teknoloji dünyasındaki hızlı gelişmeler ile kişisel verilerin toplanması ve işlenmesi olanakları olabildiğince artmıştır. Ulusal düzeydeki veri aktarımları da aynı şekilde dünya çapında birbirleri ile bağlanan internet ve bilgisayar ağ sistemleri ile uluslararası bir boyut kazanmıştır. Ulusal sınırların ötesine geçen veri aktarımı ile kişisel verilerin korunması yalnızca ulusal hukuk ile çözülemeyecek bir boyuta ulaşmıştır. Bu alanda birçok devlet ve uluslararası kuruluş, konuya dair daha etkin politikalar belirlemek ve düzenlemeler yapmak amacıyla teşvik edici çalışmalar yapmışlardır. Teknolojik gelişmeler ile kişisel verilerin toplanması ve işlenmesi maliyetleri düşmüş, verilerin sınır ötesi trafiği yoğunlaşmıştır. Aynı doğrultuda uluslararası veri bankalarının kapasitesi ve kullanımı da artmıştır. Veri bankalarında tutulan kişisel veriler konusu verinin uluslararası alanda korunması, toplanması, işlenmesi ve yayılmasına ilişkin düzenlemelerin uygulanmasında işbirliğini ve devletlerin ortak hukuki zeminde buluşmasını gerektirmiştir. Konunun uluslararası yankılarını ve uluslararası rejimi açıklayabilmek için konuya ilişkin temel uluslararası belgeler yardımcı olacaktır. Burada belirtmek isteriz ki kişisel verilerin korunması ilk olarak özel hayatın gizliliği hakkı kapsamında açıklanmaya çalışılmıştır. Bu hak, pek çok önemli insan hakları metninde güvence altına alınmıştır. Bu kapsamda Birleşmiş Milletler Evrensel İnsan Hakları Bildirisi, Birleşmiş

Milletler Uluslararası Bireysel ve Siyasal Haklar Sözleşmesi, Avrupa İnsan Hakları Sözleşmesi örnek olarak verilebilir. Bu metinlerde güvence altına alınan özel hayatın gizliliği hakkı ile kişisel verilerin korunması arasında yakın ilişki bulunmaktadır. Bununla birlikte kişisel verilere ilişkin ulusal düzeyde yapılan düzenlemelerin yanında sınır ötesi veri aktarımının sağlanmasına dair sorunların yaşanmaması için uluslararası düzeyde doğrudan düzenlemelerin de gerekliliği ortaya çıkmıştır. Çağdaş ve demokratik bir toplumda insan haklarına verilen önem de kişisel verilerin uluslararası düzenlemeler ile korunması gerekliliğini perçinlemiştir¹⁰⁴. Bu amaçlar doğrultusunda uluslararası düzeyde aşağıda ayrıntılarıyla açıklayacağımız doğrudan kişisel verilerin korunmasına dair metinler kabul edilmiştir.

1. OECD ve Kişisel Verilerin Korunması

Kişisel verilerin korunmasına dair uluslararası alanda ilk adım Ekonomik İşbirliği ve Kalkınma Örgütü (bundan sonra OECD olarak anılacaktır) tarafından atılmıştır. 1961 yılında kurulan OECD, batılı sanayileşmiş ülkelerin yanı sıra ABD, Kanada, Japonya, Yeni Zelanda, Meksika gibi Avrupa kıtası dışındaki devletlerin de dahil olduğu bir kuruluştur¹⁰⁵. OECD'nin temel hedefleri arasında küreselleşmenin ekonomik, sosyal ve yönetim sorunlarını çözmek ve böylece demokrasiye ve pazar ekonomisine bağlı devletleri bir araya getirmek, ekonomik büyümeyi desteklemek, iş alanlarını arttırmak, yaşam standartlarını yükseltmek, finansal dengeyi korumak, başka devletlerin ekonomik gelişimine yardımcı olmak bulunmaktadır¹⁰⁶.

Örgüt, verilerin korunmasına ilişkin olarak 23 Eylül 1980 tarihinde “Kişisel Verilerin Sınırışan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeler”i kabul

¹⁰⁴ Aksoy, **a.g.e.**, s. 4.

¹⁰⁵ OECD, 14 Aralık 1960 tarihinde imzalanan Konvansiyonun yürürlüğe giriş tarihi olan 30 Eylül 1961'de kurulmuştur. İkinci Dünya Savaşı sonrası Avrupa'nın Marshall Planı çerçevesinde yeniden yapılandırılması amacıyla kurulan Avrupa Ekonomik İşbirliği Örgütü'nün (OECE) ardıdır. Türkiye'nin de içinde bulunduğu 20 kurucu üye ile kurulmuş olan Örgütün halihazırda 34 üyesi bulunmaktadır.

¹⁰⁶ OECD temel hedefleri için bkz., Convention on the Organisation for Economic Co-operation and Development, m. 1. Konvansiyon'un tam metni için bkz., <http://www.oecd.org/general/conventionontheorganisationforeconomiccooperationanddevelopment.htm>.

etmiştir¹⁰⁷. Örgüt bünyesinde konunun ele alınışına baktığımızda ise ilk girişim, 1969 yılında Veri Bankası Paneli'nde bir grup uzmanın rehber ilkeler üzerinde çalışmaları ile başlamıştır. Daha sonra 1978 yılında Sınırışan Veri Transferleri ve Mahremiyetin Korunması konulu sempozyumda, şu anki OECD Rehber İlkeleri'ne dair ilk adımlar atılmıştır¹⁰⁸. OECD, esasen serbest piyasa ekonomilerinin gelişimini amaçlayan ve çalışmalarını bu çerçevede gerçekleştiren bir ticaret örgütüdür. Kişisel verilerin korunmasına ilişkin ilk uluslararası düzenlemeyi kabul etmiş olması, aynı zamanda konunun ekonomik önemini de vurgulamaktadır¹⁰⁹.

OECD'nin kişisel verilerin korunmasına ilişkin rehber ilkeleri tavsiye niteliğindedirler. Üye devletler bu ilkeleri iç hukuklarının bir parçası haline getirip getirmemekte serbesttirler¹¹⁰. İlkelerin amacı ulusal düzeydeki veri koruma düzenlemelerinin birbiri ile uyumlaştırılmasıdır. Bu anlamda rehber ilkeler, konu ile ilgili düzenlemeye sahip olmayan devletler açısından temel teşkil edecek; ilgili düzenlemeye sahip ülkeler ise asgari gerekliliklerin çerçevesinde daha kapsamlı düzenlemeler yapabileceklerdir¹¹¹. Tavsiye niteliğindeki bu ilkeler özel hayatın gizliliğinin korunmasına yönelik haklar ile gereksinimleri uyumlaştırmak için Avrupa Konseyince yürütülen çalışmalar ile paraleldirler. Bu anlamda ilkelerin kabul

¹⁰⁷ OECD Rehber İlkeleri'nin orijinal metni için bkz., <http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>

¹⁰⁸ OECD Rehber İlkeleri, m. 16.

¹⁰⁹ Metnin önsözünde de konunun ekonomik boyutuna değinilmiştir. Buna göre, ulusal veri koruma yasaları arasındaki farklılıkların sınır ötesi veri akışını engelleyeceği ve bunun sonucunda da başta bankacılık ve sigortacılık olmak üzere, ekonominin önemli alanlarının zarar görebileceğine yer verilmiştir. Bkz., Jori, "dataprotection.eu". Örgütün kuruluş amacının üyelerinin ekonomik gelişmelerini desteklemek oluşu kişisel verilerin korunması hususunu insan hakları kapsamında değerlendirme eğilimi yerine ulusal ve uluslararası düzeyde ticaretin konusu olan önemli bir meta olarak değerlendirilmesi sonucunu doğurmuştur. Verilerin korunması yoluyla özel hayatın gizliliğinin korunması, OECD için ikinci konumda olmuştur. Bkz., İkbâl Gür, **Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Ankara, Turhan Kitabevi, 2010, s. 155.

¹¹⁰ Diyebiliriz ki, OECD'nin tavsiye niteliğindeki kararları, ortak anlayıştan kaynaklanan grup baskısı ile üye devletlerin çeşitli konulardaki reform süreçlerinde etkili olmaktadır. OECD'nin üye devletler hakkında periyodik olarak hazırladığı raporlara *peer review* adı verilmektedir. Bu kavram, İngiliz demokrasisinin gelişim sürecinde Lordlar Kamarasının bazı önlemler için uyguladığı *peer pressure* (ortak baskı) kavramından esinlenilmiştir. Bkz., http://www.mfa.gov.tr/iktisadi-isbirligi_ve-gelisme-teskilati-oecd_tr.mfa.

¹¹¹ OECD Rehber İlkeleri, m. 6, m. 49. Ayrıca bkz., Clarke, "Beyond OECD Guidelines: Privacy Protection for the 21st Century".

edilmesinin bir diğer amacının, Avrupa Konseyinin kabul edeceği sözleşmenin yürürlüğe girmesine kadar geçici bir davranış standardının belirlenmesi olduğu söylenebilir¹¹².

Kişisel verilerin korunmasına ilişkin tavsiye niteliğinde öngörülen OECD Rehber İlkeleri'nde esas olarak sekiz ilkeye yer verilmiştir. Üye devletlerin yapacakları düzenlemelerinde yer alması istenen temel ilkeler şunlardır¹¹³;

- Veri toplamanın sınırlı olması ilkesi (m.7): Kişisel verilerin toplanmasına belirli sınırlar getirilmelidir. Buna göre, kişisel verilerin toplanması ancak hukuka uygun sebepler ve araçlarla toplanırken, gereken hallerde veri sahibinin rızası ve bilgisi dahilinde gerçekleşmelidir.

- Verilerin belirli bir niteliği karşılaması ilkesi (m. 8): Kişisel verileri, kullanılacakları amaç ile uygun olmalı ve bu amacın gerçekleştirilmesi ölçüsünde tam ve güncel olmalıdır.

- Amacın belirliliği ilkesi (m. 9): Kişisel verilerin toplandığı amaç en geç verilerin toplanma anında belirlenmiş olmalıdır. Verilerin toplanma amacı gerçekleştikten sonra verileri başka amaçlar için kullanma, bu amaçların asıl toplama amacıyla bağdaşmaz olmaması ve amacın her değişiminin bildirilmesi koşullarıyla sınırlıdır.

¹¹² Gür, **a.g.e.**, s. 158. Bing ise OECD Rehber İlkeleri ve Avrupa Konseyi'nin konuya ilişkin doğrudan düzenleme getirdiği "108 sayılı Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme"yi karşılaştırırken bu iki uluslararası organizasyonun kuruluş amacındaki farklılığa değinmiştir. Yazara göre, kişisel verilerin korunmasına dair insan hakkı yaklaşımı sergileyen 108 sayılı Sözleşme ile uluslararası ticarete işbirliğini sağlamaya yönelik olan OECD Rehber İlkeleri, oluşturuldukları uluslararası organizasyonların hedeflerindeki farklılık bir yana, benzer hükümleri içermektedir. Bkz., Jon Bing, "*The Council of Europe Convention and the OECD Guidelines on Data Protection*", **Michigan Yearbook of International Legal Studies**, S.5, 1984, s. 272.

¹¹³ Çalışmamızın ilgili bölümünde kişisel verilerin korunmasına özgü kriterler ayrıca incelenecektir. Bununla birlikte kabul edildiği şekliyle kriterlerin temelini OECD Rehber İlkeleri'nin oluşturduğunu söylemek yanlış olmaz.

- Kullanımının sınırlı olması ilkesi (m.10): Toplanan veriler, toplandıkları amaçlar dışında ifşa edilemez, bulundurulamaz veya başka amaçlarla kullanılamaz. Veri sahibinin rızası ve kanuna dayalı yetki bu ilkenin istisnalarını teşkil eder.

- Veri güvenliği ilkesi (m. 11): Toplanan veriler için kayıp, yetkisiz erişim, zarar verme, değiştirme, kullanma ve açıklama gibi potansiyel tehlikelere karşı makul güvenlik önlemleri alınmalıdır.

- Açıklık ilkesi (m. 12): Kişisel verilere ilişkin olarak işlemler ve önlemler genel olarak açıklık politikası çerçevesinde gerçekleşmelidir. Kişilere kendileriyle ilgili veri barındıran kurum ve kuruluşlara kolaylıkla erişebilme hakkı sağlanmalıdır.

- Bireyin katılımı ilkesi (m. 13): Veri sahibinin rızası olmaksızın veriler erişilebilir hale getirilmemeli ve açıklanmamalıdır. Ayrıca bireyin, veri sorumlusunun kendisi ile ilgili veriye sahip olup olmadığı hakkında bilgi alma hakkı vardır. Bununla birlikte bireyin, kendisiyle ilgili veri hakkında veri sorumlusu ile makul süre içinde, gerekli ise makul bir ücret ile makul bir usul ve türde ve kolayca anlaşabilecek bir şekilde bilgi alma hakkı vardır. İlgili haklar çerçevesinde yapılan bir başvuru reddedildiği takdirde bireyin buna itiraz etme hakkı; itiraz kabul edildiği takdirde bireyin verinin silinmesi, değiştirilmesi veya düzeltilmesini isteme hakkı garanti altına alınmalıdır.

- Hesap verilebilirlik ilkesi (m. 14): Veri sahiplerinin yukarıdaki ilkeler çerçevesinde veri sorumlularına hesap sorabilmeleri mümkün olmalıdır.

OECD Rehber İlkeleri üye ülkelerin bu ilkeleri iç hukuklarına adapte etmeleri noktasında bunların yorumlanmasına ilişkin yol gösterici belgelere çok az yer verildiği, yeterli açık ifadelerden uzak olduğu hakkında eleştirilmiştir¹¹⁴. Eleştirilen yönlerine karşın bu ilkeler, birçok açıdan önemlidir. Öncelikle ilkeler, kişisel

¹¹⁴ Hayrunnisa Özdemir, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Ankara, 2009, Seçkin Yay., s. 19.

verilerin korunmasına dair uluslararası düzeyde yapılan ilk girişim olma özelliği taşır. İlkelerin belirlenmesinde dünyanın çeşitli bölgelerinden üye devletlerin katkısı bulunduğundan bu rehber ilkeler, üye devletlerin ortak anlayışını yansıtmaktadır. Ayrıca ABD, 108 sayılı Sözleşme ve AB Direktifi'nin aksine OECD üye devletlerindendir. Bu anlamda OECD Rehber İlkeleri kişisel verilerin korunmasına ilişkin farklı rejimlerin hakim olduğu ABD ve AB arasındaki ortak payda olarak değerlendirilebilir¹¹⁵. OECD Rehber İlkeleri Avustralya, Kanada ve Yeni Zelanda gibi Kıta Avrupası dışındaki ülkelerdeki kişisel verilerin korunmasına ilişkin düzenlemeleri önemli oranda etkilemiştir. Yine Asya Pasifik Birliği'nin üye devletler için çerçeve ortak veri koruması ilkelerinin belirlenmesinde OECD Rehber İlkeleri etkili olmuştur¹¹⁶. Diyebiliriz ki, bağlayıcı olmayan bu ilkelerin etkisi halen daha ulusal ve uluslararası düzeyde sürmektedir¹¹⁷.

2. Birleşmiş Milletler Örgütü ve Kişisel Verilerin Korunması

Birleşmiş Milletler, adalet ve güvenliği, ekonomik kalkınma ve sosyal eşitliği uluslararasıda tüm ülkelere sağlamak amacı ile 24 Ekim 1945 tarihinde kurulmuştur¹¹⁸. BM'nin ilke ve amaçlarını belirleyen BM Şartı ile üye devletler bu şarttan doğan yükümlülükleri kabul ederler. Bu metinden doğan yükümlülüklerden biri de insan hakları ve temel özgürlüklere saygı gösterilmesi, bunların geliştirilmesi ve desteklenmesidir¹¹⁹. Nitekim, kişisel verilerin korunması hakkı, temel hak ve

¹¹⁵ Jori, “dataprotection. eu”.

¹¹⁶ Lee A. Bygrave, “*Privacy and Data Protection in an International Perspective*”, *Scandinavian Studies in Law*, 2010, S.56, s. 184. (Bu kitap bundan böyle “**Privacy and Data Protection in an International Perspective**” olarak gösterilecektir). Ayrıca Bygrave'e göre Asya Pasifik Birliği'nin belirleyeceği ilkeler OECD Rehber İlkeleri'ne nazaran daha esnek bir koruma sağlamaya yöneliktir. Bunun nedeni de temel hakları korumaktan ziyade daha çok tüketici güveninin sağlanmasının amaçlandığı söylenebilir. Bkz., Bygrave, “**Privacy and Data Protection in an International Perspective**”, s. 188.

¹¹⁷ OECD bünyesinde konuya ilişkin yürütülen çalışmalar dahilinde 1998 yılında Ottawa'da yapılan Bakanlar Konferansı'nda kabul edilen bildiriye göre OECD Rehber İlkeleri'nin her tür ortamdaki kişisel verilerin toplanması ve tutulması konusunda uluslararası uzlaşmayı temsil etmesi ve referans olarak kabulüne devam edilmesi kararlaştırılmıştır. Bkz., Working Party on Information Security and Privacy, **Ministerial Declaration on the Protection of Privacy of Global Networks**, Ottawa, 1998.

¹¹⁸ 51 devlet ile kurulan örgütün günümüzde 192 üyesi bulunmaktadır. Türkiye, BM'nin kurucu üyelerindendir. Ayrıntılı bilgi için bkz., www.un.org/eng/aboutun/index.shtml.

¹¹⁹ BM Şartı, m. 1/f.3.

özgürlüklere saygı gösterilmesi amacıyla örgüt bünyesinde kabul edilen genel nitelikli insan hakları metinlerinde özel hayatın gizliliği hakkı kapsamında görülmektedir. Ayrıca Örgüt bünyesinde konu ile ilgili doğrudan düzenlemelere de yer verilmiştir.

10 Aralık 1948 yılında kabul edilen BM Evrensel İnsan Hakları Bildirisi'nin 12. maddesinde özel hayatın gizliliği hakkına yer verilmiştir¹²⁰. İlgili maddeye göre; *“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”*.

BM Medeni ve Siyasal Haklara İlişkin Sözleşme'nin 17. maddesinde de özel hayatın korunmasına ilişkin hükme yer verilmiştir. İlgili maddeye göre;

“(1)Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz. (2)Herkesin, bu gibi müdahalelere ya da tecavüzlere karşı yasalarca korunma hakkı vardır”.

Kişisel verilerin korunması hakkının ilgili madde kapsamında görüldüğü BM İnsan Hakları Komitesi tarafından açıkça kabul edilmiştir. Buna göre Komite, 16. Genel Yorumu ile kişisel verilerin kamu otoriteleri ve özel kişi ve kurumlar tarafından toplanıp işlendiğini ve bunların da belirli bir hukuki düzenlemeye tabi olması gerektiğini belirtmiştir. Ayrıca devletlerin, kişisel verilerin yetkisiz kişilerin eline geçmesi ve Sözleşme'nin amacına aykırı olarak kullanılmasını engelleyici tedbirler alması gerektiği vurgulanmıştır. Komiteye göre, özel hayatın gizliliğinin etkin bir şekilde güvence altına alınabilmesi için bireylerin kendileri hakkında veri tabanlarında saklanan bilgilerin içeriklerini ve saklanma amaçlarını öğrenebilmesi gerekmektedir. Bireyler yanlış, hukuka aykırı toplanan veya hukuka aykırı kullanılan

¹²⁰ İlk aşamada kişisel verilerin korunması hakkının, özel hayatın gizliliği hakkı kapsamında değerlendirildiğinden yola çıkarak metin, kişisel verilerin saldırılara karşı korunması alanında ileride yapılacak düzenlemelere kaynak oluşturmuştur. Bkz., Özdemir, **a.g.e.**, s. 18.

bilgiler için bunların düzeltilmesini veya kaldırılmasını talep hakkına sahiptir¹²¹.

Görüleceği üzere Komite, 17. maddeye dair yorumu ile ulusal ve uluslararası düzenlemelerde yer verilen kişisel verilerin korunmasına ilişkin temel ilkelere değinmiştir. Ancak belirtmemiz gerekir ki, verilerin korunmasına ilişkin doğrudan düzenleme getiren belgelere nazaran konuya ilişkin bazı ilkelere yer verilmemiştir. Örnek vermek gerekirse Komite, 17. maddeyi kişisel verilerin toplanmasının sınırlandırılması gerektiğine dair yorumlamış ancak burada toplanmanın hukuka uygun olması gerektiğine değinmemiştir. Ayrıca verilerin ancak belirtilen sınırlar içinde kullanılması gerektiği ve bu amaçlar dışında veya yetkisiz kişilerce kullanılmamasına dair güvencelerin getirilmesi ifade edilmemiştir. Hassas veri kategorilerinin tanımlanması ve bunlara ilişkin özel koruma tedbirlerinin düzenlenmesi gerektiğine de yer verilmemiştir¹²².

Yukarıda yer verdiğimiz genel nitelikli insan hakları belgelerindeki düzenlemelerin yanında Örgüt, kişisel verilerin korunmasına dair doğrudan düzenlemelerde de bulunmuştur. Bunlardan en önemlisi 1985 yılında Genel Kurul'a kişisel verilerin bilgisayar aracılığıyla işlenmesi hakkında yapılan teklifin değerlendirilmesi sonucu 1990 yılında kabul edilen “Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler”dir. Bu ilkeler tavsiye niteliğindedir ve henüz konu ile ilgili düzenlemelere mevzuatında yer vermeyen üye ülkeleri teşvik etmeyi, uluslararası sivil toplum kuruluşları ile hükümet içi kuruluşların kişisel verilerin işlenmesinde bu temel ilkeler çerçevesinde hareket etmelerini yönlendirmeyi amaçlamıştır. Ayrıca BM Rehber İlkeleri, kişisel verilerin korunması için yetkili ve bağımsız olan verilerin korunması organlarının kurulmasını öngören ilk uluslararası belgedir¹²³. Ancak ilkelerin, özellikle tavsiye niteliğinde diğer bir belge olan OECD Rehber İlkeleri'ne nazaran sınırlı bir etkisi olmuştur. Uygulamadaki sınırlı etkisine

¹²¹ 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. 253. (Bundan böyle “Data Protection Pursuant to the Right to Privacy in Human Rights Treaties” olarak anılacaktır).

¹²² Bygrave, “Data Protection Pursuant to Human Right to Privacy in Human Rights”, s. 253.

¹²³ Şimşek, a.g.e., s. 16; Küzeci, a.g.e., s. 124.

rağmen BM Rehber İlkeler'i, kişisel verilerin korumasına yönelik endişelerin yalnızca gelişmiş ülkelere dair ve batı menşeli olmadığını öne çıkarması açısından önemlidir¹²⁴.

3. Avrupa Konseyi ve Kişisel Verilerin Korunması

a. Genel Olarak

Kişisel verilerin korunması ile ilgili önemli çalışmalar yürüten diğer bir uluslararası kuruluş ise Avrupa Konseyidir. Avrupa Konseyinin amacı, 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 biçimde bağlı olarak, bu ülkünün korunması ve aynı hisleri paylaşan ülkeler arasında sıkı bir birliğin kurulmasıdır¹²⁵. AK'nin amaçları arasında yer alan ilkelerin en önemlisi insan haklarının ve temel özgürlüklerin geliştirilmesi ve korunmasıdır¹²⁶.

Kişisel verilerin korunmasına yönelik AK bünyesinde çeşitli girişimlerde bulunulmuştur. Bu girişimlerden en önemlisi ve temel hak ve özgürlüklerin korunmasına yönelik olarak kişisel verilerin korunmasına ilişkin doğrudan düzenleme getireni 28 Ocak 1981 tarihli “108 sayılı Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme”dir¹²⁷.

¹²⁴ Bygrave, “**Privacy and Data Protection in an International Perspective**”, s. 185. *Küzeci*'ye göre, her ikisi de tavsiye niteliğinde olmasına rağmen OECD Rehber ilkelerinin BM Rehber İlkelerine nazaran daha etkili olmasının arkasında konu ile ilgili ilk uluslararası belge olması yatmaktadır. Bkz., *Küzeci*, **a.g.e.**, s. 124.

¹²⁵ Bkz., AK Statüsü Başlangıcı. AK'nin kurucu belgesi olan AK Statüsü 5 Mayıs 1949'da imzaya açılmış ve 3 Ağustos 1949'da yürürlüğe girmiştir. AK Statüsü Türkçe metni için bkz., http://www.avrupakonseyi.org.tr/antlasma/aas_1.htm.

¹²⁶ AK Statüsü 3. maddesine göre Konsey'e üye her devlet, hukukun üstünlüğü ilkesiyle yargı yetkisi içindeki herkesin insan hakları ve temel özgürlüklerden yararlanması ilkesini kabul etmekte ve Konsey amacının gerçekleşmesinde içten ve etkin bir biçimde işbirliği yapmayı üstlenmektedir. Ayrıca Statü'nün 8. maddesine göre insan hakları ve temel özgürlükler uymayan, bunları ciddi bir biçimde çiğneyen üye devletlerin Konsey'den çıkarılması öngörülerek, insan haklarına saygı üye devletler için yaptırıma bağlanmıştır. Bkz., Gözübüyük-Gölcüklü, **a.g.e.**, s. 8.

¹²⁷ <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

Konsey bünyesinde kişisel verilerin korunmasına ilişkin yaklaşımın değerlendirilmesinde 108 sayılı Sözleşme'nin yanında Avrupa İnsan Hakları Sözleşmesi hükümleri de önemlidir. Ayrıca AIHS hükümlerinin üye devletlerde uygulanmasını izlemekten sorumlu olan Avrupa İnsan Hakları Mahkemesinin de kişisel verilerin korunmasını AIHS'in 8. maddesi kapsamında değerlendirdiği kararları mevcuttur.

AK bünyesinde ilgili sözleşmeler dışında bazı önemli belgelerde de kişisel verilerin korunmasına ilişkin hükümlere yer verilmiştir. Bu belgelere ilk örnek 4 Nisan 1997 tarihli ve 164 sayılı İnsan Hakları ve Biyotıp Sözleşmesi'dir¹²⁸. Bu sözleşme gen teknolojisi, embriyo üzerine araştırmalar, organ nakli gibi konularda genel kuralları içermektedir. Sözleşmenin başlangıç bölümünde EİHB, AIHS ve 108 sayılı Sözleşme'ye atıfta bulunulmuştur¹²⁹. Sözleşme, konusunun pek çok düzenlemede özel olarak koruma öngörülen hassas veri kategorisi ile yakından ilişkili olmasına karşın kişisel verilerin korunmasına dair yeterli düzenlemelere sahip olmadığı gerekçesiyle eleştirilmektedir¹³⁰.

Konsey bünyesindeki dikkate değer diğer bir sözleşme ise AK Siber Suç Sözleşmesi'dir¹³¹. Anılan sözleşme internet veya diğer bilgisayar ağları ile işlenen suçlar ile mücadele için yapılan ilk sözleşmedir. Siber suç ile mücadelede kişisel verilerin toplanması, işlenmesi ve uluslararası işbirliği çerçevesinde başka devletler ile paylaşılması düzenlenmiştir¹³². Sözleşme, kişisel verilerin işlenmesi ve sınır ötesi aktarımına dair hükümlere yer vermesine karşın verilerin korunmasına dair hükümlere yer vermediği, bu yönüyle de kişisel verilerin korunması hakkına ihlal

¹²⁸ Sözleşmenin orijinal metni için bkz., <http://conventions.coe.int/Treaty/en/Treaties/Word/164.doc>.

¹²⁹ İnsan Hakları ve Biyotıp Sözleşmesi, Başlangıç Bölümü, paras. 2, 3, 6.

¹³⁰ Kişisel verilerin korunmasına ilişkin olarak eksik düzenlemeye örnek vermek gerekirse, sözleşmede yer verilen kişiye ilişkin gen testi sonuçlarının devredilmesi ile ilgili bir hukuksal düzenleme bulunmamaktadır. Bkz., Şimşek, **a.g.e.**, s. 20. *Küzeci*'ye göre de sözleşme, verilerin korunmasına yönelik yeterli düzenlemelerden yoksundur. Bkz., Küzeci, **a.g.e.**, s. 127.

¹³¹ 23 Kasım 2001 tarihinde kabul edilen 185 sayılı AK Siber Suç Sözleşmesi 1 Temmuz 2004'te yürürlüğe girmiştir. Sözleşmenin orijinal metni için bkz. <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc>.

¹³² AK Siber Suç Sözleşmesi, Başlangıç bölümü.

oluşturacağı yönünden eleştirilmektedir¹³³.

Kişisel verilerin korunmasının sağlanabilmesi için hukuki düzenlemelerin gerekliliği yanında bireylerin bu konuya ilişkin haklarının bilincinde olması ve bunları kullanabilmesi gerekmektedir. Nitekim AK'nin kişisel verilerin korunmasına dair bu alanda bilinçlendirmeyi sağlamak için pek çok çalışmaları bulunmaktadır. Bu amaçla Konsey 2007 yılında 108 sayılı Sözleşme'nin imzaya açıldığı gün olan 28 Ocak'ı Veri Koruma Günü olarak ilan etmiştir¹³⁴.

b. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme

Teknolojinin insan hakları üzerindeki etkileri ve bu haklara ilişkin olası ihlaller AK bünyesinde 1968 yılında geniş kapsamlı bir şekilde ele alınmaya başlanmıştır. Konu ile ilgili somut girişimler 1973 ve 1974 yıllarında görülür. 1973 yılında 73(22) sayılı ilke kararı ile özel sektörde, 1974 yılında 74(29) sayılı ilke kararı ile kamu sektöründe üye devletlerin iç hukuk sistemlerinde uygulanmak üzere ilkeler önerilmiştir. Kişisel verilerin işlenmesi sektörünün sınır ötesi genişlemesi ile birlikte kapsamlı bir koruma mekanizmasına ihtiyaç duyulmuştur¹³⁵. Bunun üzerine 28 Ocak 1981 yılında 108 sayılı Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme imzaya açılmıştır. 108 sayılı Sözleşme, 1 Ekim 1985 yılında yürürlüğe girmiştir¹³⁶. Sözleşme ayrıca, kişisel verilerin korunmasına ilişkin kabul edilmiş olan ilk bağlayıcı uluslararası belge olması nedeniyle de büyük bir önem taşımaktadır. Sözleşme'nin 4. maddesine göre taraf devletler Sözleşme'de yer alan kişisel verilerin korunmasına ilişkin ilkelere

¹³³ Şimşek, **a.g.e.**, s. 20; Küzeci, **a.g.e.**, s. 128.

¹³⁴ http://www.coe.int/t/dghl/standardsetting/DataProtection/Data_protection_day_en.asp.

¹³⁵ Songül Atak, “Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler”, **Türkiye Barolar Birliği Dergisi**, S.87, 2010, s. 91. Ayrıca bkz., Gür, **a.g.e.**, s. 153.

¹³⁶ Sözleşmenin orijinal metni için http://coe.int/t/e/legal_cooperation/data_protection/background/11. Bu çalışmanın yazımı sırasında 12.04.2013 tarihi itibarıyla Uruguay 108 sayılı Sözleşmeyi ve ek protokolleri imzalayan 45. devlet olmuştur. Bu sözleşme Uruguay'da 01.08.2013 tarihinde yürürlüğe girecektir. Uruguay 108 sayılı Sözleşme'yi imzalayan ilk Avrupa dışı devlettir. Rusya, Türkiye ve Ukrayna ise 108 sayılı Sözleşme'yi imzalamış ancak onaylama işlemini henüz gerçekleştirmemişlerdir.

işlerlik kazandırıcı gerekli önlemleri iç hukuklarında almalıdırlar. Bu madde hükmü taraf devletlere iç hukuklarında düzenleme yapmalarına dair yükümlülük getirmektedir¹³⁷. Nitekim bu bağlayıcı yönüyle Sözleşme, hem imzalandığı hem de ileriki dönemlerde Avrupa'daki düzenlemeler ve uluslararası hukuk üzerinde etkili olmuştur¹³⁸.

Sözleşme AK üyesi olmayan devletlerin de imzasına açıktır¹³⁹. Böylece Konsey, Sözleşme'nin geniş bir alana etkili olmasını istemiştir. Sivil toplum temsilcilerinin özellikle AK üyesi olmayan devletleri bu imkandan faydalanmaları için yönlendirme çabalarına rağmen Sözleşme'ye taraf devletler arasında AK üyesi olmayan devlet bulunmamaktadır¹⁴⁰.

AK bünyesinde Avrupa kamu düzeninin anayasal belgesi olarak kabul edilen AİHS gibi etkili bir belge bulunurken 108 sayılı Sözleşme ile kişisel verilerin korunmasına dair doğrudan bir düzenleme getirilmiş olmasının açıklanması esasen 108 sayılı Sözleşme'nin öneminin benimsenmesi açısından gereklidir. Keza AİHS, kişisel verilerin korunmasını bağımsız bir hak olarak düzenlememiş, özel hayatın gizliliği hakkı kapsamında güvence altına almıştır. Kişisel verilerin korunmasına yönelik ilkeler somut olayın şartlarına göre AİHM içtihatları ile oluşturulmaya çalışılmıştır. Ancak, kişisel verilerin korunmasının gün geçtikçe artan önemi ve konuya dair sorunların çeşitlenmesi, özel bazı düzenlemeleri gerekli kılmıştır. 108 sayılı Sözleşme'nin başlangıç kısmında da konuya ilişkin artan endişelere dikkat çekilmiştir. Bu bağlamda anılan sözleşmenin başlangıç kısmında otomatik işleme tabi tutulmuş kişisel verilerin artan miktardaki sınır ötesi veri aktarımı bakımından her insanın temel hak ve özgürlüklerinin ve özellikle kişilik alanına riayet hakkının korumaya değer olduğu yönündeki düşünce vurgulanmıştır¹⁴¹. Böylece 108 sayılı Sözleşme ile kişisel verilerin korunması bağımsız bir hak olarak tanınarak özel

¹³⁷ Atak, **a.g.m.**, s. 90; Küzeci, **a.g.e.**, s. 130.

¹³⁸ Özdemir, **a.g.e.**, s. 21.

¹³⁹ 108 sayılı Sözleşme, m. 23.

¹⁴⁰ Bygrave, **“Privacy and Data Protection in an International Perspective”**, s. 182

¹⁴¹ Şimşek, **a.g.e.**, s. 22.

hayatın gizliliği hakkı dışında kalan boşluk doldurulmaya çalışılmıştır.

108 sayılı Sözleşme'nin kapsamı incelendiğinde kamu ve özel sektör ayrımı yapılmadığı görülür. Buna göre, hem kamusal hem de özel sektörde kişisel verilerin işlenmesi koruma kapsamındadır. Sözleşme öncelikle üye devletlerin iç hukukuna etki etmektedir. Ayrıca devletlerin ulusal makamları Avrupa düzeyindeki devletlerarası ilişkilerinde de Sözleşme hükümlerine uygun davranmakla yükümlüdürler¹⁴². 108 sayılı Sözleşme yalnızca otomatik yollar ile işlenen veriler açısından güvence öngörmüş, elle işlenen veriler kapsam dışında bırakılmıştır¹⁴³. Ancak Sözleşme'ye göre otomatik işleme için sürecin tamamının otomatik olması gerekmemektedir. Bu anlamda kısmen otomatik işlenen veriler de güvenceden yararlanabilir. Sözleşme'nin 3. maddesinin 2. fıkrasının c bendine göre; taraf devlet, Sözleşme'nin uygulama alanını otomatik veri işleme kapsamına girmeyen kişisel veri dosyaları hakkında da uygulanacağını bildirebilir. İlgili madde hükmü ve kısmen otomatik işlenen verilerin de koruma kapsamında değerlendirilebilmesi Sözleşme'nin uygulama alanını genişletmektedir¹⁴⁴.

108 sayılı Sözleşme'ye göre kişisel veri *“kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgiler”* olarak tanımlanmaktadır¹⁴⁵. Buna göre, Sözleşme sadece gerçek kişilerin korunması ile sınırlıdır. Ancak taraf devletlerin yasa koyucuları iç hukuklarında ilgili düzenlemeleri yaparken tüzel kişileri ve kişi topluluklarını da koruma kapsamına dahil edebilirler¹⁴⁶.

¹⁴² Keza, Europol Anlaşması 14. maddesine göre, devletlerin Europol Antlaşması'na katılabilmesi için öncelikle 108 sayılı Sözleşme'nin asgari standartlarını karşılamaları gerekmektedir. Bkz., Şimşek, **a.g.e.**, s. 23.

¹⁴³ 108 sayılı Sözleşme, m. 3/f.1

¹⁴⁴ Küzeci, **a.g.e.**, s. 131 vd. *Atak'a* göre ise Sözleşme'nin yalnızca otomatik işlenen verilere yönelik koruma sağlaması bir eksikliktir. Ancak yazar, Sözleşme'nin 11. madde hükmüne atıf yaparak taraf devletlerin Sözleşme'de öngörülen güvencelerden daha fazla güvence sağlayabileceğini belirtmiştir. Bu anlamda taraf devletler kişisel verilerin otomatik olmayan işlemlerine yönelik güvenceleri mevzuatlarında düzenleyebilirler. Bkz. Atak, **a.g.m.**, s. 95.

¹⁴⁵ 108 sayılı Sözleşme, m. 2.

¹⁴⁶ Sözleşme'nin 3. maddesinin 2. fıkrasının b bendine göre taraf devletler Sözleşme'nin uygulama alanını 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 kuruluşlar da

Sözleşme, kişisel verilerin işlenmesinde uyulacak temel ilkelere yer vermiştir. Bu ilkeler kişisel verilerin korunmasına yönelik asgari gerekliliklerdir. Taraf devletler daha geniş koruma getirebilirler¹⁴⁷. Sözleşme'nin 5. maddesine göre kişisel veriler;

- Meşru ve yasal yoldan elde edilmeli ve işleme tabi tutulmalıdır,

-Belli ve meşru amaçlar için kaydedilmeli ve bu amaçlara aykırı şekilde kullanılmamalıdır,

- Uygun ve elverişli olmalı ve kaydedildikleri amaca göre aşırı olmamalıdır,

- Doğru ve icabında güncel olmalıdır,

- İlgili kişilerin kimliklerini belirtecek bir biçimde ve kaydedildikleri nihai amaç için gerekli görülen süreyi aşmayacak bir şekilde muhafaza edilmelidir.

Sözleşme, “hassas veri” kategorilerine yönelik özel düzenlemeye yer vermektedir. Düzenlemenin yer aldığı 6. maddeye göre; kişilerin ırksal kökenleri, siyasal düşünceleri, dinsel inançları gibi hassas veriler ilgili devletin ulusal hukukunda uygun güvenceler sağlanamadığı takdirde otomatik olarak işlenemez.

Sözleşme'nin 7. maddesi veri güvenliği ilkesine yer vermiştir. Buna göre; verilere yetkisiz erişimin bunların değiştirilmesinin ya da ortadan kaldırılmasının önlenmesi için taraf devletlerce veri güvenliği sağlanmalıdır.

Veri sahibinin sahip olacağı haklara ise Sözleşme'nin 8. maddesinde yer verilmiştir. İlgili madde hükmüne göre; her gerçek kişi, kendisine ait kişisel verileri içeren bir dosyanın varlığından haberdar edilmelidir. Bununla birlikte eğer bu veriler hukuka aykırı bir şekilde işlenmişse ilgilinin kendisine ait bu türden verileri sildirtme, yanlış verileri düzeltme; bu taleplerine uyulmadığı takdirde hukuksal yollara

kapsam dahiline alabilir. Bkz., Bing, **a.g.m.**, s. 274.

¹⁴⁷ 108 sayılı Sözleşme, m. 11.

başvurma hakkı bulunmaktadır.

Yukarıda yer verdiğimiz ilkeler ve haklara bazı sınırlamalar da getirilebilir. Ancak, bu sınırlamalar yalnızca 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 yapılabilir¹⁴⁸.

108 sayılı Sözleşme ile ayrıca Danışma Komitesi kurulması öngörülmüştür. Taraf devletlerden her biri bu Komiteye bir temsilci ve vekili görevlendirecektir¹⁴⁹. Komite, Sözleşme metninde yer alan hükümleri yorumlamaktan ve uygulamaları geliştirmekten sorumludur. Ayrıca Komite, kişisel verilerin korunmasına ilişkin raporlar hazırlamak ve rehber ilkeleri geliştirmek ile görevlendirilmiştir¹⁵⁰.

Danışma Komitesi, 2001 yılında Sözleşme'ye ek protokol yayımlanmış ve bu protokol 2004 yılında yürürlüğe girmiştir. Bu protokol ile taraf devletlere kendi iç hukuklarında aldıkları önlemlerin Sözleşme ve Protokol'de yer alan ilkelere uygunluğunu güvence altına almaktan sorumlu olacak bir ya da birden fazla kontrol makamı oluşturma zorunluluğu getirmektedir¹⁵¹. Yine ilgili ek protokol ile üçüncü ülkelere veri aktarımına dair hükümler geliştirilmeye çalışılmıştır. Ek protokol öncesinde sınır ötesi veri aktarımını düzenleyen 12. madde bir taraf devletten diğerine yapılacak veri transferinin, özel yaşam gerekçesiyle engellenmesini ya da özel bir izne tabi tutulmasını yasaklamaktadır. Ancak taraf devletin mevzuatı belirli kategorilerdeki kişisel veriler için özel bir düzenleme içeriyorsa ve diğer taraf devletin mevzuatı bu konuda eşit bir koruma içermiyorsa, o devlete yapılacak veri transferine sınırlama getirebilir. Ek protokol ile getirilen düzenlemeye göre kişisel

¹⁴⁸ 108 sayılı Sözleşme, m. 9. İlgili madde hükmünde yer verilen sınırlamanın sınırları, AİHS'in özel yaşamın gizliliği hakkını düzenleyen 8. maddesinin 2. fıkrasındaki sınırlamalara koşut bir düzenleme getirmektedir. Bkz., Küzeci, **a.g.e.**, s. 133.

¹⁴⁹ 108 sayılı Sözleşme, m. 18.

¹⁵⁰ 108 sayılı Sözleşme, m. 19.

¹⁵¹ Ek Protokol, m. 1. Taraf devletlerin iç hukuklarında kontrol makamının öngörülmesi yerinde olmak ile birlikte Sözleşme hükümlerinin uygulanmasını denetlemek ile görevli bir Sözleşme organının yoksunluğu, Sözleşme'nin eksikliği olarak eleştirilmektedir. Bkz. Atak, **a.g.e.**, s. 120.

verilerin Sözleşme'ye taraf olmayan bir uluslararası örgüte ya da ülkeye gönderilebilmesi için bu devletin ya da örgütün uygun veri koruma seviyesini göstermesi gerekmektedir¹⁵². Ancak veri aktarımında eğer kişinin üstün bir yararı veya güvenlik tedbirleri için ülkeler arası yapılan anlaşmalar söz konusu ise, kişisel veriler üçüncü ülkelere veya milletlerarası organizasyonlara gönderebilirler¹⁵³.

108 sayılı Sözleşme'nin 4. maddesine göre taraf devlet, Sözleşme'yi onaylamadan önce iç hukukunda yapacağı yasal düzenlemeler ile Sözleşme'de belirtilen temel ilkeleri yerine getirme yükümlülüğündedir. Ülkemizde konu ile ilgili bir yasal bir düzenleme yapılmadığından 108 sayılı Sözleşme 1981 tarihinde imzalanmış olmasına rağmen henüz onaylanmamıştır.

Genele baktığımızda 108 sayılı Sözleşme, kişisel verilerin korunmasına ilişkin asgari standartları belirlemesinden ötürü taraf devletlerin mevzuatlarında konu ile ilgili farklı düzenlemeleri kabul etmişlerdir. Bu durum 108 sayılı Sözleşme'nin üye devletlerde kişisel verilerin korunmasına dair uyum çalışmalarında yetersiz kaldığı yönünde eleştirilmesine neden olmuştur. Yine 108 sayılı Sözleşme bazı temel terimlere dair belirsizlikler içerdiği yönünden de eleştirilmiştir¹⁵⁴. Eksiklikleri ve eleştirildiği noktalar bir kenara bırakıldığında Sözleşme, kişisel verilerin korunmasına ilişkin bağlayıcı ilk uluslararası belge olması ve AK Konsey kararlarının etkisi nedeniyle önemini korumaktadır. Kişisel verilerin korunmasına ilişkin sorunların çeşitlenmesi ve konu ile ilgili yeni yaklaşımların sergilenmesi nedeniyle AK, Sözleşme'nin güncelliğini devam ettirmesi ve geniş bir alanda korumanın sağlanması için çalışmalarına devam etmektedir. Bu amaç doğrultusunda Danışma Komitesi 28-30 Haziran 2011 tarihindeki görüşmelerinde 108 sayılı Sözleşme'nin gözden geçirilmesini dile getirmişlerdir. Bu doğrultuda Danışma

¹⁵² Ek Protokol, m. 2.

¹⁵³ Ek Protokol, m. 2/f.2.

¹⁵⁴ Fred Cate, "The Changing Face of Privacy Protection in the European Union and the United States", **Indiana Law Review**, S. 33, 1999-2000, s. 181.

Komitesi 108 sayılı Sözleşme'nin değiştirilmesine ilişkin teklifini sunmuştur¹⁵⁵.

c. Avrupa İnsan Hakları Sözleşmesi ve Kişisel Verilerin Korunması

(1) AİHS 8. Madde Kapsamında Kişisel Verilerin Korunması

Kişisel verilerin korunmasına ilişkin düzenlemeler için Avrupa İnsan Hakları Sözleşmesi önemli bir yere sahiptir. AİHS, Avrupa ülkeleri arasında korunan temel haklar kategorisinde yer alan Anayasa Hukuku niteliğinde bir sözleşmedir ve imzaya açıldığı 1950 yılından günümüze insan haklarının en önemli kaynağı olma özelliğini korumaktadır¹⁵⁶.

Öncelikle belirtmemiz gerekir ki, AİHS'te kişisel verilerin korunması bağımsız bir hak olarak tanınmamıştır. Buna karşılık Sözleşme'nin 8. maddesinde özel yaşamın gizliliği hakkı düzenlenmiştir. AİHS'in “Özel Hayat ve Aile Hayatına Saygı” kenar başlıklı 8. maddesine göre; “(1) Herkes, özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir. (2) Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve hukuka uygun olmak koşuluyla söz konusu olabilir”.

¹⁵⁵ Danışma Komitesi tarafından hazırlanan 29.10.2012 tarihli 108 sayılı Sözleşme'ne dair değişiklik teklifi için bkz., The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS no. 108], **Modernisation of Convention 108**, T-PD(2012)4Rev3_en, (Çevrimiçi) [http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD\(2012\)4Rev3E%20-%20Modernisation%20of%20Convention%20108.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)4Rev3E%20-%20Modernisation%20of%20Convention%20108.pdf), 01.05.2013.

¹⁵⁶ Avrupa İnsan Hakları Sözleşmesi veya tam adıyla “İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi” 4 Kasım 1950'de Roma'da imzalanmış, 3 Eylül 1953'te on devletin onaylama sürecini tamamlaması ile yürürlüğe girmiştir. Türkiye AİHS'nin onaylama sürecini 18 Mayıs 1954'te tamamlamıştır. 28 Ocak 1987 tarihinde Avrupa İnsan Hakları Komisyonu'na, 22 Ocak 1990 tarihinde ise Avrupa İnsan Hakları Divanına bireysel başvuru hakkının tanınması ile Sözleşme'nin Türkiye açısından asıl önemi ortaya çıkmıştır. AİHS'in asıl önemi ortak güvence sistemine dayanan uluslararası bir yargısal denetim mekanizması kurması ve bireye sağlanan güvenceyi yaptırıma bağlamasıdır. Böylece Sözleşme, insan haklarının korunması sorununu ulusal düzeyden uluslararası düzeye taşımış, birey uluslararası hukukun süjesi haline gelmiştir. Bkz., Gölcüklü-Gözübüyük, **a.g.e.**, s. 11.

Madde hükmünden de görülebileceği gibi kişinin özel yaşamı, aile yaşamı, evi ve haberleşmesi güvence altına alınmış, ancak kişisel verilerin korunmasına dair hükümlere açıkça yer verilmemiştir¹⁵⁷. Buna karşılık AIHM kişisel verilerin özel hayat alanı içinde yer aldığını kabul etmekte ve bu konuyla ilgili başvuruları 8. madde kapsamında incelemektedir¹⁵⁸. Diyebiliriz ki, kişisel verilerin korunmasının AIHS anlamında özel hayata saygı hakkının özel olarak şekillenmiş kısmi bir alanını oluşturduğu ifade edilmektedir¹⁵⁹. Bu bağlamda, 8. madde kapsamında değerlendirilen kişisel verilerin korunması hakkına ilişkin güvenceleri açıklayabilmemiz için AIHM içtihatlarına başvurmamız gerekmektedir.

(2) Kişisel Verilerin Korunmasına İlişkin AIHM Kararları

AIHM, *Klass ve Diğerleri/Almanya* kararından itibaren kişisel verilerin korunması konusunda önemli saptamalar yapmıştır. Bu nedenledir ki, Mahkeme'nin kişisel veriler ile ilişkili ilk önemli kararı olan *Klass ve diğerleri/Almanya* kararına öncelikli olarak yer vermemiz gerekir¹⁶⁰. Bu kararda Mahkeme, gizli telefon dinlemelerini özel hayat alanına müdahale olarak değerlendirmiş, bunun gibi teknik araçlarla özel hayat alanına müdahale sırasında özel koruma tedbirlerinin, kontrol mekanizmalarının ve hukuksal araçların gerekliliğini vurgulamıştır¹⁶¹. Belirtmek isteriz ki AIHM, söz konusu kararda kişisel veri kavramını kullanmamakla birlikte kişiye ait bilgilerin gizli izleme yöntemleri ile toplanması konusunu ele almıştır.

¹⁵⁷ AIHS'nin kabul edildiği 1950 yılında kişisel verilerin korunmasına ilişkin tartışmalar henüz gelişmediğinden konuya ilişkin bir düzenleme bulunmamaktadır. Ancak AIHM, Sözleşme'yi güncel koşullar altında yorumlanması gereken yaşayan bir enstrüman olarak tanımlamakta ve bu anlamda yeni gelişmelere açık bir tutum sergilemektedir. Ayrıca 1980'lerden itibaren Avrupa Konseyi üyesi devletlerinin, özellikle 108 sayılı Sözleşme'nin de etkisiyle, kişisel verilerin korunmasına ilişkin genel ilkeleri belirleyici düzenlemeler getirme yolundaki eğilimleri AIHM ve Komisyon'un konuyu 8. madde kapsamında değerlendirmesine neden olmuştur. Bkz., Bygrave, “**Data Protection Pursuant to Right to Protection of Privacy in Human Right Treaties**”, s. 11.

¹⁵⁸ Belirtmek isteriz ki, AIHS'in ilk şeklinde ikili bir yapı öngörülmüştü. Buna göre, Avrupa İnsan Hakları Mahkemesi ve Avrupa İnsan Hakları Komisyonu olmak üzere iki ayrı organ kurulmuştu. Daha sonra 1 Kasım 1998 tarihinde yürürlüğe giren 11. Protokol ile denetim sistemi değiştirilmiştir. 11. Protokol ile Komisyon ve Mahkeme birleştirilmiş ve denetim sistemi tek organlı hale getirilmiştir.

¹⁵⁹ Şimşek, **a.g.e.**, s. 31

¹⁶⁰ *Klass ve diğerleri/Almanya*, b.n. 5029/71, k.t. 06.09.1978. Kararın Türkçe çevirisi için bkz., <http://aihm.anadolu.edu.tr/aihmgooster.asp?id=30>.

¹⁶¹ Şimşek, **a.g.e.**, s. 33

Mevcut olayda Alman Anayasası'nın 10. maddesinin 2. fıkrası hükmü ve bu hükme dayanarak çıkartılan Mektup, Posta ve Telekomünikasyonun Gizliliğinin Sınırlandırılması Yasası'nın AİHS'e aykırı olduğu öne sürülmüştür. Başvurucular mevcut olayda devletin bir yasayla denetim tedbirleri almasına itiraz etmemektedirler. Başvurucuların itirazı söz konusu yasa ile devletin kendilerini bilgilendirme yükümlülüğü bulunmaksızın haberleşmelerini ve telefon görüşmelerini izleyebilme ve kendileri hakkında önlemler alabilme yetkisinin getirilmesi ve bu uygulamaya karşı da mahkeme önünde hak arama özgürlüğünün tanınmadığı yönündedir.

Mahkemeye göre yasal bir dayanak olmaksızın kişinin iletişimin dinlenmesi 8. maddede düzenlenen özel hayatın gizliliği hakkına müdahale teşkil eder. Ayrıca, yasal dayanağı olan ve yasaya uygun olarak gerçekleştirilen arama ve telefonların dinlenmesi de 8. maddeye müdahale niteliği taşır. Yasanın varlığı dahi yasanın uygulanacağı bütün kişileri gözetim tehdidi altında tutmaktadır¹⁶². Mahkemenin müdahalenin varlığı yönündeki kararı üzerine önemli olan bu müdahalenin ikinci fıkrası kapsamında meşru olup olmadığının incelenmesidir. Buna göre kamu otoritelerince yapılan müdahale “hukuka uygun olarak”, “ulusal güvenlik”, “kamu güvenliği”, “suçun veya düzensizliğin önlenmesi”, “başkalarının hak ve özgürlüklerinin korunması” ve “demokratik bir toplumda gerekli” olarak yapıldığı takdirde meşru ve haklı kabul edilir. Bu sınırlama sebepleri ile temel haklara

¹⁶² *Klass ve diğerleri/Almanya*, para. 41. *Klass ve diğerleri/Almanya* kararı bu noktada “potansiyel mağdur” görüşüne yer vermiştir. AİHS sisteminde *actio popularis* yani kamu davası açma hakkı tanınmamıştır. Hem Komisyonun hem de Mahkemenin görüşü ile mevcut olayda doğrudan mağdur oldukları belirli olmayan başvurular olsa da bunlar, “potansiyel mağdur” olarak kabul edilmiştir. Hükümet temsilcisi, yasada öngörülen denetim önleminin hiçbir zaman başvurucular hakkında uygulanmadığı hakları somut olarak ihlal edilmemiş başvurucuların AİHS anlamında mağdur sıfatına haiz olmadıkları yönünde savunmada bulunmuştur. Ancak AİHM kararında, mevcut olayda sorunun itiraz konusu önlemlerin gizli olması ve gizli izleme yöntemlerinin doğası gereği başvurucuların belirli somut işlemi gösteremeyeceklerini vurgulamıştır. Yasanın varlığı, bütün kişileri gözetim tehdidi altına sokmaktadır. Sırf bu uygulamanın varlığı nedeniyle 8. maddenin ihlalinin ötürü başvurucuların “mağdur” olduğu iddia edilebilir. AİHM potansiyel mağdurluğa ilişkin diğer bir kararı ise *Malone* kararıdır. bkz., *Malone/Birleşik Krallık*, b.n. 8691/79, k.t. 02.08.1984, para. 86. *Küzeci*'ye göre bir İSS'nin kullanıcının hangi siteleri ziyaret ettiğini veya cep telefonu operatörünün abonesinin yer bilgilerini hükümet organları ile paylaşma potansiyel tehlikesini üzerinde hissedilen kişinin durumlarında görüleceği gibi haklarının ihlal edildiğine dair elinde somut bir bilgi bulunmayan kişi kendisini potansiyel mağdur durumuna düşüren bir yasal düzenlemeye ilişkin olarak AİHM'e itirazda bulunabilecektir. Kararın “potansiyel mağdur” yorumu bu anlamda kişisel verilerin korunması açısından önemli yararlar sağlayacaktır. Bkz. *Küzeci*, a.g.e., s. 141, d.n.146.

istisnalar getirilmekte ve bunların dar yorumlanması gerekmektedir¹⁶³. Mevcut olaydaki gibi gizli izleme yöntemlerinin mevcut oluşu hallerde 8. maddenin 2. fıkrasında yer alan “demokratik toplumun gerekliliği” istisnasına ancak kesinlikle gerekli olduğu ölçüde katlanılabilir¹⁶⁴. Bireyin 8. madde kapsamında güvence altına alınan hakkının kullanılması ile demokratik toplumun gerekliliği arasında denge kurulması zorunludur. Gizli izleme yöntemlerinin kullanılması açısından Avrupa devletleri, casusluk ve terörle mücadeleyi gerekçe göstermektedir. Ancak, casusluk ve terörle mücadele gerekçe gösterilerek gizli izleme yöntemlerinin benimsenmesinde devletlerin sınırsız takdir yetkisi yoktur¹⁶⁵. Ayrıca Mahkeme, hangi izleme yöntemi benimsenirse benimsensin, kötüye kullanmaya karşı yeterli ve etkili güvencelerin alındığına dair ikna olmalıdır. Güvencelerin değerlendirilmesinde olası önlemlerin niteliği, kapsamı ve süresi; bu önlemleri emretmek için gerekli sebepler, bu önlemler için emir veren, uygulayan ve denetleyen yetkili makamlar ve ulusal hukukta tanınan iç hukuk yollarının türü gibi olayın bütün koşulları göz önüne alınır¹⁶⁶. Bütün bu bilgilerin ışığında Mahkeme, mevcut olayda Alman mevzuatında yer alan düzenlemenin anılan güvenceleri sağladığını saptamıştır. Mahkemeye göre mevcut olayda kamu makamlarının 8. madde kapsamındaki özel hayatın gizliliği ilkesine müdahalesi olmakla birlikte bu müdahalenin 8. maddenin 2. fıkrasına göre demokratik bir toplumda gerekli olduğuna, mevcut yasanın gerekli güvenceleri sağladığını saptamış ve bu nedenle 8. maddenin ihlal edilmediğine karar vermiştir.

AIHM'in kişisel verilerin korunması ve saklanması ile ilgili ele aldığı diğer bir dava ise *Leander/İsveç* davasıdır¹⁶⁷. Mevcut olayda askeri bölgede bulunan bir müzede teknisyen olarak çalışan başvurucunun görevine işe başlamasının ardından son verilmiştir. Gerekçe olarak da polis sicil kayıtlarında geçmişi hakkında elde

¹⁶³ *Klass ve diğerleri/Almanya*, para 42.

¹⁶⁴ Belirtmemiz gerekir ki AIHM, gizli izleme yöntemlerine dair başvurularda gereklilik ölçütünü diğer başvurulara nazaran daha sıkı bir biçimde uygulamıştır. Bkz., Bygrave, “**Data Protection Pursuant to Right of Privacy in the Human Right Treaties**”, s. 273.

¹⁶⁵ *Klass ve diğerleri/Almanya*, para. 48.

¹⁶⁶ *Klass ve diğerleri/Almanya*, para. 50.

¹⁶⁷ *Leander/İsveç*, b.n. 9248/81, k.t. 26.03.1987.

edilen bilgiler dahilinde kendisi hakkında yapılan güvenlik soruşturmasının sonucunun olumsuz olması gösterilmiştir. Ayrıca bu bilgilerin içeriği hakkında kendisine bilgi verilmemiştir. Başvurucu kendisi hakkında bilgi toplanması, bu bilgilerin içeriğinin hakkında kendisine bilgi verilmemesi, bunların yanlışlığını kanıtlama hakkının kendisine tanınmamış olmasından ötürü özel hayatının gizliliği hakkının ihlal edildiğine dair başvuruda bulunmuştur. Mahkeme mevcut olayda gizli polis sicilinde tutulan bilgilerin başvurusunun özel hayatı ile ilgili olduğunu belirtmiştir. Bu tür bilgilerin toplanması ve saklanması ile birlikte söz konusu bilgilerin ilgili makamlara devri ve başvurusuya itiraz hakkı verilmemesini 8. madde açısından müdahale oluşturduğuna karar vermiştir¹⁶⁸. Mahkeme bu davada özel hayatın gizliliği hakkına yönelik bir müdahale olduğunu kabul etmekle beraber bu müdahaleyi haklı kılacak koşulların mevcut olduğu sonucuna varmıştır. Mevcut olayda müdahale yasaya dayanılarak yapılmıştır. Ayrıca Mahkemeye göre kararlara itiraz etme hakkına dair işlemlerin Meclis Adalet Komisyonu, Meclis Ombudsmanı ve Adalet Bakanı tarafından denetlenmesinden yola çıkarak yargı yoluna gerek kalmaksızın da etkili bir denetim yolunun sağlandığını belirtmiştir¹⁶⁹. Bu doğrultuda Mahkemeye göre müdahale konusunu düzenleyen yasa, yeterli güvencelere sahiptir. Başvurucuya kendisi ile ilgili toplanan verilerin içeriği hakkında bilgi verilmemesi, müdahalenin kendiliğinden ulusal güvenlik için demokratik toplumda gerekli olmayan bir müdahale olduğu sonucuna varmayı gerektirmez¹⁷⁰. Burada devletin takdir yetkisi vardır. Mahkeme, mevcut olayda davalı devletin ulusal güvenliği sağlama amacını gerçekleştirmek için geniş takdir yetkisi olduğunu vurgulamıştır¹⁷¹. Öyle ki davalı devlet, ulusal güvenliği başvurusunun bireysel menfaatleri üzerinde görme hakkına sahiptir. Müdahale, ulusal güvenliğin sağlanması amacıyla demokratik toplumun gerektirdiği bir müdahaledir ve meşru amaçla orantılıdır. Dolayısıyla mevcut olayda müdahale ile AIHS'nin 8. maddesi ihlal edilmemiştir¹⁷².

¹⁶⁸ *Leander/İsveç*, para. 48.

¹⁶⁹ *Leander/İsveç*, para. 67.

¹⁷⁰ *Leander/İsveç*, para. 66.

¹⁷¹ *Leander/İsveç*, para. 59.

¹⁷² *Leander/İsveç*, para. 67.

Mahkeme, devletin ulusal güvenliği açısından önem taşıyan görevlere getirilecek adayların bu görevler için uygun olup olmadığına karar verirken bu kişiler hakkında toplanan verileri kullanabileceğini kabul etmiştir. Ancak somut olayda başvuruçunun müzede yapacağı işin niteliği üzerinde durmamış ve işin ulusal güvenlik açısından tehlike taşıyıp taşımadığını değerlendirmemiştir¹⁷³.

AİHM, kişisel verilerin korunmasına ilişkin devletin pozitif yükümlülüğünü *Gaskin/Birleşik Krallık* kararında ele almıştır¹⁷⁴. Mevcut olayda çocukluğunu sosyal hizmetlerin bakımı altında geçirmiş olan başvuruçucu, geçmişi hakkında bilgi edinmeyi, nerelerde yaşadığı ve kimler tarafından hangi koşullarda bakıldığı konusunda tutulan raporların kendisine açıklanmasını istemektedir. Bu raporlardaki bilgilerin kendi geçmişi hakkında bilgi edinmesini sağlayacağını ve bugün yaşamış olduğu sıkıntı ve sorunların çözümüne katkıda bulunacağını ileri sürmektedir. Ancak başvuruçunun talebi, bu tür raporları hazırlayan görevlilerin söz konusu raporların ilgili kişiye açıklanmayacağını bildikleri için gerçek görüşlerini açıkça ortaya koydukları, eğer bu raporlar açıklanırsa bu görevlilerin yeterince açık olmaktan kaçınabileceği ve bu durumun mevcut sosyal hizmet sisteminin iyi işlemesine engel olabileceği gerekçeleriyle reddedilmiştir.

Mevcut olayda başvuruçucu, kendisi hakkında tutulan raporların tamamına ulaşamamaktan şikayet etmektedir. Burada devletin başvuruçunun talebine rağmen hakkındaki bilgilere erişimin sağlanmaması, yani devletin eylemsizliği söz konusudur. Bu anlamda mevcut olayda devletin pozitif yükümlülüğünü yerine getirip getirmediğinin incelenmesi gerekmektedir¹⁷⁵. Mahkemeye göre başvuruçunun

¹⁷³ Atak, **a.g.m.**, s. 106.

¹⁷⁴ *Gaskin/Birleşik Krallık*, b.n. 10454/83, k.t. 07.07.1989. Kararın Türkçesi için bkz., <http://aihm.anadolu.edu.tr/aihmgooster.asp?id=192>.

¹⁷⁵ Mahkeme, kişinin hakkındaki bilgilere erişim hakkının sağlanmamasını ve bu anlamda devletin pozitif yükümlülüğünü yerine getirip getirmediğinin incelenmesi gerektiğine dair karar verirken mevcut olayı *Leander* davası ile karşılaştırmıştır. Mevcut olayda da *Leander* davasında olduğu gibi başvuruçucu hakkında bütünüyle inceleme olanağı bulamadığı kişisel geçmişiyle ilgili ayrıntıların yer aldığı bir dosya bulunmaktadır. Ancak her iki davadaki koşullar birbirinden farklıdır. Buna göre *Leander* davasından farklı olarak mevcut olayda yerel makam tarafından derlenen ve elde tutulan bilgi, başvuruçunun temel kimlik özellikleriyle ilgili ve aslında kendisinin erken çocukluk dönemi ve oluşum yıllarına ait tek somut kayıt olduğu için, kendisinin dosyaya ulaşmasına izin verilmemesi, özel

durumundaki bir kimsenin, çocukluğunu ve gelişiminin erken dönemini bilmek ve anlamak için gerekli bilgileri almakta Sözleşme'yle korunan hayati bir menfaati vardır. Kamu belgelerinin gizliliğinin, objektif ve güvenilir bilgi elde edilmesi için önem taşımaktadır ve bu tür bir gizlilik üçüncü kişilerin korunması için gereklidir. Bununla birlikte Mahkeme, özel hayatıyla ilgili kayıtlara ulaşmak isteyen bireyin menfaatlerinin, raporlarda katkıda bulunan kişinin mevcut olmadığı veya gereksiz yere rıza göstermeyi reddettiği hallerde korunması gerektiğini düşünmektedir. Bir sistem ancak, rapora katkıda bulunan bir kimsenin yanıt vermediği veya rıza göstermediği hallerde, rapora ulaşma imkanının verilir verilmemesi gerektiğine nihai olarak bağımsız bir makamın karar vermesini öngördüğü zaman, orantılılık ilkesine uygun düşer. Mevcut olayda bu sağlanmadığından 8. maddenin öngördüğü pozitif yükümlülüğün ihlali söz konusudur¹⁷⁶.

Gaskin kararı kişisel verilere erişim hakkının her türlü kişisel veriyi kapsadığı yönünde yorumlanmamalıdır. Anılan karardaki kişisel veriler başvurunun psikolojik sağlığı ve kimliği açısından önemli bir yere sahiptirler. Bu verilere ulaşımın reddedilmesi başvurunun kişisel gelişimini önemli bir biçimde engelleyecektir. Dolayısıyla Mahkeme, her türlü kişisel verilere erişim hakkını değil, anılan karardaki gibi bireyin gelişimi için önemli olan kişisel verilere erişim hakkını kabul etmiştir¹⁷⁷.

hayatına saygı hakkına bir müdahale oluşturmaktadır. Başvurucu, *Leander* davasındaki başvurucudan farklı olarak, kendisi hakkında bilgi derlenmesi ve elde tutulmasına karşı çıkmamakta veya bu bilgilerin kendisi hakkında aleyhine kullanıldığını iddia etmemektedir. Aslında *Gaskin* davasında başvuru hakkında derlenen bilgi, *Leander* davasında olduğundan tamamen farklı bir amaca hizmet etmektedir. *Gaskin* davasında başvuru, kendisine engel çıkartmadan bilgiye ulaşma imkanı verilmemesine karşı çıkmaktadır. Gerçekten de, kendisinin dosyasına tam olarak ulaşma talebinin reddedilmesi suretiyle davalı devletin başvurunun özel hayatına "müdahale ettiği" söylenemez. Bu tür bir reddetme konusunda başvurunun şikayetin özünü, Devletin tasarrufuna değil, fakat tasarrufta bulunmamasına karşıdır. Bkz., *Gaskin/Birleşik Krallık*, para. 41. Ayrıca bkz., Bygrave, "Data Protection Pursuant to the right of Privacy in the Human Right Treaties", s. 278, d.n.129. Görüldüğü gibi Mahkeme, kişisel verilere erişim hakkını devlete pozitif ödev yükümleyen AİHS'in 8. maddesi kapsamında değerlendirmiştir.

¹⁷⁶ *Gaskin/Birleşik Krallık*, para. 49.

¹⁷⁷ Bygrave, "Data Protection Pursuant to the right of Privacy in the Human Right Treaties", s. 278. AİHM içtihatlarıyla kişisel verilerin korunmasını 8. madde kapsamında yorumlamasıyla birlikte bu yorum belirli açılardan sınırlı kalmaktadır. Kişisel verilere erişim hakkının yorumlandığı *Gaskin* kararı da bu sınırlı yoruma örnek teşkil eder. Kişisel verilerin korunması hukukunda bireye tanınan

AIHM'in bireylere ilişkin kişisel bilgilerin resmi makamlarca toplanarak arşivlenmesine ilişkin önemli bir değerlendirmesi ise *Amann/İsviçre* kararıdır¹⁷⁸. Mevcut olayda eski Sovyetler Birliği elçiliğinde çalışan bir bayan 1981 yılında ticaretle uğraşan başvurucuyu aramış ve ürün siparişi vermiştir. Telefon görüşmesi İsviçre Federal Savcılık tarafından dinlenmiştir. Bu gizli dinleme üzerine başvuru hakkında bilgi kartı (fişlik) oluşturulmuştur. 1990 yılında vatandaşlar hakkında İsviçre Federal Savcılık tarafından bilgi kartlarının oluşturulduğunun ortaya çıkmasıyla başvuru, durumdan haberdar olmuştur. Bunun üzerine başvuru tazminat talebinde bulunmuş ancak talebi İsviçre makamları tarafından reddedilmiştir. Başvuru üzerine Mahkeme hem özel hem de mesleki telefon görüşmelerinin dinlenmesinin ve kayda alınmasını özel hayat kapsamında değerlendirmiştir¹⁷⁹. Kararda Mahkeme, özel hayat kavramının geniş yorumlanması gerektiği ve bu anlamda özel hayatın diğer insanlarla ilişki kurma ve geliştirme hakkını da kapsadığını, buna iş ve mesleki faaliyetlerin de dahil edilmesi gerektiğini tespit etmiştir. Özel hayatın geniş yorumlanması gerektiği 108 sayılı Sözleşme'nin amacının düzenlendiği 1. maddesi ile kişisel verinin tanımının yapıldığı 2. maddesine atıf yapılmak suretiyle de temellendirilmiştir. 108 sayılı Sözleşme'ye göre kişisel veri, kişinin bilinmesini ve bilinebilmesini sağlayan her türlü bilgiye karşılık gelmektedir. Buna göre AIHM, başvuru hakkında Rus elçiliği ile bağlantısı olduğu ve şirketlerle ticari ilişkilerine dair bilgilerin fişlikte yer alması bireyin özel hayatına müdahale teşkil ettiğini belirtmiştir¹⁸⁰. Mahkemeye göre başvurucuyla ilgili kamu

kendisiyle ilgili kişisel verilerine erişim hakkı, AIHM'in kabul ettiği gibi söz konusu veriler ile bireyin kişisel gelişimi arasında bağlantı aranmamaktadır. İlgilinin kişisel verilerine erişim hakkı, kişisel verilerin korunmasına özgü temel ilkelerden söz konusu verilerin doğruluğunu denetleme, onları düzeltme, silme ve engelleme hakkının gerekliliğidir. Bireyin kişisel verilerine erişim hakkı, bilgilerin geleceğini belirleme hakkını temel alır. Nitekim birey ancak hangi verilerinin kimlerin elinde ve ne gibi amaçlarla tutulduğunu ve kullanıldığını bildiği takdirde bu haktan yararlanabilir. Konuya ilişkin ayrıntılı açıklamalara çalışmamızın ilgili kişisel verilerin korunmasına özgü temel ilkeler başlığı altında yer verilecektir.

¹⁷⁸ *Amann/İsviçre*, b.n. 27798/95, k.t. 16.02.2000.

¹⁷⁹ *Amann/İsviçre*, para. 44.

¹⁸⁰ *Amann/İsviçre*, paras. 65-67. AIHM eski başkanı Rolv Ryssdall da 108 sayılı Sözleşme'nin etkisine vurgu yapmış, söz konusu Sözleşme'de yer alan temel ilkelerin AIHS'nin 8. maddesinin yorumlanmasında yardımcı olacağını ifade etmiştir. Bkz., Bygrave, **“Data Protection Pursuant to the right of Privacy in the Human Right Treaties”**, s. 256. AIHM'in 8. madde kapsamında güvence altına alınan hakkın diğer insanlarla ilişki kurmak ve geliştirmek hakkını da kapsadığına dair başka

makamlarınca tutulan bilgi kartlarındaki verilerin içeriği, kamu makamlarınca söz konusu verilerin kullanılması veya bu kullanım sonucunda başvurucunun zor duruma düşmüş olması önemli değildir. Keza, kamu makamlarınca bilgi kartlarının tutulmuş olması dahi 8. madde kapsamında güvence altına alınmış olan özel hayatın gizliliği hakkına müdahalenin tespiti için yeterlidir¹⁸¹. Mahkeme, müdahalenin varlığına dair karar verdikten sonra söz konusu müdahalenin 8. maddenin 2. fıkrası uyarınca haklı ve meşru kabul edilip edilemeyeceğini değerlendirmiştir. Buna göre, mevcut yasa savcılık makamının veri toplama, kaydetme ve saklama yetkisini kullanma koşullarını ve kapsamını belirlememekte, hangi bilgilerin saklanacağı ve saklama yöntemi konularında açıklık getirmemektedir¹⁸². Mahkeme, müdahale için yeterli hukuksal temelin eksik olmasından ötürü mevcut olayda başvurucunun telefon görüşmelerinin dinlenmesi ve hakkında fişlik oluşturulmasının Sözleşme'nin 8. maddesini ihlal ettiğine karar vermiştir¹⁸³.

AİHM'in *Rotaru/Romanya* kararı kamusal nitelikteki verilerin sistematik olarak toplanıp kaydedilmesine ilişkindir¹⁸⁴. Mevcut olayda başvuru, Romanya gizli servisi tarafından hakkında 1937'deki savaş öncesinde tutulan aşırı sağcı, antisemitist ve paramiliter gruba üye olduğu yönündeki bilgilerin yanlış olduğu, bu yanlış nedeniyle uğradığı zararların karşılanması ve bilgilerin tutulduğu dosyanın silinmesi için dava açmıştır. Başvurucunun açmış olduğu bu davanın ardından

kararları da mevcuttur. Nitekim *Niemietz/Almanya* kararında Mahkeme, özel hayat kavramının dar yorumlanmaması gerektiğini vurgulamıştır. Mevcut olayda bir avukatın yürütülen ceza soruşturması nedeniyle bürosunun aranması söz konusudur. Davalı devlet, büronun mesleki yer olduğu, profesyonel faaliyetlere ilişkin olarak 8. maddenin güvence getirmediğini savunmuştur. Ancak Mahkemeye göre özel hayat kavramının tanımının yapılması mümkün ve gerekli değildir. Özel hayat kavramını sadece içerisinde insanın kişisel yaşamını kendi seçimine göre sürdürebileceği ve dış dünyayı tamamen dışarıda bırakabileceği dar bir alanla sınırlamak fazla sınırlayıcı olacaktır. Özel hayata saygı hakkı, bir dereceye kadar diğer insanlarla ilişki kurma ve geliştirme hakkını da kapsamaktadır. İnsanların çoğu iş dünyasında da dış dünya ile ilişkilerini geliştirme fırsatı bulmakta, bireylerin faaliyetlerinin mesleki yaşamının parçası olduğuna dair kesin bir ayırım yapması mümkün olamamaktadır. Özellikle serbest meslekle uğraşan insanlar açısından bireylerin hangi faaliyetlerinin mesleki alanının bir parçasını oluşturduğunu saptamak son derece güçtür. Bkz., *Niemietz/Almanya*, b.n. 13710/88, k.t., 16.11.1992, paras, 29,31,34,36. Kararın Türkçe çevirisi için bkz., Osman Doğru, **İnsan Hakları Avrupa İhtihatlari**, İstanbul, 1997.

¹⁸¹ *Amann/İsviçre*, para. 70.

¹⁸² *Amann/İsviçre*, para. 76.

¹⁸³ *Amann/İsviçre*, para. 80.

¹⁸⁴ *Rotaru/Romanya*, b.n. 28341/95, k.t. 04.05.2000.

Romanya İstihbarat Örgütü bu bilgilerin başvurucuya ait olmadığını, isim yanlışlığı ve ağır bir hatanın olduğunu başvurucuya bildirmiştir. Ancak başvurucunun tazminat istemi bu bildirimin üzerine açmış olduğu temyiz davasında reddedilmiştir.

Mahkeme, davalı devletin söz konusu bilgilerin başvurucunun açtığı davada kamuya sunulmuş olduğu ve dolayısıyla “özel hayat” kapsamında değerlendirilemeyeceği yönündeki savunmasını kabul etmemiş, kamusal bilgiler olsa dahi kişisel bilgilerin toplanması ve saklanması başlı başına 8. maddeye müdahale teşkil ettiğini belirtmiştir¹⁸⁵. Müdahalenin Sözleşme'nin 8. maddesinin 2. fıkrasına göre hukuka uygun ve meşru kabul edilebilmesine dair incelemesinde Mahkeme, ulusal mevzuatta kamu otoritelerine verilen yetkinin açıkça tanımlanmadığını, hangi verilerin kaydedileceği, hangi insanlara dair verilerin kaydedilebileceği ve toplanabileceği, hangi önlemlerin alınması gerektiği ve bunların prosedürüne dair açıklamaların yer almadığını belirtmiştir. Dolayısıyla Mahkeme, mevcut olayda 8. maddenin ihlal edildiğine karar vermiştir¹⁸⁶.

AİHM'in kişisel verileri AİHS'in 8. Maddesinde değerlendirdiği ve ilgili maddenin ihlal edildiğine yönelik bir başka kararı da Türkiye'ye yöneliktir. Buna göre Mahkeme, *Celalettin Canlı/Türkiye* davasında kişisel verilerin kamu makamları tarafından tutulmasında gerekli güvencelerin olmadığı, yasallık ilkesinin ihlal edildiği ve dolayısıyla AİHS'in 8. maddesinin ihlal edildiğine karar vermiştir¹⁸⁷. Mevcut olayda başvuru 2003 yılında yargılandığı bir davada polis tarafından hazırlanan ve başvurucunun geçmişte yargılandığını belirten raporun dava dosyasına girmesi ve basına yansması nedeniyle AİHS'in 8. maddesinin ihlal edildiğini belirtmiştir. Hükümet, raporun hazırlanmasının başvuranın AİHS'in 8. maddesi bağlamındaki haklarına müdahale olarak algılanması gerektiği hususunda söz konusu tarihte yürürlükte olan kanunlara uygun olduğunu belirtmiştir. Ayrıca, kamu

¹⁸⁵ *Rotaru/Romanya*, para. 43. Mahkeme, kararında kişisel verilerin tanımını yaparken *Amann* kararındaki gibi Avrupa Konseyinin 108 sayılı Sözleşmesi'ne atıfta bulunmuştur.

¹⁸⁶ *Rotaru/Romanya*, paras. 57-60.

¹⁸⁷ *Celallettin Canlı/Türkiye*, b.n. 22427/04, k.t. 18.11.2008.

güvenliği ve karmaşanın engellenmesi için demokratik bir toplumda gerekli olduğunu öne sürmüştür. Mahkeme, polis raporundaki bilgilerin başvuranın “özel hayatına” ilişkin veri mi, yoksa 8. maddenin kapsamı dışında kalan “kamusal bilgi” teşkil edip etmediğini daha önce önüne gelen özellikle *Amann/İsviçre* ve *Rotaru/Romanya* davalarını göz önünde tutmuştur. Ayrıca Mahkeme, oluşturmuş olduğu içtihadı göre özel hayat kavramını geniş yorumlayarak kişisel verinin bu kapsamda değerlendirilmesi gerektiğini 108 sayılı Sözleşme'nin amacının düzenlendiği 1. maddesi ile kişisel verinin tanımının yapıldığı 2. maddesine atıf yapmak suretiyle de temellendirmiştir. İtiraz edilen raporda başvurana, yasadışı örgütlere üyelikle “suçlanan”, “mahkum edilen” ya da “yargılanan” biri olarak değil, yalnızca “üye” olarak değinildiğini gözlemlemiştir. Başvuranın hiçbir zaman herhangi bir mahkeme tarafından yasadışı örgütlere üyelik suçuyla mahkum edilmediğini göz önüne alan AİHM, polis raporunda başvurana bu tür örgütlerin “üyesi” olarak değinmenin, saygınlığına zarar verebileceğini belirtmiştir. Bu bağlamda Mahkeme, AİHS 8. maddesinin kişinin saygınlığının korunması hakkının, özel hayatına saygı gösterilmesi hakkının bir parçası olarak yer aldığını yineleyerek polis raporunun saklanması ve dava dosyasına sokulmasının anılan maddeye göre başvuranın özel hayatına saygı hakkına müdahale teşkil ettiğini tespit etmiştir. Müdahalenin Sözleşme'nin 8. maddesinin 2. fıkrasına göre kanuna uygun kabul edilebilmesine dair yaptığı incelemede başvuruya konu raporda ortaya konan bilginin yanlış olduğunu, başvuranın beraatine ve cezai takibatın sona erdiği bilgilerini içermediğini, ayrıca başvuranın geçmişte itham edildiği ancak 1990'da temize çıktığına dair kararın 2003'te dava dosyasına sunulan rapora eklenmediğini belirtmiştir. Bu bağlamda AİHM, bu eksikliklerin Polis Yönetmeliği'nin tereddüte mahal bırakmayan şartlarına aykırı olduğu ve başvuranın AİHS'in 8. maddesi bağlamındaki haklarının korunması için hukukun sağladığı usuli teminatları ortadan kaldırdığından yola çıkarak AİHS'in 8. maddesinin ihlal edildiğine karar vermiştir.

Yukarıda AİHM'in verdiği kararlardan da görüleceği üzere kişisel verilerin kamu makamları tarafından toplanması ve kaydedilmesi, toplanan verilerin amacı

dışında kullanılması, kişisel verilere erişim hakkı konuları AİHS'in 8. maddesinde düzenlenen özel hayata ve aile hayatına saygı hakkı ile getirilen güvenceler kapsamında yorumlanmıştır. AİHM, başvuru konusu olayın 8. maddenin ilk fıkrasının koruma kapsamında olduğuna dair tespitte bulunduktan sonra yapılan işlemin müdahale oluşturup oluşturmadığını değerlendirecektir. Mevcut olayda müdahalenin varlığının kabulü ile birlikte Mahkeme, bunun Sözleşme'nin 8. maddesinin 2. fıkrasına göre meşru olup olmadığını incelerken de bu konudaki içtihatını genişletmiştir. Buna göre müdahalenin meşru kabul edilebilmesi için 8. maddenin 2. fıkrasında sınırlı sayıda belirtilmiş amaçlardan biri veya birkaçına yönelik, yasada öngörülmüş ve aynı zamanda demokratik toplum için gerekli ve öngörülen amaç ile orantılı olması durumlarını değerlendirmiştir. Belirtmemiz gerekir ki AİHM, konuya ilişkin pek çok kararında 8. maddenin ilk fıkrasına yönelik bir müdahaleyi, 2. fıkra uyarınca meşru kabul etmiştir¹⁸⁸. Mahkeme meşruluk değerlendirmesinde ayrıca devletin veri toplaması sırasında bireylere ulusal hukukunda yeterli güvenceleri sağlaması gerektiğini vurgulamıştır. Bunun gibi müdahalenin yasaya dayanması halinde de bu yasanın açık ve net olması gerekmektedir.

AİHM'in kişisel verilerin korunmasını 8. madde kapsamında değerlendirmesi oldukça önemlidir ancak bu değerlendirme belirli açılardan sınırlı kalmaktadır. Öncelikle kişisel verilerin korunması hukuku ile kişinin bilinmesini veya bilinebilmesini sağlayan her türden verilerin işlenmesini kapsamakla birlikte AİHM içtihadında “özel hayat” dışında görülen birtakım veriler sözleşmenin 8. maddesindeki güvenceden yararlanamayacaktır. Ayrıca, AİHS'in 8. maddesinin kimler tarafından gerçekleştirilen müdahalelere karşı güvence getirdiğinin saptanması da verilerin korunmasına getiren yorumun sınırlılığını anlayabilmek açısından önemlidir. İlgili madde ile taraf devletlerin organlarınca toplanan ve işlenen verilere yönelik bir koruma getirilmektedir. Ancak özel kişilerce veya özel

¹⁸⁸ Bygrave, “Data Protection Pursuant to the right of Privacy in the Human Right Treaties”, s. 270.

sektörce verilerin işlenmesi durumunda korumanın kapsamı cevapsız kalmaktadır¹⁸⁹.

Son olarak diyebiliriz ki konu, her bir mevcut olayın şartlarına göre ayrı olarak ele alındığından kişisel verilerin korunmasına ilişkin genel kuralların geliştirilmesinde yetersiz kalmaktadır. Yine de konuya ilişkin değerlendirmelerin içtihat yoluyla oluşturulması kişisel verilerin denetimsiz veya yeni veri işleme teknikleri ile işlenmesinin kişinin özgürlüğü ve demokratik toplum üzerinde oluşturabileceği potansiyel tehditlere karşı AİHM'in tutumunu yansıtması açısından önemlidir. Ayrıca unutulmamalıdır ki, AİHS taraf devleti olup da AB üyesi olmayan, 108 sayılı Sözleşme'yi de kabul etmemiş devletler açısından AİHM içtihadı oldukça önemlidir. Ulusal mevzuatlarında kişisel verilerin korunmasına ilişkin düzenlemelere yer veren devletlerin de bu düzenlemelerinin AİHS ile uyumlu olması gerekmektedir¹⁹⁰.

4. Avrupa Birliği'nde Kişisel Verilerin Korunması

a. Genel Olarak

İkinci Dünya Savaşı sonrası yıkıma uğrayan Avrupa'da barışın sağlanması ve Avrupa devletleri arasında ekonomik işbirliğinin kurulması amacıyla siyasi bir birliğin sağlanması düşüncesinin en ileri biçimi olan Avrupa Birliği, kendine özgü ekonomik ve siyasi bir ortaklıktır. Birlik malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımını temel düşünce olarak ve bunları kapsayan bir ortak

¹⁸⁹ AİHS 34. maddesine göre başvurular Sözleşme'yi ihlal ettiği ileri sürülen devlete karşı yapılır. Bu nedenle birey aleyhine yapılan başvurular, kişi yönünden yetkisizlik nedeniyle reddedilir. Ancak, bazı durumlarda Sözleşme ile koruma altına alınan haklara karşı özel kişi ya da kurumlardan gelecek müdahalelerden devletin sorumlu tutulması devletin AİHS 1. maddesi ile üstlendiği “pozitif yükümlülüğün” bir sonucudur. Örneğin, X ve Y/Hollanda kararında Mahkeme, “(Devletin) buradaki yükümlülükleri, bireylerin arasındaki ilişik alanında da özel hayat saygıyı koruyacak önlemlerin kabulünü de içermektedir” diye ifade etmiştir. Bkz., X ve Y/Hollanda, b.n. 8978/73, k.t. 26.04.1985, para. 23. Ayrıca bkz., Gölcüklü-Gözübüyük, **a.g.e.**, s. 45. Avrupa Konseyi Parlamenterler Meclisi 1970 yılında kitle iletişim araçları ve insan haklarına dair beyanlarını içeren 428(1970) sayılı kararını yayınlamıştır ve burada AİHS'in 8. maddesinin bireylere yalnızca kamu otoritelerine karşı değil özel kişiler ve özel sektöre karşı da güvence sağlaması gerektiğine değinmiştir. Ayrıntılı bilgi için bkz., **A.g.m.**, s. 258.

¹⁹⁰ **A.g.m.**, s. 248-249.

pazar geliştirilmesi üzerine kurulmuştur¹⁹¹. Ortak pazarın geliştirilmesi sürecinde üye devletler arası veri talepleri ve veri transferleri artmıştır. Öyle ki AB'nin dört temel hedefinin yerine getirilmesinde kişisel verilerin toplanması ve işlenmesi bir zorunluluk arz etmektedir. Avrupa'nın bütünleşmesi süreci AB üyesi devletlerin arasındaki kişisel veri akışını arttırmanın yanında bu türden verilere yönelik taleplerin de yoğunlaşmasına etken olmuştur¹⁹². Bu nedenden ötürü Avrupa Birliği, gelişen teknoloji ile beraber AB ortak pazarının gereklerini dikkate alarak serbest veri akışını temel haklara uygun işletmek amacıyla kişisel verilerin korunmasına ilişkin kuralları yürürlüğe koymuştur.

Kişisel verilerin korunmasına ilişkin düzenlemeye gidilen süreçte özellikle 1 Aralık 2009'da Lizbon Antlaşması'nın onaylanması veri koruma mevzuatı ile üye devletlerin ortak pazar hedefinin sağlanmasının ötesinde bir anlam kazanmıştır. Lizbon Antlaşması ile AB'nin İşleyişine İlişkin Sözleşme (Treaty on the Functioning of the EU) ile AB Antlaşması (Treaty on EU) birleştirilmiştir. Bunlardan AB'nin İşleyişine İlişkin Sözleşme'nin 16. maddesi ile verilerin korunması için yeni bir hukuksal temel sunulmuştur. İlgili madde hükmü uyarınca artık AB'nin eski üçüncü sütunu olarak nitelendirilen güvenlik ve adli işbirliği ile eski ikinci sütunu olan ortak dış politika ve güvenlik politikasına ilişkin alanlar da dahil olmak üzere özel ve kamu sektöründeki bütün veri işlemlerinde Direktif hükümlerine uygun hareket etmek gerekecektir¹⁹³. Bunun yanı sıra kişisel verilerin korunmasının temel insan hakkı ve özgürlüğü olarak tanınması da önemlidir. Bunlardan ilki, aşağıda ilgili bölümde de inceleneceği üzere, kişisel verilerin korunmasını ayrı bir hüküm altında düzenleyen

¹⁹¹ Avrupa'yı bütünleştirme temelleri ilk olarak 1951 yılında Avrupa Kömür ve Çelik Topluluğu'nu (AKÇT) kuran Paris Antlaşması ile atılmıştır. Bunu daha sonra 1957 yılında Avrupa Ekonomik Topluluğu'nu (AET) ve Avrupa Atom Enerji Topluluğu'nu (Euratom) kuran Roma Antlaşması ve 1986 yılında imzalanan Avrupa Tek Senedi izlemiştir. Bütünleşme sürecindeki diğer aşamaları ise AET'nin Avrupa Birliği olması yolundaki son adımı olan Maastricht, Amsterdam, Nice ve Lizbon Antlaşmaları oluşturmaktadır.

¹⁹² Paul Schwartz, “*European Data Protection Law and Restrictions on International Data Flows*”, **Iowa Law Review**, S. 80, 1994-1995, s. 485. (Bundan böyle “**European Data Protection Laws and Restrictions on International Data Flows**” olarak anılacaktır).

¹⁹³ Article 29 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, 01.12.2009, s. 5.

Avrupa Birliği Temel Haklar Şartı'nın Lizbon Antlaşması ile hukuksal bağlayıcılığa kavuşmasıdır. Bunun yanı sıra AB Antlaşması'nın 6. maddesinin 2. fıkrasında Birliğin Avrupa İnsan Hakları Sözleşmesi'ne katılımı sağlanmış ve yine aynı maddenin 3. fıkrasında Birlik üye devletleri demokratik bir toplumun temellerini oluşturan insan hakları ve temel özgürlüklere bağlı kalacaklarını taahhüt etmişlerdir. Nitekim bu yeni düzenlemeler Avrupa vatandaşlarının temel hak ve özgürlüklerine saygılı davranılmasını ve kişisel verilerin korunmasına ilişkin düzenlemenin getirilmesini zorunlu kılmıştır¹⁹⁴.

AB düzeyinde kişisel verilerin korunmasına ilişkin kabul edilen çeşitli metinler içerisinde öncelikle AB Temel Haklar Şartı'ndaki ve AB 95/46/AT sayılı Veri Koruma Direktifi'ndeki düzenlemelere değineceğiz.

b. Avrupa Birliği Temel Haklar Şartı

AB hukuk sisteminde kişisel verilerin korunmasına ilişkin metinlerden biri AB Temel Haklar Şartı'dır. Şart, 7 Aralık 2000 tarihinde imzalanmış ve AB tarihinde ilk kez Avrupa vatandaşlarının ve AB'de yaşayan bütün insanların bireysel, siyasal ve ekonomik hakları tek bir metinde toplanmıştır¹⁹⁵. AB Temel Haklar Şartı, 1 Aralık 2009 tarihinde Lizbon Antlaşması'nın yürürlüğe girmesiyle AB hukukunun bir

¹⁹⁴ Simiris Spitos, "From the Market to the Polis: The EU Directive on Protection of Personal Data", **Iowa Law Review**, C.80, 1994, s. 448. Esasen AB Antlaşması'nda insan haklarının korunmasına yapılan atıf, Avrupa Adalet Divanı'nın topluluk hukukunda insan haklarının yeri hakkında geliştirdiği içtihat hukukuna resmi bir karakter kazandırmaktadır. AAD, ERT kararında konuyu şu şekilde değerlendirmiştir; "Temel haklar, Divan'ın saygı gösterilmesini temin ettiği hukukun genel prensiplerinin dahili bir unsurunu oluşturur. Bu prensiplere riayet edilmesi için Divan, üye devletlerin ortak anayasal geleneklerinden ve üye devletlerin katıldıkları ya da imzaladıkları insan haklarının korunması hakkındaki Uluslararası antlaşmalarca sağlanan kılavuz ilkelerden ilham alacaktır ki bu meyanda AİHS'in özel bir belirleyiciliği vardır." Görüleceği üzere AB mevzuatında kişisel verilerin korunmasına ilişkin düzenlemelere gidilmesi yalnızca gelişen teknoloji, küreselleşme ve ulusal düzenlemelerde konuya ilişkin farklı koruma eşiklerinin ortak pazarın oluşturulmasına dair oluşturacağı engeller olmasının yanında-ancak bununla sınırlandırılmaksızın- AB'nin temel haklara saygı yükümlülüğüdür. Karar için bkz., Case C-260/89 ERT (1991) ECR I-2925. AAD'nin ilgili kararlarına dair değerlendirme için bkz., Gür, **a.g.e.**, s.14 vd.

¹⁹⁵ AB Temel Haklar Şartı'nın Türkçe metni için bkz., <http://ekutup.dpt.gov.tr/ab/hukuk/temelhak.pdf>. Şart'ın kabulü ile AB'nin meşruiyeti güçlenmekte, temel haklar Birlik vatandaşları için "görünür kılınmakta" ve temel hak korumasının düzeyi yükseltilmektedir. Bkz., Yüksel Metin, "Avrupa Birliği Temel Haklar Şartı", **Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi**, C.57, S.4, s. 36.

parçası olarak kabul edilmiştir¹⁹⁶.

AB Temel Hakları Şartı'nda haklar “saygınlık”, “özgürlükler”, “eşitlik”, “dayanışma”, “vatandaşlık hakları”, “adalet” adları altında altı ayrı bölümde incelenmiştir. Klasik özgürlük haklarından olan ve tarihsel süreç içerisinde kişisel verilerin korunmasına dair güvenceleri barındıran “özel hayatın gizliliğine saygı hakkı” 7. maddede düzenlenmiştir. Madde hükmüne göre; “*herkes özel ve aile yaşamına, evine ve iletişimine saygı gösterilmesini isteme hakkına sahiptir*”. Görüldüğü gibi buradaki düzenleme özel hayatın gizliliği hakkındaki geleneksel düzenleme şekline uygundur. Şart'ta temel haklar kataloğu hazırlanırken AİHS m. 8/f.1 hükmü temel alınmıştır¹⁹⁷. Şart'ı hazırlayanlar AİHS'in 8. maddesini temel almak ile birlikte, gelişen teknolojiye uyum ve modern bir temel haklar kataloğu hazırlama hedeflerinin doğrultusunda terminolojik değişikliğe gitmişlerdir. AİHS'in 8. maddesinde “haberleşme” deyimini yerine “iletişim” tercih edilmiş ve bu şekliyle maddenin yeni gelişmeler sonucunda ortaya çıkan yeni araçları da kapsamı sağlanmıştır¹⁹⁸. Metin hazırlanırken modern bir temel haklar kataloğu olması gerekliliğinden yola çıkılmıştır. Nitekim Şartı hazırlayanlar iletişim alanındaki hızlı gelişmelerden ve konunun öneminden ötürü kişisel verilerin korunması hakkını ayrı bir hüküm altında düzenlemişlerdir.

AB Temel Haklar Şartı'nın “*Kişisel Verilerin Korunması*” kenar başlıklı 8. maddesine göre; “(1)*Herkes, kendisini ilgilendiren kişisel verilerin 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.*

¹⁹⁶ AB Antlaşması m. 6/f.1. Anılan maddeye göre AB Temel Haklar Şartı, AB üyesi devletleri için Birlik antlaşmaları ile aynı hukuki bağlayıcılığa sahiptir. Ancak belirtmeliyiz ki İngiltere ve Polonya imzaladıkları bir protokolle Temel Haklar Şartı'na sınırlı bir şekilde katılmışlardır. Protokol için bkz., <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:0156:0157:EN:PDF>.

¹⁹⁷ AB Temel Haklar Şartı 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. Nitekim giriş bölümünde Şart'ın, “*anayasal teamüller, üye ülkelere ortak uluslararası yükümlülükler, AİHS ve Avrupa İnsan Hakları Mahkemesi (AİHM)'nin içtihat hukukuna saygı gösterdiği*” vurgulanmaktadır. Bunların içerisinde özellikle AİHS temel alınmış ve Şart'ın yorumlanmasında AİHS'e özel önem verilmiştir. Bkz., Metin, **a.g.m.**, s. 47

¹⁹⁸ Küzeci, **a.g.e.**, s. 160.

(3) Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir”.

Belirtilen hüküm temelini Avrupa Toplulukları Antlaşması'nın 286. maddesi, AB Direktifi, 108 sayılı Sözleşme ve AİHS'in 8. maddesinden almaktadır. Birlik bünyesinde kişisel verilerin korunması hakkı Direktif'te belirtilen koşullar çerçevesinde kullanılacağı gibi, Şart'ın 52. maddesinde düzenlenen sınırlama sebeplerine uygun olarak hakkın kullanılması kısıtlanabilir¹⁹⁹.

Madde hükmü ile herkesin kişisel verilerin korunması hakkına sahip olduğu düzenlenmiştir. Ancak belirtmemiz gerekir ki, kişisel verilerin korunması hukukunun temel mantığı ve AB Temel Haklar Şartı'na kaynak teşkil eden 95/46/AT sayılı Direktif göz önünde bulundurulduğunda koruma alanı yalnızca gerçek kişilere yöneliktir. Madde hükmündeki “herkes” deyimini tüzel kişileri koruma kapsamına almamaktadır²⁰⁰.

Kişisel verilerin korunması hakkı tarihsel süreç içerisinde özel hayatın gizliliği hakkı kapsamında değerlendirilmiştir. Ancak, gelişen teknoloji ve yeni gelişmeler verilerin korunmasının özel hayatın gizliliği ile açıklanamayacak bazı konuların ortaya çıkmasına sebebiyet vermiştir. Ayrıca AİHM'in özel hayatın gizliliği hakkına dayanarak oluşturduğu içtihatlarında tam anlamıyla cevaplayamadığı bazı hukuki sorunlar AB Temel Haklar Şartı'nda kişisel verilerin bağımsız bir hak olarak tanınmasıyla çözülmektedir²⁰¹. Şartın hukuki anlamda bağlayıcılık kazanmasıyla Birlik üyesi devletlerin vatandaşları Şartın hükümlerini dava konusu

¹⁹⁹ **A.g.e.**, s. 161. Ayrıca burada AİHS'in 8. maddesinde yer alan sınırlama sebepleri ile Şart'ın 52. maddesinde yer alan sınırlama sebeplerinin karşılaştırmasını yapabiliriz. Şart'ın 52. maddesinde yer alan sınırlama sebepleri AİHS'in 8. maddesinin 2. fıkrasında yer alan sebepler ile benzer nitelik taşımakla birlikte bazı noktalarda farklılıklar içermektedir. Örneğin, 52. maddeye göre kişisel verilerin korunması hakkına Birlik tarafından tanınan genel fayda amaçları doğrultusunda sınırlandırma getirilebilmektedir. Görüleceği üzere bu sınırlama sebebi şeffaflık ilkesine ağırlık verilmesinin önünü açmakta ve kişisel verilerin korunmasına dair AİHS'e nazaran daha az koruyucu bir şekilde yorumlanabilmektedir. Öte yandan yine ilgili maddede temel hak ve özgürlüklerin özünün korunması gerektiğine de yer verilerek korumanın dengesi sağlanmaya çalışılmıştır.

²⁰⁰ Şimşek, **a.g.e.**, s. 73.

²⁰¹ Küzeci, **a.g.e.**, s. 162.

yapabileceklerdir. Ayrıca Birlik üyesi devletlerin yanı sıra AB kurumları ve örgütleri de Şart hükümlerine uygun hareket etmekle yükümlüdürler. Şart'ın en önemli etkisi AB bünyesinde kişisel verilerin korunmasına ortak pazarın inşaaından ileri bir anlamı olduğunu ve 95/46/AT sayılı Kişisel Verilerin Korunması Direktifi'nin konuya ilişkin insan hakları yaklaşımını vurgulamasıdır.

c. 95/46/AT Sayılı Kişisel Verilerin Korunması Direktifi

(1) Amaç

AB'de kişisel verilerin korunmasına ilişkin en önemli metinlerden biri; “Kişisel verilerin işlenmesi ve bu tür verilerin serbest dolaşımına dair bireylerin korunması hakkındaki 95/46/AT sayı ve 24 Ekim 1995 tarihli Avrupa Birliği Konseyi ve Avrupa Parlamentosu Direktifi”dir²⁰². Metin, AB düzeyinde kişisel verilerin korunmasına ilişkin genel çerçeveyi belirlemektedir²⁰³. Direktif, kabul edildiği tarihten itibaren Birlik üyesi devletlerin sınırlarını aşan bir etki yaratmıştır.

Çalışmamızın ilgili bölümünde belirttiğimiz gibi, Avrupa'da kişisel verilerin korunmasına ilişkin ilk düzenlemeler 1970'li yıllardan itibaren yapılmaya başlandı. 1990'lı yıllardan itibaren de kişilerin, hizmetlerin, sermayenin ve malların serbestçe dolaştığı bir bölge olma yolunda hızla ilerleyen Avrupa açısından bölgedeki farklı koruma seviyelerinin ortak pazarın tamamlanması sürecine engel olacağından bahisle kişisel verilerin korunmasına ilişkin düzenlemelerin uyumlaştırılmasına gereksinim duyulmuştur.

²⁰²Bu dipnot bağlamında kişisel verilerin korunmasına yönelik diğer çalışmalara değinmek isteriz. AB'deki konuya ilişkin düzenlemelerin temelini oluşturan AB Direktif'ini desteklemek amacıyla eksik kalan alanlarda Avrupa Parlamentosu ve Konseyi 1997 yılında “Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi Ve Mahremiyetin Korunması Direktifi”ni yürürlüğe koymuştur. Daha sonra AB bu Direktifi tamamlayan 2002/58 Sayılı “Özel Hayatın Korunması ve Elektronik İletişim Direktifi”ni yeni bir veri saklama hukuku olarak ortaya koymuştur. Ayrıca 2006/24 sayılı “Kamu Elektronik Haberleşme Hizmetlerinin Sağlanması Direktif”i kişisel verilerin korunmasındaki diğer bir düzenlemedir.

²⁰³Üye devletler kişinin özel hayatının korunması ile serbest veri akışı arasındaki dengenin korunduğu sürece Direktif'i daha geniş yorumlayabilirler. Ayrıca üye devletler ulusal düzenlemelerinde Direktif'in uygulama kapsamını, Topluluk hukukuna dair diğer hükümlerin engellememesi şartıyla, genişletebilirler. Bkz., Bodil Lindqvist, C-101/01, 06.11.2003, paras. 97, 98, 99.

Konuya ilişkin uyumlaştırma çabaları bir anlamda 108 sayılı Sözleşme'nin etkilerinde yansımaları bulur. 108 sayılı Sözleşme'nin imzacılarının çoğu aynı zamanda Avrupa Birliği üyesidir. Ayrıca ilgili sözleşmenin 4. maddesine göre imzacı devletlerin iç hukuklarını sözleşme ile uyumlu hale getirme yükümlülükleri bulunmaktadır. Ancak, üye devletlerin ulusal mevzuatlarında konuya ilişkin farklılıklar mevcuttur. Transfer edilen veriler, başka bir devletin hukuk düzenine tabi olmaktadır. Verilerin korumasına ilişkin ilgili devlette bir veri koruması yasası yoksa koruma sağlanamayacaktır. Birey, kişisel verilerin işlenmesinde mağduriyete uğradığı takdirde kendi ülkesinin veri koruması yasalarından doğan haklarını yurtdışındaki yabancı işlem yerine karşı ileri süremeyecektir. Temel hakların kullanılması bu anlamda kısıtlamaya uğrayacaktır. Ayrıca farklılıklar rekabetin sağlıklı yürütmesine de engeldir. Nitekim birçok şirket, koruma düzeyi yüksek olmayan üye devletlere veri toplama ve işleme sistemlerini kaydırabilmekteydi²⁰⁴. Bu farklılıkların giderilmesi ve kişisel verilerin korunması konusunda AB bünyesinde uyumlu bir mekanizmanın sağlanmasına cevaben Direktif kabul edilmiştir. Buna göre Direktif'in birincil amacı, üye devletler arasındaki farklılıkların ortadan kaldırılması ve ortak pazarın sağlanmasıdır²⁰⁵. Direktifin gerekçesine göre de amaç, üye devletler arasında kişisel verilerin serbest trafiğinin sağlanmasıdır. Gerçek kişilerin haklarının ve özellikle özel hayatın korunması gibi sebeplerle veri trafiğinin engellenmesinin önüne geçilmesi gerekmektedir. Üye devletlerin düzenlemelerindeki farklılık ortak pazarın oluşumu ve işleyişi açısından engel oluşturmaktadır²⁰⁶.

²⁰⁴ Başalp, **a.g.e.**, s. 29.

²⁰⁵ Birlik bazında kişisel verilerin korunmasının iç hukukun uyumlaştırılması düzleminde yetki sorunu ortak pazarın oluşturulması ve yürütülmesi doğrultusunda çözülmüştür. Zira, AT Antlaşması'nın 94. maddesine göre AT, ortak pazarın oluşturulması ve yürütülmesi ekseninde üye devletlerin iç hukuklarının uyumlu hale getirilmesi gereğini tespit ettiğinde harekete geçecektir. Direktif, bu temelde yürürlüğe konulmuştur. Bkz., Başalp, **a.g.e.**, s. 30. Bununla birlikte AAD, *Lindqvist* kararında AT Antlaşması'nın 94. maddesi temelinde ihdas edilen bir yasama tedbirinin genel hedefi ile tedbirin uygulanmasında takip edilen somut yollar arasında ayrıma gitmiş, Direktif tarafından düzenlenmek istenen her durum için ortak pazar ile gerçek bağlantı kurulması şartını reddetmiştir. Bkz., Gür, **a.g.e.**, s. 50.

²⁰⁶ AB Direktifi, 7 numaralı gerekçe.

Görüleceği üzere Direktif'in amacı, 1. maddede de açıkça belirtildiği üzere, gerçek kişilerin haklarının korunması ve özellikle özel hayatın korunması gibi sebeplerle veri trafiğinin engellenmesinin önüne geçilmesidir. Bu iki hedef birbiri ile çelişkili görünse de birbirini tamamlamaktadırlar. *Başalp*'a göre de Direktif ile güdülen amaç yalnızca verilerin serbest trafiğinin sağlanması olsaydı veri korumasını iç hukuklarında düzenlemiş üye devletlere veri korumasına son verme talebi yöneltilebilirdi. Ancak, AB yasa koyucusu topluluk hukukuna ortak düzenleme getirirken tercihini kişilik hakkının korunmasından yana kullanmıştır²⁰⁷. Ayrıca üye devletlere veri korumasına son verme talebi gibi bir düzenlemenin varlığı halinde temel insan hakkı olan kişisel verilerin korunması Birlik bünyesinde güvence altına alınmamış olacaktır. Olası durum AB Antlaşması'nın üye devletlere insan hakları ve temel özgürlüklere bağlı olma ve AIHS'e uyma yükümlülüğünü içeren 6. maddesinin 2. fıkrası ile AB Temel Haklar Şartı'na aykırılık teşkil edecektir.

Üye devletler Direktifi iç hukuklarına aktarırken veri koruma düzeyini Direktif ile öngörülen standardın altında belirleyemeyeceklerdir. Ancak, üye devletler ulusal mevzuatlarında bu koruma düzeyinin üzerinde düzenleme getirilebilecektir²⁰⁸. Direktif ile düzenlemelere ilişkin hukuki çerçeve oluşturulmuştur. Üye devletlerin düzenlemelerinin aynı değil, yeterli veri korumasını sağlamaları şartıyla eşit ağırlıkta olması aranmaktadır²⁰⁹. Direktif ile kişisel verilerin korunmasına dair şartlar düzenlenerek olası saldırılar öncesi sistemli bir koruma sağlanmaya çalışılmıştır. Yine bu önleyici sistemin tam olarak uygulanabilmesi için üye devletlerin tamamında kişisel verilerin korunmasını güvence altına alan kuralların uygulanmasını sağlayacak birimlerin bulunması gerektiğine vurgu yapılmıştır²¹⁰.

²⁰⁷ Başalp, **a.g.e.**, s. 31.

²⁰⁸ AB Direktifi, 8 numaralı gerekçe.

²⁰⁹ AB Direktifi, 10 numaralı gerekçe.

²¹⁰ Başalp, **a.g.e.**, s. 31, Aynı yönde görüş için bkz., Özdemir, **a.g.e.**, s. 29.

(2) Uygulama Alanı ve Kapsamı

Direktif'in uygulama alanı 3. maddede düzenlenmiştir. Buna göre Direktif, kişisel verilerin tamamen veya kısmen otomatik işleme tabi tutulması ile bir dosya içerisinde kaydedilen veya kaydedilebilecek verilerin otomatik olmayan veri işleme tabi tutulmasında geçerlidir. Kişisel verilerin otomasyon işlemine tabi tutulması bu verilerin otomasyon sistemlerinin kullanıldığı yöntemlerle işlenmesi halidir. Direktifin koruma alanının kısmen otomatik işlemleri de kapsamı uygulama açısından önemlidir. Otomatik bir indeksin elden tutulan dosyalarının organize edilmesinde kullanıldığı gibi uygulamada otomasyon kısmen gerçekleştirilebilmektedir²¹¹. Ancak, kişisel verilerin otomatik işleme tabi tutularak işlenmesi ile elden işlenmesi açısından Direktif'in uygulama alanı açısından bir farka dikkat çekmek isteriz. Otomatik işleme tabi tutulan kişisel veriler açısından dosyalama sistemi oluşturulsun veya oluşturulmasın Direktif uygulanacaktır. Ancak, kişisel verilerin otomatik araçlarla işlenmesi dahi Direktif'in koruma kapsamında kabul edilebilmesi için bu verilerin ulaşımına kolaylık sağlayacak şekilde ve bireylere ilişkin özel kriterlere göre yapılandırılan bir dosyalama sisteminin parçasını oluşturması veya bir dosyalama sisteminin bir bölümünü oluşturması amacıyla işlenmesi gerekmektedir²¹².

Günümüzde kişisel verilerin büyük oranda otomatik yollar ile işlendiği göz önüne alındığında Direktif'in veri işleme usulünden bağımsız olarak neredeyse bütün kişisel verilerin korunmasını sağladığı çıkarılabilir²¹³. Direktif yöntemine bakılmaksızın kişisel verilerin tüm işleme faaliyetlerini kapsamakta; belirli bir sektör ya da kullanım alanı ile sınırlandırılmamaktadır²¹⁴.

Genel kural Direktif'in her kişisel verinin işlenmesinde uygulanması olmak ile birlikte bunun istisnaları da mevcuttur. Bunlardan ilki, Direktif'in 3. maddesinin 2.

²¹¹ Başalp, **a.g.e.**, s. 32

²¹² AB Direktifi, 15 ve 27 numaralı gerekçeler.

²¹³ Küzeci, **a.g.e.**, s. 166.

²¹⁴ Gür, **a.g.e.**, s. 27; Şimşek, **a.g.e.**, s. 43.

fıkrasında düzenlenmiştir. Buna göre kamu güvenliği, savunma, devlet güvenliği ve ceza hukuku alanında devletlerin faaliyetleri Direktif hükümlerinin uygulama alanı dışında kalmaktadır²¹⁵.

Direktif hükümlerinin uygulanmasına ilişkin diğer bir istisna ise gerçek kişilerce tamamen kişisel ya da ailevi etkinlikler çerçevesinde yapılan veri işlemleridir. Örneğin, tamamen kişisel amaçlar ile tutulan adres defteri Direktifin uygulama alanı dışındadır. Direktifin uygulama alanına getirilen bu istisna günlük yaşamın bir parçası haline gelen sosyal ağlar üzerinde yer alan verilerin “kişisel ya da ailevi etkinlikler” olarak değerlendirilip değerlendirilemeyeceği sorusunu gündeme getirir. 29. Madde Veri Çalışma Grubu'nun sosyal ağlarda verilerin paylaşılması ile ilgili görüşü burada önemlidir. Buna göre sosyal ağ hizmetlerinden faydalanan kullanıcılar bir şirket ya da kurum adına hareket edebilmekte, ekonomik

²¹⁵ Burada konunun daha iyi anlaşılması için Lizbon Antlaşması'nın yürürlüğe girmesinden önceki AB'nin kurumsal yapısına değinmemiz gerekir. AB'nin eski kurumsal yapısı topluluk hukukunun çekirdeğini oluşturan “Avrupa Topluluğu”, “Ortak Dışişleri ve Güvenlik Politikası” ve “Güvenlik ve Adalet İşbirliği” adı altına ve her birine “sütun” adı verilen görev alanlarından oluşmaktaydı. Eski kurumsal yapı bünyesinde Direktif, birinci sütun ile ilgili konularda uygulanırken ikinci ve üçüncü sütunların alanlarında uygulanmıyordu. İlgili alanlarda kişisel verilerin korunması Europol ve Schengen Antlaşmaları veya Birlik üyesi devletlerin aralarında imzaladıkları Prüm Antlaşması gibi belgelerle sağlanmaktaydı. Özellikle üçüncü sütun alanındaki düzenlemeler farklı durumlara uygulanacak karmaşık koruma rejimlerinden oluşmaktaydı. Bu rejimlerdeki kimi farklılıklar temellerini korunan alanların özgünlüklerinden bulmakta, diğerleri ise farklı hukuki geçmişlerden kaynaklanmaktadır. Bununla birlikte AB Konsey'i Direktifin üçüncü sütuna uygulanabilmesi için karar yayınlamıştı. Bu karar üçüncü sütun alanında kişisel verilerin korunmasına ilişkin genel bir çerçevenin belirlenebilmesi açısından ilk önemli adım olarak değerlendirilebilir. Karar için bkz., **Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters**, OJ L 350, 30.12.2008. Ancak Lizbon Antlaşması'nın yürürlüğe girmesi ile birlikte AB'nin sütun yapısı ilga edilmiştir. Birliğin yeni kurumsal yapısıyla birlikte kişisel verilerin korunmasına dair düzenlemeler eski birinci ve üçüncü sütun alanlarını da kapsayacaktır. Bkz., European Parliament's Committee on Civil Liberties, **Justice and Home Affairs Towards a New EU Legal Framework for Data Protection and Privacy Brussels**, 2011, www.ceps.eu/ceps/dld/6351/pdf. Sütun sisteminin ilgası ile AB Antlaşması'nın 16. maddesine göre güvenlik ve adalet işbirliği alanında düzenleme yapma yetkisi AB Konseyi ve AB Parlamentosu'ndadır. Hustnix'e göre, Lizbon Antlaşması'nın yürürlüğe girmesi ve sütun yapısının ilga edilmesi ile Direktif hükümleri güvenlik ve adli işbirliği konularında doğrudan uygulanabilirlik kazanmayacaklardır. Bunun için Direktif hükümlerinde değişiklik gerekmektedir. Bkz., Peter Hustnix, “Data Protection in the Light of the Lisbon Treaty and the consequences for Present Regulation”, **11Th Conference on Data Protection and Data Security-DuD**, Berlin, 2009, (Çevrimiçi) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2009/09-06-08_Berlin_DP_Lisbon_Treaty_EN.pdf, 01.05.2013. Nitekim 25 Ocak 2012 tarihinde AB bünyesinde kişisel verilerin korunmasına ilişkin yeni bir düzenleme paketi Avrupa Konseyi ve Parlamentosunun onayına sunulmuştur.

veya siyasal hedefler taşıdığı durumlar söz konusu olabilmektedir. Diyebiliriz ki, sosyal ağ kullanıcılarının bazı etkinlikleri kişisel veya ailevi nitelikte değildir. Sosyal ağlardaki bu tür kişisel veya ailevi nitelikte olmayan etkinlikler de Direktif hükümleri uygulanacaktır²¹⁶.

Direktif'in koruma kapsamı gerçek kişiler hakkında tutulan verilerdir. Kural olarak tüzel kişiler hakkında tutulan veriler koruma kapsamında değildir²¹⁷. Ancak üye devletler Direktif'i iç hukuklarına aktarırken yapacakları düzenlemelerinde tüzel kişileri de verilerin korunması kapsamına dahil edebilirler. Ayrıca tüzel kişilere ait veriler ile bir gerçek kişiye ulaşılabilmesi mümkün ise uygulama kapsamına dahil edilebilir²¹⁸. Yine kişisel verilerin 2. madde ile bir gerçek kişi hakkındaki olabilecek ve onu belirlenebilir kılacak her türlü bilgi olarak tanımlanmasından yola çıkarak diyebiliriz ki, kişinin kimliğinin belirlenemez olduğu anonim veriler uygulama kapsamında yer almayacaktır²¹⁹.

Avrupa Adalet Divanının geliştirdiği içtihat hukukunda Direktif'in uygulama alanının sınırlarının belirlenmesine dair kararları mevcuttur. Bu bağlamda *Österreichischer Rundfunk* ve *Lindqvist* kararları üzerinde kısaca durmak gerekir²²⁰. *Österreichischer Rundfunk* kararı; Avusturya kamusal yayın organı olan Österreichischer Rundfunk organizasyonunun çalışan ve emeklilerin isimleri ve aldıkları ücretlerine ilişkin bilgileri Ulusal Muhasebe Kurumu'na, Parlamento'ya sunacağı yıllık raporda kullanmak üzere iletip iletemeyeceğine ilişkindir. Buna göre sorun, Direktif'in mevcut olayda uygulanıp uygulanamayacağı, uygulanabilir olması halinde belirli kamu organlarının ödeme yapılan şahısların isimleri dahil olmak üzere kişisel verileri ifşa etmesini öngören ulusal mevzuatı Direktif'in yasaklayıp

²¹⁶ Article 29 Data Protection Working Party, **Opinion 5/2009 on online social networking**, 01189/09/EN WP 163, 12.06.2009. 29. Veri Çalışma Grubu, Direktif'in 29. maddesi uyarınca kurulmuştur. Bu grup, bağımsız bir danışma organı olarak görev yapmaktadır. Veri Çalışma Grubu'nun görevleri Direktif'in 30. maddesinde düzenlenmiştir.

²¹⁷ AB Direktifi, 24 numaralı gerekçe.

²¹⁸ Başalp, **a.g.e.**, s. 35.

²¹⁹ AB Direktifi, 26 numaralı gerekçe.

²²⁰ *Österreichischer Rundfunk* kararı için bkz., C-465/00, C-138/01, C-139/01 sayılı birleştirilmiş davalar, 20.05.2003. *Lindqvist* kararı için bkz., Bodil Lindqvist, C-101/01, 06.11.2003.

yasaklamadığıdır. Bu kararında AAD, Direktifin uygulanabilirliği için her somut olayda AB içerisindeki ortak pazarın işleyişi ile yeterli düzeyde bir bağlantısı olduğunun tespiti şartının gerekmeceğini tespit etmiştir. Direktifin uygulanmasında her somut olayda üye devletler arasındaki serbest dolaşım ile bağlantı aranmasına gerek yoktur. Her türlü veri aktarımı kural olarak Direktif hükümlerinin kapsamında yer almaktadır²²¹. İşveren tarafından çalışan ya da emeklilerinin ücretlerine ilişkin bilgilerin üçüncü kişilere iletilmiş olması AİHS bağlamında müdahale teşkil eder. Zira müdahalenin varlığı için üçüncü kişilere iletilen verilerin daha sonra nasıl kullanıldığı önemli değildir. Divan kararında ayrıca Direktif ile AİHS 8. madde arasındaki bağlantıyı incelemiştir. Buna göre müdahalenin meşru olup olmadığı AİHS bağlamında değerlendirilmiş, müdahale meşru olmadığı takdirde Avusturya Kanunu'nun AİHS 8. madde ile uyumsuz olması halinde aynı zamanda Direktifin hükümleri ile de uyumsuz olacağını tespit etmiştir²²².

AAD'nin, Direktifin uygulama alanına ilişkin önemli tespitleri içeren diğer bir kararı ise *Lindqvist* kararıdır. Burada Divan, Direktifin internet ortamında uygulanabilirliğini değerlendirmiştir. Mevcut olayda İsviçre'deki bir kilisede gönüllü olarak çalışan Bayan Lindqvist, cemaat ve kilise görevlilerini bilgilendirmek amacıyla açtığı internet sitesine katılımcıların rızaları olmadan isimleri, telefon bilgileri gibi kişisel bilgilerine yer vermiştir. Davalı aynı zamanda çalışanlardan birinin sağlık durumu nedeniyle izinde olduğuna dair hassas veri niteliğindeki bilgilere İsveç Veri Araştırma Heyeti'ni bilgilendirmeden yer vermiştir. Divan önüne getirilen mevcut olayda Direktifin internet ortamına uygulanabilirliğini, internete veri aktarmanın üçüncü ülkelere veri transferi teşkil edip etmediğini değerlendirmiştir. Divan'a göre internet ortamındaki bilgiler kişisel verilerdir ve bunların internet sayfasında yeniden üretilmesi işleme anlamına gelmektedir. Bu bilgilerin internete bağlanan kişilerin erişimine açmak ise kişisel verilerin otomatik

²²¹ *Österreichischer Rundfunk*, paras. 41-42.

²²² *Österreichischer Rundfunk*, paras. 76-90.

olarak işlenmesidir. Mevcut olayda kişisel veriler sınırsız sayıda insanın erişimine açılmaktadır. Bu anlamda mevcut olay, kişisel bir faaliyet olarak nitelendirilemeyecektir. Divan, davalının verileri işlemesi gönüllü bir faaliyeti sonucu da olsa, işleme ekonomik bir amaca yönelmese de “kişisel ve ailevi etkinlikler” olarak görülmesi gerekmediğine karar vermiştir. Buna göre mevcut olayın 3. maddenin 2. fıkrasında sayılan istisnalar içerisinde değerlendirilmeyeceğini vurgulamıştır. Kişisel verilerin internette yayınlanması ile bu veriler belirsiz sayıda kişinin erişimine açık hale gelmekte, “kişisel ve ailevi etkinlikler” istisnasının kapsamı dışına çıkmaktadır²²³.

Divan, internet ortamında kişisel bilgilerin yayınlanmasının üçüncü ülkelere veri aktarımı anlamına gelmeyeceğini vurgulamıştır. Üçüncü ülkelere veri aktarımı rejiminin kişisel verilerin internet sitesine her yüklenmesinde uygulanması gerektiğinin kabulü ile verinin aktarıldığı her üçüncü ülkenin yeterli düzeyde koruma sağlayıp sağlamadığının denetlenmesi gerekecektir. Ancak, her internet sitesi AB üyesi olmayan devletler için erişilebilirdir. Tek bir ülke dahi yeterli düzeyde korumayı sağlamadığı takdirde transfer yasağının uygulanması gerekecektir²²⁴. İnternetin teknik özelliklerinden yola çıkarak, mevcut olayda davalının internet sitesi sayfalarına erişmek için bir niyeti olmayan kişilere otomatik olarak bilgi yollayacak teknik imkanları sağlamamaktadır. Divan'a göre veriler, yalnızca internet ortamında yayınlanmaları dolayısıyla üçüncü ülkelere aktarılmış olmaz. Kişisel veriler bu sayfaları özel olarak aramayan kişilere gönderiliyorsa ve İnternet sunucu altyapısı AB üyesi olmayan bir ülkede bulunuyorsa üçüncü ülkelere veri transferi rejimi geçerli olacaktır²²⁵.

²²³ Bodil Lindqvist, para. 47. Ayrıca Divan'ın Lindqvist kararı ile sergilediği yaklaşım Facebook, MySpace gibi sosyal ağların gelişimlerini belirsizleştirmektedir. Ayrıntılı değerlendirme için bkz., Rebecca Wong-Joseph Savirimuthu, “All or Nothing: The Application of Article 3.2 of the Data Protection Directive 95/46/EC to the Internet”, **John Marshall J. Computer & Info. L.**, S. 211, 2008, s. 17.

²²⁴ Bodil Linqvist, para. 69.

²²⁵ Küzeci, **a.g.e.**, s. 170.

Divan'ın saptamalarından yola çıkarak diyebiliriz ki, Direktif hükümleri ve AB veri koruma modeli geniş bir kapsama ulaşmaktadır. Kararlarda geçen Direktifin uygulanma alanının yalnızca ortak pazar ile sınırlandırılmayacağı, internet ortamındaki veri işlemlerinin de Direktif kapsamına alınması bu geniş uygulamaya örnek teşkil eder. AB veri koruma modelinin küresel düzeyde etkisine bir diğer örnek ise aşağıda yer vereceğimiz Direktifin yeterli koruma sağlamayan ülkelere veri aktarımını yasaklayan düzenlemesidir.

(3) Üçüncü Ükelere Veri Aktarımı Rejimi

Çağımızda bilgi, sürekli gerçek ve sanal ağlar ile hareket halindedir. Yeni teknolojik gelişmelerin getirdikleri ile birlikte bilginin sayısallaştırılması, veri aktarımı ve işlenmesini de aynı ivmeyle arttırmıştır. Bilgi paylaşımı artık uluslararası düzeyde etkilerini göstermekte ve bireylere ait pek çok verileri içermektedir. Bu noktada bireyin kişisel verilerinin uluslararası düzeyde korunmasının önemi ortaya çıkar. Zira günümüzde, dünyanın her yerinde kişisel verilerin korunması ve veri aktarımı konularına aynı hassasiyetle yaklaşılmamaktadır. Bu durum, ulusal düzeyde korunan kişisel verilerin bir kere sınırları aştıktan sonra korumasız kalacağına, ilgilinin kendi ulusal mevzuatında sahip olduğu haklarından mahrum kalacağına dair endişeleri gündeme getirir. Bu konuyu göz önünde bulunduran AB, Direktif'te yeterli düzeyde veri koruması sağlamayan üçüncü ülkelere veri transferini yasaklayan bir rejimi kabul etmiştir²²⁶. Ancak, Direktif “veri aktarımı”na ilişkin bir tanımlama yapmamıştır. Bu bağlamda Direktifi incelerken kişisel verilerin aktarımının tanımlanmasının yapılması, üye devletlerce kişisel verilerin hangi şartları sağlaması koşuluyla üçüncü ülkelere aktarılabilceğinin incelenmesi gerekmektedir.

Öncelikle belirtmemiz gerekir ki, Direktif ile AB üyesi devletlerin kişisel verilerin korunması hukukuna dair düzenlemelerinin uyumlaştırılması hedeflenmektedir. Bunun için üye devletler arasında kişisel verilerin aynı derecede

²²⁶ Üçüncü ülkeler burada AB üyesi olmayan ülkeler anlamındadır.

korunması sağlanmaya çalışılmıştır. Kişisel verilerin korunmasına ilişkin farklı düzenlemelerin veri aktarımını engelleyici etkisine 1989 yılında, Fransız Veri Koruma Komisyonunun Fransa'dan İtalya'ya kişisel verilerin aktarımına izin vermemesi örnek olarak gösterilebilir. Örnek olaya göre, Fiat şirketinin Fransız alt şirketi yönetim kadrosunun kişisel verilerini İtalya'da bulunan merkeze aktarmak için Fransa, veri koruma komisyonundan izin istemiştir. Ancak, komisyon İtalya'da o tarihlerde henüz kişisel verilerin korunmasına ait hükümlerin bulunmaması nedeniyle verilerin aktarımına izin vermemiştir²²⁷. Bu olaydan yola çıkarak Direktif'te AB iç sınırları çerçevesinde üye devletlerin verilerin serbest dolaşımını, verileri korunmasının iç sınırlarının aşılması sebebiyle ihlal edileceği gerekçesiyle sınırlandırılmayacağı veya engelleyemeyeceği düzenlenmiştir²²⁸. Direktif, üye devletlerde tamamen aynı bir korumayı değil, dengeli bir korumayı amaçlamaktadır²²⁹.

Veri transferini üye devletler içerisinde yukarıdaki gibi düzenleyen Direktif, üçüncü ülkeler açısından ise aşamalı bir düzenleme getirmektedir. Üçüncü ülkelere veri aktarımına dair kurallar Direktif'in 25. ve 26. maddelerinde düzenlenmiştir²³⁰. Genel kural olarak baktığımızda AB sınırları dışındaki bir ülkeye (üçüncü ülkeye), kişisel verilerin iletilmesi bu ülkenin veri koruması hukukunun AB ölçütlerine

²²⁷ Milli Haberleşme ve Özgürlük Komisyonu (CNIL) Yayın No. 89-78, 11.07.1989. Ayrıca bkz.; Şimşek, **a.g.e.**, s. 54; Özdemir, **a.g.e.**, s. 32.

²²⁸ Direktif'in ilgili 1. maddesi şöyledir; "(1) Birliğe üye ülkeler; bu Direktifte belirtilen kişilerin hak ve özgürlüklerine ve kişisel verilerin işlenmesinde gerçek kişilerin özel hayatlarını garanti altına almalıdırlar. (2) Birliğe üye ülkeler, 1. maddede sayılan hak ve özgürlüklere ilişkin sebeplerden ve Avrupa Birliği'ne üye ülkeler arasında dahi, kişisel verilerin serbest dolaşımını yasaklayabilirler veya sınırlandırabilirler.". İlgili madde, temelini AB ortak pazarının sağlanmasından almaktadır. Bkz., Bygrave, "**Privacy and Data Protection in an International Perspective**", s. 186.

²²⁹ AB Direktifi, 9 numaralı gerekçe. Ayrıca Direktif, ulusal hukukların yeknesaklığından ziyade uyumu hedeflemektedir. Nitekim AB mevzuatına göre de direktifler AB üyesi ülkelerin konu ile ilgili kendi iç hukuklarında getirecekleri düzenlemelerde uymaları gereken genel kuralları belirlemektedirler. Bkz., Schwartz, "**European Data Protection Laws and Restrictions on International Data Flows**", s. 481. Ulusal hukukların yeknesaklığı yerine uyumun sağlanması için Direktif'in iç hukuklarına aktarılmasında üye ülkelere belirli sınırlar içerisinde takdir marjı tanınmıştır. Bkz., Bygrave, "**Privacy and Data Protection in an International Perspective**", s. 187.

²³⁰ Hatırlatmak isteriz ki, kişisel verilerin korunmasına ilişkin diğer temel uluslararası belgelerde de veri aktarımına dair hükümler bulunmaktadır. Buna göre 108 sayılı Sözleşme'nin 12. maddesinde, OECD Rehber İlkeleri'nin 17 ve 18. paragrafları ile BM İlkeleri'nden 9. ilkede konuya ilişkin düzenlemeler yer almaktadır. Diyebiliriz ki, ülkeler arası veri aktarımının her geçen gün daha da artmasıyla birlikte konuya ilişkin birçok çözüm yolları da artmaktadır.

göre yeterli nitelikte olmasına bağlıdır²³¹. Burada “yeterlilik” düzeyinin saptanması gereklidir. Ancak, üçüncü ülkelere veri aktarımında bu düzeyin saptanması kolay değildir. 29. Madde Veri Çalışma Grubu, yeterli düzeyi açıklamak üzere “Üçüncü Ülkeler Kişisel Verilerin Transferinde Temel Prensipler” adlı bir karar yayınlamıştır. Veri Koruma Grubu, 25. maddeye göre “yeterlilik” ölçütünün her bir somut olaya göre değerlendirilmesi gerektiğini belirtmiştir. Ancak, Grubun görüşüne göre veri aktarımının yoğunluğu, aktarımdaki tarafların sayısının çokluğu gibi nedenlerden ötürü üye devletler her bir somut olayın detaylı incelenmesini sağlayamayabilirler. Bu görüşten yola çıkan Grup, usule dair alınması gereken yöntemlere dikkat çekmiş ve veri aktarımlarına ilişkin “beyaz listeler” oluşturulmasını savunmuştur. Bu listeler hangi ülkelerin yeterli koruma düzeyini karşılayabildiğine dair bir rehber niteliğindedir. Listede yer almayan ülkeler açısından ise her somut veri aktarımı yeterlilik düzeyi bakımından incelenecektir²³². Aktarımın sağlanabilmesi için üçüncü ülkede kişisel verilerin koruma düzeyinin Direktif’in koruyucu çekirdeği ile büyük ölçüde örtüşmesi gerekmektedir²³³. Ayrıca üçüncü ülkenin konuya ilişkin olarak belirlenmiş kuralları ile birlikte bu kuralların etkili olması için oluşturulmuş sistem de göz önünde bulundurulacaktır²³⁴. Yani, üçüncü ülkedeki düzenlemelerin uygunluğu o ülkenin mevzuatına ve iç hukukunun işleyişine göre değerlendirilecektir. Değerlendirme yapılırken üçüncü ülkede temel hak ve özgürlüklerin korunması ile kişinin özel alanının korunmasındaki düzeye dikkat edilecektir²³⁵.

²³¹ Veri transferinin ön şartı olarak transferin gerçekleştirileceği üçüncü ülkelerin veri koruma düzenlemelerine dair “yeterlilik” ölçütü Avrupa sanayiini dış rekabetten koruyan, Direktif’in ekonomik amacını öne çıkaran kanıt olarak yorumlanabilmektedir. Bununla birlikte AAD’nin içtihat hukuku ve AB hukukunun genelinde konunun, özel hayatın gizliliği hakkından ayrı, bağımsız bir kişisel verilerin korunması hakkı olarak ele alınmaya başlandığı görülmektedir. Bu da konunun AB düzeyinde temel hak ve özgürlükler ekseninin öne çıktığının göstergesidir. Bkz., Bygrave, “**Privacy and Data Protection in an International Perspective**”, s. 32.

²³² Karar için bkz., Article 29 Data Protection Working Party, **First orientations on Transfers of Personal Data to Third Countries-Possible Ways Forward in Assessing Adequacy**, XV D/5020/97-EN final WP4, 26.06.1997, s. 3.

²³³ Başalp, a.g.e., s. 68.

²³⁴ Article 29 Data Protection Working Party, **First orientations on Transfers of Personal Data to Third Countries-Possible Ways Forward in Assessing Adequacy**, XV D/5020/97-EN final WP4, 26.06.1997, s. 5.

²³⁵ AB Direktifi, m. 25/f.2

Direktife göre yeterli koruma düzeyinin saptanmasında özellikle dikkat edilmesi gereken şartlar tespit edilmiştir. Bu şartlar; verinin niteliği, işlemenin amacı ve süresi, çıkış yeri ülkesi ve varacağı ülke, üçüncü ülkede geçerli olan genel ve sektörel hukuk kuralları, bu ülkede uyulan mesleki kurallar ve uygulanan güvenlik önlemleridir. Bunların dışında kişisel verilerin hukuka uygun işlenmesinde denetleyici organların varlığı ve etkinliği, verilerin hukuka aykırı işlenmesinde sorumluluk ve uygulanan yaptırımlar ile izin verilen transferin ardından izni aşan yeni transferlerin sınırlandırılmış olmasına da dikkat edilecektir.

Veri aktarımının gerçekleştirilmesi istenen üçüncü ülkelerin veri koruma düzeyinin yeterliliğinin belirlenmesinde üye devletlere görevler yüklenmekte ve Avrupa Komisyonuna mutlak bir yetki tanınmaktadır. Her üye devletin dahi koruma eşiği aynı düzeyde olmadığından, üye devletler içinde koruma düzeyi en düşük olan üye devlet AB veri koruması limanına dönüşebilmektedir. İşte bu durumun önlenmesi yalnızca üye devletlere görev yüklenilmesiyle yetinilmemiş aynı zamanda Avrupa Komisyonu'na da mutlak yetki tanınmıştır²³⁶.

Direktifin 25. maddesinin aradığı yeterli koruma düzeyine sahip olmayan üçüncü ülkelere veri aktarımı bazı istisnalar ile sağlanabilmektedir. Bu istisnalar Direktifin 26. maddesinde düzenlenmiştir. Buna göre istisnalar; (i) doğrudan sorumlu lehine etki edebilmekte veya (ii) sorumlunun yeterli garantiyi göstermesi gerekmektedir. Ayrıca Avrupa Komisyonu'na standart sözleşme kuralları öngörme yetkisi de tanınmıştır. Direktifin 25. maddesinde yer alan yeterli koruma düzeyine sahip olmayan üçüncü ülkelere kişisel veri transferine imkan veren genel istisnalar şunlardır;

- Kişisel verileri işlenen kişinin rızasının alınmış olması²³⁷: Rıza, tereddüde yer vermediği sürece geçerlidir. Bu anlamda rızanın sözlü, yazılı veya elektronik olarak verilmesi önemli değildir. Önemli olan rızanın açık ve ilgili kişinin özgür

²³⁶ Başalp, **a.g.e.**, s. 67.

²³⁷ AB Direktifi, m. 26/f.1/a

iradesiyle ve isteği konusunda tereddüde yer vermeyecek nitelikte olması gerekmektedir. Ayrıca ilgili kişinin bilgilendirilmiş olması gerekmektedir.

- Veri aktarımının ilgili kişi ile transfer eden sorumlular arasındaki bir sözleşmenin ifası veya ilgilinin talebi üzerine sözleşme öncesi bir ilişkinin yürütülmesi için gerekli olması²³⁸: Bu istisnada önemli olan gereklilik ölçütünün sağlanmasıdır. Gereklilik ölçütü tespit edilirken veri sahibi ile sözleşme arasında yakın ve gerçek bir bağ bulunması aranır. Örneğin bir seyahat acentası ile yapılan sözleşme doğrultusunda ilgili kişinin bilgilerinin kalacağı otele aktarılması bu istisna kapsamında değerlendirilecektir²³⁹.

-Aktarımın ilgili kişinin çıkarlarının korunması doğrultusunda, veri denetçisi ve üçüncü bir kişi arasında yapılan bir sözleşmenin sonuçlandırılması ve uygulanması için gerekli olması²⁴⁰;

- Aktarımın önemli kamusal menfaatlerin korunması veya mahkeme önünde taleplerin dinlenmesi için gerekli veya yasa gereği zorunlu olması²⁴¹: Vergi veya gümrük kurumları arasında veya sosyal güvenlik konularında yetkili birimler arasındaki veri aktarımı bu istisnaya örnek olarak gösterilebilir²⁴². Ancak, burada üçüncü ülkedeki kamu otoritelerinin değil, Birlik üyesi devletlerin kamusal menfaatinin varlığı göz önünde tutulacaktır. Veri aktarımının yasa gereği zorunlu olmasına ise uluslararası bir şirketin alt şirketi olarak AB toprakları dışında bulunan şirket ile AB toprakları içinde bulunan alt şirketindeki bir çalışan arasındaki hukuksal çekişme dolayısıyla bu çalışanın bilgilerinin aktarılması verilebilir. Ancak, her halükarda ileride bir uyuşmazlığın gerçekleşebileceğinden bahisle bütün işçilerin kişisel dosyalarının aktarılması istisna teşkil etmeyecektir²⁴³.

²³⁸ AB Direktifi, m. 26/f.1/b

²³⁹ Küzeci, **a.g.e.**, s. 174.

²⁴⁰ AB Direktifi, m. 26/f.1/c

²⁴¹ AB Direktifi, m. 26/f.1,d

²⁴² AB Direktifi, 58 numaralı gerekçe.

²⁴³ Article 29 Working Party, **Working Document on a common interpretation of Article 26(1) of**

- Aktarımın yaşamsal önemdeki menfaatlerin korunması için gerekli olması²⁴⁴: Kişinin sağlığına ilişkin acil bir durum söz konusu olduğunda ve bu kişinin tıbbi yardım alabilmesi için verilerin aktarılması istisna kapsamındadır²⁴⁵.

- Aktarımın aleniyet ilkesi çerçevesinde herkese veya ilgisini ispat eden herkese açık bulunan kamu sicillerinden yapılması ve veri koruma mevzuatının aradığı şartları koruması²⁴⁶: Bu ilkeye göre ilgili ülkede meşru çıkarı olan herkes bilgilere ulaşabildiği takdirde üçüncü ülkelerde bulunan kişiler de bu bilgilere ulaşabilmelidir. Aktarım, meşru çıkarı olanların talebi üzerine veya bu kişiler alıcı konumunda ise söz konusu olacaktır²⁴⁷. Üye devletler bu istisnaya dair detaylı düzenlemeler getirebileceklerdir²⁴⁸.

Yukarıda saymış olduğumuz istisnalar transfer yasağını ortadan kaldırmaktadır. Bu istisnaların dar yorumlanması gerekir. Ayrıca üye devletler çalışanlara veya hastalara ait kişisel verilerin korunması gibi özel korumayı gerektiren bazı birey grupları için istisnaların uygulanmasını kaldırabilir²⁴⁹. Ancak, kişisel verilerin aktarımı Direktif'in genel koruyucu hükümlerine halen daha tabiidir. Örnek vermek gerekirse, bu istisnaların mevcut olduğu hallerde dahi hassas veriler için geliştirilen nitelikli koruma geçerliliğini koruyacaktır²⁵⁰.

Directive 95/46/EC of 24 October 2005, 2093/05/EN, WP 114, 25.11. 2005, s. 15.

²⁴⁴ AB Direktifi, m. 26/f.1/e

²⁴⁵ Ancak bireyin sağlık durumundan sorumlu ve AB toprakları dışında bulunan kişilere, genel sağlık kontrolleri dahilinde bilgilerin aktarılması istisna kapsamı dışındadır. Bkz., Article 29 Working Party, **Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 2005**, 2093/05/EN, WP 114, 25.11.2005, s. 16.

²⁴⁶ AB Direktifi, m. 26/f.1/f

²⁴⁷ AB Direktifi, 30 numaralı gerekçe.

²⁴⁸ AB Direktifi, 31 numaralı gerekçe.

²⁴⁹ Article 29 Data Protection Working Party, **Working Document, Transfer of personal data to third countries: Applying Articles 25 and 26 of The EU data protection directive**, 2093/05/EN, WP 12, 24.07.1998.

²⁵⁰ Diğer nitelikli koruma halleri ise doğrudan pazarlama ve otomatik surette kişi hakkında verilen kararlardır. Bkz., Article 29 Data Protection Working Party, **First orientations on Transfers of Personal Data to Third Countries-Possible Ways Forward in Assessing Adequacy**, XV D/5020/97-EN final WP 4, 26.06.1997, s. 7.

Veri aktarımı yasağına bir diğer istisna ise sorumlunun ilgilinin özel alanı ile temel hak ve özgürlüklerin korunması konularında “yeterli” garanti göstermesi ve üye devletin veri aktarımına onay vermesidir. Yeterli koruma düzeyine sahip olmayan bir ülkeye sorumlularca yeterli korumanın sağlanacağı garantisi ile kişisel verilerin aktarımına izin verilmektedir. Buna göre, yeterli koruma düzeyine sahip olmayan ülkeye veri aktarımının hukuka uygun olarak gerçekleşebilmesi için; (i) konu, kişisel verilerin bir kerelik aktarımını veya doğrudan bir transfer kategorisine ilişkin olmalıdır ve (ii) sorumlu aktarımda ilgilinin temel hak ve özgürlüklerinin özellikle özel hayat alanının korunacağını da garanti etmelidir. Direktifin 16. maddesinin 2. fıkrasına göre aranılan garantiler sözleşmede yer alabilecek; sorumlu, ilgili kişinin temel haklarını korumak üzere “uygun sözleşme hükümleri” benimseyebilecektir. Aranılan garantilerin sözleşmede yer alması bir zorunluluk değildir. Direktif’te yer alan sözleşme kavramı örnek olarak kullanılmıştır ve tek taraflı taahhüt ile de yeterli garantiler sağlanabilir²⁵¹. Üye devletler onayladıkları garantileri Avrupa Komisyonu’na bildirmekle yükümlüdürler. Bildirim üzerine diğer ülkeler gerekçeli bir itirazda bulunabilirler. Üye devletlerin itirazı üzerine Direktifin 31. maddesinin 2. fıkrasında düzenlenen usule göre ihtilaf karara bağlanır. Diğer üye devletlerce verilecek itirazın verilen iznin üzerinde bir etkisi olmayacaktır. İtiraz üzerine Komisyonun vereceği karar verilen izin için önemlidir. Avrupa Komisyonu verilen izni yerinde görmez ise uygun önlemler alınmasına karar verebilecektir. Bu kararı üye devletler iç hukuklarında uygulamak zorundadırlar. Komisyonun kararına göre izin daraltılabilir veya kaldırılabilir. Ayrıca Komisyon, izin veren devlete görevler yükleyebilir. Bütün bu imkanların yanı sıra, Avrupa Komisyonu “*standart sözleşme şartları*” öngörerek yeterli garantilerin nasıl sağlanacağı belirleyebilecektir. Birlik üyesi devletler bu karara dayanarak veri aktarımına izin verebilir²⁵².

ABD’de kişisel verilerin korunması konusu AB’ye göre farklı bir şekilde ele alınmaktadır²⁵³. AB standartlarına uygun koruma düzeyine sahip olmadığından üye

²⁵¹ Başalp, **a.g.e.**, s. 73.

²⁵² AB Direktifi, m. 24/f.4.

²⁵³ Bu dipnot bağlamında ABD’de konunun ele alınış biçimine bir kere daha değinmek isteriz.

devletlerden ABD'ye kişisel verilerin aktarımı yasak kapsamında ele alınmaktadır. Bu nedenden ötürü yaşanan zorlukların aşılması için karşılıklı müzakereler sonucunda ABD şirketleri için *Safe Harbor* (Bağışıklık Sözleşmeleri) prensipleri düzenlenmiştir. *Safe Harbor* prensipleri, ABD ve AB arasında kabul edilen bir dizi veri koruma ilkesidir. Sistemin işleyişinden ABD Ticaret Bakanlığı sorumludur. Bu kurallara uymayı kabul eden Amerikan şirketlerinin AB standartlarına uygun veri koruma düzeyine sahip oldukları kabul edilir. Ayrıca söz konusu prensipler standart sözleşme şartlarına örnek teşkil eder.

Üçüncü ülkelere veri aktarımının hukuka uygunluğunu temin etmek için diğer bir alternatif çözüm ise bazı iş çevrelerince kabul gören “bağlayıcı şirket kuralları”dır (Binding Corporate Rules). Özellikle uluslararası şirketler, küresel düzeydeki karmaşık yapılarının farklı ülkelerdeki -özellikle AB sınırları dışındaki- üçüncü ülkelerdeki alt şirket gruplarına veri aktarımına engel olmasına çözüm olarak şirket gruplarının uyacakları kurallar belirlemektedirler²⁵⁴. Bu kurallara göre bir grup şirketi her bir şirket için zorunlu olan kendi veri koruma ilkelerini belirlemekte, yetkili bir veri koruma otoritesi tarafından bu kurallar kabul edildiğinde şirket grubu içerisinde uluslararası veri aktarımı da olanaklı hale gelmektedir²⁵⁵.

Üçüncü ülkelere veri aktarımı konusunda Avrupa Komisyonunun bazı olumlu yeterlilik değerlendirmeleri mevcuttur. Buna göre İsviçre, Kanada, Arjantin, İsrail gibi bazı ülkelerin yeterli düzeyde koruma getirdiği kabul edilmiştir. Ayrıca Amerika ile yapılan *Safe Harbor* prensipleri (Bağışıklık Sözleşmeleri) ve Amerika'ya PNR

Amerikan hukukunda kişisel verilerin korunması hakkını da içeren özel hayatın gizliliği hakkı anayasal bir hak değildir. Özel yaşamın gizliliği hakkı içtihatlarla kabul görmüştür. Son zamanlarda kişisel verilerin korunması gerekliliğine dair tartışmalarda artış görülmesine rağmen ABD'de kişisel verilerin korunması son derece düşük düzeydedir. ABD'de konu ile ilgili katı ve kapsayıcı bir düzenleme yerine sektörel çözümler tercih edilmiştir. Bu farklılıktan dolayı Kıta Avrupası'nda kişisel verilerin niteliği insan hakları dahilinde açıklanırken ABD'de veri pazarının etkinliğine yönelik kaygılar ve kişilerin verileri üzerinde mülkiyet hakkına sahip olduğu görüşü öne çıkmaktadır.

²⁵⁴ Article 29 Data Protection Working Party, **Working Document on 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, 03.06.2003.

²⁵⁵ Küzeci, a.g.e., s. 177.

verilerinin aktarılmasının kabulüne ilişkin kararlar da bulunmaktadır²⁵⁶.

Kişisel verilerin korunmasına ilişkin yeterli koruma düzeyini sağlamayan üçüncü ülkelere veri transferini yasaklayan rejimi Direktifin AB üyesi devletler dışında da etkili olmasına neden olmuştur. Birlik üyesi olmayan devletler, yeterli koruma düzeyini sağlamak adına ulusal mevzuatlarında yeni düzenlemeler getirmektedirler. Direktifin veri transferi rejimini düzenleyen 25. ve 26 maddelerinin yanında Direktifin AB sınırları dışında da uygulanabilirliğine dair istisnayı içeren 4. maddesinin 1. fıkrasının c bendi ile de AB modeli Birlik sınırlarını aşan bir etkiye sahip olmuştur²⁵⁷.

²⁵⁶Avrupa Komisyonunun yeterli düzeyde koruma getirildiğine dair olumlu yeterlilik kararları için bkz.,http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

²⁵⁷ Bygrave, “Privacy and Data Protection in an International Perspective”, s. 19.

İKİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HAKKINA ÖZGÜ KRİTERLER

I. GENEL OLARAK

Kişisel verilerin korunmasına ilişkin düzenlemeler ile kişisel verilerin korunması hakkının ulusal ve uluslararası düzeyde bağımsız bir hak olarak tanınmasına dair yaklaşımdan bahsetmiştik. Bu anlamda insan onuru ve öz değerinin hiçe sayılmaması, insan onuru ile bağdaşmayan uygulamaların yapılmaması için kişisel verilerin işlenmesi ve kullanılması sırasında birtakım temel ilkelerin göz önünde bulundurulması gerekmektedir. Kişisel verilerin korunmasına ilişkin düzenlemelerde konuya özgü bazı ortak ilkeler kabul edilmiştir. Bu ilkeler gerçekleşmediği takdirde kişisel verinin işlenmesinden bahsedilemez. Ayrıca bu ilkelere uyulmadığı takdirde ortada bir kötüye kullanımın varlığı kabul edilmektedir.

Kişisel verilerin korunması hakkına özgü kriterlerin değerlendirilmesi çalışma konumuz açısından da önemlidir. Kişisel verilerin korunmasına ilişkin suçlar incelendiğinde, genel olarak kişisel verilerin işlenmesine ilişkin usul ve esaslara aykırı fiillerin çeşitli yönleriyle ele alındığı görülmektedir. Bu açıdan kişisel verilerin korunmasına ilişkin suçlar, kişisel verilerin işleme usul ve esaslarına aykırı kimi fiiller esas alınarak düzenlenmiştir. Ayrıca kişisel verilerin hukuka uygun bir şekilde işlendiğinden bahsetmek için öngörülen bu usul ve esaslara ya da ilkelere uygun davranılması gerekmektedir. Kişisel verilerin korunmasına özgü kriterlerin öğrenilmesi aynı zamanda ceza hukuku alanında hangi hallerde hukuka uygunluğun sağlandığının tespiti açısından da önemlidir.

II. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN İLKELER

A. Hukuka ve Dürüstlük Kurallarına Uygun İşleme

Kişisel verilerin korunmasına ilişkin düzenlemelerde yer alan birincil ilke, kişisel verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesidir²⁵⁸. Hukuka uygunluk kişisel verilerin işlenmesinde yasalarla ve diğer hukuksal düzenlemelerde getirilen ilkelere uygun hareket edilmesidir²⁵⁹. İşleme sürecinin tamamında hukuka uygun hareket edilmesi gerekmektedir²⁶⁰. Bu açıdan işleme sürecinin tanımlamasının yapılması önemlidir. AB Direktifi'ne baktığımızda kişisel verilerin işlenmesi; 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 otomatik olmayan araçlarla, kişisel veri üzerinde uygulanan her türden işlem veya işlem dizisi olarak tanımlanmıştır²⁶¹. 108 sayılı Sözleşme'ye göre otomatik işleme bütünüyle ya da bir bölümü otomatik şekilde olmak üzere verilerin depolanması, bu verilerin üzerinde mantıksal ya da aritmetik işlemlerin uygulanması, bunların değiştirilmesi, silinmesi, düzeltilmesi veya yayınlanması işlemlerini kapsamaktadır²⁶².

Kişisel verilerin işlenmesine ilişkin her türlü eylemde dürüstlük kurallarına uyulması gereklidir²⁶³. Dürüstlük kurallarına uygun olarak kişisel verilerin işlenmesi,

²⁵⁸ Çalışma konumuz açısından da hukuka uygun ve dürüst işlemeye dair tanımlamanın yapılmasının ayrı bir önemi vardır. Keza TCK'da kişisel verilerin hukuka aykırı olarak kaydedilmesi ve ele geçirilmesi suç olarak düzenlenmiştir. Ancak kişisel verilerin işlenmesine ilişkin genel bir düzenleme bulunmaması karşısında, dürüst ve hukuka uygun işlemenin hangi hallerde gerçekleşebileceğinin tespiti önem taşımaktadır.

²⁵⁹ Konuya ilişkin düzenlemeye pek çok önemli metinde yer verilmiştir. Bkz., AB Direktifi m. 6/f.1; 108 sayılı Sözleşme m. 5/a; BM Rehber İlkeleri 1. ilke; OECD Rehber İlkeleri m. 7. Bununla birlikte konuya ilişkin düzenleme OECD Rehber İlkeleri'nde kişisel verilerin dürüst ve hukuki yollardan elde edilmesi, uygun olduğu durumlarda veri sahibine bilgi verilmesi veya veri sahibinin rızasının alınması gerektiği yer almaktadır. Görüleceği üzere hukuka ve dürüstlük kuralına uygunluk ilkesi OECD Rehber İlkeleri'nde bireyin katılım ilkesi ile birlikte düzenlenmiştir.

²⁶⁰ Küzeci, **a.g.e.**, s. 197; Özdemir, **a.g.e.**, s. 137.

²⁶¹ AB Direktifi, m. 2/b.

²⁶² 108 sayılı Sözleşme, m. 2/c

²⁶³ Dürüstlük kuralı Türk Medeni Kanunu'nun 2. maddesinde ifadesini bulmaktadır. Buna göre

süreç içerisinde kişinin toplama ve işleme amacı hususunda yanıtılmamasını ve amaçla bağdaşmayan ya da veri sahibinin anlayamayacağı bir amaç için verilerin işlenmemesi hususlarını kapsamaktadır²⁶⁴. Ayrıca bu ilkenin gereği olarak veri denetçilerini kişisel verileri işleme sürecinde ilgili kişinin özel hayatın gizliliği hakkını, maddi ve manevi bütünlüğü ile özerkliğini makul olmayan nedenlerle ihlal eden bir hareket tarzından kaçınmasını zorunlu kılmaktadır²⁶⁵. Bu bağlamda kişisel verileri hukuka ve dürüstlük kurallarına uygun işleme ilkesi aşağıda incelenen diğer veri koruma ilkelerine kaynaklık etmektedir.

B. Amaçla Bağlılık İlkesi

Kişisel verilerin işlenmesinde amaçla bağlılık ilkesi bu verilerin önceden belirlenmiş ve hukuka uygun amaç ya da amaçlar için toplanması ve bu amaçlarla bağdaşmayan şekillerde işlenmemesini gerektirmektedir²⁶⁶. Amaçla bağlılık ilkesi, kişisel verilerin dürüst ve hukuka uygun olarak işlenmesi ilkesinin somut durumda uygulanıp uygulanmadığının tespiti açısından önemlidir²⁶⁷. Ayrıca anılan ilke

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)**, İstanbul, Filiz Kitabevi, 2008, s. 222.

²⁶⁴ Kişisel verilerin dürüstlük kuralına uygun olarak işlenmesi kişisel verilerin işlenmesinde amaca uygun davranma ve bu amaçlar açısından veri sahibinin aldatılmaması gibi iki önemli unsuru kapsamaktadır. Bkz., Özdemir, **a.g.e.**, s. 138. Buna göre, aşağıda ayrıca incelenecek olan kişisel verilerin işlenmesine özgü kriterlerden amaç ile bağlılık ilkesi, dürüstlük kuralının bir parçasını oluşturmaktadır. Bkz., Ketizmen **a.g.e.**, s. 224.

²⁶⁵ Lee A. Bygrave, **Data Protection Law, (Approaching Its Rationale, Logic and Limits)**, Hollanda, 2002, s. 58'den aktaran, Küzeci, **a.g.e.**, s. 198.

²⁶⁶ Kişisel verilerin belirli bir amaç doğrultusunda toplandıktan sonra bu amaç dışında başka amaçlar ile işlenmemesi AİHM kararlarında da değerlendirilmiştir. Bu anlamda *Malone/Birleşik Krallık* kararını örnek verebiliriz. Mevcut olayda başvurunun itirazları mektuplarının ve telefon konuşmalarının izlendiği, telefonunun kendisini arayan numaraları kaydeden otomatik bir cihazla kaydedildiği yönündedir. Mahkeme başvuranın telefon konuşmalarının tespit edilmesi ve aranılan numaraların kaydedilmesinin dayandığı yasal düzenlemenin uygun olmadığını, hukuka uygun olarak yapılmış müdahalenin olmadığından yola çıkarak AİHS'nin 8. maddesinin ihlal edildiğine karar vermiştir. Mahkeme aranılan numaraların kaydedilmesine yani “sayaçlama”ya dair değerlendirmesinde bulunurken amaçla bağlılık ilkesini vurgulayıcı tespitlerde bulunmuştur. Mahkeme'ye göre sayaçlamanın amacı, “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 bilginin kaydedilmesi”dir. Buna göre bu bilgilerin sayaçlamanın meşru amacı dışında abonenin rızası haricinde polise verilmesi AİHS'nin 8. maddesine müdahale teşkil eder. Bkz., *Malone/Birleşik Krallık*, b.n. 8691/79, k.t. 02.08.1984, para. 84.

²⁶⁷ Ketizmen, **a.g.e.**, s. 225.

öncelikle verilerin işleme sürecinin belirli, açık ve meşru amaçlara dayanmasını zorunlu kılmaktadır²⁶⁸.

Verilerin toplanma amacının belirli ve açık olması konuya ilişkin hukuksal düzenlemelerde belirsiz ifadelerden kaçınılmasını ifade etmektedir. Somut olmayan genel ve belirsiz ifadeler ilgilinin kişisel verilerin kullanılma amacını önceden bilmesini engellemektedir. Nitekim ilgili kişi kendi verileri üzerindeki kontrol imkanından yoksun kalmakta, kişisel veriler bakımından önleyici koruma sağlanamamaktadır²⁶⁹. Kişisel verilerin belirli bir amaç ya da amaçlar için işlenmesine izin verilmesi bu işlemlerin kapsam ve sınırlarının belirlenmesi açısından önemlidir. İlgili kişi kişisel verilerinin hangi amaçlar ile kullanılacağını bildiği takdirde işlemeye sağlıklı bir biçimde izin verebilir ve verileri üzerindeki denetimini sağlayabilir.

Kişisel veriler kural olarak önceden belirlenmiş ve şüpheye yer vermeyecek şekilde belirli olan amaç ya da amaçlar için işlenebilmesi ilkesi gelecekte ortaya çıkma ihtimali olan ve halihazırda bilinmeyen amaç ya da amaçlar için kişisel verilerin işlenebilmesine engeldir²⁷⁰. Keza verilerin anonim olmayan bir şekilde ve belirli bir amaç olmaksızın yalnızca depolanmak üzere toplanması amaçla bağlılık ilkesine aykırılık teşkil edecektir²⁷¹. Olası durum toplumu potansiyel suçlu konumuna sokmakla birlikte kişinin kişiliğini geliştirme hakkı, bireysel özerklik ve suçsuzluk karinesi gibi çağdaş demokratik toplum değerlerine zarar verir²⁷².

Verilerin toplanma amaçlarının meşru olması, verilerin toplanmasının yasal bir temele dayanmasını ifade eder. Kişisel verilerin toplanıp işlenebilmesi için ya

²⁶⁸ Bu dipnot bağlamında meşru olmayan amaç ya da amaçlar için kişisel verilerin kaydedilmesinin çalışmamızın ilgili bölümünde ayrıca inceleyeceğimiz Türk Ceza Kanunu'nun 135. maddesindeki suç oluşturacağının altını çizmek isteriz.

²⁶⁹ Şimşek, **a.g.e.**, s. 84, d.n. 370.

²⁷⁰ Spiros Simitis, "Reviewing Privacy In an Information Society", **University of Pennsylvania Law**, S. 740, 1986-1987, s. 740. (Bundan böyle "**Reviewing Privacy In an Information Society**" olarak anılacaktır).

²⁷¹ Şimşek, **a.g.e.**, s. 84; Başalp, **a.g.e.**, s. 38.

²⁷² Küzeci, **a.g.e.**, s. 198 vd.

ilgilinin rızası olmalı ya da kamusal organlar bu konuda yasal bir yetkiye sahip olmalıdır²⁷³. Kişisel verilerin işlenmesinin kişinin rızası çerçevesinde gerçekleştirildiği hallerde rızanın dar yorumlanması gerekmektedir. Kişi, rızasını hangi işlem ve amaç için belirmişse kişisel verilerin toplanması ve işlenmesi bu amaç doğrultusunda olmalıdır²⁷⁴. Amacın yasal bir temele dayandırılması gerekliliğinin yanında ayrıca verilerin toplanmasından sonra da bütün veri işlem faaliyetlerinin konuya ilişkin diğer temel ilkelere uygun yürütülmesi gerekmektedir²⁷⁵.

Genel kural kişisel verilerin ancak toplanma anında belirtilmiş amaç doğrultusunda işlenmesinin gerekliliği olmak ile birlikte AB Direktifi bu ilkeye bir istisna tanımıştır. Buna göre AB üyesi devletler uygun önlemleri aldıkları takdirde kişisel veriler toplama ve işleme amaçları dışında tarihsel, istatistiksel ve bilimsel amaçlarla işlenebileceklerdir²⁷⁶.

Amaçla bağılılık ilkesinin gereği olarak kişisel verilerin toplanma ve işleme amaçları açısından yeterli, bunlarla ilgili ve bu amaçların gerçekleştirilmesi için gerekli olduğu miktarda sınırlı tutulması gerekmektedir²⁷⁷. Kimi metinlerde

²⁷³ Bununla birlikte AB Direktifi'nin 7. maddesinde veri işlemeyi meşru kılan ölçütler belirlenmiştir. İlgili madde hükmüne göre kişisel verilerin işlenmesi, (i) ilgili kişinin rızasının bulunması, (ii) ilgili kişinin taraf olduğu bir sözleşmenin ifa edilmesi ya da ilgili kişinin bir sözleşmenin tarafı olmadan önceki istemleri dolayısıyla işlemenin gerekli olması, (iii) veri denetçisinin tabi olduğu yasal yükümlülüğe uymak için işlemenin gerekli olması, (iv) ilgili kişinin hayati çıkarlarının korunması için işlemenin gerekli olması, (v) işlemenin kamu yararının bulunduğu bir hizmetin gerçekleştirilmesi ya da veri denetçisinin veya verinin açıklandığı üçüncü kişiyi resmi bir yetkisini kullanması için gerekli olması, (vi) Direktif'in m. 1/f.1 hükmü uyarınca ilgili kişinin temel hak ve özgürlüklerinden kaynaklı çıkarlarının baskın olduğu durumlar hariç, veri denetçisinin veya verinin açıklandığı üçüncü kişinin meşru çıkarlarından kaynaklanan amaçlar için gerekli olması durumlarından biri veya bir kaçının bulunması halinde kişisel verilerin işlenmesi meşru kabul edilecektir. Bkz., AB Direktifi, m. 7.

²⁷⁴ Özdemir, a.g.e., s. 142.

²⁷⁵ Şimşek, a.g.e., s. 85.

²⁷⁶ AB Direktifi, m. 1/b. Ayrıca konu ile ilgili ulusal bir düzenleme olarak bkz., İtalyan Veri Koruma Kanunu m. 97 vd.

²⁷⁷ AB Direktifi, m. 6/f.1/c; 108 sayılı Sözleşme, m 5/c. Ayrıca her iki metin de verilerin saklanma amaçları dışında gerekli olmadıkları takdirde anonimleştirilmelerine veya silinmelerine ilişkin hükümler içermektedir. Bkz., AB Direktifi, m. 6/f.e, 108 sayılı Sözleşme, m. 5. Her iki metine göre verilerin saklanma amaçları açısından gerekli olmadıkları zamanda anonimleştirilmeleri veya silinmeleri gerekmektedir. Bkz., AB Direktifi, m. 6/e, 108 sayılı Sözleşme, m.5/e. Verilerin toplanma amaçlarının gerektirdiği ölçüde sınırlı tutulması ilkesine OECD ve BM Rehber İlkeleri'nde açıkça yer verilmemiştir. Ancak konu dürüstlük kuralı çerçevesinde değerlendirilebilir. Bkz., Bygrave, **Data Protection Law, (Approaching Its Rationale, Logic and Limits)**, Hollanda, 2002, s. 60'dan aktaran Küzeci, a.g.e., s. 203.

“asgarilik ilkesi” olarak adlandırılan bu ilke, toplanan kişisel veri miktarının, verilerin toplanması ve daha sonra işlenmesi amaçlarını başarmak için zorunlu olan miktarla sınırlı kalınmasını ifade etmektedir. Burada kişisel verilerin işlenmesi ile istenen amaç arasındaki illiyet bağının değerlendirilmesi gerekmektedir. Veri denetçisi ilk olarak amaçlarına ulaşabilmek için kişisel verilerin mutlaka gerekli olup olmadığını saptamalıdır. Hedeflenen amaca kişisel veriler kullanılmadan ulaşılabilmesi halinde öncelikle bu yolun tercih edilmesi gerekmektedir. Bununla birlikte bazı hallerde kişisel verilerin kullanımı istenen amaca ulaşılması için zorunlu olabilmektedir. Bu gibi zorunluluk hallerinde amaca ulaşmak için gerekli olan en az sayıda verinin kullanılması gerekmektedir²⁷⁸. Örneğin, işverenin iş sözleşmesi çerçevesinde olası işçisinden edinebileceği bilgiler, iş ilişkisi için gerekli olanlar ile sınırlı tutulmalıdır²⁷⁹. Aynı şekilde ücretsiz e-posta hizmet sağlayıcısının gerekli olmamasına rağmen ilgili kişinin yaş, cinsiyet gibi bilgilerini istemesi de asgari sayıda verinin elde edilmesi ilkesine aykırılık teşkil eder²⁸⁰.

C. Kişisel Verilerin Doğru ve Eğer Gerekli İse Güncel Olarak Tutulması İlkesi

Kişisel verilerin doğru olması ilkesine pek çok metinde yer verilmiştir²⁸¹. Kişisel verilerin yanlış tutulması bireyin temel hak ve özgürlüklerini, ekonomik çıkarlarını veya manevi bütünlüğüne zarar verici sonuçlar doğurabilir. Ayrıca bu ilke bireysel katılım ilkelerinden olan erişim hakkı ile yakından ilgilidir. Keza bilgilere ulaşamadığı takdirde bunların doğruluğunun saptanması da olanaksızdır.

²⁷⁸ Nitekim Federal Almanya Veri Koruma Yasası'nın 3a hükmünde de “(...)hiçbir verinin veya olanaklı bulunan en az miktarda kişisel verinin toplanması, işlenmesi veya kullanılması(...)” ifadesine yer verilmiştir. Ayrıntılı bilgi için bkz., Küzeci, **a.g.e.**, s. 203.

²⁷⁹ Başalp, **a.g.e.**, s. 38.

²⁸⁰ Diğer teknoloji ürünleri açısından da konunun değerlendirilmesi gerekmektedir. Örneğin, güvenlik nedeniyle gizli kamera sistemini kullanan bir işletmede kameraların, işletmenin dışını da görüş alanı içine alması durumunda amacı aşan oranda veri toplanması söz konusudur. Bkz., Küzeci, **a.g.e.**, s. 204.

²⁸¹ AB Direktifi, m. 6/f.1/d; 108 sayılı Sözleşme m. 5/d. Ayrıca OECD Rehber İlkeleri'nin 8. paragrafında kişisel verilerin tam olması da zorunluluk olarak öngörülmüştür.

Kişisel verilerin doğru ve güncel tutulması veri denetçisinin yükümlülüklerindendir. Bu noktada AB Direktifi'nde üye devletlerin kişisel verilerin toplanma amaçları veya sonradan işleme için yanlış veya eksik verinin silinmesi veya düzeltilmesi için makul olan bütün adımların atılması gerekliliği göze çarpmaktadır²⁸². Diyebiliriz ki ilgili madde hükmü ile kişisel verilerin doğru ve güncel olarak tutulması ilkesinin veri denetçilerinin zorla ve sürekli olarak ilgili kişilerin bulunduğu yeni durumları araştırmaları olarak algılanmasının önüne geçilmeye çalışılmıştır. Buna göre veri denetçisi yanlış verilerin silinmesine ya da eksikliklerin giderilmesine olanak tanıyan bir sistemi oluşturduğu takdirde bu ilke uyarınca üzerine düşen görevi yerine getirmiş sayılacaktır²⁸³.

D. Amacın Gerektirdiğinden Daha Uzun Süre Tutulmama İlkesi

Kişisel veriler ancak toplanma amaçlarına bağlı olarak ve bu amacın gerektirdiği süre çerçevesinde tutulabilir²⁸⁴. Amaçla bağlılık ilkesinin bileşeni olarak da değerlendirilebilecek amacın gerektirdiğinden daha uzun süre verilerin tutulmama ilkesi, verilerin zaman bakımından kaydedilmesini de sınırlandırmaktadır²⁸⁵. Bu anlamda kişisel verilerin “yeri geldiği zaman” kullanılmak üzere bekletilmesinin önüne geçilmektedir²⁸⁶. Aksi durum haklı gerekçelerle bir kez edinilen kişisel

²⁸² AB Direktifi, m. 6/f.1/d.

²⁸³ Küzeci, **a.g.e.**, s. 209.

²⁸⁴ Kişisel verilerin gerektirdiğinden uzun süre tutulmasına dair düzenlemeler için bkz., AB Direktifi, m. 6/f.1/e, 108 sayılı Sözleşme, m. 5/e, OECD Rehber İlkeleri, par. 8. Bununla birlikte Direktif'in konuya ilişkin düzenlemesinde üye devletlerin uygun güvenceleri sağlamaları kaydıyla bilimsel, tarihi ve istatiki amaçlarla verilerin daha uzun süre saklanması olanaklı kıldığını hatırlatmak isteriz. Bkz., AB Direktifi, m. 6/f.1/e.

²⁸⁵ Şimşek, **a.g.e.**, s. 85, d.n. 385.

²⁸⁶ Nitekim AİHM de kişisel verilerin süresiz olarak tutulmasına dair değerlendirmelerde bulunmuştur. *S ve Marper/Birleşik Krallık* kararında başvuru haklarında daha önce açılan dava sürecinde alınan parmak izlerinin, hücre örneklerinin ve DNA profillerinin beraat etmelerine ve başka bir davada ceza kovuşturmasına yer olmadığına karar verilmesine rağmen süresiz biçimde tutulmasına devam edilmesine itiraz etmişlerdir. Mahkeme, söz konusu verilerin, şüphelinin işlemiş olduğu suçun türü, ağırlığı veya şüphelinin yaşından bağımsız olarak; hapisle cezalandırılmayan hafif suçlar da dahil olmak üzere polis kayıtlarına geçmesi gereken bir suçla ilgili olarak yakalanmış olan bir kişinin parmak izleri ve biyolojik örneklerinin alınması ve daha sonra da muhafaza edilmesini mevcut düzenlemenin verdiği genel yetkilendirme ile mümkün olduğuna yer vermiştir. Muhafaza etme, süreyle sınırlı değildir. Deliller, suç işlediğinden şüphelenilen kişinin, işlediği suçun türü ve ağırlığından bağımsız ve süresiz olarak muhafaza edilmektedirler. Bkz., *S ve Marper/Birleşik Krallık*, b.n. 30462/04, k.t. 04.12.2008. Mahkeme mevcut olayda söz konusu verilerin süresiz olarak

verilerin süreye bağlı olmaksızın kayıt altında tutulmasına yol açacaktır. Bu gibi durumlarda ise bireysel özerklik, bireyin maddi ve manevi bütünlüğü ve özel yaşamın gizliliği hakkı gibi değerler zarar görecektir²⁸⁷.

Nitekim AIHM de kişisel verilerin süresiz olarak tutulmasına dair değerlendirmelerde bulunmuştur. *S ve Marper/Birleşik Krallık* kararında başvuru haklarında daha önce açılan dava sürecinde alınan parmak izlerinin, hücre örneklerinin ve DNA profillerinin beraat etmelerine ve başka bir davada ceza kovuşturmasına yer olmadığına karar verilmesine rağmen süresiz biçimde tutulmasına devam edilmesine itiraz etmişlerdir. Mahkeme, söz konusu verilerin, şüphelinin işlemiş olduğu suçun türü, ağırlığı veya şüphelinin yaşından bağımsız olarak; hapisle cezalandırılmayan hafif suçlar da dahil olmak üzere polis kayıtlarına geçmesi gereken bir suçla ilgili olarak yakalanmış olan bir kişinin parmak izleri ve biyolojik örneklerinin alınması ve daha sonra da muhafaza edilmesini mevcut düzenlemenin verdiği genel yetkilendirme ile mümkün olduğuna yer vermiştir. Muhafaza etme, süreyle sınırlı değildir. Deliller, suç işlediğinden şüphelenilen kişinin, işlediği suçun türü ve ağırlığından bağımsız ve süresiz olarak muhafaza edilmektedirler. Mahkeme mevcut olayda söz konusu verilerin süresiz olarak saklanmasına izin veren uygulamanın AIHS'nin 8. maddesine aykırı olduğuna karar vermiştir²⁸⁸.

III. VERİLERİ İŞLENEN KİŞİLERİN HAKLARI

A. Kişisel Verilerin İşlenmesi Sırasında İlgilinin Bilgilendirilmesi

Kişinin verilerinin işlenmesi hakkında bilgilendirilmesi ile ilgilinin menfaatleri korunmaktadır. Öyle ki ilgili kişi kendisi hakkında veri işlendiğini bilmeden kişisel verilerinin korunmasına yönelik haklarını kullanamaz. Bu anlamda her bireyin kendisi hakkında kimin, hangi verileri, hangi amaçlarla işlediği

saklanmasına izin veren uygulamanın AIHS'nin 8. maddesine aykırı olduğuna karar vermiştir.

²⁸⁷ Küzeci, **a.g.e.**, s. 210.

²⁸⁸ *S. ve Marper/Birleşik Krallık*, b.n. 30462/04, k.t. 04.12.2008.

hususlarında veri denetçilerince bilgilendirilmesi gerekir. İlgilinin bilgilendirilmesi aynı zamanda kamusal organların veri işlem sürecinde şeffaflık ilkesinin gereğidir²⁸⁹.

İlgili kişinin bilgilendirilmesi yükümlülüğü Direktifin 10. ve 11. maddelerinde düzenlenmiştir. Bununla birlikte 108 sayılı Sözleşme'nin 8. maddesinde, OECD Rehber İlkeleri'nin 12. paragrafında, BM Rehber İlkeleri'nden 3. ilkede Direktifte yer aldığı gibi açık ve kapsamlı olmasa da dolaylı olarak ilgili kişinin bilgilendirilmesine yer verilmiştir.

Direktifin 10. maddesi uyarınca bilgiler doğrudan ilgili kişiden elde edildiği durumlarda veri denetçisi veya temsilcisi, ilgili kişinin zaten bunları bildiği durumlar hariç olmak üzere, en azından aşağıdaki bilgileri sunması gerekmektedir;

- Veri denetçisinin veya duruma göre temsilcisinin kimliği,
- Veri işleme amacı,
- Veri alıcıları veya alıcı kategorileri,
- Sorulara cevap vermenin zorunlu veya isteğe bağlı olduğu ve olası bir cevap vermeme durumunun sonuçları,
- İlgili kişinin kişisel verileri hakkında bilgi alma ve düzeltme hakkının mevcut olduğu,
- Veri işlemede hassas kişisel veriler gibi özel bazı durumların varlığı halinde dürüst işlemeyi temin edecek gerekli bilgiler.

Direktif bireye ilişkin kişisel verilerin doğrudan ilgili kişiden değil de üçüncü bir kişiden elde edilmesi durumundaki bilgilendirme yükümlülüğünü ayrıca değerlendirmiştir. Buna göre kişisel veriler ilgili kişiden alınmadığı, başka

²⁸⁹ Şimşek, **a.g.e.**, s. 88.

kaynaklardan elde edildiği durumlarda ilgili kişi bu kapsamda bilgilendirilmeli; eğer ilgili kişiden elde edilen bilgiler üçüncü kişiyle paylaşılmışsa kişi bu konuda da haberdar edilmelidir²⁹⁰.

Bildirim yükümlülüğünün birtakım istisnaları bulunmaktadır. Ancak, belirtmemiz gerekir ki, her halükarda devletin bireyi koruyucu gerekli önlemleri alması gerekmektedir. İstisnai durumlar aşağıdaki gibidir;

- Hakkında kişisel veri toplanan ilgili kişiye bilgi vermenin mümkün olmaması,
- Oransız bir çaba gerektirmesi,
- Verileri kaydetme ve işlemenin yasada açıkça öngörülmesi,
- İstatistiki, tarihi veya bilimsel amaçlarla veri işlenmesi²⁹¹.

B. İlgilinin Bilgilerine Erişim Hakkı

Kişinin verilerinin geleceğini belirleyebilmesi açısından önemli olan diğer bir hakkı ise bilgi edinme hakkıdır. Bilgilere erişim hakkı ilgilinin bilgilendirilmesi ile yakın ilişkilidir. Veri denetçisi ilgili kişiyi veri işleme konusunda bilgilendirmediği takdirde ilgilinin bilgisi dahilinde olmayan bir veri işleme faaliyeti hakkında bilgilere erişim, düzeltme, silme, engelleme gibi haklarını kullanması olanaksızdır²⁹².

İlgili kişinin başka kişi ve kurumların elinde bulunan kişisel verilere erişim hakkı pek çok metinde yer almaktadır. OECD Rehber İlkeleri'nin 13. ve 14. paragraflarında, 108 sayılı Sözleşme'nin 8. maddesinde ve BM Rehber İlkeleri'nden 4. ilkede konu ile ilgili düzenlemelere yer verilmiştir. AİHM'in de kişisel verilere erişim

²⁹⁰ AB Direktifi, m. 11.

²⁹¹ AB Direktifi, m. 11/f.2.

²⁹² Şimşek, **a.g.e.**, s. 90.

hakkını 8. maddesi kapsamında ele aldığı kararları mevcuttur²⁹³.

Bilgilere erişim hakkı, Direktif'in 12. maddesinde de düzenlenmektedir²⁹⁴. İlgili düzenlemeye göre birey serbestçe ve engellenmeksizin, aşırı gecikme ve masraf olmaksızın, makul aralıklarla veri denetçisinden şu hususlarda bilgi edinme hakkına sahiptir;

- Veri denetçisi nezdinde kendisine ilişkin verilerin işlenip işlenmediğinin teyidi, veri işlemenin amacı, ilgili verilerin kategorisi, verinin açıklandığı alıcılar ya da alıcı kategorileri,

- İşlenmekte olan verinin kaynağına ilişkin her türlü bilgi,

- Kendisini ilgilendiren verilerin otomatik veri işleme tabi tutulmasının mantıksal yapısı ve konusu.

Bilgilere erişim hakkı uygulamada bazı sorunları barındırmaktadır. Bunlardan bazıları “makul”lük derecesinin nasıl belirlenmesi gerektiği, ne oranda bilginin

²⁹³ AİHM'nin kişisel verilere erişim hakkına dair verdiği ilk kararı *Leander/İsveç* kararıdır. Bkz. *Leander/İsveç*, b.n. 92448/81, k.t. 26.03.1987. Mevcut olayda Mahkeme, başvuru hakkında bilgilerin polis kayıtlarında tutulması ve ilgili makamlara verilmesini, ayrıca başvurucuya bu bilgilere itiraz hakkı verilmemesini 8. madde kapsamında müdahale oluşturduğuna karar vermiştir. Ancak Mahkeme'ye göre ifade özgürlüğünü güvence altına alan AİHS'nin 10. maddesi ne ilgiliye kişisel durumu hakkında bilginin yer aldığı sicile erişim hakkı tanımaktadır ne de devlete bu tür bir bilgiyi ilgiliye verme gerekliliğini yüklemektedir. Bkz., *Leander/İsveç*, para. 74. İçtihatlarına baktığımızda AİHM mevcut, erişilebilir nitelikte bir bilgiye erişimin devlet tarafından engellenmesini AİHS'nin 10. maddesinde güvence altına alınan ifade özgürlüğünü ihlali olarak yorumlamaktadır. Ancak devlet tarafından tutulan kişisel nitelikteki bir kayda erişimin engellenmesi 10. maddenin ihlali olarak görülemez. Ancak Mahkeme, daha sonra verdiği kararlarda bilgilere erişim hakkını AİHS 8. madde ile güvence altına alınan hakka dair devletin pozitif yükümlülüğü kapsamında değerlendirmiştir. Mahkeme'nin bu değerlendirme kapsamında verdiği ilk kararı *Gaskin/Birleşik Krallık* kararıdır. Daha sonraki başka kararlarında da Mahkeme bu bakış açısını yinelemiş ve devlet tarafından tutulan kişisel verilere erişim taleplerini 8. madde kapsamında değerlendirmiştir. Bkz., *M.G./Birleşik Krallık*, b.n.39393/98, k.t.24.09.2002; *Rotaru/Romanya*, b.n.28341/95, k.t.04.05.2000; *Roche/Birleşik Krallık*, b.n.32555/96, k.t.19.10.2005; *Amann/İsviçre*, b.n.27798/95, k.t.16.02.2000; *Martin/Birleşik Krallık*, b.n.27533/95, k.t.28.02.1996; *Odievre/Fransa*, b.n.42326/98, k.t.13.02.2003; *McGinley ve Egan/Birleşik Krallık*, b.n.21825/93, k.t.09.06.1998. Konu ile ilgili ayrıntılı bilgi için bkz., Cavidan Soykan, “Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C.56, S. 2, s. 8.

²⁹⁴ Bilgilere erişim hakkına dair Direktif'teki düzenleme, diğer metinlere nazaran daha geniş kapsamlıdır. Bkz. Lee A. Bygrave, **Data Protection Law, (Approaching Its Rationale, Logic and Limits)**, Hollanda, 2002 s. 65'ten aktaran Küzeci, **a.g.e.**, s. 215.

sağlanması gerektiği, erişimi istenilen bilginin başkalarına ilişkin kişisel verileri de içermesi halinde bunlardan hangilerinin çıkartılması gerektiği gibi konulardır²⁹⁵. Ayrıca burada bilginin ilgili kişiye anlaşılır bir biçimde sunulması gerekliliğinin de üzerinde durulması gerekmektedir. Buna göre elektronik işlemler söz konusu olduğunda ilgilinin teknik bilgiden yoksun olduğu varsayılmalıdır. Olası elektronik işlemlerde buradan yola çıkılarak basit bir bilgi verme yolu seçilmelidir. Verilerin otomatik olarak işlenmesi halinde ise sorumlular açıklamalarında ticari sır niteliğindeki bilgiler haricinde ve fikri mülkiyet hukukunun izin verdiği ölçüde ilgili kişiyi bilgilendirme yükümlülüğü ile bağlıdır²⁹⁶.

C. İlgilinin Verilerini Düzeltme Hakkı

Direktifte bireyin kişisel verilerinin işlenmesine bireysel katılımına ilişkin olarak verilerini düzeltme hakkına yer verilmiştir. Söz konusu hak doğrultusunda ilgilinin verilerin işlenmesinin Direktif hükümlerine uymaması halinde özellikle de eksik ve yanlış olan verilerin düzeltilmesini, silinmesini veya engellenmesini isteme hakkı bulunmaktadır. Bu hak ilgilinin bilgilerine erişim hakkı ile ilişkilidir. Ancak, düzeltme hakkının kullanılması için bilgilere erişim hakkının sağlanmış olması gerekli değildir. İlgili kişi herhangi bir şekilde kendisine ilişkin olarak eksik veya hukuka aykırı bir verinin bulunduğunu öğrendiği takdirde bu verileri düzeltme hakkını kullanabilir²⁹⁷. Düzeltme hakkı ayrıca verilerin doğru ve güncel olması ilkesi ile de yakın ilişkilendirilmektedir²⁹⁸.

Düzeltme, silme ve engelleme etkinlikleri Direktifte tanımlanmamıştır. Düzeltme kavramının şekli bir tanımının yokluğu ile birlikte 12. maddeye göre verilerin maddi olarak doğru ve gerçek olmadığı hallerde düzeltme hakkından bahsedilebilecektir. Sildirme hakkı söz konusu olduğu takdirde veri denetçisinin kişisel veriler üzerinde tasarrufunun önlenmesi amaçlanmaktadır. Bu halde

²⁹⁵ Küzeci, **a.g.e.**, s.216.

²⁹⁶ AB Direktifi, 41 numaralı gerekçe.

²⁹⁷ Şimşek, **a.g.e.**, s. 92.

²⁹⁸ Küzeci, **a.g.e.**, s. 217.

dürüstlüğe ve hukuka aykırı veya yetkisiz veri işlemlerinde sildirme hakkı söz konusu olmaktadır. Verinin doğruluğunun ihtilaflı olduğu hallerde ise söz konusu kişisel verilerin kullanılmasının engellenmesi yoluna gidilecektir²⁹⁹.

D. İlgilinin İtiraz Hakkı

Bireyin kişisel verilerinin işlenmesi sırasında hukuka aykırı veri işlem faaliyetlerine yönelik diğer bir hakkı ise itiraz hakkıdır. Direktif'in 14. maddesine göre üye devletler (i) genel olarak verilerin işlenmesine dair asgari bir itiraz hakkı ile (ii) ilgili kişinin doğrudan pazarlama işlemlerine karşı itiraz etme hakkına yer vermelidir³⁰⁰.

Direktif'e göre kamusal görevlerin ifası ya da haklı çıkarların korunması gerekçeleriyle verileri işlenen kişiler, ulusal hukuklarda aksi açıkça öngörülmediği sürece, verilerin işlenmesine itiraz edebilir³⁰¹. Gerekçeli bir itiraz halinde itiraza konu olan veriler yapılan işlemlerde dikkate alınmayacaktır. Direktif'in itiraz hakkına yer verdiği diğer bir durum ise doğrudan pazarlama işlemleridir. Buna göre ilgili kişinin verilerinin doğrudan pazarlama amacıyla işlenmesi durumuna karşı ilgiliye bedelsiz itiraz hakkı tanınmalıdır. Ayrıca kişisel verilerin üçüncü şahıslara ilk kez ifşa edilmesinden veya doğrudan pazarlama amaçları için üçüncü şahıslar adına kullanılmadan önce ilgilinin bilgilendirilme ve bu açıklamalara veya kullanımlara bedelsiz olarak itiraz etme hakkı vardır. Söz konusu hak konusunda ilgilinin bilgilendirilmesi gerekmektedir.

²⁹⁹ **Ibid**, s. 93.

³⁰⁰ 108 sayılı Sözleşme'de ise ilgilinin kanun yollarına başvurma hakkına sahip olmasına yer verilmiştir. Söz konusu hakkın düzenlendiği 8. maddeye göre kişinin kendisi hakkında veri bulunup bulunmadığı konusundaki onay talebinin veya gerekli durumlarda bildirim, düzeltme veya silme talebinin yerine getirilmemesi halinde kanun yoluna başvurma hakkı öngörülmelidir.

³⁰¹ Söz konusu gerekçeler Direktif'in 7. maddesinin e ve f bentlerinde yer alan hükümlerdir. Asgari düzeyde bir itiraz hakkının gerekçesi olan bu özel durumlara ek olarak üye devletler daha geniş itiraz hakkını tanıyabileceklerdir. Ayrıca ilgili hükümde yer alan üye devletlerin ilgilinin itiraz hakkını sınırlayabilecekleri ve hatta bazı durumlarda kaldırabileceklerine dair düzenlemenin ele alınması gerekmektedir. Üye devletlerce getirilebilecek bu türden bir düzenlemenin Direktif'in amacı doğrultusunda ihdas edilmesi gerektiği açıktır. İtiraz hakkına dair bir sınırlama veya bu hakkın bazı durumlarda kaldırılması Direktif ile sağlanmaya çalışılan temel hak ve özgürlüklerin korunmasına aykırılık teşkil etmemelidir.

E. İlgilinin Otomatik Kararların Konusu Olmama Hakkı

Kişinin bireysel özerkliğinin temini olan ilgilinin otomatik kararların konusu olmama hakkı Direktif'in 15. maddesinde düzenlenmiştir³⁰². Böyle bir hakkın yoksunluğu bu türdeki kararlar nedeniyle bireyin kişilik hakkının zarar görmesi gibi ciddi sonuçlar doğuracaktır³⁰³. Her bireye işindeki performansı, kredi itibarı, güvenilirliği ve davranışları gibi kişisel durumların değerlendirilmesi amacıyla yalnızca otomatikleştirilmiş veri işlemesine dayanan ve bireyi önemli derecede etkileyen ve kendisine yönelik hukuksal sonuçlar yaratan karara bağlı kalmama hakkı tanınmaktadır³⁰⁴. Kişiye otomatikleştirilmiş kararların konusu olmama seçeneğinden kaçınmak için kararda insan müdahalesinin bulunması gerekmektedir. Örneğin kredi istemleri veya iş başvurusunda bulunan kişilere yönelik psikolojik testler insan müdahalesi olmaksızın, yalnızca bir bilgisayar sisteminin değerlendirilmesine tabi kılınamaz³⁰⁵. Kişilerin kredi istemlerinin değerlendirilmesi tipik örneğine ilaveten tıbbi teşhis sistemleri veya uzaktan ödeme sistemleri de otomatik kararların konusu olmama hakkı kapsamına girebilir³⁰⁶.

Genel kural otomatik işlem sonucunda oluşturulan profillerin kişi hakkında karar doğurmaması olmak ile birlikte bazı özel hallerde kişinin otomatik surette verilen kararlara tabi kılınması mümkündür. Bu durumlardan ilki, ilgilinin meşru çıkarlarının korunması için tatmin edici veya uygun önlemlerin şartı ile sözleşme ilişkisinden dolayı bu kararın alınmasıdır³⁰⁷. İlgilinin otomatik kararların konusu

³⁰² İlgili hüküm, 1978 tarihli eski Fransız Veri Koruma Yasası'ndan Direktif'e aktarılmıştır. Bkz., Rupert Battcock, "Data Protection: where next?", *International Journal of Law and Informational Technology*, C.3, S.2, s. 164.

³⁰³ Küzeci, *a.g.e.*, s. 219. Otomatikleştirilmiş veri işlemesinde her bir rutin işlem verinin tahrifatı tehlikesini daha da artırmaktadır. Örneğin ABD'de huzurevinde yaşayan yaşlı bir bayana sağlanan sağlık yardımına sosyal yardım listesi ve banka hesapları arasındaki otomatik eşleştirme sonuçlarına bağlı olarak son verilmiştir. Gerekçe olarak da bu otomatikleştirilmiş veri işlemesi sonucunda sağlık yardımı için gerekli limitin aşıldığı gösterilmiştir. Ancak banka hesabı kanuna göre varlık hesaplamasında değerlendirme dışı tutulması gereken cenaze masraflarını içermekteydi. Bkz., Spiros Simitis, "Reviewing Privacy In an Information Society", s. 718.

³⁰⁴ Madde hükmünde sayılan durumlar sınırlı sayıda değildir. Bkz., Başalp, *a.g.e.*, s. 54.

³⁰⁵ *A.g.e.*, s.54.

³⁰⁶ Battcock, *a.g.m.*, s. 165.

³⁰⁷ AB Direktifi, m. 15/f.2/a.

olabilmesine diğerk bir istisnai hal ise bunun veriye konu olan kişinin meşru çıkarlarını korumak için önlemler saptayan bir yasa tarafından öngörölmesidir³⁰⁸.

IV. VERİLERİN İŞLENMESİNE İLGİLİNİN RIZASI

Kişisel verilerin toplanması, işlenmesi ve saklanması işlemlerinden önce ilgili kişinin rızasının alınması gereklidir. Bireyin rıza vermesi koşulu, kişisel verilerin korunmasına ilişkin ulusal düzenlemelerde kişisel verilerin işlenmesinin hukuka uygunluk sebeplerinden biri olarak sayılmıştır. AB Temel Haklar Şartı'nda da kişinin rıza beyanında bulunması ilkesine yer verilmiş, AB Direktifi'nde de ilgili kişinin rızası veri işlemeyi meşru kılan durumlar içerisinde sayılmıştır³⁰⁹. 2010 Anayasa değişikliği kapsamında “Özel Hayatın Gizliliği” başlıklı 20 maddeye eklenen kişisel verilerin korunmasına ilişkin hükümde “*kişisel veriler, ancak kanunda öngörölülen hallerde veya kişinin açık rızasıyla işlenebilir*” denilerek bu ilkeye yer verilmiştir.

A. Rıza Beyanının Önemi

Kişisel verilerin korunması hukukunda ilgili kişinin rızasının alınması veri işleme sürecine katılmasını sağlayan önemli unsurlardan biridir. “Bilgilerin geleceğini belirleme” düşüncesinin bir yansıması olarak kabul edilen rıza beyanı, ilgili kişinin kendisiyle ilgili veriler üzerinde denetimini sağlamaktadır³¹⁰. İşte bu nedenle kişisel verilerin korunması hakkının bir insan hakkı olduğu görüşü rıza beyanı ile etkinlik kazanmaktadır. Bir görüşe göre, bireyin kişisel verilerinin işlenmesine rıza göstermesi bireyin, kişisel verilerinin korunması hakkının kullanılmasını ifade etmektedir. Diğerk bir görüşe göre ise kişinin verilerinin işlenmesine vermiş olduğu

³⁰⁸ AB Direktifi, m. 15/f.2/b.

³⁰⁹ AB Temel Haklar Şartı, m. 8; AB Direktifi m. 2/h, m. 7/a. Bu dipnot bağlamında 108 sayılı Sözleşme'de rıza koşulu ile ilgili herhangi bir hükme yer verilmediğini belirtmek isteriz. Bunun nedeni, AB Direktifi'nin aksine, 108 sayılı Sözleşme'de kişisel verilerin işlenmesini meşru kılan durumların ayrıca sayılmamasıdır. Yine de Bakanlar Komitesi konuya ilişkin verdikleri tavsiye kararlarında rıza koşuluna değinmişlerdir. Bkz., Article 29 Data Protection Working Party, **Opinion 15/2011 on the definition of consent**, 01197/11/EN WP187, 13.07.2011, s. 4, d.n. 6.

³¹⁰ Bergkamp- Dhont, **a.g.m.**, s. 78.

rıza beyanı bireyin, kişisel verilerinin korunması hakkından vazgeçmesidir³¹¹. Konuya hangi noktadan yaklaşılsa yaklaşılsın ortak amaç rıza beyanı ile bireyin veri işleme faaliyetlerinin basit bir objesi olmaktan korunması ve kişisel veriler üzerindeki denetim hakkının sağlamaştırılmasıdır. Öyle ki rıza beyanı, kişisel verilerin işlenmesinde hukuka uygunluk sebebi olmasının yanında verilerin işlenmesinde uygulanacak ilkelerin en başında gelmektedir.

Amerikan hukuku ve Kıta Avrupası hukukunda kişisel verilerin korunmasına dair yaklaşım farklılığı rıza beyanı koşulunda da etkisini göstermektedir. Amerikan hukukunda kişisel verilerin korunması müzakere edilebilir bir çıkar olarak görülmekte ve bundan kişi verilerin korunmasından feragat edebilmektedir. Ancak, bu durum kişisel verilerin korunmasını temel hak olarak benimseyen Kıta Avrupa'sında ise geçerli değildir. Kişisel verilerin korunmasının temel hak alanı olarak açıklandığı bu durumda ilgili kişi, haklarının ihlali sayılacak hareketlere rıza gösteremeyecektir³¹².

Kişisel verilerinin işlenmesine dair kişinin rızasının alınması kişisel verilerin hukuka ve dürüstlük kurallarına uygun işlenmesi ilkesi ile işlenme amacına bağlılık ilkesi gibi veri kalitesine dair ilkeleri ortadan kaldırmamaktadır. Bunların birlikte değerlendirilmesi gerekmektedir.

B. Rıza Beyanının Niteliği

Rıza beyanın geçerli sayılabilmesi için bazı gerekliliklerin karşılanması gerekir. Bu noktada AB Direktifi'ne başvurabiliriz. Nitekim AB Direktifi'nin 2. maddesinin h bendinde rızanın hukuki tanımı yapılmıştır. Buna göre rıza beyanı, hiçbir baskıya maruz kalmaksızın mevcut durumun bilincinde olarak somut işlemle sınırlı yapılan her türlü irade açıklamasıdır. Ayrıca yine Direktif'e göre rıza beyanının hukuka uygunluk koşulunu sağlayabilmesi için ilgili kişinin rızasının “tereddüde yer

³¹¹ Şimşek, **a.g.e.**, s. 108

³¹² Bergkamp-Johnt, **a.g.m.**, s. 78.

bırakmayacak nitelikte” olması gerekir³¹³. Ancak, hassas kişisel verilerin söz konusu olduğu durumlarda ise rızanın “açık” olması aranmaktadır³¹⁴.

Direktife göre, ilgili kişinin rıza gösterip göstermediği konusunda herhangi bir şüphe olmamalıdır. Rızanın tereddüde yer bırakmayacak nitelikte olması, hem açık hem de örtülü beyanın kabulünü gerektirir. Nitekim açık irade beyanı hukuki sonuç hakkındaki arzuyu tereddüde yer vermeyecek şekilde açıklayan beyandır. Şüphesiz ki açık irade beyanı, aranan ölçütü karşılamaktadır. Örtülü rıza beyanında ise kişinin beyanda bulunma arzusunu başka davranış biçimleriyle yansıtmakta, hal ve şartlara göre değerlendirilen bu davranış biçimleri kanaat verici bir davranışı ortaya koymaktadır³¹⁵. Beyanda bulunma arzusu hal ve şartlara göre değerlendirildiğinde kanaat verici bir davranışı ortaya çıkarıyorsa açık rıza beyanı gibi örtülü rıza beyanı da ölçütü karşılamaktadır. Burada ilgili kişinin susmasının nasıl değerlendirileceği tartışılmaktadır. Örneğin bir şirketin müşterilerine 2 hafta içerisinde itiraz etmedikleri takdirde kişisel verilerin öngörülen bir diğer şirkete devredileceğine dair bir bildirimde bulunduğunu düşünelim. Bu bildirimde de şirketin müşterilerinden yüzde 10'luk bir kısmının yanıt vermesi üzerine müşterilerden geri kalan yüzde 90'lık bir kesimin herhangi bir yanıt vermemesi, susmaları kişisel verilerinin devrine onay verdikleri şeklinde değerlendirilmeli midir? Burada susma dışında rıza beyanına dair herhangi bir açık belirti yoktur³¹⁶. Diyebiliriz ki ilgili kişinin susması, başka herhangi bir belirti ile desteklenmediği müddetçe rızanın varlığı için yeterli değildir.

Rıza, ilgili kişinin özgür iradesi sonucu verilmiş olmalıdır. Bu, kişinin rızasını hiçbir etki altında kalmadan vermesine bağlıdır. Kişi, verilerini işlenmesine rıza gösterip göstermeme konusunda gerçek bir seçim hakkı olması gerekir. Bu ilgili kişi

³¹³ AB Direktifi, m. 7/a.

³¹⁴ Ayrıntılı bilgi için bkz., Çalışmamızın “*Kişisel Verilerin Korunması Hakkına Özgü İlkeler*” adlı İkinci Bölümü, IV numaralı “*Hassas Verilerin Özel Olarak Korunması*” başlığı.

³¹⁵ Mustafa Dural ve Suat Sarı, **Türk Özel Hukuku Cilt I Temel Kavramlar ve Medeni Kanunun Başlangıç Hükümleri**, İstanbul, 2006, s. 166.

³¹⁶ Article 29 Data Protection Working Party, **Opinion 15/2011 on the definition of consent**, 13.07.2011, 01197/11/EN WP187, s. 12.

ile veri denetçisi arasındaki hiyerarşik ilişki, veri denetçisinin piyasa gücü veya veri denetçisinin hiç kimsenin sunmadığı hizmeti sunması gibi nedenler ile ortadan kalkabilmektedir. Bu duruma en basit örnek işçi ile işveren arasındaki ilişkidir. Örneğin işveren, işçiden kendisine ait sağlık bilgilerini istediğinde kural olarak işçinin söz konusu bilgilerin kişisel veri niteliği olduğundan bahisle işlenmemesini isteme hakkına sahiptir. Bu durumda işçi, iş olanağını kaybetme korkusuyla rızasını baskı altında vermiş olabileceği göz önüne alınmalıdır. Bu amaçla ek bazı güvencelerin sağlanması gerekmektedir. Rızanın özgür irade haricinde verilmiş olabileceği ihtimaline diğer bir durum ise ilgili kişinin veri denetçisine önemli oranda bağlı olmasıdır. Örneğin doktor ile hasta ilişkisinde hastaya, verilerinin işlenmesine rıza göstermemesinin tedavisini etkilemeyeceği kendisine açıkça belirtilmelidir³¹⁷.

Rızanın kişinin özgür iradesinin sonucunda verilmemiş olduğuna diğer bir örnek ise reddin bir yaptırımının bulunmasıdır. Örneğin sözleşmenin bir koşulu olarak belirtilen rıza, özgürce verilmiş sayılamayacaktır. Ancak, bu durum söz konusu olduğunda rıza göstermeme sonucunda karşılaşılabilecek külfetin ağırlığına bakmak gerekir. Eğer külfet hafif ise rıza, özgür iradenin ürünüdür. Örneğin ücretsiz elektronik posta hizmetlerinden yararlanmak için çerezlere (cookies) izin vermek zorunlu olabilir. Bu durumda aynı hizmet başka sitelerden bu sefer çerezlere izin verme yükümlülüğü olmaksızın sağlanabiliyorsa, önceki durum için rızanın özgürce verilmiş olduğu söylenebilir³¹⁸.

Rıza beyanı ile ilgili bir başka unsur ise bunun somut veri işlem faaliyetine ilişkin olmasıdır. Buna göre rızanın belirli bir duruma özgülenmiş olması gerekmektedir. Kişiye veri işlemenin içeriği, amacı, bu işlemin süresi, verilerin nerelerde kullanılacağı, hakkında ayrıntılı bilgi verilmelidir. Yani kişinin neye rıza gösterdiği konusunda bilgilendirilmiş olması gereklidir³¹⁹. Genel rıza beyanında bulunulmuş olması ilgili kişiden rızanın alınması anlamına gelmemektedir. Ayrıca

³¹⁷Bergkamp-Johnt, **a.g.m.**, s. 77.

³¹⁸**A.g.m.**, s. 78.

³¹⁹Küzeci, **a.g.e.**, s. 223.

ilgili kişinin neye rıza gösterdiği konusunda aydınlatılması sırasında anlaşılır bir dil kullanılmalıdır. Kişinin anlayamayacağı terimlerin ya da okuyamayacağı kadar küçük puntoların yer aldığı formlar aydınlatılmış rıza beyanı olarak kabul edilemez³²⁰.

Rıza beyanının şekline dair koşullara baktığımızda AB Direktifi'nde buna dair herhangi bir tanım yapılmadığını görürüz. Buna göre, yukarıda belirttiğimiz koşulları taşıması halinde “*her türlü işareti içeren irade*”, rıza beyanı olarak kabul edilecektir. Bu anlamda yazılı, sözlü veya elektronik ortamda açıklanmış bir rıza beyanı geçerli kabul edilecektir. Her halde rızanın yazılı olarak verilmesi ispat açısından kolaylık sağlamaktadır. Bununla birlikte İtalya ve Almanya'daki konuya ilişkin düzenlemelerde rızanın yazılı olması gerektiği aranmıştır³²¹.

Kişinin veri işlem faaliyetine ne zaman onay verdiği önemlidir. Buna göre kişinin onay verdiği tarihten sonraki veri işlem faaliyetleri hukuka uygun kabul edilecektir. Ayrıca kişi, kişisel verilerin işlenmesine ilişkin rıza beyanını her zaman geri alabilir.

V. HASSAS VERİLERİN ÖZEL OLARAK KORUNMASI

Verilerin işlenmesinden doğacak zarar ile yarar arasında bir dengenin kurulması zorunludur³²². Bazı türden verilerin işlenmesinin ise diğerlerine nazaran daha ağır zarar potansiyeli olduğu kabul edilmektedir. İşte bu nedenle kişisel verilerin korunmasına ilişkin düzenlemelerde özen gösterilmesi gerekli bir konu olan hassas veriler ve bunların işlenmesine yer verilmiştir. Bu anlamda hassas verilerin işlenmesi ilgili kişinin ayrımcılık başta olmak üzere daha ciddi zararlar ile karşı

³²⁰ Bu noktada genel işlem şartlarının içinde yer alan veri koruması şartlarının rıza beyanı olarak kabul edilip edilmeyeceğinin değerlendirilmesi gerekmektedir. Bu şekilde ilgili kişinin okuyamayacağı kadar küçük puntolarla sözleşmenin içine sıkıştırılmış ve bundan dolayı da kişinin gözünden kaçabilecek ifadeler olduğundan bahisle bu durum aydınlatılmış rıza beyanı olarak kabul edilemez. Aynı doğrultuda düzenleme için bkz., Federal Almanya Veri Koruma Yasası, m. 4/a/1.

³²¹ Korff, “EC Study on Implementation of Data Protection Directive-Comparative Summary of National Laws”, s. 32.

³²² Küzeci, a.g.e., s. 234.

karşıya kalmasına neden olabileceğinden bu türden veriler, diğerlerine nazaran daha yüksek oranda korumayı gerektirmektedir³²³. İşte, bu ilke ile de hassas sayılan bazı veri türleri diğerlerine göre özellikli ve kapsamlı bir koruma altına alınmaya çalışılmıştır.

A. Hassas Veri Türleri

Pek çok uluslararası metinde hassas verilerin özel olarak korunması gerektiğine dair düzenlemeler yer almaktadır³²⁴. Baktığımızda BM Rehber İlkeleri³²⁵, 108 sayılı Sözleşme³²⁶, AB Direktifi³²⁷, hassas veriler için özel koruma sağlanmasına dair düzenlemelere yer vermişken OECD Rehber İlkeleri ise bu türden verilere özel bir koruma öngörmemektedir³²⁸.

AB Direktifi'nin 8. maddesinin 1. fıkrasına göre işlenmesi kural olarak yasak olan özel kategorideki kişisel veriler ise şunlardır;

-İrksal veya etnik köken,

³²³ Direktif'in 33. numaralı gerekçesi de bazı verilerin işlenmesinin ilgili kişilerin temel hak ve hürriyetleri ile mahremiyetlerini ihlal edebilecek türde olduklarını vurgulamıştır. Bununla birlikte kişisel verilerin kişi açısından oluşturabileceği olası zararların ağırlığına göre belirli veri kategorilerine yönelik özel korumanın öngörülmesi yaklaşımı ilk etapta genel kabul görmemiştir. Federal Anayasa Mahkemesi'nin 1983 yılında verdiği Nüfus Kararı'nda kişisel verilerin “önemliler” ve “daha az önemliler” gibi bir ayrıma tabi tutulamayacağı karara bağlanmıştır. Nitekim başka bilgilerle bağlantı kurularak yeni verilerin yaratılması her zaman olanaklıdır. Direktif'e uyum sağlamak amacıyla gerekli yasa değişikliklerinin yapılmasından önce Avusturya ve Alman hukukunda bu yaklaşım benimsenmiştir. Ancak diyebiliriz ki, verilerin işlenmesinden doğacak zarar ile yarar arasındaki dengenin sağlanabilmesi açısından bazı verilerin diğerlerine göre daha yüksek oranda korunması yerindedir. Bkz., Küzeci, **a.g.e.**, s. 234. Ayrıca bazı verilerin “hassas” olarak değerlendirilmesine ilişkin bkz., Spiros Simitis, “*Revisiting Sensitive Data*”, (Çevrimiçi) http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Simitis_1999.pdf,

01.05.2013. (Bundan böyle “**Revisiting Sensitive Data**” olarak anılacaktır).

³²⁴ Ulusal veri koruma kanunlarında konuya ilişkin karşılaştırmalı değerlendirme için bkz., Korff, “**EC Study on the Implementation of Data Protection Directive**”.

³²⁵ BM Rehber İlkeleri, 5. ilke.

³²⁶ 108 sayılı Sözleşme, m. 6

³²⁷ AB Direktifi, m. 8. Direktif'te hassas veri kategorileri düzenlemesine ilişkin ayrıntılı değerlendirme için bkz., Cemil Kaya, “*Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi*”, **İÜHFİM**, C. LXIX, S. 1-2, s. 317-334.

³²⁸ OECD Rehber İlkeleri'nde bu türden verilere özel bir korumanın öngörülmemiş olması evrensel düzeyde “hassas” olarak nitelendirilebilecek bir veri kategorisi bulunmadığı yönündeki görüş ile temellendirilmiştir. Bkz., OECD Rehber İlkeleri, para.51.

- Siyasal görüş,
- Dini ya da felsefi inancı,
- Sendika üyeliği,
- Sağlık ya da cinsel yaşamı³²⁹.

Direktif'e göre hassas veriler yukarıdaki gibi ve sınırlı sayıda sayılmakla birlikte suçlar, mahkumiyetler ve güvenlik tedbirleri ile ilgili verilerin de hassas veri kapsamına girdiği söylenebilir. Ancak, idari ve adli mahkumiyetlere ilişkin verilerin bu kapsamda sayılması üye devletlerin takdirindedir³³⁰.

108 sayılı Sözleşme'nin 6. maddesine göre ise kişinin etnik kökeni, politik görüşleri, dini veya diğer kanaatleri ortaya çıkartacak kişisel veriler ile sağlık ve cinsel yaşamı ilgilendiren veriler ile ceza mahkumiyetine ilişkin veriler özel olarak korunmuştur. Görüleceği üzere Direktif'in aksine 108 sayılı Sözleşme sendika üyeliği ve kişinin etnik kökenine ilişkin verileri hassas veriler kategorisinden saymamıştır. Ayrıca Direktifte yer alan hassas veriler sınırlı sayıda sayılmış olmasına karşın 108 sayılı Sözleşme'de yer verilen hassas veri kategorileri sadece belirleyici niteliktedirler³³¹.

Gördüğümüz gibi sayımdaki farklılıklara rağmen genel olarak yukarıdaki konulara ilişkin bilgiler hassas veriler olarak kabul edilmektedir³³². Ancak, kişisel

³²⁹ Burada AAD'nin hassas veri kategorilerine ilişkin tutumunu hatırlatmak isteriz. Buna göre AAD, 8/f.1 hükmünün geniş yorumlanması gerektiğine dair bir tutum sergilemiştir. Divan, sağlık verilerinin kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgiyi içerdiğinden yola çıkarak önüne gelen olayda kişinin ayağını incitmesine ilişkin bilgiyi sağlık verisi kapsamında değerlendirmiştir. Bkz., Bodil Lindqvist, C-101/01, 06.01.2003, para. 50.

³³⁰ AB Direktifi, m. 8/f.5.

³³¹ Karen McCullagh, "Data Sensivity: resolving the conundrum", **Journal of International Commercial Law and Technology**, C. 2, S. 4, s.192. Ayrıca belirtmemiz gerekir ki, BM Rehber İlkeleri'nde de sendika üyeliğinin yanında her türlü dernek üyeliği, kişinin etnik kökeni ve ten rengine ilişkin bilgiler de hassas veri kategorisinde sayılmıştır.

³³² Bu dipnot bağlamında bazı veri kategorilerinin işlenmesinin diğer verilere nazaran ayrımcılık başta olmak üzere daha ciddi zararlara yol açabileceği görüşünün genel kabul görmediğini de belirtmek isteriz. Federal Almanya Anayasa Mahkemesi 1983'te verdiği Nüfus Sayım Kararı'nda kişiye ilişkin bilgilerin önemli veya önemsiz olarak ayrılmasının yanıltıcı olduğunu vurgulamıştır. Mahkemeye göre

verilerin korunmasına dair düzenlemelerde hassas veri türlerinin sayılması belirsizlikleri ortadan kaldırmamaktadır³³³. Bazı hallerde hassas veri türleri kolayca örneklendirilebilmektedir. Örneğin işverenin çalışanlarının sendika üyesi olduklarına dair kaydı, bir yolcu için tekerlekli sandalye erişimi gerektiğine dair uçuş bilgisi kaydı veya bir hotel müşterisinin dini inancına uygun yemek tercihinin gösteren bilgi kayıtları şüphesizdir ki hassas veri türleri kapsamındadırlar. Diğer taraftan bazı hallerde kişilere ilişkin bilgilerin hassas veri türü kapsamında sayılıp sayılmaması gerektiği belirli olmayabilir. Kişinin internette evinin bulunduğu yere yakın bir Bapstist Kilise araması halinde internette çevrimiçi araştırma imkanı sunan şirketin bu kişi hakkında hassas veri işlediğinin kabul edilmesi mi gerektiği veya kişinin dinsel inancını yansıtan bir adının olması bu duruma örnektir. Bu durumlarda şu sorunun değerlendirilmesi gerekmektedir. Bir bilginin yalnızca hassas veri kategorisinde yer alması mı yoksa bilginin öz olarak hassas olması mı gerekmektedir. O halde bir kişinin dinsel inancını yansıtan adının olması örneğinden yol alırsak burada değerlendirme yapılırken burada yalnızca o dini inanca sahip tüketicilere yönelik ilanlar gibi ismin içeriğinin mi kullanıldığı veya yalnızca bir isim veri tabanında mı yer aldığı göz önünde tutulmalıdır³³⁴. Nitekim İngiltere'de görülen *Naomi Campbell/MGN* davasında da mahkeme benzer yaklaşımı sergilemiştir. Anılan davada Bayan Campbell'in fotoğraflarının onun etnik kökenine ilişkin hassas verileri içerdiğini ancak, bunun fotoğrafların yayınlanma amacı ile ilişkili olmadığına karar vermiştir³³⁵. Ayrıca AAD'nin *Lindqvist* kararı da hassas veri kavramına dair yaptığı değerlendirme de unutulmamalıdır. Divan hassas veri kategorisine dair geliştirdiği yorumda AB Direktifi'nin amaçlarına atıfta bulunmuş ve Direktif'in 8. maddesinin 1. fıkrasının geniş yorumlanması gerektiğine ve bu kapsamda örneğin sağlık verilerinin

ilk aşamada önemsiz gibi görünen verilerin başka bilgiler ile bağlantı kurulması ve yeni verilen yaratılması her zaman olanaklıdır. Karar için bkz., BverfGE, 65, 1-Volkszählung. Aynı şekilde Avusturya'da da Direktif öncesi düzenlemelerde aynı yaklaşım benimsenmiştir. Ancak Direktif'e uyum zorunluluğu nedeniyle bu yaklaşım bırakılmıştır. Bkz., Küzeci, **a.g.e.**, s. 233.

³³³Kaya, **a.g.m.** s. 322.

³³⁴Peter Carey, **Data Protection A Practical Guide to UK and EU Law**, Büyük Britanya, Oxford University Press, 2004, s. 87.

³³⁵**A.g.e.**, s. 87. Ayrıca *Naomi Campbell/MGN* kararı için bkz., *Campbell/Mirror Group Newspapers* [2002] EWHC 299.

kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgiyi kapsadığına karar vermiştir. Bu doğrultuda Divan, karara konu olan olayda geçen, kişinin ayağının incindiğine ilişkin bilgiyi de hassas veri kategorisinde değerlendirmiştir³³⁶. Diyebiliriz ki, somut olayın özelliklerine göre verilerin özel koruma kapsamında değerlendirilmesinin yapılması gerekmektedir³³⁷.

Hassas verilerin kapsamına yönelik bir eleştiri de Direktif'te hassas veri olarak sayılmayan bazı veri türlerinin korunması ihtiyacının gündeme gelmesidir³³⁸. Son olarak belirtmemiz gerekir ki, bazı veri kategorilerinin özel olarak korunması ayrımının benimsenmesi beraberinde bazı sorunları da getirmektedir. Bu türden ayrımı benimseyen düzenlemelerde hassas kişisel veriler sınırlı sayım esasına göre belirlenmiştir. Sınırlı sayım prensibi nedeniyle genişletilmeleri olanaklı olmayan bu veri kategorileri, nitelikleri dolayısıyla farklı özellik taşımaktadırlar. Bu bilgilerin tamamına aynı rejim kategorilerinin uygulanması çeşitli sakıncalara yol açmaktadır³³⁹.

AIHM de bazı veri kategorilerinin özel koruma kapsamında değerlendirilmesine dair yaklaşıma kararlarında yer vermiştir. Mahkeme, hassas veri kategorisi içerisinde yer alan sağlık verilerinin korunmasına dair verdiği *Z/Finlandiya* kararında bu türden verilerin özel olarak korunması gerektiğini vurgulamıştır³⁴⁰.

³³⁶ Bodil Lindqvist, Case C-101/01, 06.11.2003, paras. 49-51.

³³⁷ Küzeci, **a.g.e.**, s. 232. *Simitis* de tüketici olarak sayılan bir hassas veri kategorisinin oluşturulması yerine, her verinin kendi özel koşulları içinde değerlendirilmesi gerektiğini vurgulamıştır. Bkz., Simitis, **“Revisiting Sensitive Data”**, s. 5.

³³⁸ McCullagh, **a.g.m.**, s. 13-14. Bu veri türlerine finansal bilgiler, biyometrik veriler, iletişim bilgileri örnek olarak verilebilir.

³³⁹ Küzeci, **a.g.e.**, s. 234. Ayrıca hassas verilerin sınırlı sayım prensibine göre oluşturulmasına karşı geliştirilen biri bağlamsal (context-oriented) diğeri de amaçsal (purpose-based) olmak üzere iki farklı yaklaşımın değerlendirmesi için bkz., Rebecca Wong, **“All Alternative Approaches to Sensitive Data”**, **Journal of International Commercial Law and Technology**, C.2, S.1, s. 9-16.

³⁴⁰ *Z/Finlandiya*, b.n. 22009/93, k.t. 25.02.1997. AIHM'nin sağlık verilerinin gizliliğine ilişkin verdiği diğer bir kararı için bkz., *M.S./İsveç*, b.n. 20837/92, k.t. 27.08.1997. Mevcut olayda başvuru geçirdiği iş kazası sonucu ağır bel ağrıları olduğu gerekçesiyle tazminat davası açmıştır. Sosyal Sigortalar Kurumu, başvurunun tedavi görmüş olduğu klinikten tıbbi kayıtlarını istemiştir. Kliniğin göndermiş olduğu raporda başvurunun geçirdiği kurtaj hakkında bilgiler yer verilmiştir. Bunun üzerine başvuru, sağlık verilerine ait bilgilerin Sosyal Sigortalar Kurumu'na gönderilmesinin sağlık verilerinin gizliliğine müdahale oluşturduğunu ileri sürmüştür. Mahkeme, raporda başvuru ile ilgili hassas verilere yer verildiğini kabul etmiştir. Bkz., para. 35. Bununla birlikte Mahkeme mevcut olayda Sosyal Sigortalar Kurumu'nun başvurunun tazminat talebine yönelik karar verebilmesi için tıbbi

Mevcut olayda hem başvurucu hem de boşanmış olduğu kocası HIV virüsü taşımaktadır. Başvurucunun eski eşine karşı hem tecavüz suçundan hem de kasten HIV virüsü bulaştırmak suçundan açılan davada başvurucunun sağlık bilgileri dosyada delil olarak kullanılmıştır. Mahkeme başvuru üzerine verdiği kararında bir kişinin bulaşıcı niteliği olan HIV virüsü taşıdığına ilişkin verilerin gizliliğinin korunmasının özellikle önem teşkil ettiğini vurgulamıştır. Bu türden verilerin açıklanması ilgilinin özel ve aile hayatının yanında sosyal durumunu ve iş durumunu da ciddi bir şekilde etkileyebilir. Bu da bilgilerinin açıklanabileceği kaygısı taşıyan kişi teşhis veya tedaviden kaçınabilir, bulaşıcı hastalıkların önlenmesi için gösterilen çaba zarar görebilir. Bundan dolayıdır ki, yapılan müdahalenin meşru amaçla orantılı olup olmadığına karar verirken, bu türden bilgilerin gizliliğinin korunmasına öncelik verilmelidir³⁴¹.

AIHM, *S. ve Marper/Birleşik Krallık* kararında ise kişisel verilerin arasında neden olabilecekleri zarar faktörüne göre bir ayırım yapılması gerektiğini vurgulamıştır. DNA profilleri ve hücre örneklerinin saklanması sorununun ele alındığı davada Mahkeme, bu verilerin niteliklerinden de yola çıkarak kişisel verilerin önem derecesine göre ayırımını kabul etmiştir. Hücre örnekleri ve DNA profili kişinin sağlığına, genetik bağlarına ve etnik kökenlerine ilişkin hassas bilgileri içermektedir. Parmak izi kayıtlarının ise bu türden bir etkisi bulunmamaktadır. Söz konusu veriler arasındaki bu nitelik farklılığından yola çıkarak Mahkeme, hücre örneklerinin ve DNA profilinin bir veri bankasında tutulmasının sonuçlarının parmak izi kayıtlarının tutulmasına nazaran daha ağır sonuçlara yol açacağına karar vermiştir³⁴².

kayıtları incelemesinin gerekli olduğundan ilgili kliniğin başvurucuya ait sağlık verilerinin iletilmesi için ilgili ve yeterli nedeni olduğuna değinmiştir. Bu anlamda Mahkeme, mevcut olayda özel hayatın gizliliği hakkının ihlal edilmediğine karar vermiştir. Bkz., *M.S./İsveç*, paras. 42-44.

³⁴¹ *Z./Finlandiya Kararı*, paras. 95-96.

³⁴² *S ve Marper/Birleşik Krallık*, b.n.30562/04, k.t.04.12.2008, paras. 70 vd.

B. Hassas Verilerde Kesin İşlem Yasağı ve İstisnaları

Hassas verilere ilişkin özel ve kapsamlı korumanın gerekliliği, bu türden kişisel verileri işleme yasağına tabii kılmaktadır. Öyle ki söz konusu kişisel veriler, kanunlarda belirtilen istisnalar dışında işleme yasağına tabidirler. AB Direktifi'ndeki düzenlemede de aynı şekilde hassas kişisel verilerin işlenmesi yasağı kabul edilmiştir. Ancak, bu kurala bazı istisnalar getirilmiştir. Hatırlatmak isteriz ki, kesin işlem yasağına getirilen istisnai haller bu türden verileri Direktif'in sağladığı korumadan yoksun bırakmamakta, yalnızca Direktif'in 8. maddesinin sağladığı hassas verilere yönelik özel koruma rejiminden yoksun bırakmaktadır. İstisnai hallerde dahi hassas veriler, Direktif'in sağladığı korumanın kapsamındadırlar³⁴³. Hassas verilerde kesin işlem yasağının istisnai halleri Direktif'in 8. maddesinin 2. fıkrasında belirtilmiştir³⁴⁴. İlgili madde hükmüne göre verilerin işlenmesine izin verilecek özel koşullar aşağıdaki gibidir:

- Veri sahibinin açık rızası³⁴⁵: Veri sahibinin açık rızası halinde hassas verileri işlenebilir. Görüleceği üzere örtülü rıza Direktif tarafından kabul edilmemiştir. Kişinin açık rızasının gerekliliği, ilgili kişinin kabule yönelik iradesini ortaya koyan olumlu bir hareketini gerektirir. Bu anlamda kişinin, iradesinin katılmama yönünde belirlediğini göstermek için harekette bulunması hassas verilerin işlenmesi için gerekli açık rızayı sağlamayacaktır. Nitekim kişinin hareketsiz kalması hassas verilerin işlenmesine rıza verdiği anlamına gelmeyeceği gibi veri sahibine katılmamayı tercih edebileceği bir araç sunulması anılan madde hükmünce aranan açık rıza koşulunu

³⁴³ Kaya, **a.g.m.**, s. 323.

³⁴⁴ Burada hassas verilerin işlenmesine ilişkin 108 sayılı Sözleşme'nin düzenlemesine de yer vermemiz gerekir. 108 sayılı Sözleşme'ye göre hassas kişisel veriler ancak taraf devletlerin ulusal hukuk sistemlerinde uygun önlemlerin alınması şartıyla işlenebileceklerdir. Görüleceği üzere Sözleşme'de Direktif'e nazaran hassas veriler açısından kesin işlem yasağının istisnai hallerine ayrıntılı olarak yer verilmemiştir. Ayrıca konuya ilişkin ulusal düzenlemelerde de hassas verilerin işlenebileceği hallere yönelik farklılıklar dikkat çekicidir. Örnek vermek gerekirse 2000 tarihli Hollanda Veri Koruma Kanunu'nda hassas verilerin işlenebileceği haller her bir hassas veri için ayrıca düzenlenmiş ve bunların haricinde bütün hassa veriler için geçerli olan işleme halleri de tek bir madde hükmünde düzenlenmiştir. Danimarka Kişisel Verilerin Korunması Kanunu'nda ise hassas verilerin işlenmesinden önce bunun Veri Koruma Otoritesi'ne bildirimi gereklidir. Bkz., Kaya, **a.g.m.**, 324.

³⁴⁵ AB Direktifi, m. 8/f.2/a

sağlamayacaktır³⁴⁶.

Açık rıza, kişinin özgür iradesiyle verilmelidir. Ayrıca bu rızanın veri sahibinin işleme hakkında yeterli ölçüde bilgilendirilmesi üzerine verilmiş olması gerekmektedir. Nihayet açık rıza, somut olaya ilişkin olmalıdır. Buna göre veri sahibi belirli hassas verilerin işlenmesine ilişkin olarak rıza vermelidir.

Yukarıda değindiğimiz gibi açık rıza, veri sahibinin olumlu bir hareketini gerektirmektedir. Diyebiliriz ki açık rızanın mutlaka yazılı olması gerekmemektedir. Ancak, örneğin sözlü olarak verilen açık rızanın ispatı daha zor olacağından rızanın yazılı olarak alınmış olması veri işleyenler için güvenilir bir ispat aracı olacaktır³⁴⁷.

- Çalışma hukuku yükümlülüklerine uyma: Veri işleme, yeterli güvenceler sağlayan ulusal hukuk tarafından yetki verildiği sürece, veri koruma görevlisinin çalışma hukukundan kaynaklanan özel hak ve yükümlülüklerini yerine getirmesi için zorunlu olması halinde hassas veriler işlenebilir³⁴⁸. Ulusal hukuk tarafından bu türden verilerin işlenmesi yasaklanmamışsa, çalışma hukuku kuralları çerçevesinde yetki verilen sorumlularca yine kişisel verilerin korunması ve çalışma hukuku ilkeleri çerçevesinde işlenmesi mümkün olacaktır. İşverenin sendika üyelik kesintisi kesme yükümlülüğü veya iş yerinde meydana gelen kazaları kaydetme yükümlülüğü bu istisnaya örnek olarak verilebilir. Maddede geçen çalışma hukukunu yalnızca iş hukuku olarak değerlendirmemek gerekir. Konu, kamu hukuku çalışma alanını da kapsayacak şekilde düşünülmelidir³⁴⁹.

- Yaşamsal çıkarların korunması: Veri sahibinin fiziki veya hukuki nedenlerle rıza veremeyeceği durumlarda, veri sahibinin ya da diğer bir kişinin yaşamsal

³⁴⁶Küzeci, **a.g.e.**, s. 240.

³⁴⁷ Article 29 Data Protection Working Party, **Opinion 15/2011 on the definition of consent**, 01197/11/EN WP187, 13.07.2011, s. 25.

³⁴⁸AB Direktifi, m. 8/f.2/b.

³⁴⁹Kaya, **a.g.m.**, 324.

çıkarlarının korunması için gerekli ise hassas veriler işlenebilir³⁵⁰.

Kişinin fiziksel olarak rıza göstermesinin olanaksız olması haline veri sahibinin geçirdiği kaza sonucu tedavisi yapılması zorunlu olan bilinci kapalı kişi olması örnek olarak verilebilir. Hukuken rıza göstermenin olanaksız olmasına ise veri sahibin küçük ya da akıl sağlığı yerinde olmayan bir kişi olması örnek olarak verilebilir. Bu olanaksızlık halleri mevcut değil ise hassas verilerin işlenmesine dair kararı verecek olan yine veri sahibidir ve burada açık rızaya ilişkin kurallara uyulması gerekir.

Bu istisna hassas verilerin sadece veri sahibi hakkında değil aynı zamanda diğer bir kişi hakkında da işlenebilmesine imkan tanımaktadır. Örneğin veri sahibinde ciddi bir bulaşıcı hastalığın bulunması halinde veri sahibi ile irtibat halinde olabilecek kişilerin yaşamsal çıkarını korumak amacıyla veri sahibinin rızası alınmaksızın onunla ilgili hassas verileri işleyebilecektir³⁵¹.

- Özel hukuk kişilerinin faaliyetleri: Demokratik toplumun vazgeçilmezleri arasında yer alan siyasi, felsefi, dini veya sendikal amaç taşıyan bir vakfın, derneğin ve benzeri diğer kar amacı gütmeyen kuruluşların meşru faaliyetleri sırasında ve uygun güvencelerin sağlanmış olması şartıyla hassas veriler işlenebilir. Bu istisnai halin geçerli olması için verilerin işlenmesinin sadece ilgili kurumların üyeleri veya amaçları için bu kurumlarla düzenli irtibat halinde olan kişiler hakkında olması ve verilerin, veri sahiplerinin muvafakati olmaksızın üçüncü kişilere açıklanmaması gerekmektedir³⁵². Görüleceği üzere bu istisna, sayılan kuruluşların amaçlarıyla doğrudan ilgili hassas verilerin işlenebilmesine ilişkindir. Zira faaliyet alanını ilgilendirmeyen hassas verilerin işlenmesi hukuka aykırıdır. AB Direktifi bu istisnayı kamu yararının sağlanması ile açıklamaktadır³⁵³.

³⁵⁰AB Direktifi, m. 8/f.2/c.

³⁵¹**Ibid**, s. 327.

³⁵²AB Direktifi, m. 8/f.2/d.

³⁵³AB Direktifi, 33, 35 ve 39 numaralı gerekçeler.

Bu istisna yalnızca siyasi, felsefi, dini veya sendikal amaçlı kar amacı gütmeyen kuruluşlar için geçerlidir. Belli etnik grupları destekleyen, tıp veya cinsellik alanında faaliyet gösteren ticari amaç güden bir kurum örneğindeki gibi bir durumda istisnai hal geçerli olmayacaktır³⁵⁴.

- Hassas verilerin ilgili kişi tarafından kamuya açıklanmış olması: Kişinin, bizzat kendisine ait hassas verileri açık şekilde kamuya açıkladığı takdirde bu veriler kesin işlem yasağından yararlanamaz³⁵⁵. Bu istisnadan bahsedebilmemiz için verilerin kamuya açıklanması yeterli olmayıp bu açıklamanın veri sahibinin iradesiyle gerçekleşmesi gerekmektedir. Örneğin, kişinin televizyon programında HIV virüsü taşıyıcısı olduğunu söylemesi halinde artık kesin işlem yasağı söz konusu olmayacaktır.

Bu istisna açısından özellikle üzerinde durulması gereken nokta kamuya açıklama kavramının ne anlama geldiğidir. AİHM'in *Von Hannover/Germany* kararı kamu kavramının yorumlanması açısından yardımcı olacaktır. Mahkeme mevcut olayda Monako Prensesi Caroline'nin kamuya açık bir yerde fotoğraflarının çekilmesinin AİHS'in 8. maddesine düzenlenen özel hayatın gizliliği hakkına ihlal niteliği taşıdığına karar vermiştir³⁵⁶. Nitekim kamusal alan ile özel alan arasındaki sınırın belirsizleştiği göz önüne alınması ve hassas verilerin işlenmesine imkan tanıyan bu istisna her somut olayda ayrıca değerlendirilmelidir.

- Hassas verilerin tıbbi tedbirler çerçevesinde işlenmesi: Tıbbi veriler, hastaların her türlü hastalık ve tedavilerine ilişkin kişisel verilerdir. Bundan dolayı bu türden veriler kural olarak kesin işlem yasağına tabidirler. Ancak, veri işlemenin önleyici hekimlik, tıbbi teşhis, tıbbi yardım veya bakım veya sağlık hizmetlerinin idari olarak yürütülmesi için gerekli olması halinde bu hassas veriler işlenebilmektedir. Burada sağlık hizmetlerinin sağlanması açısından geçerli olan bazı

³⁵⁴ *Ibid*, 329.

³⁵⁵ AB Direktifi, m. 8/f.2/e.

³⁵⁶ *Von Hannover/Germany*, b.n. 59320/00, k.t. 24.09.2004.

veri türlerini işleyebilecek kişiler yalnızca sağlık personeli veya sağlık personeli gibi sır saklama yükümlülüğüne tabi kişilerdir³⁵⁷.

- Hassas verilerin yargılama sebebiyle işlenmesi: Hukuki işlemlerin gerçekleştirilmesi veya hukuki savunmaların yapılması sırasında kişilere ait hassas veriler somut olayın gerektirdiği durumla orantılı olmak kaydıyla işlenebilirler³⁵⁸.

- Cezalara dair verilerin kaydedilmesi: Suçlar, mahkumiyetler ve güvenlik tedbirleri ile ilgili veriler ancak resmi bir makam tarafından işlenebilir. Anılan verilerin resmi makamlar dışında işlenebilmesi ancak yeterli güvenceleri öngören iç hukuk kuralları çerçevesinde mümkündür³⁵⁹. Bu son durumun uygulanabilmesi halinde Komisyona bildirimin yapılması gereklidir³⁶⁰.

Adli sicil kayıtları ancak resmi bir makam tarafından işlenebilir³⁶¹. Bu konuda bir istisna getirilemez.

- Ulusal kimlik numarası: Ulusal kimlik numarası ile diğer tanıtıcı işaretlerin işlenme şartları konusunda üye ülkeler, bunların hangi şartlarda işleme konu olabileceğini düzenlemekle yükümlüdürler³⁶². Bu konuda üye devletlere geniş bir takdir yetkisi tanınmıştır.

- Diğer istisnalar ve Komisyona bildirim yükümlülüğü: Üye ülkeler, uygun güvenceler öngörmek kaydıyla, üstün kamu yararı gerekçesiyle ulusal hukuk yoluyla ya da veri koruma otoritesinin kararıyla buraya kadar saymış olduğumuz istisnalara ek istisnalar getirebilir³⁶³. Bu ek istisnaların Komisyona bildirilmesi gerekmektedir³⁶⁴.

³⁵⁷ AB Direktifi, m. 8/f.3.

³⁵⁸ AB Direktifi, m. 8/f.2/e.

³⁵⁹ AB Direktifi, m. 8/f.5.

³⁶⁰ AB Direktifi, m. 8/f.6.

³⁶¹ AB Direktifi, m. 8/f.5.

³⁶² AB Direktifi, m. 8/f.7.

³⁶³ AB Direktifi, m. 8/f.4. . *Simitis*'e göre kamu yararı gibi ifadeler kısıtlamaların anlamını yitirmesine yol açmaktadır. Özellikle kamu yararı ve kamu güvenliği gibi kavramlar bireylerin kişisel verilerin korunması hakkına devletin müdahalelerini arttırmaktadır. Bkz, Simitis, “**Revisiting Data Sensitivity**”, s. 9.

VI. VERİ GÜVENLİĞİ İLKESİ

Kişisel verilerin tutulması kendi başına potansiyel bir risk yaratmaktadır. Veriler tutulduğu sürece bunların kazara ortadan kaldırılması, değiştirilmesi, silinmesi, yayınlanması, bunlara yetkisiz erişim gibi tehlikeler söz konusudur. Bu anlamda verilerin tutulduğu süre kapsamında güvenliklerinin sağlanması gerekmektedir. Aksi durum kişi açısından ekonomik, siyasal, sosyal zararlara yol açabilmektedir. Veri güvenliği ilkesi bu noktada kişisel verilerin korunmasının önemli bir parçasını oluşturmaktadır. Anılan ilke ile kişisel verilere yönelik her türlü haksız müdahaleye karşı alınması gereken bütün idari ve teknik tedbirlerin alınması sağlanmaktadır. Örneğin veriler kazara kaybolmalarına, değiştirilmelerine karşı yedeklenmeli; insan kaynaklı tehlikelere karşı ise verilerin tutulduğu sistemlere güvenlik duvarları kurulmalıdır. Belirtmemiz gerekir ki, kişisel verilerin korunması ile veri güvenliği birbirinden farklı kavramlardır. Kişisel verilerin korunması esas olarak kişisel verilerin işlenmesi sırasında bireyin temel hak ve özgürlüklerinin korunması ve veri işleme faaliyetlerinin sınırlandırılması amaçlanmaktadır. Veri güvenliği ise verilerin kendisinin korunması için gerekli idari ve teknik önlemlerin sağlanmasına ilişkindir³⁶⁵. Uygun idari ve teknik önlemler ile verilerin kaybedilmesi, yetkisiz kişilerin verilere ulaşması, tesadüfen veya yetkisiz kişilerce verilerin tahrip edilmesi, değiştirilmesi veya alenileştirilmesi gibi tehlikeler bertaraf edilmektedir. Bu anlamda olası tehlikeler karşısında verilerin korunması aynı zamanda kişisel verilerin korunması temel hakkının korunmasına da hizmet etmektedir.

A. Veri Güvenliğinin Sağlanabilmesinin Önemi

Bilişim teknolojilerindeki ve kitle iletişim araçlarındaki yeni olanaklarla bilgiye erişimin yer ve zaman sınırlarının ortadan kalkmasıyla birlikte sunulan hizmetlerdeki çeşitlilik ve dönüşüm yeni riskleri beraberinde getirmiştir. Kişisel verilerin kazara ortadan kaldırılması, değiştirilmesi, silinmesi ve yayınlanmasının

³⁶⁴ AB Direktifi, m. 8/f.6.

³⁶⁵ Şimşek, **a.g.e.**, s. 95.; Küzeci, **a.g.e.**, s. 242.

oluşturacağı maddi ve manevi zararlar elbette ki yalnızca bilişim sistemlerinde kayıtlı veriler için değil, elle işlenen veriler için de geçerlidir. Ancak, bilgi ortamının bilişim teknolojilerine bağlı olarak değişmesi, diğer ortamlara oranla teknik bilginin gerekliliği bilişim ortamındaki bilginin kontrolünü her geçen gün daha da zorlaştırmaktadır.

Veri güvenliğinin yeterli düzeyde sağlanamaması ekonomik, siyasal, sosyal ve fiziksel zararlara neden olur. Kimlik bilgileri, banka hesap numaraları gibi bilgilerin çalınması sonucu oluşan ekonomik zarar buna en somut örnektir. Ayrıca bilgi işlem sistemlerini kullanan kurumlara yalnızca dışarıdan değil, kurum içerisinden de gelebilecek saldırılar sanayi casusluğu gibi eylemler de büyük bir tehlike oluşturmaktadır.

Risk altındaki çocukların isimleri, adresleri, durumlarına ilişkin verileri içeren bir veri tabanında güvenliğin sağlanamaması, bu verilerin yetkisiz kişilerin eline geçmesi çocukların suistimal edilmesi tehlikesine neden olacaktır. İngiltere’de kredi kartı verilerinin basına sızması sonucu politikacıların iddia edilen ölçsüz alkol tüketimlerine ilişkin kişilik haklarına zarar verici bilgiler basında yayınlamıştır. Aynı şekilde hastanın HIV virüsü taşıdığına dair verinin yetkisiz kişilerin eline geçmesi kişinin yaşam tarzını, iş umutlarını tehlikeye atabileceği gibi şiddete maruz kalmalarına dahi neden olabilir³⁶⁶.

Veri güvenliğine ilişkin yukarıda vermiş olduğumuz olaylar konunun önemini açıkça ortaya koymaktadır. Görüleceği üzere veri güvenliğinin sağlanması kişisel verilerin korunması açısından oldukça önemlidir. Kişinin temel hak ve özgürlüklerinin korunması için veri işlem faaliyetleri sırasında uygun teknik ve idari önlemlerin alınması yoluyla kişisel verilerin güvenliğini sağlamak verilerin korunmasına yönelik temel bir ilke olarak hukuka uygun veri işlemenin ve ilgilinin haklarını korumanın temel unsurları arasındadır. Bu noktada veri denetçilerinin ve

³⁶⁶ **Dilemmas of Privacy and Surveillance, Challenges of Technological Change**, The Royal Academy of Engineering, Mart 2007, s. 22.

işleyicilerinin yükümlülükleri doğmaktadır.

B. Kişisel Verilerin Korunmasına Dair Düzenlemelerde Veri Güvenliği İlkesi

Kişisel verilerin korunması hakkı ile arasındaki ilişki nedeniyle verilerin güvenliği ilkesine konuya ilişkin metinlerin tamamında yer verilmiştir. 108 sayılı Sözleşme'nin 7. maddesine göre, *“yetkisiz erişim, değiştirme veya yayımlama yanında kazara veya yetkisiz tahribe karşı otomatik veri dosyalarında yer alan kişisel verilerin korunması için uygun güvenlik önlemleri alınacaktır”*. BM Rehber İlkeleri'ne göre 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”* ifadesine yer verilmiştir³⁶⁷. OECD Rehber İlkeleri'ndeki düzenlemeye göre ise kayıp veya yetkisiz erişim, tahrip, kullanım, değiştirilme, ya da yayımlamaya karşı kişisel verilerin uygun güvenceler ile korunması gerekmektedir. Verilerin güvenliği için uygun tedbirlerin alınması temelini, verilerin güvenliğinin sağlanması suretiyle ilgilinin haklarının en iyi şekilde korunmasının sağlanmasından almaktadır³⁶⁸.

Direktif'te ise *“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 diğer hukuka aykırı işleme biçimlerinden korunması için gerekli teknik ve örgütsel önlemleri almasını sağlayacaklardır”* ifadesi yer alır³⁶⁹.

Direktif'te yer verilen veri güvenliğinin sağlanması için uygun önlemlerin alınması zorunluluğu hem ilgili sistem kurulurken hem de daha sonra verilerin işlenmesi sürecini kapsamaktadır. Tekniğin ulaştığı düzey, korunacak verilerin

³⁶⁷ BM Rehber İlkeleri, para.7.

³⁶⁸ Şimşek, **a.g.e.**, s. 96.

³⁶⁹ AB Direktifi, m. 17/f.1.

niteliği, mevcut ihlal tehlikesi ve korumanın neden olacağı maliyet dikkate alınarak uygun önlemlerin neler olacağı tespit edilecektir³⁷⁰. Veri denetçisi, bir sözleşme veya yasal hüküm uyarınca veri işleyen çalıştırdığı takdirde de teknik ve örgütsel güvenlik önlemler yoluyla yeterli güvenceyi sağlama yükümlülüğü altındadır³⁷¹. Ayrıca alınan bu önlemlerin belgelendirilmesi gerekmektedir³⁷². Veri güvenliğini sağlamaya yönelik yasal düzenlemelerin teknolojik dönüşümlere uygun şekilde tasarlanması gerekmektedir. Keza veri güvenliğinin sağlanmasına yönelik araçlar geliştikçe bunların aşılmasını sağlayan yöntemler de gelişmektedir. Bu anlamda verilerin korunmasının sağlanması için güvenlik önlemlerinin güncelleştirilmesi zorunludur. Aynı zamanda baktığımızda veri güvenliği yalnızca bir teknoloji veya bilgisayar güvenliği olarak anlaşılmaması gerekmektedir. Kurumlar açısından ele aldığımızda veri güvenliği, bir maliyet veya ek yük olarak görülmemeli, bir kurum kültürü haline getirilmelidir. Günümüzde bilgiyi ve teknolojiyi hiç kullanmadan işletilen şirket, kurum veya örgüt neredeyse olanaksızdır. Bu nedenle veri güvenliği değişik oranlarda ve düzeyde olsa bile herkes için geçerli bir unsurdur. Son olarak unutmamalıyız ki veri güvenliğinde kilit faktörlerden birisi ve belki de en önemlisi insandır. Bu anlamda veri güvenliğinin yalnızca verileri işleyen kişilerin bir yükümlülük olarak algılanmaması gerekmektedir. Bireyler de kendilerini gerek özel bilgisayarlarında ya da başka elektronik araçlarda aldıkları önlemler ile korumalıdır. Yeterli ve uzun soluklu veri güvenliği, insanların bu konuda bilinçlendirilmeleri ile sağlanabilir.

³⁷⁰ AB Direktifi, 46 numaralı gerekçe. *Küzeci*'ye göre, Direktifte kişisel verilerin korunması için uygun tedbirler için tekniğin ulaştığı düzeyin dikkate alınması her döneme uygulanabilmesi sayesinde Direktif'in teknik gelişmeler karşısında aşınmasını önlemektedir. Bkz., Küzeci, **a.g.e.**, s. 56. Bu dipnot bağlamında hatırlatmak isteriz ki hassas veri olarak kabul edilen veri kategorileri açısından veri güvenliğinin sağlanmasında bu türden veriler için daha yüksek seviyede korumanın arandığı göz önünde bulundurulmalıdır.

³⁷¹ AB Direktifi, m. 17/f.2.

³⁷² AB Direktifi, m. 17/f.4.

VII. DENETİM VE YAPTIRIM SİSTEMLERİ

Buraya kadar kişisel verilerin korunabilmesi için özgü kriterlerin neler olduğundan bahsettik. Kişisel verilerin sağlanması için öncelikle bu ilkelerin benimsenmesi gerekmektedir. Yine de korumanın sağlanması için yalnızca bu ilkeler doğrultusunda oluşturulan düzenlemenin kabulü ile mümkün değildir. Ayrıca bu ilkelere uygun davranılıp davranılmadığını denetleyen bağımsız bir organın oluşturulması, bunların ihlal edilmesi halinde bireylerin şikayetlerini dile getirebilecekleri ve zararlarını tazmin edebildikleri sistemlerin sağlanması da önemli güvencelerdendir. Diyebiliriz ki kişisel verilerin korunmasına dair ilkelerin ve kuralların varlığının yanında bunların uygulanmasının sağlanması da son derece önemlidir.

A. Verilerin İşlenmesinde Bildirim ve Ön Kontrol Uygulaması

Kişisel verilerin işlenmesinde dair düzenlemelerde verileri toplayan ve işleyenlerin hareketlerini denetlemeyi sağlayacak çeşitli kurallar benimsenmiştir. AB Direktifi'nde benimsenen sistemde ise verileri işleyenlerin ve toplayanların kişisel verilerin işlenmesinden veya belirli bir amaca yönelik birçok işlemin gerçekleştirilmesinden önce veri koruma otoritesine bildirimde bulunma zorunluluğu kabul edilmiştir³⁷³. Bu bildirim yükümlülüğü ile birlikte kural olarak, tamamen özel ve kişisel faaliyetler dışında, hiç kimse devletin haberi olmaksızın verileri toplayamayacak veya işleyemeyecektir. Söz konusu yükümlülük ile kişisel verilerin işlenmesinin şeffaflığı ve bu işlemin hukuka uygunluğunun denetimi sağlanmaktadır³⁷⁴. Direktif'te ayrıca, üye devletlerin bildirim yükümlülüğüne bazı istisnalar getirebilecekleri veya bu bildirimi basitleştirebilecekleri öngörülmüştür³⁷⁵.

AB Direktifi'nde veri işlem faaliyetlerinin hukuka uygunluğunun denetimini sağlayan diğer bir yükümlülük olarak ön kontrol uygulaması öngörülmüştür. Belirli

³⁷³ AB Direktifi, m. 18/f.1.

³⁷⁴ Başalp, **a.g.e.**, s. 57.

³⁷⁵ AB Direktifi, m. 18/f.2.

bazı veri işleme faaliyetleri özleri, kapsamaları veya amaçları nedeniyle kişinin temel hak ve özgürlükleri açısından özel risk taşıyabilmektedir. Bu risk, kişinin bir haktan, çıkardan veya sözleşmeden mahrum kalmasından kaynaklanabileceği gibi, yeni bir teknolojinin kullanımı nedeniyle de ortaya çıkabilir³⁷⁶. İşte bu nedenle, Direktifte veri işlem faaliyetlerinin kişi temel hak ve özgürlükleri için özel riskler taşıması durumunda bu durumun belirlenmesi ve bu tür işleme faaliyetlerinin önceden incelenmesine yer verilmiştir³⁷⁷. Ön kontrol yükümlülüğünün bildirim yükümlülüğünden farkı, ilkinin veri işleme faaliyetinin özel risk taşıdığı bazı durumlarda işlemenin önceden incelenmesi anlamına gelmesidir. Bu bağlamda ön kontrol, bildirim yükümlülüğünün aksine sınırlı bir uygulama alanına sahiptir³⁷⁸.

B. Yargı Yolları ve Yaptırımlara İlişkin Düzenlemelerin Gerekliliği

Kişisel verilerin korunması hukuku, kişisel verilerin işlenmesi sırasında ilgili hükümlerin ihlal edilmesi halinde başvurulacak hukuksal yollar ve yaptırımın gerekliliğini de öngörmektedir. Şüphesiz ki bu, aynı zamanda hukuk devleti ilkesinin de bir gerekliliğidir. O halde veri işlem faaliyetleri dolayısıyla hakları ihlal edilen ilgiliye hakkını araması için yargısal yolların garanti edilmesi gerekmektedir.

Yargı yolları ve yaptırım konusu OECD Rehber İlkeleri, 108 sayılı Sözleşme ve BM Rehber İlkeleri'nde sınırlı olarak düzenlenmiştir. AB Direktifi ise konuya dair ayrıntılı bir düzenleme öngörmüştür. Buna göre üye devletler, Direktif hükümlerinin etkin bir şekilde uygulanmasını sağlamak için gerekli önlemleri almalıdırlar³⁷⁹. Bu kapsamda ilgili kişilerin veri koruma otoritesine başvurmadan önce doğrudan mahkemeye erişimlerine izin verme üye devletlerin takdirine bırakılmıştır³⁸⁰. Ayrıca ilgili kişilerin zarardan sorumlu olan veri denetçisinden tazminat hakkı bulunmaktadır³⁸¹. Ancak veri denetçisi, zarara neden olan olaydan sorumlu

³⁷⁶ AB Direktifi, 53 numaralı gerekçe.

³⁷⁷ AB Direktifi, m. 20/f.1.

³⁷⁸ AB Direktifi, 54 numaralı gerekçe.

³⁷⁹ AB Direktifi, m. 24.

³⁸⁰ AB Direktifi, m. 22.

³⁸¹ AB Direktifi, m. 23/f.1.

olmadığını kanıtlarsa sorumluluktan kısmen veya tamamen muaf tutulabilir³⁸².

C. Kişisel Verilerin İşlenmesinin Bağımsız Organlarca Denetimi

Kişisel verilerin korunması açısından oldukça önemli bir diğer güvence ise veri işleme faaliyeti sırasında ilgili kurallara uyulup uyulmadığının bağımsız organlarca denetlenmesidir. Bağımsız organlarca denetim sayesinde hem kamusal organların kişisel verilere özgü ilkelere uymasını hem de bireyin hak ve özgürlüklerinin korunması sağlanır³⁸³. Bu bağlamda kişisel verilerin korunmasına dair düzenlemelere ulusal hukuklarında yer veren birçok devlet bu düzenlemelerin uygulanmasını denetleyen kurumlar kurmuşlardır³⁸⁴. Uluslararası belgelere baktığımızda ise Direktif'in aksine diğer uluslararası belgelerde bağımsız denetim organlarına sınırlı yer verildiğini görürüz. 108 sayılı Sözleşme'nin orijinal metninde bağımsız denetim organlarının kurulmasına yer verilmezken bu durum, AK Bakanlar Komitesi tarafından kabul edilen ek protokol ile değiştirilmiştir. Söz konusu ek protokolde bağımsız bir denetim organının kurulmasına yer verilmiştir³⁸⁵. BM Rehber İlkeleri'nde de tarafsız, bağımsız ve teknik olarak yeterli bir denetim organının ulusal düzeyde atanması gerektiğine yer verilmiştir³⁸⁶. OECD Rehber İlkeleri'nde ise konuya ilişkin bir düzenleme getirilmemiştir. AIHM de konuya ilişkin verdiği kararlarında da bağımsız denetim organının gerekliliğine vurgu yapılmıştır³⁸⁷.

³⁸² AB Direktifi, m. 23/f.2.

³⁸³ Şimşek, **a.g.e.**, s. 102.

³⁸⁴ Bu devletlere istisna olarak Amerika ve Japonya örnek olarak verilebilir. Avrupa'daki veri koruma denetim organlarının kurumsal yapısı ve yetkilerinin incelemesi için bkz., Dilek Yüksel Civelek, “*Kişisel Verilerin Korunması ve Kurumsal Yapılanma Önerisi*”, (Çevrimiçi) http://www.bilgitoplumu.gov.tr/Documents/1/tezler/Kisisel_Verilerin_Korunmasi-Dilek_Civelek-DPT_Uzmanlik_Tezi.pdf, 01.05.2013, s. 93 vd.

³⁸⁵ Additional Protocol on the Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, ETS No. 181, m. 1

³⁸⁶ BM Rehber İlkeleri, para.8.

³⁸⁷ *Ekimdzhev/Bulgaristan* davasında Mahkeme, gizli izlemenin AIHS'in 8. maddesine göre meşru kabul edilip edilemeyeceğine dair yaptığı değerlendirmede gizli izlemeye olanak tanınması durumunda bunun kötüye kullanılmasının engellenmesi için yeterli ve etkili güvencelerin sağlanması gerektiğini vurgulamıştır. Bu güvencelerden biri de gizli izlemenin bağımsız idari otoriteler tarafından denetlenebilmesidir. Mevcut olayda ise gizli izlemenin denetiminin işçileri bakanı gibi siyasi bir kimliğin denetimine bırakılması bağımsız idari otoriteden yoksunluktur. Bu anlamda Mahkeme, bağımsız otorite eksikliğinden dolayı mevcut olayda AIHS'nin 8. maddesinin ihlal edildiğine karar vermiştir. Bkz., *Ekimdzhev/Bulgaristan*, b.n. 62540/00, k.t. 30.01.2008, paras. 87-89.

Aynı şekilde AB Temel Haklar Şartı'nda da kişisel verilerin korunması hakkına ilişkin kurallara uyulup uyulmadığının bağımsız bir makam tarafından denetlenmesi gerektiği belirtilmiştir³⁸⁸.

Bağımsız denetim organlarına ilişkin en ayrıntılı düzenleme Direktif'te yer almaktadır. Bu bağlamda Direktif'te söz konusu organların oluşturulması öngörülmüş, böylece üye devletlerde eşdeğer bir koruma düzeyinin yaratılması ile kişilik hakkının gerçek anlamda korunması temel alınmıştır³⁸⁹. Ayrıca tekrar hatırlatmak isteriz ki, Direktif uyarınca üçüncü ülkelere veri transferinde aranan yeterli koruma düzeyi ölçüsü değerlendirilirken bağımsız veri denetleme organının olup olmadığı göz önüne alınmaktadır. Direktif'e göre üye devletlerin her biri Direktif'te belirlenen hükümlerin uygulanmasını kontrol etmek amacıyla en az bir denetim mercii oluşturmak zorundadır³⁹⁰.

Kişisel verilerin işlenmesinde denetimin tam anlamıyla sağlanması ve bu sayede bireylerin temel hak ve özgürlüklerinin korunması için denetim organının bağımsızlığı ifadesi önemlidir. Keza özerk bir statüden yoksun, siyasal müdahalelere açık bir denetim organının bireyin hak ve özgürlüklerinin korunmasını sağlayacağından bahsetmek mümkün değildir. Aynı şekilde bağımsız karakterden yoksun bir denetim organı hukuk devleti ilkesine de aykırıdır. Nitekim Direktif'te de veri denetim otoritelerinin kurulmasının yanında bunların işlevlerini bağımsız olarak gerçekleştirmelerinin bireylerin kişisel verilerin korunması hakkının korunması açısından temel esas olduğu vurgulanmıştır³⁹¹. Bu anlamda veri denetleme otoritelerinin en önemli özelliği olan bağımsızlık ifadesinin açıklanması gerekmektedir.

³⁸⁸ AB Temel Haklar Şartı, m. 8./f.3.

³⁸⁹ Başalp, **a.g.e.**, s. 78.

³⁹⁰ AB Direktifi, m. 28.

³⁹¹ AB Direktifi, 62 numaralı gerekçe.

Konumuz açısından bağımsızlık, denetim organının somut olayda kanaatini verirken başka bir organdan bu olaya yönelik talimat almamasını gerektirir³⁹². Bağımsızlığın sağlanması için gerekli asgari hususlar (i) ilgili kanunun veri denetleme otoritesinin bağımsız olduğunu vurgulaması, (ii) veri denetleme otoritesinin yeterli mali ve insan kaynaklarına sahip olması, (iii) işlerini doğru ve kesintisiz yerine getirebilmesi ve bu suretle de siyasi etkilere maruz kalmamasının sağlanması olarak sayılabilir. Ayrıca veri koruma otoritesi üyelerinin atanması, görevden alınması ve özlük haklarının kanunla düzenlenmesi gibi koşullar da bağımsızlığı sağlamada önemli etkenlerdir³⁹³.

Buraya kadar veri işlem faaliyetlerini denetleyecek bağımsız denetim organlarının oluşturulmasının hem birey temel hak ve özgürlüklerinin bir garantisi olduğunu hem de hukuk devleti ilkesinin bir gerekliliği olduğunun üzerinde durduk. Nitekim bilgi toplumuna geçmeyi hedefleyen Türkiye açısından da kişisel verilerin korunması ihlalleri karşısında hızlı kararların alma ve uygulama yetisine sahip ve bu konuda uzmanlaşmış bir otoritenin varlığı temel bir gereksinimdir. Ancak, kişisel verilerin korunmasına ilişkin özel bir hüküm getiren 2010 Anayasa değişikliği ve halen daha başbakanlıkta bulunan Kişisel Verilerin Korunması Kanunu Tasarısı uluslararası sözleşmelerde yer alan bağımsız denetim otoritesi yapılanmasını sağlamaktan uzaktır. Öncelikle 2010 Anayasa değişikliğini ele aldığımızda bu değişiklikte bağımsız bir denetim otoritesi yer almamaktadır. Kişisel Verilerin Korunması Kanunu Tasarısı'nın 26. maddesinde ise Kişisel Verileri Koruma Kurulunun oluşturulması düzenlenmektedir³⁹⁴. Kişisel Verileri Koruma Kurulu, Bakanlar Kurulunun seçtiği yedi üyeden oluşur³⁹⁵. Kurulun başkanı yine Bakanlar

³⁹²Küzeci, **a.g.e.**, s. 253.

³⁹³Yüksel Civelek, **a.g.m.**, s. 101.

³⁹⁴ **“Kurul” MADDE 26:** *“(1) Bu Kanunla verilen görevleri yapmak üzere, Kişisel Verileri Koruma Kurulu oluşturulmuştur. (2) Kurul, yetkilerini bağımsız olarak kullanır. Hiçbir organ, makam, merci ve kişi Kurulun kararını etkilemek amacıyla emir ve talimat veremez. (3) Kurul, görevleri ile ilgili konularda tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden her türlü bilgi ve belgeyi isteyebilir. Kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler, söz konusu isteğe cevap vermek ve gereken kolaylığı göstermekle yükümlüdür.”*

³⁹⁵ Kişisel Verilerin Korunması Kanun Tasarısı, m. 27/f.1.

Kurulunca, başkan vekili ise Kurul tarafından kendi üyeleri arasından seçilir³⁹⁶. Tasarı'nın bu haliyle kabul edilmesi halinde yürütmeye bağımlı bir Kurul oluşturulacaktır. Açıktır ki bu Kurul, her ne kadar yetkilerini bağımsız olarak kullanacağı Tasarı'da belirtilmişse de, bağımsızlık niteliğini sağlamaktan uzaktır³⁹⁷. Yine 2010 Anayasa değişikliğine döndüğümüzde ise Anayasa değişikliği ile Kurula ilişkin Tasarı'daki yapılanmayı beraber okunduğunda kişisel verilerin korunması olanağı bulunmamaktadır. Kişisel verilerin korunmasının en önemli güvenlerinden biri olan bağımsız denetim organı Anayasa değişikliğinde yer almamakta, Başbakanlıktaki Tasarı'da ise bağımsız olamayan bir kurul yapılanması öngörülmektedir. Üstelik Tasarı bu haliyle kabul edildiği takdirde Anayasa değişikliği ile getirilen kişisel verilerin korunması hakkına dair hükme aykırı olmayacaktır. Çünkü Anayasa'daki ilgili hükümde bağımsız kurul oluşturma yükümlülüğü yoktur³⁹⁸. Türkiye'de kişisel verilerin korunması açısından bağımsız denetim organının sağlanması kilit bir konumdadır. Bu anlamda bağımsız denetim organının anayasal bir kurum olarak kabul edilmesi ve Tasarı yasalaşmadan önce Kurulun yapılanmasında değişiklik yapılarak bağımsız bir kuruluş haline getirilmesi gerekmektedir.

³⁹⁶ Kişisel Verilerin Korunması Kanun Tasarısı, m. 27/f.4.

³⁹⁷ Kişisel Verilerin Korunması Kanun Tasarısı, m. 26/f.2.

³⁹⁸ Sultan Üzeltürk, “*Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği*”, **Legal Hukuk Dergisi**, C.8, S. 93, 2010, s. 3154 vd. (Bundan böyle “**Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği**” olarak anılacaktır.).

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN TÜRK CEZA KANUNU KAPSAMINDA KORUNMASI

I. GENEL OLARAK

Hukuk dalları içerisinde toplumun gelişim sürecine paralel olarak en hızlı değişmesi gereken dallardan biri hiç kuşkusuz ceza hukukudur. Toplumu etkileyen siyasi, teknolojik ve kültürel değişimler ile zarar verici eylemler ortaya çıkmaktadır. Bu bağlamda kişileri ve toplumu koruyabilmek adına yeni suç tipleri yaratılması gerekmektedir.

Kişisel veriler ve bu verilerin korunması sorunu toplumun dinamik yapısının izlerini taşımaktadır. Kişisel verilerin teknolojik sistemler aracılığıyla işlenmesine görülen artış, bireyin teknolojik gelişmeler karşısında korunmasını gerekli kılmıştır. Bu kapsamda bir değer ve korunan bir hak olarak kişisel verilerin korunması hakkı günümüzde tartışılmaya başlanmıştır.

Kişisel verilerin korunmasının yansıması olarak kabul gören kişisel verilerin korunması hakkı teknolojinin hızlı gelişen yapısı sonucu gündeme gelmiş olsa da kişisel verilerin bir değer olarak kabul edilmesi yalnızca teknoloji temelinde değerlendirilmemelidir. Kişisel verilerin korunması sosyolojik, siyasi, ekonomik bazı nedenler ile de ilişkilidir. Benzer şekilde koruma, bireylerin hem dikey hem de yatay ilişkileri bakımından önemlidir. Resmi makamlar bireylere ilişkin verileri toplayarak ve bunları kullanarak gücünü genişletmektedir. Yatay ilişkiler ise diğer bireyler, kişi toplulukları ve özellikle özel teşebbüsler ile bireyin ilişkilerini tanımlamaktadır. Bu bağlamda örneğin iş verimliliğini arttırmak amacıyla çalışanlar kameralar aracılığıyla gözetlenmektedir. Özel teşebbüsler ise bireyin ticari ilişkilerine yön vermek, olası eğilimleri ve piyasa davranışlarını ölçmek amacıyla kişisel verilere başvurmaktadır. Konunun diğer bir boyutu ise dikey ilişkilerde güvenliğin sağlanması, yatay

ilişkilerde ise ifade özgürlüğü gibi değerlerle kişisel verilerin korunmasının dengelenmesidir. Ayrıca kişisel verilerin korunması hakkı söz konusu verilerin dikey ve yatay ilişkilerde aktarımının ortadan kaldırılması değil, bireye bu süreçte bilgileri üzerinde denetim hakkı sağlanarak bireysel özerkliğinin sağlanmasını amaçlamaktadır.

Bütün bu gelişmeler çerçevesinde Türk Ceza Kanununda kişisel veriler bağlamında kişinin bireysel özerkliğine, özel hayatına ve insan onuruna yönelik zarar verici eylemler suç tipleri olarak öngörülmüştür. Bu bağlamda 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu ile 765 sayılı mülga TCK'dan farklı olarak kişisel verilerin korunmasına ilişkin suçlara yer verilmiştir. Buna göre çalışmamızın konusunu oluşturan 5237 sayılı TCK'da “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı 9. bölümünün 135. maddesinde “kişisel verilerin kaydedilmesi”, 136. maddesinde “verileri hukuka aykırı olarak verme veya ele geçirme”, 138. maddesinde ise “verileri yok etmeme” suçları düzenlenmiştir. Ayrıca 137. maddede 135. ve 136. maddelerde düzenlenen suçların “kamu görevlisi tarafından veya görevinin verdiği yetkiyi kötüye kullanmak suretiyle” ve “belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle” işlenmesi halinde cezayı arttırıcı nedenler öngörülmüştür³⁹⁹.

Ulusal düzenlemelerinde kişisel verilerin korunmasına yer veren ülkelerde iki yaklaşım göze çarpmaktadır. İtalya ve Almanya'da kişisel verilerin korunmasına ilişkin usul ve esasların yer aldığı kanunlarda kişisel verilerin korunmasına ilişkin suçlara da yer verilmiştir. Kişisel verilerin korunmasına ceza hukuku açısından diğer

³⁹⁹ Mevzuatımızca verilerin korunması konusu şu ana kadar yeterli ve gerekli ilgiyi görmemiştir. Konuya ilişkin herhangi bir yasal düzenlemenin yokluğu nedeniyle bu konu öncelikle kişilik haklarının koruması kapsamında incelenmiştir. Buna göre kişisel verilerin korunması genel olarak MK 23. ve 24. maddelerinde yer alan genel kişilik hakkı altında değerlendirilmekteydi. Ayrıca kişilik hakkının ihlali halinde ihlalin sona erdirilmesi ve tazminat sorunları MK'nın 25. maddesi ve BK'nın 49. maddelerine göre ele alınmaktaydı. Bkz., Başalp, **a.g.e.**, s. 101. Özel hukukta ceza hukukundaki suçta ve cezada kanunilik ilkesi yer almadığından ihlal hangi araçla ve hangi alanda gerçekleşirse gerçekleşsin anılan madde hükümlerine başvurulabilmektedir. Kişisel verilerin hukuka aykırı olarak ele geçirilmesi, kullanılması gibi eylemlerin artması ve bu bağlamda kişilerin temel hak ve özgürlüklerine yönelik ihlallerin de artış göstermesi ile ceza hukukundaki suçta ve cezada kanunilik ilkesi gereğince bu eylemlerin suç tipi haline getirilmesi gerekmiştir

bir yaklaşım ise Fransa'da olduğu gibi kişisel verilerin korunmasına ilişkin suçların ceza kanunu kapsamında düzenlenmesidir. 5237 sayılı TCK'da ise kişisel verilerin korunmasına ilişkin suçlar düzenlenirken Fransa'da benimsenen yöntem takip edilmiştir⁴⁰⁰. Şüphesiz ki TCK'da kişisel verilerin korunmasına ilişkin suç tiplerinin düzenlenmesi korumanın sağlanması açısından önemlidir. Ancak bu düzenleme açısından eksiklik kişisel verileri korunmasına dair bütüncül bir yasanın halen daha kabul edilmemiş olmasıdır. Bu bağlamda kişisel veri Türk hukukunda henüz yasal olarak tanımlanmamıştır. Ayrıca TCK'daki ilgili suçlar açısından burada öngörülen etkinlikler tanımlanmamıştır. Bu haliyle düzenleme kanunilik ilkesine aykırıdır⁴⁰¹. Bu eksiklikler nedeniyle maddeler henüz pek uygulanmamaktadır⁴⁰². Kişisel verilerin korunmasına ilişkin bütüncül bir yasanın yürürlüğe girmesi ile ortaya konacak hukuksal rejim çalışma konumuzu oluşturan suç tipleri açısından ceza hukukunda kişisel verilerin tabi olacağı hukukun temel esaslarının belirlenmesi açısından gereklidir. Bununla birlikte kişisel verilerin korunması açısından 2010 yılında 1982 Anayasası'nda yapılan değişiklik kuşkusuz önemli bir adımdır. Bu değişiklik kapsamında Anayasa'nın 20. maddesine 07.05.2010 tarih ve 5982 sayılı kanunun 2. maddesiyle eklenen fıkra ile kişisel verilerin korunması hakkı temel haklar ve ödevler altında doğrudan düzenlenerek anayasal bir niteliğe kavuşmuştur.

II. KİŞİSEL VERİLERİN KAYDEDİLMESİ SUÇU

TCK'nın 135. maddesinin 1. fıkrasıyla, hukuka aykırı olarak kişisel verilerin kaydedilmesi eylemi suç haline getirilmiştir. Maddenin 2. fıkrasıyla ise kişilerin siyasi, felsefi ve dinsel görüşlerinin, ırksal kökenlerinin ve hukuka aykırı olarak sendikal bağlantılarının, cinsel yaşamlarının ve sağlık durumlarının kişisel veri

⁴⁰⁰ TCK'daki düzenleme yalnızca yöntemsel değil aynı zamanda kişisel verilerin korunmasına ilişkin suçlar bağlamında da Fransa'daki düzenleme benimsenmiştir. Ancak bu dipnot bağlamında Fransa'da kişisel verilerin korunmasına ilişkin bütüncül bir kanunun varlığını ve burada kişisel verilerin işlenmesine ilişkin usul ve esasların ayrıntılı olarak düzenlendiğini belirtmek isteriz. Bkz., Ketizmen, **a.g.e.**, 217.

⁴⁰¹ Ersan Şen, “5237 sayılı TCK'da Özel Hayata Karşı Suçlar”, **İstanbul Barosu Dergisi**, C. 79, S.3, 2005, s. 717-718.

⁴⁰² Akyürek, **a.g.e.**, s. 202.

olarak kaydedilmesi eylemleri suç tipi olarak düzenlenmiştir. Buna göre ilgili madde şöyledir;

“(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir. (2) Kişilerin siyasi, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.”

A. Suçla Korunan Hukuksal Değer

TCK'nın 135. maddesinde düzenlenen kişisel verilerin işlenmesi ile ilgili suç tipleri ile korunmak istenen hukuksal değer için ilgili suçun düzenlendiği bölümü değerlendirebiliriz. Anılan suç tipi TCK'nın “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı bölümde düzenlenmektedir. Nitekim bu sistematığe göre inceleme konusu suç ile kişilerin özel hayatının gizliliği korunmaktadır. Bu haliyle düzenleme kişisel verilerin korumasının kaynağını öncelikle özel hayatın gizliliğinin korunması hakkından alan uluslararası düzenlemeler ile paralellik sağlamaktadır. Nitekim Anayasa Mahkemesinin de kişisel verilerin 1982 Anayasası'nın 20. maddesinde düzenlenen özel hayatın gizliliği hakkı ile olan ilişkisini teyit ettiği kararları mevcuttur. Nitekim Mahkeme, 1999 yılında 1774 sayılı Kimlik Bildirme Kanunu'na eklenen hükmün iptali istemine dair yaptığı incelemede kişisel verilerin korunmasını 1982 Anayasası'nın 20. maddesi kapsamında değerlendirmiştir⁴⁰³. Buna göre, kişisel verilerin işlenmesine ilişkin düzenlemelerin Anayasa'da yer alan özel

⁴⁰³AYMK, E. 1996/68; K. 1999/1; t. 06.01.1999. Söz konusu karar 4178 sayılı Kanun'un 10. maddesi ile 1774 sayılı Kimlik Bildirme Kanunu'na eklenen Ek-1 maddesinin 1982 Anayasası'na aykırılığına ilişkindir. İlgili madde 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 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 para cezası verilir. Tekrarı halinde işletme ruhsatı iptal edilir”*.

hayatın gizliliğinin sınırlandırılmasına ilişkin usul ve esaslara uyması gerekmektedir. Hükmün iptali isteminin gerekçesine göre ilgili hüküm ile genel kolluk kuvvetlerine tanınan bilgisayarlarında kişisel bilgilerin toplanmasına ilişkin yetkinin hangi koşullarda verileceği ve bu yetkiyi kullanırken uyulması gerekli temel ilkelerin belirtilmemesi nedeniyle kural, demokratik toplum düzeninin gerekleri ile Anayasa'nın 2., 13., ve 20. maddelerine aykırılık teşkil eder. Ancak Mahkeme, istemin reddi gerekçesinde 1774 sayılı Kanunun genel gerekçesinden yola çıkarak dava konusu kuralın kamu düzeni, genel asayiş ve demokratik toplum düzeninin gereklerine aykırı bir yönü bulunmaması nedeniyle Anayasa'nın 2., 13., ve 20. maddelerine aykırı olmadığını belirtmiştir⁴⁰⁴.

Mahkemenin konu ile ilgili diğer bir önemli kararı ise 2008 yılında 5429 sayılı Türkiye İstatistik Kanunu'nun istatistiksel birimlerin kendilerinden istenen veri veya bilgileri vermekle yükümlü olduklarına ve bu yükümlülüğe uymayanların para cezası ile cezalandırılacaklarına ilişkin hükmün iptaline ilişkindir⁴⁰⁵. Mahkeme bu kararında kişisel verilerin özel hayatın gizliliği hakkı ve düşünce özgürlüğü kapsamında değerlendirilmesi gerektiğine vurgu yapmıştır. Anayasa Mahkemesine göre;

⁴⁰⁴Bu dipnot bağlamında değinmek isteriz ki Anayasa Mahkemesinin dayandığı 13. ve 20. maddeleri 2001 yılında yapılan Anayasa değişiklikleri ile yeniden düzenlenmiştir. Bu değişiklikler öncesinde Mahkeme, 1774 sayılı Kanunun genel gerekçesine atıf yaparak iptali istenen hükmü 1982 Anayasasının 13. maddesinde yer alan genel sınırlandırma sebeplerinden “kamu düzeni”, “genel asayiş” ve “kamu yararı”nı sağlamaya yönelik olarak değerlendirmiş ve iptal etmemiştir. Ancak 2001 yılında yapılan değişiklikler ile birlikte Anayasasının 13. maddesi temel hak ve özgürlükleri genel sınırlandırma sebeplerinden çıkartılmıştır. Değişiklik sonrası Anayasasının 13. maddesi şöyledir; “*Temel hak ve hürriyetler; özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz*”. Buna göre ilgili hüküm temel hak ve özgürlüklere yönelik sınırlamaların sınırını belirlemektedir. Ayrıca değişiklik kapsamında 20. maddesinde yer alan “*Adli soruşturma ve kovuşturmaların getirdiği istisnalar saklıdır*” hükmü madde metninden çıkarılmış ve ikinci fıkrada yalnızca kişilerin üstü, özel kağıtları ve eşyasının aranması ve bunlara el konulmasına ilişkin koşullara yer verilmiştir. Ayrıca burada aşağıda da değineceğimiz üzere 2010 yılında yapılan Anayasa değişiklikleri kapsamında 20. maddeye eklenen kişisel verilerin korunmasına ilişkin hüküm de sınırlamanın sınırlarının belirlenebilmesi açısından önemlidir. Bu konuya aşağıda tekrar değinilecektir.

⁴⁰⁵AYMK, E. 2006/167, K. 2008/86, t. 20.03.2008.

“Maddede açıklayıcı bir düzenleme bulunmadığı için, ‘kişisel veri’ veya ‘isteme bağlı veri’ olarak adlandırılan, belirli veya belirlenebilir kişilerle ilgili her türlü bilgilerin istenebileceği kuşkusuzdur. İstatistiki birimlerin kendilerinden istenen bilgileri belirlenen şekil ve sürede eksiksiz ve hatasız olarak vermek zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmış olmasına karşın, istenecek 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. Anayasanın 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. AİHM kararlarında da belirtildiği gibi, özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililer hakkında rızası olmaksızın bilgi toplanmasının 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. Anayasanın 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.”

Görüleceği üzere Anayasa Mahkemesi kişisel verilerin korunmasına geliştirdiği içtihat ile kişisel verilerin korunmasını öncelikli olarak özel hayatın gizliliği hakkına dayandırmıştır. 2010 yılında 1982 Anayasası'nda yapılan değişiklikler sonucunda içtihat yolu ile geliştirilen bu normatif temel artık doğrudan anayasal dayanağa sahiptir. Keza bu değişiklikler kapsamında 1982 Anayasasının 20. maddesinde düzenlenen özel hayatın gizliliği hakkına eklenen hüküm ile kişisel verilerin korunması hakkı Türk hukukunda bağımsız bir anayasal hak alanı olarak yer verilmiştir. Ayrıca bu değişiklik ile kişisel verilerin özel hayatın gizliliği hakkı ile bağlantısı da açıkça ortaya konulmuştur. Eklenen hüküm şöyledir;

“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”

Türk hukukunda kişisel verilerin korunmasının sağlanmasında önemli bir adımdır. Yine de burada hakkın sınırlandırılmasına ilişkin hükümlere değinilmesi gerekmektedir⁴⁰⁶. Nitekim eklenen maddede yer alan “*kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebilir. Kişisel verilerin*

⁴⁰⁶Bu dipnot bağlamında yapılan Anayasa değişikliğinde kişisel verilerin korunması hakkında dair yapılan bir diğer eleştiriye de burada yer vermemiz gerekir. Söz konusu Anayasa değişikliğinde çalışmamızın ilgili bölümlerinde değindiğimiz 108 sayılı Sözleşme ve AB Temel Haklar Şartı'na aykırı olarak bir bağımsız denetim otoritesi yer almamaktadır. Ayrıntılı bilgi için bkz., Üzeltürk, “**Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği**”, s. 3151-3156.

korunmasına ilişkin esas ve usuller kanunla düzenlenir” hükmü ile sınırlamanın sınırına ilişkin değerlendirmeyi gerektirmektedir. Buna göre Anayasa'nın 13. maddesine göre temel hak ve özgürlükler “yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak” sınırlanabilir. Ancak 20. maddeye eklenen madde hükmünde özel bir sınırlandırma sebebine yer verilmemiş, kişisel verilerin hangi durumlarda işlenebileceğinin kanun ile belirleneceği düzenlenmiştir. Yine 13. maddede geçen “Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine” aykırı olamayacağı ilkesi sınırlamaların sınırlarını belirlese de değişiklikler kapsamında 20. maddeye eklenen madde hükmünde kişisel verilerin korunmasının sınırlanmasına ilişkin özel sebeplere Anayasada doğrudan yer verilmemesi korumanın etkinliğini engelleyebilir⁴⁰⁷.

Sonuç olarak TCK'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçu ile korunmak istenen hukuksal değer özel hayatın gizliliği hakkı ve kişilerin kendileri ile ilgili verilerin hangi amaçlarla kimler tarafından nasıl kullanılacağını belirleme hakkı olarak ifade edilen kişisel verilerin korunması hakkıdır.

B. Maddi Unsur

1. Suçun Konusu

TCK'nın 135. maddesinde düzenlenen suçun konusunu “kişisel veriler” oluşturmaktadır. Ancak TCK'da kişisel verilerin tanımlaması yapılmamıştır. Suçun hukuki konusunu oluşturan “kişisel veri”nin tanımının yapılması, suç failinin eyleminin yöneldiği “şey”in tanımlanması ve ceza hukukunda geçerli olan kanunilik ilkesine uygunluğun sağlanması açısından gereklidir⁴⁰⁸. Bu noktada tekrar belirtmek

⁴⁰⁷ Küzeci, **a.g.e.**, s. 266.

⁴⁰⁸ TCK'da kişisel verinin tanımlanmasının yapılmaması ve konunun genişliği, sınırlarının çizilmesinin zorluğu açısından bu durum uygulamada sorunlara yol açabilmekte ve aynı zamanda ceza hukukunun kanunilik ilkesine aykırılık teşkil etmektedir. Akyürek, **a.g.e.**, s. 202. Özbek'e göre ise ceza kanunlarının kazuistik yöntemle yazılmayışlarından ötürü kişisel verinin tanımlanmasına yer verilmemesi yerindedir. Yazara göre suçun maddi unsurunu oluşturan kişisel veri kavramı kıyas

isteriz ki kişisel verinin hukuksal tanımlamasının yapıldığı bütüncül bir yasanın kabul edilmemesi önemli bir sorundur. Bu durumda inceleme konusu suç tipleri açısından uluslararası sözleşmelerin ve Kişisel Verilerin Korunması Kanun Tasarısı'nın göz önünde tutulması gerekmektedir. Nitekim 135. maddenin gerekçesinde söz konusu suç ile 108 sayılı Sözleşme'ye geçerlilik kazandırıldığı belirtilmiştir. Bu anlamda yasakoyucu düzenlemelerinde 108 sayılı Sözleşme'yi dikkate almıştır⁴⁰⁹. Aynı doğrultuda her ne kadar bu ifade yalnızca 135. maddenin gerekçesinde belirtilmiş olsa da konuya ilişkin diğer suç tipleri için de 108 sayılı Sözleşme'nin dikkate alındığı kabul edilmelidir⁴¹⁰.

135. maddenin gerekçesinde kişisel veri, “gerçek kişiyle ilgili her türlü bilgi” olarak tanımlanmaktadır⁴¹¹. Buna göre kişinin tanınabilmesini ya da bilinebilmesini sağlayan kişinin ismi, adresi, kimlik numarası, vergi numarası, nüfus bilgisi, parmak izi, işinden aldığı ücret, DNA bilgisi kişisel veri olarak kabul edilmelidir⁴¹². Burada altını çizmek istediğimiz bir diğer nokta ise kişisel olmaktan öte daha çok kurumsal olan verilerin 135. maddenin kapsamına girip girmediğidir. Bir anonim şirkete ait ticari sırlar, bankacılık sırrı veya müşteri sırrı ile fenni keşif ve buluşlar veya sınai

yaşasını ihlal etmeden yorum yoluyla ortaya konulabilmektedir. Bkz., Veli Özer Özbek, **Yeni Türk Ceza Kanununun Anlamı (TCK İzmir Şerhi), (Madde 76-169), C. II**, Ankara, 2008, s. 948. Ancak kişisel verilerin korunmasına dair izlenen yöntem, bu verilerin tanımlanmasına dayanmaktadır. Suçun konusunun en azından belirli bir çerçeveye oturtulması gereklidir.

⁴⁰⁹ Özbek, **a.g.e.**, s. 947.

⁴¹⁰ Küzeci, **a.g.e.**, s. 287, d.n. 68.

⁴¹¹ Bu dipnot bağlamında çalışmamızın yazım sürecinde halen daha Başbakanlıkta bulunan Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı'nın 3. maddesinin ç bendindeki kişisel veri tanımına değinmemiz gerekir. Tasarı bu haliyle kabul edilirse, ilgili maddede kişisel veri “*belirli veya belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler*” olarak tanımlanmıştır. TCK'nın 135. maddesindeki gerekçede kişisel veri tanımı açısından gerçek kişiler hakkında bilgi olarak sınırlama yapılmasına karşın Tasarıda tüzel kişiler hakkındaki bilgiler de kişisel veri kapsamına alınmıştır. Gerekçe ve Tasarı'daki bu fark, uluslararası düzenlemelerdeki kişisel veri kapsamına yalnızca gerçek kişilere ilişkin bilgilerin alındığı veya buna tüzel kişilere ilişkin bilgilerin de dahil edildiği farklı yaklaşımlara ilişkindir. Konu ile ilgili ayrıntılı bilgi için bkz., Çalışmamızın “*Kişisel Veri Kavramı ve İlgili Düzenlemeler*” adlı Birinci Bölümü, I numaralı “*Kişisel Veri Kavramının Açıklanması*” başlığı altındaki “*Kimliği Belirli veya Belirlenebilir Kişi*” B bölüm altbaşlığı.

⁴¹² 1 Haziran 2005'te yürürlüğe giren 5271 sayılı Ceza Muhakemesi Kanunu da kişisel veriler konusunda zengin bir içeriğe sahiptir. CMK'nın 81. maddesinin birinci fıkrasına göre kaydedilen “kişinin fotoğrafı, benden ölçüleri, parmak ve avuç içiz izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri”, 78 ile 80. maddelerindeki “moleküler genetik inceleme sonucu”, 75 ve 76. maddelerindeki “beden muayenesi ve/veya vücuttan örnek alınması suretiye elde edilen” veriler ve 135. maddeye göre kayda alınan “telekomünikasyon yoluyla iletişim” gibi veriler kişisel veri niteliğindedirler.

uygulamaya ilişkin bilgiler TCK'nın 239. maddesinde düzenlenen suç ile koruma altına alınmıştır⁴¹³. Bu nedenle saydığımız türden bilgiler 135. maddenin konusunu oluşturmazlar. Kaldı ki bu veriler bakımından yasakoyucu özel hayatın gizliliğinden çok toplumun korunması ile ekonomi, sanayi ve ticaret alanındaki güvenliği korunan hukuksal değer olarak kabul etmiş ve bu amaçla da TCK'nın 239. maddesindeki suç “Topluma Karşı Suçlar” kısmında “Ekonomi, Sanayi ve Ticarete İlişkin Suçlar” bölüm altbaşlığı altında ayrıca düzenlenmiştir⁴¹⁴.

Kişisel verinin kapsamı açısından tartışmalı olan bir diğer husus ise TCK açısından ses ve görüntülerin kişisel veri kapsamına girip girmediğidir. Çalışmamızın ilgili bölümünde belirttiğimiz gibi ses ve görüntüler konuya ilişkin uluslararası düzenlemelerde kişisel veri olarak kabul edilmiş; bu husus AB Direktifi'nde açıkça belirtilmiştir⁴¹⁵. Çalışma konumuzu oluşturan TCK açısından ise, 135. maddenin gerekçesindeki kişisel veri kapsamının kişiyle ilgili kayda geçirilmiş bilgi ve enformasyon olarak değerlendirildiği sonucuna varılmıştır. Uluslararası düzenlemelere nazaran varılan dar yorum nedeniyle kişiyle ilgili ses ve görüntülerin kişisel veri kapsamında değerlendirilmediği ileri sürülmüştür. Konuya açıklık getirmek açısından kimi yazarlar bu dar yorumun dikkate alınmaması gerekir. Kişiyle ilgili olan ve kişinin tanınabilmesini ya da bilinebilmesini sağlayan her türlü verinin kişisel veri olduğu değerlendirilmesinin kişiyle ilgili ses ve görüntüleri de kapsamına aldığı savunulmuştur⁴¹⁶. Bazı yazarlara göre ise, kanun hükümleri incelendiğinde

⁴¹³“ **Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması” MADDE 239** “(1) Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, şikâyet üzerine, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır. Bu bilgi veya belgelerin, hukuka aykırı yolla elde eden kişiler tarafından yetkisiz kişilere verilmesi veya ifşa edilmesi hâlinde de bu fıkra göre cezaya hükmolunur. (2) Birinci fıkra hükümleri, fennî keşif ve buluşları veya sınâî uygulamaya ilişkin bilgiler hakkında da uygulanır. (3) Bu sırlar, Türkiye’de oturmayan bir yabancıya veya onun memurlarına açıklandığı takdirde, faile verilecek ceza üçte biri oranında artırılır. Bu hâlde şikâyet koşulu aranmaz. (4) Cebir veya tehdit kullanarak bir kimseyi bu madde kapsamına giren bilgi veya belgeleri açıklamaya mecbur kılan kişi, üç yıldan yedi yıla kadar hapis cezasıyla cezalandırılır.”

⁴¹⁴ Özbek, **a.g.e.**, s. 950.

⁴¹⁵ Ayrıntılı bilgi için bkz., çalışmamızın “*Kişisel Veri Kavramı ve İlgili Düzenlemeler*” adlı Birinci Bölümü, I numaralı “*Kişisel Veri Kavramının Açıklanması*” başlığı altındaki “*Her Tür Veri*” A bölüm altbaşlığı.

⁴¹⁶ Ketizmen, **a.g.e.**, s. 230.

kişinin görüntü veya sesinin kişisel veri olarak değerlendirilemeyecektir. Bu anlamda kişinin ses ve görüntülerinin, kişiyle ilgili onu belirli kılan ya da belirlenebilir kılacak her türlü veri kavramının içinde kabul edilmemesi halinde özel hayatın gizliliği hakkının korunmasına yönelik torba suç niteliğindeki 134. maddede düzenlenen özel hayatın gizliliğini ihlal suçu, ilgili maddedeki diğer tipiklik unsurları da gerçekleştiği takdirde, gündeme gelebilecektir⁴¹⁷. Aynı görüş doğrultusunda Yargıtay, kişinin ses ve görüntüsünün özel hayatın gizliliği kapsamında değerlendirebileceği durumlarda 134. maddenin 2. fıkrasında yer alan özel hayata ilişkin görüntü veya seslerin ifşa edilmesi suçunun değerlendirilmesi yerine, yerel mahkemece sanık hakkında verileri hukuka aykırı olarak verme veya ele geçirme suçundan beraat kararı verilmesini bozma nedeni olarak görmüştür. 2012 tarihli Yargıtay kararına göre; *“sanık hakkında verileri hukuka aykırı olarak verme veya ele geçirme suçundan verilen beraat hükmüne yönelik temyiz istemlerinin incelenmesine gelince; 5237 sayılı TCK’nın 136/1. maddesinde düzenlenen ‘Verileri hukuka aykırı olarak verme veya ele geçirme’ suçunun oluşabilmesi için, belirli veya belirlenebilir bir kişiye ait her türlü bilginin, başkasına verilmesi, yayılması ya da ele geçirilmesi gerekmekte olup, bir özel hayat görüntüsü ya da sesinin kaydedilmesi 5237 sayılı TCK’nın 134/1. maddesinin 2. cümlesinde; özel hayata ilişkin görüntü ya da sesin, taksirle ya da tamamen hukuka uygun elde edilmiş olsa dahi, ilgisinin bilgisi ve rızası dışında ifşa edilmesi, yani; yayılması, açığa vurulması, afişe edilmesi, ilan edilmesi, kamuoyuna duyurulması, aleniyet kazandırılması, özetle; içeriğini öğrenme yetkisi bulunmayan kişi veya kişilerin bilgisine sunulması 5237 sayılı TCK’nın 134/2. maddesinde suç olarak düzenlenmiştir. Dosya içeriğine göre sanığın, mağdurenin bilgisi dahilinde çıplak vaziyetteki görüntü ve fotoğraflarını kaydedip, elde ettiği kayıtlarla oluşturduğu CD’leri, mağdurenin rızası olmaksızın, değişik zamanlarda farklı kurumlara göndermek fiilinin 5237 sayılı TCK’nın 134/2. maddesi kapsamında değerlendirilmesi yerine yasal ve yeterli olmayan gerekçelerle, sanık hakkında beraat kararı verilmesi”* bozmayı gerektirmiştir⁴¹⁸. Bütün bu bilgilerin ışığında

⁴¹⁷ Akyürek, a.g.e., 203.

⁴¹⁸ Yargıtay 12. Ceza Dairesi, E. 2012/17703, K. 2012/1822, t. 11.09.2012.

diyebiliriz ki kişiyle ilgili onu belirli kılan ya da belirlenebilir kılacak her türlü veri kavramının ses ve görüntüleri de içermediği kabul edildiği takdirde genel hüküm olan 134. maddeye göre yargılama yapılacaktır. Kişisel verinin kapsamına dair belirsizlik nedeniyledir ki kişisel verilerin korunmasına ilişkin suçlar ses ve görüntü söz konusu olduğunda uygulanamamaktadır. Bu eksikliğin giderilmesi, kişisel veri kavramının netleşmesi ve konuya ilişkin uluslararası düzenlemeler ile paralelliğin sağlanması ancak bütüncül bir yasanın kabulü ile mümkündür.

Veri ile kişi arasındaki doğrudan veya dolaylı olarak bağlantının kurulması arandığından anonim veriler 135. maddede yer alan kişisel verilerin hukuka aykırı olarak kaydı suçunun konusunu oluşturmayacaktır. TCK'nın 135. maddesinin gerekçesinde ayrıca verileri sanal ortamda ya da somut kağıt üzerinde kayda alınması açısından fark gözetilmediği yer almaktadır. Buna göre yalnızca bilişim sistemlerinde yer alan kişisel veriler değil, örneğin kağıda yazılmış, dosyalanmış kişisel veriler dahi bu suçun kapsamındadır⁴¹⁹.

TCK'nın 135. maddesinin ikinci fıkrası *“kişilerin siyasi, felsefi veya dini görüşlerine, ırk 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”* şeklinde bir düzenleme getirmiştir. Görüleceği üzere hükümde geçen söz konusu *“...bilgileri kişisel veri olarak kaydeden”* ibaresi yerinde değildir. Bu ibare, ilgili hükümde yer verilen bilgilerin kişisel veri olmadığı gibi bir anlama yol açmaktadır. Hiç şüphesiz ki, bu veriler de kişisel veri niteliğindedirler. Hatta ulusal ve uluslararası düzenlemelerde bu türden veriler işlenmeleri halinde diğer veri türlerine göre kişilerin daha ağır zararlar ile karşı karşıya kalabileceklerinden bahisle “hassas veri kategorileri”nden sayılmış ve özel olarak korunmasına dair düzenlemeler getirilmiştir. 135. maddenin 2. fıkrasındaki düzenleme için bir diğer tartışma konusu ise bu türden veriler için yine

⁴¹⁹ TCK'nın 135. maddenin gerekçesinde de aynı doğrultuda, *“verilerin sanal ortamda ya da somut kağıt üzerinde kayda alınması açısından fark gözetilmediği”*ni belirtilmiştir.

aynı maddenin ilk fıkrası hükmü uyarınca cezalandırılacağıının öngörülmesidir. Bu tür veriler diğer kişisel verilerden farklı olarak ayrımcılığa yol açabilecek nitelikte olmaları bakımından bireyler açısından özellikli bir yere sahiptir ve hassas veri olarak adlandırılmaktadır⁴²⁰. Bu nedenle söz konusu hassas verilerin kaydedilmesi ile diğer kişisel verilerin kaydedilmesi eylemleri için aynı cezanın öngörülmüş olması yerinde olmamıştır. Bu tür verilerin bireyler açısından taşıdıkları önem göz önüne alınarak daha ağır cezayı gerektiren nitelikli hal olarak öngörülmeleri daha yerinde olacaktır⁴²¹. Ancak TCK'nın mevcut düzenlemesine göre hassas veri olarak nitelendirilen bu tür verilerin kaydedilmesi halinde, TCK'nın 61. maddesine göre suç konusunun önem ve ağırlığı göz önüne alınarak cezanın tayininde alt sınırdan uzaklaşma nedeni sayılması gerekmektedir⁴²².

2. Fail ve Mağdur

İnceleme konusu kişisel verilerin kaydedilmesi suçu açısından maddede suçu işleyecek kişi açısından “kimse” ibaresi kullanılmıştır. Anılan suç tipi açısından fail, herkes olabilir. Ancak, suçu işleyen kamu görevlisi olması TCK'nın 137. maddesine göre inceleme konusu suçun nitelikli halini oluşturur. Bu nedenle fail, kamu görevlisi olduğu takdirde bu durum ceza tayin edilirken göz önünde bulundurulacaktır. Konu ile ilgili açıklamalar suça etki eden sebepler başlığı altında ayrıca incelenecektir.

Kişisel verilerin kaydedilmesi suçu açısından herkes suçun mağduru olabilir. Bu noktada önemli olan veriler ile kişi arasında bağlantının kurulabilmesi, kaydedilen kişisel verilerin bireyle ilgili olması gerekmektedir.

⁴²⁰ Ayrıntılı bilgi için bkz., Çalışmamızın “*Kişisel Verilerin Korunması Hakkına Özgü Kriterler*” adlı İkinci Bölümü, III numaralı başlık altındaki “*Hassas Verilerin Özel Olarak Korunması*” adlı bölüm. Ayrıca paralel bir düzenleme için bkz., Kişisel Verilerin Korunması Hakkında Kanun Tasarısı, m. 50.

⁴²¹ Özbek, **a.g.e.**, s. 949.

⁴²² İsmail Malkoç, **Açıklamalı-İçtihatlı 5237 sayılı Yeni Türk Ceza Kanunu, (Madde 82–149), C. II**, Ankara, 2013, s. 2198.

Gerçek veya tüzel kişilerin mağdur olabileceği yönünde bir ayrıma gidilmediği yönündeki değerlendirme görecelidir⁴²³. 135. maddenin gerekçesinde gerçek kişi ile ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğine yer verilmiştir. Bu anlamda TCK'da tanımlaması yapılmayan kişisel veri kavramı için ilgili maddenin gerekçesinden yararlanıldığında mağdurun yalnızca gerçek kişi olabileceği kabul edilmelidir. Burada sorunun çözümü için kişisel verinin tanımının yapılması gerekmektedir.

3. Hareket

135. maddede düzenlenen suçun hareketi kişisel verilerin kaydedilmesidir. Maddenin gerekçesine göre “*söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayrım gözetilmemiştir*” denilerek suçun oluşabilmesi için kişisel verilerin sistemli olarak kayıt edilmesi veya bilişim sistemlerinde tutulması aranmamaktadır⁴²⁴. Kişisel verinin mekanik, manyetik, elektronik veya başka herhangi yöntemlerle kaydedilmesi, yazılı kayıtlara geçirilmesi eylemleri ilgili madde açısından suç teşkil edecektir. Kişisel verilerin herhangi bir şekilde kayıt edilmesi suretiyle suç oluşacağından bu suç, serbest hareketli bir suçtur⁴²⁵.

⁴²³ Dülger'e göre kanunda ayrıca bir ayrıma gidilmemiştir. Yazara göre mağdur gerçek veya tüzel kişi olabilmektedir. Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, Ankara, Seçkin Yay., 2012, s. 563.

⁴²⁴ TCK Öntasarısı ve Tasarısı'nın gerekçelerinde 108 sayılı Sözleşme'nin ilgili maddelerine işlerlik kazandırılmak istendiği belirtilmiştir. Çalışmamızın ilgili bölümünde belirttiğimiz gibi 108 sayılı Sözleşme tamamen veya kısmen otomatik yollar ile işlenen verileri kapsamaktadır. Bkz., 108 sayılı Sözleşme, m. 3/f.1. 108 sayılı Sözleşme'nin koruma kapsamı belirtildiği gibi olmakla birlikte taraf devlet, Sözleşme'nin uygulama alanını otomatik veri işleme kapsamına girmeyen kişisel veri dosyaları hakkında da uygulanacağını bildirebilir. Bkz., 108 sayılı Sözleşme, m. 3/f.2/c. Bu doğrultuda TCK Öntasarısı ve Tasarısı'nda düzenlenen suç, herhangi bir şekilde kayıt ya da işleme yerine bilişim sistemine ve fişliklere kaydetme ve bilişim sistemlerine veya fişliklere bağlı olarak işleme şeklinde gerçekleşecektir. Bkz., Ketizmen, **a.g.e.**, s. 232. Kişisel verilerin korunmasına dair düzenlemelerin kabul edilmesinde bilgisayar ve bilişim sistemlerindeki gelişmeler etkili olmuştur. Yine de kağıt üzerindeki veriler ile elektronik ortamdaki verilerin kişi açısından taşıdığı hukuksal önemi yadsınamaz. İşte bu nedenle AB Direktifi kişisel verilerin tamamen veya kısmen otomatik işlenmesini kapsadığı gibi kişisel verilerin ayrıca otomatik işleme dışında bir dosyalama sisteminin bir parçası ya da bunun parçasını oluşturması niyetiyle işlenmesi hallerini de uygulama kapsamına almaktadır.

⁴²⁵ Dülger, **a.g.e.**, s. 565.

TCK'nın 135. maddesinde suç olarak düzenlenen kişisel verilerin kaydedilmesi kişisel verilerin işlenmesi sürecinin bir parçasıdır. Keza kişisel verilerin işlenmesi kayıt etme yanında kişisel verilerin toplanmasını, kullanılmasını, aktarılmasını da kapsayan bir süreçtir. Söz konusu maddenin gerekçesinde kişisel veriler için *“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”* denilerek kişisel verilerin hukuka aykırı olarak kullanılmasına dair bir gerçek yansıtılmıştır. Ancak madde gerekçesinde saptaması yapılan bu tehlikeye karşın kanunda, kişisel verilerin hukuka aykırı olarak kullanılmasına ilişkin düzenlemeye yer verilmemiştir. Buna göre hukuka uygun olarak kaydedilen kişisel veri, daha sonra kaydetme amacı dışında kullanıldığında bu eylem suç olarak tanımlanmadığından yaptırımsız kalacaktır⁴²⁶. Bu şekilde bir düzenleme kişisel verilerin korunması açısından kişisel verilerin meşru olmayan ikincil bir amaç için işlenmesine yönelik *“amaç ile bağlılık”* ilkesine aykırılık teşkil edecektir. Daha etkin bir koruma için kişisel verilerin işlenmesine ilişkin koşulların belirgin hale getirilmesi ve kişisel verilerin hukuka aykırı olarak işlenmesinin de suç olarak tanımlanması gerekmektedir⁴²⁷.

⁴²⁶ 12.05.2003 tarihinde TBMM'ye sunulan TCK Tasarısı'ndaki düzenleme ise şöyledir; **“Madde 197:** (1)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. Veriler, hileli veya kanun dışı yollarla elde edildiğinde verilecek ceza üçte biri oranında arttırılır. (2)Kanuna uygun olarak bilişim sistemlerine yerleştirilmek veya işlenmekle beraber muhafazaları için gerekli güvenlik tedbirlerinin alınmaması nedeni ile kişisel verilerin başkalarının ellerine geçmesine veya bozulmasına veya zarar görmesine neden olan kimse hakkında bir yıldan dört yıla kadar hapis cezası verilir. Fiil taksirle işlendiğinde elli milyon liradan iki yüz milyon liraya kadar ağır para cezası verilir. (3)Kanunun öngördüğü haller dışında, kişilerin ahlaki niteliklerini, siyasal, felsefi veya dinsel görüşlerin 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”. Bu madde ile suçun gerçekleşmesi için gerekli seçimlik hareketlerden biri olarak kişisel verilerin korunmasına ilişkin bütün süreci kapsayan kişisel verilerin işlenmesi eylemine de suç tanımında yer verilmişti. Ancak mevcut düzenlemede bu eyleme yer verilmemesi nedeniyle hukuka uygun bir şekilde toplanan kişisel verilerin daha sonradan bu amaç dışında işlenmesi durumunda TCK'nın 135. maddesindeki suç oluşmayacaktır.

⁴²⁷ Ketizmen, **a.g.e.**, s. 238. 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 kaynaktan hukuka uygun olarak bulunan bir bilginin bir bilişim sistemine ya da kişisel dosyaya hukuka aykırı şekilde girilmesi şeklinde de gerçekleştirilebilecektir”*. Bkz., Dülger,

TCK'nın 135. maddesinin ikinci fıkrasında sayılan kişilerin siyasi, felsefi veya dini görüşlerine, ırk kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgiler açısından maddede geçen “kişisel veri olarak kaydetmek” eyleminin ilk fıkra hükmünde geçen “kişisel verileri kaydetmek” eyleminden ayrı bir suç olarak düzenlenmemiştir⁴²⁸. Burada yasakoyucu 2. fıkra hükmünde sayılan konular açısından örneğin sağlık durumuna ilişkin veriyi ele aldığımızda bu bilgi, bir kişiye yönelik olarak değil de “(x) bölgesinde ... hastalığı yaygındır” şeklinde genel olarak kaydedilmişse 135. maddenin 2. fıkrasındaki suç oluşmayacaktır. Diyebiliriz ki “kişisel veri olarak kaydetmek” ibaresi ile yasakoyucu maddede “kişisel verileri kaydetmek” eyleminden farklı bir eylemi suç olarak tanımlamak değil, ilgili bilgilerin kaydedilmesi eylemini sınırlandırmak içindir⁴²⁹.

4. Netice

Kişisel verilerin elektronik ortama, bilişim sistemine veya yazılı tutanaklara kaydedilmesi ile suç gerçekleşmiş olacaktır. Her somut olayda gerçekleştirilen harekete göre suç oluşturan eylemin sonuçlanma anı değişecektir.

Kaydetme işleminin gerçekleştirilmesi ile suç meydana gelecektir. Ayrıca bir zararın meydana gelmesi aranmadığından TCK'nın 135. maddesine düzenlenen kişisel verilerin kaydedilmesi suçu bir tehlike suçudur.

a.g.e., s. 565. Kişisel Verilerin Korunması Kanunu Tasarısı'nın 50. maddesinde yer alan hukuka aykırı olarak kişisel verilerin işlenmesinin TCK'nın 135. maddesine göre cezalandırılacağını düzenlenmiştir.

⁴²⁸ Aksi görüş için bkz., Hafızogulları-Özen, **a.g.e.**, s. 276. Yazarlara göre TCK'nın 135. maddesinin ilk fıkrasında “kişisel verileri kaydetmek” eylemi suç olarak tanımlanmakta, 2. fıkra ise fıkra hükmünde sayılan kişinin bazı niteliklerine ilişkin bilgileri “kişisel veri olarak kaydetmek” eylemi suç olarak tanımlanmıştır.

⁴²⁹ Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Ankara, Seçkin Yay., 2013, s. 398.

C. Manevi Unsur

Kişisel verilerin kaydedilmesi suçunun manevi unsuru kasttır. Suçun oluşması için genel kast yeterlidir. Buna göre fail, kişisel verileri kaydederken hukuka aykırı şekilde hareket ettiğini bilmelidir. Ancak, 135. maddenin 2. fıkrasında “kişilerin siyasi, felsefi, veya dini görüşlerine, ırkı kökenlerine” ait bilgilerin kaydedilmesinde “hukuka aykırı olarak” ibaresi belirtilmediğinden burada failin kastının hukuka aykırılığı ayrıca kapsamış olması aranmayacaktır. Bunun yanı sıra failin gerçekleştirdiği eylemi ve sonuçlarını istemesi, suç işleme kastının varlığı için gereklidir. Suçun oluşması için failin suçun hangi saikle işlediğinin önemi yoktur⁴³⁰. Suçun oluşması için failin bilerek ve isteyerek hareket etmesi arandığı için bu suç tipinin taksirle işlenmesi mümkün değildir.

D. Hukuka Aykırılık

TCK'nın 135. maddesindeki suç tanımlamalarında yasa koyucu hukuka aykırılık vasfına dair ikili bir ayrıma gitmiştir. İlgili maddenin ilk fıkrasında düzenlenen genel olarak her türlü kişisel verinin kaydedilmesi ile kişilerin “*ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kişisel veri olarak kaydedilmesi*”nin suç teşkil edebilmesi için bunların “hukuka aykırı olarak” kaydedilmesi aranmıştır. Oysa, yine TCK'nın 135. maddesinin ikinci fıkrasında yer alan “*kişilerin siyasi, felsefi veya dini görüşlerine, ırkı kökenlerine*” ilişkin bilgilerin kayıt edilmesi açısından bu ibareye yer verilmemiştir. İlgili maddedeki bu ifade ile bu türden bilgilerin kaydedilmesinin her

⁴³⁰ İtalya ve Almanya'da ise kişisel verilerin korunmasına ilişkin suçlar açısından özel kast aranmaktadır. Örneğin, İtalyan hukukunda kişisel verilerin korunmasına dair yasada hukuka aykırı olarak kişisel verilerin işlenmesi suçunun oluşabilmesi için failin kendisi veya başkası için kazanç sağlama amacıyla veya kişiye zarar vermek saikiyle hareket etmesi aranmıştır. Bkz., İtalyan Veri Koruma Kanunu, Sec. 167. İngilizce çevirisi için bkz., (Çevrimiçi) <http://www.privacy.it> (01.05.2013). TCK'da kişisel verilerin korunmasına ilişkin suçlar düzenlenirken manevi unsur bakımından da Fransız Ceza Kanunu'nda yer alan ve genel kast ile işlenebilen suçlar olarak düzenlenen kişisel verilerin korunmasına ilişkin suçlar örnek alınmıştır. Bkz., Ketizmen, **a.g.e.**, s. 204.

zaman, mutlak olarak, hukuka aykırı olduğu sonucu çıkmaktadır⁴³¹.

Kişilerin siyasal, felsefi, dini görüşleri ve ırksal kökenlerine ilişkin olmayan diğer kişisel veri türleri açısından ise “hukuka aykırı” ibaresinin açıklanması gerekmektedir. Ceza kanunlarında yer alan tüm suçlar temel olarak hukuka aykırılık vasfı taşımaktadırlar. Herhangi bir hukuka uygunluk nedeninin bulunmaması durumunda tipe uygun eylem aynı zamanda hukuka da aykırı olur⁴³². Dolayısıyla suç tipleri hukuka aykırılığın karinesini oluştururlar. Bazı hallerde ise yasakoyucu, 135. maddede yer aldığı gibi hukuka aykırılıktan özel olarak söz eder. Öğretide “hukuka özel aykırılık” olarak adlandırılan bu durumda eylemin tipe uygunluğu ile hukuka da aykırı olduğunu söylemek mümkün değildir. Bu gibi hallerde failin suçun maddi unsurlarını bilmesi ve istemesi suçun oluşması için yeterli değildir⁴³³. Failin kastının tipte yer alan diğer unsurların yanında hukuka aykırılık hallerini de içermesi aranmakta ve somut yargılamada faile herhangi bir ceza yaptırımının uygulanabilmesi için bu hususun da kanıtlanması gerekmektedir⁴³⁴.

TCK'nın 135. maddesinin ilk fıkrasında ve ikinci fıkrasında sayılan kişinin ahlaki eğilimine, cinsel yaşamına, sağlık durumuna ve sendikal bağlantılarına ilişkin veriler açısından hukuka aykırılığın suç tipinde ayrıca belirtilmesinin sebebi tipte yer alan eylemin esasında hukuka uygun da olabileceğini ifade etmek içindir. Buna göre

⁴³¹ Zeki Hafizoğulları ve Muharrem Özen, **Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar**, Ankara, US-A Yayıncılık, 2011, s. 277.

⁴³² Kayıhan İçel *et al.*, **Suç Teorisi (Suç Kavramına İlişkin Genel Bilgiler-Suçun Yapısal Unsurları-Suçun Özel Görünüş Biçimleri) 2. Kitap**, İstanbul, Beta Yay., 2000, s. 92.

⁴³³ Ahmet Emin Artuk, Ahmet Gökçen ve Ahmet Caner Yenidünya, **Ceza Hukuku Genel Hükümler**, Ankara, Turhan Kitabevi, 2007, s. 270.

⁴³⁴ İçel, **a.g.e.**, s. 111. Bu dipnot bağlamında “haksızlık yanılığı”na değinmek isteriz. TCK'nın 30. maddesinin 4. fıkrasına göre; “*işlediği fiilin haksızlık oluşturduğu hususunda kaçınılmaz bir hataya düşen kişi, cezalandırılmaz*”. Haksızlık yanılığı ile ifade edilmek istenen kişinin işlediği fiilin haksızlık oluşturduğu, meşru olmadığı hususunda hataya düşmesidir. Failin haksızlık yanılığı içerisinde bulunması, kasta etkili değildir. Haksızlık yanılığı, kusurluluğu ortadan kaldırmaktadır. Buna göre haksızlık yanılığının mevcut olduğu hallerde kişi, işlediği suç açısından kasten hareket etmektedir. Ancak bilerek ve isteyerek gerçekleştirdiği fiilin, meşru, hukuk düzenine ve davranış kurallarına uygun olduğunu tasavvur etmektedir. İşte kişinin işlediği fiilin bu şekilde, hukuka aykırı olduğunun, bir haksızlık teşkil ettiğinin bilincinde olmaması halinde, haksızlık yanılığında kaçınılmaz olması halinde kişi gerçekleştirdiği fiil dolayısıyla sorumlu tutulamaz. Bkz., Artuk-Gökçen-Yenidünya, **a.g.e.**, s. 695; İzzet Özgenç, **Türk Ceza Hukuku Genel Hükümler**, Ankara, 2008, s.414. Hukuka özel aykırılık hallerinde ise haksızlık yanılığının varlığı daha önem taşır.

genel olarak kişisel verilerin kaydedilmesi ile yukarıda ayrıca belirttiğimiz türden verilerin kaydedilmesi mevzuata uygun ise hukuka aykırı değildir⁴³⁵. *Ketizmen* de “hukuka aykırı” ibaresini inceleme konusu maddenin kaynağını oluşturan Fransız Ceza Kanunu'ndaki düzenleme ile değerlendirirken Türk mevzuatında konunun eksikliğini dile getirmiştir. Yazara göre Fransız Ceza Kanunu'nda yer alan kişisel verilerin korunmasına ilişkin suçlar eksik norm olarak düzenlenmiştir. Ayrı bir kanunla kişisel verilerin korunması düzenlenmiş ve bu kanunda gösterilen usul ve esaslara uyulmamasının yaptırım altına alınması Fransız Ceza Kanunu'na yapılan atıf ile sağlanmıştır. Ancak 135. maddede düzenlenen suç bakımından Fransız hukukunda olduğu gibi bağlantı kurulabilecek kişisel verilerin korunmasına ilişkin bir düzenleme bulunmamaktadır. Türk hukukunda kişisel verilerin korunmasına ilişkin bütüncül bir yasanın kabul edilmesine kadar maddede yer alan hukuka aykırı olarak kaydetmenin yorumlanması gerekmektedir⁴³⁶.

Özetle, maddenin birinci fıkrasında düzenlenen genel olarak kişisel verilerin kaydedilmesi ve ikinci fıkrasında düzenlenen hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kişisel veri olarak kaydedilmesi bakımından hukuka özel aykırılığın var olduğu kabul edildiği takdirde sorun, manevi unsur içerisinde değerlendirilecek; yani failin kastının hukuka aykırılığı da kapsamı gerekecektir. TCK'nın 135. maddesindeki kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin

⁴³⁵ Özbek, **a.g.e.**, s. 955; Karagülmez, **a.g.e.**, s. 400. Karşıt görüşte olan *Dülger* ise suç tipinde kullanılan “hukuka aykırı” ibaresinin yasakoyucu tarafından yalnızca hukuka uygunluk nedenlerinin varlığı konusunda hakimi uyarmak üzere kullanıldığını, bu tür hukuka aykırılığın kastın kapsamında olmasının gerekmediğini savunmaktadır. Yazara göre suç tipinde yer alan “hukuka aykırı olarak” ibaresi suçun unsurlarında herhangi bir değişiklik yapmaksızın kullanılmıştır. Bkz., *Dülger*, **a.g.e.**, s. 569. Ayrıca ceza hukukunda hukuka aykırılık hakkındaki görüşler için bkz., Tuğrul Katoğlu, **Ceza Hukukunda Hukuka Aykırılık**, Ankara, 2003. Yazara göre yasakoyucunun suçun tipinde hukuka aykırılık kavramına açıkça veya örtülü olarak atıf yaptığı ve hukuka özel aykırılık olarak adlandırılan durumların tümünün aynı olduklarını söylemek güçtür. Bu durumlar yerine göre ya özel kasıt, ya özel bir hukuka uygunluk nedeni, ya da fiilin özel bir biçimi olarak karşımıza çıkmaktadır. Her biri farklı doğalara haiz bu durumların yine kendilerine özgü bu farklı doğalarına göre değerlendirilmelerinin yapılması bir zorunluluktur. Bu anlamda bütün bu farklı hallerin öğretide tek bir başlık olan “hukuka özel aykırılık” altında toplanmaları doğru değildir. Bundan yola çıkan yazar, hukuka genel aykırılık ve hukuka özel aykırılık ayrımının kabul edilebilir bir ayırım olmadığını savunmaktadır. Katoğlu, **a.g.e.**, s. 122-126.

⁴³⁶ *Ketizmen*, **a.g.e.**, s. 235.

bilgilerin kişisel veri olarak kaydedilmesi başlı başına hukuka aykırılığın karinesini oluşturacaktır. Bu türden veriler için ise TCK'nın 24 vd. maddelerinde düzenlenen genel hukuka uygunluk nedenleri geçerli olacaktır⁴³⁷.

Hukuka uygunluk sebepleri açısından rızaya bağlı olarak verinin kaydedilmesi, hukukun genel ilkeleri gereği rızaya ilişkin iradenin şiddet, hata, hile gibi iradeyi bozan nedenlerle sakatlanmamış olması aranmaktadır. Ayrıca rızaya ilişkin irade, kişisel verilere özgü kriterlerden olan dürüstlük kuralı çerçevesinde de yorumlanmalıdır. Buna göre hangi tür kişisel verinin kaydedildiği, kayıt amaç veya amaçları ile ilgili olarak kişinin yanıltılmaması gerekmektedir. Kişinin rızasına bağlı olarak verilerin kaydedilebilmesine ilişkin önemli bir husus da kişilerin sanal ortamlarda özellikle sosyal paylaşım ağlarında kişisel verilerini paylaşımlarının bunların başkaları tarafından kullanılabileceği şeklinde bir rıza olarak kabul edilip edilemeyeceğidir. Belirtmek isteriz ki, rızanın geçerliliği ancak hangi eyleme ilişkin

⁴³⁷ Bu dipnot bağlamında 2003 tarihli TCK Tasarısı'nda ilgili suçun düzenlenmesine değinmemiz gerekir. TCK Tasarısı'nın 197 maddesinin birinci fıkrasında “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” ve son fıkrasında “Kanunun öngördüğü haller dışında, kişilerin ahlaki niteliklerini, siyasal, felsefi veya dinsel görüşleri veya ırki kökenlerine 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” hükümleri esas alınmıştır. Bu haliyle düzenleme özellikle TCK'nın 26. maddesinde düzenlenen hukuka uygunluk sebeplerinden olan ilgilinin rızasına ilişkin “kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere” hükmünün TCK Tasarısı'nın 197. maddesinin son fıkrasında düzenlenen eylemler açısından geçerli olmadığını ifade etmekteydi. Mevcut düzenlemeye baktığımızda ise genel olarak her türlü kişisel verinin hukuka aykırı olarak kaydı için 135. maddenin gerekçesinde, “Bu suçun oluşabilmesi için, kişisel verilerin hukuka aykırı bir şekilde kayda alınması gerekir. Kişinin rızası ile kendisiyle ilgili bilgilerin kayda alınmasının suç oluşturmayacağı muhakkaktır. Belirli nitelikteki kişisel verilerin kayda alınması kanun hükmünün gereği olarak yapılmaktadır. Bu bakımdan, çeşitli kamu kurumlarında verilen kamu hizmetinin gereği olarak kişilerle ilgili bazı bilgiler ilgili kanun hükümlerine istinaden kayda alınmaktadır. Bu durumlarda, söz konusu suç oluşmayacaktır” ifadesi yer almaktadır. Maddenin gerekçesi genel olarak yorumlandığında mağdurun rızası ya da kanun hükmünün yerine getirilmesinin hukuka uygunluk sebebi olarak sayılmasının hükmün birinci fıkrasının kastedildiği anlamı çıkmaktadır. Aynı maddenin ikinci fıkrasında düzenlenen hususlar için ise gerekçede, “Ancak, bunlardan kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kayda alınmasına kanunlarda özellikle suçlulukla mücadele bağlamında, suç ve suçluların ortaya çıkarılmasını sağlamak amacıyla belli ölçüde izin verilebilir. Bu durumlarda söz konusu suç oluşmayacaktır” ifadesine yer verilmiştir. Belirtilen bilgilere ilişkin verilerin hukuka aykırı olarak kaydedilmesi durumunda maddenin birinci fıkrasındaki genel kurala dönülmüştür. Ancak gerekçede ilk fıkrada geçen ifadenin aksine kişinin rızasının bir meşruluk nedeni olarak görülüp görülmeyeceğine yer verilmemiştir. Mevcut düzenleme açısından 135. maddenin ikinci fıkrasında düzenlenen eylemler açısından rızanın geçerli olup olmadığına açıkça yer verilmesi yerinde olurdu.

olduğu belirlenebilir ve açık olmasına bağlıdır. Bu anlamda kişinin kendisiyle ilgili kişisel verileri internet sayfasına koyması somut bir veri işlem faaliyetine verilen rıza anlamında değildir. Dolayısıyla olası durumda rızaya dayalı bir hukuka uygunluk nedeninin varlığı kabul edilemez⁴³⁸.

Kişisel verilerin kaydedilmesi suçu bakımından diğer bir hukuka uygunluk sebebi ise kanun hükmünün yerine getirilmesidir⁴³⁹. Buna göre eğer mevzuatta kişisel verilerin kaydedilmesine imkan veren bir hukuk kuralı bulunmakta ise kanun hükmünün yerine getirilmesinden bahisle suç oluşmayacaktır. 2006 yılında yürürlüğe giren 5490 sayılı Nüfus Hizmetleri Kanunu, yine bu Kanun ile kurulan “Merkezi Nüfus İdaresi Sistemi” (MERNİS) bireylere ait kişisel veri niteliğindeki pek çok bilginin kaydedilmesine izin vermektedir. Kanuna göre; kişilerin kimlik numaraları, ad ve soyadları, cinsiyetleri, baba ve ana adı ile soyadları, doğum yeri ile tarihleri, evlenme, boşanma, soy bağının kurulması veya reddi, vatandaşlığın kazanılması ve kaybedilmesi gibi kişisel durumda meydana gelen değişiklikler, dini, medeni hali, yerleşim yeri adresi, fotoğrafı gibi bilgiler tutulacak aile kütüklerine kaydedilebilecektir⁴⁴⁰. Kişisel verilerin hukuka uygun olarak kaydedilmesine olanak

⁴³⁸ Aksi yönde görüş için bkz., Karagülmez, **a.g.e.**, s. 400.

⁴³⁹ TCK, m. 24/f.1.

⁴⁴⁰ Bu dipnot bağlamında kişinin dinine ilişkin bilgiler üzerinde özel olarak durmamız gerekir. Aile kütüklerinde ve nüfus cüzdanlarında kişinin dininin yazılması zorunluluğu, aile kütüklerinde ve nüfus cüzdanlarında kişinin dininin yazılması zorunluluğu 1587 sayılı Nüfus Kanununda yer almaktaydı. Anayasanın “din ve vicdan özgürlüğü”nü düzenleyen 24. maddesine aykırılığı iddiasıyla iki kez Anayasa Mahkemesinin önüne götürülen bu hükmü AYM, inanç özgürlüğüne ve anayasaya aykırı bulmamıştır. Anayasa Mahkemesinin ilgili kararları için bkz. AYMK, E. 1979/9, t 27.11.1979; AYMK, E. 1995/17 K. 1995/16, t. 21.06.1995. Mahkeme, Anayasanın m.24/3'te yer alan “kimse .. .dini inancı ve kanaatlerini açıklamaya zorlanamaz” hükmünden kişilerin hangi dine bağlı olduklarının bir bilgi olarak resmi kayıtlara geçirilemeyeceğinin çıkartılamayacağını belirtmiştir. İlgili madde ile yasaklanan, kişinin dininin öğrenilmesi değil, dini inanç ve kanaatlerinin zorla açıklattırılmasıdır. Mahkemenin bu görüşüne göre kişilerin hangi dine inandıklarının salt demografik bilgi olarak öğrenilmesi, kişilerin dini inanç ve kanaatlerini açıklamaya zorlanmaları olarak değerlendirilemez. Bu gerekçelerle Mahkeme, düzenlemeyi Anayasaya aykırı bulmamış ve iptal istemini reddetmiştir. Ancak bu karara muhalif kalan üyeler söz konusu düzenlemenin kişinin iç dünyasında kalması gereken bir durumun açıklanması anlamına geldiğini, bu yasal düzenleme ile kişinin dinini nüfus idarelerine beyan ve açıklamak zorunda bırakıldığını ifade etmişlerdir. Anayasa Mahkemesi bu karardan kısa süre sonra verdiği başka bir kararda ise 1412 sayılı Ceza Muhakemeleri Usulü Kanunun tanığa yemininden önce diğer bilgilerin yanında dininin de sorulmasına ilişkin ifadeyi, kişinin isteği dışında inancının açıklaması sonucu doğuracağından bahisle Anayasanın m. 24/f.3'e aykırılıktan iptal etmiştir. Bkz., AYMK, E: 1995/25, K. 1996/5, t. 02.02.1996. Mahkemenin sonradan verdiği bu karara katılmakla birlikte kişinin dinine ilişkin bilginin nüfus cüzdanlarında yer alması ile tanığa dininin sorulması arasında kesin ayrımın yapılmış olmasını anlamak güçtür. Ayrıntılı bilgi için bkz., Küzeci,

sağlayan diğer bir düzenleme ise Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğinin Tespiti Hakkında Yönetmeliği'dir. Anılan yönetmeliğin 15. maddesine göre şüpheli veya sanığın kimlik tespiti için gerekli olması halinde fotoğrafı, iris görüntüsü, beden ölçüleri, diş izi, parmak ve avuç içi izi, bedeninde yer alan ve teşhisi kolaylaştıracak eşkal bilgileri, kulak, dudak gibi organların bıraktığı kimlik tespitine yarayabilecek vücut izleri ile sesi ve görüntüleri kayda alınarak dosyasına konur. Elde edilen bu veriler, yine aynı yönetmeliğin 17. maddesine göre, mahkumiyet kararı verilmesi halinde arşivlenir.

E. Suçun Özel Görünüş Biçimleri

1. Teşebbüs

Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu sırf hareket suçudur. Buna göre hareketin gerçekleştirilmesi yani kaydetme eylemi ile suç tamamlanmış olacaktır. Sırf hareket suçlarında netice olmadığından ya da neticenin harekete bitişik olmasından dolayı hareketin tamamlanması ancak neticenin elinde olmayan nedenlerle tamamlanmamasının mümkün olmadığı görüşü mevcuttur. Bu görüşe göre hareketin gerçekleştirilmesiyle suç tamamlanacağından bu türden suçlara teşebbüs mümkün değildir. Ancak hareketleri parçalara ayrılabilen veya hareketleri bir oluşum süreci içerisinde gerçekleşen sırf hareket suçlarında hareketlerin kişinin iradesi dışındaki nedenlerden dolayı tamamlanamaması halinde teşebbüs mümkün olabilecektir⁴⁴¹. Buna göre kişisel verilerin kaydedilmesi suçu açısından somut olayda suçun icrasının yani kaydetme eyleminin tamamlanıp tamamlanmadığının objektif ölçütten hareketle belirlenmesi gerekmektedir.

Diyebiliriz ki, salt hareket suçu niteliğinde olan kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu açısından ancak icra hareketlerinin bölünebilmesi

a.g.e., s. 326. Kaldı ki, kişinin dini inancı oldukça hassas nitelikte bir kişisel bilgi olmakta ve uluslararası metinlerde bu türdeki verilerin kayıt altında tutulmasının şartları özel olarak düzenlenmektedir.

⁴⁴¹ Nur Centel, Hamide Zafer ve Özlem Çakmut, **Türk Ceza Hukukuna Giriş**, İstanbul, Beta Yay., 2011, s. 458.

durumunda teşebbüs söz konusu olabilir⁴⁴².

2. İştirak

İnceleme konusu suç, suça iştirak bakımından bir özellik göstermemektedir. TCK'nın 37., 38., 39. ve 40. maddelerinde düzenlenen suça iştirake ilişkin genel hükümlere göre her somut olay değerlendirilecektir. Ayrıca suça iştirak edenlerin kamu görevlisi sıfatı taşıması ya da bu konuyla ilgili belli meslek sahibi veya sanat sahibi olması halinde bu kişilere ceza TCK'nın 137. maddesi gereğince arttırılarak verilecektir.

3. İçtima

Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun TCK'nın 43. maddesine göre zincirleme suç şeklinde işlenmesi mümkündür. Fail, aynı suç işleme kararının icrası kapsamında aynı kişiye ilişkin kişisel verileri farklı zamanlarda kaydedebilir. Bu durumda faile sadece bir suçun cezası verilecek ancak cezada artırıma gidilecektir. Ayrıca inceleme konusu suçun zincirleme suç şeklinde işlenmesi olasılığında suç, devam eden eylemin bittiği zaman gerçekleşmiş kabul edilecek ve zamanaşımı bu andan itibaren geçerli olacaktır.

Hukuka aykırı olarak kişisel verinin kaydedilmesi ile bu verilerin başkasına verilmesi ya da yayılması eylemleri aynı anda gerçekleştirilebilmektedir. Mağdurun rızası veya yasanın verdiği yetki haricinde kişiye ait kişisel verileri herkesin ulaşabileceği bir internet sitesine kaydedilmesi örneğinde olduğu gibi failin, tek bir fiil ile kişisel verileri hukuka aykırı olarak kaydetmesi ve başkasına vermesi ya da yayması mümkündür. Bu durumda fikri içtima kuralları uygulanarak faile daha ağır cezayı gerektiren TCK'nın 136. maddesi uyarında ceza verilecektir⁴⁴³. Ancak işverenin işyerinde çalışan işçileri cinsel eğilimlerine göre sınıflandırıp bu verileri

⁴⁴² Ali Parlar ve Muzaffer Hatipoğlu, **Açıklamalı-Yeni İctihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu**, Ankara, Seçkin Yay., 2010, s. 2090.

⁴⁴³ Özbek, **a.g.e.**, s. 958.

kayıt altına aldığı takdirde TCK 135. maddenin ikinci fıkrasında düzenlenen kişisel verilerin kaydedilmesi suçu oluşacak; bu verileri bir başka kişiye iletmesi halinde ise 136. maddede düzenlenen verileri hukuka aykırı olarak verme suçu işlenmiş olacaktır. Bu halde hem 135. maddeye hem de 136. maddeye uyan iki ayrı suç gerçekleşmiş olacak ve gerçek içtima kurallarına göre suç adedince failin cezalandırılması gerekecektir⁴⁴⁴.

F. Suça Etki Eden Sebepler

İnceleme konusu suç bakımından TCK'nın 137. maddesinde cezayı ağırlaştırıcı iki nitelikli hal düzenlenmiştir. Bunlar inceleme konusu suçun; (a) kamu görevlisi tarafından ve görevinin sağladığı yetki kötüye kullanılmak suretiyle, ve (b) belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesidir. Anılan hallerde verilecek ceza yarı oranında arttırılır.

Cezayı ağırlaştırıcı nitelikli haller bağlamında 135. maddenin ikinci fıkrasında suçun konusuna ilişkin olarak belirtilen kişisel verilere yönelik düzenlemeye değinmemiz gerekir. Yukarıda da belirttiğimiz gibi söz konusu hükümde belirtilen kişisel verilerin işlenmesi kişiler için daha ağır zarar potansiyeli taşımakta ve bu türden veriler uluslararası düzenlemelerde de hassas veriler olarak ayrı düzenlemeye tabi tutulmaktadır. Benzer şekilde 2003 tarihli TCK Tasarısı'nda da söz konusu kişisel verilerin suçun konusunu oluşturması hali ağırlaştırıcı neden olarak öngörülmüştü. Mevcut düzenlemede ise bu verilerin suçun konusunu oluşturması cezayı ağırlaştırıcı bir neden olarak öngörülmemiştir.

1. Suçun Kamu Görevlisi Tarafından ve Görevinin Sağladığı Yetki Kötüye Kullanılmak Suretiyle İşlenmesi

Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun cezanın ağırlaştırılmasını gerektiren ilk nitelikli hali, suçun kamu görevlisi tarafından ve

⁴⁴⁴ Aynı yöndeki görüşler için bkz., Malkoç, **a.g.e.**, 2201; Hafizoğulları-Özen, **a.g.e.**, s. 278.

görevinin sağladığı yetki kötüye kullanılarak işlenmesidir. Söz konusu nitelikli halin uygulanması bakımından görevin gereklerine aykırılıktan söz edildiğine göre öncelikle kötüyü kullanmayı ifade eden hareketin kamu görevlisinin görevine giriyor olması gerekmektedir. Eğer yapılan hareket kamu görevlisinin görev alanına girmiyorsa bu nitelikli halin uygulanması mümkün değildir.

“Kamu görevlisi” kavramı TCK’nın 6. maddesinin c bendinde tanımlanmıştır. Bu tanıma göre kamu görevlisi, kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli ya da geçici olarak katılan kişidir. Burada yalnızca Cumhuriyet savcısı, kolluk görevlisi, yargıç gibi kişilerin mi kamu görevlisi sayılacağı yoksa avukat, noter, bilirkişilerin de TCK’ya göre kamu görevlisi kapsamında olduğunu tanımda geçen “kamusal faaliyet” kavramının açıklanması ile cevaplayabiliriz. Yine aynı maddenin gerekçesine göre kamusal faaliyet; “*anayasa ve kanunlarla belirlenmiş olan usullere göre verilmiş olan bir siyasal kararla, bir hizmetin kamu adına yürütülmesi*” olarak tanımlanmış; bu hizmetin yürütülmesine katılan kişilerin maaş, ücret ve sair bir maddi karşılık alıp almamalarının bir öneminin bulunmadığı belirtilmiştir. Bu bakımdan TCK’ya göre kişinin kamu görevlisi sayılmasının ölçütü faaliyetin niteliğindendir. TCK’ya göre kamu görevlisi kamusal faaliyeti yerine getiren kişidir. Bu bakımdan, mesleklerinin icrası bağlamında avukat veya noter kamu görevlisi niteliği taşımaktadırlar. Keza bilirkişilik, tercümanlık ve tanıklık faaliyetinin icraası kapsamında kişinin kamu görevlisi niteliğinde olduğu kabul edilir⁴⁴⁵. Söz konusu ağırlaştırıcı nedenden bahsedilebilmesi için eylemin kamu görevlisi tarafından gerçekleştirilmesi yeterli olmayıp ayrıca görevinden kaynaklanan yetkisini kötüye kullanması aranmaktadır. Buna göre kamu görevlisi kendisine verilen görev gereği sahip olduğu yetkiye uygun davranmaması veya bu yetkinin dışında hareket etmesi gerekmektedir.

CMK’nın 81. maddesinde “fiziki kimliğin tespiti” düzenlenmekte olup, kişisel veri niteliği taşıyan kişinin fotoğrafı, beden ölçüleri, parmak ve avuç izi,

⁴⁴⁵Parlar-Hatipoğlu, a.g.e., s. 2096.

bedeninde yer alan teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntülerinin kayda alınabilmesine imkan sağlamaktadır. Ancak bunun için kişinin üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanık olması gerekmektedir. Buna göre, kişinin bu nitelikleri taşımamasına rağmen söz konusu kişisel verilerinin kaydedilmesi durumunda nitelikli halin uygulanması gerekmektedir.

Kamu görevlilerine yönelik bu türden bir cezayı ağırlaştırıcı neden olarak belirlenmesi kişisel verilerin kaydedilmesinde kişi ve kamu görevlisinin karşı karşıya geldiği zamanlarda kişinin yönetime güveninin sağlanmasına ilişkindir.

2. Suçun Belli Bir Meslek ve Sanatın Sağladığı Kolaylıktan Yararlanmak Suretiyle İşlenmesi

İnceleme konusu suçun cezasının ağırlaştırılmasını gerektiren diğer nitelikli hal ise suçun belli bir meslek veya sanatın sağladığı kolaylıktan yararlanılması suretiyle işlenmesidir. Madde hükmünde meslek veya sanatın kapsamı belirtilmemiştir. Buradaki “bir meslek ve sanat” kavramı her somut olayda değerlendirilmelidir. Bununla birlikte meslek veya sanatın icrası ile suçun işlenmesi arasında nedensellik bağının bulunması gerekmektedir. Ayrıca söz konusu meslek veya sanatın faile mağdur hakkında kişisel verilere ulaşma imkanı sağlamış olmalıdır. Örneğin, hastanede görevli ve bilgisayar ortamına girebilen bir hemşire ya da doktor burada kayıtlı hastalara ilişkin verilere; bir banka memuru da kayıtlı müşteri bilgilerine kolaylıkla ulaşabilir ve kaydedebilir⁴⁴⁶.

⁴⁴⁶ Özbek, a.g.e., s. 954. “Katılanların görevli olduğu okulda hizmetli olarak çalışan sanığın bayan öğretmenlerin kullandığı tuvalete görevinin sağladığı kolaylıktan yararlanmak suretiyle gizli kamera yerleştirdiği anlaşılmışna rağmen sanık hakkında 5237 sayılı TCK’nın 137/1-b maddesinin tatbik edilmemesi kanuna aykırıdır”. Yargıtay 12. Ceza Dairesi, 2011/ 12221 E., 2012/12232 K, t. 16.05.2012.

G. Yaptırım ve Usul

Kişisel verilerin kaydedilmesi suçunun cezası altı aydan üç yıla kadar hapis cezasıdır.

TCK'nın 139. maddesine göre kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun soruşturma ve kovuşturması şikayete tabi değildir. Buna göre 135. maddenin ilk ve ikinci fıkrası arasında bir ayırım yapılmadığından kaydedilen verilerin niteliğine bakılmaksızın suç, re'sen soruşturulan ve kovuşturulan bir suçtur. Hükümde öngörülen cezanın üst sınırı 3 yıl olduğuna göre görevli mahkeme asliye ceza mahkemesidir.

II. VERİLERİ HUKUKA AYKIRI OLARAK VERME, YAYMA VEYA ELE GEÇİRME

136. maddede kişisel verilerin yetkisiz üçüncü kişilere aktarılmasını yaptırım altına almak amacıyla bu verileri hukuka aykırı olarak verme veya yayma eylemleri; yetkisiz üçüncü kişilerin eline geçmesinin önlenmesi amacıyla bu verilerin hukuka aykırı olarak ele geçirilmesi eylemleri yaptırıma bağlanmaktadır. Buna göre kişisel verilerin dürüst ve hukuka uygun olarak işlenmesi ayrıca toplandıkları amaçlar dışında kullanılmamaları ilkeleri ceza hukukunda görünüm kazanmaktadır. Kişi hakkındaki veri ancak ilgili kişinin kendi rızası ile ya da kanunen yetkili kişilerce, bu kanun hükümleri uyarınca işlenebilir. Bu anlamda kişinin, hakkındaki verilerin kimlerin tarafından işlendiğini bilebilmesi veya öngörebilmesi gerekmektedir. Aksi durum kişinin kendisi hakkındaki verileri denetim hakkını engelleyecektir. Ayrıca günümüzde internetten müşterilerin ismi, doğum tarihi, sosyal güvenlik numaraları, kredi kartı bilgileri, kişinin haberi olmadan alınmakta ve daha sonra bu veriler ile haksız kazanç elde etmek üzere, internet dolandırıcılığı da dahil olmak üzere pek çok suç işlenmektedir. TCK'nın 136. maddesinde düzenlenen suç ile kişisel verilerin yetkisiz üçüncü kişilerin eline geçmesi, kimlik hırsızlığı olarak adlandırılan bu suç tipinin önlenmesi amaçlanmıştır.

A. Suçla Korunan Hukuksal Değer

TCK'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçunda korunan hukuksal değer ile bu suç tipiyle korunan hukuksal değer aynıdır⁴⁴⁷. Buna göre bu suç tipiyle genel olarak kişilerin özel hayatının gizliliği hakkı ve 2010 tarihli anayasa değişiklikleri ile ayrı bir hak alanı olarak anayasal temele kavuşan kişisel verilerin korunması hakkı korunmaktadır.

B. Maddi Unsur

1. Suçun Konusu

Kişisel verileri hukuka aykırı olarak verme, ele geçirme veya yayma suçu ile 135. maddede düzenlenen kişisel verileri kaydetme suçunun konusu aynıdır. Buna göre bu suçun konusunu kişisel veriler oluşturmaktadır⁴⁴⁸.

2. Fail ve Mağdur

Madde metninde suçu işleyecek kişi açısından herhangi bir özellik belirtilmemiştir. Bu haliyle söz konusu suçun faili herkes olabilir. Ancak bu suçu işleyenin kamu görevlisi olması TCK'nın 137. maddesi açısından cezayı ağırlaştırıcı sebep olarak öngörülmüştür. O halde failin kamu görevlisi olması halinde verilecek ceza tayin edilirken TCK'nın 137. maddesi dikkate alınacaktır.

Kişisel verileri verme ve ele geçirme suçunda herkes suçun mağduru olabilmektedir. Ancak bu suç tipi açısından da TCK 135. maddesinde mağdura ilişkin açıklamalarımızda yer alan kişisel verinin “gerçek kişiyle ilgili her türlü bilgi” olarak tanımlanmasının kabul edilmesi halinde mağdurun gerçek kişi olabileceği geçerlidir. Bu anlamda mağdurun tayini açısından gerçek veya tüzel kişi ayrımının netlik kazanması için kişisel verinin tanımını yapan bütüncül yasanın bir an önce kabul

⁴⁴⁷ Geniş açıklama için 135. maddede düzenlenen suçla korunan hukuksal değere dair açıklamalarına bakılmalıdır.

⁴⁴⁸ Ayrıntılı bilgi için 135. maddede konu açısından yapılan geniş açıklamaya bakınız.

edilmesinin önemini bir kere daha belirtmek isteriz. Suçun mağduru olabilmek için kaydedilen verinin maliki ya da zilyedi olmaya gerek yoktur. Ele geçirilen verinin mağdur ile ilgili olması yeterlidir.

3. Hareket

TCK'nın 136. maddesinde kişisel verilerin hukuka aykırı olarak başkasına verilmesi, yayılması veya ele geçirilmesi eylemleri suç olarak düzenlenmiştir.

İnceleme konusu suç tipinde yer verilen kişisel verilerin başkasına verilmesi yazılı verilerin elden veya posta yoluyla verilmesi veya sanal ortamda bulunan kişisel verilerin bir cd-rom üzerine kaydedilmesi ya da internet üzerinden elektronik posta yoluyla gönderilmesi şeklinde olabilir. Kişisel verilerin yayılması bu verilerin yazılı olarak birden fazla kişiye gönderilmesi veya internet üzerinden bu verilerin web sitesi aracılığıyla başkaları için erişilebilir kılınması şeklinde olabilir. Yine yazılı, görsel ya da sanal basın yolu ile de kişisel verilerin yayılması eylemi gerçekleştirilebilir. Kişisel verilerin ele geçirilmesi, bu verilerin üzerinde yazılı olduğu belgelerin alınması şeklinde olabileceği gibi kişisel verilerin elektronik ortamdan veya bir bilişim sistemine girerek buradan alınması şeklinde olabilir. Belirtmemiz gerekir ki inceleme konusu maddede geçen “başkası” kelimesi, gerçek kişi olabileceği gibi bir tüzel kişi de olabilmektedir. TCK'nın 136. maddesinde aksi yönde bir sınırlandırma yoktur⁴⁴⁹.

İnceleme konusu suç tipi seçimlik hareketli bir suçtur. Suçun maddi unsuru olarak belirtilen verme, yayma veya ele geçirme eylemlerinden biri veya birkaçı aynı anda gerçekleştirildiği takdirde tek bir suç işlenmiş sayılacak ve faile tek bir ceza verilecektir⁴⁵⁰.

⁴⁴⁹ Karagülmez, **a.g.e.**, s. 402.

⁴⁵⁰ *Malkoç* da TCK'nın 136. maddesinde düzenlenen suçun seçimlik hareketli suç niteliği taşıdığını belirtmek ile birlikte birden çok seçimlik hareketi gerçekleştirenin TCK'nın 61. maddesi uyarınca cezası belirlenirken alt sınırdan uzaklaşılması gerektiğini belirtmiştir. Bkz., *Malkoç*, **a.g.e.**, s. 2201.

Başkasına verilen, yayılan ya da ele geçirilen verilerin daha önceden hukuka uygun olarak kaydedilmiş olup olmamasının suçun oluşması açısından bir önemi bulunmamaktadır⁴⁵¹. Buna göre, daha önceden kişisel verinin kaydedilmesinin hukuka uygun olup olmaması ilgili madde açısından önem teşkil etmemektedir. İnceleme konusu suç tipi ile kişisel verilerin yetkisiz üçüncü kişilerce ele geçirilmesi önlenmek istenmiştir. Bu doğrultuda kişisel verileri daha önceden kaydedilmiş olsun veya olmasın hukuka aykırı olarak vermek, yaymak veya ele geçirmek 136. madde hükmü gereğince suç teşkil edecektir.

136. maddesinde kişisel verilerin başkasına verilmesi, yayılması ve ele geçirilmesi eylemleri suç teşkil eden eylemler olarak sayılmış fakat bu verilerin “açıklanması” eylemine yer verilmemiştir. Bu noktada Kişisel Verilerin Korunması Kanunu Tasarısı'nın da değerlendirilmesi gereklidir. Tasarı'nın 34. maddesinin 3. fıkrasında ise yayma, verme, aktarma gibi eylemlerin yanında “açıklama” eylemine de yer verilmiş ve bu gibi hallerde TCK 136. maddenin uygulanacağı belirtilmiştir. Diyebiliriz ki mevcut düzenleme ile kişisel verilerin açıklanması eylemi TCK 134. maddenin kapsamına girmemektedir. Bu anlamda Tasarı'nın 34. maddesi yukarıda belirttiğimiz şekliyle kanunlaşınca kadar kişisel verilerin açıklanması eyleminin TCK'nın 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilmesi gerekecektir⁴⁵².

4. Netice

Maddede kişisel verilerin başkasına verilmesi, yayılması ve ele geçirilmesi eylemleri neticesinde bir zararın meydana gelmesi gerekmemektedir. Maddede sayılan bu eylemlerin yapılmasıyla suç gerçekleşmiş olacaktır. Buna göre maddede tanımlanan eylem tehlike suçunu oluşturmaktadır.

⁴⁵¹ Aynı doğrultuda maddenin gerekçesi şöyledir; “*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*”.

⁴⁵² Akyürek, **a.g.e.**, s. 203.

C. Manevi Unsur

İnceleme konusu suçun manevi unsuru bilerek ve isteyerek genel suç işleme kastıdır. Failin suçu bilerek ve isteyerek işlemesi istendiğinden, taksirle işlenmesi mümkün değildir. Madde metninde hukuka özel aykırılık hali bulunduğundan, failin kastında eyleminin hukuka aykırı olduğunu bilmesi ve istemesi de aranmaktadır. Sadece suç işlediğini bilmesi yetmeyip, gerçekleştirdiği eylemi ve sonuçlarını istemesi kastın varlığı için gerekmektedir.

D. Hukuka Aykırılık

Madde metninde “*kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi...*” şeklindeki düzenlemeden anlaşılacağı üzere hukuka özel aykırılık hali aranmaktadır. Yani failin yargılanması esnasında, yaptığı eylemin hukuka aykırı olduğunu bilerek ve isteyerek hareket edip etmediği araştırılmaktadır.

Hukuka aykırılığı ortadan kaldıran bazı durumlar vardır. Mağdurun, yani verinin sahibi ya da ilgisinin rızası söz konusuysa, verinin ele geçirilmesi, yayılması, başkasına verilmesi suç oluşturmaz. Aynı şekilde yasanın verdiği yetkiye dayanarak, görevli bir kişinin bu eylemi gerçekleştirmesi yasaya aykırı olmayacaktır.

CMK'nın 80. maddesinin 1. fıkrası hükmünde bu kanunun 75., 76. ve 78. madde hükümlerine göre şüpheli veya sanığın veya diğer kişilerin vücudu üzerinde dış veya iç beden muayenesi yapılması ve vücutlarından kan ve benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınması veya bu işlemlerle elde edilen örnekler üzerinde moleküler genetik incelemeler yapılmasına ilişkin olup, bir suçla ilgili delil elde etmek için yapılan bu inceleme sonuçları, kişisel veri niteliğinde olduğundan bunlar başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez. Bu hükme aykırı olarak anılan kişisel verileri başkasına veren, yayan veya ele geçiren kişilerin eylemi

TCK'nın 136. maddesine uyan suçu oluřturur⁴⁵³.

E. Suçun Özel Görünüş Biçimleri

1. Teşebbüs

Kişisel verileri hukuka aykırı olarak verme, yayma ve ele geçirme suçu sırf hareket suçu olmakla birlikte somut olaya göre kişisel verileri verme, yayma ve ele geçirme parçalara ayrılabiliyorsa teşebbüsün gerçekleşmesi düşünülebilir. Örneğin, önceden reklam veya ilan verilip açıklamaya başlanırken engellenme, açıklama belgelerinin yayınlanmak veya bir başka yere ulaştırılmak üzere gönderilmesinde belgelere postada el konulması ya da ulaşmadan geri verilmesi halinde suçun teşebbüs halinde kaldığının kabulü gereklidir⁴⁵⁴.

2. İştirak

Suçta iştirak açısından bir özellik söz konusu olmayıp TCK'nın 37., 38., 39. ve 40. maddelerinde düzenlenen suçta iştirake ilişkin genel hükümlere göre her somut olay değerlendirilecektir.

Ayrıca suçta iştirak edenlerin kamu görevlisi sıfatı taşıması ya da bu konuyla ilgili belli meslek sahibi veya sanat sahibi olması halinde bu kişilere ceza, TCK'nın 137. maddesi gereğince arttırılarak verilecektir.

3. İçtima

İnceleme konusu suçun aynı suç işleme kastıyla kişisel verilerin birkaç kez yayılması, başkasına verilmesi örneklerinde olduğu gibi zincirleme şeklinde işlenmesi mümkündür.

⁴⁵³ Parlar-Hatipoğlu, **a.g.e.**, s. 2093.

⁴⁵⁴ Malkoç, **a.g.e.**, s. 2202.

Suçun mütemadi şekilde işlenmesi de mümkündür. Bu durumda suç, devam eden eylemin bittiği zaman gerçekleşmiş kabul edilecek ve zamanaşımı bu andan itibaren geçerli olacaktır.

İçtima konusuna dair bir diğer husus ise TCK'nın 243. maddesinde düzenlenen “hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu” ile 136. maddedeki inceleme konusu suç tipi arasındaki ilişkidir. Günümüzde kişisel veriler özellikle bilişim sistemlerinde kaydedilip bu ortamlarda tutulmaktadır. Bu anlamda birçok olayda kişisel verilerin başkasına verilmesi, yayılması ya da ele geçirilmesi için öncelikle bilişim sistemine hukuka aykırı olarak girilmesi ve orada hukuka aykırı kalınması gerekecektir. Bu olası durumlar 243. maddenin 136. madde açısından bir geçit suçu olup olmadığı değerlendirmesini gündeme getirir. Diyebiliriz ki 243. maddede düzenlenen suçun 136. maddede düzenlenen suç açısından geçit suçu oluşturmamaktadır. Geçit suçundan bahsedebilmemiz için ilk suç işlenmeden ikincisinin işlenmesinin mümkün olmaması gerekmektedir ve suçların aynı hukuksal değeri koruması gerekmektedir⁴⁵⁵. Olası duruma döndüğümüzde ise, kişisel verilerin ele geçirilmesi için bunların mutlaka bilişim sisteminde kayıtlı olması gerekmemektedir. Ayrıca her iki suç tipinin koruduğu değerler de farklıdır⁴⁵⁶. Bu

⁴⁵⁵ Kayıhan İçel, “Görünüşte Birleşme (İçtima) İlkeleri ve Yeni Türk Ceza Kanunu”, **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, S. 14, 2008/2, s. 47.

⁴⁵⁶ TCK'nın 243. maddesinde düzenlenen yetkisiz erişim suçu ile korunmak istenen hukuksal değer ile ilgili doktrinde çeşitli görüşler ileri sürülmüştür. Bu görüşler özel hayat alanı, mülkiyet hakkı, malvarlığı kapsamında şekillenmektedir. Kurt'a göre sistem ve içinde bulunan verilerin, programların sistem sahibinin özel alanında bulunması ile ilişkilidir. Yazara göre, bu suç ile özel alana girilmesi suretiyle güvenlik ve sükun duygusunun sarsılması önlenmeye çalışılmıştır. Yine yazara göre, ilgili suç sistemde bulunan verilerin elde edilmesi gibi bir unsuru barındırmadığından, mülkiyet hakkı korunan hukuki yarar değildir. Ancak maddenin 3. fıkrasındaki suçun ağırlaştırıcı nedeni olarak düzenlenen suç işlendiğinde, yani sistemin içerdiği veriler yok edilir veya değiştirilirse mülkiyet hakkı da korunan hukuki değer haline gelecektir. Ayrıntılı bilgi için bkz., Levent Kurt, **Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara, Seçkin Yay., 2005, s. 148. Bıçkın'a göre ise, 243. maddede düzenlenen suçla korunan hukuksal değer karma bir özellik göstermektedir. Anılan madde ile ilk olarak bireyin özel hayatı korunmaktadır. İkinci fıkrada ise malvarlığı da korunan hukuksal değerlerden sayılabilir çünkü burada bedel karşılığında yararlanılabilen sistemler ile ilgili suçun işlenmesi hali düzenlenmiştir. Ayrıntılı bilgi için bkz., İnci Bıçkın, “Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları”, **Ankara Barosu Bilişim ve Hukuk Dergisi**, Ocak-Mart 2006, s. 68. Genel yaklaşım ise bilişim alanında işlenen suçların konusunu oluşturan hareketler arasında önem derecesine göre bir sıralamaya gidilmiş, yetkisiz erişim önem derecesi bakımından en alt sırada yer alırken en önemli hususun sistemin bozulması olduğu ifade edilmiştir. Bu haliyle 243. maddedeki düzenleme malvarlığının korunmasına ilişkin bir düzenlemedir ve özel hayatın korunmasına ilişkin değerler ikinci plana itilmiştir. Ayrıntılı

bilgiler ışığında diyebiliriz ki bir bilişim sistemine girerek oradaki kişisel verileri ele geçiren kişi bakımından hem 243. maddenin hem de 136. maddenin uygulanması gerekecektir⁴⁵⁷.

TCK'nın 135. maddesinde düzenlenen kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu ile 136. maddede düzenlenen suç açısından da suçların içtiması söz konusu olabilecektir⁴⁵⁸. Buna göre TCK'nın 135. maddesinin de göz önünde bulundurulması ve iki ayrı suç oluşup oluşmadığının değerlendirilmesi gereklidir⁴⁵⁹.

Suçların içtimasına örnek verilebilecek bir diğer olası durum ise kişisel verilerin açıklanmasının aynı zamanda TCK'nın 125. maddesinde düzenlenen hakaret suçunu da oluşturmasıdır. Bu durumda bir eylem ile birden fazla suçun neden olduğundan bahisle fail en ağır cezayı gerektiren suçtan sorumlu olacaktır. Böyle bir olası durumda faile kişisel verilerin açıklanması suçunun cezasının daha fazla olmasından dolayı ilgili suçtan ceza verilecektir⁴⁶⁰.

F. Suça Etki Eden Sebepler

TCK'nın 137. maddesinde failin sıfatından kaynaklanan ağırlaştırıcı nedenler öngörülmüştür. Buna göre inceleme konusu suçun; (a) kamu görevlisi tarafından ve görevinin sağladığı yetki kötüye kullanılmak suretiyle, ve (b) belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesidir. Anılan hallerde verilecek ceza yarı oranında arttırılır.

G. Yaptırım ve Usul

Kişisel verileri hukuka aykırı olarak başkasına verme, yayma ve ele geçirme suçu açısından bir yıldan dört yıla kadar hapis cezası öngörülmüştür. Suçun, kamu

bilgi için bkz., Ketizmen, **a.g.e.**, s. 89 vd.

⁴⁵⁷ Dülger, **a.g.e.**, s. 595.

⁴⁵⁸ Aynı yönde görüş için bkz., **a.g.e.**, s. 595; Parlar-Hatipoğlu, **a.g.e.**, s. 2090.

⁴⁵⁹ Geniş açıklama için 135. maddede düzenlenen suçun içtimasına dair açıklamalarına bakılmalıdır.

⁴⁶⁰ Dülger, **a.g.e.**, s. 596.

görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, verilecek ceza TCK'nın 137. maddesi uyarınca yarı oranında arttırılır.

TCK'nın 140. maddesi uyarınca, bu suçun işlenmesi dolayısıyla tüzel kişiler hakkında TCK'nın 60. maddesinde gösterilen güvenlik tedbirleri uygulanacaktır.

TCK'nın 139. maddesine göre ilgili suçun soruşturma ve kovuşturması şikayete tabi değildir. Hükümde öngörülen cezanın üst sınır 4 yıl olduğuna göre görevli mahkeme asliye ceza mahkemesidir.

III. VERİLERİN YOK EDİLMEMESİ SUÇU

Kişisel verilerin korunmasına ilişkin olarak TCK'da yer alan diğer bir suç ise kişisel verilerin yok edilmemesidir. Söz konusu suçun düzenlendiği 138. madde şöyledir;

“Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir.”

İlgili madde ile verileri yok etmekle yükümlü olanların görevlerini ihmal etmeleri yaptırım altına alınarak kişisel verilere her an ulaşılabilirliğin önüne geçilmeye çalışılmıştır.

Kişiler zaman içerisinde birtakım sebeplerden dolayı kişisel bilgilerini vermek zorunda kalabilirler. Kişisel verilerin dürüstlük kurallarına ve hukuka uygun olarak toplanmış olması, bu verilerin toplandıkları sistemde süresiz olarak tutulması anlamına gelmemektedir. Aksi halde kişi, kendisine ait bu verilerin başkalarının bilgisinde olmasından ötürü güvensizlik duyabilecektir. Ayrıca, kişisel verilerin işlenmesi özel hayatın gizliliğini sınırlayan bir durumdur. Bu halde kişisel veriye ihtiyaç duyulmaması halinde verinin yok edilmesi veya ilgili kişiyle olan doğrudan

ya da dolaylı bağlantısının ortadan kaldırılması gerekmektedir. Meşruiyetini bireysel ve toplumsal ihtiyaçtan alan bu istisnai durum için söz konusu bireysel ve toplumsal ihtiyaç kalktığı takdirde müdahalenin meşruiyeti de kalkmaktadır⁴⁶¹. Bu durum çoğulcu, özgürlükçü ve demokratik devletin gerekliliklerine aykırıdır ve toplumun da aynı doğrultuda bu çağdaş ilkelere bağlılığını engeller. Kaldı ki kişisel verilerin amaca uygun toplanması ilkesinin uzantısı olarak kişisel verilerin işlenmesinde özellikle keyfiliğin önlenmesi amacıyla bu toplanma amacının ortadan kalkması veya amacın gerçekleşmesi sonucunda kişisel verilerin bulundukları sistemlerden kaldırılması gerekmektedir.

Kişisel verilerin süresiz olarak tutulmaması gerekliliği amaçla bağlılık ilkesi ile de ilişkilidir. İşte, TCK'nın 138. maddesinde düzenlenen suç tipi ile hukuka uygun olarak toplanan kişisel verilerin sürekli olarak sistemde bulunması ve her an ulaşılabilirliğinin sağlanması engellenmek suretiyle çoğulcu, demokratik ve özgürlükçü devlet modeli pekiştirilmeye çalışılmıştır.

A. Suçla Korunan Hukuksal Değer

Verilerin yok edilmemesi suç tipiyle iki farklı hukuksal değer korunmaktadır. Buna göre bu suç tipiyle genel olarak kişilerin özel hayatının gizliliği hakkı ve 2010 tarihli Anayasa değişiklikleri ile ayrı bir hak alanı olarak anayasal temele kavuşan kişisel verilerin korunması hakkı korunmaktadır. Böylece, kişilerin sürekli olarak kendilerine ait verilerin kaydedilmesi sonucu fişlenmiş şekilde yaşamalarının önüne geçilmek istenmektedir.

İnceleme konusu suç ile korunan diğer bir hukuksal değer ise kamu görevinin yerine getirilmesiyle bundan sağlanacak kamu yararının elde edilmesidir. Verileri yok etmekle görevli kişinin bunu yapmaması kamu görevinin yerine getirilmesinde gereken disiplini bozmaktadır. Bu koruma sayesinde kamuya olan güven duygusu ve

⁴⁶¹ Ketizmen, **a.g.e.**, s. 240.

kamu yönetimin güvenilirliği güçlendirilmeye çalışılmaktadır⁴⁶².

B. Maddi Unsur

1. Suçun Konusu

İnceleme suçun konusunu kişisel veriler oluşturmaktadır. Yukarıda incelenen kişisel verilerin kaydedilmesi ve hukuka aykırı olarak verme, yayma ve ele geçirme suçlarındaki konu ile tamamen aynı olduğundan konu ile ilgili yapılan açıklamalar bu suç tipi açısından da geçerlidir.

Burada dikkat edilmesi gereken nokta bu suç tipi açısından yalnızca otomatik yolla işlenen verilere ilişkin olup olmadığıdır. 138. maddede “verileri sistem içinde yok etmek”ten söz edilmesidir. Ancak yukarıda incelenen kişisel verilerin kaydedilmesi ve hukuka aykırı olarak verme, yayma ve ele geçirme suçlarında ise bu ifadeye yer verilmemiştir. Bu noktada 138. maddede geçen “sistem”in bilişim veya otomatik sistemleri ifade ettiğinin kabulü, ilgili maddenin genel olarak otomatik işlemeye tabi olan kişisel verilere ilişkin olduğu izlenimini yaratmaktadır. Yukarıda incelediğimiz kişisel verilerin korunması açısından ise kişisel verilerin otomatik işleme tabi tutulup tutulmaması yönünden bir ayrıma gidilmemiştir. Bu durum maddeler arasında çelişki yaratmaktadır. Bunun giderilmesi ve maddeler arasında uyumun sağlanması için verilerin yok edilmesi açısından sistemde bulunmaya ilişkin şartın maddeden çıkartılması gerekmektedir⁴⁶³.

⁴⁶² TCK'nın 257. maddesinin ilk fıkrasında “görevi yerine getirmeme”, ikinci fıkrasında ise “görevi ihmal suçu” düzenlenmiştir. Anılan suç tiplerinin düzenlendiği her iki fıkra hükmünde de “*kanunda ayrıca suç olarak tanımlanan haller dışında*” ifadesine yer verilmiştir. Bu anlamda anılan suç tiplerinin genel nitelikte oldukları kabul edilmiş, bunun dışındaki görevi yerine getirmeme ve görevi ihmal suçlarının başka maddelerde özel eylemler açısından düzenlenebileceği belirtilmiştir. TCK'nın 138. maddesinde düzenlenen verilerin yok edilmemesi suçu da böyle bir görevi yerine getirmeme ve görevi ihmal suçudur. Bkz., Dülger, **a.g.e.**, s. 597. Ayrıca bu dipnot bağlamında düzenlenen suç tipi ile kamu yararının sağlanması amaçlansa da kişisel verileri sistemden yok etmekle görevli kişinin kamu görevlisi sıfatını taşımasının gerekmediğini belirtmek isteriz.

⁴⁶³ Ketizmen, **a.g.e.**, s. 242.

2. Fail ve Mağdur

Suçun faili “*verileri sistem içinde yok etmekle görevli olan*” kişidir. Bu düzenlemeye göre bu suç bir özgü suçtur. Kimlere hangi kapsamda veriyi yok etme görevi verildiği ilgili özel kanunlara ve her somut olaya göre ayrıca tespit edilecektir. Her ne kadar düzenlenen suç tipi ile kamu yararının sağlanması amaçlansa da verileri sistem içinde yok etmekle görevli olan kişinin kamu görevlisi olması zorunlu değildir⁴⁶⁴. Fail bir kamu görevlisi olabileceği gibi bir meslek ve sanat sahibi de olabilir. Bu nedenle yasakoyucu yukarıda incelediğimiz diğer suçlar bakımından kabul ettiği TCK'nın 137. maddesindeki cezayı ağırlaştıran nitelikli unsurları bu suç bakımından öngörmemiştir⁴⁶⁵. Bu durum özellikle kişisel verilerin korunmasına dair bütüncül bir yasanın kabulü ile birlikte ilgili bu yasada kişisel verileri yok etme türünden görevlerin verilmesi halinde önemlidir.

TCK 138. maddenin mağduru kişisel verileri yok edilmeyen kişidir. Verilerin yok edilmemesi suçu işlendiğinde kamu idaresine duyulan güven kırılacağından bu suçun mağduru aynı zamanda kamu olacaktır⁴⁶⁶.

3. Hareket

Kişisel verileri yok etmeme suçu bir “gerçek ihmali suç”tur. Yasal yükümlülük altında kişisel verileri yok etmekle yükümlü olanların ihmalen bunu yerine getirmediklerinde suç gerçekleşmiş olur. Verilerin yok edilmemesinin nasıl gerçekleştirileceği ise söz konusu görevin verildiği düzenlemede gösterilecektir.

⁴⁶⁴ Maddede hukuka uygun olarak kaydedilmiş kişisel verilerden söz edilmesi nedeniyle, kanunlarda kendisine böyle bir yükümlülük yüklenen kişi, sıfatı ister kamu görevlisi isterse gerçek kişi olsun, bu suçun faili olabilecektir. Fakat, özel hukuka yönelik hukuka uygun müdahalelerle kişisel verilerin kaydedilmesi, kamu düzeninin korunması amacıyla ve özellikle adli kovuşturmalarda delil elde edilmesi amacıyla gerçekleştirildiğinden verileri yok etmeme suçunun faili çoğu kez kanunda sıfatı belirlenen kamu görevlileridir. Bkz., Parlar-Hatipoğlu, **a.g.e.**, s. 2099.

⁴⁶⁵ Özbek, **a.g.e.**, s. 965.

⁴⁶⁶ Dülger'e göre ise bu suçun mağduru belli bir birey değildir. Yazara göre bu suç tipiyle kamu idaresine duyulan güven korunmak istendiğinden suçun mağduru kamu olacaktır. Kendisi ile ilgili kişisel verileri yok edilmeyen kişi ise suçtan zarar gören kişi olacak ve suçla ilgili olarak yapılan yargılamada müdahil sıfatıyla bulunabilecektir. Bkz., Dülger, **a.g.e.**, s. 598.

Verilerin kısmen veya tamamen yok edilmesi ise somut olaya göre değerlendirilmelidir. Buna göre kişisel verinin kısmen yok edilmesi halinde kalan kısım hala bir kişiye doğrudan veya dolaylı olarak ilişkilendirilebiliyorsa suç gerçekleşmiş olacaktır.

138. maddede düzenlenen ihmalî harekete bazı özellikler yüklenmiştir. Buna göre tipte yer alan ihmalî hareketin gerçekleşmiş sayılması bakımından (i) kanunların belirlediği sürelerin geçmiş olması ve, (ii) failin verileri sistem içinde yok etmekle görevli olması gereklidir. Failin yerine getirmediği yok etme göreviyle yükümlü olup olmadığının anlaşılması için 138. maddedeki kanun terimi geniş yorumlanmalı ve idarenin herhangi bir düzenleyici işlemiyle bir verinin belirli bir süre sonra yok edilmesinin öngörülüp öngörülmediğine de bakılması gereklidir⁴⁶⁷.

4. Netice

Suçun oluşması için kişinin kişisel verileri sistem içinde yok etme yükümlülüğünü kasten yerine getirmemiş olması yeterlidir. Bu ihmalî davranışın sonucunda ayrıca herhangi bir neticenin meydana gelmesi suçun oluşması için zorunlu değildir⁴⁶⁸. Kanunda belirtilen sürelerin sonunda verileri yok etme eyleminin gerçekleştirilmesi gereklidir. Bu sürenin geçmesine rağmen veriler yok edilmediği takdirde suç gerçekleşmiş olacaktır.

Yok etme, veriyi geri getirilemeyecek şekilde tümüyle ortadan kaldırmayı ifade eder. Ancak veri kısmen yok edildiği takdirde verinin kalan kısmının veri niteliği taşıyıp taşımadığına bakılması gerekir. Yok edilmeyen kısım kişisel veri niteliğini devam ettirdiği takdirde 138. maddedeki suç oluşur⁴⁶⁹.

Verileri yok etmekle görevli kişi açıkça bu işlemi gerçekleştirmeyeceğini söylemişse ya da bunun bir emirle kendisine bildirilmesi halinde amirin emrini

⁴⁶⁷ Özbek, **a.g.e.**, s. 965; Karagülmez, **a.g.e.**, s. 411.

⁴⁶⁸ Parlar-Hatipoğlu, **a.g.e.**, s. 2100.

⁴⁶⁹ Karagülmez, **a.g.e.**, 412.

yerine getirmeyeceğini ifade etmesi halinde de bu sürenin geçmesine gerek olmaksızın suç gerçekleşmiş olacaktır⁴⁷⁰.

İnceleme konusu suçun oluşabilmesi için “kanunların belirlediği sürelerin geçmiş olması” ölçütü esas alınmıştır. Amaçla bağlılık ilkesinin gereği olarak işlenme amacının ortadan kalktığı ya da ilgili amacın gerçekleşmesi sonucunda kişisel veriye ihtiyacın kalmaması halinde kişisel veriler yok edilmelidir. Ancak 138. maddede kişisel verilerin işlenme amacının ortadan kalkması veya bu amacın gerçekleşmiş olmasına karşın bu verilerin yok edilmemesine yer verilmemiş, bu verilerin yalnızca kanunların belirlediği sürelerin geçmiş olmasına rağmen yok edilmemesi esas alınmıştır⁴⁷¹. Düzenleme bu haliyle toplanma amacı ortadan kalkmış ya da gerçekleşmiş olsa dahi kişisel verilerin sırf kanunlarda belirlenen sürenin geçmemesinden dolayı saklanabilmesine olanak tanımaktadır. Her ne kadar kişisel verilerin toplanılmasına dair bir “süre sınırı” getirilerek keyfiliğin önüne geçilmeye çalışılmış ise de bu ölçüt ile amaçla bağlılık ilkesinin bağlantısı tam kurulamamaktadır.

Maddede yer verilen “kanunda belirtilen süre” sınırı yalnızca kesin bir zaman dilimi değildir. Örneğin, CMK'nın 81. maddesinin 2. fıkrasına göre şüpheli veya sanığın fizik kimliğinin saptanması için tutulan fotoğrafı, parmak izi gibi kayıtlar; itirazın reddi, beraat gibi bazı durumlarda Cumhuriyet savcısının huzurunda derhal yok edilmelidir. Bu kurala uygun hareket etmeyen memurun TCK 138. maddeye göre cezai sorumluluğu doğacaktır⁴⁷².

C. Manevi Unsur

Verileri yok etmeme suçunun manevi unsuru genel suç işleme kastıdır. Buna göre suçun kanuni tanımındaki maddi unsurların fail tarafından bilinmesi ve istenmesi suçun oluşması için yeterlidir.

⁴⁷⁰ Dülger, **ag.e.**, s. 600.

⁴⁷¹ Ketizmen, **a.g.e.**, s. 241.

⁴⁷² Özbek, **a.g.e.**, s. 965.

D. Hukuka Aykırılık

Verileri yok etmeme suçu, kişisel verilerin kaydedilmesi ve kişisel verileri hukuka aykırı olarak verme ele geçirme suçlarından farklı olarak mağdurun rızasını hukuka uygunluk sebebi olarak görmemektedir. Mağdur aynı zamanda kamu düzeni olduğundan, mağdurun rızası eylemi hukuka uygun hale getirememektedir. Ayrıca bu suç tipi açısından kanundan kaynaklanan bir hukuka uygunluk sebebi de bulunmamaktadır. Aynı şekilde süre aşıldıktan sonra kişisel verileri yok etmekle yükümlüler tarafından verilerin yok edilmesi de eylemi hukuka uygun yapmaz.

E. Suçun Özel Görünüş Biçimleri

1. Teşebbüs

İnceleme konusu suç tipi ihmal suretiyle işlenebilmektedir. Bundan dolayı bu suçun gerçekleştirilmesine yönelik eylemlerin teşebbüs derecesinde kalması mümkün değildir⁴⁷³.

2. İştirak

Suçta iştirak açısından bir özellik söz konusu olmayıp TCK'nın 37., 38., 39. ve 40. maddelerinde düzenlenen suça iştirake ilişkin genel hükümlere göre her somut olay değerlendirilecektir. Bu suç tipi açısından TCK'nın 39. maddesinin 2. fıkrasının b bendinde yer alan “suçun nasıl işleneceği hususunda yol göstermek veya fiilin işlenmesinde kullanılan araçları sağlamak” ile c bendinde yer alan “suçun işlenmesinden önce veya işlenmesi sırasında yardımda bulunarak icrasını kolaylaştırmak” suça iştirak çeşitlerinin gerçekleşmesi pek mümkün değildir⁴⁷⁴. Ayrıca inceleme konusu suç, kişisel verileri yok etme yükümlülüğü olan görevlilerce işlenebilen özgü suç niteliğinden dolayı, böyle bir yükümlülüğü bulunmayan kimseler bu suça şerik sıfatıyla iştirak edebilirler.

⁴⁷³ Özgenç, **a.g.e.**, s. 435.

⁴⁷⁴ Dülger, **a.g.e.**, s. 602.

3. İçtima

Fail, hukuka uygun olarak kaydedilmiş olan kişisel veriler kanunda belirlenen sürelerin geçmiş olmasına karşın yok etmediği gibi bu kişisel verileri örneğin hukuka aykırı olarak başkasına verir veya yaydığı takdirde 136. ve 138. maddelere uyan iki ayrı suç oluşacağından gerçek içtima kurallarının uygulanması gerekir.

F. Suça Etki Eden Sebepler

138. maddede bu suçla ilgili cezanın ağırlştırılmasına veya daha az ceza verilmesini öngören herhangi bir hükme yer verilmemiştir.

G. Yaptırım ve Usul

İnceleme konusu suçun failine uygulanacak ceza, altı aydan bir yıla kadar hapis cezasıdır.

TCK'nın 140. maddesi uyarınca bu suçun işlenmesinden tüzel kişilerin hukuka aykırı yarar sağlaması halinde bunlara TCK'nın 60. maddesinde gösterilen tüzel kişilere özgü güvenlik tedbirleri uygulanacaktır.

TCK'nın 139. maddesine göre kişisel verileri yok etmeme suçunun soruşturma ve kovuşturması şikayete tabi değildir. Bu suç re'sen soruşturulan ve kovuşturulan bir suçtur. Hükümde öngörülen cezanın üst sınırı bir yıl olduğuna göre görevli mahkeme sulh ceza mahkemesidir.

SONUÇ

Bilişim ve iletişim teknolojilerinin gelişimi, küreselleşmenin etkileri ve bu iki dinamiğin oluşturduğu küresel ağlar zamanımıza damgasını vuran bilgi toplumu dönüşümüne yol açmıştır. Bilgi, artık bir erdem olmaktan çıkıp bir meta halini almıştır. Burada kimliği belirli veya belirlenebilen bir kişiye ait tüm bilgiler olarak ifade edilen kişisel verilerin akıbeti ve bu türden verilerin korunmasına çözüm bulunmasına dair tartışmalar gündeme gelmiştir. Nitekim veriye kimin sahip olduğu, bunların kimler tarafından nasıl kullanılacağı sorusu bu tartışmaların merkezini oluşturmaktadır.

Kişisel verilerin işlenmesini etkin kılan bilişim ve iletişim teknolojilerinin sunduğu olanaklarla bu veri işleme faaliyetlerindeki çeşitlilik artmıştır. Ayrıca bilginin artık bir güç olarak nitelendirildiği günümüzde kişisel verilere yönelik kamu kurumlarının ve özel teşebbüslerin açlığı artmıştır. Bu noktada bireyin veri işlem faaliyetleri kapsamında geri planda tutulması bireyin kişiliğini koruması, geliştirmesi, bireysel özerklik ve insan onuru gibi çok geniş yelpazede sorunlara yol açabilmektedir. Burada kişiye tekrardan kendisine ilişkin verilerin geleceğini belirleme hakkını sağlayan kişisel verilerin korunması hakkı ile küresel düzeye erişmiş bilgi akışının karşısında kişi temel hak ve özgürlüklerinin dengelenmesi amaçlanmıştır.

Bu düşüncelerden hareketle 1960'lı yıllardan itibaren kişisel verilerin korunması tartışılmış, 1970'li yıllarda ise ilk ulusal düzenleme örnekleri verilmiştir. Bunları takiben bilgi akışının önlenemez hızı ve küresel nitelik kazanması konunun OECD, BM, AK ve AB gibi önemli uluslararası ve ulusüstü kuruluşlar nezdinde ele alınmasına neden olmuştur. Halen daha bu kuruluşlar daha etkin bir korumanın sağlanması için araştırma ve çalışmalarını sürdürmektedirler.

Bilgi toplumuna geçmeyi hedefleyen ülkemizde, uluslararası yaklaşımın aksine, kişisel verilerin korunması yeni tartışılmaya başlanan bir konudur. İnsan

haklarına saygılı, demokratik bir hukuk devleti olma idealindeki Türkiye açısından da kişisel verilerin korunmasına yönelik bir düzenlemeye gidilmesi bir zorunluluk halini almıştır. Ayrıca Türkiye'nin Avrupa Birliği'ne aday ülke olmasından kaynaklanan Avrupa Birliği müktesebatına uyum çalışmaları da unutulmamalıdır. Bu noktada kişisel verilerin korunmasına ilişkin suçlara bazı ülkeler kişisel verilerin işlenmesine dair usul ve esasların belirlendiği kanunlarda yer vermiş bazı ülkeler ise bu suçlar genel ceza kanunlarında düzenlenmiştir. Türk Ceza Hukuku'nda ise ikinci yöntem tercih edilmiş ve 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu ile 765 sayılı mülga TCK'dan farklı olarak kişisel verilerin korunmasına ilişkin suçlara 135 vd. maddelerinde yer verilmiştir.

Suçun hukuki konusu bakımından incelendiğinde 135 vd. maddelerinde kişisel veriler güvence altına alınmıştır. Ancak çalışmamızda birçok defa belirttiğimiz gibi kişisel veri kavramının Türk hukukunda henüz yasal olarak tanımlanmamış olması anılan maddelerde düzenlenen suçların uygulama alanını belirsizleştirmektedir. Şüphesiz ki düzenleme bu haliyle ceza hukukunun önemli ilkelerinden biri olan kanunilik ilkesine aykırıdır. Keza kişisel veri kavramının tanımlanmaması nedeniyle, çalışmamızda yer verdiğimiz Yargıtay Ceza Dairesi içtihatlarından da görüleceği üzere, uluslararası yaklaşımın aksine kişinin ses ve görüntüleri kişisel veri kapsamında değerlendirilmemektedir. Bu durum 135 vd. maddelerinin somut olaylarda neden pek fazla uygulanamadığına en açık örnektir.

Bir diğer tartışma konusu ise 135. maddede yer alan hassas veri kategorilerine ilişkindir. İlgili maddede yer verilen veri türleri uluslararası ölçekte diğer veri türlerine göre işlenmesinin kişi açısından daha ağır tehlikelere yol açabileceği savunulan hassas veri kategorilerindendirler. Ancak bunlara yönelik özel koruma getirilmesi gerekliliği dikkate alınmayarak genel olarak kişisel verilerin kaydedilmesi ile aynı yaptırıma tabi tutulmaları eleştirilmiştir.

Yine aynı maddeden devam edecek olursak burada yer verilen “hukuka aykırı olarak” kaydetmenin niteliği yönünden de farklı görüşler ileri sürülmüştür. Kanımızca, 135. maddenin birinci fıkrasında düzenlenen genel olarak kişisel verilerin kaydedilmesi ve ikinci fıkrasında düzenlenen hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kişisel veri olarak kaydedilmesi bakımından hukuka özel aykırılığın var olduğu kabul edildiği takdirde sorun, manevi unsur içerisinde değerlendirilecek; yani failin kastının hukuka aykırılığı da kapsamı gerekecektir. TCK'nın 135. maddesindeki kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin bilgilerin kişisel veri olarak kaydedilmesi başlı başına hukuka aykırılığın karinesini oluşturacaktır. Bu türden veriler için ise TCK'nın 24 vd. maddelerinde düzenlenen genel hukuka uygunluk nedenleri geçerli olacaktır.

Çalışmamızda belirttiğimiz gibi kişisel verilerin koruması açısından önemli olan bir kriter de veri işleme faaliyetinin amaçla bağlı olması, işlenme amacının ortadan kalktığı ya da ilgili amacın gerçekleşmesi sonucunda kişisel veriye ihtiyacın kalmaması halinde kişisel veriler yok edilmesi gerektiğidir. Bu noktada çalışma konumuzu oluşturan suç tiplerinden TCK'nın 138. maddesi gündeme gelmektedir. Çalışmamızın üçüncü bölümünde incelediğimiz gibi ilgili maddedeki suçun oluşabilmesi için “kanunların belirlediği sürelerin geçmiş olması” ve buna rağmen kişisel verilerin sistemden silinmemiş olması gerekir. Düzenleme bu haliyle toplanma amacı ortadan kalkmış ya da gerçekleşmiş olsa dahi kişisel verilerin sırf kanunlarda belirlenen sürenin geçmemesinden dolayı saklanabilmesine olanak tanımaktadır. Her ne kadar kişisel verilerin toplanılmasına dair bir “süre sınırı” getirilerek keyfiliğin önüne geçilmeye çalışılmış ise de bu ölçüt ile amaçla bağlılık ilkesinin bağlantısı tam kurulamamaktadır.

Bütün bunların yanında 2010 yılında yapılan Anayasa değişikliği ile “Özel Hayatın Gizliliği” başlıklı 20. maddesine eklenen fıkra ile getirilen kişisel verilerin korunmasına ilişkin özel hükmün Türkiye'de kişisel verilerin korunması için önemli

bir adım olduğunu belirtmemiz gerekmektedir. Böylece kişisel verilerin korunması hakkı normatif olarak da anayasal bir niteliğe kavuşturulmuştur.

Gerçek ve etkin bir koruma için yalnızca TCK'nın 135 vd. maddeleriyle yetinilmemesi gerekmektedir. Bu anlamda mevzuatın bilişim ve iletişim teknolojilerinin gelişimine ve hukuk devleti ilke ve normlarına uygun, hem ulusal hem de uluslararası düzenlemelerle tutarlı olması gerekmektedir. Ayrıca gelişimin yalnızca teknolojik değil insani boyutu da atlanmamalıdır. Kişisel verilerin korunmasının tam anlamıyla sağlanabilmesi için bireylerin bilinçlendirilmesi gerekmektedir.

Sonuç olarak vurgulanmalıdır ki, TCK'nın 135 vd. maddelerinde kişisel verileri koruyan bir düzenlemenin bulunması önemli bir aşamadır. Ancak kişisel veri kavramının henüz yasal olarak tanımlanmamış olması ve kişisel verilerin işlenmesine ilişkin çeşitli kanunlardaki dağınık hükümler bir yana bırakılacak olursa, halihazırda kişisel verilerin işlenmesi usul ve esaslarının yer aldığı özel bir kanunun bulunmaması söz konusu hükümlerin uygulanabilmesinde sorunlara ve belirsizliğe yol açmaktadır. Aynı doğrultuda temel hak ve özgürlüklerin kanunla düzenlenmesi gerektiği de gözetilerek çalışma konumuzu oluşturan suçlar açısından hukuka uygunluk sebebi oluşturabilecek yasal düzenlemelerin geç kalınmadan yapılması gerekmektedir. Bu anlamda halen daha başbakanlıkta bulunan Kişisel Verilerin Korunması Kanunu Tasarısı'nın eleştirilen yanları gözden geçirilerek kanunlaşması gerekmektedir.

KAYNAKÇA

I- KİTAP VE MAKALELER

- Akyürek, Güçlü **Özel Hayatın Gizliliğini İhlal Suçu**, Ankara, Seçkin Yay., 2011.
- Aksoy, Hüseyin Can **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Ankara, Çakmak Yay., 2010.
- Araslı, Oya **Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi**, Ankara, 1979 (yayınlanmamış doçentlik tezi).
- Artuk, Ahmet Emin
Gökçen, Ahmet
Yenidünya, Ahmet Caner **Ceza Hukuku Genel Hükümler**, Ankara, Turhan Kitabevi, 2007.
- Atak, Songül *“Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler”*, **Türkiye Barolar Birliği Dergisi**, S.87, 2010, s. 90-120.
- Bartow, Ann *“Our Data, Ourselves: Privacy, Propertization and Gender”*, **University of San Francisco Law Review**, C. 34, 2000, s. 633-704.
- Başalp, Nilgün **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin Yay., 2004.
- Battcock, Rupert *“Data Protection: Where Next?”*, **International Journal of Law and Informational Technology**, C.3, 1995, s. 156-178.
- 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, 2000, s. 71-114.

- Bıçkın, İnci “Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları”, **Ankara Barosu Bilişim ve Hukuk Dergisi**, Ocak-Mart 2006, s. 65-74.
- Bing, Jon “The Council of Europe Convention and the OECD Guidelines on Data Protection”, **Michigan Yearbook of International Legal Studies**, C.5, 1984, s. 271-304.
- Bozkurt, Veysel “Gözetim ve İnternet: Özel Yaşamın Sonu Mu?”, **Birikim Dergisi**, S.136, 2000.
- Bygrave, Lee A. “Privacy and Data Protection in an International Perspective”, **Scandinavian Studies in Law**, 2010, S.56, s. 166-200.
- 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.
- Carey, Peter **Data Protection A Practical Guide to UK and EU Law**, Büyük Britanya, Oxford University Press, 2004.
- Cate, Fred “The Changing Face of Privacy Protection in the European Union and the United States”, **Indiana Law Review**, C. 33, 1999-2000, s. 173-232.
- Centel, Nur
Zafer, Hamide
Çakmut, Özlem **Türk Ceza Hukukuna Giriş**, İstanbul, Beta Yay., 2011.
- Charlesworth, Andrew “Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?”, **Hastings Law Journal**, C.54, 2002-2003, s. 931-969.
- Clarke, Roger “Beyond OECD Rules: Privacy Protection for the 21st Century”, (Çevrimiçi) <http://www.rogerclarke.com/DV/PP21C.html>, 01.05.2013.

- Clarke, Roger
“Dataveillance: Delivering '1984'”, February 1993, (Çevrimiçi)
<http://www.rogerclarke.com/DV/PaperPopular.html>, 01.05.2013.
- Dedeoğlu, Gözde
“Gözetleme, Mahremiyet ve İnsan Onuru”, **TBD Bilişim Dergisi**, 2004, (Çevrimiçi)
<http://dergi.tbd.org.tr>, 01.05.2013.
- Dural, Mustafa – Sarı, Suat
Türk Özel Hukuku Cilt I Temel Kavramlar ve Medeni Kanunun Başlangıç Hükümleri, İstanbul, Filiz Kitabevi, 2006.
- Dülger, Murat Volkan
Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, Seçkin Yay., 2012.
- Goold, Benjamin J.
Lazarus, Liora
Security and Human Rights, Portland, 2007.
- Gözübüyük, A. Şeref
Gölcüklü, Feyyaz
Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, Ankara, Turhan Kitabevi, 2009.
- Gür, İkbâl
Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları, Ankara, Turhan Kitabevi, 2010.
- Hafızoğulları, Zeki
Özen, Muharrem
Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, Ankara, US-A Yayıncılık, 2011.
- Hustnix, 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, Berlin, 2009, (Çevrimiçi)
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2009/09-06-08_Berlin_DP_Lisbon_Treaty_EN.pdf, 01.05.2013.
- İçel, Kayıhan
“Görünüşte Birleşme (İçtima) İlkeleri ve Yeni Türk Ceza Kanunu”, **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, S. 14, 2008/2, s. 35-49.

- İçel, Kayıhan et al., **Suç Teorisi (Suç Kavramına İlişkin Genel Bilgiler-Suçun Yapısal Unsurları-Suçun Özel Görünüş Biçimleri) 2. Kitap**, İstanbul, Beta Yay., 2000.
- Jori, Andreas "dataprotection.eu", (Çevrimiçi) <http://www.dataprotection.eu>, 01.05.2013.
- Kang, Jerry *"Information Privacy in Cyberspace Transactions"*, **Stanford Law Review**, C.50, 1998, s. 1193-1294.
- Karagülmez, Ali **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Ankara, Seçkin Yay., 2013.
- Katoğlu, Tuğrul **Ceza Hukukunda Hukuka Aykırılık**, Ankara, Seçkin Yay., 2003.
- Kaya, Cemil *"Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi"*, **İÜHFİM**, C. LXIX, S. 1-2, s. 317-334.
- Ketizmen, Muammer **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Adalet Yay., 2008.
- Korff, Douwe **EC Study on Implementation of Data Protection Directive-Comparative Summary of National Laws**, Cambridge, 2002.
- Korff, Douwe **Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons**, Study Contract ETD/97/B5-9500/78.
- Kurt, Levent **Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara, Seçkin Yay., 2005.
- Küzeci, Elif **Kişisel Verilerin Korunması**, Ankara, Turhan Kitabevi, 2010.
- Lyon, David **Günlük Hayatı Kontrol Etmek, Gözetlenen Toplum**, çev. Gözde Soykan, İstanbul, Kalkedon Yay., 2006.

- Malkoç, İsmail **Açıklamalı-İçtihatlı 5237 sayılı Yeni Türk Ceza Kanunu, (Madde 82–149), C. II, Ankara, 2013.**
- Marx, Garry T. “Privacy and Technology”, January 1996, (Çevrimiçi) <http://web.mit.edu/gtmarx/www/privantt.html>., 01.05.2013.
- Mayer-Schönberger, Viktor *“Beyond Privacy, Beyond Rights-Toward a 'Systems' Theory of Information Governance”*, **California Law Review**, C. 98, 2010, s. 1853-1885.
- Metin, Yüksel *“Avrupa Birliği Temel Haklar Şartı”*, **Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi**, C.57, S.4, 2002, s. 35-63.
- McCullagh, Karen *“Data Sensivity: resolving the conundrum”*, **Journal of International Commercial Law and Technology**, C. 2, S. 4, 2007, s. 190-201.
- Oğuzman, Kemal
Barlas, Nami **Medeni Hukuk (Giriş, Kaynaklar, Temel Kavramlar)**, İstanbul, Filiz Kitabevi, 2008.
- Özbek, Veli Özer **Yeni Türk Ceza Kanunun Anlamı (TCK İzmir Şerhi), (Madde 76-169), C. II, Ankara, 2008.**
- Özbudun, Ergun *“Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği”*, **Ankara Üniversitesi Hukuk Fakültesi Dergisi 50.Yıl Armağanı**, C.1, Ankara, 1977, s. 265-296.
- Özdemir, Hayrunnisa **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Ankara, Seçkin Yay., 2009.
- Özgenç, İzzet **Türk Ceza Hukuku Genel Hükümler**, Ankara, Seçkin Yay., 2008.
- Özön, Mustafa Nihat **Osmanlıca-Türkçe Sözlük**, İstanbul, İnkılap ve Aka Yay., 1979.

Parlar, Ali
Hatipoğlu, Muzaffer

Açıklamalı-Yeni İçtihatlarla 5237 Sayılı Türk Ceza Kanunu Yorumu, Ankara, Seçkin Yay., 2010.

Prins, Corien

“When Personal Data, Behavior and Virtual Identities Become A Commodity: Would A Property Rights Approach Matter?”, **SCRIPT-ed A Journal of Law, Technology and Society**, C.3, S.4, 2006, s. 270-303.

Samuelson, Pamela

“Privacy as Intellectual Property”, **Stanford Law Review**, C.52, 2000, s. 1125-1173.

Schwartz, Paul M.

“European Data Protection Law and Restrictions on International Data Flows”, **Iowa Law Review**, S. 80, 1994-1995

Schwartz, Paul M.

“Property, Privacy and Personal Data”, **Harvard Law Review**, S.117, 2003-2004, s. 2055-2128.

Sırabaşı, Volkan

İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (İnternet Rejimi), Ankara, Adalet Yayınevi, 2003.

Simitis, Spiros

“From the Market to the Polis: The EU Directive on Protection of Personal Data”, **Iowa Law Review**, C.80, 1994, s. 445-469.

Simitis, Spiros

“Reviewing Privacy In an Information Society”, **University of Pennsylvania Law**, C. 740, 1986-1987, s. 707-746.

Simitis, Spiros

“Revisiting Sensitive Data”, (Çevrimiçi) http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Simitis_1999.pdf, 01.05.2013.

Solove, Daniel J.

The Digital Person Technology and Privacy in the Information Age, ABD, New York University Press 2004.

Soykan, Cavidan

“Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C.56, S. 2, s. 63-74.

- Şen, Ersan “5237 sayılı TCK'da Özel Hayata Karşı Suçlar”, **İstanbul Barosu Dergisi**, C. 79, S.3, 2005, s. 707-720.
- Şimşek, Oğuz **Anayasa Hukukunda Kişisel Verilerin Korunması**, İstanbul, Beta Yay., 2008.
- Tezcan, Durmuş “Bilgisayar Karşısında Özel Hayatın Korunması”, **Anayasa Yargısı Dergisi**, C.8, 1991, s. 385-392.
- Üzeltürk, Sultan **1982 Anayasası ve İnsan Hakları Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı**, İstanbul, Beta Yay., 2004.
- Üzeltürk, Sultan “Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği”, **Legal Hukuk Dergisi**, C.8, S.93, 2010, s. 3151-3156.
- Walden, Ian “Anonymising Personal Data”, **International Journal of Law and Information Technology**, C.10, S.2, 2002, s. 224-237.
- Walden, I.N.- Savage, R.N. “Data Protection and Privacy Laws: Should Organisations Be Protected?”, **International and Comparative Law Quarterly**, C. 37. S. 22, 1988, s. 337-347.
- Warren, Samuel D.
Brandeis, Louis D. “The Right to Privacy”, **Harvard Law Review**, S. 5, 15.11.1890, s. 193-220.
- Wong, Rebecca “All Alternative Approaches to Sensitive Data”, **Journal of International Commercial Law and Technology**, C.2, S.1, s.9-16
- Wong, Rebecca
Savirimuthu, Joseph “All or Nothing: The Application of Article 3.2 of the Data Protection Directive 95/46/EC to the Internet”, **John Marshall J. Computer & Info. L.**, S. 211, 2008.
- Yüksel Civelek, Dilek “Kişisel Verilerin Korunması ve Kurumsal Yapılanma Önerisi”, (Çevrimiçi) http://www.bilgitoplumu.gov.tr/Documents/1/tezler/Kisisel_Verilerin_Korunmasi-Dilek_Civelek-DPT_Uzmanlik_Tezi.pdf, 01.05.2013.

II- GÖRÜŞ, ARAŞTIRMA VE RAPORLAR

Article 29 Data Protection
Working Party

First orientations on Transfers of PersonalData to Third Countries-Possible Ways Forward in Assesing Adequacy, XV D/5020/97, EN final WP 4, 26.06.1997.

Article 29 Data Protection
Working Party

Opinion 4/2007 on the Concept of Personal Data,, 01248/07/EN, WP 136, 20.06.2007

Article 29 Data Protection
Working Party

Opinion 5/2009 on online social networking, 01189/09/EN WP 163, 12.06.2009.

Article 29 Data Protection
Working Party

Opinion 15/2011 on the definition of consent, 01197/11/EN WP187, 13.07.2011.

Article 29 Data Protection
Working Party

Working Document on transfer of personal data to third countries: Applying Articles 25 and 26 of The EU data protection directive, 2093/05/EN, WP 12, 24.07.1998.

Article 29 Data Protection
Working Party

Working Document on 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, 03.06.2003.

Article 29 Data Protection
Working Party

Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 2005, 2093/05/EN, WP 114, 25.11.2005.

Article 29 Data Protection
Working Party

Working Party on Police and Justice, The Future of Privacy: Joint contribution to the Consultation of the European Commision on the legal framework for the fundamental right to protection of personal data, WP 168, 01.12.2009.

European Parliament's
Committee on Civil Liberties

Justice and Home Affairs Towards a New EU Legal Framework for Data Protection and Privacy Brussels, 2011, (Çevrimiçi) www.ceps.eu/ceps/dld/6351/pdf, 01.05.2013.

For the Informational
Commissioner by the
Surveillance Society Network

A Report on the Surveillance Society, haz. David Murakami Wodd, Eylül 2006.

Parliamentary Assembly of
the Council of Europe

Right to Privacy, Resolution No. 1165(1998).

The Consultative Committee of
the Convention for
the Protection of Individuals
with Regard to
Automatic Processing of
Personal Data [ETS no. 108]

Modernisation of Convention 108, (Çevrimiçi) [http://www.coe.int/t/dghl/standardsetting/dataprtection/TPD_documents/TPD\(2012\)4Rev3E%20-%20Modernisation%20of%20Convention%20108.pdf](http://www.coe.int/t/dghl/standardsetting/dataprtection/TPD_documents/TPD(2012)4Rev3E%20-%20Modernisation%20of%20Convention%20108.pdf), 01.05.2013.

The Council of
the European Union

Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008.

The Royal Academy of
Engineering

Dilemmas of Privacy and Surveillance, Challenges of Technological Change, Mart 2007.

Working Party on
Information Security and
Privacy

Ministerial Declaration on the Protection of Privacy of Global Networks, Ottawa, 1998.

III- YARARLANILAN BAŞLICA İNTERNET SİTELERİ

95/46/AT sayılı Veri Koruma Direktifi <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

2002/58/AT sayılı Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunması Direktifi <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML>

AB Temel Haklar Şartı http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Avrupa Adalet Divanı Kararları http://curia.europa.eu/jcms/jcms/j_6/

Avrupa İnsan Hakları Mahkemesi Kararları <http://www.echr.coe.int/>

Avrupa Konseyi Sözleşmeleri <http://www.conventions.coe.int/>
BM Rehber İlkeleri <http://www.unhchr.ch/html/menu3/b/71.htm>

Kişisel Verilerin Korunması Kanunu Tasarısı
<http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Kanuntas/kisiselveriler.pdf>

OECD Rehber İlkeleri
<http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>